



Acunetix Threat Level 2

One or more medium-severity type vulnerabilities have been discovered by the scanner. You should investigate each of these vulnerabilities to ensure they will not escalate to more severe problems.

Scan Detail

Target	http://172.26.99.119:8000/
Scan Type	Full Scan
Start Time	Feb 10, 2023, 10:50:54 AM GMT+5
Scan Duration	5 hours, 12 minutes
Requests	22252
Average Response Time	4ms
Maximum Response Time	29935ms



High







Medium



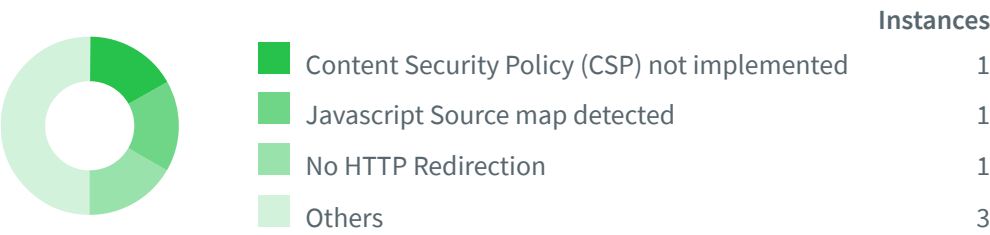
Low



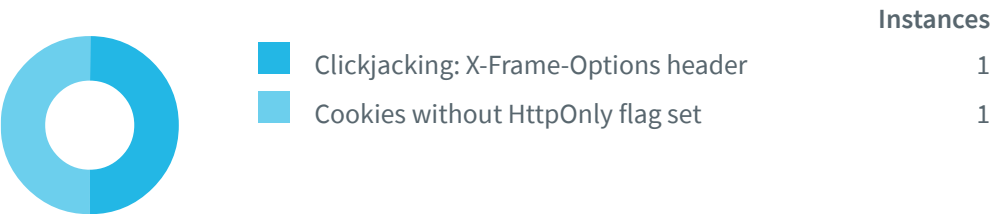
Informational

Severity	Vulnerabilities	Instances
 High	0	0
 Medium	3	4
 Low	2	2
 Informational	6	6
Total	11	12

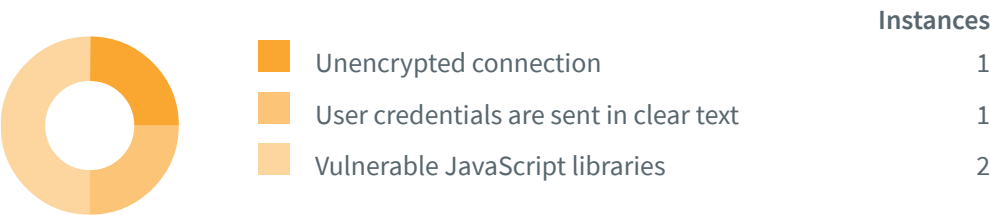
Informational














Low Severity



Medium Severity



Impacts

SEVERITY	IMPACT	
 Medium	1	Unencrypted connection
 Medium	1	User credentials are sent in clear text
 Medium	2	Vulnerable JavaScript libraries
 Low	1	Clickjacking: X-Frame-Options header
 Low	1	Cookies without HttpOnly flag set
 Informational	1	Content Security Policy (CSP) not implemented
 Informational	1	Javascript Source map detected
 Informational	1	No HTTP Redirection
 Informational	1	Outdated JavaScript libraries
 Informational	1	Permissions-Policy header not implemented
 Informational	1	PHP Version Disclosure

Unencrypted connection

This scan target was connected to over an unencrypted connection. A potential attacker can intercept and modify data sent and received from this site.

Impact

Possible information disclosure.

<http://172.26.99.119:8000/>

Verified

Request

```
GET /css/Main.css HTTP/1.1
Host: 172.26.99.119:8000
Pragma: no-cache
Cache-Control: no-cache
accept: text/css,*/*;q=0.1
accept-language: en-US
cookie: XSRF-
TOKEN=eyJpdiI6InV2MW4rVkJzZjFZN3VPdFd6bzJIWVE9PSIsInZhbnVlIjoiWk5TRl10SzQ5Tm5KbHM3VVhoYWNIdXZ3Q1RkdW
tWczdnWXhLZl1VJUXBkclJzK1h3Y1JPZWZ1Sm5EU2ZmaVBjL0FBYzd0VzlmQjh0ZkxRc3gvd2pyNVhjeXB6MzZwc0JralVXeWlCS3
NHV1dhZE1ta054UVpGeHZ0bXdESkpsQmMiLCJtYWMiOiI0YjczMTg4MWJkYmYwNWRIZjRhNzE1MWQwMWI3YmYwOTZlNGVlZjQwZG
FhODc2NzZlNGJlZjZjNTdjMjI2Zjg0IiwidGFuIjoiIn0%3D;
laravel_session=eyJpdiI6IndTTjV3MDNrS2t2UUtSSytLTHVEVVE9PSIsInZhbnVlIjoiVWVlclhZWjhV0lCaTgvNmtzRWVl
a0N0Y0xUU1BEaHE0N2QybnlvV1NWTHlkYkMvbG1ZSDJlZjZStpcFFVZlVXaFhjWGloeUxWYVNXTjNzMm5Sc2FZVFdXckl4NHBO
YStpdVVMQTNUY3BLZXVMZWxGMGZBMlFoYUE3TnZoejYiLCJtYWMiOiJhMTA5MWRjNjZhMzY3NmYwN2QzNjQwOGZhOGI3MWRkMDA4
YzYyY2ZjNDVhNmQlNzdzYzI1MDQ1MWVhMWQ1MWViIiwidGFuIjoiIn0%3D
Referer: http://172.26.99.119:8000/
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/108.0.0.0 Safari/537.36
```

Recommendation

The site should send and receive data over a secure (HTTPS) connection.

User credentials are sent in clear text

User credentials are transmitted over an unencrypted channel. This information should always be transferred via an encrypted channel (HTTPS) to avoid being intercepted by malicious users.

Impact

A third party may be able to read the user credentials by intercepting an unencrypted HTTP connection.

<http://172.26.99.119:8000/>

Forms with credentials sent in clear text:

- <http://172.26.99.119:8000/>

```
Form name: <empty>
Form action: login
Form method: POST
Password input: password
```

- <http://172.26.99.119:8000/index.php>

```
Form name: <empty>
Form action: login
Form method: POST
Password input: password
```

Request

```
GET / HTTP/1.1
Host: 172.26.99.119:8000
Pragma: no-cache
Cache-Control: no-cache
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=0.9
accept-language: en-US
upgrade-insecure-requests: 1
Accept-Encoding: gzip,deflate,br
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/108.0.0.0 Safari/537.36
```

Recommendation

Because user credentials are considered sensitive information, should always be transferred to the server over an encrypted connection (HTTPS).

Vulnerable JavaScript libraries

You are using one or more vulnerable JavaScript libraries. One or more vulnerabilities were reported for this version of the library. Consult Attack details and Web References for more information about the affected library and the vulnerabilities that were reported.

Impact

Consult References for more information.

<http://172.26.99.119:8000/>

Confidence: 95%

- **jQuery 3.1.1**
 - URL: <http://172.26.99.119:8000/login>
 - Detection method: The library's name and version were determined based on its dynamic behavior.
 - CVE-ID: CVE-2020-11022, CVE-2020-11023, CVE-2019-11358
 - Description: In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. `.html()`, `.append()`, and others) may execute untrusted code. This problem is patched in jQuery 3.5.0. / In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing option elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. `.html()`, `.append()`, and others) may execute untrusted code. This problem is patched in jQuery 3.5.0. / jQuery mishandles `jQuery.extend(true, {}, ...)` because of Object.prototype pollution. If an unsanitized source object contained an enumerable `__proto__` property, it could extend the native Object.prototype.
 - References:
 - <https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/>
 - <https://mksben.l0.cm/2020/05/jquery3.5.0-xss.html>
 - <https://jquery.com/upgrade-guide/3.5/>
 - <https://api.jquery.com/jQuery.htmlPrefilter/>
 - <https://www.cvedetails.com/cve/CVE-2020-11022/>
 - <https://github.com/advisories/GHSA-gxr4-xjj5-5px2>
 - <https://www.cvedetails.com/cve/CVE-2020-11023/>
 - <https://github.com/advisories/GHSA-jpcq-cgw6-v4j6>
 - <https://github.com/jquery/jquery/pull/4333>
 - <https://nvd.nist.gov/vuln/detail/CVE-2019-11358>
 - <https://nvd.nist.gov/vuln/detail/CVE-2019-5428>
 - <https://blog.jquery.com/2019/04/10/jquery-3-4-0-released/>

Request

```
POST /login HTTP/1.1
Host: 172.26.99.119:8000
Content-Length: 391
```

```
accept: /*  
accept-language: en-US  
content-type: multipart/form-data; boundary=----WebKitFormBoundaryWV8sReG8grpWrXyQ  
cookie: XSRF-  
TOKEN=eyJpdiI6InV2MW4rVkJzZjFZN3VPdFd6bzJIWVE9PSIsInZhbHVlIjoiwk5TRl10SzQ5Tm5kbHM3VVhoYWNidXZ3Q1RkdW  
tWczdnWXhLZlVJUXBkc1JzK1h3Y1JPZWZ1Sm5EU2ZmaVBJL0FBYzd0VzlmQjh0ZkxRc3gvd2pyNVhjeXB6MzZwc0JralVXewlCS3  
NHVldhZE1ta054UVpGeHZ0bXdESkpsQmMiLCJtYWMiOiI0YjczMTg4MWJkYmYwNWRiZjRhNzE1MWQwMWI3YmYwOTZlNGVlZjQwZG  
FhODc2NzZlNGJlZjZjNTdjMjI2Zjg0IiwidGFnIjoiiIn0%3D;  
laravel_session=eyJpdiI6IndTTjV3MDNrS2t2UUtSSytLTHVEVVE9PSIsInZhbHVlIjoivVWLclhZWJhV01CaTgvNmtzRWVl  
a0N0Y0xUU1BEaHE0N2QybnlvV1NWTHlkYkMvbG1ZSDJlUWZzZStpcFFVZlVXaFhjWGloeUxWYVNXtjNzNm5Sc2FZVFdXckl4NHB0  
YStpdVVMQTNUY3BLZlVVMZWwGMGZBMlFoYUE3TnZoejYiLCJtYWMiOiJhMTA5MWRjNjZmZyY3NmYwN2QzNjQwOGZhOGI3MWRkMDA4  
YzYyY2ZjNDVhNmQ1NzdjYzIiMDQ1MWVmMWQ1MWViIiwidGFnIjoiiIn0%3D  
origin: http://172.26.99.119:8000  
Referer: http://172.26.99.119:8000/  
Accept-Encoding: gzip, deflate, br  
Connection: keep-alive  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)  
Chrome/108.0.0.0 Safari/537.36  
  
-----WebKitFormBoundaryWV8sReG8grpWrXyQ  
Content-Disposition: form-data; name="_token"  
  
t5f5sEYsuPdCEomCr6O87vM6paFiHNRHQYOBkUAF  
-----WebKitFormBoundaryWV8sReG8grpWrXyQ  
Content-Disposition: form-data; name="username"  
  
pHqghUme  
-----WebKitFormBoundaryWV8sReG8grpWrXyQ  
Content-Disposition: form-data; name="password"  
  
u]H[ww6KrA9F.x-F  
-----WebKitFormBoundaryWV8sReG8grpWrXyQ--
```

<http://172.26.99.119:8000/>

Verified

- **jQuery 3.3.1**

- URL: <http://172.26.99.119:8000/js/jquery.min.js>
- Detection method: The library's name and version were determined based on the file's syntax fingerprint. Acunetix verified the library version and the associated vulnerabilities with the file's unique syntax fingerprint, which matched the syntax fingerprint expected by Acunetix.
- CVE-ID: CVE-2020-11022, CVE-2020-11023, CVE-2019-11358
- Description: In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. `.html()`, `.append()`, and others) may execute untrusted code. This problem is patched in jQuery 3.5.0. / In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing option elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. `.html()`, `.append()`, and others) may execute untrusted code. This problem is patched in jQuery 3.5.0. / jQuery mishandles `jQuery.extend(true, {}, ...)` because of Object.prototype pollution. If an unsanitized source object contained an enumerable `__proto__` property, it could extend the native Object.prototype.

- References:

- <https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/>
- <https://mksben.l0.cm/2020/05/jquery3.5.0-xss.html>
- <https://jquery.com/upgrade-guide/3.5/>
- <https://api.jquery.com/jQuery.htmlPrefilter/>
- <https://www.cvedetails.com/cve/CVE-2020-11022/>
- <https://github.com/advisories/GHSA-gxr4-xjj5-5px2>
- <https://www.cvedetails.com/cve/CVE-2020-11023/>
- <https://github.com/advisories/GHSA-jpcq-cgw6-v4j6>
- <https://github.com/jquery/jquery/pull/4333>
- <https://nvd.nist.gov/vuln/detail/CVE-2019-11358>
- <https://nvd.nist.gov/vuln/detail/CVE-2019-5428>
- <https://blog.jquery.com/2019/04/10/jquery-3-4-0-released/>

Request

```
GET /js/jquery.min.js HTTP/1.1
Referer: http://172.26.99.119:8000/login
Cookie: XSRF-
TOKEN=eyJpdii6IkRYSVpQcUlZYLjQnRPTHMzOUltS3c9PSIsInZhbHVlIjoiZ2tsdkpRLzdMbjdCQ2xjLzEzOXJISlNNY1VXRj
FMevVIVkVpM0ZTZ1ZBUUs2d1FURWNFVEudFpFMldPMXZsYm43c09rSszZ3MVfZOTlnRFZzSDRZS0dQzFzFSNTVaOTQvMDF5VStkQk
dLTUczTXNDWwluRkpIZVJmUC85R0hYtKsiLCJtYWMiOiI3NWEwNzFkZmEwM2ExNDEzOWRmZjU0ODVhMDM4Y2M4NjYxMWZhN2M4MD
dkMGNmNzYyMDJmNzFmOTM4M2E0YWEwIiwidGFnIjoiIn0%3D;
laravel_session=eyJpdii6IkKkbjJtb2NvUTdQbHhlZlF3b3p6eHc9PSIsInZhbHVlIjoiNVhya0xOVnV5VUZja1FleGtxalRJ
MllQbDl0TEhQMjcrVWRpR3NSb1h3aVpBTlJXew9lMW9DVmFHQWRNcU5XQmpUNDRMZ04rMTThWQmxJdU5JME5wdTBXV0h3VDJDbW9H
WVoxaHh0eHBFR0V3MmpQTVZNRRk82TElTVG5PRmZxTGMiLCJtYWMiOiIyNWFMOGI3NjM0NTMlMGYiYODFjNjU0YyJ2MmNmMTFhMWI3
NDJkNDdmZTBhZjE0MDIwZGIyY2NkZjQ0NmRjZDQyIiwidGFnIjoiIn0%3D
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/108.0.0.0 Safari/537.36
Host: 172.26.99.119:8000
Connection: Keep-alive
```

Recommendation

Upgrade to the latest version.

Clickjacking: X-Frame-Options header

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 did not return an **X-Frame-Options** header with the value DENY or SAMEORIGIN, 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 untrusted sites.

Impact

The impact depends on the affected web application.

http://172.26.99.119:8000/

Paths without secure XFO header:

- <http://172.26.99.119:8000/>
- <http://172.26.99.119:8000/login>
- <http://172.26.99.119:8000/css/>
- <http://172.26.99.119:8000/Main>
- <http://172.26.99.119:8000/images/>
- <http://172.26.99.119:8000/index.php>
- <http://172.26.99.119:8000/register>
- <http://172.26.99.119:8000/BatteryPower>
- <http://172.26.99.119:8000/CellBlocking>
- <http://172.26.99.119:8000/Logout>
- <http://172.26.99.119:8000/MicrowaveNetwork>
- <http://172.26.99.119:8000/SolarPower>
- <http://172.26.99.119:8000/WiBASNetwork>
- <http://172.26.99.119:8000/fonts/>
- <http://172.26.99.119:8000/js/>

Request

```
GET / HTTP/1.1
Host: 172.26.99.119:8000
Pragma: no-cache
Cache-Control: no-cache
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=0.9
accept-language: en-US
upgrade-insecure-requests: 1
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/108.0.0.0 Safari/537.36
```

Recommendation

Configure your web server to include an X-Frame-Options header and a CSP header with frame-ancestors directive. Consult Web references for more information about the possible values for this header.

References

[The X-Frame-Options response header](https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options)

<https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options>

[Clickjacking](https://en.wikipedia.org/wiki/Clickjacking)

<https://en.wikipedia.org/wiki/Clickjacking>

[OWASP Clickjacking](https://cheatsheetseries.owasp.org/cheatsheets/Clickjacking_Defense_Cheat_Sheet.html)

https://cheatsheetseries.owasp.org/cheatsheets/Clickjacking_Defense_Cheat_Sheet.html

[Frame Buster Buster](https://stackoverflow.com/questions/958997/frame-buster-buster-buster-code-needed)

<https://stackoverflow.com/questions/958997/frame-buster-buster-buster-code-needed>

Cookies without HttpOnly flag set

One or more cookies don't have the HttpOnly flag set. When a cookie is set with the HttpOnly flag, it instructs the browser that the cookie can only be accessed by the server and not by client-side scripts. This is an important security protection for session cookies.

Impact

Cookies can be accessed by client-side scripts.

<http://172.26.99.119:8000/>

Verified

Cookies without HttpOnly flag set:

- <http://172.26.99.119:8000/>

```
Set-Cookie: XSRF-  
TOKEN=eyJpdii6InV2MW4rVkJzZjFZN3VPdFd6bzJIWVE9PSIsInZhbHVlIjoiWk5TRl10SzQ5Tm5KbHM3VWVoYWNIIdXZ3QlRkdWtWczdnWXhLZlVJUXBkc1JzK1h3YlJPZWZlSm5EU2ZmaVBjL0FBYzd0VzlmQjh0ZkxRc3gvb2pyNVhjeXB6MzZwc0JralVXeWlCS3NHVldhZE1ta054UVpGeHZ0bXdESkpsQmMiLCJtYWMiOiI0YjczMTg4MWJkYmYwNWRiZjRhNzE1MWQwMWI3YmYwOTZlNGVlZjQwZGFhODc2NzZlNGJlZjZjNTdjMjI2Zjg0IiwidGFuIjoiIn0%3D; expires=Fri, 10 Feb 2023 06:20:58 GMT; Max-Age=3600; path=/; samesite=lax
```

- <http://172.26.99.119:8000/login>

```
Set-Cookie: XSRF-  
TOKEN=eyJpdii6IjNwbEM1c0lJVVVuNm5BKzJHalleYke9PSIsInZhbHVlIjoidHgxZjZNVW9hWFVMVHZpaTgyaUdQcklwdG5hZUpiUGQ2UC8vMElnSlZVOUUNFmNmJkZS9NRWZHb0c4Y2ZyYjdKWDlERENjWnMxbzYxVEE2Qlo5SlZCZE4xbFpxQ2x0bUVjcGYwOXo2ZE5DNTg5SVNWNVvk4dndxaFZuUzhlZVAiLCJtYWMiOiI0YjYjF1MmMyMTkyYzk2NGI2MDAwMmMwMWQ4NmJlMzEyMDVjN2QwYWI0MGI2YjBmMDQlZDk3YzA4M2VlYzZkZjZjNkIiwidGFuIjoiIn0%3D; expires=Fri, 10 Feb 2023 06:21:05 GMT; Max-Age=3600; path=/; samesite=lax
```

- <http://172.26.99.119:8000/index.php>

```
Set-Cookie: XSRF-  
TOKEN=eyJpdii6IjRzWk5kLzNxV3lJc0VzTEZhNUZ2SWc9PSIsInZhbHVlIjoiKy8wc2x1VE9RYldEaitkTGR3RDEvNVpKNzJSZzErWjFqSDFmaFpDZCtVMjhBeEF5Nlh1NlA0VXZ5bTlQb2FxK2lSd25aMWZma1JEM3U3WTlNbGFhNDF2cEprQ1ZlZG9teVMzd1FHRjhCcldpNlpsa1NkcjFybG1tWDNuM2M2cSsiLCJtYWMiOiIzOGY0NmYxOTlkN2NiZTI4Mjg0YTUwZTY3ZTZmMzZkZTkyN2VjN2ZkNGI1YmNmMTA4OTViZGVjMTBiMGQ3YmQxIiwidGFuIjoiIn0%3D; expires=Fri, 10 Feb 2023 06:37:37 GMT; Max-Age=3600; path=/; samesite=lax
```

- <http://172.26.99.119:8000/register>

```
Set-Cookie: XSRF-  
TOKEN=eyJpdii6Ilk4WwNJK2VZTlV4a0wxSFpoTi9tNlE9PSIsInZhbHVlIjoiYmMiLCJtYWMiOiI0YjYjF1MmMyMTkyYzk2NGI2MDAwMmMwMWQ4NmJlMzEyMDVjN2QwYWI0MGI2YjBmMDQlZDk3YzA4M2VlYzZkZjZjNkIiwidGFuIjoiIn0%3D; expires=Fri, 10 Feb 2023 06:37:37 GMT; Max-Age=3600; path=/; samesite=lax
```

```
iI2ZTA4YmMxZTJjMmVmNWQyMGQ5ZGI1NDIzMzUxYzg2MjQ4ZTRjOThlNjI0ZDU1M2E0MDZmYzNlODQzND
A1YzAyIiwidGFnIjoiIn0%3D; expires=Fri, 10 Feb 2023 06:37:47 GMT; Max-Age=3600;
path=/; samesite=lax
```

- <http://172.26.99.119:8000/Dashboard>

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IitaTEJJbnpDTU81RTBMbitzRjNuWFE9PSIsInZhbnHVlIjoiWEltNnZpQWNzZy9ibmU
2U3pRclYrV0hVdlI1Q0JwQVZYTz12dGpnL2hTbDZLY01yUzQ1bC81M2thRzFYREdWNS9ER2Y0VjBlUHpo
QWVPbDFaMVdRYUQxUmFzMWg3OGhWbEJHVHRyQ2JaRXd4STVKYmFhNWJWZ1RYYUNyUnFLMlUiLCJtYWMiO
iI5MDg0YjZmYTAYMzZjMzNkNjk4MmQ5OTFjZTdhdjZlZTgwYmFhOGIzNDVlNmE5Mzk3MTJiMTAYMWUxND
hmYWNiIiwidGFnIjoiIn0%3D; expires=Fri, 10 Feb 2023 06:38:02 GMT; Max-Age=3600;
path=/; samesite=lax
```

- <http://172.26.99.119:8000/Generators>

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IlM5d1A3ajFFQTh3OFRXZUEyTnM1S3c9PSIsInZhbnHVlIjoiLlRTTnh5NUNSa3RVQ2x
rUz1CaDhQVXRIYVZONWRZWjRYd0NHYkF4QUprM284N1NtR2w4OGtWS0NVmZdCRjc4U2RleUUwM2ZjWWdw
UUVwQVovL1V6TldGTmlxUDlySTB3Q1lGUtF0WlZmZi9MYkRlPcVNPOFBiZnp0UW15WnQvRW0iLCJtYWMiO
iJkNDQ5OWE2ODZlNzI3ZGE0YTgyYTBhMDA5YjM3Yjk2NzZkMj1hNjYzNjM0YjExMD1lOGM3Njc4MzYzNG
FmOGQyIiwidGFnIjoiIn0%3D; expires=Fri, 10 Feb 2023 06:38:03 GMT; Max-Age=3600;
path=/; samesite=lax
```

- <http://172.26.99.119:8000/GridPower>

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IktBRk5VVy8xc1FXTlhkMkUxOW9IakE9PSIsInZhbnHVlIjoiRXpKa0F4cXN3VHplZFUJ
3ZnZVT0hxY3JkSnNKQXppdzdiYjU1RlVKQ1RCWmFIVnRkMks2T3h6RTdXWnAxWE4yc0ltNE05K0pEdHla
U2lod0k0LytQK21KUDNGRHFFQWVlcXhuY0dybmZkZ202UFZWSmlvV3BUUlVlaFB0OGhPb1oiLCJtYWMiO
iI0NGVhODdhYThkMzZmNjUzZDVmMzViM2YzZDYxZGMxMWY1ZjdjNzJjMTk4YzZmNmE1OTg5MjU3YWVjZj
BkNmZiIiwidGFnIjoiIn0%3D; expires=Fri, 10 Feb 2023 06:38:05 GMT; Max-Age=3600;
path=/; samesite=lax
```

- <http://172.26.99.119:8000/IPNetwork>

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IlRiRFNyYUgyMFRMR2VKaHZXTlhpMEE9PSIsInZhbnHVlIjoiNlVwK2kzc1Rmw4OXdx
qQW1SMlF6d3J3VzFnUkVwbVh1L3VqZ1dNWmZxOXY2NTN3Y3o3ck5aeUVnQ2ZUaFFyWXdyOTFvY2RWeVBu
TmhUc1NqYjcySG1zNXNkMkI2dEJvQjZmOFdYQjVmRTZ1Q0NMSVVQUStCTmR1TVJuek4zc3UiLCJtYWMiO
```

```
iIXyZiXNDMxYmFmNjlmNmY3NWM1MjUyYWVjMTMzZDRiMGE1NTE5YmQxNmIzYjdiZmRkMGZlOTkxYjZiNG
ElN2JjIiwidGFnIjoiIn0%3D; expires=Fri, 10 Feb 2023 06:38:05 GMT; Max-Age=3600;
path=/; samesite=lax
```

- <http://172.26.99.119:8000/Logout>

```
Set-Cookie: XSRF-  
TOKEN=eyJpdjI6IjREa2lmVTN2MDhJQnpnL3RpcEFjOFE9PSIsInZhbHVlIjoId0hIYzZKUkpyblV4aXdiQnRNajA3bldiV3grWWwrUTM2YjI1QjV4UXFzREDBUWF6S2h2eW9oelherUH2VnJXYVBpWi9DWEtURLN2U0NqaHl3eXN3YkjqRW8rMVg1Y05ZU2lwWjRtcmdZVFFVaEZ2eTJMMnlacTUwZHNVZExrV0giLCJtYWMiOiIwMmElNTZmYzdjBlnZlWmcxNjgyMjVkJm1YzliNGI2MjM3NmM2NjMyOWY2NDNkZWU4ZmUxNjAwMzA0MmQ4IiwidGFniGFnIjoiIn0%3D; expires=Fri, 10 Feb 2023 06:38:08 GMT; Max-Age=3600;  
path=/; samesite=lax
```

- <http://172.26.99.119:8000/PSCore>

Set-Cookie: XSRF-
TOKEN=eyJpdiI6IlcxRWZh3VjN0YjY5UFYlVG10VWYvbFE9PSIsInZhbHVlIjoiOVRlOXBueFZZNTFac2dKMk5YdFo2ZTVId04zdHk2ckJYejdNS1JvOVRaUDMzM2IyNDJDaUo5RTVpYSthTDlsOWF4TGfueCt6aVdFM0E3cm1wVFR2YVNGNXJsd29XTEJ5bXcxbURzeXBPWWZrMjcwaHlqa0E0d0JYb2pGWm42aXAiLCJtYWMiOiJiYThmNWY4MmI0MTg4YjQxN2U1ZjhmYzZM5ZDU4ZDRiNDY0ZTQ3NGQ2ZDgzOGNjZjVjNDIzZTRmZDE5YmQ5ZmRhIiwidGFnIjoiIn0%3D; expires=Fri, 10 Feb 2023 06:38:19 GMT; Max-Age=3600; path=/; samesite=lax

- <http://172.26.99.119:8000/Railway>

```
Set-Cookie: XSRF-  
TOKEN=eyJpdii6IjhnMVUybFAyK0tCU3hOZlBvcjJCMnc9PSIsInZhbmHVlIjoibzBMZHNYRVNzdXZXUXR  
HL0l2YXRybFVGUjFHL2J4YXhJU0tWNDM0SVp3RWFHT2o2MVFUaUtEN3NidHNJL25xMDFxwGVKck95cENE  
S0kxc1JWOE5IMGxSR3ZOWmJ2OVlvMnVUaElrY0ZuN081VWNQZ2UvRS8vRkQ3MWlxRmpWNCsiLCJtYWMiO  
iJkZDVmZTE4NzZmYzRjYzgONTdiZDQ5MGMyM2ExOGQxMTRMzYzFiZjBhMWYzNDAAzNzViN2VhZjVlZjc0Mz  
ElMzYyIiwidGFniJoiIn0%3D; expires=Fri, 10 Feb 2023 06:38:19 GMT; Max-Age=3600;  
path=/; samesite=lax
```

- <http://172.26.99.119:8000/SiteData>

Set-Cookie: XSRF-
TOKEN=eyJpdiI6IkxibzhoTHJXZXVxN3NkelJnT3h0YVE9PSIsInZhbHVlIjoiVzY0djROaHJXVmNWenp
FZEJwNUpibmFQUHZsTm5aWGlvV1d2eU5OZU9Sb2MwTGtCamRKUDM0U0hza2l1ZzFZSG9WSkpvVTN0bk45
Zmk5MkZEcnlzOUkvTVhpMHE0c2lRYkovVXRnLE2WEJ4WmhiU25Wbm5PZUVNK3orb0ZUL1UiLCJtYWMiO

iI0NDVhZGNkZjRmMjMxZWQwNzJhNjhlZGVhOGNiMTJkY2JmZWVmMjc5NDFiOTE4ZTQwMWZhNjNjMmY2ZD
QzNWYwIiwidGFnIjoiIn0%3D; expires=Fri, 10 Feb 2023 06:38:32 GMT; Max-Age=3600;
path=/; samesite=lax

- <http://172.26.99.119:8000/>

Set-Cookie: XSRF-
TOKEN=eyJpdiI6IkkI3QWJpP0oxMWRrRlBwRUswbFgwd0E9PSIsInZhbnHVlIjoiK0lmREJnMEdZMmZxakR
Zek1ldVpKQjJ5TGd3Qm5IaytRdXBMM0JBNWk1VE9VOUVObjV2dFVYsUNUEg9pVVhwMldYT3E3V0VrNDB1
U1ZjK3hYKzh1SDVkrDRrc1pSEhIaw9GWHdqZjMybDhqOFRmK2s2OUp3bnUrUjEyTmsrbXAiLCJtYWMiO
iJkNmI1MjAwY2M1NzZkxNDM3ZjI4YmMyYWE2ODQ5ZWE2MmIzMGZiYmJkOWE0ZD1lZmMxMmJjYTBmN2Q5NT
E2MzMzIiwidGFnIjoiIn0%3D; expires=Fri, 10 Feb 2023 07:07:39 GMT; Max-Age=3600;
path=/; samesite=lax

- <http://172.26.99.119:8000/Dashboard>

Set-Cookie: XSRF-
TOKEN=eyJpdiI6InRDYTNRUkxCaUlKN3NyVzE2aGYvelE9PSIsInZhbnHVlIjoiRVBkVnZaMHBIV0FKVXE
OK3hFV096Nk9oL2R4dFllVWJia01FYlZkbmxRUlVReXAxYzhFYkYvTnJvWFh4YlloamZTbjZGaDQ0Uzg0
NHE2VDEyeDZPQS9TREU2bHlmNzZyUmlNR3R3RnkvcWhhNmZSUXVWakJ4U2p0cTdtTEFIMjgiLCJtYWMiO
iJiNDdlNGRhNTJmYzZzMDBhZjhlY2IxMWIwNDhmMjIzOTVjYWZiNmZmZTk0NWl0NmFhMGE2ZGE5ZmE3Nm
IyYzVkIiwidGFnIjoiIn0%3D; expires=Fri, 10 Feb 2023 07:07:49 GMT; Max-Age=3600;
path=/; samesite=lax

- <http://172.26.99.119:8000/Generators>

Set-Cookie: XSRF-
TOKEN=eyJpdiI6IjdCejBralliczVocUlpdXBBV25LZXc9PSIsInZhbnHVlIjoiVlBla2dCMzlwZlgyM1l
neU1RZVpZTTJHamU3a2FGelAydENzMXhmSVNpbTdTktW5aVElZV2x6aEo4VlZzRy9nRj10Zyt6YU5DNDNs
cmk1Ulh5SmJFwJzhTjhwUE9sVVEvU01JZlZlRQ1RuZlZnQnVBWUF4TlNrR0c3VUhJTmhtTFMiLCJtYWMiO
iJhNWJiMjExNmViNTM3MmJjODQ0YzU3MmZmN2NiMjZmMDJmYzVmNGFkZDQ4OGM4M2RhOWYyZGI0ZTUxMz
cwYTNhIiwidGFnIjoiIn0%3D; expires=Fri, 10 Feb 2023 07:07:49 GMT; Max-Age=3600;
path=/; samesite=lax

- <http://172.26.99.119:8000/GridPower>

Set-Cookie: XSRF-
TOKEN=eyJpdiI6InpxeVlZRMqrdDdKM2lyR0NuYTFSOVE9PSIsInZhbnHVlIjoiU2pTRmFCY3lwZXpOQTZ
Lakswc2I2K2ROZHZJLZHYxOWtkL1dzSDhaMURXM2I5SWNTd2R6cmpXbHE5NlRjZUdYQkFjWXJ2L05pWG1q
M1RCWFdjQlpTSGpPMnVJZFV5OFU2WGl0a2U4WnVSemVvUz1UOHZqNVQyVVNMU1VvY2czOFMiLCJtYWMiO

```
iIxOTVvkY2M2Yjc4ZjYzMGRhODFlN2I3NmRlN2JlZWZzODMwMzZiYzAzOTQ4ZTM5ZDA1Y2JhMDkyMmYwNT
ZkYmIxiwidGFniJoiIn0%3D; expires=Fri, 10 Feb 2023 07:07:50 GMT; Max-Age=3600;
path=/; samesite=lax
```

- <http://172.26.99.119:8000/IPNetwork>

```
Set-Cookie: XSRF-  
TOKEN=eyJpdiI6Ik82bURRdlNiRkQ3d0syTVh2bTdZU1E9PSIsInZhbnVlIjoiQnhzV052aUVSTnExbGtMbVR2dE5xeU9Nd2V5TytMK0h2Mzh1Q0dkL080b2lWRzVxYjVvZ3JkcW9lNEoxUTJJZHQ0eGZPTzcvQ1gzYlFBWHJ3cFhxMVVlbjdBCTk55MVl5aFpUL240cTdoZmdGVtY3YmVnSmlxVWpEeE5LNmwzdWoiLCJtYWMiOiI4OWViMmU0NDQ4NjYxNDcyYjllOTljMDVmZWZkMGE2ODk1ZDBkNjJhYjVmNzBjMWNkMzM3MThiODY1NGUyZWVjIiwidGFnIjoiIn0%3D; expires=Fri, 10 Feb 2023 07:07:50 GMT; Max-Age=3600;  
path=/; samesite=lax
```

- <http://172.26.99.119:8000/Logout>

Set-Cookie: XSRF-
TOKEN=eyJpdiI6IkNhM1A1Y0UvVjJjYmwlYWNEK0FGZmc9PSIsInZhbHVlIjoiSUtNbTN4eDYxMGowMEM5YkhENThmZUxVTkt6ZlhljeEVLMEZjbUhjS1M5d3VPUzYyUFNJd3EwUTIrQ3ZxaUdsWS9JbGsvOUtNWxzTSWN3eW5UVTR0VjVlNGJlZ3dOUkhEejFudUp6VFZBYzZpaTZ2M2d1NTV3NUlWUmhlYXJrdDciLCJtYWMiOiJlNDcxMGIlNDk3NzNkMjF1MzRkN2NmMjFkYThkZjJmYjEwN2Q0NDZjM2EwOGJhZDY4MGVjYWE4NTA2ODVkMmM5IiwidGFnIjoiIn0%3D; expires=Fri, 10 Feb 2023 07:07:50 GMT; Max-Age=3600; path=/; samesite=lax

- <http://172.26.99.119:8000/index.php>

```
Set-Cookie: XSRF-  
TOKEN=eyJpdii6ImRMTHkwMG9RYzBPSEFaRVBwbWdsbnc9PSIsInZhbHVlIjoiaUXFqOWYxZDZrOGdpTlN  
ieDB3djNYM292SjBvbFh3RFclQ19vWGNMcHR0UnVidzBFcnpsdGRvU11ldTRJa1p5Z2tyMUIzSnVTRElT  
dTZUZfZzhQlIwakxtSUx3REpqYm9GNUMhnempuVkZoUnFqeEM3cEZRdU1adVY1SjAyaGNWRzYiLCJtYWMiO  
iI0NmVmMtc3NDdjN2MyMGNmMjAzMDBmYTc5YjYyODI4YTAyMGFiMDJkNTMxNjg5NzdkNjUzNGIyZTc4Mz  
NmMDVjIiwidGFnIjoiaW0%3D; expires=Fri, 10 Feb 2023 10:55:29 GMT; Max-Age=3600;  
path=/; samesite=lax
```

- <http://172.26.99.119:8000/register>

Set-Cookie: XSRF-TOKEN=eyJpdiI6Ilk2bGxhVF12RTZOYkovczdjVVFxVXc9PSIsInZhbnHV1IjoiR3drVWJaZ051b3pYnk9IamlMTFsSzhHTC9rWnlSN2FFbVlk2czVMTjMxclE5VjJDa2JGL1QwVWhvTDZpVk05QTM3Y1k0Ly9LQjh1OUxnRnhmTjFVWkpGcnhUL1ZiamxiakU2VESrU3hXcTN5WE9paXRjMGNTtR3ZYZy9ZbnMxR3UiLCJtYWMiO


```
iI5MWNhNzU5ODk2MjQ1ZjM3ZGIyYTM5NDZiYzUwYTI2YTZhYTIZMjY3NjdkMGQ0ODVlNWExMTU5N2Y2ND
dlNjA3IiwidGFnIjoiIn0%3D; expires=Fri, 10 Feb 2023 10:55:33 GMT; Max-Age=3600;
path=/; samesite=lax
```

Request

```
GET / HTTP/1.1
Host: 172.26.99.119:8000
Pragma: no-cache
Cache-Control: no-cache
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=0.9
accept-language: en-US
upgrade-insecure-requests: 1
Accept-Encoding: gzip,deflate,br
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/108.0.0.0 Safari/537.36
```

Recommendation

If possible, you should set the HttpOnly flag for these cookies.

Content Security Policy (CSP) not implemented

Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks.

Content Security Policy (CSP) can be implemented by adding a **Content-Security-Policy** header. The value of this header is a string containing the policy directives describing your Content Security Policy. To implement CSP, you should define lists of allowed origins for the all of the types of resources that your site utilizes. For example, if you have a simple site that needs to load scripts, stylesheets, and images hosted locally, as well as from the jQuery library from their CDN, the CSP header could look like the following:

```
Content-Security-Policy:
default-src 'self';
script-src 'self' https://code.jquery.com;
```

It was detected that your web application doesn't implement Content Security Policy (CSP) as the CSP

header is missing from the response. It's recommended to implement Content Security Policy (CSP) into your web application.

Impact

CSP can be used to prevent and/or mitigate attacks that involve content/code injection, such as cross-site scripting/XSS attacks, attacks that require embedding a malicious resource, attacks that involve malicious use of iframes, such as clickjacking attacks, and others.

http://172.26.99.119:8000/

Paths without CSP header:

- <http://172.26.99.119:8000/>
- <http://172.26.99.119:8000/css/>
- <http://172.26.99.119:8000/Main>
- <http://172.26.99.119:8000/images/>
- <http://172.26.99.119:8000/index.php>
- <http://172.26.99.119:8000/register>
- <http://172.26.99.119:8000/BatteryPower>
- <http://172.26.99.119:8000/CellBlocking>
- <http://172.26.99.119:8000/Logout>
- <http://172.26.99.119:8000/MicrowaveNetwork>
- <http://172.26.99.119:8000/SolarPower>
- <http://172.26.99.119:8000/WiBASNetwork>
- <http://172.26.99.119:8000/fonts/>
- <http://172.26.99.119:8000/js/>

Request

```
GET / HTTP/1.1
Host: 172.26.99.119:8000
Pragma: no-cache
```

```
Cache-Control: no-cache
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=0.9
accept-language: en-US
upgrade-insecure-requests: 1
Accept-Encoding: gzip,deflate,br
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/108.0.0.0 Safari/537.36
```

Recommendation

It's recommended to implement Content Security Policy (CSP) into your web application. Configuring Content Security Policy involves adding the **Content-Security-Policy** HTTP header to a web page and giving it values to control resources the user agent is allowed to load for that page.

References

[Content Security Policy \(CSP\)](https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP)

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

[Implementing Content Security Policy](https://hacks.mozilla.org/2016/02/implementing-content-security-policy/)

<https://hacks.mozilla.org/2016/02/implementing-content-security-policy/>

Javascript Source map detected

Client side Javascript source code can be combined, minified or compiled. A source map is a file that maps from the transformed source to the original source. Source map may help an attacker to read and debug Javascript.

Impact

Access to source maps may help an attacker to read and debug Javascript code. It simplifies finding client-side vulnerabilities

<http://172.26.99.119:8000/>

Confidence: 80%

URLs where links to SourceMaps were found:

- sourceMappingURL in JS body - <http://172.26.99.119:8000/js/bootstrap.min.js>
- sourceMappingURL in JS body - <http://172.26.99.119:8000/js/popper.js>

Request

```
GET /js/bootstrap.min.js HTTP/1.1
Referer: http://172.26.99.119:8000/login
Cookie: XSRF-
TOKEN=eyJpdiI6IitaTEJJbnpDTU81RTBMbitzRjNuWFE9PSIsInZhbnVlIjoiWEltNnZpQWNzZy9ibmU2U3pRclYrV0hVdlI1Q0
JwQVZYTz12dGpnL2hTbDZLY0lyUzQ1bC81M2thRzFYREdWNS9ER2Y0VjBlUHpoQWVPbDFaMVdRYUQxUmFzMWg3OGhWbEJHVHRyQ2
JaRXd4STVKYmFhNWJWZlRYYUNyUnFLMlUiLCJtYWMiOiI5MDg0YjZmYTAYMzZjMzNkNjk4MmQ5OTFjZTdhMjZlZTgwYmFhOGIzND
VlNmE5Mzk3MTJiMTAyMWUxNDhmYWNiIiwidGFuIjoiIn0%3D;
laravel_session=eyJpdiI6Ik01dm5oMXVPNWljTUfuaGJOc0Rjb1E9PSIsInZhbnVlIjoiM0Y0YkRPSmQ2aHluZ01jYW90V0lp
QlQxb3R0N2dJTWMxS3FuMFBUVVFck1PZU1JN2NYZUM0RU1TWllFVW9GUJvUWlxMnowZXQ2ZkJEekFLMmxSVGlxc0xzRmZqbDBx
UFFNTVhCOEDHJ1MrUzNmbndYUGwzU2hTaFhGbmNwNEgilCJtYWMiOiI3MDEyZWZWM0YmNlODJlNGE4ZWZWM5MGQzYTU1NDI0NDhhM2I1
NGJjYWM3N2E0YWE2ZTRMODUwZDY1Njc4MDkwMWI0IiwidGFuIjoiIn0%3D
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/108.0.0.0 Safari/537.36
Host: 172.26.99.119:8000
Connection: Keep-alive
```

Recommendation

According to the best practices, source maps should not be accesible for an attacker. Consult web references for more information

References

[Using sourcemaps on production without exposing the source code](https://itnext.io/using-sourcemaps-on-production-without-revealing-the-source-code-%EF%B8%8F-d41e78e20c89)

<https://itnext.io/using-sourcemaps-on-production-without-revealing-the-source-code-%EF%B8%8F-d41e78e20c89>

[SPA source code recovery by un-Webpacking source maps](https://medium.com/@rarecoil/spa-source-code-recovery-by-un-webpacking-source-maps-ef830fc2351d)

<https://medium.com/@rarecoil/spa-source-code-recovery-by-un-webpacking-source-maps-ef830fc2351d>

No HTTP Redirection

It was detected that your web application uses HTTP protocol, but doesn't automatically redirect users to HTTPS.

Impact

In some circumstances, it could be used for a man-in-the-middle (MitM) attack

http://172.26.99.119:8000/

Request

```
GET / HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/108.0.0.0 Safari/537.36
Host: 172.26.99.119:8000
Connection: Keep-alive
```

Recommendation

It's recommended to implement best practices of HTTP Redirection into your web application. Consult web references for more information

References

HTTP Redirections

https://infosec.mozilla.org/guidelines/web_security#http-redirections

Outdated JavaScript libraries

You are using an outdated version of one or more JavaScript libraries. A more recent version is available. Although your version was not found to be affected by any security vulnerabilities, it is recommended to keep libraries up to date.

Impact

Consult References for more information.

http://172.26.99.119:8000/

Confidence: 95%

- **bootstrap.js 4.3.1**
 - URL: <http://172.26.99.119:8000/login>
 - Detection method: The library's name and version were determined based on its dynamic behavior.
 - References:
 - <https://github.com/twbs/bootstrap/releases>

Request

```
POST /login HTTP/1.1
Host: 172.26.99.119:8000
Content-Length: 391
accept: */*
accept-language: en-US
content-type: multipart/form-data; boundary=----WebKitFormBoundaryWV8sReG8grpWrxYq
cookie: XSRF-
TOKEN=eyJpdiI6InV2MW4rVkJsZjFZN3VPdFd6bzJIWVE9PSIsInZhbnHVlIjoiWk5TRl10SzQ5Tm5KbHM3VWhoYWNIdXZ3Q1RkdW
tWczdnWXhLZl1VJUXBkc1JzK1h3YlJPZWZ1Sm5EU2ZmaVBjL0FBYzd0VzlmQjh0ZkxRc3gvb2pyNVhjeXB6MzZwc0JralVXeWlCS3
NHVldhZElta054UVpGeHZ0bXdESkpsQmMiLCJtYWMiOiI0YjczMTg4MWJkYmYwNWNRiZjRhNzE1MWQwMWI3YmYwOTZlNGVlZjQwZG
FhODc2NzZlNGJlZjZjNTdjMjI2Zjg0IiwidGFuIjoiIn0%3D;
laravel_session=eyJpdiI6IndTTjV3MDNrsS2t2UUtSSytLTHVEVVE9PSIsInZhbnHVlIjoiVWVLC1hZWJhV0lCaTgvNmtzRWVl
a0N0Y0xUULBEaHE0N2QybnlvVlNWTHlkYkMvbGlZSDJlUQmYzZStpcFFVZXXVXaFhjWGlloeUxWYVNXTjNzMm5Sc2FZVFdXckl4NHB0
YStpdVVMQTNUY3BLZXVMZWxGMGZBMlFoYUE3TnZoejYiLCJtYWMiOiJhMTA5MWRjNjZmZyY3NmYwN2QzNjQwOGZhoGI3MWRkMDA4
YzYyY2ZjNDVhNmQ1NzdjYzI1MDQ1MwVmMwQ1MwViIiwidGFuIjoiIn0%3D
origin: http://172.26.99.119:8000
Referer: http://172.26.99.119:8000/
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/108.0.0.0 Safari/537.36

-----WebKitFormBoundaryWV8sReG8grpWrxYq
Content-Disposition: form-data; name="_token"

t5f5sEYsuPdCEomCr6O87vM6paFiHNRHQYOBkUAf
-----WebKitFormBoundaryWV8sReG8grpWrxYq
Content-Disposition: form-data; name="username"

pHqghUme
-----WebKitFormBoundaryWV8sReG8grpWrxYq
Content-Disposition: form-data; name="password"

u]H[ww6KrA9F.x-F
-----WebKitFormBoundaryWV8sReG8grpWrxYq--
```

Recommendation

Upgrade to the latest version.

Permissions-Policy header not implemented

The Permissions-Policy header allows developers to selectively enable and disable use of various browser features and APIs.

<http://172.26.99.119:8000/>

Locations without Permissions-Policy header:

- <http://172.26.99.119:8000/>
- <http://172.26.99.119:8000/login>
- <http://172.26.99.119:8000/css/>
- <http://172.26.99.119:8000/Main>
- <http://172.26.99.119:8000/images/>
- <http://172.26.99.119:8000/index.php>
- <http://172.26.99.119:8000/register>
- <http://172.26.99.119:8000/BatteryPower>
- <http://172.26.99.119:8000/CellBlocking>
- <http://172.26.99.119:8000/Logout>
- <http://172.26.99.119:8000/MicrowaveNetwork>
- <http://172.26.99.119:8000/SolarPower>
- <http://172.26.99.119:8000/WiBASNetwork>
- <http://172.26.99.119:8000/fonts/>
- <http://172.26.99.119:8000/js/>

Request

```
GET / HTTP/1.1
Host: 172.26.99.119:8000
Pragma: no-cache
Cache-Control: no-cache
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=0.9
accept-language: en-US
upgrade-insecure-requests: 1
Accept-Encoding: gzip,deflate,br
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/108.0.0.0 Safari/537.36
```

References

[Permissions-Policy / Feature-Policy \(MDN\)](#)

<https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Feature-Policy>

[Permissions Policy \(W3C\)](#)

<https://www.w3.org/TR/permissions-policy-1/>

PHP Version Disclosure

The web server is sending the X-Powered-By: response headers, revealing the PHP version.

Impact

An attacker might use the disclosed information to harvest specific security vulnerabilities for the version identified.

<http://172.26.99.119:8000/>

Version detected: PHP/8.1.13.

Recommendation

Configure your web server to prevent information leakage from its HTTP response.

References


[PHP Documentation: header_remove\(\)](https://www.php.net/manual/en/function.header-remove.php)

<https://www.php.net/manual/en/function.header-remove.php>

[PHP Documentation: php.ini directive expose_php](https://www.php.net/manual/en/ini.core.php#ini.expose_php)

https://www.php.net/manual/en/ini.core.php#ini.expose_php

Coverage

 http://172.26.99.119:8000

 css

 font-awesome.min.css

 GoogleFont.css

 jquery.dataTables.min.css

 Main.css

 sweetalert.css

 fonts

 images

 js

 bootstrap.min.js

 dataTables.fixedHeader.min.js

 Internal.js

 jquery-3.1.1.min.js

 jquery.dataTables.min.js

 jquery.min.js

 main.js

 popper.js

 sweetalert.js

 BatteryPower

 CellBlocking

 Dashboard

 Generators

 GridPower

 index.php

 IPNetwork

 login

 #fragments

 #pageSubmenu

 #pageSubmenu1

 #pageSubmenu11

 pageSubmenu12

 pageSubmenu13

 pageSubmenu2

 pageSubmenu3

 pageSubmenu4

 pageSubmenu5

 pageSubmenu9

 Logout

 Main

 MicrowaveNetwork

 PSCore

 Railway

 register

 robots.txt

 SiteData

 SolarPower

 WiBASNetwork