



### 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.



High



Medium



Low

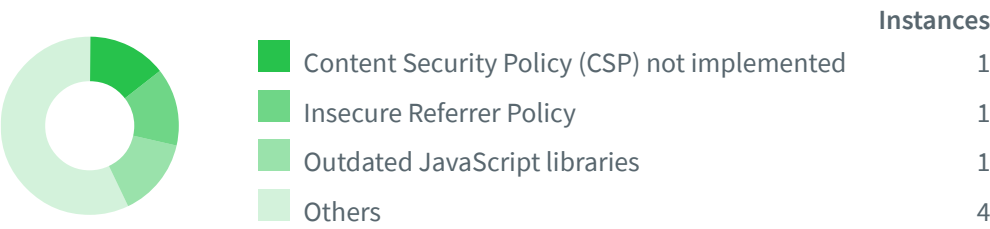


Informational

Severity	Vulnerabilities	Instances
High	0	0
Medium	2	2
Low	6	6
Informational	7	7
Total	15	15

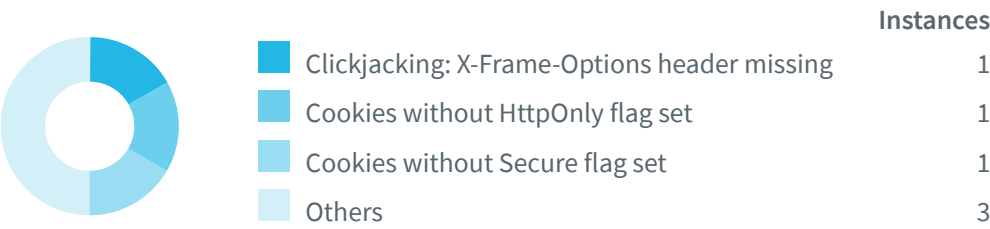
## Informational

---



## Low Severity

---


















## Medium Severity

---



# Impacts

SEVERITY	IMPACT
 Medium	<div>1</div> Slow HTTP Denial of Service Attack
 Medium	<div>1</div> Vulnerable JavaScript libraries
 Low	<div>1</div> Clickjacking: X-Frame-Options header missing
 Low	<div>1</div> Cookies without HttpOnly flag set
 Low	<div>1</div> Cookies without Secure flag set
 Low	<div>1</div> HTTP Strict Transport Security (HSTS) not implemented
 Low	<div>1</div> Login page password-guessing attack
 Low	<div>1</div> Possible sensitive files
 Informational	<div>1</div> Content Security Policy (CSP) not implemented
 Informational	<div>1</div> Insecure Referrer Policy
 Informational	<div>1</div> Outdated JavaScript libraries
 Informational	<div>1</div> Password type input with auto-complete enabled
 Informational	<div>1</div> PHP Version Disclosure
 Informational	<div>1</div> Possible server path disclosure (Unix)
 Informational	<div>1</div> Subresource Integrity (SRI) not implemented

# Slow HTTP Denial of Service Attack

---

Your web server is vulnerable to Slow HTTP DoS (Denial of Service) attacks.

Slowloris and Slow HTTP POST DoS attacks rely on the fact that the HTTP protocol, by design, requires requests to be completely received by the server before they are processed. If an HTTP request is not complete, or if the transfer rate is very low, the server keeps its resources busy waiting for the rest of the data. If the server keeps too many resources busy, this creates a denial of service.

## Impact

---

A single machine can take down another machine's web server with minimal bandwidth and side effects on unrelated services and ports.



Time difference between connections: 9968 ms

## Recommendation

---

Consult Web references for information about protecting your web server against this type of attack.

## References

---

[Slowloris DOS Mitigation Guide](https://www.funtoo.org/Slowloris_DOS_Mitigation_Guide)

[https://www.funtoo.org/Slowloris\\_DOS\\_Mitigation\\_Guide](https://www.funtoo.org/Slowloris_DOS_Mitigation_Guide)

[Protect Apache Against Slowloris Attack](https://web.archive.org/web/20180329210925/http://blog.secaserver.com/2011/08/protect-apache-slowloris-attack/)

<https://web.archive.org/web/20180329210925/http://blog.secaserver.com/2011/08/protect-apache-slowloris-attack/>

# 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.

Confidence: 80%

- **jQuery 1.8.2**

- URL: [https://www.example.com/assets/js/compiled.min.js](#)
- Detection method: The library's name and version were determined based on the file's contents. Acunetix performed a syntax analysis of the file and detected functional differences between the file and the original library version. As the file was likely modified on purpose, the confidence level of the vulnerability alert has been lowered.
- References:
  - <https://github.com/jquery/jquery/issues/2432>
  - <http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/>

## Request

```
GET /assets/js/compiled.min.js HTTP/1.1
Referer: https://www.example.com
Cookie: XSRF-
TOKEN=eyJpdiI6InJ2UjldQXNlRUFPRGs4bVJkT29YaFE9PSIsInZhbnVlIjoiY25IRzdXak1RMUg4bmKZzNRcmp0Y1NUT3lQU
mZuWmFVRlJJWWNTcU5lYy9jRXIyTlozejIybzA4MjlrUl4UjYk4Zjlsckl2YkM3dUtaOSs2WWxMZHBjMVhrQTVVCZDdNemZ2ckhZ
S0pYbzZoa2taeTdkOUwvR1NDNct1Y2ozTXUiLCJtYWMiOiJjMTkyNjYyU2MzU1ODAlZDc3ZmJkYjhmMzZhY2JhNmIyYmU2ZTJ
jNGIwMjE5OTc5NGM1ZjNkZWEMzRhNDhkIiwidGFniIjoiIn0%3D;imikrofv4_session=eyJpdiI6IlpSblAwaUw5aDBRZWxHV
Tg1OGZTaE9PSIsInZhbnVlIjoiEJCVMVM5Ky8vRU1BSGdMdTAyV0p6ZFlqRmFSQVRsQ1JFV0FrM1NTbDFycnRWelpURVZFdVJC
UGQrWWFXVHVtMEFKZ2FGZDc5QS9zSWtvcHlraZkODRUajE0dzRTNDhBK0g0dUpBNk10QmlWYXc4d1RCS2ZQcVdtM2c3TVVOUTU
iLCJtYWMiOiIwZGYzOTkwZjU1YWJjYTJkMTljMDU3ZWYyM2U5YWQ5NTRmMDVlNzczMmM2ZjI3YzBkNTQzMmMxZDIwYmVjZGRlIi
widGFniIjoiIn0%3D
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/83.0.4103.61 Safari/537.36
Host: https://www.example.com
Connection: Keep-alive
```

## Recommendation

Upgrade to the latest version.

# Clickjacking: X-Frame-Options header missing

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.

## Impact

The impact depends on the affected web application.

<https://tim-familief.com/>

Paths without XFO header:

- [https://tim-familief.com/reports/month\\_wise/](https://tim-familief.com/reports/month_wise/)
- <https://tim-familief.com/reports/>
- <https://tim-familief.com/reports/mra/>
- <https://tim-familief.com/reports/mranbd/>
- <https://tim-familief.com/assets/css/images/>
- <https://tim-familief.com/assets/img/glyphicons-halflings-white.html>
- <https://tim-familief.com/assets/img/glyphicons-halflings.html>
- <https://tim-familief.com/assets/css/assets/images/>
- <https://tim-familief.com/assets/img/>
- <https://tim-familief.com/assets/css/assets/>
- <https://tim-familief.com/advance-due-register>
- <https://tim-familief.com/member-migration-balance>

## Request

```
GET /reports/month_wise/ HTTP/1.1
Referer: https://tim-familief.com/reports/month_wise/
Cookie: XSRF-
TOKEN=eyJpdiI6Ilp4WTRSnbnMYVkb3OFJzaTZ2b2hzcEE9PSIsInZhbnVlIjoicXhXK1BTWVhGS0x5S1VDejBMQU92ZFBlE1kR
UJYcjZuQWZlS3grZG52UEpPZTVybFNUcFhMMkRMK2paQVJmclUrV0xEcHAXRjdodmp3ZzIwVzlhUm1JQ1hzODZRYUV5emUxUWNj
ZFdUcUpjTW4rc0hNTXZodm1BRWlSSUcrZm0iLCJtYWMiOiIzZGI5MWRkZjRhODgyNDU4ZDExOTNmMzRiZTkxMzg4MzJmZDZmYmM
0YTMzMzQwYjg0NDZmZjYjOGU1YWFjMGEyIiwidGFuIjoicXhXK1BTWVhGS0x5S1VDejBMQU92ZFBlE1kR
nNndjNHM3c9PSIsInZhbnVlIjoicXhXK1BTWVhGS0x5S1VDejBMQU92ZFBlE1kR
```

```
RExJRfHRejN0QS85amZndXJCbGRkTytSbjJ6YlBsVWxsVFZxSVBmbU9LQlpKc0J3K1RpN00xWkVHdEJKc01iOXpVR1ZOMEJXQ20
iLCJtYWMiOiI0M2FiZWQyOWY5ZDhlOWFkN2ZkNDY4Y2FmNmRhODA0YWI1NjIyMDFlODVjZDY3MjU4NjU2ZmY3YmEwMTc4N2FhIi
widGFhIjoiIn0%3D
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/83.0.4103.61 Safari/537.36
Host: [REDACTED]
Connection: Keep-alive
```

## 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](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.

[https://\[REDACTED\].com/](https://[REDACTED].com/)

Verified

Cookies without HttpOnly flag set:

- [http://10.10.10.10:8080/](#)

Set-Cookie: XSRF-

TOKEN=eyJpdiI6IlRER3NNb0E3Rm9IMUx0bWNU0lHMnc9PSIsInZhbnVlIjoiVTdIZHpiekI4YVJpT3VWVQVg5aFVRyZjJxeHVCT3o5aFNNd2ZyTXBJQWpoOVZMRW5mV25Xckl0S1A4MzFXSDhxZU5TSzZ2MFRzeU0yUkNNAgZYOWx3VTdNTjJZalltTETyUVNzaGwrQXBDeVhGb1NFYXBIVjJmT3p5V0pxbXJEQ1QiLCJtYWMiOiIzYzFjMTE5MTI5MjdmZWYzOWRiNWYxNjFhNDVhOVRlNmYxMmM3NzFhZjA2NTk4MTYxYjUxMWVhNTFjYTBkYzkyIiwidGFuIjoiIn0%3D; expires=Thu, 08-Dec-2022 18:23:08 GMT; Max-Age=7200; path=/; samesite=lax

- [http://10.10.10.10:8080/login](#)

Set-Cookie: XSRF-

TOKEN=eyJpdiI6Ikxjc2lqejAwaTc0dFFqMWxxVks0OVE9PSIsInZhbnVlIjoiN2VrVHFpME5YTXQwV2lhWXg2S2ZNPFE5TVpYYzZmY2kreVFHMG83UnU3UVJhV0dVOXJHqkYxVUxvL3psNlVleVhMV0dPV0hVbE1MYnhqYVl3STg1YXBSUXFoVDRIQ0FVRVZGd0lteUZFYXZzSHNHAm9MNWhzTVhCTzZzbU44VGgiLCJtYWMiOiJiNjM3YjVkmjQyNTM1YzJhNGQyOTNlYjYzNjI5NjM2ZDkwYTQxNzQ5ZDQ1YjhhNTdkOGU4NTNhNTllNGM3ZTc0IiwidGFuIjoiIn0%3D; expires=Thu, 08-Dec-2022 18:22:21 GMT; Max-Age=7200; path=/; samesite=lax

- [http://10.10.10.10:8080/login](#)

Set-Cookie: XSRF-

TOKEN=eyJpdiI6ImxBQmtDVTErM0ppN2s0Z3d0a0d3U1E9PSIsInZhbnVlIjoiL2puQWcxMHB6ZGlWTnVkrZIxMGtoSUQ5dGZ0OEcx3pySjRjMlpsGS3U1UG01U3p4bkhyaTJtbHVtd3IvR2N0dXdCc1hPT0hBWTlyQ2h3di9kbDc3Tj10dCtmNlJ2OVRiTXN4OHlGNXpiRW8xZlZ3UjBlampHdW9jVU1XU2szUFAiLCJtYWMiOiI5MDFkZTIwN2M1MDUxZGF1N2M0ZDA5MzA0ODIxY2NhMzY2YmVhMGVhMGVhNDVmNTRlMWZiYjYk0MjQxYWNlNzQwIiwidGFuIjoiIn0%3D; expires=Thu, 08-Dec-2022 18:26:36 GMT; Max-Age=7199; path=/; samesite=lax

- [http://10.10.10.10:8080/login](#)

Set-Cookie: XSRF-

TOKEN=eyJpdiI6ImxPckp4YTBHV2luOWVxcUVGZy9YQ1E9PSIsInZhbnVlIjoiSFVYy1NvMXE4OEhWYWJlBWZSby95SnNZekxPckx0R0NMUDA0RnRjaUhlQyt6MENsMTFDbXlaS2RBYnpHY3IyR28rNGtYcWtGL3VPTU5vSG5vc2E1SzZxMkFXZXhKM2l5NWhrQzJNS2xHOVB5ejhmMhJDR0x6eks2aFdsWFhjSlIiLCJtYWMiOiI0NTAxYjc2MGNkYTgxMDQzNDA5MzMlODlkZjc1NWNmMzA5YTE0ZDQ1YmY3NDJiNTJjMzBjN2Y1N2UyMmY5YzY0IiwidGFuIjoiIn0%3D; expires=Thu, 08-Dec-2022 18:22:21 GMT; Max-Age=7200; path=/; samesite=lax



- [/or\\_log/have\\_error](#)

Set-Cookie: XSRF-

TOKEN=eyJpdiI6Ik8ySTNMMHJpSmpjUjg3YlBxN2VPTmc9PSIsInZhbnVlIjoiaFd6bjFXendEUKRiZVJYdFcyL0pPbU5pRWxaeUdoTGJvRWpvcjBUeEJKT0hwcncZmbVc5ckxWNm9MdDdwYkVLbm52UUZwSXVBUG9ZSllOc3M1MG1TTC9TUFZRQm5xYTVJZEZFM1lTOHkyUGFXVDBFbmJlZXFTeEVlVitWWGlJTjkiLCJtYWMiOiJlZTkzNDhhNGJiNjVhNzBkYzBmYzE5OWY0NDU5MGFiNzc4NTA4ODJhYmQxODU4NDNiNjZjNzZkOGM1NTI0NDM4IiwidGFuIjoiaW0%3D; expires=Thu, 08-Dec-2022 18:33:20 GMT; Max-Age=7200; path=/; samesite=lax

- [/n/](#)

Set-Cookie: XSRF-

TOKEN=eyJpdiI6IkdhRGQ5ZlFIWEN5bWtFKzdjbkpUeFE9PSIsInZhbnVlIjoiaSm9Mc093c0pQSHVMM2ExaEtkUWVHYkJRT2xTNkdRU0hmNGtZN09DOFFhS2l6QmJwNHR0ZU15ZFpMZ3Y0U2wyM01NbKp2Y2loTi9nVG12ak9jdGE5RkJKR2Uwenl6SHdqNET3M0NhaklXNlZ2WW1ZU0wydmNrRVhCSXZ2anZYXxiLCJtYWMiOiIzZGVmMGRhNDZjYWNhNDVmNWl4NWE4ZDQ4OTg5OTJjYjk5Yjg5NDViYTVhNTg2MTA5ZTY5Y2Q2OTk2MDkwMjRiIiwidGFuIjoiaW0%3D; expires=Thu, 08-Dec-2022 18:34:54 GMT; Max-Age=7200; path=/; samesite=lax

- [login](#)

Set-Cookie: XSRF-

TOKEN=eyJpdiI6ImloQ09YOUc0K0cxRm56bzZ5V1hrUnc9PSIsInZhbnVlIjoiaQVBWSFF4d3QrMWh6YWc5RUxvRlhqRXQ3cXViWFJoMzk4WDJ3L3VtMnN0V0J2TXBuNmQzSHV5clpaNys5OWxYU3pxck5zZ0xLNUd3WnVoOGJBBeW4RVp4TUJWwnNZOXQzVjdwNis3c0hHWnQzckxyOSTpY0g4ZmRrNWVQUlhvbEUiLCJtYWMiOiI3NTUwMjIyYmRjYzA1OGYwOTgwMGZhMGQ4ZDY3NDJkYzZjZjVhNzg0OTYxMTc3YTYxMGViYmU3NTc1MTRmMTlkIiwidGFuIjoiaW0%3D; expires=Thu, 08-Dec-2022 18:26:14 GMT; Max-Age=7200; path=/; samesite=lax

- [thlyTarget](#)

Set-Cookie: XSRF-

TOKEN=eyJpdiI6IldyT2lqMG1IQVBQVDBGWHhueHBHOVE9PSIsInZhbnVlIjoia3EwRVluMlF6dWpBK3Rmc3Q3V3pXV2FNcEs0eHdPeWJ6RzNUU2YrcG1WVjN4Um13cnIyNmMwMUQ1VG5EQkFrY01VaTZOOTZRbTlwMVp6OW5lLzVmRFdlNjVDWGFmbnVNZk1iRURRdE5vTkxDai9aUm9TbWFySVJGVmw4ZytvUlIiLCJtYWMiOiI5YTZmZGZlYjlyYjM5NDZhZmJmZmUwZGVmMjUxOGZhNjdmNmM2NjI5Y2U5Y2Q2YzU5NzU4MDE4ZWYwNzk1ZGUyIiwidGFuIjoiaW0%3D; expires=Thu, 08-Dec-2022 18:34:58 GMT; Max-Age=7200; path=/; samesite=lax

- [http://10.10.10.10/AIS](#)

Set-Cookie: XSRF-

TOKEN=eyJpdiI6Iko4Ny90Ti9sODB3ZXlpNXRSeXcvcm9PSIsInZhbnVlIjoiVS9LRnA0QzU0VC9TTm1UZ0JZa3VsVzE5OFZreXVWZlF5QmV2OGdhcHM3N2NybjM0UGZFeDlNaG53SjZjTlA0cEQ1QmswbURibWpiaGErckYvd3BxbUc1bTBldHh2cGRka1ZUcnU3L3BuM3hyY2cyOG10VG4rZ1B4WG1YeHRGNi8iLCJtYWMiOiI2M2ZmZTA1YTQ0OTUyMDY1ODMwYjNiOGJiOGQ0NzA5YTU5OTUzODFhMmFhNTMyMmUxOTAYNzVmYTg1MjJhMTk5IiwidGFhIjoiIn0%3D; expires=Thu, 08-Dec-2022 18:36:25 GMT; Max-Age=7200; path=/; samesite=lax

- [http://10.10.10.10/session\\_register\\_report](#)

Set-Cookie: XSRF-

TOKEN=eyJpdiI6IldreGtyNnFkYTF2ZGhZa2dPUjY2dkE9PSIsInZhbnVlIjoiEYZS9UVGVlRlZBRHBtdG5hWCtRWkZ2amlxR0RNQmRfbk2amFRcm1vRmQ4VmE1TTF3V3lIdWhMcDZKeUFWdGRYb0pxczlQcnVCaHRTVUhZzEZjYUpUMG5oQldrUUxxbUtVTk10RnFdaURiVFBaMUtSdEpHQ243d0xJVWVEEdXQiLCJtYWMiOiI5NzljMzNlNzViNDc2N2U2NWJmZjUzYmQwN2JmMThmNTg1NTQyMGFiOGM4M2VkMzA2NjBlNDYwOGNiZmI4ZjU4IiwidGFhIjoiIn0%3D; expires=Thu, 08-Dec-2022 18:36:25 GMT; Max-Age=7200; path=/; samesite=lax

- [http://10.10.10.10/RebateRegister](#)

Set-Cookie: XSRF-

TOKEN=eyJpdiI6InVlN2JRcmRqUnVKK1l5RG5DcWRhbGc9PSIsInZhbnVlIjoidHVIdkpwZeGNvTkVLMFNvZ2pOK0Riend4dUttOFhVSFNUmu5FZ0xWZ3JaNU5RVGIvT29NSUJHZGxyYnFVTk1lWWFGexl4bml2ZnlmQitIR2ZzN2Q1ZklUaXVPSH1Tzm85Z0F0TUdKbUpuWGw2czlLMk50a0R2ZkdRdGNyUnh4QXEiLCJtYWMiOiI3NjY3M2UyNjg5MDA5NGExNjZhMGYwMzk5NjM0YmZmOGRjOTM5ODMwMmIwNDIzNjc0NTkxMmNhZmI5NTEzZTlhIiwidGFhIjoiIn0%3D; expires=Thu, 08-Dec-2022 18:36:46 GMT; Max-Age=7200; path=/; samesite=lax

- [https://10.10.10.10/awslas\\_ledger](#)

Set-Cookie: XSRF-

TOKEN=eyJpdiI6InEwWXlCaUJpZUzmZTJpMFNScDl2UEE9PSIsInZhbnVlIjoiUlRYVUp1MGRFQld5ZkRBZyZFKaHRMUEsxM0w5VnNwTzdIdEVrMkNlKzRkbGhESy9VRUVxTzRPa09UU3JkZ2lYNXM4YU8yVlJnZXEvUTRpL3d0anzGcEVZK0NhK0F3OEhWek94NGQyUHNCR0ZGN1k4U3Z0dnpZN1BUZitsNVBtWGEiLCJtYWMiOiI5ZTgzMGMyZTYzMzlmNjYyY2E5MDJlMDIwNGU4MWJlZjhhN2U0MDYwYTazZTdhdNDYzYmY3Mzk2MWE0Njk4MWQ4IiwidGFhIjoiIn0%3D; expires=Thu, 08-Dec-2022 18:36:47 GMT; Max-Age=7200; path=/; samesite=lax

- [http://10.10.10.10:8080/voc\\_register](#)

Set-Cookie: XSRF-

TOKEN=eyJpdiI6ImZnMnk0UVpIT2h3NlNaamtGYy81L3c9PSIsInZhbnVlIjoiMEMyUWF6RHY0VGNUMk  
k4UDRCUzdDNzJnNnlyaGk0Y0JaRHBINXd5V3kyTzRuT0w1Q3pPV0kyRExtUS9lcHE1WmxxV3VDM2lrcn  
ZBaStzRzlxYm5tOFVGc29aRGtxOWhiUGlqZUh4c09NNFJQZWpFOXlYN2Vyd1hUSHdFYnlaNXciLCJtYW  
MiOiIzMTYwZGU3ZGRhNGRkYjg3YzczNWFiNjAzYjQwOWVjM2UyNWJmMzk2YzlmNzBiMTk1YTMzY2RkND  
YxOWZiZDNmIiwidGFuIjoiIn0%3D; expires=Thu, 08-Dec-2022 18:37:02 GMT; Max-  
Age=7200; path=/; samesite=lax

- [http://10.10.10.10:8080/pbb\\_register](#)

Set-Cookie: XSRF-

TOKEN=eyJpdiI6ImJXdn9leTBIVFhqZjFYZ2V0Q1lNNHc9PSIsInZhbnVlIjoiWlpwNnYrUHI4TlhKWF  
ZERGRLaHBxQUJGamszMTltWFRuSkNVaTMvTVFjb1ZIditsSDIzczkzWVRyYbWxJYnlYeW8wYXZ3MjJvZl  
VkK1cyM2lXcmVKTWRFeEp0VXZlVHhZrZCtpMTlHOTN2WkJEZmdoUlhEaVpha0dzSjJmY1hvVjUiLCJtYW  
MiOiI3OTlkMWIzOWJjZDNhYjNiNzg0MzliZjg1NDEwNjk4N2VhMTM2MTAwNjNmZDVjMTY4YTQ1ZjAxZW  
JhMdBhNzMyIiwidGFuIjoiIn0%3D; expires=Thu, 08-Dec-2022 18:37:03 GMT; Max-  
Age=7200; path=/; samesite=lax

- [http://10.10.10.10:8080/permission\\_role](#)

Set-Cookie: XSRF-

TOKEN=eyJpdiI6ImV6OXVCeIN2ZUdRYlBFUW5FSVkvN3c9PSIsInZhbnVlIjoiYjNzZ3M1RXBlUUkzb0  
F1Y0doRFAxbVRPUG1pYTZTbXNjMkVDUHR2a3BRbkZVZ2c4ZHRlU2RwNkxXWVhaVHBPR0xNeHRyUUxrdn  
FIM0JGSDlTSSsreE96K2xhdmZvSjdWdlNrSkZQejk5YzZyUzFOSVfhVzViQTdSNGhJUDVjRGoiLCJtYW  
MiOiIwNThjM2RlMGY5YzY0ZjY4ZTEzNDU4NGJlMWFhNTcxZGNjYzdhZGJmImJhYjY0ZjY4ZTEzNDU4  
VjNjQ5MTk4IiwidGFuIjoiIn0%3D; expires=Thu, 08-Dec-2022 18:37:04 GMT; Max-  
Age=7200; path=/; samesite=lax

- [http://10.10.10.10:8080/ports/mra/mrallp-6](#)

Set-Cookie: XSRF-

TOKEN=eyJpdiI6IitmanZhZFZud1lhdEdYRGRJVGJIVGc9PSIsInZhbnVlIjoiQ0NQZmlONkxkMnlSVn  
hSRUo1UkNWaVVBkbHuzL1FjWXJ4WGxrTDVhRnNXT0JORKZUa3VLd3FHbj1FOGJPb055ZWFCWGdpK3NuL3  
kxTk9RYUR3RWpYUkNjdE1HL1o5bERwUmdkcmlqa0diMFRzNXlkeEQyWWEyL2xVUStXTnBxRjEiLCJtYW  
MiOiJiNTdkZDg4NWJjYTZjMzEyZWYyViOWNlMTgwYjU0NTQ0MDEwYjhiOWY4NGNhZWU5MWIyYzVmMz  
k0ZTZiY2Q5IiwidGFuIjoiIn0%3D; expires=Thu, 08-Dec-2022 18:37:30 GMT; Max-  
Age=7200; path=/; samesite=lax

- `/usr/share/ansible/roles/ansible-role-ansible_`

Set-Cookie: XSRF-

TOKEN=eyJpdii6IkFHTWp6NWZlZnpGRtV2d0VhYjc2d0E9PSIsInZhbnVlIjoiaai9iVjBxYlM2di9lV0gwK2RaSEXaNklzTnB5RXpqMU43a3pYUTd5WVdIQTdUjEybenPtJg4VjBPdWZjakFwWllGeWVEM3pFT3kzWE9iQnV3UkJ2alJoMUVVZGgydzBaWlg3cERSZ2Rbc2JiZlZUZ0lmZUQvR25Xd2Jrc3lhN3ciLCJtYWMiOiILOWYZyji3OWIxYWE5NWYzYjYwJmGE1NGE3YjY4MmI0NzcXNzVjOGVkNjclYjBhNGE1NjkwYjI4YWU4OTg2Y2M2MTQzIiwidGFniJoiIn0%3D; expires=Thu, 08-Dec-2022 18:37:30 GMT; Max-Age=7200; path=/; samesite=lax

- [\[redacted\]m/](#)

```
Set-Cookie: XSRF-
```

TOKEN=eyJpdiI6IkRCWC9qR3p6SEhkWXQ4OUtyK1BRTkE9PSIsInZhbnVlIjoiYklyYXNRS0YxY1IjSHFaMEednesS82bVpXdFc5TjFCYlEYeUZjbmVaVGEwVm1HbVRVQk1NWkwxNEtFaGZMc2Q1dlBtTnRyYURPNmV3bnB4NGFEemhlU0J0cjB2ZFwcEswcHpkK2V2Q3hsbE5SS1RHNHU3RTBIMlFHWkpTalRjOEUiLCJtYWMiOiJjMjZhZDVlZDM5YmRkOTA1ZDAyNDZlMmQwNjdkOTdiNW11ZTY3ZGNhOTRiMWEwNjFmMzJjNjRiOTE0NWZzNTAwIiwidGFnIjoiIn0%3D; expires=Thu, 08-Dec-2022 18:39:09 GMT; Max-Age=7200; path=/; samesite=lax

- `Component_Wise_Daily_Collection`

Set-Cookie: XSRF-

TOKEN=eyJpdiiI6Ij1lFUmMra1lFfbzhFaDBMUecvRXpheVE9PSIsInZhbnV1IjoiMUZHU3VyTHkyRGJMTk  
pNSDVGbm1KUURxQVZPcjNyNXpDMit5Si9iUHlib1cwK2lvbEJocDVGUxBEY1VJdTNPmFFHOv1HYVFveV  
RsamdsTFZwC0VOZ3pxSE00aGsxY1l1b3clenVra1lDekZUUGUvSFQrVk5tL0wwc0JwVGs3enUiLCJtYW  
MiOiI0NmZmZTBjN2EzNzcxNmE5YzE2MmVlN2U2ZmE3ZGU3ZTdhNWlYzTc0ODEwMjViMGZiZjFmMmVkNT  
AzNDNhZTQwIiwidGFnIjoiIn0%3D; expires=Thu, 08-Dec-2022 18:39:11 GMT; Max-  
Age=7200; path=/; samesite=lax

- [\[redacted\]error\\_log/](#)

Set-Cookie: XSRF-

TOKEN=eyJpdiI6ImQ4Z2wmg45TU5iT1VobU04WUNDN1E9PSIsInZhbnVlIjoioUZYy11SenA2dEU0Y1ZKQThlM0RGSVkdZklUSEV3Y1psdFJ2YURxN3RuL2lyV2ElL1g1TDU5NHJZOU9Kdm51WlVMZOU2MWZSUfJvZm1UaW1VWlo3NHhnOE2RnFGNTI0anVOOFcl3czT05oNFQrbjJXRmJ4VVG2UGtLdXNtenciLCJtYWMiOiIyYzJkNjUwOTVmMzk4Y2QyNzcxMDdkYjg3ZmElNjcwZTgyNmQwNGI1ZGIxOTg5M2FlMjRmNWU4MWMQ1YjExZTZkIiwidGFniIjoioIn0%3D; expires=Thu, 08-Dec-2022 18:39:11 GMT; Max-Age=7200; path=/; samesite=lax

- [https://www.wisecoders.com/ports/mranbd/branch-wise-saving-info](#)

```
Set-Cookie: XSRF-  
TOKEN=eyJpdiI6IlgzWWlKQlp1MjR3c24ydDJBaE56dGc9PSIsInZhbnVlIjoiUFNlWjJ2amE1MXFXNF  
YrWXlCNndQVUY1ZjN4b25yME9rVU96aWxkTGxLbmtINm1nQWZEOTI2M3dJTU9kM0xlUGxuQmc3TTZiRD  
R6RFRnRQUpNS3h2N0ZxRHVMS0Z0aS9LRm5qTC9tbEUxTE00WEwPb09GRkpGOXZxVjRBekprajIiLCJtYW  
MiOiI3MjBhZWUxYmMxMDJmNTdhMzI2ZjI4NjM3MDU5YTIxNDExYjM0MDNiYTEwNWQ1MTUyNmQ5YzZM5OD  
c1NDhly2RlIiwidGFniIjoiIn0%3D; expires=Thu, 08-Dec-2022 18:40:43 GMT; Max-  
Age=7200; path=/; samesite=lax
```

## Request

```
GET / HTTP/1.1  
Referer: https://[redacted]  
Cookie: XSRF-  
TOKEN=eyJpdiI6ImxPckp4YTBHV2luOWVxcUVGZy9YQ1E9PSIsInZhbnVlIjoiSFVYy1NvMXE4OEhWYWJlZWZSby95SnNZekxPc  
kx0R0NMUDA0RnRjaUhlQyt6MENsMTFDbXlaS2RBYnpHY3IyR28rNGtycWtGL3VPTU5vSG5vc2E1S2ZxMkFXZlZlODk1NWhrQzJN  
S2xHOVB5ejhmMhJDR0x6eks2aFdsWFhjSlIiLCJtYWMiOiI0NTAxYjc2MGnkYTgxMDQzNDA5MzM1ODlkZjc1NWNmMzA5YTE0ZDQ  
1YmY3NDJiNTJmZjN2Y1N2UyMmY5YzZ0IiwidGFniIjoiIn0%3D; imikrofv4_session=eyJpdiI6IjdFVVpxK29HelpMMnpkO  
WhQQUZTN1E9PSIsInZhbnVlIjoiZ2R2elZKYkNXL3RZzkpHVzQ4cXJLZmlrZlF3SS9IK0FhMURpN1N5OE9KVzc3cUxWclM2aXpS  
bEVRaFUrWGx1RUxWL3Q3RDZStm5vMW41NiswOUJa295R2xXS3E4cXpEM1hxQlorWnB6VVVFVkdQvV0orOXZQWEw5WUs3Z0E5U0w  
iLCJtYWMiOiJhY2ZkNTBhZjBkNjJiZmM3ODAlMjFjZDIzNTF1MjIwZDZmZiYwQ3NWZmOGRmOThlZmYwZjU5YmFiODMyNTlmIi  
widGFniIjoiIn0%3D  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8  
Accept-Encoding: gzip, deflate  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)  
Chrome/83.0.4103.61 Safari/537.36  
Host: [redacted].com  
Connection: Keep-alive
```

## Recommendation

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

# Cookies without Secure flag set

One or more cookies does not have the Secure flag set. When a cookie is set with the Secure flag, it instructs the browser that the cookie can only be accessed over secure SSL/TLS channels. This is an important security protection for session cookies.

## Impact

Cookies could be sent over unencrypted channels.

Verified

Cookies without Secure flag set:

- [https://\[redacted\]](#)

Set-Cookie: XSRF-

TOKEN=eyJpdiI6IlRER3NNb0E3Rm9IMUx0bWNU01HMnc9PSIsInZhbnVlIjoiVTdIZHpiekI4YVJpT3VWQVg5aFVRYzJxeHVCT3o5aFNND2ZyTXBJQWpoOVZMRW5mV25Xckl0S1A4MzFXSDhxZU5TSzZ2MFRzeU0yUkNNaGZYOWx3VTdNTjJZalltTETyUVNzaGwrQXBDeVhGb1NFYXBIVjJmT3p5V0pxbXJEQ1QiLCJtYWMiOiIzYzFjMTE5MTI5MjdmZWYzOWRiNWYxNjFhNDVkdWRlNmYxMmM3NzFhZjA2NTk4MTYxYjUxMWVhNTFjYTBkYzkyIiwidGFuIjoiIn0%3D; expires=Thu, 08-Dec-2022 18:23:08 GMT; Max-Age=7200; path=/; samesite=lax

- [https://\[redacted\]](https://[redacted])

Set-Cookie:

imikrofv4\_session=eyJpdiI6IkhlLVVNpU3pIRTZ2Ymo5MlhBYzFvc0E9PSIsInZhbnVlIjoiN1luUShtNa2xRWFaxNm9Rb2N6clovdTdsOWVkd1ZQTfc3NGdEOS9OdHZXTETzPeGVoYi9TOFJrNks5OUdXdnJzMXh3dWdXRlVpM1ltSnJ2a28xQk02N3pxeHVzYU92YkZFTW1Cdnc5VWE0Zk5KMkU1a3hjZWNYanhNT3pzN05hRksiLCJtYWMiOiI2YjMzMmEwNmM2ZmIyNWQwNzRjZmE2ZDVhMjk0NGRmNGFkMmIxODM3OTRlZTUwNmI1ZmYzNzBlOTM4OWZjZjQxIiwidGFuIjoiIn0%3D; expires=Thu, 08-Dec-2022 18:23:08 GMT; Max-Age=7200; path=/; httponly; samesite=lax

- [https://\[redacted\]](https://[redacted]) login

Set-Cookie: XSRF-

TOKEN=eyJpdiI6Ikxjc2lqejAwaTc0dFFqMWxxVks0OVE9PSIsInZhbnVlIjoiN2VrVHFpME5YTXQwV2lhWXg2SzNPRFE5TVpYYzZmY2kreVFHMG83UnU3UVJhV0dVOXJHQkYxVUxvL3psNlVleVhMV0dPV0hVbE1MYnhqYVl3STg1YXBSUXFoVDRIQ0FVRVZGd0lteUZFYXZzSHNHAm9MNWhzTVhCTzZzbU44VGgiLCJtYWMiOiJiNjM3YjVkJyNTM1YzJhNGQyOTNlYjYzNjI5NjM2ZDkwYTQxNzQ5ZDJlYjhjNTdkOGU4NTNhNTllNGM3ZTc0IiwidGFuIjoiIn0%3D; expires=Thu, 08-Dec-2022 18:22:21 GMT; Max-Age=7200; path=/; samesite=lax

- [https://\[redacted\]](https://[redacted]) login

Set-Cookie:

imikrofv4\_session=eyJpdiI6Im0xWGtUaDlJQ1lQYnByV2xXSjYVE9PSIsInZhbnVlIjoiYjA5aEt5RWJnbjhDa2VHWGNvbWEyZmJWbS9IZlBQZzEwMHVCrWNxcWdOSzFRYm55TU1wcFlvUTEwMjFjXDM5nZnpGNm

wxeWhzYkJ1U1lZUVprVlVsU283YjRHOGtYODlKeUpVbzRPUy9sVzVLby9yMHBldW82M05YsFQ0bjNvOG  
s1dlkiLCJtYWMiOiIyNjM5Zjk5YjJlNmM5Njc1ZTdhdVlNzFlZmU1Njg0NjM5OTdiYTk0MmZkM2ZjYm  
VlZTk5NGQ4NzgxYTZkMzU3IiwidGFnIjoiIn0%3D; expires=Thu, 08-Dec-2022 18:22:21 GMT;  
Max-Age=7200; path=/; httponly; samesite=lax

- [https://\[redacted\].com/login](https://[redacted].com/login)

Set-Cookie: XSRF-  
TOKEN=eyJpdiI6ImxBQmtDVTErM0ppN2s0Z3dOa0d3U1E9PSIsInZhbmHVlIjoiL2puQWcxMHB6ZG1WTn  
VkRzIxMGtoSUQ5dGZ0OExWc3pySjRJMlpGS3U1UG01U3p4bkhyaTJtbHVtd3IvR2N0dXdCc1hPT0hBWT  
lyQ2h3di9kbDc3Tjl0dCtmNlJ2OVRiTXN4OHlGNXpiRW8xZlZ3UjBlampHdW9jVU1XU2szUFAiLCJtYW  
MiOiI5MDFkZTIwN2M1MDUxZGF1N2M0ZDA5MzA0ODIxY2NhMzY2YmVhMGVhMGQ1NDVmNTRlMWZiYjk0Mj  
QxYWNlNzQwIiwidGFnIjoiIn0%3D; expires=Thu, 08-Dec-2022 18:26:36 GMT; Max-  
Age=7199; path=/; samesite=lax

- [https://\[redacted\].com/login](https://[redacted].com/login)

Set-Cookie:  
imikrofv4\_session=eyJpdiI6IklaMzNIRitGcjEwWELYZW54UVhSYke9PSIsInZhbmHVlIjoiVpFel  
VablNCWms3YmpSNHpyYjkwUEJJRml5YmVXbFpSTElizZnsdG8vTkE4a0FZWmJ3d1cwVi9xUzlxZUxOTU  
9vQ3EzV2NIYnQ3S1A3VFhocUNJZVY4OWtvbzcxNVd1V0Q1MXpzT1d3ZlY3OTRETGt1WG9jbjk1Y1k5dF  
RZUnIiLCJtYWMiOiI3YWRiODYyYjQ0MDc5MGUyOTJlYjYk2NWU1YmQyODcyNjNmNTVhMWE5NWY2MGJhND  
FiZmU4MmU5MmZkNTlmZGIzIiwidGFnIjoiIn0%3D; expires=Thu, 08-Dec-2022 18:26:36 GMT;  
Max-Age=7199; path=/; httponly; samesite=lax

- [https://\[redacted\].com/home](https://[redacted].com/home)

Set-Cookie: XSRF-  
TOKEN=eyJpdiI6ImxPckp4YTBHV2luOWVxcUVGZy9YQ1E9PSIsInZhbmHVlIjoiSFVYy1NvMXE4OEhWYW  
JlBwZSby95SnNZekxPckx0R0NMUDA0RnRjaUhlQyt6MENsMTFDbXlaS2RBYnpHY3IyR28rNGtYcWtGL3  
VPTU5vSG5vc2E1S2ZxMkFXZlZkM2l5NWwhRzQJNS2xHOVB5ejhMdHJDR0x6eks2aFdsWFhjSlIiLCJtYW  
MiOiI0NTAxYjY2MGZkYjY2MDQzNDA5MzA0ODIxY2NhMzY2YmVhMGVhMGQ1NDVmNTRlMWZiYjk0Mj  
UyMmY5Yzc0IiwidGFnIjoiIn0%3D; expires=Thu, 08-Dec-2022 18:22:21 GMT; Max-  
Age=7200; path=/; samesite=lax

- [https://\[redacted\].com](https://[redacted].com)

Set-Cookie:  
imikrofv4\_session=eyJpdiI6IjdFVVPxK29HelpMMnpkOWhQUZTN1E9PSIsInZhbmHVlIjoiZ2R2e1  
ZKYkNXl3RZzKpHVzQ4cXJlZm1rZlF3SS9IK0FhMURpN1N5OE9KVzc3cUxWclM2aXpSbEVRAfUrWGx1RU  
xWL3Q3RDZStm5vMW41NiswOUpJa295R2xXS3E4cXpEM1hxQlorWnB6VVVfVvKQvV0orOXZQWEx5WUs3Z0

E5U0wiLCJtYWMiOiJhY2ZkNTBhZjBkNjJiZmM3ODAlMjFjZDIzNTFlMjIwZDZhM2ZiYWQ3NWZmOGRmOT  
hlZmYwZjU5YmFiODMyNTlmIiwidGFnIjoiIn0%3D; expires=Thu, 08-Dec-2022 18:22:21 GMT;  
Max-Age=7200; path=/; httponly; samesite=lax

- [https://\[REDACTED\].com/login?have\\_error](https://timf.imikrof.com/login?have_error)

Set-Cookie: XSRF-  
TOKEN=eyJpdiI6Ik8ySTNMMHJpSmpjUjg3YlBxN2VPTmc9PSIsInZhbnVlIjoiaFd6bjFXendEUKRiZV  
JYdFcyL0pPbU5pRWxaeUdoTGJvRWpvcjBUeEJKT0hwcNzmbVc5ckxWNm9MdDdwYkVLbm52UUZwSXVBUG  
9ZS1lOc3M1MG1TTC9TUFZRQm5xYTVJZEZFM1lTOHkyUGFXVDBFbmJlZXFTeEVlVitWWGLJTjkiLCJtYW  
MiOiJlZTkzNDhhNGJiNjVknzBkYzBmYzE5OWY0NDU5MGFiNzc4NTA4ODJhYmQxODU4NDNiNjZjNzZkOG  
M1NTI0NDM4IiwidGFnIjoiIn0%3D; expires=Thu, 08-Dec-2022 18:33:20 GMT; Max-  
Age=7200; path=/; samesite=lax

- [https://\[REDACTED\].com/login?have\\_error](https://timf.imikrof.com/login?have_error)

Set-Cookie:  
imikrofv4\_session=eyJpdiI6IjFtZGt0QUc3Q1YvSWFWQWhTVjRlZlE9PSIsInZhbnVlIjoiaY3J4Y0  
dTMXE1cFMxZz1DYzVxbEMwU25PbWtDTzVONlNISWIwQnBWZmRLWm5FNDE3ODh4QlppSzdNaTU3dzd5bn  
lqV2NXUUtIbWxRU2piSVhkSWJKblc4SHRUv1ZqQWxITW9QQkx0a3JyMWIyZnVRNHJieThURDRoMwdlL0  
pxNW0iLCJtYWMiOiI1YThhNGVlOTBkMzA2NjU2NTQ2MWEwNmNjZmQ5OTkzMzQ4ZTFiYWQwYmE5ZGQwMm  
RkYzAyNGQ0ZmRhODglZGM5IiwidGFnIjoiIn0%3D; expires=Thu, 08-Dec-2022 18:33:20 GMT;  
Max-Age=7200; path=/; httponly; samesite=lax

- [https://\[REDACTED\].com/](https://timf.imikrof.com/)

Set-Cookie: XSRF-  
TOKEN=eyJpdiI6IkdhRGQ5ZlFIWEN5bWtFKzdjbkpUeFE9PSIsInZhbnVlIjoiaSm9Mc093c0pQSHVMM2  
ExaEtUWVHYkJRT2xTNkdRU0hmNGtZN09DOFFhS2l6QmJwNHR0ZU15ZFpMZ3Y0U2wyM01NbKp2Y2l0Ti  
9nVG12ak9jdGE5RkJKR2Uwenl6SHdqNET3M0NhaklXN1Z2WW1ZU0wydmNrRVhCSXZ2anzYXXIiLCJtYW  
MiOiIzZGVmMGRhNDZjYWNhNDVmNW14NWE4ZDQ4OTg5OTJjYjk5Yjg5NDViYTVhNTg2MTA5ZTY5Y2Q2OT  
k2MDkwMjRiIiwidGFnIjoiIn0%3D; expires=Thu, 08-Dec-2022 18:34:54 GMT; Max-  
Age=7200; path=/; samesite=lax

- <https://timf.imikrof.com/>

Set-Cookie:  
imikrofv4\_session=eyJpdiI6IkwlU2VwWHpEK0U2aTRvd0RXyUZXMke9PSIsInZhbnVlIjoiaVFpuZm  
pSODMzYnNoOF1XZERPOUthTGoxeHRiVU9sK0JpcThHMUNHYjNTWktJaWt6UXM4REMwVTA5RHpSZz1Vd2  
xxbUxRR21XNTdxbe9rbk9xT0hQRTJ3M2xCSzdldjZCM1VvVzJxb2J4V1dwckF6cFpVOWtoR2tQMgdUYj  
Vjd1kiLCJtYWMiOiJlNGE3NTQ4MTC0ZjA0M2YwN2E0OWU5MzEwY2E5YnJBJnZyY5YTU4ODkxMGY5MGE4N2



ZlOTk3Y2Y4OWI1YmYwMGRhIiwiidGFnIjoiIn0%3D; expires=Thu, 08-Dec-2022 18:34:54 GMT; Max-Age=7200; path=/; httponly; samesite=lax

- [https://\[redacted\].login](https://[redacted].login)

Set-Cookie: XSRF-TOKEN=eyJpdiI6ImloQ09YOUc0K0cxRm56bzZ5VlhrUnc9PSIsInZhbnVlIjoiQVBWSFF4d3QrMWh6YWc5RUxvRlhqRXQ3cXViWFJoMzk4WDJ3L3VtMnN0V0J2TXBuNmQzSHV5c1paNys5OWxYU3pxck5zZ0xLNUd3WnVoOGJBBeWd4RVp4TUJWwNnZOXQzVjdwnis3c0hHWnQzckxyOSTpY0g4ZmRrNWVQUlhvbEUiLCJtYWMiOiI3NTUwMjIyYmRjYzA1OGYwOTgwMGZhMGQ4ZDY3NDJkYzczZjVhNzg0OTYxMTc3YTYxMGViYmU3NTc1MTRmMTlkIiwiidGFnIjoiIn0%3D; expires=Thu, 08-Dec-2022 18:26:14 GMT; Max-Age=7200; path=/; samesite=lax

- [https://\[redacted\].login](https://[redacted].login)

Set-Cookie: imikrofv4\_session=eyJpdiI6IlBZRTBkUjFlelFTWVBUTk5GVFkxT1E9PSIsInZhbnVlIjoiSFU3eEiwSEZoSHFY0Z5eXB0VDZmMHdGbE5GUFlITFYybWN0R0tUWkx1NUJTWfDvc05oQU04ZkFqY2FGUEVwMzdQS1YxN09CRG1sMlhqNkkvY0E5NHlNam9HUVQxZjRqZnNBStib0g2ZmU3Mi9JMmhiUVZhb2FTTis3VnRjBzQiLCJtYWMiOiJhNmU3OTA2MTc5ZDU1MzVlMTM3ZjZhNmQ3ZTYwMmFkZjc2ZWl0MzczMzI3YTU2NmVlMDlkNDEzNGNkZjUwMTNkIiwiidGFnIjoiIn0%3D; expires=Thu, 08-Dec-2022 18:26:14 GMT; Max-Age=7200; path=/; httponly; samesite=lax

- [https://\[redacted\].login/Target](https://[redacted].login/Target)

Set-Cookie: XSRF-TOKEN=eyJpdiI6IlldyT2lqMG1IQVBQVDBGWHhueHBHOVE9PSIsInZhbnVlIjoid3EwRVluMlF6dWpBK3Rmc3Q3V3pXV2FNcEs0eHdPeWJ6RzNUU2YrcG1WVjN4Uml3cnIyNmMwMUQ1VG5EQkFrY01VaT20OTZRbTlwMVp6OW5lLzVmRFdlNjVDWGFmbnVNZkliRURRdE5vTkxDai9aUm9TbWFySVJGVmw4ZytvUlIiLCJtYWMiOiI5YTZmZGZlYjlyYjY5NDZhZmJmZmUwZGVmMjUxOGZhNjdmNmM2NjI5Y2U5Y2Q2YzU5NzU4MDE4ZWYwNzk1ZGUyIiwiidGFnIjoiIn0%3D; expires=Thu, 08-Dec-2022 18:34:58 GMT; Max-Age=7200; path=/; samesite=lax

- [https://\[redacted\].login/Target](https://[redacted].login/Target)

Set-Cookie: imikrofv4\_session=eyJpdiI6InBFUjhxOTNhWDQzYlZBaXIyN2N0ZFE9PSIsInZhbnVlIjoidy85amphEgZKeVlwdzY4MTQvWmIrSHVBUMlCVVdPN1lTV1JFaHpxTi9PeWEzZC9mQmR4Z2xYc3lPbW9pQVJ5TFJ4NlZ3TFZTEHRsNGVBanVqZmZpZGVqTTNUcVpIT29TRVV4Z1gwVmNNQ2YrdG1hdDZDcDZCU2ZPVlo1aGpGaXAiLCJtYWMiOiI0MTg0MWNkYjVlMTUxZGZmN2NmYTRjMjNlNjRhZWFiNDQ5ZTIwNWExZGUxZjA3Zj

FkM2FjNTg4MzJhZjEwOWZiIiwiZGFuIjoiIn0%3D; expires=Thu, 08-Dec-2022 18:34:58 GMT; Max-Age=7200; path=/; httponly; samesite=lax

- [https://\[REDACTED\]S](https://[REDACTED]S)

Set-Cookie: XSRF-TOKEN=eyJpdiI6Iko4Ny90Ti9sODB3ZXlpNXRSeXcvcm9PSIsInZhbHVlIjoiVS9LRnA0QzU0VC9TTm1lUz0JZa3VsVzE5OFZreXVWZlF5QmV2OGdhcHM3N2NybjM0UGZFeDlNaG53SjZjTlA0cEQlQmswbURibWpiaGErckYvd3BxbUclbTBldHh2cGRka1ZUcnU3L3BuM3hyY2cyOG10VG4rZ1B4WG1YeHRGNi8iLCJtYWMiOiI2M2ZmZTA1YTQ0OTUyMDY1ODMwYjNiOGJiOGQ0NzA5YTU5OTUzODFhMmFhNTMyMmUxOTAyNzVmYTg1MjJhMTk5IiwiZGFuIjoiIn0%3D; expires=Thu, 08-Dec-2022 18:36:25 GMT; Max-Age=7200; path=/; samesite=lax

- [https://\[REDACTED\]IS](https://[REDACTED]IS)

Set-Cookie: imikrofv4\_session=eyJpdiI6IldJUzY0S1ptdFlmS0lhTVRlVG1CYkE9PSIsInZhbHVlIjoiVTNra3lDQUlmYVFSREdRSG5tUFdyb3lITmdLeVA2TW5kVEpDRVptUXFacTNJWlprNFpENUZnbDlDdkQ0bEJ5Rm1BcU5LcStFUWovanZPcDBNOTIXaytaUXdWVERNOER5cWE5SDBONHYzYXMwOFNybnU5cEcrUHpWSWl4UUVxUksiLCJtYWMiOiJiMjM0MDIyNGNhYjhlZTZkMzQ5NDU2ZDcyODM1NGQ2NjNlODcxNmZjNDVhODU5NDJhZmU4YWNlZWJiODY0YmY4IiwiZGFuIjoiIn0%3D; expires=Thu, 08-Dec-2022 18:36:25 GMT; Max-Age=7200; path=/; httponly; samesite=lax

- [https://\[REDACTED\]ster\\_report](https://[REDACTED]ster_report)

Set-Cookie: XSRF-TOKEN=eyJpdiI6IldreGtyNnFkYTTF2ZGhZa2dPUjY2dkE9PSIsInZhbHVlIjoiEZYYS9UVGVlRlZBRHBtdG5hWCtRwKZ2amlxR0RNQmRFbk2amFRcm1vRmQ4VmE1TTF3V3lIdWhMcDZKeUFWdGRYb0pxczlQcnVCaHRTVUhZzEZjYUpUMG5oQ1drUUxxbUtVTk10RnFDaURiVFBAUUtSdEpHQ243d0xJVWVEdXQiLCJtYWMiOiI5NzljMzNlNzViNDc2N2U2NWJmZjUzYmQwN2JmMThmNTg1NTQyMGFiOGM4M2VhMzA2NjBlNDYwOGNiZmI4ZjU4IiwiZGFuIjoiIn0%3D; expires=Thu, 08-Dec-2022 18:36:25 GMT; Max-Age=7200; path=/; samesite=lax

- [https://\[REDACTED\]\\_register\\_report](https://[REDACTED]_register_report)

Set-Cookie: imikrofv4\_session=eyJpdiI6IjNsMUNOdWhlK2hpKys1T1lHcFVYdEE9PSIsInZhbHVlIjoiNWV3UGFoNUUzemRjOCtGVjcrTjJaUEJtU05walR0aTg2T2Z6NEV2MnlEM3N0dEFNZ3N6bDlMNk1pcG4zZ1ZjdEZRcjNmVlZhbTBxKzlsRXR2MGNINlY2dHJvNFF0Y2NlZlFVkb1hWWktaelFZdHBHRkNwZG1jUy9lQnN2Z01vZ20iLCJtYWMiOiIyNTgxYmE3ODY3NjM3MDdmZTYwYjgwZWNiYjU0MDI5NThhNWZhNWw1YmE5ZjllOT

g5ZGMyYTQwMTEyZDg5OWU0IiwidGFnIjoiIn0%3D; expires=Thu, 08-Dec-2022 18:36:25 GMT; Max-Age=7200; path=/; httponly; samesite=lax

- [https://\[redacted\]/?eRegister](https://[redacted]/?eRegister)

Set-Cookie: XSRF-TOKEN=eyJpdiI6InVlN2JRcmRqUnVKK1l5RG5DcWRhbGc9PSIsInZhbnVlIjoidHVIdkpZeGNvTkVLMFNvV2pOK0Riend4dUttOFhVSFNU5FZ0xWZ3JaNU5RVGIVt29NSUJHZGxycnFVTkjlWWFGexl4bml2Zn1mQitIR2ZzN2Q1ZklUaXVPSHlTm85Z0F0TUdKbUpuWGw2czlLMk50a0R2ZkdRdGNyUnh4QXEiLCJtYW1mOiI3NjY3M2UyNjg5MDA5NGExNjZhMGYwMzk5NjM0YzM4OGRjOTM5ODMwMmIwNDIzNjc0NTkxMmNhZmI5NTEzZTlhIiwidGFnIjoiIn0%3D; expires=Thu, 08-Dec-2022 18:36:46 GMT; Max-Age=7200; path=/; samesite=lax

## Request

GET / HTTP/1.1  
Referer: [redacted].com/  
Cookie: XSRF-TOKEN=eyJpdiI6ImxPckp4YTBHV2luOWVxcUVGZy9YQ1E9PSIsInZhbnVlIjoiSFVYy1NvMXE4OEhWYWJlZWZSby95SnNZekxPckx0R0NMUDA0RnRjaUhlQyt6MENsMTFDbXlaS2RBYnpHY3IyR28rNGtycWtGL3VPTU5vSG5vc2E1SzZxMkFXZXhKM2l5NWhrQzJNS2xHOVB5ejhmMhJDR0x6eks2aFdsWFhjSlIiLCJtYWMiOiI0NTAxYjc2MGnkYTgxMDQzNDA5MzMlODlkZjc1NWNmMzA5YTE0ZDQ1YmY3NDJiNTJjMzBjN2Y1N2UyMmY5Yzc0IiwidGFnIjoiIn0%3D; imikrofv4\_session=eyJpdiI6IjdFVVpxK29HelpMMnpkOWhQQUZTN1E9PSIsInZhbnVlIjoiZ2R2elZKYkNXL3RZZkpHVzQ4cXJLZmlrZlF3SS9IK0FhMURpN1N5OE9KVzc3cUxWclM2aXpSbEVRaFUrWGx1RUxWL3Q3RDZStm5vMW41NiswOUUpJa295R2xXS3E4cXpEM1hxQlorWnB6VVVhVWkQvV0orOXZQWE5WU3Z0E5U0wiLCJtYWMiOiI0NTAxYjc2MGnkYTgxMDQzNDA5MzMlODlkZjc1NWNmMzA5YTE0ZDQ1YmY3NDJiNTJjMzBjN2Y1N2UyMmY5Yzc0IiwidGFnIjoiIn0%3D  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  
Accept-Encoding: gzip, deflate  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.61 Safari/537.36  
Host: [redacted].com  
Connection: Keep-alive

## Recommendation

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

# HTTP Strict Transport Security (HSTS) not implemented

HTTP Strict Transport Security (HSTS) tells a browser that a web site is only accessible using HTTPS. It was detected that your web application doesn't implement HTTP Strict Transport Security (HSTS) as the Strict

Transport Security header is missing from the response.

## Impact

HSTS can be used to prevent and/or mitigate some types of man-in-the-middle (MitM) attacks

https://[redacted]m/

URLs where HSTS is not enabled:

- https://[redacted]gin
- https://[redacted]home
- https://[redacted]
- https://[redacted]month\_wise/
- https://[redacted]ports/
- https://[redacted]ports/mra/
- https://[redacted]reports/mranbd/
- https://[redacted]ss/images/
- https://[redacted]icons-halfings-white.html
- https://[redacted]phicons-halfings.html
- https://[redacted]/assets/images/
- https://[redacted]sets/img/
- https://[redacted]css/assets/
- https://[redacted]ce-due-register
- https://[redacted]igration-balance

## Request

```
GET /login HTTP/1.1
Referer: https://[redacted]com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
```

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)  
Chrome/83.0.4103.61 Safari/537.36  
Host: [REDACTED].com  
Connection: Keep-alive

## Recommendation

It's recommended to implement HTTP Strict Transport Security (HSTS) into your web application. Consult web references for more information

## References

[hstspreload.org](https://hstspreload.org)

<https://hstspreload.org/>

[Strict-Transport-Security](https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security)

<https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security>

# Login page password-guessing attack

A common threat web developers face is a password-guessing attack known as a brute force attack. A brute-force attack is an attempt to discover a password by systematically trying every possible combination of letters, numbers, and symbols until you discover the one correct combination that works.

This login page doesn't have any protection against password-guessing attacks (brute force attacks). It's recommended to implement some type of account lockout after a defined number of incorrect password attempts. Consult Web references for more information about fixing this problem.

## Impact

An attacker may attempt to discover a weak password by systematically trying every possible combination of letters, numbers, and symbols until it discovers the one correct combination that works.

[https://\[REDACTED\].com/login](https://[REDACTED].com/login)

Confidence: 80%

## Request

POST /login HTTP/1.1  
Referer: https://[REDACTED].com/login  
Cookie: XSRF-  
TOKEN=eyJpdiI6InBTQXpUdlRWam8ydUkxUklPcGs1aHc9PSIsInZhbnVlIjoibXBMN093RU9ERWlIM01PRkVFdTVZT1N3N05aTjdsSHVjUUZqRlA3ejlRa29qYUxOdnpnazJCeFFWdGZGNkhVQWNvOE5HOFRRTVo5eEtQds91b2QzMSSzdFVYdnN0Z1hyYmlXMlZt

dVRKY2VQbW9xZHdFU3JqUHHvSnNVWlp0REEiLCJtYWMiOiI5Yzg0MTMwZTJiOWY1MzA2OTk5ZGJhOWVlMmEwODJiNjQ5NDk0MGI2MjMlMmJmNmZhMzYyNjI3MjI0ZmU5MDdlIiwidGFnIjoiIn0%3D;imikrofv4\_session=eyJpdjI6IjFqSlZNVWY3ZVd6a1Z2SEJTDkRhQXc9PSIsInZhbHVlIjoiZzFONVRtYTNlZGtSemFKUnd5VDNnOVhFaXQxN3AybzRHTm5HTHM4c3dNdmI4dEdwQXJ5aGJYeGtmck5sS2Y4bVhpNFg2SnF1d2c0ek5NRkJEbHJrWUcyWprcmdjUm4zRUJXN251eUVYQ2diMTdHMGdWQS9CNXo1WlV0RnhjMFYiLCJtYWMiOiJlZjE3YjAyMGQ2YmJmJi0MmVkJmZjM2ZDRmMmNmNmFjZTJiYWQ3NzViNjI4NDNjODc2MGQ3YWNjNGJjNTUwMTQzIiwidGFnIjoiIn0%3D;

Content-Type: application/x-www-form-urlencoded

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

Accept-Encoding: gzip, deflate

Content-Length: 105

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)

Chrome/83.0.4103.61 Safari/537.36

Host: [REDACTED].com

Connection: Keep-alive

\_token=WWzAUcbwVKttwhsGtnXqJlJm9uHOUrbnaALyxCRG&user\_name=username&password=testing&=Login&remember\_me=1&

## Recommendation

It's recommended to implement some type of account lockout after a defined number of incorrect password attempts.

## References

### [Blocking Brute Force Attacks](https://www.owasp.org/index.php/Blocking_Brute_Force_Attacks)

[https://www.owasp.org/index.php/Blocking\\_Brute\\_Force\\_Attacks](https://www.owasp.org/index.php/Blocking_Brute_Force_Attacks)

## Possible sensitive files

A possible sensitive file has been found. This file is not directly linked from the website. This check looks for common sensitive resources like password files, configuration files, log files, include files, statistics data, database dumps. Each one of these files could help an attacker to learn more about his target.

## Impact

This file may expose sensitive information that could help a malicious user to prepare more advanced attacks.

[https://\[REDACTED\].com/](https://[REDACTED].com/)

Possible sensitive files:

- [https://\[REDACTED\].com/config](https://[REDACTED].com/config)

## Request

```
GET /web.config HTTP/1.1
Accept: acunetix/wvs
Cookie: XSRF-
TOKEN=eyJpdiI6Ijk3R3VHqjcrNmxxL2NZevNPMThOZmc9PSIsInZhbnVlIjoid1gyTjgzMlNmVG1rQlp6Si9xak5vY2FDbmliTlRVUkVDQ2NwdTBGUfZnWEY5VWpSMisycFkyOHh0Mj1RRjB6NGN1M294b29kV215SFTrRjE4Nld6ekxLWVhYeSthLzBUUENiV1czSnhVa0V1UmJBREVYNnZ2Ui9VQThObDFQakIiLCJtYWMiOiI2YWNiMGQ5ODc4MjNlMzEyYjk4ZjZhNzQyMmI2ZTU0ZThhZWUyNjc4ZWQ3Nzk5ODg4ZTYwZWRLMjFhYmE5Mzc4IiwidGFuIjoiIn0%3D;imikrofv4_session=eyJpdiI6IjAwREpJa3U5d0JVSWSzdXZZSlFwSlE9PSIsInZhbnVlIjoiQVJ0ZXBiz1ZiRzhKNULibV43Y5ZFN5MXUwMytSM3pMem82N1VzQk1XQkgzcTZOSkhDY3ZYK21URVUxK3p6c1JUMXo2aE55aUJ2YW5yUDdQNGF5K1VETzBFR2JSR1RMDk93eERYMzVlc2Q5Z2RsR3dYcTfoQVhIeTVHNUtSVngiLCJtYWMiOiI5MTM0N2E2ZDhkOGYzOWM5MmRmMjY0ZDZiMmRiYjRkYzc0NzVlY2RlYmFiMTVhMzk5NTBjZTAwODliZTg3YTE2IiwidGFuIjoiIn0%3D
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.61 Safari/537.36
Host: [REDACTED].m
Connection: Keep-alive
```

## Recommendation

Restrict access to this file or remove it from the website.

## References

[Web Server Security and Database Server Security](https://www.acunetix.com/websitesecurity/webserver-security/)

<https://www.acunetix.com/websitesecurity/webserver-security/>

# 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.

https://[redacted].com/

Paths without CSP header:

- https://[redacted].com/login
- https://[redacted].com/home
- https://[redacted].com/
- https://[redacted].com/with\_wise/
- https://[redacted].com/reports/
- https://[redacted].com/reports/mra/
- https://[redacted].com/reports/mranbd/
- https://[redacted].com/css/images/
- https://[redacted].com/glyphicons-halflings-white.html
- https://[redacted].com/glyphicons-halflings.html
- https://[redacted].com/assets/images/
- https://[redacted].com/assets/img/
- https://[redacted].com/css/assets/
- https://[redacted].com/duo-register
- https://[redacted].com/duo-transaction-balance

## Request



```
GET /login HTTP/1.1
Referer: https://[REDACTED].com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/83.0.4103.61 Safari/537.36
Host: [REDACTED].com
Connection: Keep-alive
```

## 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>

### [Implementing Content Security Policy](#)

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

# Insecure Referrer Policy

---

Referrer Policy controls behaviour of the Referrer header, which indicates the origin or web page URL the request was made from. The web application uses insecure Referrer Policy configuration that may leak user's information to third-party sites.

## Impact

---

In some situations, an attacker may leak a user's private data

[https://\[REDACTED\].com/](https://[REDACTED].com/)

URLs where Referrer Policy configuration is insecure:

- [https://\[REDACTED\].com/login](https://[REDACTED].com/login)
- [https://\[REDACTED\].com/home](https://[REDACTED].com/home)
- [https://\[REDACTED\].com/](https://[REDACTED].com/)
- [https://\[REDACTED\].com/month\\_wise/](https://[REDACTED].com/month_wise/)

- [https://\[redacted\]/](https://[redacted]/)
- [https://\[redacted\]/mra/](https://[redacted]/mra/)
- [https://\[redacted\]/s/mranbd/](https://[redacted]/s/mranbd/)
- [https://\[redacted\]/s/](https://[redacted]/s/)
- [https://\[redacted\]/s-halflings-white.html](https://[redacted]/s-halflings-white.html)
- [https://\[redacted\]/s-halflings.html](https://[redacted]/s-halflings.html)
- [https://\[redacted\]/assets/images/](https://[redacted]/assets/images/)
- [https://\[redacted\]/img/](https://[redacted]/img/)
- [https://\[redacted\]/s/assets/](https://[redacted]/s/assets/)
- [https://\[redacted\]/due-register](https://[redacted]/due-register)
- [https://\[redacted\]/user-migration-balance](https://[redacted]/user-migration-balance)

## Request

---

```
GET /login HTTP/1.1
Referer: https://[redacted].com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/83.0.4103.61 Safari/537.36
Host: [redacted].m
Connection: Keep-alive
```

## Recommendation

---

Consider setting Referrer-Policy header to 'strict-origin-when-cross-origin' or a stricter value

## References

---

### [Referrer-Policy](#)

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

# 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.

[\[REDACTED\].com/](#)

Confidence: 95%

- **Chart.js 2.7.3**
  - URL: [https://\[REDACTED\].com/js/Chart.min.js](https://[REDACTED].com/js/Chart.min.js)
  - Detection method: The library's name and version were determined based on the file's contents.
  - References:
    - <https://github.com/chartjs/Chart.js/releases>
- **Chart.js 2.7.3**
  - URL: [https://\[REDACTED\].com/assets/js/Chart.min.js](https://[REDACTED].com/assets/js/Chart.min.js)
  - Detection method: The library's name and version were determined based on the file's contents.
  - References:
    - <https://github.com/chartjs/Chart.js/releases>

## Request

```
GET /js/Chart.min.js HTTP/1.1
Host: [REDACTED].com
Pragma: no-cache
Cache-Control: no-cache
accept-language: en-US
accept: */*
cookie: XSRF-
TOKEN=eyJpdiI6ImxPckp4YTBHV2luOWVxcUVGZy9YQ1E9PSIsInZhbnVlIjoiSFVY1NvMXE4OEhWYWJlZWZSby95SnNZekxPc
kx0R0NMUDA0RnRjaUhlQyt6MENsMTFDbXlaS2RBYnpHY3IyR28rNGtycWtGL3VPTU5vSG5vc2E1S2ZxMkFXZXhKM2l5NWhrQzJN
S2xHOVB5ejhMdHJDR0x6eks2aFdsWFhjSlIiLCJtYWMiOiI0NTAxYjc2MGNkYTgxMDQzNDA5MzM1ODlkZjc1NWNmMzA5YTE0ZDQ
1YmY3NDJiNTJmZjN2Y1N2UyMmY5Yzc0IiwidGFuIjoiIn0%3D;
imikrofv4_session=eyJpdiI6IjdfVWpxK29HelpMMnpkOWhQUUZTN1E9PSIsInZhbnVlIjoiZ2R2elZKYkNXL3RZZkpHVzQ4c
XJLZmlrZlF3SS9IK0FhMURpN1N5OE9KVzc3cUxwclM2aXpSbEVRaFUrWGx1RUxWL3Q3RDZSTm5vMW41NiswOUJa295R2xXS3E4
cXpEm1hxQlorWnB6VVVfVWkQvV0orOXZQWEx5WUs3Z0E5U0wiLCJtYWMiOiJhY2ZkNTBhZjBkNjJiZmM3ODA1MjFjZDIzNTF1MjI
wZDZhM2ZiYWQ3NWZmOGRmOThlZmYwZjU5YmFiODMyNTlmIiwidGFuIjoiIn0%3D
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Referer: [REDACTED]/home
Accept-Encoding: gzip, deflate
Connection: keep-alive
```

## Recommendation

---

Upgrade to the latest version.

# Password type input with auto-complete enabled

---

When a new name and password is entered in a form and the form is submitted, the browser asks if the password should be saved. Thereafter when the form is displayed, the name and password are filled in automatically or are completed as the name is entered. An attacker with local access could obtain the cleartext password from the browser cache.

## Impact

---

Possible sensitive information disclosure.

**[REDACTED]**

Pages with auto-complete password inputs:

- **[REDACTED]**/login

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

- **[REDACTED]**om/

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

## Request

---

GET /login HTTP/1.1  
Referer: https://**[REDACTED]**com/  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  
Accept-Encoding: gzip,deflate  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)  
Chrome/83.0.4103.61 Safari/537.36

## Recommendation

---

The password auto-complete should be disabled in sensitive applications.

To disable auto-complete, you may use a code similar to:

```
<INPUT TYPE="password" AUTOCOMPLETE="off">
```

## 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.

[REDACTED]

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>

[PHP Documentation: php.ini directive expose\\_php](#)

<https://www.php.net/manual/en/ini.core.php#ini.expose-php>

## Possible server path disclosure (Unix)

---

One or more fully qualified path names were found. From this information the attacker may learn the file system structure from the web server. This information can be used to conduct further attacks.

This alert may be a false positive, manual confirmation is required.

Possible sensitive information disclosure.

- `l [REDACTED] m/`  
`>/usr/share/nginx/html/50x.html`
- `l [REDACTED] logout`  
`>/usr/share/nginx/html/50x.html`
- `l [REDACTED] /month_wise/month_wiseloan_report_3_13`  
`>/usr/share/nginx/html/50x.html`
- `l [REDACTED] /login`  
`>/usr/share/nginx/html/50x.html`

```
GET / HTTP/1.1
Referer: https://[REDACTED]assets/js/jquery-ui.js
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/83.0.4103.61 Safari/537.36
Cookie: XSRF-
TOKEN=eyJpdii6ImxLRm5JcXVtc093TG1wVFR4WG13NlE9PSIsInZhbnV1IjoiUSsxdldkDWFoeGluakxLOWI0S3NHVYVJQY3hWa
kxXTHhNNzNyeldiYwdqT3JadFNqZFMhNU9XejluaTBqWGlJS1I5RHRxdjFxaGZzL1BkdqdpVWdxVFZBS1l0WFhsTElvZlozBUY0
VmFSODRpr0p3bUxSai9JU1RiNDhBZl1Q0YTUilCJtYWMiOiJjYWNmZTZmYWZkNTJiOWMzODFhMzRiMWUwMTElZWUxNDQ3ZWE5YzA
yYzU5NTVlNDA0NjgwYzE3YmJkZTEyN2QwIiwidGFniJoiIn0%3D;imikrofv4_session=eyJpdii6InZRWi83d3VSdzFieFc3a
1hzSUF5Znc9PSIsInZhbnV1IjoiS9ocU5udkZ2WmFETmdHTEgvWHFGZlNwQ2JuMj1JT3h2M0syL2RmaVhU0Rtc1ltbFkxM1BM
c3BZeHBoYjBuVmFYL2l5RHpXNnhvQnhGR3ZVR3RUckgzczF2Mcm94WFBxZmRPMmhtY3c4V0s3Z2NTN0dlU0tTRGRPcUwvb3djWGk
iLCJtYWMiOiIyNThiMjU3MzI0NGM2MzFlMWVjNWRkY2M3ZDBiNWl5YjEyYmM3ZGZjMTE4ZTQyNDQ1MDRlYjlkMjU5MjJlZTAxIi
widGFniJoiIn0%3D
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: [REDACTED].om
Connection: Keep-alive
```

Prevent this information from being displayed to the user.

## Full Path Disclosure

[https://www.owasp.org/index.php/Full\\_Path\\_Disclosure](https://www.owasp.org/index.php/Full_Path_Disclosure)

# Subresource Integrity (SRI) not implemented

Subresource Integrity (SRI) is a security feature that enables browsers to verify that third-party resources they fetch (for example, from a CDN) are delivered without unexpected manipulation. It works by allowing developers to provide a cryptographic hash that a fetched file must match.

Third-party resources (such as scripts and stylesheets) can be manipulated. An attacker that has access or has hacked the hosting CDN can manipulate or replace the files. SRI allows developers to specify a base64-encoded cryptographic hash of the resource to be loaded. The integrity attribute containing the hash is then added to the <script> HTML element tag. The integrity string consists of a base64-encoded hash, followed by a prefix that depends on the hash algorithm. This prefix can either be sha256, sha384 or sha512.

The script loaded from the external URL specified in the Details section doesn't implement Subresource Integrity (SRI). It's recommended to implement Subresource Integrity (SRI) for all the scripts loaded from external hosts.

## Impact

An attacker that has access or has hacked the hosting CDN can manipulate or replace the files.

[REDACTED]/home

Pages where SRI is not implemented:

- [REDACTED]/home  
Script SRC: <https://www.googletagmanager.com/gtag/js?id=UA-178124947-1>

## Request

```
GET /home HTTP/1.1
Host: [REDACTED].om
Pragma: no-cache
Cache-Control: no-cache
upgrade-insecure-requests: 1
accept-language: en-US
accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/s
igned-exchange;v=b3;q=0.9
cookie: XSRF-
TOKEN=eyJpdiI6Ikxjc2lqeJAWaTc0dFFqMWxxVks0OVE9PSIsInZhbnV1IjoIn2VrVHFpME5YTXQwV21hWXg2SzNPRFE5TVpYY
zMvY2kreVFHMG83UnU3UVJhV0dVOXJHQkYxvUxvL3psNlVleVhMV0dPV0hVbE1MYnhqYVl3STg1YXBSUXFoVDRIQ0FVRVZGd01t
eUZFYXZzSHNHAM9MNWhzTVhCTzZzbU44VGgiLCJtYWMiOiJiNjM3YjVkJmJQyNTM1YzJhNGQyOTNlYjYzNjI5NjM2ZDkwYTQxNzQ
5ZDJIYjhtNTdkOGU4NTNhNTl1NGM3ZTc0IiwidGFuIjoIn0%3D;
imikrofv4_session=eyJpdiI6Im0xWGtUaDlJQ1lQYnByV2xXSmJjYVE9PSIsInZhbnV1IjoiaEt5RWJnbjhDa2VHWGNVbWEyZ
mJWbS9IZlBQZzEwMHVCRWNxcWdOSzFRYm55TU1wcFlvUTEwMjFjXm9nZnMwxeWhzYkI1U1lZUVprVlVsU283YjRHOGtYODlK
```

```
eUpVbzRPUy9sVzVLby9yMHBldW82M05YSFQ0bjNvOGs1dlkiLCJtYWMMiOiIyNjM5Zjk5YjJlNmM5Njc1ZTdhdzDVlNzFlZmU1Njg
ONjM5OTdiYTk0MmZkM2ZjYmVlZTk5NGQ4Nzg5YTZkMzU3IiwidGFnIjoiIn0%3D
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://[REDACTED].com/
Accept-Encoding: gzip, deflate
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/83.0.4103.61 Safari/537.36
```

## Recommendation

---

Use the SRI Hash Generator link (from the References section) to generate a `<script>` element that implements Subresource Integrity (SRI).

For example, you can use the following `<script>` element to tell a browser that before executing the `https://example.com/example-framework.js` script, the browser must first compare the script to the expected hash, and verify that there's a match.

```
<script src="https://example.com/example-framework.js"
integrity="sha384-oqVuAfXRKap7fdgcCY5uykM6+R9GqQ8K/uxy9rx7HNQlGYl1kPzQho1wx4JwY8wC"
crossorigin="anonymous"></script>
```

## References

---

### [Subresource Integrity](https://developer.mozilla.org/en-US/docs/Web/Security/Subresource_Integrity)

[https://developer.mozilla.org/en-US/docs/Web/Security/Subresource\\_Integrity](https://developer.mozilla.org/en-US/docs/Web/Security/Subresource_Integrity)

### [SRI Hash Generator](https://www.srihash.org/)

<https://www.srihash.org/>



# Coverage

---

[redacted]om/

---

[redacted]n/home

---

[redacted]/login