Netsparker

5/10/2022 4:03:43 PM (UTC+05:00)

Detailed Scan Report

https://www.hawkamah.org/

Scan Time	5/10/2022 3:54:49 PM (UTC+05:00)
Scan Duration	00:00:07:17
Total Requests	: 1,905
Average Speed	: 4.4r/s

Risk Level:
HIGH

29
IDENTIFIED

11
CONFIRMED

0
CRITICAL

2
HIGH

5
MEDIUM

9
LOW

6
BEST PRACTICE

7
INFORMATION

Identified Vulnerabilities

Critical	0
High	2
Medium	5
Low	9
Best Practice	6
Information	7
TOTAL	**29**

Confirmed Vulnerabilities

Critical	0
High	1
Medium	1
Low	5
Best Practice	0
Information	4
TOTAL	**11**

Vulnerability Summary

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	Out-of-date Version (Moment.js)	GET	https://www.hawkamah.org/events	
	Session Cookie Not Marked as Secure	GET	https://www.hawkamah.org/status-check	
	HTTP Strict Transport Security (HSTS) Errors and Warnings	GET	https://www.hawkamah.org/	
	Out-of-date Version (jQuery UI Autocomplete)	GET	https://www.hawkamah.org/	
	Out-of-date Version (jQuery UI Dialog)	GET	https://www.hawkamah.org/	
	Out-of-date Version (jQuery UI Tooltip)	GET	https://www.hawkamah.org/	
	Weak Ciphers Enabled	GET	https://www.hawkamah.org/	
	[Possible] Cross-site Request Forgery	GET	https://www.hawkamah.org/	
	[Possible] Cross-site Request Forgery in Login Form	GET	https://www.hawkamah.org/	
	[Possible] Phishing by Navigating Browser Tabs	GET	https://www.hawkamah.org/	
	Missing X-Frame-Options Header	GET	https://www.hawkamah.org/	
	Autocomplete is Enabled	GET	https://www.hawkamah.org/	
	Cookie Not Marked as HttpOnly	GET	https://www.hawkamah.org/	
	Cookie Not Marked as Secure	GET	https://www.hawkamah.org/status-check	
	Insecure Frame (External)	GET	https://www.hawkamah.org/	
	Internal Server Error	POST	https://www.hawkamah.org/subscribe	

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	Content Security Policy (CSP) Not Implemented	GET	https://www.hawkamah.org/	
	Expect-CT Not Enabled	GET	https://www.hawkamah.org/	
	Missing X-XSS-Protection Header	GET	https://www.hawkamah.org/	
	Referrer-Policy Not Implemented	GET	https://www.hawkamah.org/	
	SameSite Cookie Not Implemented	GET	https://www.hawkamah.org/status-check	
	Subresource Integrity (SRI) Not Implemented	GET	https://www.hawkamah.org/	
	[Possible] Login Page Identified	GET	https://www.hawkamah.org/	
	Apache Web Server Identified	GET	https://www.hawkamah.org/	
	Generic Email Address Disclosure	GET	https://www.hawkamah.org/contact-us	
	Autocomplete Enabled (Password Field)	GET	https://www.hawkamah.org/	
	Forbidden Resource	GET	https://www.hawkamah.org/js/?hTTp://r87.com/n	
	OPTIONS Method Enabled	OPTIONS	https://www.hawkamah.org/	
	Robots.txt Detected	GET	https://www.hawkamah.org/robots.txt	

1. Out-of-date Version (Moment.js)

HIGH | 1

Netsparker identified that the target web site is using Moment.js and detected that it is out of date.

Impact

Since this is an old version of the software, it may be vulnerable to attacks.

Moment.js Uncontrolled Resource Consumption Vulnerability

The moment module before 2.19.3 for Node.js is prone to a regular expression denial of service via a crafted date string, a different vulnerability than CVE-2016-4055.

Affected Versions

0.3.0 to 2.19.2

CVSS

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

External References

- CVE-2017-18214

Vulnerabilities

1.1. https://www.hawkamah.org/events

Identified Version

- 2.18.1

Latest Version

- 2.29.2

Vulnerability Database

- Result is based on 04/29/2022 20:00:00 vulnerability database content.

Certainty

Request

```
GET /events HTTP/1.1
Host: www.hawkamah.org
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Connection: Keep-Alive
Cookie: 10+20+cmd|' /C calc'!A0; _pps=eyJpdiI6Ikhlb0lHZnAxUWRpcEh1MzI4enorenc9PSIsInZhbHVlIjoiUEQwT0
56T3pOek5zMDZ1NEJaMXJ3Zz09IiwibWFjIjoiNjUwODRmMTEwODA5MDY4MWE2MzczMTI0NDk2YWJkZTIwZTE1Njg1Nzg0Y2UwYz
VjNzFjNTY5MmJmNTdiNTRjZCJ9; MCPopupClosed=yes; XSRF-TOKEN=eyJpdiI6IlNVTWh5N09BVHBST1lqYWhFNFc3Z1E9PS
IsInZhbHVlIjoiVVdFMWd5VWVyeHlvOHUzQ0xwU21XWVBIN0I3eGlwQlJQMW9JVndWM1JCYlNGTFwvTlJtV3B6aENHenBqRGZ4d0
tRbVZ4K2RtUzc2dWxZWHZOb2ZpNXd3PT0iLCJtYWMiOiI5ODA4OWUyYzEyYjM4NzlmN2U0ZWIxMjJjODYxZDQxNmJlZjNiMTA4Mj
JlMzJlZWI1ODU3ZGE1N2U3NjAyMDZmIn0%3D; laravel_session=eyJpdiI6ImlmV0pRYVFOdjNGdkZEdXRzaFR1OFE9PSIsIn
ZhbHVlIjoiN3JVdjY1QzFaQlBpcEhPRjUxNFhGOGhJNlppYWlnanNaRXdjVlEzWURuY2cyd0VPRzJ6ZlRxYkxEOVJ3dU9FSXdpdj
NHTFFHWDV3TXFrYm9yMXJnVFE9PSIsIm1hYyI6ImMxNjU2NzE2MjY4MmMzNWFlM2VlZWE5ZWI3NjczYWMwYTcyMjg5MDQ3OTNiOT
hlZDcwZTZlMWFkMmZmOWQzYzMifQ%3D%3D
Referer: https://www.hawkamah.org/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
```

Response

Response Time (ms) : 2238.9695 Total Bytes Received : 67152 Body Length : 66036 Is Compressed : No

```
HTTP/1.1 200 OK
Set-Cookie: XSRF-TOKEN=eyJpdiI6IithUzVCbkxDcHZ6SXRFcUYwT1FWbGc9PSIsInZhbHVlIjoiZFRvemIxOEZTSHRKT0pvY
jdkanduN2ZxRWV4R3JOMzQrNzdBOGZQcldjWlRlQkZudjJjMDJFUDJZbFVTTTlBRFZNU1pBb1J4cjR1VEFuWTlFWjJnOGc9PSIsI
m1hYyI6IjYxZDg3NjBiNWU3ZDEzNThiMmRkYjBiZGJhZDNiM2VmNmIxZGU4N2FlNTkxZTdmZmI2Njg5YWQ5MTE3MDU4ODkifQ%3
D%3D; expires=Tue, 10-May-2022 12:56:30 GMT; Max-Age=7200; path=/
Set-Cookie: laravel_session=eyJpdiI6ImZTb1U2SzhMcUFoNmM5NG8yWkkxTlE9PSIsInZhbHVlIjoieW5EN0R0Y1pWVytu
NmM2QUZLckw3anEzQTlwbzU1SUliSEJIXC95VkJkT0tIdWhHZWVYY1FoUmdWWjl6OWRTaU9rdHRQQTZRemtcL1dJdmhsSnlaTnRY
UT09IiwibWFjIjoiMmNiZDgzOWM4YzI1YjY1MGFiZmI3MjkyNjhjODM3MDg4ZDc2ZTRlNWI3YTQ2OTM5MmQyOTU3NGI1MWZiMTVk
OCJ9; expires=Tue, 10-May-2022 12:56:30 GMT; Max-Age=7200; path=/; HttpOnly
Server: Apache
Expires: Tue, 10 May 2022 10:56:31 GMT
Vary: Accept-Encoding
Keep-Alive: timeout=5, max=98
Content-Length: 13126
Strict-Transport-Security: max-age=31536000; includeSubDomains
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
Content-Encoding:
Date: Tue, 10 May 2022 10:56:30 GMT
Cache-Control: no-cache, max-age=1

<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=n
o">
<link rel="icon" type="image/png" href="https://www.hawkamah.org/images/favico.png">
<title>Hawkamah |       Events
</title>
<style>
.do-mainloader{ position: fixed; display:block; width: 100%; height: 100%; background-color: #fff; z
-index: 999; background-image: url(https://www.hawkamah.org/images/mainloader.gif); background-repea
t: no-repeat; background-position: center;}
</style>
<link href="https://www.hawkamah.org/css/all.css?v1.2" rel="stylesheet" type="text/css">
<style>
.fc-row .fc-content-skeleton tr td .fc-hover {
top:0px!important;
height: calc(100%)!important;
}
.fc-day-grid-event .fc-title {
font-size: 11px!impo
…
```

Remedy

Please upgrade your installation of Moment.js to the latest stable version.

Remedy References

- Downloading Moment.js

CLASSIFICATION

PCI DSS v3.2	6.2
OWASP 2013	A9
OWASP 2017	A9
CWE	937, 1035
CAPEC	310
HIPAA	164.308(A)(1)(I)
ASVS 4.0	1.14.3
NIST SP 800-53	CM-6
DISA STIG	6.6.2
OWASP Proactive Controls	C1
ISO27001	A.14.1.2

2. Session Cookie Not Marked as Secure

HIGH 1 CONFIRMED 1

Netsparker identified a session cookie not marked as secure, and transmitted over HTTPS.

This means the cookie could potentially be stolen by an attacker who can successfully intercept the traffic, following a successful man-in-the-middle attack.

It is important to note that Netsparker inferred from the its name that the cookie in question is session related.

Impact

This cookie will be transmitted over a HTTP connection, therefore an attacker might intercept it and hijack a victim's session. If the attacker can carry out a man-in-the-middle attack, he/she can force the victim to make an HTTP request to your website in order to steal the cookie.

Vulnerabilities

2.1. https://www.hawkamah.org/status-check

CONFIRMED

Identified Cookie(s)

- laravel_session

Cookie Source

- HTTP Header

Request

```
GET /status-check HTTP/1.1
Host: www.hawkamah.org
Accept: */*
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Connection: Keep-Alive
Cookie: 10+20+cmd|' /C calc'!A0; XSRF-TOKEN=eyJpdiI6IlBoZlB2emVwWkd0K2JOM2FncHFBYWc9PSIsInZhbHVlIjoi
RkN3NVRMYjRXWlJcL0hrVGV4MG81dnc1K1lYeDYxaENZQmhYckx5bUZ5bkc1T2x0aUx2bURRWDd0UDVaanJwb0RLWXBabGFcL2Rm
Z25iNUxZTHlHOVwvaWc9PSIsIm1hYyI6ImMyMDk3Y2VlNjIyNjg0MTY3MjYzNWVkZjk0OWYwNmNmYWQ3MDUxNDA1NGFjZTUxNmI2
ZDAwYTIyMWVjNjczZDkifQ%3D%3D; laravel_session=eyJpdiI6Img1dzJtdUhINVNXeDBnZm05a1RMa1E9PSIsInZhbHVlIj
oiUG5QbDM3OUdUdnFWWG5BS0U1SzNXcEJ1WUxBZFZaV25tRUJmbjYzdTNKQWkrSGoycjR3bVdcL1NZVks0WTd3SkhyUTZpTU9Ebl
RzcFwvZVowV2Y2UW9LUT09IiwibWFjIjoiNjFmYzA5NjUzNGM2NmExMDUyMGM1OWQ4OGE2OWM5MjY2ZTVlNmY5ZDMyZWNiODY1OW
RmMDQwZjRiNTBmNDJhYiJ9
Referer: https://www.hawkamah.org/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
X-Requested-With: XMLHttpRequest
```

Response

Response Time (ms) : 849.8372 Total Bytes Received : 1301 Body Length : 1 Is Compressed : No

```
HTTP/1.1 200 OK
Set-Cookie: _pps=eyJpdiI6Ikhlb0lHZnAxUWRpcEh1MzI4enorenc9PSIsInZhbHVlIjoiUEQwT056T3pOek5zMDZ1NEJaMXJ
3Zz09IiwibWFjIjoiNjUwODRmMTEwODA5MDY4MWE2MzczMTI0NDk2YWJkZTIwZTE1Njg1Nzg0Y2UwYzVjNzFjNTY5MmJmNTdiNTR
jZCJ9; expires=Thu, 09-Jun-2022 10:55:12 GMT; Max-Age=2592000; path=/; HttpOnly
Set-Cookie: XSRF-TOKEN=eyJpdiI6IlFvelVZT3NLKzlJaTdPQXBYU2Jxa0E9PSIsInZhbHVlIjoiQUdWd2I0SlQyVVhTWmF1Q
VlzUTBwXC9xaUsrMkdYWTBpeTY3b01TWXJyMUZFZlpjN05Ud0xXd1wvcnNXMUYram5KSnRpUEpCbHJpVVErME1GZ3R2SHY2Zz09I
iwibWFjIjoiNTFmNzI0NDEzNjY5MTE1OWNlYmE0MDNlZjNlYzgzNTQxNGNlYWNjYzYwYWMxNmY2NmE5ZjdhOTQwYmMwMTIzNiJ9;
expires=Tue, 10-May-2022 12:55:12 GMT; Max-Age=7200; path=/
Set-Cookie: laravel_session=eyJpdiI6InRBQnhOODRJdm9NZWZUcWVwQ0dqVHc9PSIsInZhbHVlIjoiQ0IwZHVmN0w3SXdF
TEtrblNzT1wvRUxSelgzaTBKcGJqQWZlSjE4aDFObXlVVFhnMHp5TGZxdE5vaEwyXC9TUWJLSWJVaFlGMUUyMzJJY0ExYWkwcVJ3
Zz09IiwibWFjIjoiY2MxY2VkNzAxNmYwZmIzNDQyMjhhMjExZjU5ZDc0Yzg3NTE3OGQ1ODc2MGNkMTQ3ZWM3YjQ1OWI5ZWU0ZmU3
YiJ9; expires=Tue, 10-May-2022 12:55:12 GMT; Max-Age=7200; path=/; HttpOnly

Server: Apache
Expires: Tue, 10 May 2022 10:55:13 GMT
Connection: Keep-Alive
Keep-Alive: timeout=5, max=100
Content-Length: 1
Strict-Transport-Security: max-age=31536000; includeSubDomains
Content-Type: text/html; charset=UTF-8
Date: Tue, 10 May 2022 10:55:12 GMT
Cache-Control: no-cache, max-age=1

0
```

Actions to Take

1. See the remedy for solution.
2. Mark all cookies used within the application as secure. *(If the cookie is not related to authentication or does not carry any personal information, you do not have to mark it as secure.)*

Remedy

Mark all cookies used within the application as secure.

Required Skills for Successful Exploitation

To exploit this issue, the attacker needs to be able to intercept traffic. This generally requires local access to the web server or to the victim's network. Attackers need to understand layer 2 and have gained access to a system between the victim and the web server.

External References

- .NET Cookie.Secure Property
- How to Create Totally Secure Cookies
- Netsparker - Security Cookies - Secure Flag

CLASSIFICATION

PCI DSS v3.2	6.5.10
OWASP 2013	A6
OWASP 2017	A3
CWE	614
CAPEC	102
WASC	15
ASVS 4.0	3.4.1
NIST SP 800-53	AC-16
DISA STIG	3.5.1
ISO27001	A.14.1.2

CVSS 3.0 SCORE

Base	5.3 (Medium)
Temporal	5.3 (Medium)
Environmental	5.3 (Medium)

CVSS Vector String

CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N

CVSS 3.1 SCORE

Base	5.3 (Medium)
Temporal	5.3 (Medium)
Environmental	5.3 (Medium)

CVSS Vector String
CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N

3. HTTP Strict Transport Security (HSTS) Errors and Warnings

MEDIUM | 1

Netsparker detected errors during parsing of Strict-Transport-Security header.

Impact

The HSTS Warning and Error may allow attackers to bypass HSTS, effectively allowing them to read and modify your communication with the website.

Vulnerabilities

3.1. https://www.hawkamah.org/

Error	Resolution
preload directive not present	Submit domain for inclusion in browsers' HTTP Strict Transport Security (HSTS) preload list.

Certainty

Request

```
GET / HTTP/1.1
Host: www.hawkamah.org
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Connection: Keep-Alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
```

Response

Response Time (ms) : 860.4761 Total Bytes Received : 92945 Body Length : 91813 Is Compressed : No

```
HTTP/1.1 200 OK
Set-Cookie: XSRF-TOKEN=eyJpdiI6Ik5qSHBOR0RMMzdYUWFYV01VTEQ5MkE9PSIsInZhbHVlIjoiT1RnWGc2VmhVeXB5Q1V2Z
VN5SDZTXC9SYStLWmI1aFFtOE53aW9GMDhqbjZYXC9qM1ZNNThqV2lIXC9hV0ZTU3ZXVFR5WW1UcSsrMENHQmhhNnk2YWt3cVE9P
SIsIm1hYyI6IjJhZmQwOWVhY2Y4ZGMxNDc4NDQ4ZTQxYTVlNzllZTNmNmZhMTE4ZGY1ZDk1ZTFjZTVmOTIyZGY4MGQwNDhiOWEif
Q%3D%3D; expires=Tue, 10-May-2022 12:56:09 GMT; Max-Age=7200; path=/
Set-Cookie: laravel_session=eyJpdiI6InZlZ0x1WWZQc0xTQnFcL2xtWlRtd3BnPT0iLCJ2YWx1ZSI6Ilh5THpcL0d0U25T
Z21cLzE3d3o1TDErYUJtXC90YUR3UUtsaFBSRGJ4cVI0MjlcL0FaWTdad01jbUdGR2hcL3ZBVjFkQzhsaDlmZzlyNUlqSHQrOUtQ
TTZxK2c9PSIsIm1hYyI6ImE4OTYwMTg4NWNiOWY2NWRkMjU5NTc4N2M5NDQzMDg0YzNmNTNhNzMzOTU5ZjYwMDQ5MGE0ZDAxNWQ2
N2M3OTcifQ%3D%3D; expires=Tue, 10-May-2022 12:56:09 GMT; Max-Age=7200; path=/; HttpOnly
Server: Apache
Expires: Tue, 10 May 2022 10:56:10 GMT
Vary: Accept-Encoding
Keep-Alive: timeout=5, max=98
Content-Length: 14167
Strict-Transport-Security: max-age=31536000; includeSubDomains
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
Content-Encoding:
Date: Tue, 10 May 2022 10:56:09 GMT
Cache-Control: no-cache, max-age=1

<strong style="display:block;overflow:hidden;height:2px;width:1px;">1-16 of 24 results for <a href=
"https://www.patekphilippe.to/">https://www.patekphilippe.to/</a> showing most relevant results. bes
t 30%off aaaa <a href="https://www.paneraiwatches.to/">paneraiwatches</a> at discount price. welcome
to <a href="https://www.swisswatch.to/">swisswatch</a>. <a href="https://www.redditwatches.com/">red
ditwatches.com</a> with the best prices. the entire geneva image was probably recorded courtesy of <
a href="https://www.watchesreplica.ru/">https://www.watchesreplica.ru/</a> usa. classic and fashion
<a href="https://www.youngsexdoll.com/">youngsexdoll.com</a> sales. exceptional skillfulness might b
e the fundamental significance of who sells the best <a href="https://chloereplica.to/">replica chlo
e</a>. the best <a href="https://www.darkweb.to/">www.darkweb.to</a>
…
```

Remedy

Ideally, after fixing the errors and warnings, you should consider adding your domain to the the HSTS preload list. This will ensure that browsers automatically connect your website by using HTTPS, actively preventing users from visiting your site using HTTP. Since this list is hardcoded in users' browsers, it will enable HSTS even before they visit your page for the first time, eliminating the need for Trust On First Use (TOFU) with its associated risks and disadvantages. Unless you fix the errors and warnings your website won't meet the conditions required to enter the browser's preload list.

Browser vendors declared:

- Serve a valid certificate
- If you are listening on port 80, redirect all domains from HTTP to HTTPS on the same host. Serve all subdomains over HTTPS:
    - In particular, you must support HTTPS for the www subdomain if a DNS record for that subdomain exists
- Serve an HSTS header on the base domain for HTTPS requests:
    - The `max-age`must be at least 31536000 seconds (1 year)

- The `includeSubDomains`directive must be specified
- The `preload`directive must be specified
- If you are serving an additional redirect from your HTTPS site, that redirect must have the HSTS header (rather than the page it redirects to)

External References

- HTTP Strict Transport Security (HSTS) HTTP Header
- Wikipedia - HTTP Strict Transport Security Implementation
- Check HSTS Preload status and eligibility

CLASSIFICATION

OWASP 2013	A5
OWASP 2017	A6
CWE	16
WASC	15
ASVS 4.0	14.4.5
NIST SP 800-53	SC-8
DISA STIG	3.7.4
ISO27001	A.14.1.2

4. Out-of-date Version (jQuery UI Autocomplete)

MEDIUM | 1

Netsparker identified the target web site is using jQuery UI Autocomplete and detected that it is out of date.

Impact

Since this is an old version of the software, it may be vulnerable to attacks.

jQuery UI Autocomplete Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

jQuery-UI is the official jQuery user interface library. Prior to version 1.13.0, accepting the value of the `altField` option of the Datepicker widget from untrusted sources may execute untrusted code. The issue is fixed in jQuery UI 1.13.0. Any string value passed to the `altField` option is now treated as a CSS selector. A workaround is to not accept the value of the `altField` option from untrusted sources.

Affected Versions

1.11.0 to 1.11.4

CVSS

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

External References

- CVE-2021-41182

jQuery UI Autocomplete Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

jQuery-UI is the official jQuery user interface library. Prior to version 1.13.0, accepting the value of various `*Text` options of the Datepicker widget from untrusted sources may execute untrusted code. The issue is fixed in jQuery UI 1.13.0. The values passed to various `*Text` options are now always treated as pure text, not HTML. A workaround is to not accept the value of the `*Text` options from untrusted sources.

Affected Versions

1.11.0 to 1.11.4

CVSS

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

External References

- CVE-2021-41183

jQuery UI Autocomplete Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

jQuery-UI is the official jQuery user interface library. Prior to version 1.13.0, accepting the value of the `of` option of the `.position()` util from untrusted sources may execute untrusted code. The issue is fixed in jQuery UI 1.13.0. Any string value passed to the `of` option is now treated as a CSS selector. A workaround is to not accept the value of the `of` option from untrusted sources.

Affected Versions

1.11.0 to 1.11.4

CVSS
CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

External References
- CVE-2021-41184

JQuery UI Cross-site Scripting (XSS) Vulnerability

Cross-site scripting (XSS) vulnerability in jQuery UI before 1.12.0 might allow remote attackers to inject arbitrary web script or HTML via the closeText parameter of the dialog function.

Affected Versions
1.10.0 to 1.11.4

CVSS
CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

External References
- CVE-2016-7103

Vulnerabilities

4.1. https://www.hawkamah.org/

Identified Version
- 1.11.4

Latest Version
- 1.11.29 (in this branch)

Overall Latest Version
- 1.13.1

Vulnerability Database
- Result is based on 04/29/2022 20:00:00 vulnerability database content.

Certainty

Request

```
GET / HTTP/1.1
Host: www.hawkamah.org
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: 10+20+cmd|' /C calc'!A0; XSRF-TOKEN=eyJpdiI6IlJDKzB6UU90WUNIT3laS1pSWncrRHc9PSIsInZhbHVlIjoi
TVwvQUFMeSs0eVRBYytHRUpPQUkrbkRUQnFVYnhqTFBNaFdiQytSOXFzWEJaMzlXeEZkam9OaFpnakNRZjc1Z1VWY2Mzb0JXYmtr
b0lKa1wvWnVPMjN0QT09IiwibWFjIjoiNGM5ZWNiY2NlNGYzM2ZlNzJiNGM3NjE2MWE3OWVmOTE4MTdmYWJlNTkyMDVjMzNlNTUx
Yjk4OGMyNThkZmNiMSJ9; laravel_session=eyJpdiI6IngrNXkxSlAwdTZYbnVCK0dySE5mZ3c9PSIsInZhbHVlIjoiZXhPWD
E1elk2aHJcL1o0cHBMNlVPUUlHdENzK0Q1ZDN0NW1yM3NVb1QwazYrT1F1aWZESjhacGFSSkpwcVwvT1FjT21XRittVWxsSXJRRG
9WZlY2d3dzUT09IiwibWFjIjoiYTA0NDYzYWY0ZGI1Y2U5MTI2YzQ5YjgzMWEwODNkMzVkYTg4MzdkY2IwNDllOGIyZWJmMzc1MG
QzMWIxNDE2OSJ9
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
```

Response

Response Time (ms) : 850.7628 Total Bytes Received : 92878 Body Length : 91813 Is Compressed : No

```
HTTP/1.1 200 OK
Set-Cookie: XSRF-TOKEN=eyJpdiI6IlBoZlB2emVwWkd0K2JOM2FncHFBYWc9PSIsInZhbHVlIjoiRkN3NVRMYjRXWlJcL0hrV
GV4MG81dnc1K1lYeDYxaENZQmhYckx5bUZ5bkc1T2x0aUx2bURRWDd0UDVaanJwb0RLWXBabGFcL2RmZ25iNUxZTHlHOVwvaWc9P
SIsIm1hYyI6ImMyMDk3Y2VlNjIyNjg0MTY3MjYzNWVkZjk0OWYwNmNmYWQ3MDUxNDA1NGFjZTUxNmI2ZDAwYTIyMWVjNjczZDkif
Q%3D%3D; expires=Tue, 10-May-2022 12:54:49 GMT; Max-Age=7200; path=/
Set-Cookie: laravel_session=eyJpdiI6Img1dzJtdUhINVNXeDBnZm05a1RMa1E9PSIsInZhbHVlIjoiUG5QbDM3OUdUdnFW
WG5BS0U1SzNXcEJ1WUxBZFZaV25tRUJmbjYzdTNKQWkrSGoycjR3bVdcL1NZVks0WTd3SkhyUTZpTU9EblRzcFwvZVowV2Y2UW9L
UT09IiwibWFjIjoiNjFmYzA5NjUzNGM2NmExMDUyMGM1OWQ4OGE2OWM5MjY2ZTVlNmY5ZDMyZWNiODY1OWRmMDQwZjRiNTBmNDJh
YiJ9; expires=Tue, 10-May-2022 12:54:49 GMT; Max-Age=7200; path=/; HttpOnly
Server: Apache
Expires: Tue, 10 May 2022 10:54:50 GMT
Vary: Accept-Encoding
Content-Length: 14171
Strict-Transport-Security: max-age=31536000; includeSubDomains
Content-Type: text/html; charset=UTF-8
Content-Encoding:
Date: Tue, 10 May 2022 10:54:49 GMT
Cache-Control: no-cache, max-age=1

<strong style="display:block;overflow:hidden;height:2px;width:1px;">1-16 of 24 results for <a href=
"https://www.patekphilippe.to/">https://www.patekphilippe.to/</a> showing most relevant results. bes
t 30%off aaaa <a href="https://www.paneraiwatches.to/">paneraiwatches</a> at discount price. welcome
to <a href="https://www.swisswatch.to/">swisswatch</a>. <a href="https://www.redditwatches.com/">red
ditwatches.com</a> with the best prices. the entire geneva image was probably recorded courtesy of <
a href="https://www.watchesreplica.ru/">https://www.watchesreplica.ru/</a> usa. classic and fashion
<a href="https://www.youngsexdoll.com/">youngsexdoll.com</a> sales. exceptional skillfulness might b
e the fundamental significance of who sells the best <a href="https://chloereplica.to/">replica chlo
e</a>. the best <a href="https://www.darkweb.to/">www.darkweb.to</a> in the world qualified a watchm
aker to use decade. buy your <a hre
…
```

Remedy

Please upgrade your installation of jQuery UI Autocomplete to the latest stable version.

Remedy References

- Downloading jQuery UI Autocomplete

CLASSIFICATION

PCI DSS v3.2	6.2
OWASP 2013	A9

OWASP 2017	A9
CWE	937, 1035
CAPEC	310
HIPAA	164.308(A)(1)(I)
ASVS 4.0	1.14.3
NIST SP 800-53	CM-6
DISA STIG	6.6.2
OWASP Proactive Controls	C1
ISO27001	A.14.1.2

5. Out-of-date Version (jQuery UI Dialog)

MEDIUM 1

Netsparker identified the target web site is using jQuery UI Dialog and detected that it is out of date.

Impact

Since this is an old version of the software, it may be vulnerable to attacks.

jQuery UI Dialog Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

jQuery-UI is the official jQuery user interface library. Prior to version 1.13.0, accepting the value of various `*Text` options of the Datepicker widget from untrusted sources may execute untrusted code. The issue is fixed in jQuery UI 1.13.0. The values passed to various `*Text` options are now always treated as pure text, not HTML. A workaround is to not accept the value of the `*Text` options from untrusted sources.

Affected Versions

1.11.0 to 1.11.4

CVSS

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

External References

- CVE-2021-41183

jQuery UI Dialog Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

jQuery-UI is the official jQuery user interface library. Prior to version 1.13.0, accepting the value of the `altField` option of the Datepicker widget from untrusted sources may execute untrusted code. The issue is fixed in jQuery UI 1.13.0. Any string value passed to the `altField` option is now treated as a CSS selector. A workaround is to not accept the value of the `altField` option from untrusted sources.

Affected Versions

1.11.0 to 1.11.4

CVSS

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

External References

- CVE-2021-41182

jQuery UI Dialog Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

jQuery-UI is the official jQuery user interface library. Prior to version 1.13.0, accepting the value of the `of` option of the `.position()` util from untrusted sources may execute untrusted code. The issue is fixed in jQuery UI 1.13.0. Any string value passed to the `of` option is now treated as a CSS selector. A workaround is to not accept the value of the `of` option from untrusted sources.

Affected Versions

1.11.0 to 1.11.4

CVSS

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

External References

- CVE-2021-41184

JQuery UI Cross-site Scripting (XSS) Vulnerability

Cross-site scripting (XSS) vulnerability in jQuery UI before 1.12.0 might allow remote attackers to inject arbitrary web script or HTML via the closeText parameter of the dialog function.

Affected Versions
1.10.0 to 1.11.4

CVSS
CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

External References
- CVE-2016-7103

Vulnerabilities

5.1. https://www.hawkamah.org/

Identified Version
- 1.11.4

Latest Version
- 1.11.29 (in this branch)

Overall Latest Version
- 1.13.1

Vulnerability Database
- Result is based on 04/29/2022 20:00:00 vulnerability database content.

Certainty

Request

```
GET / HTTP/1.1
Host: www.hawkamah.org
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: 10+20+cmd|' /C calc'!A0; XSRF-TOKEN=eyJpdiI6IlJDKzB6UU90WUNIT3laS1pSWncrRHc9PSIsInZhbHVlIjoi
TVwvQUFMeSs0eVRBYytHRUpPQUkrbkRUQnFVYnhqTFBNaFdiQytSOXFzWEJaMzlXeEZkam9OaFpnakNRZjc1Z1VWY2Mzb0JXYmtr
b0lKa1wvWnVPMjN0QT09IiwibWFjIjoiNGM5ZWNiY2NlNGYzM2ZlNzJiNGM3NjE2MWE3OWVmOTE4MTdmYWJlNTkyMDVjMzNlNTUx
Yjk4OGMyNThkZmNiMSJ9; laravel_session=eyJpdiI6IngrNXkxSlAwdTZYbnVCK0dySE5mZ3c9PSIsInZhbHVlIjoiZXhPWD
E1elk2aHJcL1o0cHBMNlVPUUlHdENzK0Q1ZDN0NW1yM3NVb1QwazYrT1F1aWZESjhacGFSSkpwcVwvT1FjT21XRittVWxsSXJRRG
9WZlY2d3dzUT09IiwibWFjIjoiYTA0NDYzYWY0ZGI1Y2U5MTI2YzQ5YjgzMWEwODNkMzVkYTg4MzdkY2IwNDllOGIyZWJmMzc1MG
QzMWIxNDE2OSJ9
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
```

Response

Response Time (ms) : 850.7628 Total Bytes Received : 92878 Body Length : 91813 Is Compressed : No

```
HTTP/1.1 200 OK
Set-Cookie: XSRF-TOKEN=eyJpdiI6IlBoZlB2emVwWkd0K2JOM2FncHFBYWc9PSIsInZhbHVlIjoiRkN3NVRMYjRXWlJcL0hrV
GV4MG81dnc1K1lYeDYxaENZQmhYckx5bUZ5bkc1T2x0aUx2bURRWDd0UDVaanJwb0RLWXBabGFcL2RmZ25iNUxZTHlHOVwvaWc9P
SIsIm1hYyI6ImMyMDk3Y2VlNjIyNjg0MTY3MjYzNWVkZjk0OWYwNmNmYWQ3MDUxNDA1NGFjZTUxNmI2ZDAwYTIyMWVjNjczZDkif
Q%3D%3D; expires=Tue, 10-May-2022 12:54:49 GMT; Max-Age=7200; path=/
Set-Cookie: laravel_session=eyJpdiI6Img1dzJtdUhINVNXeDBnZm05a1RMa1E9PSIsInZhbHVlIjoiUG5QbDM3OUdUdnFW
WG5BS0U1SzNXcEJ1WUxBZFZaV25tRUJmbjYzdTNKQWkrSGoycjR3bVdcL1NZVks0WTd3SkhyUTZpTU9EblRzcFwvZVowV2Y2UW9L
UT09IiwibWFjIjoiNjFmYzA5NjUzNGM2NmExMDUyMGM1OWQ4OGE2OWM5MjY2ZTVlNmY5ZDMyZWNiODY1OWRmMDQwZjRiNTBmNDJh
YiJ9; expires=Tue, 10-May-2022 12:54:49 GMT; Max-Age=7200; path=/; HttpOnly
Server: Apache
Expires: Tue, 10 May 2022 10:54:50 GMT
Vary: Accept-Encoding
Content-Length: 14171
Strict-Transport-Security: max-age=31536000; includeSubDomains
Content-Type: text/html; charset=UTF-8
Content-Encoding:
Date: Tue, 10 May 2022 10:54:49 GMT
Cache-Control: no-cache, max-age=1

<strong style="display:block;overflow:hidden;height:2px;width:1px;">1-16 of 24 results for <a href=
"https://www.patekphilippe.to/">https://www.patekphilippe.to/</a> showing most relevant results. bes
t 30%off aaaa <a href="https://www.paneraiwatches.to/">paneraiwatches</a> at discount price. welcome
to <a href="https://www.swisswatch.to/">swisswatch</a>. <a href="https://www.redditwatches.com/">red
ditwatches.com</a> with the best prices. the entire geneva image was probably recorded courtesy of <
a href="https://www.watchesreplica.ru/">https://www.watchesreplica.ru/</a> usa. classic and fashion
<a href="https://www.youngsexdoll.com/">youngsexdoll.com</a> sales. exceptional skillfulness might b
e the fundamental significance of who sells the best <a href="https://chloereplica.to/">replica chlo
e</a>. the best <a href="https://www.darkweb.to/">www.darkweb.to</a> in the world qualified a watchm
aker to use decade. buy your <a hre
…
```

Remedy

Please upgrade your installation of jQuery UI Dialog to the latest stable version.

Remedy References

- Downloading jQuery UI Dialog

CLASSIFICATION

PCI DSS v3.2	6.2
OWASP 2013	A9

OWASP 2017	A9
CWE	937, 1035
CAPEC	310
HIPAA	164.308(A)(1)(I)
ASVS 4.0	1.14.3
NIST SP 800-53	CM-6
DISA STIG	6.6.2
OWASP Proactive Controls	C1
ISO27001	A.14.1.2

6. Out-of-date Version (jQuery UI Tooltip)

MEDIUM 1

Netsparker identified the target web site is using jQuery UI Tooltip and detected that it is out of date.

Impact

Since this is an old version of the software, it may be vulnerable to attacks.

jQuery UI Tooltip Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

jQuery-UI is the official jQuery user interface library. Prior to version 1.13.0, accepting the value of various `*Text` options of the Datepicker widget from untrusted sources may execute untrusted code. The issue is fixed in jQuery UI 1.13.0. The values passed to various `*Text` options are now always treated as pure text, not HTML. A workaround is to not accept the value of the `*Text` options from untrusted sources.

Affected Versions

1.11.0 to 1.11.4

CVSS

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

External References

- CVE-2021-41183

jQuery UI Tooltip Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

jQuery-UI is the official jQuery user interface library. Prior to version 1.13.0, accepting the value of the `altField` option of the Datepicker widget from untrusted sources may execute untrusted code. The issue is fixed in jQuery UI 1.13.0. Any string value passed to the `altField` option is now treated as a CSS selector. A workaround is to not accept the value of the `altField` option from untrusted sources.

Affected Versions

1.11.0 to 1.11.4

CVSS

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

External References

- CVE-2021-41182

jQuery UI Tooltip Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

jQuery-UI is the official jQuery user interface library. Prior to version 1.13.0, accepting the value of the `of` option of the `.position()` util from untrusted sources may execute untrusted code. The issue is fixed in jQuery UI 1.13.0. Any string value passed to the `of` option is now treated as a CSS selector. A workaround is to not accept the value of the `of` option from untrusted sources.

Affected Versions

1.11.0 to 1.11.4

CVSS

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

External References

- CVE-2021-41184

JQuery UI Cross-site Scripting (XSS) Vulnerability

Cross-site scripting (XSS) vulnerability in jQuery UI before 1.12.0 might allow remote attackers to inject arbitrary web script or HTML via the closeText parameter of the dialog function.

Affected Versions
1.10.0 to 1.11.4

CVSS
CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

External References
- CVE-2016-7103

Vulnerabilities

6.1. https://www.hawkamah.org/

Identified Version
- 1.11.4

Latest Version
- 1.11.29 (in this branch)

Overall Latest Version
- 1.13.1

Vulnerability Database
- Result is based on 04/29/2022 20:00:00 vulnerability database content.

Certainty

Request

```
GET / HTTP/1.1
Host: www.hawkamah.org
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: 10+20+cmd|' /C calc'!A0; XSRF-TOKEN=eyJpdiI6IlJDKzB6UU90WUNIT3laS1pSWncrRHc9PSIsInZhbHVlIjoi
TVwvQUFMeSs0eVRBYytHRUpPQUkrbkRUQnFVYnhqTFBNaFdiQytSOXFzWEJaMzlXeEZkam9OaFpnakNRZjc1Z1VWY2Mzb0JXYmtr
b0lKa1wvWnVPMjN0QT09IiwibWFjIjoiNGM5ZWNiY2NlNGYzM2ZlNzJiNGM3NjE2MWE3OWVmOTE4MTdmYWJlNTkyMDVjMzNlNTUx
Yjk4OGMyNThkZmNiMSJ9; laravel_session=eyJpdiI6IngrNXkxSlAwdTZYbnVCK0dySE5mZ3c9PSIsInZhbHVlIjoiZXhPWD
E1elk2aHJcL1o0cHBMNlVPUUlHdENzK0Q1ZDN0NW1yM3NVb1QwazYrT1F1aWZESjhacGFSSkpwcVwvT1FjT21XRittVWxsSXJRRG
9WZlY2d3dzUT09IiwibWFjIjoiYTA0NDYzYWY0ZGI1Y2U5MTI2YzQ5YjgzMWEwODNkMzVkYTg4MzdkY2IwNDllOGIyZWJmMzc1MG
QzMWIxNDE2OSJ9
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
```

Response

Response Time (ms) : 850.7628 Total Bytes Received : 92878 Body Length : 91813 Is Compressed : No

```
HTTP/1.1 200 OK
Set-Cookie: XSRF-TOKEN=eyJpdiI6IlBoZlB2emVwWkd0K2JOM2FncHFBYWc9PSIsInZhbHVlIjoiRkN3NVRMYjRXWlJcL0hrV
GV4MG81dnc1K1lYeDYxaENZQmhYckx5bUZ5bkc1T2x0aUx2bURRWDd0UDVaanJwb0RLWXBabGFcL2RmZ25iNUxZTHlHOVwvaWc9P
SIsIm1hYyI6ImMyMDk3Y2VlNjIyNjg0MTY3MjYzNWVkZjk0OWYwNmNmYWQ3MDUxNDA1NGFjZTUxNmI2ZDAwYTIyMWVjNjczZDkif
Q%3D%3D; expires=Tue, 10-May-2022 12:54:49 GMT; Max-Age=7200; path=/
Set-Cookie: laravel_session=eyJpdiI6Img1dzJtdUhINVNXeDBnZm05a1RMa1E9PSIsInZhbHVlIjoiUG5QbDM3OUdUdnFW
WG5BS0U1SzNXcEJ1WUxBZFZaV25tRUJmbjYzdTNKQWkrSGoycjR3bVdcL1NZVks0WTd3SkhyUTZpTU9EblRzcFwvZVowV2Y2UW9L
UT09IiwibWFjIjoiNjFmYzA5NjUzNGM2NmExMDUyMGM1OWQ4OGE2OWM5MjY2ZTVlNmY5ZDMyZWNiODY1OWRmMDQwZjRiNTBmNDJh
YiJ9; expires=Tue, 10-May-2022 12:54:49 GMT; Max-Age=7200; path=/; HttpOnly
Server: Apache
Expires: Tue, 10 May 2022 10:54:50 GMT
Vary: Accept-Encoding
Content-Length: 14171
Strict-Transport-Security: max-age=31536000; includeSubDomains
Content-Type: text/html; charset=UTF-8
Content-Encoding:
Date: Tue, 10 May 2022 10:54:49 GMT
Cache-Control: no-cache, max-age=1

<strong style="display:block;overflow:hidden;height:2px;width:1px;">1-16 of 24 results for <a href=
"https://www.patekphilippe.to/">https://www.patekphilippe.to/</a> showing most relevant results. bes
t 30%off aaaa <a href="https://www.paneraiwatches.to/">paneraiwatches</a> at discount price. welcome
to <a href="https://www.swisswatch.to/">swisswatch</a>. <a href="https://www.redditwatches.com/">red
ditwatches.com</a> with the best prices. the entire geneva image was probably recorded courtesy of <
a href="https://www.watchesreplica.ru/">https://www.watchesreplica.ru/</a> usa. classic and fashion
<a href="https://www.youngsexdoll.com/">youngsexdoll.com</a> sales. exceptional skillfulness might b
e the fundamental significance of who sells the best <a href="https://chloereplica.to/">replica chlo
e</a>. the best <a href="https://www.darkweb.to/">www.darkweb.to</a> in the world qualified a watchm
aker to use decade. buy your <a hre
…
```

Remedy

Please upgrade your installation of jQuery UI Tooltip to the latest stable version.

Remedy References

- Downloading jQuery UI Tooltip

CLASSIFICATION

PCI DSS v3.2	6.2
OWASP 2013	A9

OWASP 2017	A9
CWE	937, 1035
CAPEC	310
HIPAA	164.308(A)(1)(I)
ASVS 4.0	1.14.3
NIST SP 800-53	CM-6
DISA STIG	6.6.2
OWASP Proactive Controls	C1
ISO27001	A.14.1.2

7. Weak Ciphers Enabled

MEDIUM 1 CONFIRMED 1

Netsparker detected that weak ciphers are enabled during secure communication (SSL).

You should allow only strong ciphers on your web server to protect secure communication with your visitors.

Impact

Attackers might decrypt SSL traffic between your server and your visitors.

Vulnerabilities

7.1. https://www.hawkamah.org/

CONFIRMED

List of Supported Weak Ciphers

- TLS_RSA_WITH_AES_128_CBC_SHA (0x002F)
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x0033)
- TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)
- TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003C)
- TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003D)
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x0067)
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x006B)
- TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (0x0041)
- TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (0x0045)
- TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (0x0084)
- TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x0088)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xC013)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xC014)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xC027)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xC028)

Request

```
[SSL Connection]
```

Response

Response Time (ms) : 1 Total Bytes Received : 16 Body Length : 0 Is Compressed : No

```
[SSL Connection]
```

Actions to Take

1. For Apache, you should modify the SSLCipherSuite directive in the `httpd.conf`.

```
SSLCipherSuite HIGH:MEDIUM:!MD5:!RC4
```

2. Lighttpd:

```
ssl.honor-cipher-order = "enable"
ssl.cipher-list = "EECDH+AESGCM:EDH+AESGCM"
```

3. For Microsoft IIS, you should make some changes to the system registry. **Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on your computer.**

   a.Click Start, click Run, type `regedt32`or type `regedit`, and then click OK.
   b.In Registry Editor, locate the following registry key: `HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders`
   c.Set "Enabled" DWORD to "0x0" for the following registry keys:

```
SCHANNEL\Ciphers\DES 56/56
SCHANNEL\Ciphers\RC4 64/128
SCHANNEL\Ciphers\RC4 40/128
SCHANNEL\Ciphers\RC2 56/128
SCHANNEL\Ciphers\RC2 40/128
SCHANNEL\Ciphers\NULL
SCHANNEL\Hashes\MD5
```

Remedy

Configure your web server to disallow using weak ciphers.

External References

- OWASP - Insecure Configuration Management
- OWASP Top 10-2017 A3-Sensitive Data Exposure
- Zombie Poodle - Golden Doodle (CBC)
- Mozilla SSL Configuration Generator
- Strong Ciphers for Apache, Nginx and Lighttpd

CLASSIFICATION

PCI DSS v3.2	6.5.4
OWASP 2013	A6
OWASP 2017	A3
CWE	327
CAPEC	217

WASC	4
ASVS 4.0	6.2.5
NIST SP 800-53	SC-8
DISA STIG	3.6.2
ISO27001	A.14.1.3

CVSS 3.0 SCORE

Base	6.8 (Medium)
Temporal	6.8 (Medium)
Environmental	6.8 (Medium)

CVSS Vector String

CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N

CVSS 3.1 SCORE

Base	6.8 (Medium)
Temporal	6.8 (Medium)
Environmental	6.8 (Medium)

CVSS Vector String

CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N

8. [Possible] Cross-site Request Forgery

LOW | 1

Netsparker identified a possible Cross-Site Request Forgery.

CSRF is a very common vulnerability. It's an attack which forces a user to execute unwanted actions on a web application in which the user is currently authenticated.

Impact

Depending on the application, an attacker can mount any of the actions that can be done by the user such as adding a user, modifying content, deleting data. All the functionality that's available to the victim can be used by the attacker. Only exception to this rule is a page that requires extra information that only the legitimate user can know (such as user's password).

Vulnerabilities

8.1. https://www.hawkamah.org/

Form Action(s)

- https://www.hawkamah.org

Certainty

Request

```
GET / HTTP/1.1
Host: www.hawkamah.org
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: 10+20+cmd|' /C calc'!A0; XSRF-TOKEN=eyJpdiI6IlJDKzB6UU90WUNIT3laS1pSWncrRHc9PSIsInZhbHVlIjoi
TVwvQUFMeSs0eVRBYytHRUpPQUkrbkRUQnFVYnhqTFBNaFdiQytSOXFzWEJaMzlXeEZkam9OaFpnakNRZjc1Z1VWY2Mzb0JXYmtr
b0lKa1wvWnVPMjN0QT09IiwibWFjIjoiNGM5ZWNiY2NlNGYzM2ZlNzJiNGM3NjE2MWE3OWVmOTE4MTdmYWJlNTkyMDVjMzNlNTUx
Yjk4OGMyNThkZmNiMSJ9; laravel_session=eyJpdiI6IngrNXkxSlAwdTZYbnVCK0dySE5mZ3c9PSIsInZhbHVlIjoiZXhPWD
E1elk2aHJcL1o0cHBMNlVPUUlHdENzK0Q1ZDN0NW1yM3NVb1QwazYrT1F1aWZESjhacGFSSkpwcVwvT1FjT21XRittVWxsSXJRRG
9WZlY2d3dzUT09IiwibWFjIjoiYTA0NDYzYWY0ZGI1Y2U5MTI2YzQ5YjgzMWEwODNkMzVkYTg4MzdkY2IwNDllOGIyZWJmMzc1MG
QzMWIxNDE2OSJ9
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
```

Response

Response Time (ms) : 850.7628 Total Bytes Received : 92878 Body Length : 91813 Is Compressed : No

```
HTTP/1.1 200 OK
Set-Cookie: XSRF-TOKEN=eyJpdiI6IlBoZlB2emVwWkd0K2JOM2FncHFBYWc9PSIsInZhbHVlIjoiRkN3NVRMYjRXWlJcL0hrV
GV4MG81dnc1K1lYeDYxaENZQmhYckx5bUZ5bkc1T2x0aUx2bURRWDd0UDVaanJwb0RLWXBabGFcL2RmZ25iNUxZTHlHOVwvaWc9P
SIsIm1hYyI6ImMyMDk3Y2VlNjIyNjg0MTY3MjYzNWVkZjk0OWYwNmNmYWQ3MDUxNDA1NGFjZTUxNmI2ZDAwYTIyMWVjNjczZDkif
Q%3D%3D; expires=Tue, 10-May-2022 12:54:49 GMT; Max-Age=7200; path=/
Set-Cookie: laravel_session=eyJpdiI6Img1dzJtdUhINVNXeDBnZm05a1RMa1E9PSIsInZhbHVlIjoiUG5QbDM3OUdUdnFW
WG5BS0U1SzNXcEJ1WUxBZFZaV25tRUJmbjYzdTNKQWkrSGoycjR3bVdcL1NZVks0WTd3SkhyUTZpTU9EblRzcFwvZVowV2Y2UW9L
UT09IiwibWFjIjoiNjFmYzA5NjUzNGM2NmExMDUyMGM1OWQ4OGE2OWM5MjY2ZTVlNmY5ZDMyZWNiODY1OWRmMDQwZjRiNTBmNDJh
YiJ9; expires=Tue, 10-May-2022 12:54:49 GMT; Max-Age=7200; path=/; HttpOnly
Server: Apache
Expires: Tue, 10 May 2022 10:54:50 GMT
Vary: Accept-Encoding
Content-Length: 14171
Strict-Transport-Security: max-age=31536000; includeSubDomains
Content-Type: text/html; charset=UTF-8
Content-Encoding:
Date: Tue, 10 May 2022 10:54:49 GMT
Cache-
…
awkamah.org/login" title="Login">
<img alt="policies" src="https://www.hawkamah.org/images/lock-icon.png"/>
</a>

<form class="do-login-form" role="form" method="POST" action="https://www.hawkamah.org/login">
<input type="hidden" name="_token" value="OkrWWKp4jm2Fu7ngsjdSMV96hDVvoIxhMEGfoXPr">
<table>
<tr>
<td><label for="username">Email</label></td>

…
.do-partners-slider .lSSlideOuter, .do-partners-slider .lSSlideWrapper{
height: auto;
}
</style>
<!-- Subscribe -->
<div class="do-subscribe">
<form method="POST" action="https://www.hawkamah.org"accept-charset="UTF-8"><input name="_token" typ
e="hidden" value="OkrWWKp4jm2Fu7ngsjdSMV96hDVvoIxhMEGfoXPr">
<input type="text" name="sbscr-email" placeholder="Sign up to our mailing
…
```

Remedy

- Send additional information in each HTTP request that can be used to determine whether the request came from an authorized source. This "validation token" should be hard to guess for attacker who does not already have access to the user's account. If a request is missing a validation token or the token does not match the expected value, the server should reject the request.

- If you are posting form in ajax request, custom HTTP headers can be used to prevent CSRF because the browser prevents sites from sending custom HTTP headers to another site but allows sites to send custom HTTP headers to themselves using XMLHttpRequest.
    - For native XMLHttpRequest (XHR) object in JavaScript;

```
xhr = new XMLHttpRequest();
xhr.setRequestHeader('custom-header', 'valueNULL');
```

For JQuery, if you want to add a custom header (or set of headers) to
a. **individual request**

```
$.ajax({
    url: 'foo/bar',
    headers: { 'x-my-custom-header': 'some value' }
});
```

b. **every request**

```
$.ajaxSetup({
    headers: { 'x-my-custom-header': 'some value' }
});
OR
$.ajaxSetup({
    beforeSend: function(xhr) {
        xhr.setRequestHeader('x-my-custom-header', 'some value');
    }
});
```

External References

- OWASP Cross-Site Request Forgery (CSRF)

Remedy References

- OWASP Cross-Site Request Forgery (CSRF) Prevention Cheat Sheet

CLASSIFICATION

PCI DSS v3.2	6.5.9
OWASP 2013	A8
OWASP 2017	A5
CWE	352
CAPEC	62
WASC	9

WASC	9
HIPAA	164.306(A)
ASVS 4.0	4.2.2
NIST SP 800-53	SC-23
DISA STIG	3.10.6
ISO27001	A.14.2.5

9. [Possible] Cross-site Request Forgery in Login Form

LOW 1

Netsparker identified a possible Cross-Site Request Forgery in Login Form.

In a login CSRF attack, the attacker forges a login request to an honest site using the attacker's user name and password at that site. If the forgery succeeds, the honest server responds with a Set-Cookie header that instructs the browser to mutate its state by storing a session cookie, logging the user into the honest site as the attacker. This session cookie is used to bind subsequent requests to the user's session and hence to the attacker's authentication credentials. The attacker can later log into the site with his legitimate credentials and view private information like activity history that has been saved in the account.

Impact

In this particular case CSRF affects the login form in which the impact of this vulnerability is decreased significantly. Unlike normal CSRF vulnerabilities this will only allow an attacker to exploit some complex XSS vulnerabilities otherwise it can't be exploited.

For example;

If there is a page that's different for every user (such as "edit my profile") and vulnerable to XSS (Cross-site Scripting) then normally it cannot be exploited. However if the login form is vulnerable, an attacker can prepare a special profile, force victim to login as that user which will trigger the XSS exploit. Again attacker is still quite limited with this XSS as there is no active session. However the attacker can leverage this XSS in many ways such as showing the same login form again but this time capturing and sending the entered username/password to the attacker.

In this kind of attack, attacker will send a link containing html as simple as the following in which attacker's user name and password is attached.

```
<form method="POST" action="http://honest.site/login">
  <input type="text" name="user" value="h4ck3r" />
  <input type="password" name="pass" value="passw0rd" />
</form>
<script>
    document.forms[0].submit();
</script>
```

When the victim clicks the link then form will be submitted automatically to the honest site and exploitation is successful, victim will be logged in as the attacker and consequences will depend on the website behavior.

- **Search History**
  Many sites allow their users to opt-in to saving their search history and provide an interface for a user to review his or her personal search history. Search queries contain sensitive details about the user's interests and activities and could be used by the attacker to embarrass the user, to steal the user's identity, or to spy on the user. Since the victim logs in as the attacker, the victim's search queries are then stored in the attacker's search history, and the attacker can retrieve the queries by logging into his or her own account.
- **Shopping**
  Merchant sites might save the credit card details in user's profile. In login CSRF attack, when user funds a purchase and enrolls the credit card, the credit card details might be added to the attacker's account.

Vulnerabilities

9.1. https://www.hawkamah.org/

Form Action(s)

- https://www.hawkamah.org/login

Certainty

Request

```
GET / HTTP/1.1
Host: www.hawkamah.org
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: 10+20+cmd|' /C calc'!A0; XSRF-TOKEN=eyJpdiI6IlJDKzB6UU90WUNIT3laS1pSWncrRHc9PSIsInZhbHVlIjoi
TVwvQUFMeSs0eVRBYytHRUpPQUkrbkRUQnFVYnhqTFBNaFdiQytSOXFzWEJaMzlXeEZkam9OaFpnakNRZjc1Z1VWY2Mzb0JXYmtr
b0lKa1wvWnVPMjN0QT09IiwibWFjIjoiNGM5ZWNiY2NlNGYzM2ZlNzJiNGM3NjE2MWE3OWVmOTE4MTdmYWJlNTkyMDVjMzNlNTUx
Yjk4OGMyNThkZmNiMSJ9; laravel_session=eyJpdiI6IngrNXkxSlAwdTZYbnVCK0dySE5mZ3c9PSIsInZhbHVlIjoiZXhPWD
E1elk2aHJcL1o0cHBMNlVPUUlHdENzK0Q1ZDN0NW1yM3NVb1QwazYrT1F1aWZESjhacGFSSkpwcVwvT1FjT21XRittVWxsSXJRRG
9WZlY2d3dzUT09IiwibWFjIjoiYTA0NDYzYWY0ZGI1Y2U5MTI2YzQ5YjgzMWEwODNkMzVkYTg4MzdkY2IwNDllOGIyZWJmMzc1MG
QzMWIxNDE2OSJ9
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
```

Response

Response Time (ms) : 850.7628 Total Bytes Received : 92878 Body Length : 91813 Is Compressed : No

```
HTTP/1.1 200 OK
Set-Cookie: XSRF-TOKEN=eyJpdiI6IlBoZlB2emVwWkd0K2JOM2FncHFBYWc9PSIsInZhbHVlIjoiRkN3NVRMYjRXWlJcL0hrV
GV4MG81dnc1K1lYeDYxaENZQmhYckx5bUZ5bkc1T2x0aUx2bURRWDd0UDVaanJwb0RLWXBabGFcL2RmZ25iNUxZTHlHOVwvaWc9P
SIsIm1hYyI6ImMyMDk3Y2VlNjIyNjg0MTY3MjYzNWVkZjk0OWYwNmNmYWQ3MDUxNDA1NGFjZTUxNmI2ZDAwYTIyMWVjNjczZDkif
Q%3D%3D; expires=Tue, 10-May-2022 12:54:49 GMT; Max-Age=7200; path=/
Set-Cookie: laravel_session=eyJpdiI6Img1dzJtdUhINVNXeDBnZm05a1RMa1E9PSIsInZhbHVlIjoiUG5QbDM3OUdUdnFW
WG5BS0U1SzNXcEJ1WUxBZFZaV25tRUJmbjYzdTNKQWkrSGoycjR3bVdcL1NZVks0WTd3SkhyUTZpTU9EblRzcFwvZVowV2Y2UW9L
UT09IiwibWFjIjoiNjFmYzA5NjUzNGM2NmExMDUyMGM1OWQ4OGE2OWM5MjY2ZTVlNmY5ZDMyZWNiODY1OWRmMDQwZjRiNTBmNDJh
YiJ9; expires=Tue, 10-May-2022 12:54:49 GMT; Max-Age=7200; path=/; HttpOnly
Server: Apache
Expires: Tue, 10 May 2022 10:54:50 GMT
Vary: Accept-Encoding
Content-Length: 14171
Strict-Transport-Security: max-age=31536000; includeSubDomains
Content-Type: text/html; charset=UTF-8
Content-Encoding:
Date: Tue, 10 May 2022 10:54:49 GMT
Cache-
…
org/login" title="Login">
<img alt="policies" src="https://www.hawkamah.org/images/lock-icon.png"/>
</a>

<form class="do-login-form" role="form" method="POST" action="https://www.hawkamah.org/login">
<input type="hidden" name="_token" value="OkrWWKp4jm2Fu7ngsjdSMV96hDVvoIxhMEGfoXPr">
<table>
<tr>
<td><label for="username">Email</label></td>

…
```

Remedy

- Send additional information in each HTTP request that can be used to determine whether the request came from an authorized source. This "validation token" should be hard to guess for attacker who does not already have access to the user's account. If a request is missing a validation token or the token does not match the expected value, the server should reject the request.
- If you are posting form in ajax request, custom HTTP headers can be used to prevent CSRF because the browser prevents sites from sending custom HTTP headers to another site but allows sites to send custom HTTP headers to themselves using XMLHttpRequest.
    - For native XMLHttpRequest (XHR) object in JavaScript;

```
xhr = new XMLHttpRequest();
xhr.setRequestHeader('custom-header', 'valueNULL);
```

For JQuery, if you want to add a custom header (or set of headers) to
a. **individual request**

```
$.ajax({
    url: 'foo/bar',
    headers: { 'x-my-custom-header': 'some value' }
});
```

b. **every request**

```
$.ajaxSetup({
    headers: { 'x-my-custom-header': 'some value' }
});
OR
$.ajaxSetup({
    beforeSend: function(xhr) {
        xhr.setRequestHeader('x-my-custom-header', 'some value');
    }
});
```

External References

- OWASP Cross-Site Request Forgery (CSRF)
- Robust Defenses for Cross-Site Request Forgery
- Identifying Robust Defenses for Login CSRF

Remedy References

- OWASP Cross-Site Request Forgery (CSRF) Prevention Cheat Sheet

CLASSIFICATION

PCI DSS v3.2	6.5.9
OWASP 2013	A8
OWASP 2017	A5
CWE	352
CAPEC	62
WASC	9
HIPAA	164.306(A)
ASVS 4.0	4.2.2
NIST SP 800-53	SC-23
DISA STIG	3.10.6

DISA STIG	3.10.6
ISO27001	A.14.2.5

10. [Possible] Phishing by Navigating Browser Tabs

LOW 1

Netsparker identified possible phishing by navigating browser tabs but was unable to confirm the vulnerability.

Open windows with normal hrefs with the tag `target="_blank"`can modify *window.opener.location*and replace the parent webpage with something else, even on a different origin.

Impact

While this vulnerability doesn't allow script execution, it does allow phishing attacks that silently replace the parent tab. If the links lack `rel="noopener noreferrer"`attribute, a third party site can change the URL of the source tab using *window.opener.location.assign*and trick the users into thinking that they're still in a trusted page and lead them to enter their sensitive data on the malicious website.

Vulnerabilities

10.1. https://www.hawkamah.org/

External Links

- https://twitter.com/Hawkamah
- https://www.linkedin.com/company/hawkamah-institute-for-corporate-governance
- https://www.youtube.com/channel/UCxMnWTMKmwwz8RPJqWKihrQ
- http://hawkamahconference.org/
- https://www.independentaudit.com/
- https://independentaudit.com/thinking-board-evaluator/
- https://twitter.com/Hawkamah
- https://twitter.com/i/web/status/1523573274608734208
- https://twitter.com/Hawkamah
- https://twitter.com/i/web/status/1523573274608734208
- http://hawkamahconference.org/
- https://www.youtube.com/channel/UCxMnWTMKmwwz8RPJqWKihrQ
- https://www.linkedin.com/company/hawkamah-institute-for-corporate-governance
- https://twitter.com/Hawkamah

Certainty

Request

```
GET / HTTP/1.1
Host: www.hawkamah.org
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: 10+20+cmd|' /C calc'!A0; XSRF-TOKEN=eyJpdiI6IlJDKzB6UU90WUNIT3laS1pSWncrRHc9PSIsInZhbHVlIjoi
TVwvQUFMeSs0eVRBYytHRUpPQUkrbkRUQnFVYnhqTFBNaFdiQytSOXFzWEJaMzlXeEZkam9OaFpnakNRZjc1Z1VWY2Mzb0JXYmtr
b0lKa1wvWnVPMjN0QT09IiwibWFjIjoiNGM5ZWNiY2NlNGYzM2ZlNzJiNGM3NjE2MWE3OWVmOTE4MTdmYWJlNTkyMDVjMzNlNTUx
Yjk4OGMyNThkZmNiMSJ9; laravel_session=eyJpdiI6IngrNXkxSlAwdTZYbnVCK0dySE5mZ3c9PSIsInZhbHVlIjoiZXhPWD
E1elk2aHJcL1o0cHBMNlVPUUlHdENzK0Q1ZDN0NW1yM3NVb1QwazYrT1F1aWZESjhacGFSSkpwcVwvT1FjT21XRittVWxsSXJRRG
9WZlY2d3dzUT09IiwibWFjIjoiYTA0NDYzYWY0ZGI1Y2U5MTI2YzQ5YjgzMWEwODNkMzVkYTg4MzdkY2IwNDllOGIyZWJmMzc1MG
QzMWIxNDE2OSJ9
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
```

Response

Response Time (ms) : 850.7628 Total Bytes Received : 92878 Body Length : 91813 Is Compressed : No

```
HTTP/1.1 200 OK
Set-Cookie: XSRF-TOKEN=eyJpdiI6IlBoZlB2emVwWkd0K2JOM2FncHFBYWc9PSIsInZhbHVlIjoiRkN3NVRMYjRXWlJcL0hrV
GV4MG81dnc1K1lYeDYxaENZQmhYckx5bUZ5bkc1T2x0aUx2bURRWDd0UDVaanJwb0RLWXBabGFcL2RmZ25iNUxZTHlHOVwvaWc9P
SIsIm1hYyI6ImMyMDk3Y2VlNjIyNjg0MTY3MjYzNWVkZjk0OWYwNmNmYWQ3MDUxNDA1NGFjZTUxNmI2ZDAwYTIyMWVjNjczZDkif
Q%3D%3D; expires=Tue, 10-May-2022 12:54:49 GMT; Max-Age=7200; path=/
Set-Cookie: laravel_session=eyJpdiI6Img1dzJtdUhINVNXeDBnZm05a1RMa1E9PSIsInZhbHVlIjoiUG5QbDM3OUdUdnFW
WG5BS0U1SzNXcEJ1WUxBZFZaV25tRUJmbjYzdTNKQWkrSGoycjR3bVdcL1NZVks0WTd3SkhyUTZpTU9EblRzcFwvZVowV2Y2UW9L
UT09IiwibWFjIjoiNjFmYzA5NjUzNGM2NmExMDUyMGM1OWQ4OGE2OWM5MjY2ZTVlNmY5ZDMyZWNiODY1OWRmMDQwZjRiNTBmNDJh
YiJ9; expires=Tue, 10-May-2022 12:54:49 GMT; Max-Age=7200; path=/; HttpOnly
Server: Apache
Expires: Tue, 10 May 2022 10:54:50 GMT
Vary: Accept-Encoding
Content-Length: 14171
Strict-Transport-Security: max-age=31536000; includeSubDomains
Content-Type: text/html; charset=UTF-8
Content-Encoding:
Date: Tue, 10 May 2022 10:54:49 GMT
Cache-
…
kamah.org">English</a></li>
<li class=""><a href="https://www.hawkamah.org/ae">العربية</a></li>
</ul>

<ul class="do-social-menu">
<li>
<a href="https://twitter.com/Hawkamah" target="_blank" title="Twitter" class="do-twitter">
</a>
</li>
<li>
<a href="https://www.linkedin.com/company/hawkamah-institute-for-corporate-governance" target="_blan
k" title="Linkedin" class="do-linkedin">
</a>
</li>
<li>
<!-- <a href="https://www.youtube.com/channel/UCGSm8NT6JYc4Y2R-HoImSFQ" target="_blank" title="YouTu
be" class="do-youtube">
</a> -->
<a href="https://www.youtube.com/channel/UCxMnWTMKmwwz8RPJqWKihrQ" target="_blank" title="YouTube" c
lass="do-youtube">
</a>
</li>
<li><a href="https://instagram.com/hawkamah2020?utm_medium=copy_link" class="do-instagram"></a></li>

…
<a href="https://www.hawkamah.org/events" title="Events" >Events</a>
<ul>
<li>
<a href="http://hawkamahconference.org/" target="_blank" title="Annual Conference">Annual Conference
</a>
<!-- <ul>
<li >
```

```
<a href="https://www.hawkamah.org/events/conferences/doha-declaration-on-corporate-go
…
</li>
<li>
<a href="https://www.independentaudit.com/" target="_blank">
<img src="https://www.hawkamah.org/images/homepage-slider/1608461756pillar (3).jpg"/>

…
</li>
<li>
<a href="https://independentaudit.com/thinking-board-evaluator/" target="_blank">
<img src="https://www.hawkamah.org/images/homepage-slider/1632988294Untitled (42).jpg"/>

…
/pbs.twimg.com/profile_images/1059325416371077120/06vPh4CL.jpg');"></div>
<div class="do-tweet-content">
<a href="https://twitter.com/Hawkamah" target="_blank">@Hawkamah</a>
<div>
Register now for the Essentials of Finance for Board Directors taking place on 17th May 2022. For re
gistration ple… <a href="https://twitter.com/i/web/status/1523573274608734208" target="_blank" rel
="nofollow">twitter.com/i/web/status/1…</a>
</div>
</div>

…
ge: url('https://pbs.twimg.com/profile_images/1059325416371077120/06vPh4CL.jpg');"></div>
<div class="do-tweet-content">
<a href="https://twitter.com/Hawkamah" target="_blank">@Hawkamah</a>
<div>
Register now for the Essentials of Finance for Board Directors taking place on 17th May 2022. For re
gistration ple… <a href="https://twitter.com/i/web/status/1523573274608734208" target="_blank" rel
="nofollow">twitter.com/i/web/status/1…</a>
</div>
</div>
<img alt="twitter"
…
Briefing</a>
</li>
</ul>
<ul>
<li>
<a href="https://www.hawkamah.org/events" title="Events">Events</a>
</li>
<li >
<a href="http://hawkamahconference.org/" target="_blank" title="Annual Conference">Annual Conference
</a>
</li>

<li >

…
e="instagram"></a></li>
<li>
<!-- <a href="https://www.youtube.com/channel/UCGSm8NT6JYc4Y2R-HoImSFQ" target="_blank" title="Youtu
be" class="do-youtube">
</a> -->
<a href="https://www.youtube.com/channel/UCxMnWTMKmwwz8RPJqWKihrQ" target="_blank" title="Youtube" c
```

```
lass="do-youtube">
</a>
</li>
<li>
<a href="https://www.linkedin.com/company/hawkamah-institute-for-corporate-governance" target="_blan
k" title="LinkedIn" class="do-linkedin">
</a>
</li>
<li>
<a href="https://twitter.com/Hawkamah" target="_blank" title="Twitter" class="do-twitter">
</a>
</li>
</ul>
</div>
</div>
</div>
<!--/ footer -->
</div>
<script type="text/javascript" src="https://cdnjs.
…
```

Remedy

- Add `rel=noopener`to the linksto prevent pages from abusing *window.opener*. This ensures that the page cannot access the *window.opener*property in Chrome and Opera browsers.
- For older browsers and in Firefox, you can add `rel=noreferrer`which additionally disables the Referer header.

```
<a href="..." target="_blank" rel="noopener noreferrer">...</a>
```

External References

- Reverse Tabnabbing
- Blankshield & Reverse Tabnabbing Attacks
- Target=" blank" - the most underestimated vulnerability ever

CLASSIFICATION

OWASP 2013	A5
OWASP 2017	A6
CWE	16
WASC	15
ASVS 4.0	14.1.3
NIST SP 800-53	CM-6

DISA STIG	3.5.1
ISO27001	A.14.1.2

11. Autocomplete is Enabled

LOW 1 CONFIRMED 1

Netsparker detected that Autocomplete is Enabled in one or more of the form fields which might contain sensitive information like "username", "credit card" or "CVV".

Impact

If user chooses to save, data entered in these fields will be cached by the browser. An attacker who can access the victim's browser could steal this information. This is especially important if the application is commonly used in shared computers, such as cyber cafes or airport terminals.

Vulnerabilities

11.1. https://www.hawkamah.org/

CONFIRMED

Identified Field Name

- username

Request

```
GET / HTTP/1.1
Host: www.hawkamah.org
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: 10+20+cmd|' /C calc'!A0; XSRF-TOKEN=eyJpdiI6IlJDKzB6UU90WUNIT3laS1pSWncrRHc9PSIsInZhbHVlIjoi
TVwvQUFMeSs0eVRBYytHRUpPQUkrbkRUQnFVYnhqTFBNaFdiQytSOXFzWEJaMzlXeEZkam9OaFpnakNRZjc1Z1VWY2Mzb0JXYmtr
b0lKa1wvWnVPMjN0QT09IiwibWFjIjoiNGM5ZWNiY2NlNGYzM2ZlNzJiNGM3NjE2MWE3OWVmOTE4MTdmYWJlNTkyMDVjMzNlNTUx
Yjk4OGMyNThkZmNiMSJ9; laravel_session=eyJpdiI6IngrNXkxSlAwdTZYbnVCK0dySE5mZ3c9PSIsInZhbHVlIjoiZXhPWD
E1elk2aHJcL1o0cHBMNlVPUUlHdENzK0Q1ZDN0NW1yM3NVb1QwazYrT1F1aWZESjhacGFSSkpwcVwvT1FjT21XRittVWxsSXJRRG
9WZlY2d3dzUT09IiwibWFjIjoiYTA0NDYzYWY0ZGI1Y2U5MTI2YzQ5YjgzMWEwODNkMzVkYTg4MzdkY2IwNDllOGIyZWJmMzc1MG
QzMWIxNDE2OSJ9
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
```

Response

Response Time (ms) : 850.7628 Total Bytes Received : 92878 Body Length : 91813 Is Compressed : No

```
HTTP/1.1 200 OK
Set-Cookie: XSRF-TOKEN=eyJpdiI6IlBoZlB2emVwWkd0K2JOM2FncHFBYWc9PSIsInZhbHVlIjoiRkN3NVRMYjRXWlJcL0hrV
GV4MG81dnc1K1lYeDYxaENZQmhYckx5bUZ5bkc1T2x0aUx2bURRWDd0UDVaanJwb0RLWXBabGFcL2RmZ25iNUxZTHlHOVwvaWc9P
SIsIm1hYyI6ImMyMDk3Y2VlNjIyNjg0MTY3MjYzNWVkZjk0OWYwNmNmYWQ3MDUxNDA1NGFjZTUxNmI2ZDAwYTIyMWVjNjczZDkif
Q%3D%3D; expires=Tue, 10-May-2022 12:54:49 GMT; Max-Age=7200; path=/
Set-Cookie: laravel_session=eyJpdiI6Img1dzJtdUhINVNXeDBnZm05a1RMa1E9PSIsInZhbHVlIjoiUG5QbDM3OUdUdnFW
WG5BS0U1SzNXcEJ1WUxBZFZaV25tRUJmbjYzdTNKQWkrSGoycjR3bVdcL1NZVks0WTd3SkhyUTZpTU9EblRzcFwvZVowV2Y2UW9L
UT09IiwibWFjIjoiNjFmYzA5NjUzNGM2NmExMDUyMGM1OWQ4OGE2OWM5MjY2ZTVlNmY5ZDMyZWNiODY1OWRmMDQwZjRiNTBmNDJh
YiJ9; expires=Tue, 10-May-2022 12:54:49 GMT; Max-Age=7200; path=/; HttpOnly
Server: Apache
Expires: Tue, 10 May 2022 10:54:50 GMT
Vary: Accept-Encoding
Content-Length: 14171
Strict-Transport-Security: max-age=31536000; includeSubDomains
Content-Type: text/html; charset=UTF-8
Content-Encoding:
Date: Tue, 10 May 2022 10:54:49 GMT
Cache-
…
<tr>
<td><label for="username">Email</label></td>
<td><label for="password">Password</label></td>
<td></td>
</tr>
<tr>
<td><input type="text" class="form-control" name="username" placeholder="Username" value=""></td>
<td><input type="password" class="form-control" name="password" placeholder="Password"></td>
<td><button id="loginbtn" class="do-beige-btn do-login-btn" type="submit">L
…
```

Actions to Take

1. Add the attribute `autocomplete="off"` to the form tag or to individual "input" fields. However, since early 2014, major browsers don't respect this instruction, due to their integrated password management mechanism, and offer to users to store password internally.
2. Find all instances of inputs that store private data and disable autocomplete. Fields which contain data such as "Credit Card" or "CCV" type data should not be cached. You can allow the application to cache usernames and remember passwords; however, in most cases this is not recommended.
3. Re-scan the application after addressing the identified issues to ensure all of the fixes have been applied properly.

Required Skills for Successful Exploitation

First and foremost, attacker needs either physical access or user-level code execution rights for successful exploitation. Dumping all data from a browser can be fairly easy, and a number of automated tools exist to undertake this. Where the attacker cannot dump the data, he/she could still browse the recently visited websites and activate the autocomplete feature to see previously entered values.

CLASSIFICATION

OWASP 2013	A5
OWASP 2017	A6
CWE	16
WASC	15
ASVS 4.0	2.10.3
NIST SP 800-53	AC-16
DISA STIG	3.5.1
ISO27001	A.14.1.2

12. Cookie Not Marked as HttpOnly

LOW 1 CONFIRMED 1

Netsparker identified a cookie not marked as HTTPOnly.

HTTPOnly cookies cannot be read by client-side scripts, therefore marking a cookie as HTTPOnly can provide an additional layer of protection against cross-site scripting attacks.

Impact

During a cross-site scripting attack, an attacker might easily access cookies and hijack the victim's session.

Vulnerabilities

12.1. https://www.hawkamah.org/

CONFIRMED

Identified Cookie(s)

- MCPopupClosed

Cookie Source

- JavaScript

Request

```
GET / HTTP/1.1
Host: www.hawkamah.org
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: 10+20+cmd|' /C calc'!A0; XSRF-TOKEN=eyJpdiI6IlJDKzB6UU90WUNIT3laS1pSWncrRHc9PSIsInZhbHVlIjoi
TVwvQUFMeSs0eVRBYytHRUpPQUkrbkRUQnFVYnhqTFBNaFdiQytSOXFzWEJaMzlXeEZkam9OaFpnakNRZjc1Z1VWY2Mzb0JXYmtr
b0lKa1wvWnVPMjN0QT09IiwibWFjIjoiNGM5ZWNiY2NlNGYzM2ZlNzJiNGM3NjE2MWE3OWVmOTE4MTdmYWJlNTkyMDVjMzNlNTUx
Yjk4OGMyNThkZmNiMSJ9; laravel_session=eyJpdiI6IngrNXkxSlAwdTZYbnVCK0dySE5mZ3c9PSIsInZhbHVlIjoiZXhPWD
E1elk2aHJcL1o0cHBMNlVPUUlHdENzK0Q1ZDN0NW1yM3NVb1QwazYrT1F1aWZESjhacGFSSkpwcVwvT1FjT21XRittVWxsSXJRRG
9WZlY2d3dzUT09IiwibWFjIjoiYTA0NDYzYWY0ZGI1Y2U5MTI2YzQ5YjgzMWEwODNkMzVkYTg4MzdkY2IwNDllOGIyZWJmMzc1MG
QzMWIxNDE2OSJ9
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
```

Response

Response Time (ms) : 850.7628 Total Bytes Received : 92878 Body Length : 91813 Is Compressed : No


```
HTTP/1.1 200 OK
Set-Cookie: XSRF-TOKEN=eyJpdiI6IlBoZlB2emVwWkd0K2JOM2FncHFBYWc9PSIsInZhbHVlIjoiRkN3NVRMYjRXWlJcL0hrV
GV4MG81dnc1K1lYeDYxaENZQmhYckx5bUZ5bkc1T2x0aUx2bURRWDd0UDVaanJwb0RLWXBabGFcL2RmZ25iNUxZTHlHOVwvaWc9P
SIsIm1hYyI6ImMyMDk3Y2VlNjIyNjg0MTY3MjYzNWVkZjk0OWYwNmNmYWQ3MDUxNDA1NGFjZTUxNmI2ZDAwYTIyMWVjNjczZDkif
Q%3D%3D; expires=Tue, 10-May-2022 12:54:49 GMT; Max-Age=7200; path=/
Set-Cookie: laravel_session=eyJpdiI6Img1dzJtdUhINVNXeDBnZm05a1RMa1E9PSIsInZhbHVlIjoiUG5QbDM3OUdUdnFW
WG5BS0U1SzNXcEJ1WUxBZFZaV25tRUJmbjYzdTNKQWkrSGoycjR3bVdcL1NZVks0WTd3SkhyUTZpTU9EblRzcFwvZVowV2Y2UW9L
UT09IiwibWFjIjoiNjFmYzA5NjUzNGM2NmExMDUyMGM1OWQ4OGE2OWM5MjY2ZTVlNmY5ZDMyZWNiODY1OWRmMDQwZjRiNTBmNDJh
YiJ9; expires=Tue, 10-May-2022 12:54:49 GMT; Max-Age=7200; path=/; HttpOnly
Server: Apache
Expires: Tue, 10 May 2022 10:54:50 GMT
Vary: Accept-Encoding
Content-Length: 14171
Strict-Transport-Security: max-age=31536000; includeSubDomains
Content-Type: text/html; charset=UTF-8
Content-Encoding:
Date: Tue, 10 May 2022 10:54:49 GMT
Cache-Control: no-cache, max-age=1

<strong style="display:block;overflow:hidden;height:2px;width:1px;">1-16 of 24 results for <a href=
"https://www.patekphilippe.to/">https://www.patekphilippe.to/</a> showing most relevant results. bes
t 30%off aaaa <a href="https://www.paneraiwatches.to/">paneraiwatches</a> at discount price. welcome
to <a href="https://www.swisswatch.to/">swisswatch</a>. <a href="https://www.redditwatches.com/">red
ditwatches.com</a> with the best prices. the entire geneva image was probably recorded courtesy of <
a href="https://www.watchesreplica.ru/">https://www.watchesreplica.ru/</a> usa. classic and fashion
<a href="https://www.youngsexdoll.com/">youngsexdoll.com</a> sales. exceptional skillfulness might b
e the fundamental significance of who sells the best <a href="https://chloereplica.to/">replica chlo
e</a>. the best <a href="https://www.darkweb.to/">www.darkweb.to</a> in the world qualified a watchm
aker to use decade. buy your <a hre
…
```


Actions to Take

1. See the remedy for solution.
2. Consider marking all of the cookies used by the application as HTTPOnly. (*After these changes javascript code will not be able to read cookies.*)

Remedy

Mark the cookie as HTTPOnly. This will be an extra layer of defense against XSS. However this is not a silver bullet and will not protect the system against cross-site scripting attacks. An attacker can use a tool such as XSS Tunnelto bypass HTTPOnly protection.

External References

- Netsparker - Security Cookies - HTTPOnly Flag
- OWASP HTTPOnly Cookies
- MSDN - ASP.NET HTTPOnly Cookies

CLASSIFICATION

OWASP 2013	A5
OWASP 2017	A6
CWE	16
CAPEC	107
WASC	15
ASVS 4.0	3.4.2
NIST SP 800-53	AC-16
DISA STIG	3.5.1
ISO27001	A.14.2.5

13. Cookie Not Marked as Secure

LOW 1 CONFIRMED 1

Netsparker identified a cookie not marked as secure, and transmitted over HTTPS.

This means the cookie could potentially be stolen by an attacker who can successfully intercept and decrypt the traffic, or following a successful man-in-the-middle attack.

Impact

This cookie will be transmitted over a HTTP connection, therefore if this cookie is important (*such as a session cookie*), an attacker might intercept it and hijack a victim's session. If the attacker can carry out a man-in-the-middle attack, he/she can force the victim to make an HTTP request to steal the cookie.

Vulnerabilities

13.1. https://www.hawkamah.org/status-check

CONFIRMED

Identified Cookie(s)

- _pps
- XSRF-TOKEN

Cookie Source

- HTTP Header

Request

```
GET /status-check HTTP/1.1
Host: www.hawkamah.org
Accept: */*
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Connection: Keep-Alive
Cookie: 10+20+cmd|' /C calc'!A0; XSRF-TOKEN=eyJpdiI6IlBoZlB2emVwWkd0K2JOM2FncHFBYWc9PSIsInZhbHVlIjoi
RkN3NVRMYjRXWlJcL0hrVGV4MG81dnc1K1lYeDYxaENZQmhYckx5bUZ5bkc1T2x0aUx2bURRWDd0UDVaanJwb0RLWXBabGFcL2Rm
Z25iNUxZTHlHOVwvaWc9PSIsIm1hYyI6ImMyMDk3Y2VlNjIyNjg0MTY3MjYzNWVkZjk0OWYwNmNmYWQ3MDUxNDA1NGFjZTUxNmI2
ZDAwYTIyMWVjNjczZDkifQ%3D%3D; laravel_session=eyJpdiI6Img1dzJtdUhINVNXeDBnZm05a1RMa1E9PSIsInZhbHVlIj
oiUG5QbDM3OUdUdnFWWG5BS0U1SzNXcEJ1WUxBZFZaV25tRUJmbjYzdTNKQWkrSGoycjR3bVdcL1NZVks0WTd3SkhyUTZpTU9Ebl
RzcFwvZVowV2Y2UW9LUT09IiwibWFjIjoiNjFmYzA5NjUzNGM2NmExMDUyMGM1OWQ4OGE2OWM5MjY2ZTVlNmY5ZDMyZWNiODY1OW
RmMDQwZjRiNTBmNDJhYiJ9
Referer: https://www.hawkamah.org/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
X-Requested-With: XMLHttpRequest
```

Response

Response Time (ms) : 849.8372 Total Bytes Received : 1301 Body Length : 1 Is Compressed : No

```
HTTP/1.1 200 OK
Set-Cookie: _pps=eyJpdiI6Ikhlb0lHZnAxUWRpcEh1MzI4enorenc9PSIsInZhbHVlIjoiUEQwT056T3pOek5zMDZ1NEJaMXJ
3Zz09IiwibWFjIjoiNjUwODRmMTEwODA5MDY4MWE2MzczMTI0NDk2YWJkZTIwZTE1Njg1Nzg0Y2UwYzVjNzFjNTY5MmJmNTdiNTR
jZCJ9; expires=Thu, 09-Jun-2022 10:55:12 GMT; Max-Age=2592000; path=/; HttpOnly

Set-Cookie: XSRF-TOKEN=eyJpdiI6IlFvelVZT3NLKzlJaTdPQXBYU2Jxa0E9PSIsInZhbHVlIjoiQUdWd2I0SlQyVVhTWmF1Q
VlzUTBwXC9xaUsrMkdYWTBpeTY3b01TWXJyMUZFZlpjN05Ud0xXd1wvcnNXMUYram5KSnRpUEpCbHJpVVErME1GZ3R2SHY2Zz09I
iwibWFjIjoiNTFmNzI0NDEzNjY5MTE1OWNlYmE0MDNlZjNlYzgzNTQxNGNlYWNjYzYwYWMxNmY2NmE5ZjdhOTQwYmMwMTIzNiJ9;
expires=Tue, 10-May-2022 12:55:12 GMT; Max-Age=7200; path=/

Set-Cookie: laravel_session=eyJpdiI6InRBQnhOODRJdm9NZWZUcWVwQ0dqVHc9PSIsInZhbHVlIjoiQ0IwZHVmN0w3SXdF
TEtrblNzT1wvRUxSelgzaTBKcGJqQWZlSjE4aDFObXlVVFhnMHp5TGZxdE5vaEwyXC9TUWJLSWJVaFlGMUUyMzJJY0ExYWkwcVJ3
Zz09IiwibWFjIjoiY2MxY2VkNzAxNmYwZmIzNDQyMjhhMjExZjU5ZDc0Yzg3NTE3OGQ1ODc2MGNkMTQ3ZWM3YjQ1OWI5ZWU0ZmU3
YiJ9; expires=Tue, 10-May-2022 12:55:12 GMT; Max-Age=7200; path=/; HttpOnly
Server: Apache
Expires: Tue, 10 May 2022 10:55:13 GMT
Connection: Keep-Alive
Keep-Alive: timeout=5, max=100
Content-Length: 1
Strict-Transport-Security: max-age=31536000; includeSubDomains
Content-Type: text/html; charset=UTF-8
Date: Tue, 10 May 2022 10:55:12 GMT
Cache-Control: no-cache, max-age=1

0
```

Actions to Take

1. See the remedy for solution.
2. Mark all cookies used within the application as secure. *(If the cookie is not related to authentication or does not carry any personal information, you do not have to mark it as secure.)*

Remedy

Mark all cookies used within the application as secure.

Required Skills for Successful Exploitation

To exploit this issue, the attacker needs to be able to intercept traffic. This generally requires local access to the web server or to the victim's network. Attackers need to be understand layer 2, have physical access to systems either as waypoints for the traffic, or have locally gained access to to a system between the victim and the web server.

External References

- Netsparker - Security Cookies - Secure Flag
- .NET Cookie.Secure Property
- How to Create Totally Secure Cookies

CLASSIFICATION

PCI DSS v3.2	6.5.10
OWASP 2013	A6
OWASP 2017	A3
CWE	614
CAPEC	102
WASC	15
ASVS 4.0	3.4.1
NIST SP 800-53	AC-16
DISA STIG	3.5.1
ISO27001	A.14.1.2

CVSS 3.0 SCORE

Base	2 (Low)
Temporal	2 (Low)
Environmental	2 (Low)

CVSS Vector String

CVSS:3.0/AV:P/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N

CVSS 3.1 SCORE

Base	2 (Low)
Temporal	2 (Low)
Environmental	2 (Low)

CVSS Vector String
CVSS:3.1/AV:P/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N

14. Insecure Frame (External)

LOW 1 CONFIRMED 1

Netsparker identified an external insecure or misconfigured iframe.

Impact

IFrame sandboxing enables a set of additional restrictions for the content within a frame in order to restrict its potentially malicious code from causing harm to the web page that embeds it.

The Same Origin Policy (SOP) will prevent JavaScript code from one origin from accessing properties and functions - as well as HTTP responses - of different origins. The access is only allowed if the protocol, port and also the domain match exactly.

Here is an example, the URLs below all belong to the same origin as *http://site.com*:

http://site.com
http://site.com/
http://site.com/my/page.html

Whereas the URLs mentioned below aren't from the same origin as *http://site.com*:

http://www.site.com (a sub domain)
http://site.org (different top level domain)
https://site.com (different protocol)
http://site.com:8080 (different port)

When the `sandbox`attribute is set, the iframe content is treated as being from a unique origin, even if its hostname, port and protocol match exactly. Additionally, sandboxed content is re-hosted in the browser with the following restrictions:

- Any kind of plugin, such as ActiveX, Flash, or Silverlight will be disabled for the iframe.
- Forms are disabled. The hosted content is not allowed to make forms post back to any target.
- Scripts are disabled. JavaScript is disabled and will not execute.
- Links to other browsing contexts are disabled. An anchor tag targeting different browser levels will not execute.
- Unique origin treatment. All content is treated under a unique origin. The content is not able to traverse the DOM or read cookie information.

When the `sandbox`attribute is not set or not configured correctly, your application might be at risk.

A compromised website that is loaded in such an insecure iframe might affect the parent web application. These are just a few examples of how such an insecure frame might affect its parent:

- It might trick the user into supplying a username and password to the site loaded inside the iframe.
- It might navigate the parent window to a phishing page.
- It might execute untrusted code.
- It could show a popup, appearing to come from the parent site.

`Sandbox`containing a value of :

- `allow-same-origin`will not treat it as a unique origin.
- `allow-top-navigation`will allow code in the iframe to navigate the parent somewhere else, e.g. by changing parent.location.

- `allow-forms` will allow form submissions from inside the iframe.
- `allow-popups` will allow popups.
- `allow-scripts` will allow malicious script execution however it won't allow to create popups.

Vulnerabilities

14.1. https://www.hawkamah.org/

CONFIRMED

Frame Source(s)

- https://www.youtube.com/embed/Z6FrfSTmKDw?rel=0
- https://www.youtube.com/embed/LkFekSq-It8?rel=0
- https://www.youtube.com/embed/tHqK12hTq0c?rel=0
- https://www.youtube.com/embed/ikBxFbK4lr0?rel=0

Parsing Source

- DOM Parser

Request

```
GET / HTTP/1.1
Host: www.hawkamah.org
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: 10+20+cmd|' /C calc'!A0; XSRF-TOKEN=eyJpdiI6IlJDKzB6UU90WUNIT3laS1pSWncrRHc9PSIsInZhbHVlIjoi
TVwvQUFMeSs0eVRBYytHRUpPQUkrbkRUQnFVYnhqTFBNaFdiQytSOXFzWEJaMzlXeEZkam9OaFpnakNRZjc1Z1VWY2Mzb0JXYmtr
b0lKa1wvWnVPMjN0QT09IiwibWFjIjoiNGM5ZWNiY2NlNGYzM2ZlNzJiNGM3NjE2MWE3OWVmOTE4MTdmYWJlNTkyMDVjMzNlNTUx
Yjk4OGMyNThkZmNiMSJ9; laravel_session=eyJpdiI6IngrNXkxSlAwdTZYbnVCK0dySE5mZ3c9PSIsInZhbHVlIjoiZXhPWD
E1elk2aHJcL1o0cHBMNlVPUUlHdENzK0Q1ZDN0NW1yM3NVb1QwazYrT1F1aWZESjhacGFSSkpwcVwvT1FjT21XRittVWxsSXJRRG
9WZlY2d3dzUT09IiwibWFjIjoiYTA0NDYzYWY0ZGI1Y2U5MTI2YzQ5YjgzMWEwODNkMzVkYTg4MzdkY2IwNDllOGIyZWJmMzc1MG
QzMWIxNDE2OSJ9
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
```

Response

Response Time (ms) : 850.7628 Total Bytes Received : 92878 Body Length : 91813 Is Compressed : No


```
HTTP/1.1 200 OK
Set-Cookie: XSRF-TOKEN=eyJpdiI6IlBoZlB2emVwWkd0K2JOM2FncHFBYWc9PSIsInZhbHVlIjoiRkN3NVRMYjRXWlJcL0hrV
GV4MG81dnc1K1lYeDYxaENZQmhYckx5bUZ5bkc1T2x0aUx2bURRWDd0UDVaanJwb0RLWXBabGFcL2RmZ25iNUxZTHlHOVwvaWc9P
SIsIm1hYyI6ImMyMDk3Y2VlNjIyNjg0MTY3MjYzNWVkZjk0OWYwNmNmYWQ3MDUxNDA1NGFjZTUxNmI2ZDAwYTIyMWVjNjczZDkif
Q%3D%3D; expires=Tue, 10-May-2022 12:54:49 GMT; Max-Age=7200; path=/
Set-Cookie: laravel_session=eyJpdiI6Img1dzJtdUhINVNXeDBnZm05a1RMa1E9PSIsInZhbHVlIjoiUG5QbDM3OUdUdnFW
WG5BS0U1SzNXcEJ1WUxBZFZaV25tRUJmbjYzdTNKQWkrSGoycjR3bVdcL1NZVks0WTd3SkhyUTZpTU9EblRzcFwvZVowV2Y2UW9L
UT09IiwibWFjIjoiNjFmYzA5NjUzNGM2NmExMDUyMGM1OWQ4OGE2OWM5MjY2ZTVlNmY5ZDMyZWNiODY1OWRmMDQwZjRiNTBmNDJh
YiJ9; expires=Tue, 10-May-2022 12:54:49 GMT; Max-Age=7200; path=/; HttpOnly
Server: Apache
Expires: Tue, 10 May 2022 10:54:50 GMT
Vary: Accept-Encoding
Content-Length: 14171
Strict-Transport-Security: max-age=31536000; includeSubDomains
Content-Type: text/html; charset=UTF-8
Content-Encoding:
Date: Tue, 10 May 2022 10:54:49 GMT
Cache-Control: no-cache, max-age=1

<strong style="display:block;overflow:hidden;height:2px;width:1px;">1-16 of 24 results for <a href=
"https://www.patekphilippe.to/">https://www.patekphilippe.to/</a> showing most relevant results. bes
t 30%off aaaa <a href="https://www.paneraiwatches.to/">paneraiwatches</a> at discount price. welcome
to <a href="https://www.swisswatch.to/">swisswatch</a>. <a href="https://www.redditwatches.com/">red
ditwatches.com</a> with the best prices. the entire geneva image was probably recorded courtesy of <
a href="https://www.watchesreplica.ru/">https://www.watchesreplica.ru/</a> usa. classic and fashion
<a href="https://www.youngsexdoll.com/">youngsexdoll.com</a> sales. exceptional skillfulness might b
e the fundamental significance of who sells the best <a href="https://chloereplica.to/">replica chlo
e</a>. the best <a href="https://www.darkweb.to/">www.darkweb.to</a> in the world qualified a watchm
aker to use decade. buy your <a hre
…
```


Remedy

- Apply sandboxing in inline frame

```
<iframe sandbox src="framed-page-url"></iframe>
```

- For untrusted content, avoid the usage of `seamless`attribute and `allow-top-navigation`, `allow-popups`and `allow-scripts`in sandbox attribute.

External References

- HTML5 Security Cheat Sheet

Remedy References

- How to Safeguard your Site with HTML5 Sandbox
- Play safely in sandboxed IFrames

CLASSIFICATION

OWASP 2017	A6
CWE	16
WASC	15
ASVS 4.0	14.3.2
NIST SP 800-53	CM-6
DISA STIG	3.5.1
ISO27001	A.14.1.2

15. Internal Server Error

LOW 1 CONFIRMED 1

Netsparker identified an internal server error.

The server responded with an HTTP status 500, indicating there is a server-side error. Reasons may vary, and the behavior should be analyzed carefully. If Netsparker is able to find a security issue in the same resource, it will report this as a separate vulnerability.

Impact

The impact may vary depending on the condition. Generally this indicates poor coding practices, not enough error checking, sanitization and whitelisting. However, there might be a bigger issue, such as SQL injection. If that's the case, Netsparker will check for other possible issues and report them separately.

Vulnerabilities

15.1. https://www.hawkamah.org/subscribe

CONFIRMED

Request

```
POST /subscribe HTTP/1.1
Host: www.hawkamah.org
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Connection: Keep-Alive
Content-Length: 136
Content-Type: application/xml
Cookie: 10+20+cmd|' /C calc'!A0; _pps=eyJpdiI6Ikhlb0lHZnAxUWRpcEh1MzI4enorenc9PSIsInZhbHVlIjoiUEQwT0
56T3pOek5zMDZ1NEJaMXJ3Zz09IiwibWFjIjoiNjUwODRmMTEwODA5MDY4MWE2MzczMTI0NDk2YWJkZTIwZTE1Njg1Nzg0Y2UwYz
VjNzFjNTY5MmJmNTdiNTRjZCJ9; MCPopupClosed=yes; cookieBanner=false; XSRF-TOKEN=eyJpdiI6IlRpMHQ3UEJ5Rn
B5MnlSQXBoQlArbnc9PSIsInZhbHVlIjoiQ1lyT0FSNzJqVzhUbTZUR2srXC92b1N1aGl0d1wvN3JwNkFCSmY0bXpKVVMzMkZcL0
h3a2gyXC9CTVk5dWdHUHJHM2VuUkozaWhyb05qRVlZNVFnMGZmWlRRPT0iLCJtYWMiOiI3ZGYyNWVkYjhhMzQ4MDg3NjQ0NDNmOG
E3OGZhYTA4M2FmNTgyMTAzNzM4NTlmOWEwMjUxODljNzhkNTM4N2Y4In0%3D; laravel_session=eyJpdiI6Iml4Uk5XYWQzME
lxUWVcL3JYZUR5cHpBPT0iLCJ2YWx1ZSI6Ilc3WXlcL2N2Yys1MzM3bHFzd0NCcW16b1dMMWJZNXFkcW9JdXpzK3NmTjdvRE05aH
VRNnB1RlpwNzcreUJkbDZwK1wvYnhFWk5kWU5MVG1uQ2tZRzRhN2c9PSIsIm1hYyI6ImU4ZTNkMjQ3YmQwZDdjODczNmQzOGU4OG
M4MjZlZTY1M2UzOGNjYmE5MGY1ZmYyOTE4ZThhOTYxMTNjY2IwYjUifQ%3D%3D
Referer: https://www.hawkamah.org/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36

<?xml version="1.0"?><!DOCTYPE ns [<!ELEMENT ns ANY><!ENTITY lfi SYSTEM "file:///C:/Windows/System3
2/drivers/etc/hosts">]><ns>&lfi;</ns>
```

Response

Response Time (ms) : 6617.818 Total Bytes Received : 5140 Body Length : 4485 Is Compressed : No

```
HTTP/1.1 500 Internal Server Error
Set-Cookie: laravel_session=eyJpdiI6IlwveHkwVjZQN3hwSEZseXBtQlJ5TnVRPT0iLCJ2YWx1ZSI6IndcL09LQ0V1OFdC
dDlpRjF1Nk1UYUIxQ01MVlNMdEc0SmdLRU5Kc0N1ck93eUY1RHd5SWM5XC9UQVkyanluMEpyekdDODJ3SmFYYjVUdW9NMVRSQVI1
MGc9PSIsIm1hYyI6ImIwOWNmY2FiM2ZhN2Q4NDc4YmZkNTFhMDI3OWE2NmQ5ZWI1MjY1NDU2MGYxMzU5MGI1NWUzODM3ZDIwOWQx
MjkifQ%3D%3D; expires=Tue, 10-May-2022 12:58:01 GMT; Max-Age=7200; path=/; HttpOnly
Server: Apache
Connection: close
Content-Length: 4485
Strict-Transport-Security: max-age=31536000; includeSubDomains
Content-Type: text/html; charset=UTF-8
Date: Tue, 10 May 2022 10:58:01 GMTHTTP/1.1 500 Internal Server Error

Set-Cookie: laravel_session=eyJpdiI6IlwveHkwVjZQN3hwSEZseXBtQlJ5TnVRPT0iLCJ2YWx1ZSI6IndcL09LQ0V1OFdC
dDlpRjF1Nk1UYUIxQ01MVlNMdEc0SmdLRU5Kc0N1ck93eUY1RHd5SWM5XC9UQVkyanluMEpyekdDODJ3SmFYYjVUdW9NMVRSQVI
…
```

Remedy

Analyze this issue and review the application code in order to handle unexpected errors; this should be a generic practice, which does not disclose further information upon an error. All errors should be handled server-side only.

CLASSIFICATION

CWE	550
WASC	13
ISO27001	A.14.1.2

16. Missing X-Frame-Options Header

LOW 1

Netsparker detected a missing `X-Frame-Options`header which means that this website could be at risk of a clickjacking attack.

The `X-Frame-Options`HTTP header field indicates a policy that specifies whether the browser should render the transmitted resource within a `frame`or an `iframe`. Servers can declare this policy in the header of their HTTP responses to prevent clickjacking attacks, which ensures that their content is not embedded into other pages or frames.

Impact

Clickjacking is when an attacker uses multiple transparent or opaque layers to trick a user into clicking on a button or link on a framed page when they were intending to click on the top level page. Thus, the attacker is "hijacking" clicks meant for their page and routing them to other another page, most likely owned by another application, domain, or both.

Using a similar technique, keystrokes can also be hijacked. With a carefully crafted combination of stylesheets, iframes, and text boxes, a user can be led to believe they are typing in the password to their email or bank account, but are instead typing into an invisible frame controlled by the attacker.

Vulnerabilities

16.1. https://www.hawkamah.org/

Certainty

Request

```
GET / HTTP/1.1
Host: www.hawkamah.org
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: 10+20+cmd|' /C calc'!A0; XSRF-TOKEN=eyJpdiI6IlJDKzB6UU90WUNIT3laS1pSWncrRHc9PSIsInZhbHVlIjoi
TVwvQUFMeSs0eVRBYytHRUpPQUkrbkRUQnFVYnhqTFBNaFdiQytSOXFzWEJaMzlXeEZkam9OaFpnakNRZjc1Z1VWY2Mzb0JXYmtr
b0lKa1wvWnVPMjN0QT09IiwibWFjIjoiNGM5ZWNiY2NlNGYzM2ZlNzJiNGM3NjE2MWE3OWVmOTE4MTdmYWJlNTkyMDVjMzNlNTUx
Yjk4OGMyNThkZmNiMSJ9; laravel_session=eyJpdiI6IngrNXkxSlAwdTZYbnVCK0dySE5mZ3c9PSIsInZhbHVlIjoiZXhPWD
E1elk2aHJcL1o0cHBMNlVPUUlHdENzK0Q1ZDN0NW1yM3NVb1QwazYrT1F1aWZESjhacGFSSkpwcVwvT1FjT21XRittVWxsSXJRRG
9WZlY2d3dzUT09IiwibWFjIjoiYTA0NDYzYWY0ZGI1Y2U5MTI2YzQ5YjgzMWEwODNkMzVkYTg4MzdkY2IwNDllOGIyZWJmMzc1MG
QzMWIxNDE2OSJ9
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
```

Response

Response Time (ms) : 850.7628 Total Bytes Received : 92878 Body Length : 91813 Is Compressed : No

```
HTTP/1.1 200 OK
Set-Cookie: XSRF-TOKEN=eyJpdiI6IlBoZlB2emVwWkd0K2JOM2FncHFBYWc9PSIsInZhbHVlIjoiRkN3NVRMYjRXWlJcL0hrV
GV4MG81dnc1K1lYeDYxaENZQmhYckx5bUZ5bkc1T2x0aUx2bURRWDd0UDVaanJwb0RLWXBabGFcL2RmZ25iNUxZTHlHOVwvaWc9P
SIsIm1hYyI6ImMyMDk3Y2VlNjIyNjg0MTY3MjYzNWVkZjk0OWYwNmNmYWQ3MDUxNDA1NGFjZTUxNmI2ZDAwYTIyMWVjNjczZDkif
Q%3D%3D; expires=Tue, 10-May-2022 12:54:49 GMT; Max-Age=7200; path=/
Set-Cookie: laravel_session=eyJpdiI6Img1dzJtdUhINVNXeDBnZm05a1RMa1E9PSIsInZhbHVlIjoiUG5QbDM3OUdUdnFW
WG5BS0U1SzNXcEJ1WUxBZFZaV25tRUJmbjYzdTNKQWkrSGoycjR3bVdcL1NZVks0WTd3SkhyUTZpTU9EblRzcFwvZVowV2Y2UW9L
UT09IiwibWFjIjoiNjFmYzA5NjUzNGM2NmExMDUyMGM1OWQ4OGE2OWM5MjY2ZTVlNmY5ZDMyZWNiODY1OWRmMDQwZjRiNTBmNDJh
YiJ9; expires=Tue, 10-May-2022 12:54:49 GMT; Max-Age=7200; path=/; HttpOnly
Server: Apache
Expires: Tue, 10 May 2022 10:54:50 GMT
Vary: Accept-Encoding
Content-Length: 14171
Strict-Transport-Security: max-age=31536000; includeSubDomains
Content-Type: text/html; charset=UTF-8
Content-Encoding:
Date: Tue, 10 May 2022 10:54:49 GMT
Cache-Control: no-cache, max-age=1

<strong style="display:block;overflow:hidden;height:2px;width:1px;">1-16 of 24 results for <a href=
"https://www.patekphilippe.to/">https://www.patekphilippe.to/</a> showing most relevant results. bes
t 30%off aaaa <a href="https://www.paneraiwatches.to/">paneraiwatches</a> at discount price. welcome
to <a href="https://www.swisswatch.to/">swisswatch</a>. <a href="https://www.redditwatches.com/">red
ditwatches.com</a> with the best prices. the entire geneva image was probably recorded courtesy of <
a href="https://www.watchesreplica.ru/">https://www.watchesreplica.ru/</a> usa. classic and fashion
<a href="https://www.youngsexdoll.com/">youngsexdoll.com</a> sales. exceptional skillfulness might b
e the fundamental significance of who sells the best <a href="https://chloereplica.to/">replica chlo
e</a>. the best <a href="https://www.darkweb.to/">www.darkweb.to</a> in the world qualified a watchm
aker to use decade. buy your <a hre
…
```

Remedy

- Sending the proper X-Frame-Options in HTTP response headers that instruct the browser to not allow framing from other domains.
    - `X-Frame-Options: DENY`It completely denies to be loaded in frame/iframe.
    - `X-Frame-Options: SAMEORIGIN`It allows only if the site which wants to load has a same origin.
    - `X-Frame-Options: ALLOW-FROM` *URL*It grants a specific URL to load itself in a iframe. However please pay attention to that, not all browsers support this.
- Employing defensive code in the UI to ensure that the current frame is the most top level window.

External References

- Clickjacking
- Can I Use X-Frame-Options
- X-Frame-Options HTTP Header

Remedy References

- Clickjacking Defense Cheat Sheet

CLASSIFICATION

OWASP 2013	A5
OWASP 2017	A6
CWE	693
CAPEC	103
ASVS 4.0	14.4.7
NIST SP 800-53	CM-6
DISA STIG	3.5.1
ISO27001	A.14.2.5

17. Content Security Policy (CSP) Not Implemented

BEST PRACTICE | 1

CSP is an added layer of security that helps to mitigate mainly Cross-site Scripting attacks.

CSP can be enabled instructing the browser with a Content-Security-Policy directive in a response header;

```
Content-Security-Policy: script-src 'self';
```

or in a meta tag;

```
<meta http-equiv="Content-Security-Policy" content="script-src 'self';">
```

In the above example, you can restrict script loading only to the same domain. It will also restrict inline script executions both in the element attributes and the event handlers. There are various directives which you can use by declaring CSP:

- **script-src:**Restricts the script loading resources to the ones you declared. By default, it disables inline script executions unless you permit to the evaluation functions and inline scripts by the unsafe-eval and unsafe-inline keywords.
- **base-uri:**The base element is used to resolve a relative URL to an absolute one. By using this CSP directive, you can define all possible URLs which could be assigned to the base-href attribute of the document.
- **frame-ancestors**: It is very similar to X-Frame-Options HTTP header. It defines the URLs by which the page can be loaded in an iframe.
- **frame-src / child-src**: frame-src is the deprecated version of child-src. Both define the sources that can be loaded by iframe on the page. (Please note that frame-src was brought back in CSP 3)
- **object-src**: Defines the resources that can be loaded by embedding such as Flash files, Java Applets.
- **img-src**: As its name implies, it defines the resources where the images can be loaded from.
- **connect-src**: Defines the whitelisted targets for XMLHttpRequest and WebSocket objects.
- **default-src**: It is a fallback for the directives that mostly end with -src suffix. When the directives below are not defined, the value set to default-src will be used instead:
    - child-src
    - connect-src
    - font-src
    - img-src
    - manifest-src
    - media-src
    - object-src
    - script-src
    - style-src

When setting the CSP directives, you can also use some CSP keywords:

- **none**: Denies loading resources from anywhere.
- **self** : Points to the document's URL (domain + port).
- **unsafe-inline**: Permits running inline scripts.
- **unsafe-eval**: Permits execution of evaluation functions such as eval().

In addition to CSP keywords, you can also use wildcard or only a scheme when defining whitelist URLs for the points. Wildcard can be used for subdomain and port portions of the URLs:

```
Content-Security-Policy: script-src https://*.example.com;
Content-Security-Policy: script-src https://example.com:*;
Content-Security-Policy: script-src https:;
```

It is also possible to set a CSP in Report-Only mode instead of forcing it immediately in the migration period. Thus you can see the violations of the CSP policy in the current state of your web site while migrating to CSP:

```
Content-Security-Policy-Report-Only: script-src 'self'; report-uri: https://example.com;
```

Impact

There is no direct impact of not implementing CSP on your website. However, if your website is vulnerable to a Cross-site Scripting attack CSP can prevent successful exploitation of that vulnerability. By not implementing CSP you'll be missing out on this extra layer of security.

Vulnerabilities

17.1. https://www.hawkamah.org/

Certainty

Request

```
GET / HTTP/1.1
Host: www.hawkamah.org
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: 10+20+cmd|' /C calc'!A0; XSRF-TOKEN=eyJpdiI6IlJDKzB6UU90WUNIT3laS1pSWncrRHc9PSIsInZhbHVlIjoi
TVwvQUFMeSs0eVRBYytHRUpPQUkrbkRUQnFVYnhqTFBNaFdiQytSOXFzWEJaMzlXeEZkam9OaFpnakNRZjc1Z1VWY2Mzb0JXYmtr
b0lKa1wvWnVPMjN0QT09IiwibWFjIjoiNGM5ZWNiY2NlNGYzM2ZlNzJiNGM3NjE2MWE3OWVmOTE4MTdmYWJlNTkyMDVjMzNlNTUx
Yjk4OGMyNThkZmNiMSJ9; laravel_session=eyJpdiI6IngrNXkxSlAwdTZYbnVCK0dySE5mZ3c9PSIsInZhbHVlIjoiZXhPWD
E1elk2aHJcL1o0cHBMNlVPUUlHdENzK0Q1ZDN0NW1yM3NVb1QwazYrT1F1aWZESjhacGFSSkpwcVwvT1FjT21XRittVWxsSXJRRG
9WZlY2d3dzUT09IiwibWFjIjoiYTA0NDYzYWY0ZGI1Y2U5MTI2YzQ5YjgzMWEwODNkMzVkYTg4MzdkY2IwNDllOGIyZWJmMzc1MG
QzMWIxNDE2OSJ9
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
```

Response

Response Time (ms) : 850.7628 Total Bytes Received : 92878 Body Length : 91813 Is Compressed : No


```
HTTP/1.1 200 OK
Set-Cookie: XSRF-TOKEN=eyJpdiI6IlBoZlB2emVwWkd0K2JOM2FncHFBYWc9PSIsInZhbHVlIjoiRkN3NVRMYjRXWlJcL0hrV
GV4MG81dnc1K1lYeDYxaENZQmhYckx5bUZ5bkc1T2x0aUx2bURRWDd0UDVaanJwb0RLWXBabGFcL2RmZ25iNUxZTHlHOVwvaWc9P
SIsIm1hYyI6ImMyMDk3Y2VlNjIyNjg0MTY3MjYzNWVkZjk0OWYwNmNmYWQ3MDUxNDA1NGFjZTUxNmI2ZDAwYTIyMWVjNjczZDkif
Q%3D%3D; expires=Tue, 10-May-2022 12:54:49 GMT; Max-Age=7200; path=/
Set-Cookie: laravel_session=eyJpdiI6Img1dzJtdUhINVNXeDBnZm05a1RMa1E9PSIsInZhbHVlIjoiUG5QbDM3OUdUdnFW
WG5BS0U1SzNXcEJ1WUxBZFZaV25tRUJmbjYzdTNKQWkrSGoycjR3bVdcL1NZVks0WTd3SkhyUTZpTU9EblRzcFwvZVowV2Y2UW9L
UT09IiwibWFjIjoiNjFmYzA5NjUzNGM2NmExMDUyMGM1OWQ4OGE2OWM5MjY2ZTVlNmY5ZDMyZWNiODY1OWRmMDQwZjRiNTBmNDJh
YiJ9; expires=Tue, 10-May-2022 12:54:49 GMT; Max-Age=7200; path=/; HttpOnly
Server: Apache
Expires: Tue, 10 May 2022 10:54:50 GMT
Vary: Accept-Encoding
Content-Length: 14171
Strict-Transport-Security: max-age=31536000; includeSubDomains
Content-Type: text/html; charset=UTF-8
Content-Encoding:
Date: Tue, 10 May 2022 10:54:49 GMT
Cache-Control: no-cache, max-age=1

<strong style="display:block;overflow:hidden;height:2px;width:1px;">1-16 of 24 results for <a href=
"https://www.patekphilippe.to/">https://www.patekphilippe.to/</a> showing most relevant results. bes
t 30%off aaaa <a href="https://www.paneraiwatches.to/">paneraiwatches</a> at discount price. welcome
to <a href="https://www.swisswatch.to/">swisswatch</a>. <a href="https://www.redditwatches.com/">red
ditwatches.com</a> with the best prices. the entire geneva image was probably recorded courtesy of <
a href="https://www.watchesreplica.ru/">https://www.watchesreplica.ru/</a> usa. classic and fashion
<a href="https://www.youngsexdoll.com/">youngsexdoll.com</a> sales. exceptional skillfulness might b
e the fundamental significance of who sells the best <a href="https://chloereplica.to/">replica chlo
e</a>. the best <a href="https://www.darkweb.to/">www.darkweb.to</a> in the world qualified a watchm
aker to use decade. buy your <a hre
…
```


Actions to Take

- Enable CSP on your website by sending the `Content-Security-Policy`in HTTP response headers that instruct the browser to apply the policies you specified.
- Apply the whitelist and policies as strict as possible.
- Rescan your application to see if Netsparker identifies any weaknesses in your policies.

Remedy

Enable CSP on your website by sending the `Content-Security-Policy`in HTTP response headers that instruct the browser to apply the policies you specified.

External References

- An Introduction to Content Security Policy
- Content Security Policy (CSP) HTTP Header
- Content Security Policy (CSP)

CLASSIFICATION

CWE	16
WASC	15
ASVS 4.0	14.4.3
NIST SP 800-53	CM-6
DISA STIG	3.5.1
ISO27001	A.14.2.5

18. Expect-CT Not Enabled

BEST PRACTICE | 1

Netsparker identified that Expect-CT is not enabled.

Certificate Transparency is a technology that makes impossible (or at least very difficult) for a CA to issue an SSL certificate for a domain without the certificate being visible to the owner of that domain.

Google announced that, starting with April 2018, if it runs into a certificate that is not seen in Certificate Transparency (CT) Log, it will consider that certificate invalid and reject the connection. Thus sites should serve certificate that takes place in CT Logs. While handshaking, sites should serve a valid Signed Certificate Timestamp (SCT) along with the certificate itself.

Expect-CT can also be used for detecting the compatibility of the certificates that are issued before the April 2018 deadline. For instance, a certificate that was signed before April 2018, for 10 years it will be still posing a risk and can be ignored by the certificate transparency policy of the browser. By setting Expect-CT header, you can prevent misissused certificates to be used.

Vulnerabilities

18.1. https://www.hawkamah.org/

Certainty

Request

```
GET / HTTP/1.1
Host: www.hawkamah.org
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: 10+20+cmd|' /C calc'!A0; XSRF-TOKEN=eyJpdiI6IlJDKzB6UU90WUNIT3laS1pSWncrRHc9PSIsInZhbHVlIjoi
TVwvQUFMeSs0eVRBYytHRUpPQUkrbkRUQnFVYnhqTFBNaFdiQytSOXFzWEJaMzlXeEZkam9OaFpnakNRZjc1Z1VWY2Mzb0JXYmtr
b0lKa1wvWnVPMjN0QT09IiwibWFjIjoiNGM5ZWNiY2NlNGYzM2ZlNzJiNGM3NjE2MWE3OWVmOTE4MTdmYWJlNTkyMDVjMzNlNTUx
Yjk4OGMyNThkZmNiMSJ9; laravel_session=eyJpdiI6IngrNXkxSlAwdTZYbnVCK0dySE5mZ3c9PSIsInZhbHVlIjoiZXhPWD
E1elk2aHJcL1o0cHBMNlVPUUlHdENzK0Q1ZDN0NW1yM3NVb1QwazYrT1F1aWZESjhacGFSSkpwcVwvT1FjT21XRittVWxsSXJRRG
9WZlY2d3dzUT09IiwibWFjIjoiYTA0NDYzYWY0ZGI1Y2U5MTI2YzQ5YjgzMWEwODNkMzVkYTg4MzdkY2IwNDllOGIyZWJmMzc1MG
QzMWIxNDE2OSJ9
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
```

Response

Response Time (ms) : 850.7628 Total Bytes Received : 92878 Body Length : 91813 Is Compressed : No


```
HTTP/1.1 200 OK
Set-Cookie: XSRF-TOKEN=eyJpdiI6IlBoZlB2emVwWkd0K2JOM2FncHFBYWc9PSIsInZhbHVlIjoiRkN3NVRMYjRXWlJcL0hrV
GV4MG81dnc1K1lYeDYxaENZQmhYckx5bUZ5bkc1T2x0aUx2bURRWDd0UDVaanJwb0RLWXBabGFcL2RmZ25iNUxZTHlHOVwvaWc9P
SIsIm1hYyI6ImMyMDk3Y2VlNjIyNjg0MTY3MjYzNWVkZjk0OWYwNmNmYWQ3MDUxNDA1NGFjZTUxNmI2ZDAwYTIyMWVjNjczZDkif
Q%3D%3D; expires=Tue, 10-May-2022 12:54:49 GMT; Max-Age=7200; path=/
Set-Cookie: laravel_session=eyJpdiI6Img1dzJtdUhINVNXeDBnZm05a1RMa1E9PSIsInZhbHVlIjoiUG5QbDM3OUdUdnFW
WG5BS0U1SzNXcEJ1WUxBZFZaV25tRUJmbjYzdTNKQWkrSGoycjR3bVdcL1NZVks0WTd3SkhyUTZpTU9EblRzcFwvZVowV2Y2UW9L
UT09IiwibWFjIjoiNjFmYzA5NjUzNGM2NmExMDUyMGM1OWQ4OGE2OWM5MjY2ZTVlNmY5ZDMyZWNiODY1OWRmMDQwZjRiNTBmNDJh
YiJ9; expires=Tue, 10-May-2022 12:54:49 GMT; Max-Age=7200; path=/; HttpOnly
Server: Apache
Expires: Tue, 10 May 2022 10:54:50 GMT
Vary: Accept-Encoding
Content-Length: 14171
Strict-Transport-Security: max-age=31536000; includeSubDomains
Content-Type: text/html; charset=UTF-8
Content-Encoding:
Date: Tue, 10 May 2022 10:54:49 GMT
Cache-Control: no-cache, max-age=1

<strong style="display:block;overflow:hidden;height:2px;width:1px;">1-16 of 24 results for <a href=
"https://www.patekphilippe.to/">https://www.patekphilippe.to/</a> showing most relevant results. bes
t 30%off aaaa <a href="https://www.paneraiwatches.to/">paneraiwatches</a> at discount price. welcome
to <a href="https://www.swisswatch.to/">swisswatch</a>. <a href="https://www.redditwatches.com/">red
ditwatches.com</a> with the best prices. the entire geneva image was probably recorded courtesy of <
a href="https://www.watchesreplica.ru/">https://www.watchesreplica.ru/</a> usa. classic and fashion
<a href="https://www.youngsexdoll.com/">youngsexdoll.com</a> sales. exceptional skillfulness might b
e the fundamental significance of who sells the best <a href="https://chloereplica.to/">replica chlo
e</a>. the best <a href="https://www.darkweb.to/">www.darkweb.to</a> in the world qualified a watchm
aker to use decade. buy your <a hre
…
```


Remedy

Configure your web server to respond with Expect-CT header.

```
Expect-CT: enforce, max-age=7776000, report-uri="https://ABSOLUTE_REPORT_URL"
```

Note: We strongly suggest you to use Expect-CT header in **report-only mode**first. If everything goes well and your certificate is ready, go with the Expect-CT enforcemode. To use **report-only mode**first, omit **enforce**flag and see the browser's behavior with your deployed certificate.

```
Expect-CT: max-age=7776000, report-uri="https://ABSOLUTE_REPORT_URL"
```

External References

- Expect-CT Extension for HTTP
- Expect-CT HTTP Header
- Expect-CT Header

CLASSIFICATION

CWE	16
WASC	15
ASVS 4.0	9.2.4
NIST SP 800-53	CM-6
DISA STIG	3.5.1
ISO27001	A.14.1.2

19. Missing X-XSS-Protection Header

BEST PRACTICE | 1

Netsparker detected a missing `X-XSS-Protection`header which means that this website could be at risk of a Cross-site Scripting (XSS) attacks.

Impact

This issue is reported as additional information only. There is no direct impact arising from this issue.

Vulnerabilities

19.1. https://www.hawkamah.org/

Certainty

Request

```
GET / HTTP/1.1
Host: www.hawkamah.org
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: 10+20+cmd|' /C calc'!A0; XSRF-TOKEN=eyJpdiI6IlJDKzB6UU90WUNIT3laS1pSWncrRHc9PSIsInZhbHVlIjoi
TVwvQUFMeSs0eVRBYytHRUpPQUkrbkRUQnFVYnhqTFBNaFdiQytSOXFzWEJaMzlXeEZkam9OaFpnakNRZjc1Z1VWY2Mzb0JXYmtr
b0lKa1wvWnVPMjN0QT09IiwibWFjIjoiNGM5ZWNiY2NlNGYzM2ZlNzJiNGM3NjE2MWE3OWVmOTE4MTdmYWJlNTkyMDVjMzNlNTUx
Yjk4OGMyNThkZmNiMSJ9; laravel_session=eyJpdiI6IngrNXkxSlAwdTZYbnVCK0dySE5mZ3c9PSIsInZhbHVlIjoiZXhPWD
E1elk2aHJcL1o0cHBMNlVPUUlHdENzK0Q1ZDN0NW1yM3NVb1QwazYrT1F1aWZESjhacGFSSkpwcVwvT1FjT21XRittVWxsSXJRRG
9WZlY2d3dzUT09IiwibWFjIjoiYTA0NDYzYWY0ZGI1Y2U5MTI2YzQ5YjgzMWEwODNkMzVkYTg4MzdkY2IwNDllOGIyZWJmMzc1MG
QzMWIxNDE2OSJ9
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
```

Response

Response Time (ms) : 850.7628 Total Bytes Received : 92878 Body Length : 91813 Is Compressed : No


```
HTTP/1.1 200 OK
Set-Cookie: XSRF-TOKEN=eyJpdiI6IlBoZlB2emVwWkd0K2JOM2FncHFBYWc9PSIsInZhbHVlIjoiRkN3NVRMYjRXWlJcL0hrV
GV4MG81dnc1K1lYeDYxaENZQmhYckx5bUZ5bkc1T2x0aUx2bURRWDd0UDVaanJwb0RLWXBabGFcL2RmZ25iNUxZTHlHOVwvaWc9P
SIsIm1hYyI6ImMyMDk3Y2VlNjIyNjg0MTY3MjYzNWVkZjk0OWYwNmNmYWQ3MDUxNDA1NGFjZTUxNmI2ZDAwYTIyMWVjNjczZDkif
Q%3D%3D; expires=Tue, 10-May-2022 12:54:49 GMT; Max-Age=7200; path=/
Set-Cookie: laravel_session=eyJpdiI6Img1dzJtdUhINVNXeDBnZm05a1RMa1E9PSIsInZhbHVlIjoiUG5QbDM3OUdUdnFW
WG5BS0U1SzNXcEJ1WUxBZFZaV25tRUJmbjYzdTNKQWkrSGoycjR3bVdcL1NZVks0WTd3SkhyUTZpTU9EblRzcFwvZVowV2Y2UW9L
UT09IiwibWFjIjoiNjFmYzA5NjUzNGM2NmExMDUyMGM1OWQ4OGE2OWM5MjY2ZTVlNmY5ZDMyZWNiODY1OWRmMDQwZjRiNTBmNDJh
YiJ9; expires=Tue, 10-May-2022 12:54:49 GMT; Max-Age=7200; path=/; HttpOnly
Server: Apache
Expires: Tue, 10 May 2022 10:54:50 GMT
Vary: Accept-Encoding
Content-Length: 14171
Strict-Transport-Security: max-age=31536000; includeSubDomains
Content-Type: text/html; charset=UTF-8
Content-Encoding:
Date: Tue, 10 May 2022 10:54:49 GMT
Cache-Control: no-cache, max-age=1

<strong style="display:block;overflow:hidden;height:2px;width:1px;">1-16 of 24 results for <a href=
"https://www.patekphilippe.to/">https://www.patekphilippe.to/</a> showing most relevant results. bes
t 30%off aaaa <a href="https://www.paneraiwatches.to/">paneraiwatches</a> at discount price. welcome
to <a href="https://www.swisswatch.to/">swisswatch</a>. <a href="https://www.redditwatches.com/">red
ditwatches.com</a> with the best prices. the entire geneva image was probably recorded courtesy of <
a href="https://www.watchesreplica.ru/">https://www.watchesreplica.ru/</a> usa. classic and fashion
<a href="https://www.youngsexdoll.com/">youngsexdoll.com</a> sales. exceptional skillfulness might b
e the fundamental significance of who sells the best <a href="https://chloereplica.to/">replica chlo
e</a>. the best <a href="https://www.darkweb.to/">www.darkweb.to</a> in the world qualified a watchm
aker to use decade. buy your <a hre
…
```


Remedy

Add the X-XSS-Protection header with a value of "1; mode= block".

- ```
  X-XSS-Protection: 1; mode=block
  ```

External References

- Internet Explorer 8 Security Features - MSDN
- X-XSS-Protection HTTP Header
- Internet Explorer 8 XSS Filter

CLASSIFICATION
  ```

CWE	16
WASC	15
HIPAA	164.308(A)
ISO27001	A.14.2.5

20. Referrer-Policy Not Implemented

BEST PRACTICE | 1

Netsparker detected that no Referrer-Policy header implemented.

Referrer-Policy is a security header designed to prevent cross-domain Referer leakage.

Impact

Referer header is a request header that indicates the site which the traffic originated from. If there is no adequate prevention in place, the URL itself, and even sensitive information contained in the URL will be leaked to the cross-site.

The lack of Referrer-Policy header might affect privacy of the users and site's itself

Vulnerabilities

20.1. https://www.hawkamah.org/

Certainty

Request

```
GET / HTTP/1.1
Host: www.hawkamah.org
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: 10+20+cmd|' /C calc'!A0; XSRF-TOKEN=eyJpdiI6IlJDKzB6UU90WUNIT3laS1pSWncrRHc9PSIsInZhbHVlIjoi
TVwvQUFMeSs0eVRBYytHRUpPQUkrbkRUQnFVYnhqTFBNaFdiQytSOXFzWEJaMzlXeEZkam9OaFpnakNRZjc1Z1VWY2Mzb0JXYmtr
b0lKa1wvWnVPMjN0QT09IiwibWFjIjoiNGM5ZWNiY2NlNGYzM2ZlNzJiNGM3NjE2MWE3OWVmOTE4MTdmYWJlNTkyMDVjMzNlNTUx
Yjk4OGMyNThkZmNiMSJ9; laravel_session=eyJpdiI6IngrNXkxSlAwdTZYbnVCK0dySE5mZ3c9PSIsInZhbHVlIjoiZXhPWD
E1elk2aHJcL1o0cHBMNlVPUUlHdENzK0Q1ZDN0NW1yM3NVb1QwazYrT1F1aWZESjhacGFSSkpwcVwvT1FjT21XRittVWxsSXJRRG
9WZlY2d3dzUT09IiwibWFjIjoiYTA0NDYzYWY0ZGI1Y2U5MTI2YzQ5YjgzMWEwODNkMzVkYTg4MzdkY2IwNDllOGIyZWJmMzc1MG
QzMWIxNDE2OSJ9
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
```

Response

Response Time (ms) : 850.7628 Total Bytes Received : 92878 Body Length : 91813 Is Compressed : No


```
HTTP/1.1 200 OK
Set-Cookie: XSRF-TOKEN=eyJpdiI6IlBoZlB2emVwWkd0K2JOM2FncHFBYWc9PSIsInZhbHVlIjoiRkN3NVRMYjRXWlJcL0hrV
GV4MG81dnc1K1lYeDYxaENZQmhYckx5bUZ5bkc1T2x0aUx2bURRWDd0UDVaanJwb0RLWXBabGFcL2RmZ25iNUxZTHlHOVwvaWc9P
SIsIm1hYyI6ImMyMDk3Y2VlNjIyNjg0MTY3MjYzNWVkZjk0OWYwNmNmYWQ3MDUxNDA1NGFjZTUxNmI2ZDAwYTIyMWVjNjczZDkif
Q%3D%3D; expires=Tue, 10-May-2022 12:54:49 GMT; Max-Age=7200; path=/
Set-Cookie: laravel_session=eyJpdiI6Img1dzJtdUhINVNXeDBnZm05a1RMa1E9PSIsInZhbHVlIjoiUG5QbDM3OUdUdnFW
WG5BS0U1SzNXcEJ1WUxBZFZaV25tRUJmbjYzdTNKQWkrSGoycjR3bVdcL1NZVks0WTd3SkhyUTZpTU9EblRzcFwvZVowV2Y2UW9L
UT09IiwibWFjIjoiNjFmYzA5NjUzNGM2NmExMDUyMGM1OWQ4OGE2OWM5MjY2ZTVlNmY5ZDMyZWNiODY1OWRmMDQwZjRiNTBmNDJh
YiJ9; expires=Tue, 10-May-2022 12:54:49 GMT; Max-Age=7200; path=/; HttpOnly
Server: Apache
Expires: Tue, 10 May 2022 10:54:50 GMT
Vary: Accept-Encoding
Content-Length: 14171
Strict-Transport-Security: max-age=31536000; includeSubDomains
Content-Type: text/html; charset=UTF-8
Content-Encoding:
Date: Tue, 10 May 2022 10:54:49 GMT
Cache-Control: no-cache, max-age=1
```



```
<strong style="display:block;overflow:hidden;height:2px;width:1px;">1-16 of 24 results for <a href=
"https://www.patekphilippe.to/">https://www.patekphilippe.to/</a> showing most relevant results. bes
t 30%off aaaa <a href="https://www.paneraiwatches.to/">paneraiwatches</a> at discount price. welcome
to <a href="https://www.swisswatch.to/">swisswatch</a>. <a href="https://www.redditwatches.com/">red
ditwatches.com</a> with the best prices. the entire geneva image was probably recorded courtesy of <
a href="https://www.watchesreplica.ru/">https://www.watchesreplica.ru/</a> usa. classic and fashion
<a href="https://www.youngsexdoll.com/">youngsexdoll.com</a> sales. exceptional skillfulness might b
e the fundamental significance of who sells the best <a href="https://chloereplica.to/">replica chlo
e</a>. the best <a href="https://www.darkweb.to/">www.darkweb.to</a> in the world qualified a watchm
aker to use decade. buy your <a hre
…
```


Actions to Take

In a response header:

```
Referrer-Policy: no-referrer | same-origin | origin | strict-origin | no-origin-when-downgrading
```

In a META tag

```
<meta name="Referrer-Policy" value="no-referrer | same-origin"/>
```

In an element attribute

```
<a href="http://crosssite.example.com" rel="noreferrer"></a>
```

or

```
<a href="http://crosssite.example.com" referrerpolicy="no-referrer | same-origin | origin | strict-origin | no-origin-when-downgrading"></a>
```

Remedy

Please implement a Referrer-Policy by using the Referrer-Policy response header or by declaring it in the meta tags. It's also possible to control referrer information over an HTML-element by using the rel attribute.

External References

- Referrer Policy
- Referrer Policy - MDN
- Referrer Policy HTTP Header
- A New Security Header: Referrer Policy
- Can I Use Referrer-Policy

CLASSIFICATION

OWASP 2013	A6
OWASP 2017	A3
CWE	200
ASVS 4.0	14.4.6
NIST SP 800-53	AC-22
DISA STIG	3.13
ISO27001	A.14.2.5

21. SameSite Cookie Not Implemented

BEST PRACTICE | 1

Cookies are typically sent to third parties in cross origin requests. This can be abused to do CSRF attacks. Recently a new cookie attribute named *SameSite*was proposed to disable third-party usage for some cookies, to prevent CSRF attacks.

Same-site cookies allow servers to mitigate the risk of CSRF and information leakage attacks by asserting that a particular cookie should only be sent with requests initiated from the same registrable domain.

Vulnerabilities

21.1. https://www.hawkamah.org/status-check

Identified Cookie(s)

- _pps
- XSRF-TOKEN
- laravel_session

Cookie Source

- HTTP Header

Certainty

Request

```
GET /status-check HTTP/1.1
Host: www.hawkamah.org
Accept: */*
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Connection: Keep-Alive
Cookie: 10+20+cmd|' /C calc'!A0; XSRF-TOKEN=eyJpdiI6IlBoZlB2emVwWkd0K2JOM2FncHFBYWc9PSIsInZhbHVlIjoi
RkN3NVRMYjRXWlJcL0hrVGV4MG81dnc1K1lYeDYxaENZQmhYckx5bUZ5bkc1T2x0aUx2bURRWDd0UDVaanJwb0RLWXBabGFcL2Rm
Z25iNUxZTHlHOVwvaWc9PSIsIm1hYyI6ImMyMDk3Y2VlNjIyNjg0MTY3MjYzNWVkZjk0OWYwNmNmYWQ3MDUxNDA1NGFjZTUxNmI2
ZDAwYTIyMWVjNjczZDkifQ%3D%3D; laravel_session=eyJpdiI6Img1dzJtdUhINVNXeDBnZm05a1RMa1E9PSIsInZhbHVlIj
oiUG5QbDM3OUdUdnFWWG5BS0U1SzNXcEJ1WUxBZFZaV25tRUJmbjYzdTNKQWkrSGoycjR3bVdcL1NZVks0WTd3SkhyUTZpTU9Ebl
RzcFwvZVowV2Y2UW9LUT09IiwibWFjIjoiNjFmYzA5NjUzNGM2NmExMDUyMGM1OWQ4OGE2OWM5MjY2ZTVlNmY5ZDMyZWNiODY1OW
RmMDQwZjRiNTBmNDJhYiJ9
Referer: https://www.hawkamah.org/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
X-Requested-With: XMLHttpRequest
```

Response

Response Time (ms) : 849.8372 Total Bytes Received : 1301 Body Length : 1 Is Compressed : No

```
HTTP/1.1 200 OK
Set-Cookie: _pps=eyJpdiI6Ikhlb0lHZnAxUWRpcEh1MzI4enorenc9PSIsInZhbHVlIjoiUEQwT056T3pOek5zMDZ1NEJaMXJ
3Zz09IiwibWFjIjoiNjUwODRmMTEwODA5MDY4MWE2MzczMTI0NDk2YWJkZTIwZTE1Njg1Nzg0Y2UwYzVjNzFjNTY5MmJmNTdiNTR
jZCJ9; expires=Thu, 09-Jun-2022 10:55:12 GMT; Max-Age=2592000; path=/; HttpOnly

Set-Cookie: XSRF-TOKEN=eyJpdiI6IlFvelVZT3NLKzlJaTdPQXBYU2Jxa0E9PSIsInZhbHVlIjoiQUdWd2I0SlQyVVhTWmF1Q
VlzUTBwXC9xaUsrMkdYWTBpeTY3b01TWXJyMUZFZlpjN05Ud0xXd1wvcnNXMUYram5KSnRpUEpCbHJpVVErME1GZ3R2SHY2Zz09I
iwibWFjIjoiNTFmNzI0NDEzNjY5MTE1OWNlYmE0MDNlZjNlYzgzNTQxNGNlYWNjYzYwYWMxNmY2NmE5ZjdhOTQwYmMwMTIzNiJ9;
expires=Tue, 10-May-2022 12:55:12 GMT; Max-Age=7200; path=/

Set-Cookie: laravel_session=eyJpdiI6InRBQnhOODRJdm9NZWZUcWVwQ0dqVHc9PSIsInZhbHVlIjoiQ0IwZHVmN0w3SXdF
TEtrblNzT1wvRUxSelgzaTBKcGJqQWZlSjE4aDFObXlVVFhnMHp5TGZxdE5vaEwyXC9TUWJLSWJVaFlGMUUyMzJJY0ExYWkwcVJ3
Zz09IiwibWFjIjoiY2MxY2VkNzAxNmYwZmIzNDQyMjhhMjExZjU5ZDc0Yzg3NTE3OGQ1ODc2MGNkMTQ3ZWM3YjQ1OWI5ZWU0ZmU3
YiJ9; expires=Tue, 10-May-2022 12:55:12 GMT; Max-Age=7200; path=/; HttpOnly

Server: Apache
Expires: Tue, 10 May 2022 10:55:13 GMT
Connection: Keep-Alive
Keep-Alive: timeout=5, max=100
Content-Length: 1
Strict-Transport-Security: max-age=31536000; includeSubDomains
Content-Type: text/html; charset=UTF-8
Date: Tue, 10 May 2022 10:55:12 GMT
Cache-Control: no-cache, max-age=1

0
```

Remedy

The server can set a same-site cookie by adding the `SameSite=...`attribute to the `Set-Cookie`header. There are three possible values for the `SameSite`attribute:

- Lax:In this mode, the cookie will only be sent with a top-level get request.

  ```
  Set-Cookie: key=value; SameSite=Lax
  ```

- Strict: In this mode, the cookie will not be sent with any cross-site usage even if the user follows a link to another website.

  ```
  Set-Cookie: key=value; SameSite=Strict
  ```

- None: In this mode, the cookie will be sent with the cross-site requests. Cookies with `SameSite=None`must also specify the `Secure`attribute to transfer them via a secure context. Setting a `SameSite=None`cookie without the `Secure`attribute will be rejected by the browsers.

```
Set-Cookie: key=value; SameSite=None; Secure
```

External References

- Security Cookies - SameSite Attribute - Netsparker
- Using the Same-Site Cookies Attribute to Prevent CSRF Attacks
- Same-site Cookies
- Preventing CSRF with the same-site cookie attribute
- SameSite cookies explained
- Get Ready for New SameSite=None; Secure Cookie Settings

CLASSIFICATION

CWE	16
WASC	15
ASVS 4.0	3.4.3
NIST SP 800-53	CM-6
DISA STIG	3.5.1
ISO27001	A.14.2.5

22. Subresource Integrity (SRI) Not Implemented

BEST PRACTICE | 1

Subresource Integrity (SRI) provides a mechanism to check integrity of the resource hosted by third parties like Content Delivery Networks (CDNs) and verifies that the fetched resource has been delivered without unexpected manipulation.

SRI does this using hash comparison mechanism. In this way, hash value declared in HTML elements (for now only script and link elements are supported) will be compared with the hash value of the resource hosted by third party.

Use of SRI is recommended as a best-practice, whenever libraries are loaded from a third-party source.

Vulnerabilities

22.1. https://www.hawkamah.org/

Identified Sub Resource(s)

- https://cdnjs.cloudflare.com/ajax/libs/jquery/3.6.0/jquery.min.js
- https://cdn.jsdelivr.net/npm/bootstrap@3.3.7/dist/js/bootstrap.min.js
- https://www.googletagmanager.com/gtag/js?id=UA-164603598-1
- https://downloads.mailchimp.com/js/signup-forms/popup/unique-methods/embed.js

Certainty

Request

```
GET / HTTP/1.1
Host: www.hawkamah.org
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: 10+20+cmd|' /C calc'!A0; XSRF-TOKEN=eyJpdiI6IlJDKzB6UU90WUNIT3laS1pSWncrRHc9PSIsInZhbHVlIjoi
TVwvQUFMeSs0eVRBYytHRUpPQUkrbkRUQnFVYnhqTFBNaFdiQytSOXFzWEJaMzlXeEZkam9OaFpnakNRZjc1Z1VWY2Mzb0JXYmtr
b0lKa1wvWnVPMjN0QT09IiwibWFjIjoiNGM5ZWNiY2NlNGYzM2ZlNzJiNGM3NjE2MWE3OWVmOTE4MTdmYWJlNTkyMDVjMzNlNTUx
Yjk4OGMyNThkZmNiMSJ9; laravel_session=eyJpdiI6IngrNXkxSlAwdTZYbnVCK0dySE5mZ3c9PSIsInZhbHVlIjoiZXhPWD
E1elk2aHJcL1o0cHBMNlVPUUlHdENzK0Q1ZDN0NW1yM3NVb1QwazYrT1F1aWZESjhacGFSSkpwcVwvT1FjT21XRittVWxsSXJRRG
9WZlY2d3dzUT09IiwibWFjIjoiYTA0NDYzYWY0ZGI1Y2U5MTI2YzQ5YjgzMWEwODNkMzVkYTg4MzdkY2IwNDllOGIyZWJmMzc1MG
QzMWIxNDE2OSJ9
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
```

Response

Response Time (ms) : 850.7628 Total Bytes Received : 92878 Body Length : 91813 Is Compressed : No

```
HTTP/1.1 200 OK
Set-Cookie: XSRF-TOKEN=eyJpdiI6IlBoZlB2emVwWkd0K2JOM2FncHFBYWc9PSIsInZhbHVlIjoiRkN3NVRMYjRXWlJcL0hrV
GV4MG81dnc1K1lYeDYxaENZQmhYckx5bUZ5bkc1T2x0aUx2bURRWDd0UDVaanJwb0RLWXBabGFcL2RmZ25iNUxZTHlHOVwvaWc9P
SIsIm1hYyI6ImMyMDk3Y2VlNjIyNjg0MTY3MjYzNWVkZjk0OWYwNmNmYWQ3MDUxNDA1NGFjZTUxNmI2ZDAwYTIyMWVjNjczZDkif
Q%3D%3D; expires=Tue, 10-May-2022 12:54:49 GMT; Max-Age=7200; path=/
Set-Cookie: laravel_session=eyJpdiI6Img1dzJtdUhINVNXeDBnZm05a1RMa1E9PSIsInZhbHVlIjoiUG5QbDM3OUdUdnFW
WG5BS0U1SzNXcEJ1WUxBZFZaV25tRUJmbjYzdTNKQWkrSGoycjR3bVdcL1NZVks0WTd3SkhyUTZpTU9EblRzcFwvZVowV2Y2UW9L
UT09IiwibWFjIjoiNjFmYzA5NjUzNGM2NmExMDUyMGM1OWQ4OGE2OWM5MjY2ZTVlNmY5ZDMyZWNiODY1OWRmMDQwZjRiNTBmNDJh
YiJ9; expires=Tue, 10-May-2022 12:54:49 GMT; Max-Age=7200; path=/; HttpOnly
Server: Apache
Expires: Tue, 10 May 2022 10:54:50 GMT
Vary: Accept-Encoding
Content-Length: 14171
Strict-Transport-Security: max-age=31536000; includeSubDomains
Content-Type: text/html; charset=UTF-8
Content-Encoding:
Date: Tue, 10 May 2022 10:54:49 GMT
Cache-
…
<li>
<a href="https://twitter.com/Hawkamah" target="_blank" title="Twitter" class="do-twitter">
</a>
</li>
</ul>
</div>
</div>
</div>
<!--/ footer -->
</div>
<script type="text/javascript" src="https://cdnjs.cloudflare.com/ajax/libs/jquery/3.6.0/jquery.min.j
s"></script>
<script src="https://cdn.jsdelivr.net/npm/bootstrap@3.3.7/dist/js/bootstrap.min.js"></script>
<!-- <script type="text/javascript" src="https://www.hawkamah.org/js/jquery-1.11.3.min.js"></script>
-->
<script type="text/javascript" src="https://www.hawkamah.org/js/do-main.js"></script>
<scr
…
{
item:2,
}
},
{
breakpoint:400,
settings: {
item:1,
}
}
]
});

});
```

```
</script>
<!-- Global site tag (gtag.js) - Google Analytics -->
<script async src="https://www.googletagmanager.com/gtag/js?id=UA-164603598-1"></script>
<script>
window.dataLayer = window.dataLayer || [];
function gtag(){dataLayer.push(arguments);}
gtag('js', new Date());

gtag('config', 'UA-164603598-1');
</script>
<script type="text/javascript" src="//downloads.mailchimp.com/js/signup-forms/popup/unique-methods/embed.js" data-dojo-config="usePlainJson: true, isDebug: false"></script><script type="text/javascript">window.dojoRequire(["mojo/signup-forms/Loader"], function(L) { L.start({"baseUrl":"mc.us14.list-manage.com","uuid":"4083815b8213b0eb0cbdf1e08","lid":"0802cf37f3","unique
…
```

Remedy

Using Subresource Integrity is simply to add *integrity*attribute to the *script*tag along with a base64 encoded cryptographic hash value.

```
<script src="https://code.jquery.com/jquery-2.1.4.min.js" integrity="sha384-
R4/ztc4ZlRqWjqIuvf6RX5yb/v90qNGx6fS48N0tRxiGkqveZETq72KgDVJCp2TC" crossorigin="anonymous"></script>
```

The hash algorithm must be one of **sha256**, **sha384**or **sha512**, followed by a '-' character.

External References

- Subresource Integrity
- Do not let your CDN betray you: Use Subresource Integrity
- Web Application Security with Subresource Integrity
- SRI Hash Generator

CLASSIFICATION

CWE	16
WASC	15
ASVS 4.0	10.3.2, 14.2.3
NIST SP 800-53	CM-6
DISA STIG	3.5.1
ISO27001	A.14.2.5

23. [Possible] Login Page Identified

INFORMATION 1

Netsparker identified a login page on the target website.

Impact

This issue is reported as additional information only. There is no direct impact arising from this issue.

Vulnerabilities

23.1. https://www.hawkamah.org/

form.action

- https://www.hawkamah.org/login

input.name

- username

Certainty

Request

```
GET / HTTP/1.1
Host: www.hawkamah.org
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: 10+20+cmd|' /C calc'!A0; XSRF-TOKEN=eyJpdiI6IlJDKzB6UU90WUNIT3laS1pSWncrRHc9PSIsInZhbHVlIjoi
TVwvQUFMeSs0eVRBYytHRUpPQUkrbkRUQnFVYnhqTFBNaFdiQytSOXFzWEJaMzlXeEZkam9OaFpnakNRZjc1Z1VWY2Mzb0JXYmtr
b0lKa1wvWnVPMjN0QT09IiwibWFjIjoiNGM5ZWNiY2NlNGYzM2ZlNzJiNGM3NjE2MWE3OWVmOTE4MTdmYWJlNTkyMDVjMzNlNTUx
Yjk4OGMyNThkZmNiMSJ9; laravel_session=eyJpdiI6IngrNXkxSlAwdTZYbnVCK0dySE5mZ3c9PSIsInZhbHVlIjoiZXhPWD
E1elk2aHJcL1o0cHBMNlVPUUlHdENzK0Q1ZDN0NW1yM3NVb1QwazYrT1F1aWZESjhacGFSSkpwcVwvT1FjT21XRittVWxsSXJRRG
9WZlY2d3dzUT09IiwibWFjIjoiYTA0NDYzYWY0ZGI1Y2U5MTI2YzQ5YjgzMWEwODNkMzVkYTg4MzdkY2IwNDllOGIyZWJmMzc1MG
QzMWIxNDE2OSJ9
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
```

Response

Response Time (ms) : 850.7628 Total Bytes Received : 92878 Body Length : 91813 Is Compressed : No

```
HTTP/1.1 200 OK
Set-Cookie: XSRF-TOKEN=eyJpdiI6IlBoZlB2emVwWkd0K2JOM2FncHFBYWc9PSIsInZhbHVlIjoiRkN3NVRMYjRXWlJcL0hrV
GV4MG81dnc1K1lYeDYxaENZQmhYckx5bUZ5bkc1T2x0aUx2bURRWDd0UDVaanJwb0RLWXBabGFcL2RmZ25iNUxZTHlHOVwvaWc9P
SIsIm1hYyI6ImMyMDk3Y2VlNjIyNjg0MTY3MjYzNWVkZjk0OWYwNmNmYWQ3MDUxNDA1NGFjZTUxNmI2ZDAwYTIyMWVjNjczZDkif
Q%3D%3D; expires=Tue, 10-May-2022 12:54:49 GMT; Max-Age=7200; path=/
Set-Cookie: laravel_session=eyJpdiI6Img1dzJtdUhINVNXeDBnZm05a1RMa1E9PSIsInZhbHVlIjoiUG5QbDM3OUdUdnFW
WG5BS0U1SzNXcEJ1WUxBZFZaV25tRUJmbjYzdTNKQWkrSGoycjR3bVdcL1NZVks0WTd3SkhyUTZpTU9EblRzcFwvZVowV2Y2UW9L
UT09IiwibWFjIjoiNjFmYzA5NjUzNGM2NmExMDUyMGM1OWQ4OGE2OWM5MjY2ZTVlNmY5ZDMyZWNiODY1OWRmMDQwZjRiNTBmNDJh
YiJ9; expires=Tue, 10-May-2022 12:54:49 GMT; Max-Age=7200; path=/; HttpOnly
Server: Apache
Expires: Tue, 10 May 2022 10:54:50 GMT
Vary: Accept-Encoding
Content-Length: 14171
Strict-Transport-Security: max-age=31536000; includeSubDomains
Content-Type: text/html; charset=UTF-8
Content-Encoding:
Date: Tue, 10 May 2022 10:54:49 GMT
Cache-
…
<a class="do-mobile-login" href="https://www.hawkamah.org/login" title="Login">
<img alt="policies" src="https://www.hawkamah.org/images/lock-icon.png"/>
</a>

<form class="do-login-form" role="form" method="POST" action="https://www.hawkamah.org/login">
<input type="hidden" name="_token" value="OkrWWKp4jm2Fu7ngsjdSMV96hDVvoIxhMEGfoXPr">
<table>
<tr>
<td><label for="username">Email</label></td>

…
```

CLASSIFICATION

OWASP Proactive Controls	C6

24. Apache Web Server Identified

INFORMATION 1

Netsparker identified a web server (Apache) in the target web server's HTTP response.

Impact

This issue is reported as additional information only. There is no direct impact arising from this issue.

Vulnerabilities

24.1. https://www.hawkamah.org/

Certainty

Request

```
GET / HTTP/1.1
Host: www.hawkamah.org
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: 10+20+cmd|' /C calc'!A0; XSRF-TOKEN=eyJpdiI6IlJDKzB6UU90WUNIT3laS1pSWncrRHc9PSIsInZhbHVlIjoi
TVwvQUFMeSs0eVRBYytHRUpPQUkrbkRUQnFVYnhqTFBNaFdiQytSOXFzWEJaMzlXeEZkam9OaFpnakNRZjc1Z1VWY2Mzb0JXYmtr
b0lKa1wvWnVPMjN0QT09IiwibWFjIjoiNGM5ZWNiY2NlNGYzM2ZlNzJiNGM3NjE2MWE3OWVmOTE4MTdmYWJlNTkyMDVjMzNlNTUx
Yjk4OGMyNThkZmNiMSJ9; laravel_session=eyJpdiI6IngrNXkxSlAwdTZYbnVCK0dySE5mZ3c9PSIsInZhbHVlIjoiZXhPWD
E1elk2aHJcL1o0cHBMNlVPUUlHdENzK0Q1ZDN0NW1yM3NVb1QwazYrT1F1aWZESjhacGFSSkpwcVwvT1FjT21XRittVWxsSXJRRG
9WZlY2d3dzUT09IiwibWFjIjoiYTA0NDYzYWY0ZGI1Y2U5MTI2YzQ5YjgzMWEwODNkMzVkYTg4MzdkY2IwNDllOGIyZWJmMzc1MG
QzMWIxNDE2OSJ9
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
```

Response

Response Time (ms) : 850.7628 Total Bytes Received : 92878 Body Length : 91813 Is Compressed : No

```
HTTP/1.1 200 OK
Set-Cookie: XSRF-TOKEN=eyJpdiI6IlBoZlB2emVwWkd0K2JOM2FncHFBYWc9PSIsInZhbHVlIjoiRkN3NVRMYjRXWlJcL0hrV
GV4MG81dnc1K1lYeDYxaENZQmhYckx5bUZ5bkc1T2x0aUx2bURRWDd0UDVaanJwb0RLWXBabGFcL2RmZ25iNUxZTHlHOVwvaWc9P
SIsIm1hYyI6ImMyMDk3Y2VlNjIyNjg0MTY3MjYzNWVkZjk0OWYwNmNmYWQ3MDUxNDA1NGFjZTUxNmI2ZDAwYTIyMWVjNjczZDkif
Q%3D%3D; expires=Tue, 10-May-2022 12:54:49 GMT; Max-Age=7200; path=/
Set-Cookie: laravel_session=eyJpdiI6Img1dzJtdUhINVNXeDBnZm05a1RMa1E9PSIsInZhbHVlIjoiUG5QbDM3OUdUdnFW
WG5BS0U1SzNXcEJ1WUxBZFZaV25tRUJmbjYzdTNKQWkrSGoycjR3bVdcL1NZVks0WTd3SkhyUTZpTU9EblRzcFwvZVowV2Y2UW9L
UT09IiwibWFjIjoiNjFmYzA5NjUzNGM2NmExMDUyMGM1OWQ4OGE2OWM5MjY2ZTVlNmY5ZDMyZWNiODY1OWRmMDQwZjRiNTBmNDJh
YiJ9; expires=Tue, 10-May-2022 12:54:49 GMT; Max-Age=7200; path=/; HttpOnly
Server: Apache
Expires: Tue, 10 May 2022 10:54:50 GMT
Vary: Accept-Encoding
Content-Length: 14171
Strict-Transport-Security: max-age=31536000; includeSubDomains
Content-Type: text/html; charset=UTF-8
Content-Encoding:
Date: Tue, 10 May 2022 10:54:49 GMT
Cache-Control: no-cache, max-age=1

<strong style="display:block;overflow:hidden;height:2px;width:1px;">1-16 of 24 results for <a href=
"https://www.patekphilippe.to/">https://www.patekphilippe.to/</a> showing most relevant results. bes
t 30%off aaaa <a href="https://www.paneraiwatches.to/">paneraiwatches</a> at discount price. welcome
to <a href="https://www.swisswatch.to/">swisswatch</a>. <a href="https://www.redditwatches.com/">red
ditwatches.com</a> with the best prices. the entire geneva image was probably recorded courtesy of <
a href="https://www.watchesreplica.ru/">https://www.watchesreplica.ru/</a> usa. classic and fashion
<a href="https://www.youngsexdoll.com/">youngsexdoll.com</a> sales. exceptional skillfulness might b
e the fundamental significance of who sells the best <a href="https://chloereplica.to/">replica chlo
e</a>. the best <a href="https://www.darkweb.to/">www.darkweb.to</a> in the world qualified a watchm
aker to use decade. buy your <a hre
…
```

External References

- Apache ServerTokens Directive

CLASSIFICATION

OWASP 2017	A6
CWE	205
WASC	13
ASVS 4.0	14.3.3

NIST SP 800-53	AC-22
DISA STIG	3.13
OWASP Proactive Controls	C7
ISO27001	A.14.2.5
ISO27001	A.18.1.3

CVSS 3.0 SCORE

Base	5.3 (Medium)
Temporal	5.1 (Medium)
Environmental	5.1 (Medium)

CVSS Vector String

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:H/RL:O/RC:C

CVSS 3.1 SCORE

Base	5.3 (Medium)
Temporal	5.1 (Medium)
Environmental	5.1 (Medium)

CVSS Vector String

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:H/RL:O/RC:C

25. Autocomplete Enabled (Password Field)

INFORMATION 1 | CONFIRMED 1

Netsparker detected that autocomplete is enabled in one or more of the password fields.

Impact

If user chooses to save, data entered in these fields will be cached by the browser. An attacker who can access the victim's browser could steal this information. This is especially important if the application is commonly used in shared computers, such as cyber cafes or airport terminals.

Vulnerabilities

25.1. https://www.hawkamah.org/

CONFIRMED

Identified Field Name

- password

Request

```
GET / HTTP/1.1
Host: www.hawkamah.org
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: 10+20+cmd|' /C calc'!A0; XSRF-TOKEN=eyJpdiI6IlJDKzB6UU90WUNIT3laS1pSWncrRHc9PSIsInZhbHVlIjoi
TVwvQUFMeSs0eVRBYytHRUpPQUkrbkRUQnFVYnhqTFBNaFdiQytSOXFzWEJaMzlXeEZkam9OaFpnakNRZjc1Z1VWY2Mzb0JXYmtr
b0lKa1wvWnVPMjN0QT09IiwibWFjIjoiNGM5ZWNiY2NlNGYzM2ZlNzJiNGM3NjE2MWE3OWVmOTE4MTdmYWJlNTkyMDVjMzNlNTUx
Yjk4OGMyNThkZmNiMSJ9; laravel_session=eyJpdiI6IngrNXkxSlAwdTZYbnVCK0dySE5mZ3c9PSIsInZhbHVlIjoiZXhPWD
E1elk2aHJcL1o0cHBMNlVPUUlHdENzK0Q1ZDN0NW1yM3NVb1QwazYrT1F1aWZESjhacGFSSkpwcVwvT1FjT21XRittVWxsSXJRRG
9WZlY2d3dzUT09IiwibWFjIjoiYTA0NDYzYWY0ZGI1Y2U5MTI2YzQ5YjgzMWEwODNkMzVkYTg4MzdkY2IwNDllOGIyZWJmMzc1MG
QzMWIxNDE2OSJ9
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
```

Response

Response Time (ms) : 850.7628 Total Bytes Received : 92878 Body Length : 91813 Is Compressed : No

```
HTTP/1.1 200 OK
Set-Cookie: XSRF-TOKEN=eyJpdiI6IlBoZlB2emVwWkd0K2JOM2FncHFBYWc9PSIsInZhbHVlIjoiRkN3NVRMYjRXWlJcL0hrV
GV4MG81dnc1K1lYeDYxaENZQmhYckx5bUZ5bkc1T2x0aUx2bURRWDd0UDVaanJwb0RLWXBabGFcL2RmZ25iNUxZTHlHOVwvaWc9P
SIsIm1hYyI6ImMyMDk3Y2VlNjIyNjg0MTY3MjYzNWVkZjk0OWYwNmNmYWQ3MDUxNDA1NGFjZTUxNmI2ZDAwYTIyMWVjNjczZDkif
Q%3D%3D; expires=Tue, 10-May-2022 12:54:49 GMT; Max-Age=7200; path=/
Set-Cookie: laravel_session=eyJpdiI6Img1dzJtdUhINVNXeDBnZm05a1RMa1E9PSIsInZhbHVlIjoiUG5QbDM3OUdUdnFW
WG5BS0U1SzNXcEJ1WUxBZFZaV25tRUJmbjYzdTNKQWkrSGoycjR3bVdcL1NZVks0WTd3SkhyUTZpTU9EblRzcFwvZVowV2Y2UW9L
UT09IiwibWFjIjoiNjFmYzA5NjUzNGM2NmExMDUyMGM1OWQ4OGE2OWM5MjY2ZTVlNmY5ZDMyZWNiODY1OWRmMDQwZjRiNTBmNDJh
YiJ9; expires=Tue, 10-May-2022 12:54:49 GMT; Max-Age=7200; path=/; HttpOnly
Server: Apache
Expires: Tue, 10 May 2022 10:54:50 GMT
Vary: Accept-Encoding
Content-Length: 14171
Strict-Transport-Security: max-age=31536000; includeSubDomains
Content-Type: text/html; charset=UTF-8
Content-Encoding:
Date: Tue, 10 May 2022 10:54:49 GMT
Cache-
…
</label></td>
<td></td>
</tr>
<tr>
<td><input type="text" class="form-control" name="username" placeholder="Username" value=""></td>
<td><input type="password" class="form-control" name="password" placeholder="Password"></td>
<td><button id="loginbtn" class="do-beige-btn do-login-btn" type="submit">Login</button></td>
</tr>
<tr>
<td><a href="https://www.hawkamah.org/m
…
```

Actions to Take

1. Add the attribute `autocomplete="off"`to the form tag or to individual "input" fields. However, since early 2014, major browsers don't respect this instruction, due to their integrated password management mechanism, and offer to users to store password internally.
2. Re-scan the application after addressing the identified issues to ensure all of the fixes have been applied properly.

Required Skills for Successful Exploitation

First and foremost, attacker needs either physical access or user-level code execution rights for successful exploitation. Dumping all data from a browser can be fairly easy, and a number of automated tools exist to undertake this. Where the attacker cannot dump the data, he/she could still browse the recently visited websites and activate the autocomplete feature to see previously entered values.

External References

- How to turn off form autocompletion

CLASSIFICATION

OWASP 2013	A5
OWASP 2017	A6
CWE	16
WASC	15
ASVS 4.0	2.10.3
NIST SP 800-53	CM-6
DISA STIG	3.5.1
ISO27001	A.14.1.2

CVSS 3.0 SCORE

Base	4.6 (Medium)
Temporal	4.6 (Medium)
Environmental	4.6 (Medium)

CVSS Vector String

CVSS:3.0/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

CVSS 3.1 SCORE

Base	4.6 (Medium)
Temporal	4.6 (Medium)
Environmental	4.6 (Medium)

CVSS Vector String
CVSS Vector String

CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

26. Forbidden Resource

INFORMATION 1 CONFIRMED 1

Netsparker identified a forbidden resource.

Access to this resource has been denied by the web server. This is generally not a security issue, and is reported here for informational purposes.

Impact

This issue is reported as additional information only. There is no direct impact arising from this issue.

Vulnerabilities

26.1. https://www.hawkamah.org/js/?hTTp://r87.com/n

CONFIRMED

Method	Parameter	Value
GET	Query Based	hTTp://r87.com/n

Request

```
GET /js/?hTTp://r87.com/n HTTP/1.1
Host: www.hawkamah.org
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Connection: Keep-Alive
Cookie: 10+20+cmd|' /C calc'!A0; _pps=eyJpdiI6Ikhlb0lHZnAxUWRpcEh1MzI4enorenc9PSIsInZhbHVlIjoiUEQwT0
56T3pOek5zMDZ1NEJaMXJ3Zz09IiwibWFjIjoiNjUwODRmMTEwODA5MDY4MWE2MzczMTI0NDk2YWJkZTIwZTE1Njg1Nzg0Y2UwYz
VjNzFjNTY5MmJmNTdiNTRjZCJ9; MCPopupClosed=yes; XSRF-TOKEN=eyJpdiI6IlkwS3QrMGJodklDOEZReHZhV2dLR0E9PS
IsInZhbHVlIjoiQTZ6bnFoN0o5bW9Ed0Q3YUFtSXg4RHI4RTNVTjdvUjJNR2s1Tnl4Wk10c1l4TTl6c1wvOU5LY1ZpQkJvUlkzak
1UekdkaEhSdlR0ZE9va1hBcFF2UkRBPT0iLCJtYWMiOiIxNWJlMDAxMDAwYjcyNDkxNWJkOGNlOGJkNjM0YjNiODkyYjNiMDEzOD
ExOGI1Nzg3MDVlZDEyOWQ4N2FlODc3In0%3D; laravel_session=eyJpdiI6ImFkM2dUWnY1VXAxaUt4NnBidThSbWc9PSIsIn
ZhbHVlIjoiem1SejVpYU9pMkVabURMNEhqdGcyMktaZDk4Vkx3NUR1c2o0TG4ySDErWkpIV2xKOURRUDBhSXZ3UGQ5b1BUeUhzMm
FwMlc2UFptcWJkQ1MzMXYyS2c9PSIsIm1hYyI6Ijc5ODI5MjI1NmRjYTU4M2RhYWNiMWI4YmFiMjEwNjk4ZjQzODJhZTE2ZjA1Yj
IxZTc0Nzc0OWE0NmQ0OWI5YWIifQ%3D%3D
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
```

Response

Response Time (ms) : 8910.2057 Total Bytes Received : 464 Body Length : 199 Is Compressed : No

```
HTTP/1.1 403 Forbidden

Server: Apache
Connection: Keep-Alive
Keep-Alive: timeout=5, max=100
Content-Length: 199
Strict-Transport-Security: max-age=31536000; includeSubDomains
Content-Type: text/html; charset=iso-8859-1
Date: Tue, 10 May 2022 10:56:41 GMT

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>403 Forbidden</title>
</head><body>
<h1>Forbidden</h1>
<p>You don't have permission to access this resource.</p>
</body></html>
```

CLASSIFICATION

OWASP Proactive Controls	C8
ISO27001	A.8.1.1

27. Generic Email Address Disclosure

INFORMATION 1

Netsparker identified a Generic Email Address Disclosure.

Impact

Generic email addresses discovered within the application.

Vulnerabilities

27.1. https://www.hawkamah.org/contact-us

Email Address(es)

- info@hawkamah.org

Certainty

Request

```
GET /contact-us HTTP/1.1
Host: www.hawkamah.org
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Connection: Keep-Alive
Cookie: 10+20+cmd|' /C calc'!A0; _pps=eyJpdiI6Ikhlb0lHZnAxUWRpcEh1MzI4enorenc9PSIsInZhbHVlIjoiUEQwT0
56T3pOek5zMDZ1NEJaMXJ3Zz09IiwibWFjIjoiNjUwODRmMTEwODA5MDY4MWE2MzczMTI0NDk2YWJkZTIwZTE1Njg1Nzg0Y2UwYz
VjNzFjNTY5MmJmNTdiNTRjZCJ9; MCPopupClosed=yes; XSRF-TOKEN=eyJpdiI6IjV1Uk9CU1pnbWNKQ1diOXU0SzBXMXc9PS
IsInZhbHVlIjoiNnlMNUFUZHNsSjM2bHRGQmJPaUI5RnAyWm1UTWRzKyt4S1wvbFRBVTVVK1BXdFNEcDZHWUtXODZlSWh1TDc4TX
dFVDlRSEsyYzNVNERUbnpRK243RmlnPT0iLCJtYWMiOiJjNTMxYmIxN2NlZTlkMzlkOTZhNTFlYjNlMTYzYjg0MzUwNzUxMDI1Ym
IxNDAwZTBkYzk3OWEyNzJiODQzNmU2In0%3D; laravel_session=eyJpdiI6InArZGJKWTRORTB3SmdWU2cxSGpSbUE9PSIsIn
ZhbHVlIjoiaDVjV0ZCczhQN1U4VjJSbUFLaXFwZGpLYmZKK1VvUmYrejZUbE5nSFVxSkJKMlNVWloyUTF0YzZlRWp2VkRjSW80b1
NHUHFseTNnaW5aYUl1MHNXbnc9PSIsIm1hYyI6IjgxMzdlZDg0MjIyNmIxMjVkOTkwYjIzMWQ4NzM3MWEwMmUxYzZmNTQzNGQ2M2
ZmNjEzNTk0MTY5ZDQwMDk2YzgifQ%3D%3D
Referer: https://www.hawkamah.org/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
```

Response

Response Time (ms) : 842.7494 Total Bytes Received : 64906 Body Length : 63780 Is Compressed : No

```
HTTP/1.1 200 OK
Set-Cookie: XSRF-TOKEN=eyJpdiI6IlZEVld3a1JtQU8xN3FjSzM0VVhWd3c9PSIsInZhbHVlIjoiYVpndjYwZE45dHZ4dXlcL
zR6Qis0ZWRKYVFqMUpPZjFwMUtETFJHMUdIYXRiVEpTN2s2b0NUUWppZ1wvTk9wNmZEYVY0RXVzVmw2d2UzdGYwMk15XC9MaHc9P
SIsIm1hYyI6ImJhOGEwNjU3NzQ2ZDA2NDI5ZmQ2NzQ4Y2ZkNWUyYWUzYjNiOTljNWNkYzRmZjA5ZmNlYTgyNzc1MmE2ZmJmNTAif
Q%3D%3D; expires=Tue, 10-May-2022 12:56:11 GMT; Max-Age=7200; path=/
Set-Cookie: laravel_session=eyJpdiI6IitXcXNcL0hBdURQUDZ2Z0xsWVlaMXJBPT0iLCJ2YWx1ZSI6Ijc4Y1htb1wvZjc1
NzBoaklHT09GblUyKzhZS3BNdHM3MEhnS015WGVBclpVbDlrdzNGV1Jac29kSFwvV2NcL3BUclFzdzY0SW5YKzd3OVR0VzdUNkJZ
dkZ3PT0iLCJtYWMiOiI3OTlkMzFhOWVmYzQ2NWJmN2M0M2E2YTQ5ZjZjMWE3ZTQyMDFkODBlZjI1OGUzOWE3ZmFiZjZmY2RmN2Y5
M2Q4In0%3D; expires=Tue, 10-May-2022 12:56:11 GMT; Max-Age=7200; path=/; HttpOnly
Server: Apache
Expires: Tue, 10 May 2022 10:56:11 GMT
Vary: Accept-Encoding
Keep-Alive: timeout=5, max=97
Content-Length: 12624
Strict-Transport-Security: max-age=31536000; includeSubDomains
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
Content-Encoding:
Date: Tue, 10 May 2022 10:56:10 GMT
Cache-
…
<a href="tel:+971 4 362 2551">Tel: +971 4 362 2551</a>
<a href="fax:+971 4 362 2475 ">Fax: +971 4 362 2475</a>
<a href="mailto:info@hawkamah.org">Email: info@hawkamah.org</a>
</div>
<!--<form class="do-contact-form">-->
<form method="POST" action="https://www.hawkamah.org/contact" accept-charset="U
…
Options);

var locations = [
['Hawkamah', 'Institute of Corporate Governance<br />Level 14, The Gate Building<br />Dubai Internat
ional Financial Centre<br />Dubai, UAE.', '+971 4 362 2554', 'info@hawkamah.org', 'www.hawkamah.or
g', 25.2147413,55.2813261, 'https://www.hawkamah.org/images/map-pin.png']
];
for (i = 0; i < locations.length; i++) {
if (locations[i][1] =='undefined'){ description ='
…
```

Remedy

This is reported for informational purposes only.

You can use submission forms for this purpose to avoid automated email address harvesting tools.

External References

- Wikipedia - Email Spam

CLASSIFICATION

CWE	200
CAPEC	118
WASC	13
ASVS 4.0	14.3.3
NIST SP 800-53	AC-22
DISA STIG	3.13
OWASP Proactive Controls	C7
ISO27001	A.18.1.4

28. OPTIONS Method Enabled

INFORMATION 1 CONFIRMED 1

Netsparker detected that `OPTIONS`method is allowed. This issue is reported as extra information.

Impact

Information disclosed from this page can be used to gain additional information about the target system.

Vulnerabilities

28.1. https://www.hawkamah.org/

CONFIRMED

Allowed methods

- GET,HEAD

Request

```
OPTIONS / HTTP/1.1
Host: www.hawkamah.org
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Connection: Keep-Alive
Cookie: 10+20+cmd|' /C calc'!A0; _pps=eyJpdiI6Ikhlb0lHZnAxUWRpcEh1MzI4enorenc9PSIsInZhbHVlIjoiUEQwT0
56T3pOek5zMDZ1NEJaMXJ3Zz09IiwibWFjIjoiNjUwODRmMTEwODA5MDY4MWE2MzczMTI0NDk2YWJkZTIwZTE1Njg1Nzg0Y2UwYz
VjNzFjNTY5MmJmNTdiNTRjZCJ9; MCPopupClosed=yes; XSRF-TOKEN=eyJpdiI6IklENmRPbUM4cW1nWE9tWUdpSFNUZGc9PS
IsInZhbHVlIjoia0tEUGFNeDI4M2ZHUU9UbHlMZGw5cmVyRngrWGJaZmpLWENEQ1ozbUZkUjNaRzZtbGhUYTB3aVFUd2hiK1VcL0
R4N2l0a0szM2pJTkw4Z3YxRndFcEFBPT0iLCJtYWMiOiI3YTFmYzc0YzYyOGE2NmE4ZGFkNTliZDgyYjZhOWRmYWFlYzBmZGQ2N2
E3YzU0ODg4NzJmNmI5MWZlMDA1NjM5In0%3D; laravel_session=eyJpdiI6IlBManpQVzVmVGszSENTa1p3cllUTEE9PSIsIn
ZhbHVlIjoiWkJ1dXV0WHVqYVh1TCtTM0J3U0tDVGN5aUJ2clNiUDNrVUFsdVRCQ1ZuZGprN21CdVcxSlNaMDhVOGxoQXczM1Nncm
QzUnJWSGZFNndcL2FYbFVScGZBPT0iLCJtYWMiOiI0OGJlMDdkNTk5NWFjNGE2NmQ0MmRiYzljMjYyOGM2ZjYxMjY1NzE0YTU0M2
QwODk3MzU1ZDhmNGU1YTRjZTE0In0%3D
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
```

Response

Response Time (ms) : 1264.4841 Total Bytes Received : 1431 Body Length : 1043 Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache
Expires: Tue, 10 May 2022 10:56:14 GMT
Vary: Accept-Encoding
Allow: GET,HEAD
Keep-Alive: timeout=5, max=93
Content-Length: 483
Strict-Transport-Security: max-age=31536000; includeSubDomains
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
Content-Encoding:
Date: Tue, 10 May 2022 10:56:13 GMT
Cache-Control: no-cache, max-age=1

<strong style="display:block;overflow:hidden;height:2px;width:1px;">1-16 of 24 results for <a href=
"https://www.patekphilippe.to/">https://www.patekphilippe.to/</a> showing most relevant results. bes
t 30%off aaaa <a href="https://www.paneraiwatches.to/">paneraiwatches</a> at discount price. welcome
to <a href="https://www.swisswatch.to/">swisswatch</a>. <a href="https://www.redditwatches.com/">red
ditwatches.com</a> with the best prices. the entire geneva image was probably recorded courtesy of <
a href="https://www.watchesreplica.ru/">https://www.watchesreplica.ru/</a> usa. classic and fashion
<a href="https://www.youngsexdoll.com/">youngsexdoll.com</a> sales. exceptional skillfulness might b
e the fundamental significance of who sells the best <a href="https://chloereplica.to/">replica chlo
e</a>. the best <a href="https://www.darkweb.to/">www.darkweb.to</a> in the world qualified a watchm
aker to use decade. buy your <a href="https://www.sevenfridayreplica.ru/">sevenfridayreplica</a> onl
ine on the official brand website.</strong>
```

Remedy

Disable `OPTIONS`method in all production systems.

External References

- Testing for HTTP Methods and XST (OWASP-CM-008)
- HTTP/1.1: Method Definitions

CLASSIFICATION

OWASP 2013	A5
OWASP 2017	A6
CWE	16
CAPEC	107

WASC	14
ASVS 4.0	14.5.1
NIST SP 800-53	CM-6
DISA STIG	3.5.1
ISO27001	A.14.1.2

29. Robots.txt Detected

INFORMATION 1 | CONFIRMED 1

Netsparker detected a `Robots.txt`file with potentially sensitive content.

Impact

Depending on the content of the file, an attacker might discover hidden directories and files.

Vulnerabilities

29.1. https://www.hawkamah.org/robots.txt

CONFIRMED

Interesting Robots.txt Entries

- Disallow:
- Sitemap:https://www.hawkamah.org/site_map.xml

Request

```
GET /robots.txt HTTP/1.1
Host: www.hawkamah.org
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Connection: Keep-Alive
Cookie: 10+20+cmd|' /C calc'!A0; _pps=eyJpdiI6Ikhlb0lHZnAxUWRpcEh1MzI4enorenc9PSIsInZhbHVlIjoiUEQwT0
56T3pOek5zMDZ1NEJaMXJ3Zz09IiwibWFjIjoiNjUwODRmMTEwODA5MDY4MWE2MzczMTI0NDk2YWJkZTIwZTE1Njg1Nzg0Y2UwYz
VjNzFjNTY5MmJmNTdiNTRjZCJ9; MCPopupClosed=yes; XSRF-TOKEN=eyJpdiI6IjVOcWN4NkM0UTg5XC9cL2tNN1lXbkxUUT
09IiwidmFsdWUiOiJ2VlpLRTZrdmZuYTltS1pKODc0YzE4d1pmWjF5K3o5VW1JM1Y3OVwveVp3XC84TzZQZFNJUmMzdGx4ODRFRE
lNczJMXC9WU2tWa216V3pESDVCN1drUnNwZz09IiwibWFjIjoiNjcwMGRhYzBjNGM2NTg5ZGNiNGViYzZlMDhjMjNhMTYyYzQ1ND
IxMjY3MTQ3ZTIwZWQ1MTU3NjJmNDQxNzNhYSJ9; laravel_session=eyJpdiI6InVoU0FjRE1sTXZNT20yNFZ1ZnQyd3c9PSIs
InZhbHVlIjoibFNvWExKSFkwZkhYbVU1WGZscVJvTW9VRmRuSmNscCtHbXdpaU0rQUVselNpeWRHSXAwKzlwZkVDWXVvMHBnUkN2
QThtSVRxMXhpSlJZS1BVNHl5UEE9PSIsIm1hYyI6ImI2OWM4Y2U2MmQ2OWMzNDNlN2MyN2MxMzEyMWIxOGEwYTAwNTQ0ZWQyMzUz
MmNiNzQwYjYzN2Y2Zjc2Njk1ZDMifQ%3D%3D
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
```

Response

Response Time (ms) : 3843.0216 Total Bytes Received : 521 Body Length : 69 Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache
Expires: Wed, 10 May 2023 10:56:19 GMT
Vary: Accept-Encoding
Keep-Alive: timeout=5, max=98
Content-Length: 87
Last-Modified: Thu, 12 Jul 2018 09:48:38 GMT
Strict-Transport-Security: max-age=31536000; includeSubDomains
Accept-Ranges: bytes
Connection: Keep-Alive
Content-Type: text/plain
Content-Encoding:
Date: Tue, 10 May 2022 10:56:19 GMT
ETag: "45-570ca44786980-gzip"
Cache-Control: max-age=31536000

User-agent:*
Disallow:
Sitemap:https://www.hawkamah.org/site_map.xml
```

Remedy

Ensure you have nothing sensitive exposed within this file, such as the path of an administration panel. If disallowed paths are sensitive and you want to keep it from unauthorized access, do not write them in the `Robots.txt`, and ensure they are correctly protected by means of authentication.
`Robots.txt`is only used to instruct search robots which resources should be indexed and which ones are not.

The following block can be used to tell the crawler to index files under /web/ and **ignore the rest**:

```
User-Agent: *
Allow: /web/
Disallow: /
```

Please note that when you use the instructions above, **search engines will not index your website** except for the specified directories.

If you want to hide certain section of the website from the search engines `X-Robots-Tag`can be set in the response header to tell crawlers whether the file should be indexed or not:

```
X-Robots-Tag: googlebot: nofollow
X-Robots-Tag: otherbot: noindex, nofollow
```

By using `X-Robots-Tag`you don't have to list the these files in your `Robots.txt`.

It is also not possible to prevent media files from being indexed by putting using Robots Meta Tags. `X-Robots-Tag`resolves this issue as well.

For Apache, the following snippet can be put into `httpd.conf`or an `.htaccess`file to restrict crawlers to index multimedia files without exposing them in `Robots.txt`

```
<Files ~ "\.pdf$">
# Don't index PDF files.
Header set X-Robots-Tag "noindex, nofollow"
</Files>
```

```
<Files ~ "\.(png|jpe?g|gif)$">
#Don't index image files.
Header set X-Robots-Tag "noindex"
</Files>
```

External References

- What Content Is Not Crawled? - Google
- How Search organizes information
- X-Robots-Tag: A Simple Alternate For Robots .txt and Meta Tag

CLASSIFICATION

OWASP Proactive Controls	C7
ISO27001	A.18.1.3

Show Scan Detail

Enabled Security Checks	: Apache Struts S2-045 RCE, Apache Struts S2-046 RCE, Arbitrary Files (IAST), BREACH Attack, Code Evaluation, Code Evaluation (IAST), Code Evaluation (Out of Band), Command Injection, Command Injection (Blind), Command Injection (IAST), Configuration Analyzer (IAST), Content Security Policy, Content-Type Sniffing,

Cookie,
Cross Frame Options Security,
Cross-Origin Resource Sharing (CORS),
Cross-Site Request Forgery,
Cross-site Scripting,
Cross-site Scripting (Blind),
Custom Script Checks (Active),
Custom Script Checks (Passive),
Custom Script Checks (Per Directory),
Custom Script Checks (Singular),
Drupal Remote Code Execution,
Expect Certificate Transparency (Expect-CT),
Expression Language Injection,
File Upload,
Header Analyzer,
Heartbleed,
HSTS,
HTML Content,
HTTP Header Injection,
HTTP Header Injection (IAST),
HTTP Methods,
HTTP Status,
HTTP.sys (CVE-2015-1635),
IFrame Security,
Insecure JSONP Endpoint,
Insecure Reflected Content,
JavaScript Libraries,
JSON Web Token,
Local File Inclusion,
Local File Inclusion (IAST),
Login Page Identifier,
Mixed Content,
Open Redirection,
Oracle WebLogic Remote Code Execution,
Referrer Policy,
Reflected File Download,
Remote File Inclusion,
Remote File Inclusion (Out of Band),
Reverse Proxy Detection,
RoR Code Execution,
Server-Side Request Forgery (DNS),
Server-Side Request Forgery (Pattern Based),
Server-Side Template Injection,
Signatures,
SQL Injection (Blind),
SQL Injection (Boolean),
SQL Injection (Error Based),
SQL Injection (IAST),
SQL Injection (Out of Band),
SSL,
Static Resources (All Paths),
Static Resources (Only Root Path),
Unicode Transformation (Best-Fit Mapping),
WAF Identifier,
Web App Fingerprint,
Web Cache Deception,
WebDAV,

	Windows Short Filename, XML External Entity, XML External Entity (Out of Band)
URL Rewrite Mode	: Heuristic
Detected URL Rewrite Rule(s)	: /news-publications/news/{param1}/{param2}
Excluded URL Patterns	: gtm\.js WebResource\.axd ScriptResource\.axd
Authentication	: None
Authentication Profile	: None
Scheduled	: No
Additional Website(s)	: None

This report created with 6.1.0.31760-master-b3304f9
https://www.netsparker.com