Web Application Scanning Detailed Scan Export: jumex web app

June 19, 2025 at 20:48 (UTC)

Table of Contents

Scan Summary

Vulnerability Breakdown

0 CRITICAL	0 HIGH	5 MEDIUM	13 LOW

Scan Details

NAME	jumex web app
STATUS	Completed
CREATE TIME	06/17/2025 at 05:45 PM UTC
START TIME	06/17/2025 at 05:47 PM UTC
END TIME	06/17/2025 at 06:16 PM UTC
TEMPLATE	Scan
SCANNER	Cloud
TARGET	https://jmx.ambiente-de-pruebas-devcts.site
DESCRIPTION	

Scan Notes

Severity	Scan Notes	Description

No tuning recommendations for this scan.

Scan Results

Vulnerabilities

Severity	Plugin Id	Name	Family	Instances
Medium	98056	Missing HTTP Strict Transport Security Policy	HTTP Security Header	3
Medium	114322	PHP Input Variables Exceeded	Web Applications	2
Low	98618	HTTP Header Information Disclosure	HTTP Security Header	3
Low	98064	Cookie Without Secure Flag Detected	HTTP Security Header	2
Low	112529	Missing 'X-Content-Type-Options' Header	HTTP Security Header	2
Low	98060	Missing 'X-Frame-Options' Header	HTTP Security Header	2
Low	112539	SSL/TLS Weak Cipher Suites Supported	SSL/TLS	1
Low	98063	Cookie Without HttpOnly Flag Detected	HTTP Security Header	1
Low	112551	Missing Content Security Policy	HTTP Security Header	1
Low	112553	Missing 'Cache-Control' Header	HTTP Security Header	1

Missing HTTP Strict Transport Security Policy

VULNERABILITY   MEDIUM   PLUGIN ID 98056

Description

The HTTP protocol by itself is clear text, meaning that any data that is transmitted via HTTP can be captured and the contents viewed. To keep data private and prevent it from being intercepted, HTTP is often tunnelled through either Secure Sockets Layer (SSL) or Transport Layer Security (TLS). When either of these encryption standards are used, it is referred to as HTTPS.

HTTP Strict Transport Security (HSTS) is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. This will be enforced by the browser even if the user requests a HTTP resource on the same server.

Cyber-criminals will often attempt to compromise sensitive information passed from the client to the server using HTTP. This can be conducted via various Man-in-The-Middle (MiTM) attacks or through network packet captures.

Scanner discovered that the affected application is using HTTPS however does not use the HSTS header.

Solution

Depending on the framework being used the implementation methods will vary, however it is advised that the `Strict-Transport-Security` header be configured on the server.
One of the options for this header is `max-age`, which is a representation (in milliseconds) determining the time in which the client's browser will adhere to the header policy.
Depending on the environment and the application this time period could be from as low as minutes to as long as days.

See Also

https://hstspreload.org/
https://tools.ietf.org/html/rfc6797
https://www.chromium.org/hsts
https://www.owasp.org/index.php/HTTP_Strict_Transport_Security_Cheat_Sheet

Plugin Details

PUBLICATION DATE	2017-03-31T00:00:00+00:00
MODIFICATION DATE	2025-05-16T00:00:00+00:00
FAMILY	HTTP Security Header
SEVERITY	Medium
PLUGIN ID	98056

Risk Information

CVSSV4 BASE SCORE	6.3
CVSSV4 VECTOR	CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N
CVSSV3 BASE SCORE	6.5
CVSSV3 VECTOR	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N
CVSS BASE SCORE	5.8

CVSS VECTOR	CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:N

Reference Information

CWE	319, 523
WASC	Insufficient Transport Layer Protection
OWASP	2010-A9, 2013-A6, 2017-A3, 2021-A2, 2023-API8, 2019-API7
CVE	-
BID	-

Missing HTTP Strict Transport Security Policy Instances (3)

VULNERABILITY **MEDIUM** PLUGIN ID 98056

INSTANCE

https://jmx.ambiente-de-pruebas-devcts.site/

Identification

OUTPUT

The scanner did not find any Strict-Transport-Security header in the response returned by the target when querying URL 'https://jmx.ambiente-de-pruebas-devcts.site/'.

HTTP Info

REQUEST MADE
GET https://jmx.ambiente-de-pruebas-devcts.site/

REQUEST HEADERS
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application
/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
Sec-Ch-Ua: "Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36

RESPONSE HEADERS
HTTP/1.1 200 OK
Alt-Svc: h3=":443"; ma=2592000
Cache-Control: no-cache, private
Content-Encoding: br
Content-Type: text/html; charset=UTF-8
Date: Tue, 17 Jun 2025 17:47:19 GMT
Server: swoole-http-server
Set-Cookie: XSRF-
TOKEN=eyJpdiI6InZsN3Q4MWF1RkNlRngzOUlreEcxWUE9PSIsInZhbHVlIjoiNXRhTVlKakhpbHNsZTNkN2FKdmwxY3dZaGtobkhwWGptOGhRUm1lY2Z1WWFI
3D; expires=Tue, 17-Jun-2025 19:47:19 GMT; Max-Age=7200; path=/; SameSite=lax
laravel_session=eyJpdiI6ImxaY0g0K0lhUjhWYzdwVExhbHpiQmc9PSIsInZhbHVlIjoibGNQZlM2TWZvYVhzaFhmeVJVNnFYYUhPazVxdS9MMmdlK0k0WI
3D; expires=Tue, 17-Jun-2025 19:47:19 GMT; Max-Age=7200; path=/; HttpOnly; SameSite=lax
Content-Length: 4463

INSTANCE

https://jmx.ambiente-de-pruebas-devcts.site/auth/redirect

Identification

OUTPUT

The scanner did not find any Strict-Transport-Security header in the response returned by the target when querying URL 'https://jmx.ambiente-de-pruebas-devcts.site/auth/redirect'.

HTTP Info

REQUEST MADE
GET /auth/redirect HTTP/2

REQUEST HEADERS
Host: jmx.ambiente-de-pruebas-devcts.site
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US,en;q=0.5
Cookie: XSRF-TOKEN=eyJpdiI6ImlsVGtWRkFvQzl6RG1nWnFhY3U0V3c9PSIsInZhbHVlIjoic3AzQlUrdmxyTDV3L0NVSmt5ZXd4K0NvWEJXQ016LytMNC9sQUgwVnBlVFM<

3D;
laravel_session=eyJpdiI6Ikc5RC8wc1gyNVlkSW93NzR3NGFUnc9PSIsInZhbHVlIjoiUjJtR1ZlVWVybThkWVpzUjEwSW9MVTVzazI3TTI0bEU2K2drNV<

3D

RESPONSE HEADERS
HTTP/2 302
alt-svc: h3=":443"; ma=2592000
cache-control: no-cache, private
content-encoding: br
content-type: text/html; charset=utf-8
date: Tue, 17 Jun 2025 17:58:21 GMT
location: https://login.microsoftonline.com/a88efafd-1953-4e7f-a7a4-a9e6b72cb2f5/oauth2/v2.0/authorize?
client_id=03e01ab5-f758-4123-9797-f9e3af71c658&redirect_uri=https%3A%2F%2Fjmx.ambiente-de-pruebas-devcts.site%2Fauth%
2Fvalidate&scope=User.Read&response_type=code&state=MUHW8lRK0jwkavUgULrQEy5NHUJJHaBGS77aNq1d
server: swoole-http-server
set-cookie: XSRF-TOKEN=eyJpdiI6Iktsa1I0T3pHSXY5UGVDWElwbEUrY0E9PSIsInZhbHVlIjoiZUJ2bmM4SXkzNEs1NWxHRVBwYXh3Z2FZYW5MT3NaSitxRzlaUHlKSnJsZE5<

3D; expires=Tue, 17-Jun-2025 19:58:21 GMT; Max-Age=7200; path=/; SameSite=lax
set-cookie:
laravel_session=eyJpdiI6Iisvc3htcU1nNjFSSkc1QjlnaU0vMlE9PSIsInZhbHVlIjoibHBENFZraEovVmlvbFhGS2RPd1lLc1F4Zkt0RjRrd1dyM3dpZ<

3D; expires=Tue, 17-Jun-2025 19:58:21 GMT; Max-Age=7200; path=/; HttpOnly; SameSite=lax
content-length: 447

INSTANCE

https://jmx.ambiente-de-pruebas-devcts.site/img/paisajes.mp4

Identification

OUTPUT
The scanner did not find any Strict-Transport-Security header in the response returned by the target when querying URL
'https://jmx.ambiente-de-pruebas-devcts.site/img/paisajes.mp4'.

HTTP Info

REQUEST MADE
GET https://jmx.ambiente-de-pruebas-devcts.site/img/paisajes.mp4

REQUEST HEADERS
Accept: */*
Accept-Encoding: identity;q=1, *;q=0
Cookie: XSRF-TOKEN=eyJpdiI6InovclBzTkU2VG51UEF5a3U5MFFlU0E9PSIsInZhbHVlIjoiRUUvWWhNY2FNRVJJRHRBcFFWRjVSZHkzYjJ4WFNlZkxxjaCtkTE80UDBPZTk<

3D;
laravel_session=eyJpdiI6IjZKZXBiTGVCQlorSmppczZDZk9KVmc9PSIsInZhbHVlIjoid1FUVFZYZDl2TkFISVUxaXBnbUNOalNNWlMVWtBYXJjVzNMaI<

3D
Priority: i
Range: bytes=0-
Referer: https://jmx.ambiente-de-pruebas-devcts.site/img/paisajes.mp4
Sec-Ch-Ua: "Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Sec-Fetch-Dest: video
Sec-Fetch-Mode: no-cors

```
Sec-Fetch-Site: same-origin
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS
```
H3 200
Content-Type: video/mp4
Date: Tue, 17 Jun 2025 17:59:38 GMT
Server: swoole-http-server
Content-Length: 30616863
```

PHP Input Variables Exceeded

VULNERABILITY   MEDIUM   PLUGIN ID 114322

Description

By default, PHP accepts a maximum of 1000 variables in a request. If there are more input variables than specified, an E_WARNING is issued, and further input variables are truncated from the request depending on server configuration and application code, this can have various impacts such as bypassing function call.

Solution

Disable all notice, warning and error displaying. Configure the application to log such messages in a file. A code review is also necessary to check the impact it may have on the application.

See Also

https://hackmd.io/@terjanq/justCTF2020-writeups#Baby-CSP-web-6-solves-406-points
https://www.php.net/manual/en/info.configuration.php#ini.max-input-vars
https://x.com/pilvar222/status/1784618120902005070

Plugin Details

PUBLICATION DATE	2024-06-26T00:00:00+00:00
MODIFICATION DATE	2024-06-26T00:00:00+00:00
FAMILY	Web Applications
SEVERITY	Medium
PLUGIN ID	114322

Risk Information

CVSSV4 BASE SCORE	6.9
CVSSV4 VECTOR	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:L/SC:N/SI:N/SA:N
CVSSV3 BASE SCORE	5.3
CVSSV3 VECTOR	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L
CVSS BASE SCORE	5.0
CVSS VECTOR	CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P

Reference Information

CWE	473
WASC	Improper Input Handling
OWASP	2013-A1, 2010-A1, 2017-A1, 2021-A8, 2023-API3, 2019-API8
CVE	-
BID	-

PHP Input Variables Exceeded Instances (2)

VULNERABILITY MEDIUM PLUGIN ID 114322

INSTANCE

https://jmx.ambiente-de-pruebas-devcts.site/?
x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=

Identification

OUTPUT

The scanner was able to detected a PHP Warning caused by too many injected variables.

HTTP Info

REQUEST MADE

GET /?
x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=
HTTP/2

REQUEST HEADERS

Host: jmx.ambiente-de-pruebas-devcts.site
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application
/signed-exchange;v=b3;q=0.7
Accept-Language: en-US,en;q=0.5
Cookie: XSRF-
TOKEN=eyJpdiI6InVsNk8xVWlIWTdrWWJTMndmWm5OSlE9PSIsInZhbHVlIjoiclZVRHBqWG9GTzFnR1E1YWFCYTJ5YmhyQlZzQTdJM0dsczzUvTE5jS1FSYVR
3D;
laravel_session=eyJpdiI6ImF5emw1djlvYnhrWjZNUFdDcGgrcEE9PSIsInZhbHVlIjoiSGloeHHeVVGWjdndnM3c1A3S3NuSnBMaE83WU9UUzZOczU0ZI
3D

RESPONSE HEADERS

HTTP/2 500
alt-svc: h3=":443"; ma=2592000
cache-control: no-cache, private
content-encoding: br
content-type: text/html; charset=UTF-8
date: Tue, 17 Jun 2025 17:52:41 GMT
server: swoole-http-server
content-length: 62310

INSTANCE

https://jmx.ambiente-de-pruebas-devcts.site/auth/redirect/?
x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=

Identification

OUTPUT

The scanner was able to detected a PHP Warning caused by too many injected variables.

HTTP Info

REQUEST MADE

```
GET /auth/redirect/?
x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x:
HTTP/2
```

REQUEST HEADERS

```
Host: jmx.ambiente-de-pruebas-devcts.site
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application
/signed-exchange;v=b3;q=0.7
Accept-Language: en-US,en;q=0.5
Cookie: XSRF-
TOKEN=eyJpdiI6InduaWdlMFdSclg2QWRZOHJpamt0V3c9PSIsInZhbHVlIjoiaUR6VllZZWwrUUV0U2trMjF4SitOQWxSK1lFVll4QzAvNk9iSzJlbVYzcXVyXAv
3D;
laravel_session=eyJpdiI6IkNrdGjh2dGRJVlB5RFpsSW1KK25hMnc9PSIsInZhbHVlIjoiYkdoVmVQWDRESVhTQ0RncC9BSkl2UVZnZllTeEwrSllBWUUwSI
3D
```

RESPONSE HEADERS

```
HTTP/2 500
alt-svc: h3=":443"; ma=2592000
cache-control: no-cache, private
content-encoding: br
content-type: text/html; charset=UTF-8
date: Tue, 17 Jun 2025 17:58:37 GMT
server: swoole-http-server
content-length: 62322
```

Missing 'X-Frame-Options' Header

VULNERABILITY LOW PLUGIN ID 98060

Description

Clickjacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages.

The server didn't return an `X-Frame-Options` header which means that this website could be at risk of a clickjacking attack.

The `X-Frame-Options` HTTP response header can be used to indicate whether or not a browser should be allowed to render a page inside a frame or iframe. Sites can use this to avoid clickjacking attacks, by ensuring that their content is not embedded into other sites.

Solution

Configure your web server to include an `X-Frame-Options` header.

See Also

http://tools.ietf.org/html/rfc7034
https://developer.mozilla.org/en-US/docs/Web/HTTP/X-Frame-Options
https://www.owasp.org/index.php/Clickjacking

Plugin Details

PUBLICATION DATE	2017-03-31T00:00:00+00:00
MODIFICATION DATE	2024-03-25T00:00:00+00:00
FAMILY	HTTP Security Header
SEVERITY	Low
PLUGIN ID	98060

Risk Information

CVSSV4 BASE SCORE	2.1
CVSSV4 VECTOR	CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:A/VC:N/VI:L/VA:N/SC:L/SI:L/SA:N
CVSSV3 BASE SCORE	3.1
CVSSV3 VECTOR	CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:N
CVSS BASE SCORE	2.6
CVSS VECTOR	CVSS2#AV:N/AC:H/Au:N/C:N/I:P/A:N

Reference Information

CWE	1021, 346
WASC	Application Misconfiguration
OWASP	2021-A7, 2017-A6, 2021-A4, 2013-A5, 2010-A6, 2023-API8, 2019-API7
CVE	-

BID	-

Missing 'X-Frame-Options' Header Instances (2)

VULNERABILITY LOW PLUGIN ID 98060

INSTANCE

https://jmx.ambiente-de-pruebas-devcts.site/

Identification

OUTPUT

Page https://jmx.ambiente-de-pruebas-devcts.site/ has no X-Frame-Options header defined

HTTP Info

REQUEST MADE
GET https://jmx.ambiente-de-pruebas-devcts.site/

REQUEST HEADERS
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application
/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
Sec-Ch-Ua: "Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36

RESPONSE HEADERS
HTTP/1.1 200 OK
Alt-Svc: h3=":443"; ma=2592000
Cache-Control: no-cache, private
Content-Encoding: br
Content-Type: text/html; charset=UTF-8
Date: Tue, 17 Jun 2025 17:47:19 GMT
Server: swoole-http-server
Set-Cookie: XSRF-
TOKEN=eyJpdiI6InZsN3Q4MWFlRkNlRngzOUlreEcxWUE9PSIsInZhbHVlIjoiNXRhTVlKKakhpbHNsZTNkN2FKdmwxY3dZaGtobkhwWGptOGhRUm1lY2Z1WWFI
3D; expires=Tue, 17-Jun-2025 19:47:19 GMT; Max-Age=7200; path=/; SameSite=lax
laravel_session=eyJpdiI6ImxaY0g0K0lhUjhWYzdwVExhbHpiQmc9PSIsInZhbHVlIjoibGNQZlM2TWZvYVhzaFhmeVJVNnFYYUhPazVxdS9MMmdlK0k0WI
3D; expires=Tue, 17-Jun-2025 19:47:19 GMT; Max-Age=7200; path=/; HttpOnly; SameSite=lax
Content-Length: 4463

INSTANCE

https://jmx.ambiente-de-pruebas-devcts.site/img/paisajes.mp4

Identification

OUTPUT

Page https://jmx.ambiente-de-pruebas-devcts.site/img/paisajes.mp4 has no X-Frame-Options header defined

HTTP Info

REQUEST MADE

```
GET https://jmx.ambiente-de-pruebas-devcts.site/img/paisajes.mp4
```

REQUEST HEADERS
```
Accept: */*
Accept-Encoding: identity;q=1, *;q=0
Cookie: XSRF-
TOKEN=eyJpdiI6InovclBzTkU2VG51UEF5a3U5MFFlU0E9PSIsInZhbHVlIjoiRUUvWWhNY2FNRVJJRHRBcFFWRjVSZHkzYjJ4WFNlZkxjaCtkTE80UDBPZTk:
3D;
laravel_session=eyJpdiI6IjZKZXBiTGVCQlorSmppczZDZk9KVmc9PSIsInZhbHVlIjoid1FUVFZYZDl2TkFISVUxaXBnbUNOalNSNWlMVWtBYXJjVzNMaI:
3D
Priority: i
Range: bytes=0-
Referer: https://jmx.ambiente-de-pruebas-devcts.site/img/paisajes.mp4
Sec-Ch-Ua: "Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Sec-Fetch-Dest: video
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS
```
H3 200
Content-Type: video/mp4
Date: Tue, 17 Jun 2025 17:59:38 GMT
Server: swoole-http-server
Content-Length: 30616863
```

Cookie Without HttpOnly Flag Detected

VULNERABILITY LOW PLUGIN ID 98063

Description

The HttpOnly flag assists in the prevention of client side-scripts (such as JavaScript) from accessing and using the cookie.

This can help prevent XSS attacks from targeting the cookies holding the client's session token (setting the HttpOnly flag does not prevent, nor safeguard against XSS vulnerabilities themselves).

Solution

The initial step to remedy this would be to determine whether any client-side scripts (such as JavaScript) need to access the cookie and if not, set the HttpOnly flag.
It should be noted that some older browsers are not compatible with the HttpOnly flag; therefore, setting this flag will not protect those clients against this form of attack.

See Also

https://www.owasp.org/index.php/HttpOnly

Plugin Details

PUBLICATION DATE	2017-03-31T00:00:00+00:00
MODIFICATION DATE	2023-12-11T00:00:00+00:00
FAMILY	HTTP Security Header
SEVERITY	Low
PLUGIN ID	98063

Risk Information

CVSSV4 BASE SCORE	2.1
CVSSV4 VECTOR	CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:A/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N
CVSSV3 BASE SCORE	3.1
CVSSV3 VECTOR	CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N
CVSS BASE SCORE	2.6
CVSS VECTOR	CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N

Reference Information

CWE	1004
WASC	Application Misconfiguration
OWASP	2010-A9, 2013-A6, 2017-A3, 2021-A5
CVE	-
BID	-

Cookie Without HttpOnly Flag Detected Instances (1)

VULNERABILITY LOW PLUGIN ID 98063

INSTANCE

https://jmx.ambiente-de-pruebas-devcts.site/

INPUT TYPE	cookie
INPUT NAME	XSRF-TOKEN

Identification

PROOF
```
Set-Cookie : XSRF-
TOKEN=eyJpdiI6InZsN3Q4MWF1RkNlRngzOUlreEcxWUE9PSIsInZhbHVlIjoiNXRhTVlKakhpbHNsZTNkN2FKdmwxY3dZaGtobkhwWGptOGhRUm1lY2lWWFF
3D; Expires=2025-06-17 19:47:19 +0000; Max_age=7200; Path=/; SameSite=lax
```

OUTPUT
```
The scanner detected a cookie named 'XSRF-TOKEN' set through a 'Set-Cookie' that does not set the HttpOnly flag.

If the cookie is set to handle sensitive information (for example session-based information), it should be set via the
HTTP method.
```

HTTP Info

REQUEST MADE
```
GET https://jmx.ambiente-de-pruebas-devcts.site/
```

REQUEST HEADERS
```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application
/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
Sec-Ch-Ua: "Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS
```
HTTP/1.1 200 OK
Alt-Svc: h3=":443"; ma=2592000
Cache-Control: no-cache, private
Content-Encoding: br
Content-Type: text/html; charset=UTF-8
Date: Tue, 17 Jun 2025 17:47:19 GMT
Server: swoole-http-server
Set-Cookie: XSRF-
TOKEN=eyJpdiI6InZsN3Q4MWF1RkNlRngzOUlreEcxWUE9PSIsInZhbHVlIjoiNXRhTVlKakhpbHNsZTNkN2FKdmwxY3dZaGtobkhwWGptOGhRUm1lY2lWWFF
3D; expires=Tue, 17-Jun-2025 19:47:19 GMT; Max-Age=7200; path=/; SameSite=lax
laravel_session=eyJpdiI6ImxaY0g0K0lhUjhWYzdwVExhbHpiQmc9PSIsInZhbHVlIjoibGNQZlM2TWZvYVhzaFhmeVJVNnFYYUhPazVxdS9MMmdlK0k0WI
3D; expires=Tue, 17-Jun-2025 19:47:19 GMT; Max-Age=7200; path=/; HttpOnly; SameSite=lax
Content-Length: 4463
```

Cookie Without Secure Flag Detected

VULNERABILITY · LOW · PLUGIN ID 98064

Description

When the `secure` flag is set on a cookie, the browser will prevent it from being sent over a clear text channel (HTTP) and only allow it to be sent when an encrypted channel is used (HTTPS).

The scanner discovered that a cookie was set by the server without the secure flag being set. Although the initial setting of this cookie was via an HTTPS connection, any HTTP link to the same server will result in the cookie being sent in clear text.

Note that if the cookie does not contain sensitive information, the risk of this vulnerability is mitigated.

Solution

If the cookie contains sensitive information, then the server should ensure that the cookie has the `secure` flag set.

See Also

https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#secure-attribute

Plugin Details

PUBLICATION DATE	2017-03-31T00:00:00+00:00
MODIFICATION DATE	2023-12-11T00:00:00+00:00
FAMILY	HTTP Security Header
SEVERITY	Low
PLUGIN ID	98064

Risk Information

CVSSV4 BASE SCORE	2.1
CVSSV4 VECTOR	CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:A/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N
CVSSV3 BASE SCORE	3.1
CVSSV3 VECTOR	CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N
CVSS BASE SCORE	2.6
CVSS VECTOR	CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N

Reference Information

CWE	614
WASC	Insufficient Transport Layer Protection
OWASP	2010-A9, 2013-A6, 2017-A3, 2021-A5
CVE	-
BID	-

Cookie Without Secure Flag Detected Instances (2)

VULNERABILITY LOW   PLUGIN ID 98064

INSTANCE

https://jmx.ambiente-de-pruebas-devcts.site/

INPUT TYPE	cookie
INPUT NAME	laravel_session

Identification

PROOF

```
Set-Cookie :
laravel_session=eyJpdiI6ImxaY0g0K0lhUjhWYzdwVExhbHpiQmc9PSIsInZhbHVlIjoibGNQZ1M2TWZvYVhzaFhmeVJVNnFYYUhPazVxdS9MMmdlK0k0Wl
3D; Expires=2025-06-17 19:47:19 +0000; Max_age=7200; Path=/; HttpOnly; SameSite=lax
```

OUTPUT

The scanner detected a cookie named 'laravel_session' set through a 'Set-Cookie' header without the Secure flag set.

HTTP Info

REQUEST MADE

GET https://jmx.ambiente-de-pruebas-devcts.site/

REQUEST HEADERS

```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application
/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
Sec-Ch-Ua: "Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc: h3=":443"; ma=2592000
Cache-Control: no-cache, private
Content-Encoding: br
Content-Type: text/html; charset=UTF-8
Date: Tue, 17 Jun 2025 17:47:19 GMT
Server: swoole-http-server
Set-Cookie: XSRF-
TOKEN=eyJpdiI6InZsN3Q4MWFlRkNlRngzOUlreEcxWUE9PSIsInZhbHVlIjoiNXRhTVlKakhpbHNsZTNkN2FKdmwxY3dZaGtobhwWGptOGhRUm1lY2Z1WWFI
3D; expires=Tue, 17-Jun-2025 19:47:19 GMT; Max-Age=7200; path=/; SameSite=lax
laravel_session=eyJpdiI6ImxaY0g0K0lhUjhWYzdwVExhbHpiQmc9PSIsInZhbHVlIjoibGNQZ1M2TWZvYVhzaFhmeVJVNnFYYUhPazVxdS9MMmdlK0k0Wl
3D; expires=Tue, 17-Jun-2025 19:47:19 GMT; Max-Age=7200; path=/; HttpOnly; SameSite=lax
Content-Length: 4463
```

INSTANCE

https://jmx.ambiente-de-pruebas-devcts.site/

INPUT TYPE	cookie
INPUT NAME	XSRF-TOKEN

Identification

PROOF

```
Set-Cookie : XSRF-
TOKEN=eyJpdiI6InZsN3Q4MWF1RkNlRngzOUlreEcxWUE9PSIsInZhbHVlIjoiNXRhTVlKakhpbHNsZTNkN2FKdmwxY3dZaGtobkhwWGptOGhRUm1lY2ZlWWFI
3D; Expires=2025-06-17 19:47:19 +0000; Max_age=7200; Path=/; SameSite=lax
```

OUTPUT

The scanner detected a cookie named 'XSRF-TOKEN' set through a 'Set-Cookie' header without the Secure flag set.

HTTP Info

REQUEST MADE

GET https://jmx.ambiente-de-pruebas-devcts.site/

REQUEST HEADERS

```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application
/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
Sec-Ch-Ua: "Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc: h3=":443"; ma=2592000
Cache-Control: no-cache, private
Content-Encoding: br
Content-Type: text/html; charset=UTF-8
Date: Tue, 17 Jun 2025 17:47:19 GMT
Server: swoole-http-server
Set-Cookie: XSRF-
TOKEN=eyJpdiI6InZsN3Q4MWF1RkNlRngzOUlreEcxWUE9PSIsInZhbHVlIjoiNXRhTVlKakhpbHNsZTNkN2FKdmwxY3dZaGtobkhwWGptOGhRUm1lY2ZlWWFI
3D; expires=Tue, 17-Jun-2025 19:47:19 GMT; Max-Age=7200; path=/; SameSite=lax
laravel_session=eyJpdiI6ImxaY0g0K0lhUjhWYzdwVExhbHpiQmc9PSIsInZhbHVlIjoibGNQZ1M2TWZvYVhzaFhmeVJVNnFYYUhPazVxdS9MMmdlK0k0Wl
3D; expires=Tue, 17-Jun-2025 19:47:19 GMT; Max-Age=7200; path=/; HttpOnly; SameSite=lax
Content-Length: 4463
```

HTTP Header Information Disclosure

VULNERABILITY LOW PLUGIN ID 98618

Description

The HTTP headers sent by the remote web server disclose information that can aid an attacker, such as the server version and technologies used by the web server.

Solution

Modify the HTTP headers of the web server to not disclose detailed information about the underlying web server.

See Also

http://projects.webappsec.org/w/page/13246925/Fingerprinting

https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers

Plugin Details

PUBLICATION DATE	2019-06-12T00:00:00+00:00
MODIFICATION DATE	2024-03-25T00:00:00+00:00
FAMILY	HTTP Security Header
SEVERITY	Low
PLUGIN ID	98618

Risk Information

CVSSV4 BASE SCORE	2.1
CVSSV4 VECTOR	CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:A/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N
CVSSV3 BASE SCORE	3.1
CVSSV3 VECTOR	CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N
CVSS BASE SCORE	2.6
CVSS VECTOR	CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N

Reference Information

CWE	200
WASC	Information Leakage
OWASP	2017-A6, 2021-A1, 2013-A5, 2010-A6, 2023-API8, 2019-API7
CVE	-
BID	-

HTTP Header Information Disclosure Instances (3)

VULNERABILITY `LOW` PLUGIN ID 98618

INSTANCE

https://jmx.ambiente-de-pruebas-devcts.site/

Identification

OUTPUT

The following header information disclosures have been detected on https://jmx.ambiente-de-pruebas-devcts.site/:

- Server: swoole-http-server

HTTP Info

REQUEST MADE
GET https://jmx.ambiente-de-pruebas-devcts.site/

REQUEST HEADERS
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application
/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
Sec-Ch-Ua: "Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36

RESPONSE HEADERS
HTTP/1.1 200 OK
Alt-Svc: h3=":443"; ma=2592000
Cache-Control: no-cache, private
Content-Encoding: br
Content-Type: text/html; charset=UTF-8
Date: Tue, 17 Jun 2025 17:47:19 GMT
Server: swoole-http-server
Set-Cookie: XSRF-
TOKEN=eyJpdiI6InZsN3Q4MWF1RkNlRngzOUlreEcxWUE9PSIsInZhbHVlIjoiNXRhTVlKakhpbHNsZTNkN2FKdmwxY3dZaGtobkhwWGptOGhRUm1lY2ZlWWFI
3D; expires=Tue, 17-Jun-2025 19:47:19 GMT; Max-Age=7200; path=/; SameSite=lax
laravel_session=eyJpdiI6ImxaY0g0K0lhUjhWYzdwVExhbHpiQmc9PSIsInZhbHVlIjoibGNQZlM2TWZvYVhzaFhmeVJVNnFYYUhPazVxdS9MMmdlK0k0WI
3D; expires=Tue, 17-Jun-2025 19:47:19 GMT; Max-Age=7200; path=/; HttpOnly; SameSite=lax
Content-Length: 4463

INSTANCE

https://jmx.ambiente-de-pruebas-devcts.site/img/paisajes.mp4

Identification

OUTPUT

The following header information disclosures have been detected on https://jmx.ambiente-de-pruebas-devcts.site/img
/paisajes.mp4:

- Server: swoole-http-server

HTTP Info

REQUEST MADE
GET https://jmx.ambiente-de-pruebas-devcts.site/img/paisajes.mp4

REQUEST HEADERS
```
Accept: */*
Accept-Encoding: identity;q=1, *;q=0
Cookie: XSRF-
TOKEN=eyJpdiI6InovclBzTkU2VG51UEF5a3U5MFFlU0E9PSIsInZhbHVlIjoiRUUvWWhNY2FNRVJJRHRBcFFWRjVSZHkzYjJ4WFNlZkxjaCtTE80UDBPZTk]
3D;
laravel_session=eyJpdiI6IjZKZXBiTGVCQlorSmppczZDZk9KVmc9PSIsInZhbHVlIjoid1FUVFZYZDl2TkFISVUxaXBnbUNOalNSNWlMVWtBYXJjVzNMal
3D
Priority: i
Range: bytes=0-
Referer: https://jmx.ambiente-de-pruebas-devcts.site/img/paisajes.mp4
Sec-Ch-Ua: "Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Sec-Fetch-Dest: video
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS
```
H3 200
Content-Type: video/mp4
Date: Tue, 17 Jun 2025 17:59:38 GMT
Server: swoole-http-server
Content-Length: 30616863
```

INSTANCE

https://jmx.ambiente-de-pruebas-devcts.site/auth/redirect

Identification

OUTPUT
The following header information disclosures have been detected on https://jmx.ambiente-de-pruebas-devcts.site/auth
/redirect:

- Server: swoole-http-server

HTTP Info

REQUEST MADE
GET /auth/redirect HTTP/2

REQUEST HEADERS
```
Host: jmx.ambiente-de-pruebas-devcts.site
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application
/signed-exchange;v=b3;q=0.7
Accept-Language: en-US,en;q=0.5
Cookie: XSRF-
TOKEN=eyJpdiI6ImlsVGtWRkFvQzl6RG1nWnFhY3U0V3c9PSIsInZhbHVlIjoic3AzQlUrdmxyTDV3L0NVSmt5Zxd4K0NvWEJXQ016LytMNC9sQUgwVnBlVFM(
3D;
laravel_session=eyJpdiI6Ikc5RC8wc1gyNVlkSW93NzR3NGFUUnc9PSIsInZhbHVlIjoiUjJtR1ZlVWVybThkWVpzUjEwSW9MVTVzazI3TTI0bEU2K2drNV
3D
```

RESPONSE HEADERS
```
HTTP/2 302
alt-svc: h3=":443"; ma=2592000
cache-control: no-cache, private
```

```
content-encoding: br
content-type: text/html; charset=utf-8
date: Tue, 17 Jun 2025 17:58:21 GMT
location: https://login.microsoftonline.com/a88efafd-1953-4e7f-a7a4-a9e6b72cb2f5/oauth2/v2.0/authorize?
client_id=03e01ab5-f758-4123-9797-f9e3af71c658&redirect_uri=https%3A%2F%2Fjmx.ambiente-de-pruebas-devcts.site%2Fauth%
2Fvalidate&scope=User.Read&response_type=code&state=MUHW8lRK0jwkavUgULrQEy5NHUJJHaBGS77aNq1d
server: swoole-http-server
set-cookie: XSRF-
TOKEN=eyJpdiI6Iktsa1I0T3pHSXY5UGVDWElwbEUrY0E9PSIsInZhbHVlIjoiZUJ2bmM4SXkzNEs1NWxHRVBwYXh3Z2FZYW5MT3NaSitxRzlaUHlKSnJsZE5l
3D; expires=Tue, 17-Jun-2025 19:58:21 GMT; Max-Age=7200; path=/; SameSite=lax
set-cookie:
laravel_session=eyJpdiI6Iisvc3htcU1nNjFSSkc1QjlnaU0vMlE9PSIsInZhbHVIIjoibHBENFZraEovVmlvbFhGGS2RPd1lLc1F4Zkt0RjRrd1dyM3dpZ(
3D; expires=Tue, 17-Jun-2025 19:58:21 GMT; Max-Age=7200; path=/; HttpOnly; SameSite=lax
content-length: 447
```

Missing 'X-Content-Type-Options' Header

VULNERABILITY LOW PLUGIN ID 112529

Description

The HTTP 'X-Content-Type-Options' response header prevents the browser from MIME-sniffing a response away from the declared content-type.

The server did not return a correct 'X-Content-Type-Options' header, which means that this website could be at risk of a Cross-Site Scripting (XSS) attack.

Solution

Configure your web server to include an 'X-Content-Type-Options' header with a value of 'nosniff'.

See Also

https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Content-Type-Options
https://www.owasp.org/index.php/OWASP_Secure_Headers_Project#xcto

Plugin Details

PUBLICATION DATE	2018-11-28T00:00:00+00:00
MODIFICATION DATE	2024-03-25T00:00:00+00:00
FAMILY	HTTP Security Header
SEVERITY	Low
PLUGIN ID	112529

Risk Information

CVSSV4 BASE SCORE	2.1
CVSSV4 VECTOR	CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:A/VC:L/VI:N/VA:N/SC:L/SI:L/SA:N
CVSSV3 BASE SCORE	3.1
CVSSV3 VECTOR	CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N
CVSS BASE SCORE	2.6
CVSS VECTOR	CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N

Reference Information

CWE	693
WASC	Application Misconfiguration
OWASP	2017-A6, 2013-A5, 2010-A6, 2023-API8, 2019-API7
CVE	-
BID	-

Missing 'X-Content-Type-Options' Header Instances (2)

VULNERABILITY LOW PLUGIN ID 112529

INSTANCE

https://jmx.ambiente-de-pruebas-devcts.site/

Identification

OUTPUT

The scanner detected the lack of a correct X-Content-Type-Options header configuration in the target application response

HTTP Info

REQUEST MADE

GET https://jmx.ambiente-de-pruebas-devcts.site/

REQUEST HEADERS

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application
/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
Sec-Ch-Ua: "Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36

RESPONSE HEADERS

HTTP/1.1 200 OK
Alt-Svc: h3=":443"; ma=2592000
Cache-Control: no-cache, private
Content-Encoding: br
Content-Type: text/html; charset=UTF-8
Date: Tue, 17 Jun 2025 17:47:19 GMT
Server: swoole-http-server
Set-Cookie: XSRF-
TOKEN=eyJpdiI6InZsN3Q4MWF1RkNlRngzOUlreEcxWUE9PSIsInZhbHVlIjoiNXRhTVlKakhpbHNsZTNkN2FKdmwxY3dZaGtobkhwWGptOGhRUm1lY2Z1WWF1
3D; expires=Tue, 17-Jun-2025 19:47:19 GMT; Max-Age=7200; path=/; SameSite=lax
laravel_session=eyJpdiI6ImxaY0g0K0lhUjhWYzdwVExhbHpiQmc9PSIsInZhbHVlIjoibGNQZ1M2TWZvYVhzaFhmeVJVNnFYYUhPazVxdS9MMmdlK0k0WL
3D; expires=Tue, 17-Jun-2025 19:47:19 GMT; Max-Age=7200; path=/; HttpOnly; SameSite=lax
Content-Length: 4463

INSTANCE

https://jmx.ambiente-de-pruebas-devcts.site/img/paisajes.mp4

Identification

OUTPUT

The scanner detected the lack of a correct X-Content-Type-Options header configuration in the target application response

HTTP Info

REQUEST MADE

GET https://jmx.ambiente-de-pruebas-devcts.site/img/paisajes.mp4

REQUEST HEADERS

Accept: */*
Accept-Encoding: identity;q=1, *;q=0
Cookie: XSRF-
TOKEN=eyJpdiI6InovclBzTkU2VG51UEF5a3U5MFFlU0E9PSIsInZhbHVlIjoiRUUvWWhNY2FNRVJJRHRBcFFWRjVSZHkzYjJ4WFN1ZkxjjaCtkTE80UDBPZTk1
3D;
laravel_session=eyJpdiI6IjZKZXBiTGVCQlorSmppczZDZk9KVmc9PSIsInZhbHVlIjoid1FUVFZYZDl2TkFISVUxaXBnbUNOalNSNWlMVWtBYXJjVzNMaE
3D
Priority: i
Range: bytes=0-
Referer: https://jmx.ambiente-de-pruebas-devcts.site/img/paisajes.mp4
Sec-Ch-Ua: "Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Sec-Fetch-Dest: video
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36

RESPONSE HEADERS

H3 200
Content-Type: video/mp4
Date: Tue, 17 Jun 2025 17:59:38 GMT
Server: swoole-http-server
Content-Length: 30616863

SSL/TLS Weak Cipher Suites Supported

VULNERABILITY LOW PLUGIN ID 112539

Description

The remote host supports the use of SSL/TLS ciphers that offer weak encryption (including RC4 and 3DES encryption).

Solution

Reconfigure the affected application, if possible to avoid the use of weak ciphers.

See Also

https://www.iana.org/assignments/tls-parameters/tls-parameters.xhtml

Plugin Details

PUBLICATION DATE	2019-01-21T00:00:00+00:00
MODIFICATION DATE	2022-10-07T00:00:00+00:00
FAMILY	SSL/TLS
SEVERITY	Low
PLUGIN ID	112539

Risk Information

CVSSV4 BASE SCORE	2.3
CVSSV4 VECTOR	CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:P/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N
CVSSV3 BASE SCORE	3.7
CVSSV3 VECTOR	CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N
CVSS BASE SCORE	2.6
CVSS VECTOR	CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N

Reference Information

CWE	326
WASC	Application Misconfiguration
OWASP	2010-A7, 2013-A6, 2017-A3, 2021-A2, 2023-API8, 2019-API7
CVE	-
BID	-

SSL/TLS Weak Cipher Suites Supported Instances (1)

VULNERABILITY LOW PLUGIN ID 112539

INSTANCE

https://jmx.ambiente-de-pruebas-devcts.site/

Identification

OUTPUT

```
Protocol Cipher Suite Name (RFC) Key Exchange Strength
------------------------------------------------------------------
TLS1.2 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA x25519 256
TLS1.2 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA x25519 256
```

Missing Content Security Policy

VULNERABILITY LOW PLUGIN ID 112551

Description

Content Security Policy (CSP) is a web security standard that helps to mitigate attacks like cross-site scripting (XSS), clickjacking or mixed content issues. CSP provides mechanisms to websites to restrict content that browsers will be allowed to load.

No CSP header has been detected on this host. This URL is flagged as a specific example.

Solution

Configure Content Security Policy on your website by adding 'Content-Security-Policy' HTTP header or meta tag http-equiv='Content-Security-Policy'.

See Also

https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP

https://csp-evaluator.withgoogle.com/

https://content-security-policy.com/

https://developers.google.com/web/fundamentals/security/csp/

https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Content-Security-Policy

Plugin Details

PUBLICATION DATE	2019-02-14T00:00:00+00:00
MODIFICATION DATE	2024-03-25T00:00:00+00:00
FAMILY	HTTP Security Header
SEVERITY	Low
PLUGIN ID	112551

Risk Information

CVSSV4 BASE SCORE	2.1
CVSSV4 VECTOR	CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:A/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N
CVSSV3 BASE SCORE	3.1
CVSSV3 VECTOR	CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N
CVSS BASE SCORE	2.6
CVSS VECTOR	CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N

Reference Information

CWE	1021
WASC	Application Misconfiguration
OWASP	2017-A6, 2021-A4, 2013-A5, 2010-A6, 2023-API8, 2019-API7
CVE	-

BID	-

Missing Content Security Policy Instances (1)

VULNERABILITY LOW PLUGIN ID 112551

INSTANCE

https://jmx.ambiente-de-pruebas-devcts.site/

Identification

OUTPUT

https://jmx.ambiente-de-pruebas-devcts.site/ has no Content Security Policy defined.

HTTP Info

REQUEST MADE

GET https://jmx.ambiente-de-pruebas-devcts.site/

REQUEST HEADERS

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application
/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
Sec-Ch-Ua: "Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36

RESPONSE HEADERS

HTTP/1.1 200 OK
Alt-Svc: h3=":443"; ma=2592000
Cache-Control: no-cache, private
Content-Encoding: br
Content-Type: text/html; charset=UTF-8
Date: Tue, 17 Jun 2025 17:47:19 GMT
Server: swoole-http-server
Set-Cookie: XSRF-
TOKEN=eyJpdiI6InZsN3Q4MWFlRkNlRngzOUlreEcxWUE9PSIsInZhbHVlIjoiNXRhTVlKakhpbHNsZTNkN2FKdmwxY3dZaGtobkhwWGptOGhRUm1lY2ZlWWFF
3D; expires=Tue, 17-Jun-2025 19:47:19 GMT; Max-Age=7200; path=/; SameSite=lax
laravel_session=eyJpdiI6ImxaY0g0K0lhUjhWYzdwVExhbHpiQmc9PSIsInZhbHVlIjoibGNQZlM2TWZvYVhzaFhmeVJVNnFYYUhPazVxdS9MMmdlK0k0WI
3D; expires=Tue, 17-Jun-2025 19:47:19 GMT; Max-Age=7200; path=/; HttpOnly; SameSite=lax
Content-Length: 4463

Missing 'Cache-Control' Header

VULNERABILITY LOW PLUGIN ID 112553

Description

The HTTP 'Cache-Control' header is used to specify directives for caching mechanisms.

The server did not return or returned an invalid 'Cache-Control' header which means page containing sensitive information (password, credit card, personal data, social security number, etc) could be stored on client side disk and then be exposed to unauthorised persons. This URL is flagged as a specific example.

Solution

Configure your web server to include a 'Cache-Control' header with appropriate directives. If page contains sensitive information 'Cache-Control' value should be 'no-store' and 'Pragma' header value should be 'no-cache'.

See Also

https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control
https://www.owasp.org/index.php/Testing_for_Browser_cache_weakness_(OTG-AUTHN-006)

Plugin Details

PUBLICATION DATE	2019-02-15T00:00:00+00:00
MODIFICATION DATE	2024-03-25T00:00:00+00:00
FAMILY	HTTP Security Header
SEVERITY	Low
PLUGIN ID	112553

Risk Information

CVSSV4 BASE SCORE	2.1
CVSSV4 VECTOR	CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:A/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N
CVSSV3 BASE SCORE	3.7
CVSSV3 VECTOR	CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N
CVSS BASE SCORE	2.6
CVSS VECTOR	CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N

Reference Information

CWE	525
WASC	Application Misconfiguration
OWASP	2017-A6, 2021-A4, 2013-A5, 2010-A6, 2023-API8, 2019-API7
CVE	-
BID	-

Missing 'Cache-Control' Header Instances (1)

VULNERABILITY LOW PLUGIN ID 112553

INSTANCE

https://jmx.ambiente-de-pruebas-devcts.site/img/paisajes.mp4

Identification

OUTPUT

https://jmx.ambiente-de-pruebas-devcts.site/img/paisajes.mp4 has no Cache Control header defined.

HTTP Info

REQUEST MADE

GET https://jmx.ambiente-de-pruebas-devcts.site/img/paisajes.mp4

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: identity;q=1, *;q=0
Cookie: XSRF-
TOKEN=eyJpdiI6InovclBzTkU2VG51UEF5a3U5MFFlU0E9PSIsInZhbVlIjoiRUUvWWhNY2FNRVJJRHRBcFFWRjVSZHkzYjJ4WFN1ZkxjjaCtkTE80UDBPZTkl3D;
laravel_session=eyJpdiI6IjZKZXBiTGVCQlorSmppczZDZk9KVmc9PSIsInZhbVlIjoid1FUVFZYZDl2TkFISVUxaXBnbUNOalNNWlMVWtBYXJjVzNMaI3D
Priority: i
Range: bytes=0-
Referer: https://jmx.ambiente-de-pruebas-devcts.site/img/paisajes.mp4
Sec-Ch-Ua: "Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Sec-Fetch-Dest: video
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
H3 200
Content-Type: video/mp4
Date: Tue, 17 Jun 2025 17:59:38 GMT
Server: swoole-http-server
Content-Length: 30616863
```

Scan Information

VULNERABILITY INFO PLUGIN ID 98000

Description

Provides scan information and statistics of plugins run.

Solution

-

See Also

Plugin Details

PUBLICATION DATE	2017-03-31T00:00:00+00:00
MODIFICATION DATE	2023-11-17T00:00:00+00:00
FAMILY	General
SEVERITY	Info
PLUGIN ID	98000

Risk Information

CVSSV4 BASE SCORE	-
CVSSV4 VECTOR	-
CVSSV3 BASE SCORE	-
CVSSV3 VECTOR	-
CVSS BASE SCORE	-
CVSS VECTOR	-

Reference Information

CWE	-
WASC	-
OWASP	-
CVE	-
BID	-

Scan Information Instances (1)

VULNERABILITY INFO PLUGIN ID 98000

INSTANCE

https://jmx.ambiente-de-pruebas-devcts.site

Identification

OUTPUT

```
Engine Version 2.33.16-1861
Plugins Version 202506170623
Scan ID eda37387-84f7-4cc0-9e5b-0f1ee30645a6

Start Time 2025-06-17 17:47:15 +0000
Duration 00:29:25

Requests 8304
Crawler Requests 46
Requests/s 11.211
Mean Response Time 0.538s

Bandwidth Usage
- Data to Target 8.77 MB
- Data from Target 8.48 GB

Timeouts Encountered
Network Timeouts 0
Browser Timeouts 0

Browser Respawns 0

HTTP Protocols Detected
- HTTPs


Authentication Identified
- None


Plugins
- 845 have been included per scan policy
- 627 have been started based on target information collected

List of plugins is available in 'plugins.csv' attachment.


Settings used to conduct this scan are available in 'configuration.csv' attachment.
```

Web Application Sitemap

VULNERABILITY INFO PLUGIN ID 98009

Description

Publishes the sitemap of the web application as seen by the scan.

The list of all URLs that have been detected during the scan are available as an attachment. For each URL in the sitemap, the following information is provided:

- The first time the URL is detected - The logic used to detect the URL. This information may be found by: crawling rendering the page by a specific plugin - The parent URL requested to detect the URL - If the URL has been requested at least once, information about the response - Whether or not the URL has been queued for audit - If the URL has not been queued for audit, the reason why the URL does not need an audit - Whether or not the URL has been effectively audited - If the URL has not been effectively audited, the reason that the scanner was unable to audit the URL

Reasons for not adding a URL to the audit queue are as follows:

- not_in_domain: The domain of the URL does not match main target URL - scope_configuration: The URL does not match scope include list scan settings - directory_depth: The number of directories in the URL path exceeds the scan configuration setting - exclude_file_extension: The URL file extension matched one entry of the file extension blacklist setting - exclude_path_patterns: The URL matched one entry of the URL exclusion blacklist setting - redundant_path: The number of URLs to be audited with the same path and query string parameters has been reached - request_redirect_limit: The number of HTTP redirects allowed per scan configuration setting has been reached - queue_full: The number of URLs to audit has been reached

If a scan fails to audit a URL that has been queued for audit, reasons for the failure are as follows:

- timeout: The request timed out when trying to retrieve URL contents - filesize_exceeded: URL response exceeded file size limit defined in the scan configuration - scan_timelimit_reached: The URL couldn't be audited before the scan time limit - user_abort: The user stopped the scan before the URL could be audited

Solution

-

See Also

Plugin Details

PUBLICATION DATE	2017-03-31T00:00:00+00:00
MODIFICATION DATE	2023-11-17T00:00:00+00:00
FAMILY	General
SEVERITY	Info
PLUGIN ID	98009

Risk Information

CVSSV4 BASE SCORE	-
CVSSV4 VECTOR	-
CVSSV3 BASE SCORE	-
CVSSV3 VECTOR	-
CVSS BASE SCORE	-
CVSS VECTOR	-

Reference Information

CWE	-
WASC	-
OWASP	-
CVE	-
BID	-

Web Application Sitemap Instances (1)

VULNERABILITY **INFO** PLUGIN ID 98009

INSTANCE

https://jmx.ambiente-de-pruebas-devcts.site

Identification

OUTPUT

```
The scan has discovered 15 distinct URLs.

The following is a breakdown of which URLs were audited:

- 3 effectively audited
- 8 not queued due to the URL not being in the target domain
- 4 not queued due to file extension exclusions

For URLs we received responses for, here is a distribution of the content type headers:

- 2 application/javascript; charset=utf-8
- 2 image/png
- 2 text/css
- 4 text/css; charset=utf-8
- 2 text/html; charset=utf-8
- 1 video/mp4

Response times ranged between 0.106454s and 0.26807s.

You can access the complete list of URLs with the information collected by the scan as an attachment to this plugin.
```

Allowed HTTP Methods

VULNERABILITY INFO PLUGIN ID 98047

Description

There are a number of HTTP methods that can be used on a webserver (`OPTIONS`, `HEAD`, `GET`, `POST`, `PUT`, `DELETE` etc.). Each of these methods perform a different function and each have an associated level of risk when their use is permitted on the webserver.

By sending an HTTP OPTIONS request and a direct HTTP request for each method, the scanner discovered the methods that are allowed by the server.

Solution

It is recommended that a whitelisting approach be taken to explicitly permit only the HTTP methods required by the application and block all others.

See Also

http://httpd.apache.org/docs/2.2/mod/core.html#limitexcept

Plugin Details

PUBLICATION DATE	2017-03-31T00:00:00+00:00
MODIFICATION DATE	2024-02-27T00:00:00+00:00
FAMILY	Web Applications
SEVERITY	Info
PLUGIN ID	98047

Risk Information

CVSSV4 BASE SCORE	-
CVSSV4 VECTOR	-
CVSSV3 BASE SCORE	-
CVSSV3 VECTOR	-
CVSS BASE SCORE	-
CVSS VECTOR	-

Reference Information

CWE	-
WASC	-
OWASP	-
CVE	-
BID	-

Allowed HTTP Methods Instances (1)

VULNERABILITY INFO PLUGIN ID 98047

INSTANCE

https://jmx.ambiente-de-pruebas-devcts.site

Identification

OUTPUT

The scanner was able to identify several HTTP methods that can be used for one or several URLs. The results are available as attachments.

Interesting Response

VULNERABILITY INFO PLUGIN ID 98050

Description

The scanner identified some responses with a status code other than the usual 200 (OK), 301 (Moved Permanently), 302 (Found) and 404 (Not Found) codes. These codes can provide useful insights into the behavior of the web application and identify any unexpected responses to be addressed.

Solution

-

See Also

http://www.w3.org/Protocols/rfc2616/rfc2616-sec10.html

https://en.wikipedia.org/wiki/List_of_HTTP_status_codes

Plugin Details

PUBLICATION DATE	2017-03-31T00:00:00+00:00
MODIFICATION DATE	2021-06-14T00:00:00+00:00
FAMILY	Web Applications
SEVERITY	Info
PLUGIN ID	98050

Risk Information

CVSSV4 BASE SCORE	-
CVSSV4 VECTOR	-
CVSSV3 BASE SCORE	-
CVSSV3 VECTOR	-
CVSS BASE SCORE	-
CVSS VECTOR	-

Reference Information

CWE	-
WASC	-
OWASP	-
CVE	-
BID	-

Interesting Response Instances (4)

VULNERABILITY INFO PLUGIN ID 98050

INSTANCE

https://jmx.ambiente-de-pruebas-devcts.site/auth/redirect

Identification

PROOF
HTTP/2 405

OUTPUT
A response has been received with a response code '405' which may require further investigation to verify if this response is due to an abnormal behavior of the target.

The response has been triggered by an HTTP POST request made on the URL 'https://jmx.ambiente-de-pruebas-devcts.site/auth/redirect'.

HTTP Info

REQUEST MADE
POST /auth/redirect HTTP/2

REQUEST HEADERS
Host: jmx.ambiente-de-pruebas-devcts.site
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Spring.cloud.function.routing-Expression: T(java.net.InetAddress).getByName
('wasahp7qewz7thjj4k7pucwhjerge3i4bmuv6luysizmdi3u65lq.was.nessus.org')
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application
/signed-exchange;v=b3;q=0.7
Accept-Language: en-US,en;q=0.5
Cookie: XSRF-
TOKEN=eyJpdiI6InduaWdlMFdSclg2QWRZOHJpamt0V3c9PSIsInZhbVlIjoiaUR6VllZZWwrUUV0U2trMjF4SitOQWxSK1lFFVll4QzAvNk9iSzJ1bVYzcXA\
3D;
laravel_session=eyJpdiI6IkNrddjh2dGRJVlB5RFpsSW1KKK25hMnc9PSIsInZhbVlIjoiYkdoVmVQWDRESVhTQ0RncC9BSkl2UVZnZllTeEwrSllBWUUwSk\
3D
Content-Length: 7
Content-Type: application/x-www-form-urlencoded

RESPONSE HEADERS
HTTP/2 405
allow: GET, HEAD
alt-svc: h3=":443"; ma=2592000
cache-control: no-cache, private
content-encoding: br
content-type: text/html; charset=UTF-8
date: Tue, 17 Jun 2025 17:58:29 GMT
server: swoole-http-server
content-length: 63559

INSTANCE

https%3A%2F%2Fjmx.ambiente-de-pruebas-devcts.site%2Fauth%2Fcgi-bin%2F.%25%2532%2565%2F.%25%2532%2565%2F.%25%2532%2565%2F.%25%2532%2565%2F.%25%2532%2565%2F.%25%2532%2565%2Fetc%2Fpasswd

Identification

PROOF

```
HTTP/1.1 400 Bad Request
```

OUTPUT

A response has been received with a response code '400' which may require further investigation to verify if this
response is due to an abnormal behavior of the target.

The response has been triggered by an HTTP GET request made on the URL 'https://jmx.ambiente-de-pruebas-devcts.site/auth
/cgi-bin/.%%32%65/.%%32%65/.%%32%65/.%%32%65/.%%32%65/etc/passwd'.

HTTP Info

REQUEST MADE

```
GET /auth/cgi-bin/.%%32%65/.%%32%65/.%%32%65/.%%32%65/.%%32%65/etc/passwd HTTP/1.1
```

REQUEST HEADERS

```
Host: jmx.ambiente-de-pruebas-devcts.site
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application
/signed-exchange;v=b3;q=0.7
Accept-Language: en-US,en;q=0.5
Cookie: XSRF-
TOKEN=eyJpdiI6InduaWdlMFdSclg2QWRZOHJpamt0V3c9PSIsInZhbHVlIjoiaUR6VllZZWwrUUV0U2trMjF4SitOQWxSK1lFVll4QzAvNk9iSzJlbVYzcXAv
3D;
laravel_session=eyJpdiI6IkNrdj2hdGdGRJVlB5RFpsSW1KK25hMnc9PSIsInZhbHVlIjoiYkdoVmVVQWDRESVhTQ0RncC9BSkl2UVZnZllTeEwrSllBWUUwS2
3D
```

RESPONSE HEADERS

```
HTTP/1.1 400 Bad Request
Content-Type: text/plain; charset=utf-8
Connection: close
```

INSTANCE

https://jmx.ambiente-de-pruebas-devcts.site/?PHPRC=/dev/fd/0

Identification

PROOF
```
HTTP/2 405
```

OUTPUT

A response has been received with a response code '405' which may require further investigation to verify if this
response is due to an abnormal behavior of the target.

The response has been triggered by an HTTP POST request made on the URL 'https://jmx.ambiente-de-pruebas-devcts.site/?
PHPRC=/dev/fd/0'.

HTTP Info

REQUEST MADE

```
POST /?PHPRC=/dev/fd/0 HTTP/2
```

REQUEST HEADERS

```
Host: jmx.ambiente-de-pruebas-devcts.site
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application
/signed-exchange;v=b3;q=0.7
Accept-Language: en-US,en;q=0.5
Cookie: XSRF-
TOKEN=eyJpdiI6Ijh2NUNrdnE4bnpYbi9kb3dRVVdCWGc9PSIsInZhbHVlIjoiQ3FXODF5Sy94OGhSdGGxMkxkanZPdXJxTU9sU0xBcjF2cXFPVkxMMm9GcE5l
3D;
laravel_session=eyJpdiI6InFTVGd0RkN4L3cxK21IUEtQZTM5UkE9PSIsInZhbHVlIjoiWGZEWWg3T2krbUt0YkdMbTZybnBQY2pRSEl1OFB6OTlDSG9GK1
```

```
3D
Content-Length: 31
Content-Type: application/x-www-form-urlencoded
```

RESPONSE HEADERS
```
HTTP/2 405
allow: GET, HEAD
alt-svc: h3=":443"; ma=2592000
cache-control: no-cache, private
content-encoding: br
content-type: text/html; charset=UTF-8
date: Tue, 17 Jun 2025 17:55:01 GMT
server: swoole-http-server
content-length: 63449
```

INSTANCE

https://jmx.ambiente-de-pruebas-devcts.site/auth/redirect/?
x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=

Identification

PROOF
```
HTTP/2 500
```

OUTPUT
```
A response has been received with a response code '500' which may require further investigation to verify if this
response is due to an abnormal behavior of the target.

The response has been triggered by an HTTP GET request made on the URL 'https://jmx.ambiente-de-pruebas-devcts.site/auth
/redirect/?
x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x
```

HTTP Info

REQUEST MADE
```
GET /auth/redirect/?
x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x=&x
HTTP/2
```

REQUEST HEADERS
```
Host: jmx.ambiente-de-pruebas-devcts.site
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application
/signed-exchange;v=b3;q=0.7
Accept-Language: en-US,en;q=0.5
Cookie: XSRF-
TOKEN=eyJpdiI6InduaWdlMFdSclg2QWRZOHJpamt0V3c9PSIsInZhbVlIIjoiaUR6VllZZWwrUUV0U2trMjF4SitOQWxSK1lFVll4QzAvNk9iSzJ1bVYzcXA
3D;
laravel_session=eyJpdiI6IkNrdjh2dGRJVlB5RFpsSW1KK25hMnc9PSIsInZhbVlIIjoiYkdoVmVQWDRESVhTQ0RncC9BSkl2UVZnZllTeEwrSllBWUUwS
3D
```

RESPONSE HEADERS
```
HTTP/2 500
alt-svc: h3=":443"; ma=2592000
cache-control: no-cache, private
content-encoding: br
content-type: text/html; charset=UTF-8
date: Tue, 17 Jun 2025 17:58:37 GMT
server: swoole-http-server
content-length: 62322
```

Technologies Detected

VULNERABILITY INFO PLUGIN ID 98059

Description

This is an informational plugin to inform the user what technologies the framework has detected on the target application, which can then be examined and checked for known vulnerable software versions

Solution

Only use components that do not have known vulnerabilities, only use components that when combined to not introduce a security vulnerability, and ensure that a misconfiguration does not cause any vulnerabilities

See Also

Plugin Details

PUBLICATION DATE	2017-12-06T00:00:00+00:00
MODIFICATION DATE	2023-11-17T00:00:00+00:00
FAMILY	Web Applications
SEVERITY	Info
PLUGIN ID	98059

Risk Information

CVSSV4 BASE SCORE	-
CVSSV4 VECTOR	-
CVSSV3 BASE SCORE	-
CVSSV3 VECTOR	-
CVSS BASE SCORE	-
CVSS VECTOR	-

Reference Information

CWE	-
WASC	-
OWASP	-
CVE	-
BID	-

Technologies Detected Instances (1)

VULNERABILITY INFO PLUGIN ID 98059

INSTANCE

https://jmx.ambiente-de-pruebas-devcts.site

Identification

OUTPUT

The framework has detected the following technologies in the target application:

- Laravel (version unknown)

Cookies Collected

VULNERABILITY INFO PLUGIN ID 98061

Description

The scanner collected the cookies returned by the application during the scan. The list includes the following information for each cookie:
- Name: name of the cookie
- Value: value of the cookie
- Domain: hosts to which the cookie will be sent
- Path: URL path which must exist in the requested resource before sending the cookie
- Expires: maximum lifetime of the cookie as an HTTP-date timestamp
- Max-Age: number of seconds until the cookie expires
- HttpOnly: cookie is set to be not accessible via JavaScript, XMLHttpRequest and Request APIs
- Secure: cookie will be sent to the server only when a request is made using HTTPS
- SameSite: cookie will be sent along with cross-site request according the defined policy
- URL: first URL discovered which set the cookie in its response
- Set-Method: method used by the application to set the cookie (Set-Cookie or JavaScript)
- Audited: cookie will be audited by plugins during the scan
- Reason Not Audited: reason given for the cookie not being audited during the scan

Solution

-

See Also

https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies

https://en.wikipedia.org/wiki/HTTP_cookie

https://tools.ietf.org/html/rfc6265

Plugin Details

PUBLICATION DATE	2020-09-01T00:00:00+00:00
MODIFICATION DATE	2023-11-17T00:00:00+00:00
FAMILY	Web Applications
SEVERITY	Info
PLUGIN ID	98061

Risk Information

CVSSV4 BASE SCORE	-
CVSSV4 VECTOR	-
CVSSV3 BASE SCORE	-
CVSSV3 VECTOR	-
CVSS BASE SCORE	-
CVSS VECTOR	-

Reference Information

CWE	-
WASC	-
OWASP	-
CVE	-
BID	-

Cookies Collected Instances (1)

VULNERABILITY INFO PLUGIN ID 98061

INSTANCE

https://jmx.ambiente-de-pruebas-devcts.site

Identification

OUTPUT

The following cookies have been collected during the scan of the target:
- 9 cookie(s) specified via Set-Cookie
- 22 cookie(s) set via JavaScript code
The complete list of the cookies is available in attachment.

Target Information

VULNERABILITY INFO PLUGIN ID 98136

Description

Publishes the target information of the starting url as evaluated by the scan.

Solution

-

See Also

Plugin Details

PUBLICATION DATE	2017-07-27T00:00:00+00:00
MODIFICATION DATE	2024-04-26T00:00:00+00:00
FAMILY	General
SEVERITY	Info
PLUGIN ID	98136

Risk Information

CVSSV4 BASE SCORE	-
CVSSV4 VECTOR	-
CVSSV3 BASE SCORE	-
CVSSV3 VECTOR	-
CVSS BASE SCORE	-
CVSS VECTOR	-

Reference Information

CWE	-
WASC	-
OWASP	-
CVE	-
BID	-

Target Information Instances (1)

VULNERABILITY · INFO · PLUGIN ID 98136

INSTANCE

https://jmx.ambiente-de-pruebas-devcts.site

Identification

OUTPUT

```
Access to URL 'https://jmx.ambiente-de-pruebas-devcts.site' has been confirmed.


Target Information
----------------------

Domain Name : jmx.ambiente-de-pruebas-devcts.site
IP Address : 195.35.14.19


Response Information
-------------------------

Status Code : 200
Return Code : ok
Return Message: No error
Response Time : 0.189855s
Response Size : 4721 bytes
Content-Type : text/html; charset=UTF-8
```

HTTP Info

REQUEST MADE

```
GET / HTTP/2
```

REQUEST HEADERS

```
Host: jmx.ambiente-de-pruebas-devcts.site
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application
/signed-exchange;v=b3;q=0.7
Accept-Language: en-US,en;q=0.5
```

RESPONSE HEADERS

```
HTTP/2 200
alt-svc: h3=":443"; ma=2592000
cache-control: no-cache, private
content-encoding: br
content-type: text/html; charset=UTF-8
date: Tue, 17 Jun 2025 17:47:18 GMT
server: swoole-http-server
set-cookie: XSRF-
TOKEN=eyJpdiI6Ilh2eXZZMZndPWnMrditsQ1Zlc2ZDUmc9PSIsInZhbVlIjoiaGRBQk1EeXR2Si85K3JOZVY2VVZMV0E4Yi9OZGgvNEJDMVFJaGVkU2gvQUF
3D; expires=Tue, 17-Jun-2025 19:47:18 GMT; Max-Age=7200; path=/; SameSite=lax
set-cookie:
laravel_session=eyJpdiI6ImprZTBXVmgxY01QWDRCbmlNMEtPdFE9PSIsInZhbVlIjoidWlGem8zNitlbHBBGTzF2OEIxU0JyZ21CSkNVc081T21QRVhIOI
3D; expires=Tue, 17-Jun-2025 19:47:18 GMT; Max-Age=7200; path=/; HttpOnly; SameSite=lax
content-length: 1534
```

Screenshot

VULNERABILITY INFO PLUGIN ID 98138

Description

Screenshot of the target web page, see attached image. This screenshot should show you the target page we are launching the scan against. If the image is not of the intended target page, please check the provided url in the scan configuration.

Solution

-

See Also

Plugin Details

PUBLICATION DATE	2018-01-23T00:00:00+00:00
MODIFICATION DATE	2018-02-14T00:00:00+00:00
FAMILY	General
SEVERITY	Info
PLUGIN ID	98138

Risk Information

CVSSV4 BASE SCORE	-
CVSSV4 VECTOR	-
CVSSV3 BASE SCORE	-
CVSSV3 VECTOR	-
CVSS BASE SCORE	-
CVSS VECTOR	-

Reference Information

CWE	-
WASC	-
OWASP	-
CVE	-
BID	-

Screenshot Instances (1)

VULNERABILITY INFO PLUGIN ID 98138

INSTANCE

https://jmx.ambiente-de-pruebas-devcts.site

Identification

OUTPUT
WAS Scanner has taken a screenshot of the page at url 'https://jmx.ambiente-de-pruebas-devcts.site' with dimensions 1600x1200.

Please see the attachment for the screenshot image.

Form Detected

VULNERABILITY INFO PLUGIN ID 98148

Description

The scanner has detected the presence of a form during the crawling of the target web application. Details about the form are provided in the plugin output.

Solution

-

See Also

Plugin Details

PUBLICATION DATE	2021-10-21T00:00:00+00:00
MODIFICATION DATE	2021-10-21T00:00:00+00:00
FAMILY	Web Applications
SEVERITY	Info
PLUGIN ID	98148

Risk Information

CVSSV4 BASE SCORE	-
CVSSV4 VECTOR	-
CVSSV3 BASE SCORE	-
CVSSV3 VECTOR	-
CVSS BASE SCORE	-
CVSS VECTOR	-

Reference Information

CWE	-
WASC	-
OWASP	-
CVE	-
BID	-

Form Detected Instances (1)

VULNERABILITY INFO PLUGIN ID 98148

INSTANCE	
https://jmx.ambiente-de-pruebas-devcts.site/	

INPUT TYPE	form
INPUT NAME	combined:get::https://jmx.ambiente-de-pruebas-devcts.site/auth/redirect

Identification

OUTPUT

A form with no identifier has been detected on the following URL https://jmx.ambiente-de-pruebas-devcts.site/ with no input fields

This form is submitted by using the following action : https://jmx.ambiente-de-pruebas-devcts.site/auth/redirect

HTTP Info

REQUEST MADE

GET https://jmx.ambiente-de-pruebas-devcts.site/

REQUEST HEADERS

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application
/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
Sec-Ch-Ua: "Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36

RESPONSE HEADERS

HTTP/1.1 200 OK
Alt-Svc: h3=":443"; ma=2592000
Cache-Control: no-cache, private
Content-Encoding: br
Content-Type: text/html; charset=UTF-8
Date: Tue, 17 Jun 2025 17:47:19 GMT
Server: swoole-http-server
Set-Cookie: XSRF-
TOKEN=eyJpdiI6InZsN3Q4MWF1RkNlRngzOUlreEcxWUE9PSIsInZhbHVlIjoiNXRhTVlKakhpbHNsZTNkN2FKdmwxY3dZaGtobkhwWGptOGhRUmllY2lWWF
3D; expires=Tue, 17-Jun-2025 19:47:19 GMT; Max-Age=7200; path=/; SameSite=lax
laravel_session=eyJpdiI6ImxaY0g0K0lhUjhWYzdwVExhbHpiQmc9PSIsInZhbHVlIjoibGNQZlM2TWZvYVhzaFhmeVJVNnFYYUhPazVxdS9MMmdlK0k0WI
3D; expires=Tue, 17-Jun-2025 19:47:19 GMT; Max-Age=7200; path=/; HttpOnly; SameSite=lax
Content-Length: 4463

External URLs

VULNERABILITY INFO PLUGIN ID 98154

Description

An external URL is an URL for which the Fully Qualified Domain Name (FQDN) is not the same as the web target URL one. The scanner detected the presence of external URLs on the target web application and have listed them based on two types : URLs with a domain name in common with the web target URL and all the other external URLs.

Solution

-

See Also

Plugin Details

PUBLICATION DATE	2022-11-30T00:00:00+00:00
MODIFICATION DATE	2022-12-12T00:00:00+00:00
FAMILY	General
SEVERITY	Info
PLUGIN ID	98154

Risk Information

CVSSV4 BASE SCORE	-
CVSSV4 VECTOR	-
CVSSV3 BASE SCORE	-
CVSSV3 VECTOR	-
CVSS BASE SCORE	-
CVSS VECTOR	-

Reference Information

CWE	-
WASC	-
OWASP	-
CVE	-
BID	-

External URLs Instances (1)

VULNERABILITY INFO PLUGIN ID 98154

INSTANCE

https://jmx.ambiente-de-pruebas-devcts.site

Identification

OUTPUT

The scanner detected the presence of 5 URLs on the target application:

- 0 URLs which use a hostname related to the target hostname
- 5 URLs which use a third party hostname

The list of the detected URLs is provided in attachment.

Missing Permissions Policy

VULNERABILITY INFO PLUGIN ID 98526

Description

Permissions Policy provides mechanisms to websites to restrict the use of browser features in its own frame and in iframes that it embeds.

Solution

Configure Permissions Policy on your website by adding 'Permissions-Policy' HTTP header.

See Also

https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Feature-Policy
https://scotthelme.co.uk/goodbye-feature-policy-and-hello-permissions-policy/

Plugin Details

PUBLICATION DATE	2019-03-27T00:00:00+00:00
MODIFICATION DATE	2024-03-25T00:00:00+00:00
FAMILY	HTTP Security Header
SEVERITY	Info
PLUGIN ID	98526

Risk Information

CVSSV4 BASE SCORE	-
CVSSV4 VECTOR	-
CVSSV3 BASE SCORE	-
CVSSV3 VECTOR	-
CVSS BASE SCORE	-
CVSS VECTOR	-

Reference Information

CWE	-
WASC	-
OWASP	-
CVE	-
BID	-

Missing Permissions Policy Instances (2)

VULNERABILITY INFO PLUGIN ID 98526

INSTANCE

https://jmx.ambiente-de-pruebas-devcts.site/img/paisajes.mp4

Identification

OUTPUT

No Permissions-Policy headers were found on https://jmx.ambiente-de-pruebas-devcts.site/img/paisajes.mp4

HTTP Info

REQUEST MADE

GET https://jmx.ambiente-de-pruebas-devcts.site/img/paisajes.mp4

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: identity;q=1, *;q=0
Cookie: XSRF-
TOKEN=eyJpdiI6InovclBzTkU2VG51UEF5a3U5MFFlU0E9PSIsInZhbVlIjoiRUUvWWhNY2FNRVJJRHRBcFFWRjVSZHkzYjJ4WFN1ZkxjaCtTE80UDBPZTkl
3D;
laravel_session=eyJpdiI6IjZKZXBiTGVCQlorSmppczZDZk9KVmc9PSIsInZhbVlIjoid1FUVFZYZDl2TkFISVUxaXBnbUNOalNSNWlMVWtBYXJjVzNMa 
3D
Priority: i
Range: bytes=0-
Referer: https://jmx.ambiente-de-pruebas-devcts.site/img/paisajes.mp4
Sec-Ch-Ua: "Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Sec-Fetch-Dest: video
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
H3 200
Content-Type: video/mp4
Date: Tue, 17 Jun 2025 17:59:38 GMT
Server: swoole-http-server
Content-Length: 30616863
```

INSTANCE

https://jmx.ambiente-de-pruebas-devcts.site/

Identification

OUTPUT

No Permissions-Policy headers were found on https://jmx.ambiente-de-pruebas-devcts.site/

HTTP Info

REQUEST MADE

GET https://jmx.ambiente-de-pruebas-devcts.site/

REQUEST HEADERS

```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application
/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
Sec-Ch-Ua: "Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS
```
HTTP/1.1 200 OK
Alt-Svc: h3=":443"; ma=2592000
Cache-Control: no-cache, private
Content-Encoding: br
Content-Type: text/html; charset=UTF-8
Date: Tue, 17 Jun 2025 17:47:19 GMT
Server: swoole-http-server
Set-Cookie: XSRF-
TOKEN=eyJpdiI6InZsN3Q4MWFlRkNlRngzOUlreEcxWUE9PSIsInZhbHVlIjoiNXRhTVlKakhpbHNsZTNkN2FKdmwxY3dZaGtobkhwWGptOGhRUm1lY2Z1WWFI
3D; expires=Tue, 17-Jun-2025 19:47:19 GMT; Max-Age=7200; path=/; SameSite=lax
laravel_session=eyJpdiI6ImxaY0g0K0lhUjhWYzdwVExhbHpiQmc9PSIsInZhbHVlIjoibGNQZlM2TWZvYVhzaFhmeVJVNnFYYUhPazVxdS9MMmdlK0k0WI
3D; expires=Tue, 17-Jun-2025 19:47:19 GMT; Max-Age=7200; path=/; HttpOnly; SameSite=lax
Content-Length: 4463
```

Missing Referrer Policy

VULNERABILITY INFO PLUGIN ID 98527

Description

Referrer Policy provides mechanisms to websites to restrict referrer information (sent in the referer header) that browsers will be allowed to add.

No Referrer Policy header or metatag configuration has been detected.

Solution

Configure Referrer Policy on your website by adding 'Referrer-Policy' HTTP header or meta tag referrer in HTML.

See Also

https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy

Plugin Details

PUBLICATION DATE	2019-04-02T00:00:00+00:00
MODIFICATION DATE	2024-03-25T00:00:00+00:00
FAMILY	HTTP Security Header
SEVERITY	Info
PLUGIN ID	98527

Risk Information

CVSSV4 BASE SCORE	-
CVSSV4 VECTOR	-
CVSSV3 BASE SCORE	-
CVSSV3 VECTOR	-
CVSS BASE SCORE	-
CVSS VECTOR	-

Reference Information

CWE	-
WASC	-
OWASP	-
CVE	-
BID	-

Missing Referrer Policy Instances (2)

VULNERABILITY INFO PLUGIN ID 98527

INSTANCE

https://jmx.ambiente-de-pruebas-devcts.site/img/paisajes.mp4

Identification

OUTPUT

No Referrer-Policy headers or body meta tags were found on https://jmx.ambiente-de-pruebas-devcts.site/img/paisajes.mp4

HTTP Info

REQUEST MADE

GET https://jmx.ambiente-de-pruebas-devcts.site/img/paisajes.mp4

REQUEST HEADERS

```
Accept: */*
Accept-Encoding: identity;q=1, *;q=0
Cookie: XSRF-
TOKEN=eyJpdiI6InovclBzTkU2VG51UEF5a3U5MFFlU0E9PSIsInZhbVlIjoiRUUvWWhNY2FNRVJJRHRBcFFWRjVSZHkzYjJ4WFN1ZkxjjaCtkTE80UDBPZTkl3D;
3D;
laravel_session=eyJpdiI6IjZKZXBiTGVCQlorSmppczZDZk9KVmc9PSIsInZhbVlIjoid1FUVFZYZDl2TkFlSVUxaXBnbUNOalNNWlMVWtBYXJjjVzNMaI
3D
Priority: i
Range: bytes=0-
Referer: https://jmx.ambiente-de-pruebas-devcts.site/img/paisajes.mp4
Sec-Ch-Ua: "Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Sec-Fetch-Dest: video
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
H3 200
Content-Type: video/mp4
Date: Tue, 17 Jun 2025 17:59:38 GMT
Server: swoole-http-server
Content-Length: 30616863
```

INSTANCE

https://jmx.ambiente-de-pruebas-devcts.site/

Identification

OUTPUT

No Referrer-Policy headers or body meta tags were found on https://jmx.ambiente-de-pruebas-devcts.site/

HTTP Info

REQUEST MADE

GET https://jmx.ambiente-de-pruebas-devcts.site/

REQUEST HEADERS

```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application
/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
Sec-Ch-Ua: "Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
```

RESPONSE HEADERS

```
HTTP/1.1 200 OK
Alt-Svc: h3=":443"; ma=2592000
Cache-Control: no-cache, private
Content-Encoding: br
Content-Type: text/html; charset=UTF-8
Date: Tue, 17 Jun 2025 17:47:19 GMT
Server: swoole-http-server
Set-Cookie: XSRF-
TOKEN=eyJpdiI6InZsN3Q4MWFlRkNlRngzOUlreEcxWUE9PSIsInZhbHVlIjoiNXRhTVlKakhpbHNsZTNkN2FKdmwxY3dZaGtobkhwWGptOGhRUm1lY2Z1WWFI
3D; expires=Tue, 17-Jun-2025 19:47:19 GMT; Max-Age=7200; path=/; SameSite=lax
laravel_session=eyJpdiI6ImxaY0g0K0lhUjhWYzdwVExhbHpiQmc9PSIsInZhbHVlIjoibGNQZlM2TWZvYVhzaFhmeVJVNnFYYUhPazVxdS9MMmdlK0k0WI
3D; expires=Tue, 17-Jun-2025 19:47:19 GMT; Max-Age=7200; path=/; HttpOnly; SameSite=lax
Content-Length: 4463
```

Missing Subresource Integrity

VULNERABILITY INFO PLUGIN ID 98647

Description

Subresource Integrity (SRI) is a web security standard that enables browsers to verify that resources hosted by third parties (CDN for example) are delivered without unexpected manipulation.

SRI works by comparing a cryptographic hash declared in the integrity attribute of the resource tag (like script or link) used to fetch the resource and the calculated hash value of this resource.

No SRI have been detected for one or more resources.

Solution

Add a integrity attribute to the resource tag with prefixed and base64 encoded hash of the resource.

See Also

https://developer.mozilla.org/en-US/docs/Web/Security/Subresource_Integrity
https://www.owasp.org/index.php/3rd_Party_Javascript_Management_Cheat_Sheet#Subresource_Integrity

Plugin Details

PUBLICATION DATE	2019-08-01T00:00:00+00:00
MODIFICATION DATE	2023-01-17T00:00:00+00:00
FAMILY	Web Applications
SEVERITY	Info
PLUGIN ID	98647

Risk Information

CVSSV4 BASE SCORE	-
CVSSV4 VECTOR	-
CVSSV3 BASE SCORE	-
CVSSV3 VECTOR	-
CVSS BASE SCORE	-
CVSS VECTOR	-

Reference Information

CWE	-
WASC	-
OWASP	-
CVE	-
BID	-

Missing Subresource Integrity Instances (1)

VULNERABILITY INFO PLUGIN ID 98647

INSTANCE

https://jmx.ambiente-de-pruebas-devcts.site

Identification

OUTPUT

The scanner detected 2 resources without subresource integrity defined :
- 1 URLs related to 'script' resources
- 1 URLs related to 'link' resources

The list of all the detected resources is provided in attachment.

Fetch/XHR Detected

VULNERABILITY INFO PLUGIN ID 98772

Description

The scan detected that the web application makes requests that appear to be using Fetch or XMLHTTPRequests (XHRs) to communicate with a backend API server. Fetchs/XHRs allow retrieval of data from an API without triggering a page reload, making them especially useful for Single Page Applications.

Solution

-

See Also

https://developer.mozilla.org/en-US/docs/Web/API/XMLHttpRequest

Plugin Details

PUBLICATION DATE	2019-11-14T00:00:00+00:00
MODIFICATION DATE	2023-11-17T00:00:00+00:00
FAMILY	General
SEVERITY	Info
PLUGIN ID	98772

Risk Information

CVSSV4 BASE SCORE	-
CVSSV4 VECTOR	-
CVSSV3 BASE SCORE	-
CVSSV3 VECTOR	-
CVSS BASE SCORE	-
CVSS VECTOR	-

Reference Information

CWE	-
WASC	-
OWASP	-
CVE	-
BID	-

Fetch/XHR Detected Instances (1)

VULNERABILITY INFO PLUGIN ID 98772

INSTANCE

https://jmx.ambiente-de-pruebas-devcts.site

Identification

OUTPUT

The scan detected 5 unique XMLHttpRequests. Here is the distribution of MIME types used by the detected requests:

- 5 as "application/json"

SSL/TLS Certificate Information

VULNERABILITY INFO PLUGIN ID 112491

Description

This plugin displays information about the X.509 certificate extracted from the HTTPS connection.

Solution

-

See Also

Plugin Details

PUBLICATION DATE	2018-10-03T00:00:00+00:00
MODIFICATION DATE	2023-05-05T00:00:00+00:00
FAMILY	SSL/TLS
SEVERITY	Info
PLUGIN ID	112491

Risk Information

CVSSV4 BASE SCORE	-
CVSSV4 VECTOR	-
CVSSV3 BASE SCORE	-
CVSSV3 VECTOR	-
CVSS BASE SCORE	-
CVSS VECTOR	-

Reference Information

CWE	-
WASC	-
OWASP	-
CVE	-
BID	-

SSL/TLS Certificate Information Instances (1)

VULNERABILITY INFO PLUGIN ID 112491

INSTANCE

https://jmx.ambiente-de-pruebas-devcts.site/

Identification

OUTPUT

```
Certificate 1
-------------
Common Name: jmx.ambiente-de-pruebas-devcts.site
Alternative Names: jmx.ambiente-de-pruebas-devcts.site
Issuer: Let's Encrypt
Valid from: 2025-05-14 02:36:21 UTC
Valid until: 2025-08-12 02:36:20 UTC (expires in 1 month, 3 weeks, 3 days)
Validity Period: 89 days
Key: RSA 4096-bit
Signature: sha256WithRSAEncryption

Certificate 2
-------------
Common Name: r10
Issuer: Internet Security Research Group
Valid from: 2024-03-13 00:00:00 UTC
Valid until: 2027-03-12 23:59:59 UTC (expires in 1 year, 8 months, 3 weeks, 3 days)
Validity Period: 1094 days
Key: RSA 2048-bit
Signature: sha256WithRSAEncryption
```

SSL/TLS Versions Supported

VULNERABILITY INFO PLUGIN ID 112530

Description

This plugin displays information about the SSL/TLS versions supported by remote server for HTTPS connection.

Solution

-

See Also

https://www.iana.org/assignments/tls-parameters/tls-parameters.xhtml

Plugin Details

PUBLICATION DATE	2018-10-03T00:00:00+00:00
MODIFICATION DATE	2020-10-02T00:00:00+00:00
FAMILY	SSL/TLS
SEVERITY	Info
PLUGIN ID	112530

Risk Information

CVSSV4 BASE SCORE	-
CVSSV4 VECTOR	-
CVSSV3 BASE SCORE	-
CVSSV3 VECTOR	-
CVSS BASE SCORE	-
CVSS VECTOR	-

Reference Information

CWE	-
WASC	-
OWASP	-
CVE	-
BID	-

SSL/TLS Versions Supported Instances (1)

VULNERABILITY INFO PLUGIN ID 112530

INSTANCE

https://jmx.ambiente-de-pruebas-devcts.site/

Identification

OUTPUT

```
Protocol Supported
--------------------
SSL 2.0 No
SSL 3.0 No
TLS 1.0 No
TLS 1.1 No
TLS 1.2 Yes
TLS 1.3 Yes
```

SSL/TLS Server Cipher Suite Preference

VULNERABILITY INFO PLUGIN ID 112598

Description

The remote server is configured with a SSL/TLS cipher suite preference list used to determine the cipher suite during the negotiation with the client.

Solution

-

See Also

http://www.exploresecurity.com/testing-for-cipher-suite-preference/

https://wiki.mozilla.org/Security/Server_Side_TLS

Plugin Details

PUBLICATION DATE	2020-09-24T00:00:00+00:00
MODIFICATION DATE	2020-09-24T00:00:00+00:00
FAMILY	SSL/TLS
SEVERITY	Info
PLUGIN ID	112598

Risk Information

CVSSV4 BASE SCORE	-
CVSSV4 VECTOR	-
CVSSV3 BASE SCORE	-
CVSSV3 VECTOR	-
CVSS BASE SCORE	-
CVSS VECTOR	-

Reference Information

CWE	-
WASC	-
OWASP	-
CVE	-
BID	-

SSL/TLS Server Cipher Suite Preference Instances (1)

VULNERABILITY INFO PLUGIN ID 112598

INSTANCE

https://jmx.ambiente-de-pruebas-devcts.site/

Identification

OUTPUT

```
The scanner detected that the remote host is configured with cipher suite preference on the following protocol(s):

TLS v1.3
-------
TLS_AES_128_GCM_SHA256
TLS_AES_256_GCM_SHA384

TLS v1.2
-------
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
```

Allowed HTTP Versions

VULNERABILITY INFO PLUGIN ID 112613

Description

The Hypertext Transfer Protocol (HTTP) is the underlying protocol of the World Wide Web. Since its first release, HTTP has evolved to support modern web usages and currently exists in three versions:
- HTTP/1.0
- HTTP/1.1
- HTTP/2

The scanner identified the supported versions of the HTTP protocol on the target web application.

Solution

-

See Also

https://developer.mozilla.org/en-US/docs/Web/HTTP/Basics_of_HTTP/Evolution_of_HTTP

Plugin Details

PUBLICATION DATE	2020-10-13T00:00:00+00:00
MODIFICATION DATE	2023-01-17T00:00:00+00:00
FAMILY	Web Applications
SEVERITY	Info
PLUGIN ID	112613

Risk Information

CVSSV4 BASE SCORE	-
CVSSV4 VECTOR	-
CVSSV3 BASE SCORE	-
CVSSV3 VECTOR	-
CVSS BASE SCORE	-
CVSS VECTOR	-

Reference Information

CWE	-
WASC	-
OWASP	-
CVE	-
BID	-

Allowed HTTP Versions Instances (1)

VULNERABILITY INFO PLUGIN ID 112613

INSTANCE

https://jmx.ambiente-de-pruebas-devcts.site

Identification

OUTPUT

The scanner detected the following HTTP versions on the target application :

- HTTP/1.0
- HTTP/1.1
- HTTP/2

The list of requests and responses observed is provided in attachment.

API Detected

VULNERABILITY INFO PLUGIN ID 112616

Description

The scan detected that some XHR requests seem to call an API. The scanner generated an OpenAPI file based on the observed requests and attached it to the plugin output. This OpenAPI file can then be used to run a scan against the API with WAS API Scanning.

Solution

-

See Also

Plugin Details

PUBLICATION DATE	2020-10-21T00:00:00+00:00
MODIFICATION DATE	2020-10-21T00:00:00+00:00
FAMILY	General
SEVERITY	Info
PLUGIN ID	112616

Risk Information

CVSSV4 BASE SCORE	-
CVSSV4 VECTOR	-
CVSSV3 BASE SCORE	-
CVSSV3 VECTOR	-
CVSS BASE SCORE	-
CVSS VECTOR	-

Reference Information

CWE	-
WASC	-
OWASP	-
CVE	-
BID	-

API Detected Instances (1)

VULNERABILITY INFO PLUGIN ID 112616

INSTANCE

https://jmx.ambiente-de-pruebas-devcts.site

Identification

OUTPUT

```
API endpoints have been detected for the following host(s):
- https://login.microsoftonline.com
- https://browser.events.data.microsoft.com
```

Security.txt File Not Detected

VULNERABILITY INFO PLUGIN ID 112723

Description

A Security.txt file has not been detected on the target.

When security risks in web services are discovered by independent security researchers, this file defines the channels to disclose them properly & enables 3rd party researchers to disclose issues securely in a manner defined by the organization.

Organizations should consider creating a security.txt file containing contact and other information in the defined format and place it under the .well-known directory of the server.

Solution

-

See Also

https://securitytxt.org/
https://tools.ietf.org/html/draft-foudil-securitytxt-11

Plugin Details

PUBLICATION DATE	2021-03-17T00:00:00+00:00
MODIFICATION DATE	2021-03-17T00:00:00+00:00
FAMILY	Web Servers
SEVERITY	Info
PLUGIN ID	112723

Risk Information

CVSSV4 BASE SCORE	-
CVSSV4 VECTOR	-
CVSSV3 BASE SCORE	-
CVSSV3 VECTOR	-
CVSS BASE SCORE	-
CVSS VECTOR	-

Reference Information

CWE	-
WASC	-
OWASP	-
CVE	-
BID	-

Security.txt File Not Detected Instances (1)

VULNERABILITY INFO PLUGIN ID 112723

INSTANCE

https://jmx.ambiente-de-pruebas-devcts.site/.well-known/security.txt

Identification

OUTPUT

No or a malformed security.txt was found at 'https://jmx.ambiente-de-pruebas-devcts.site/.well-known/security.txt'.

HTTP Info

REQUEST MADE

GET /.well-known/security.txt HTTP/2

REQUEST HEADERS

Host: jmx.ambiente-de-pruebas-devcts.site
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application
/signed-exchange;v=b3;q=0.7
Accept-Language: en-US,en;q=0.5
Cookie: XSRF-
TOKEN=eyJpdiI6Ijh2NUNrdnE4bnpYbi9kb3dRVVddCWGc9PSIsInZhbHVlIjoiQ3FXODF5Sy94OGhSdGxKMkxkanZPdXJxTU9sU0xBcjF2cXFPVkkxMMm9GcE51
3D;
laravel_session=eyJpdiI6InFTVGd0RkN4L3cxK21IUEtQZTM5UkE9PSIsInZhbHVlIjoiWGZEWWg3T2krbUt0YkdMbTZybnBQY2pRSEl1OFB6OTlDSG9G
3D

RESPONSE HEADERS

HTTP/2 404
alt-svc: h3=":443"; ma=2592000
cache-control: no-cache, private
content-encoding: br
content-type: text/html; charset=UTF-8
date: Tue, 17 Jun 2025 17:55:00 GMT
server: swoole-http-server
content-length: 2379

Performance Telemetry

VULNERABILITY INFO PLUGIN ID 113393

Description

This finding provides information to assist in scan performance tuning.

Solution

-

See Also

Plugin Details

PUBLICATION DATE	2022-10-17T00:00:00+00:00
MODIFICATION DATE	2024-10-03T00:00:00+00:00
FAMILY	General
SEVERITY	Info
PLUGIN ID	113393

Risk Information

CVSSV4 BASE SCORE	-
CVSSV4 VECTOR	-
CVSSV3 BASE SCORE	-
CVSSV3 VECTOR	-
CVSS BASE SCORE	-
CVSS VECTOR	-

Reference Information

CWE	-
WASC	-
OWASP	-
CVE	-
BID	-

Performance Telemetry Instances (1)

VULNERABILITY INFO PLUGIN ID 113393

INSTANCE

https://jmx.ambiente-de-pruebas-devcts.site

Identification

OUTPUT

Three attachments are included in this finding to assist in performance tuning of your scan:
-pages_telemetry.csv: Scan statistics organized by page
-plugins_telemetry.csv: Scan statistics organized by plugin
-time_telemetry.csv: Chronological scan statistics

HTML Comments Detected

VULNERABILITY INFO PLUGIN ID 113897

Description

HTML comments are often used by developers to include information related to the application inline, which are ignored by a clients browser during rendering. These comments may include sensitive information such as SQL queries, credentials or internal IP for example.

Solution

Review the HTML comments identified on the page for any information leakage, and remove any sensitive information identified.

See Also

https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/05-Review_Webpage_Content_for_Information_Leakage

Plugin Details

PUBLICATION DATE	2023-06-09T00:00:00+00:00
MODIFICATION DATE	2024-11-08T00:00:00+00:00
FAMILY	Data Exposure
SEVERITY	Info
PLUGIN ID	113897

Risk Information

CVSSV4 BASE SCORE	-
CVSSV4 VECTOR	-
CVSSV3 BASE SCORE	-
CVSSV3 VECTOR	-
CVSS BASE SCORE	-
CVSS VECTOR	-

Reference Information

CWE	-
WASC	-
OWASP	-
CVE	-
BID	-

HTML Comments Detected Instances (1)

VULNERABILITY INFO PLUGIN ID 113897

INSTANCE

https://jmx.ambiente-de-pruebas-devcts.site/

Identification

OUTPUT

2 HTML comments have been detected in the application HTTP response. Please see the attachment for further details.

HTTP Info

REQUEST MADE

GET https://jmx.ambiente-de-pruebas-devcts.site/

REQUEST HEADERS

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application
/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
Sec-Ch-Ua: "Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36

RESPONSE HEADERS

HTTP/1.1 200 OK
Alt-Svc: h3=":443"; ma=2592000
Cache-Control: no-cache, private
Content-Encoding: br
Content-Type: text/html; charset=UTF-8
Date: Tue, 17 Jun 2025 17:47:19 GMT
Server: swoole-http-server
Set-Cookie: XSRF-
TOKEN=eyJpdiI6InZsN3Q4MWF1RkNlRngzOUlreEcxWUE9PSIsInZhbHVlIjoiNXRhTVlKakhpbHNsZTNkN2FKdmwxY3dZaGtobkhwWGptOGhRUm1lY2Z1WWFI
3D; expires=Tue, 17-Jun-2025 19:47:19 GMT; Max-Age=7200; path=/; SameSite=lax
laravel_session=eyJpdiI6ImxaY0g0K0lhUjhWYzdwVExhbHpiQmc9PSIsInZhbHVlIjoibGNQZlM2TWZvYVhzaFhmeVJVNnFYYUhPazVxdS9MMmdlK0k0WI
3D; expires=Tue, 17-Jun-2025 19:47:19 GMT; Max-Age=7200; path=/; HttpOnly; SameSite=lax
Content-Length: 4463

Path Relative Stylesheet Import

VULNERABILITY INFO PLUGIN ID 114466

Description

A Path Relative Style Sheet Import occurs when the application imports a style sheet via a relative URL and uses user input in the file name. This vulnerability mainly affects older browsers such as Internet Explorer and allows an attacker to exploit the way the browser handles stylesheet imports in order to perform CSS Injection.

Solution

It is preferable not to use path-related URLs in stylesheet imports, and also to use the 'X-Content-Type-Options: nosnif' and 'X-Frame-Options: deny' headers.

See Also

https://csplite.com/csp290/

Plugin Details

PUBLICATION DATE	2024-10-30T00:00:00+00:00
MODIFICATION DATE	2024-11-08T00:00:00+00:00
FAMILY	Injection
SEVERITY	Info
PLUGIN ID	114466

Risk Information

CVSSV4 BASE SCORE	-
CVSSV4 VECTOR	-
CVSSV3 BASE SCORE	-
CVSSV3 VECTOR	-
CVSS BASE SCORE	-
CVSS VECTOR	-

Reference Information

CWE	-
WASC	-
OWASP	-
CVE	-
BID	-

Path Relative Stylesheet Import Instances (1)

VULNERABILITY INFO PLUGIN ID 114466

INSTANCE

https://jmx.ambiente-de-pruebas-devcts.site/

Identification

PROOF
The following value is extracted from a <link> tag that imports a style sheet with a 'href' that does not begin with a
/ :
* https://cdnjs.cloudflare.com/ajax/libs/flowbite/2.3.0/flowbite.min.css

OUTPUT
The scanner was able to detect a Path Relative Stylesheet Import.

HTTP Info

REQUEST MADE
GET https://jmx.ambiente-de-pruebas-devcts.site/

REQUEST HEADERS
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application
/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
Sec-Ch-Ua: "Chromium";v="124", "HeadlessChrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.207 Safari/537.36

RESPONSE HEADERS
HTTP/1.1 200 OK
Alt-Svc: h3=":443"; ma=2592000
Cache-Control: no-cache, private
Content-Encoding: br
Content-Type: text/html; charset=UTF-8
Date: Tue, 17 Jun 2025 17:47:19 GMT
Server: swoole-http-server
Set-Cookie: XSRF-
TOKEN=eyJpdiI6InZsN3Q4MWF1RkNlRngzOUlreEcxWUE9PSIsInZhbHVlIjoiNXRhTVlKakhpbHNsZTNkN2FKdmwxY3dZaGtobkhwWGptOGhRUm1lY2ZlWWFJ
3D; expires=Tue, 17-Jun-2025 19:47:19 GMT; Max-Age=7200; path=/; SameSite=lax
laravel_session=eyJpdiI6ImxaY0g0K0lhUjhWYzdwVExhbHpiQmc9PSIsInZhbHVlIjoibGNQZlM2TWZvYVhzaFhmeVJVNnFYYUhPazVxdS9MMMmdlK0k0Wl
3D; expires=Tue, 17-Jun-2025 19:47:19 GMT; Max-Age=7200; path=/; HttpOnly; SameSite=lax
Content-Length: 4463

SSL/TLS Cipher Suites Supported

VULNERABILITY INFO PLUGIN ID 115491

Description

This plugin displays supported SSL/TLS cipher suites.

Solution

-

See Also

https://www.iana.org/assignments/tls-parameters/tls-parameters.xhtml

Plugin Details

PUBLICATION DATE	2019-01-09T00:00:00+00:00
MODIFICATION DATE	2022-10-07T00:00:00+00:00
FAMILY	SSL/TLS
SEVERITY	Info
PLUGIN ID	115491

Risk Information

CVSSV4 BASE SCORE	-
CVSSV4 VECTOR	-
CVSSV3 BASE SCORE	-
CVSSV3 VECTOR	-
CVSS BASE SCORE	-
CVSS VECTOR	-

Reference Information

CWE	-
WASC	-
OWASP	-
CVE	-
BID	-

SSL/TLS Cipher Suites Supported Instances (1)

VULNERABILITY INFO PLUGIN ID 115491

INSTANCE

https://jmx.ambiente-de-pruebas-devcts.site/

Identification

OUTPUT

```
Protocol Cipher Suite Name (RFC) Key Exchange Strength
----------------------------------------------------------------------
TLS1.3 TLS_AES_128_GCM_SHA256 x25519 256
TLS1.3 TLS_AES_256_GCM_SHA384 x25519 256
TLS1.3 TLS_CHACHA20_POLY1305_SHA256 x25519 256
TLS1.2 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 x25519 256
TLS1.2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 x25519 256
TLS1.2 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA x25519 256
TLS1.2 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA x25519 256
```