



Acunetix Threat Level 3

One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.



High







Medium



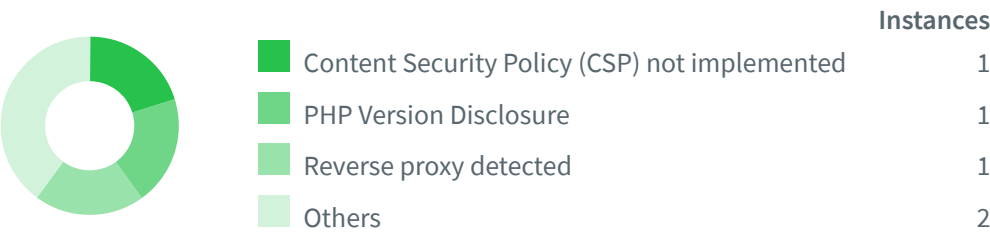
Low



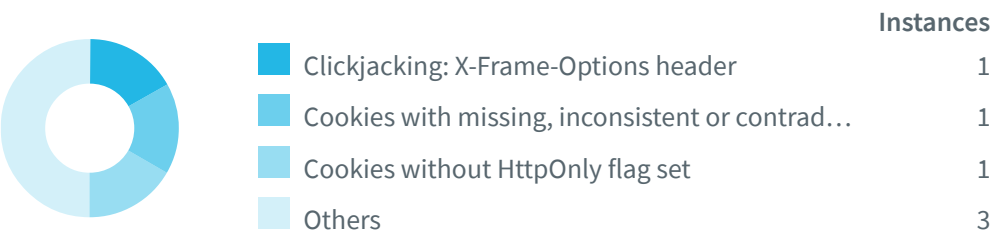
Informational

Severity	Vulnerabilities	Instances
 High	1	1
 Medium	4	4
 Low	6	6
 Informational	5	5
Total	16	16

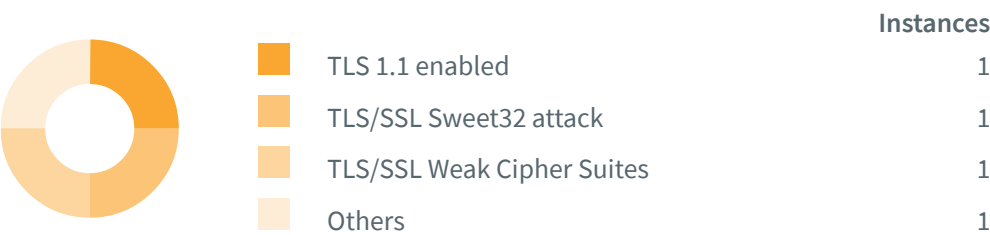
Informational



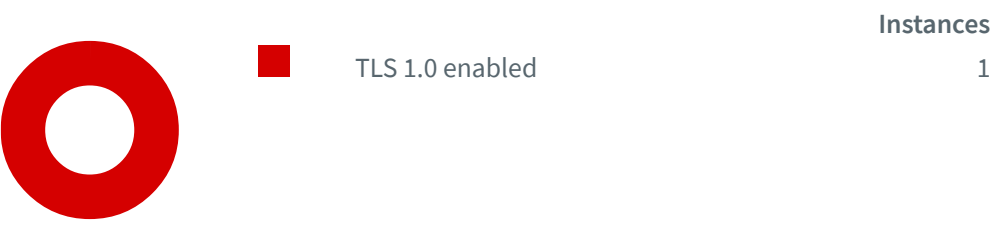
Low Severity



















Medium Severity



High Severity



Impacts

SEVERITY	IMPACT	
 High	<div>1</div>	TLS 1.0 enabled
 Medium	<div>1</div>	TLS 1.1 enabled
 Medium	<div>1</div>	TLS/SSL Sweet32 attack
 Medium	<div>1</div>	TLS/SSL Weak Cipher Suites
 Medium	<div>1</div>	Vulnerable JavaScript libraries
 Low	<div>1</div>	Clickjacking: X-Frame-Options header
 Low	<div>1</div>	Cookies with missing, inconsistent or contradictory properties
 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>	Session cookies scoped to parent domain
 Informational	<div>1</div>	Content Security Policy (CSP) not implemented
 Informational	<div>1</div>	PHP Version Disclosure
 Informational	<div>1</div>	Reverse proxy detected
 Informational	<div>1</div>	Subresource Integrity (SRI) not implemented
 Informational	<div>1</div>	Web Application Firewall detected

TLS 1.0 enabled

The web server supports encryption through TLS 1.0, which was formally deprecated in March 2021 as a result of inherent security issues. In addition, TLS 1.0 is not considered to be "strong cryptography" as defined and required by the PCI Data Security Standard 3.2(.1) when used to protect sensitive information transferred to or from web sites. According to PCI, "30 June 2018 is the deadline for disabling SSL/early TLS and implementing a more secure encryption protocol – TLS 1.1 or higher (TLS v1.2 is strongly encouraged) in order to meet the PCI Data Security Standard (PCI DSS) for safeguarding payment data.

Impact

An attacker may be able to exploit this problem to conduct man-in-the-middle attacks and decrypt communications between the affected service and clients.

<https://it-support-tag-aws.fpt-software.it/>

Confidence: 100%

The SSL server (port: 443) encrypts traffic using TLSv1.0.

Recommendation

It is recommended to disable TLS 1.0 and replace it with TLS 1.2 or higher.

References

[RFC 8996: Deprecating TLS 1.0 and TLS 1.1](#)

<https://tools.ietf.org/html/rfc8996>

[Are You Ready for 30 June 2018? Saying Goodbye to SSL/early TLS](#)

<https://blog.pcisecuritystandards.org/are-you-ready-for-30-june-2018-sayin-goodbye-to-ssl-early-tls>

[PCI 3.1 and TLS 1.2 \(Cloudflare Support\)](#)

<https://support.cloudflare.com/hc/en-us/articles/205043158-PCI-3-1-and-TLS-1-2>

TLS 1.1 enabled

The web server supports encryption through TLS 1.1, which was formally deprecated in March 2021 as a result of inherent security issues. When aiming for Payment Card Industry (PCI) Data Security Standard (DSS) compliance, it is recommended to use TLS 1.2 or higher instead. According to PCI, "30 June 2018 is

the deadline for disabling SSL/early TLS and implementing a more secure encryption protocol – TLS 1.1 or higher (TLS v1.2 is strongly encouraged) in order to meet the PCI Data Security Standard (PCI DSS) for safeguarding payment data.

Impact

An attacker may be able to exploit this problem to conduct man-in-the-middle attacks and decrypt communications between the affected service and clients.

<https://it-support-tag-aws.fpt-software.it/>

Confidence: 100%

The SSL server (port: 443) encrypts traffic using TLSv1.1.

Recommendation

It is recommended to disable TLS 1.1 and replace it with TLS 1.2 or higher.

References

[RFC 8996: Deprecating TLS 1.0 and TLS 1.1](https://tools.ietf.org/html/rfc8996)

<https://tools.ietf.org/html/rfc8996>

[Are You Ready for 30 June 2018? Saying Goodbye to SSL/early TLS](https://blog.pcisecuritystandards.org/are-you-ready-for-30-june-2018-sayin-goodbye-to-ssl-early-tls)

<https://blog.pcisecuritystandards.org/are-you-ready-for-30-june-2018-sayin-goodbye-to-ssl-early-tls>

[PCI 3.1 and TLS 1.2 \(Cloudflare Support\)](https://support.cloudflare.com/hc/en-us/articles/205043158-PCI-3-1-and-TLS-1-2)

<https://support.cloudflare.com/hc/en-us/articles/205043158-PCI-3-1-and-TLS-1-2>

TLS/SSL Sweet32 attack

The Sweet32 attack is a SSL/TLS vulnerability that allows attackers to compromise HTTPS connections using 64-bit block ciphers.

Impact

An attacker may intercept HTTPS connections between vulnerable clients and servers.

<https://it-support-tag-aws.fpt-software.it/>

Cipher suites susceptible to Sweet32 attack (TLS1.0 on port 443):

- TLS_RSA_WITH_3DES_EDE_CBC_SHA

Recommendation

Reconfigure the affected SSL/TLS server to disable support for obsolete 64-bit block ciphers.

References

[Sweet32: Birthday attacks on 64-bit block ciphers in TLS and OpenVPN](https://sweet32.info/)

<https://sweet32.info/>

TLS/SSL Weak Cipher Suites

The remote host supports TLS/SSL cipher suites with weak or insecure properties.

Impact

<https://it-support-tag-aws.fpt-software.it/>

Weak TLS/SSL Cipher Suites: (offered via TLS1.0 on port 443):

- TLS_RSA_WITH_3DES_EDE_CBC_SHA (Medium strength encryption algorithm (3DES).)

Recommendation

Reconfigure the affected application to avoid use of weak cipher suites.

References

[OWASP: TLS Cipher String Cheat Sheet](https://cheatsheetseries.owasp.org/cheatsheets/TLS_Cipher_String_Cheat_Sheet.html)

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

[OWASP: Transport Layer Protection Cheat Sheet](https://cheatsheetseries.owasp.org/cheatsheets/Transport_Layer_Protection_Cheat_Sheet.html)

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

[Mozilla: TLS Cipher Suite Recommendations](https://wiki.mozilla.org/Security/Server_Side_TLS)

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

[SSLabs: SSL and TLS Deployment Best Practices](https://github.com/ssllabs/research/wiki/SSL-and-TLS-Deployment-Best-Practices)

<https://github.com/ssllabs/research/wiki/SSL-and-TLS-Deployment-Best-Practices>

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.

Consult References for more information.

Confidence: 80%

- ## Request

8


```
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/99.0.4844.0 Safari/537.36
Host: it-support-tag-aws.fpt-software.it
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.

<https://it-support-tag-aws.fpt-software.it/>

Paths without secure XFO header:

- <https://it-support-tag-aws.fpt-software.it/9389881>
- <https://it-support-tag-aws.fpt-software.it/login>

Request

```
GET /9389881 HTTP/1.1
Referer: https://it-support-tag-aws.fpt-software.it/
Cookie: XSRF-
TOKEN=eyJpdiI6Ijd5QURRU1dQRVg2QytYclFwU1BseVE9PSIsInZhbnVlIjoiaNVdXbjd4Q3JKc0RxE5EVnNyVE56Q1RKK3FyZE
YxSmphVE0ydU5qajdpWnp3TzhhQWszV2ZsV0ltU1RPy05TbyIsIm1hYyI6IjI5NjU3ZTdiZjY5ZTQzYjYyNmUzODI2ZWlWODIwYj
QxYjYzZDZmNGFhYTliNTkyMTRmYjUxZDczMjRjMmY5ZDAifQ%3D%3D;
workplace_bot_ticket_session=eyJpdiI6Im9sR3BvRzVONE9HOG9RbjNQWGUycWc9PSIsInZhbnVlIjoiaGFuMkxS3lRbzk
```

```
1K0tkVG1hRHZBUddYQ1RiSFpid3hxU01tNFdNVWpHd2tMaDZ6cjZbk9oRm5lXC9MMk10a1IiLCJtYWMiOiI4NDA2MjQ3OTM0MzA
ONDA5Njk3YjI4OTRiMWQ2MzIiNDZlNzI1OTc4YmZlMTI5OWJhYWRLZDhkNmI2ZTAzOWY3In0%3D;
__cf_bm=TxK272th_zOIvWKtwgDKeWcrhLrMncVRqn4XMDfwESk-1672893606-0-
AYjlOHhQKwhyWWH2Xxl/hYe+r9G98Lq7AbFz4yJl46qXDUuvGqjhJ+/Cs+c2LmP/ZPJdnLyyg5kU1R5paGyuEFo=
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/99.0.4844.0 Safari/537.36
Host: it-support-tag-aws.fpt-software.it
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

[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 with missing, inconsistent or contradictory properties

At least one of the following cookies properties causes the cookie to be invalid or incompatible with either a different property of the same cookie, of with the environment the cookie is being used in. Although this is not a vulnerability in itself, it will likely lead to unexpected behavior by the application, which in turn may cause secondary security issues.

Impact

Cookies will not be stored, or submitted, by web browsers.

<https://it-support-tag-aws.fpt-software.it/>

List of cookies with missing, inconsistent or contradictory properties:

- <https://it-support-tag-aws.fpt-software.it/>

Cookie was set with:

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6Ijd5QURRU1dQRVg2QytYclFwU1BseVE9PSIsInZhbnHVlIjoiNVdXbjd4Q3JKc0RxRE5
EVnNyVE56Q1RKK3FyZEYxSmphVE0ydU5qajdpWnp3TzhhQWszV2ZsV0ltU1RPy05TbyIsImlhYyI6IjI5
NjU3ZTdizjY5ZTQzYjYyNmUzODI2ZWlwODIwYjQxYjYzZDZmNGFhYTliNTkyMTRmYjUxZDczMjRjMmY5Z
DAifQ%3D%3D; expires=Thu, 05-Jan-2023 06:40:06 GMT; Max-Age=7200; path=/
```

This cookie has the following issues:

- Cookie without SameSite attribute.

When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It is therefore recommended to add a SameSite attribute with an appropriate value of either "Strict", "Lax", or "None".

- <https://it-support-tag-aws.fpt-software.it/>

Cookie was set with:

```
Set-Cookie:
workplace_bot_ticket_session=eyJpdiI6Im9sR3BvRzVONE9HOG9RbjNQWGUycWc9PSIsInZhbnHVl
IjoiagFuMkxkS3lRbzk1K0tkVG1hRHZBUDdYQlRiSFpid3hxU01tNFdNVWpHd2tMaDZ6cjdZbk9oRm5lX
C9MMk10alIiLCJtYWMiOiI4NDA2MjQ3OTM0MzA0NDA5Njk3YjI4OTRiMWQ2MzI1NDZlNzI1OTc4YmZlMT
I5OWJhYWRLZDhkNmI2ZTAzOWY3In0%3D; expires=Thu, 05-Jan-2023 06:40:06 GMT; Max-
Age=7200; path=/; httponly
```

This cookie has the following issues:

- Cookie without SameSite attribute.

When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It is therefore recommended to add a SameSite attribute with an appropriate value of either "Strict", "Lax", or "None".

- <https://it-support-tag-aws.fpt-software.it/login>

Cookie was set with:

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IkhFQWV6MFNGaDB0XC92d0M5M1ZCNU5nPT0iLCJ2YWx1ZSI6ImtPREQ5R3pXTXlIQjl
```

```
XRWhZNEZOTF13bXpta0JYaW9Va2xVaGo4aDjLTnVTRHJNQzVxYWJDQlwwYkZcL1JEOTthaiIsIm1hYyI6
IjM2ODM2ZDk3YmI0NmJmNzRjMWUyOTlhZTmZDk5ZGZlZTUxZTYyYWQ5ZDc5NzVmYzcyZTBjODliOTgxZ
mRmYzQifQ%3D%3D; expires=Thu, 05-Jan-2023 06:42:11 GMT; Max-Age=7200; path=/
```

This cookie has the following issues:

- Cookie without SameSite attribute.

When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It is therefore recommended to add a SameSite attribute with an appropriate value of either "Strict", "Lax", or "None".

- <https://it-support-tag-aws.fpt-software.it/login>

Cookie was set with:

```
Set-Cookie:
workplace_bot_ticket_session=eyJpdiI6ImFpQ2hDTUxJOuFTWlg0cWw5Rjd5TlE9PSIsInZhbnVl
IjoicXJwQjd5Z01qbFhjCHR4N0crYXpZZDdYNThGQnpUdFljK256OXdqU1lyTG02UXQ4OU1SYjFvNjZlb
zQ3WlFndiIsIm1hYyI6IjIyNGM1N2Q3NzIxOTIyNGY0YzEyMjU5ZjI3ODk1YzcmMDQ4MzBiNzBlYjJjNz
VjNGI2NGVmMTg0Yjk4YmVhNGIifQ%3D%3D; expires=Thu, 05-Jan-2023 06:42:11 GMT; Max-
Age=7200; path=/; httponly
```

This cookie has the following issues:

- Cookie without SameSite attribute.

When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It is therefore recommended to add a SameSite attribute with an appropriate value of either "Strict", "Lax", or "None".

- <https://it-support-tag-aws.fpt-software.it/login>

Cookie was set with:

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IjheODdocDFQT3RcL1htc0N4N3UxN1hnPT0iLCJ2YWx1ZSI6IkZsYVwvUGJFNElJdDY
2dGFiznhua2hyejNjemFGR1FUK0huN25hV3hsQ09idEEySTFYOVd1XC9vYVhsYTd2bElINyIsIm1hYyI6
ImVjYzBlNWRjY2RmYzIxM2QxNjdlYzA0ZWZiYWE2ZjE4ZTUxOWEwNTNhM2NlM2RiYTU2MzQzZjkwNzMyN
2Q2MGIifQ%3D%3D; expires=Thu, 05-Jan-2023 06:43:07 GMT; Max-Age=7200; path=/
```

This cookie has the following issues:

- Cookie without SameSite attribute.

When cookies lack the SameSite attribute, Web browsers may apply different and

sometimes unexpected defaults. It is therefore recommended to add a SameSite attribute with an appropriate value of either "Strict", "Lax", or "None".

- <https://it-support-tag-aws.fpt-software.it/login>

Cookie was set with:

```
Set-Cookie:
workplace_bot_ticket_session=eyJpdiI6IjE2c0V5YzJGWXZ4aUh5azdwdWdwTFE9PSIsInZhbnHVl
IjoiUWhqcGlkQVxK0o4Um9SeTJOaWo0T29wTEF0ejlrSnZQdUVhMFJlNFpOc1p0WU53UVduejdKSytSK
1EyRmZacyIsIm1hYyI6IjhmODQ0NWQ1MGIzZTVmN2NiYWU5ZTlkYzExMTA2MDI3NDk0MWQ2ZGQ3OWYwZj
NiNDc5NjY0NmMyNTM4N2E4ZjUifQ%3D%3D; expires=Thu, 05-Jan-2023 06:43:07 GMT; Max-
Age=7200; path=/; httponly
```

This cookie has the following issues:

- Cookie without SameSite attribute.

When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It is therefore recommended to add a SameSite attribute with an appropriate value of either "Strict", "Lax", or "None".

- <https://it-support-tag-aws.fpt-software.it/login>

Cookie was set with:

```
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IjhzZbEJxMHFheVZuSDY5YlBaVURSaXc9PSIsInZhbnHVlIjoiZDRUN2g0cnlxRXhEY01
BM0hoV0dUMlg1YnpTa205KzlhV2w3MTdma2VkaJhcL0tWafhwU0pFUEdpckV3ejFqUUMiLCJtYWMiOiIw
NDBmMjcwMzdhYWVmZWJmYjM0NmUwZGUxZmQwNjIxMWRhYjllOGZiY2NiNjYlMzg1OTIzY2ZhYjgwMTkyY
2ExIn0%3D; expires=Thu, 05-Jan-2023 06:47:57 GMT; Max-Age=7200; path=
```

This cookie has the following issues:

- Cookie without SameSite attribute.

When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It is therefore recommended to add a SameSite attribute with an appropriate value of either "Strict", "Lax", or "None".

- <https://it-support-tag-aws.fpt-software.it/login>

Cookie was set with:

workplace_bot_ticket_session=eyJpdii6IjhXcWt4djBHWjRaazF2eWlyOUx0dGc9PSIsInZhbHVl
IjoivVktGSXdwOHJEc2EzVDBTdExwR0lVWlQ5Q2srOEZJVTVNXT3IwalpQZYtvZmdrREYwRGpBZDhxSTdaR
CtCbzdQUSIsIm1hYyI6IjBhMDDdhZWlOOWRlODhhYmYlYTgzMDc4YTY4NTFmNjdkYmNhODNJYTlkYWJkYT
gyNmFhNDU4NDI3YjBiNGFjZTgifQ%3D%3D; expires=Thu, 05-Jan-2023 06:47:57 GMT; Max-Age=7200; path=/; httponly

- Cookie without SameSite attribute.

When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It is therefore recommended to add a SameSite attribute with an appropriate value of either "Strict", "Lax", or "None".

- Cookie was set with:

TOKEN=eyJpdiI6ImRcLzdoQXJ0bFFiYnVSWGxyNHhQVjBBPT0iLCJ2YWx1ZSI6IjhPd0JqbGR3MEYwaFR
CRmJQY0ZsTctDaFlIeTRHeDBlShkdGFwY05xT0p2cHJsZ2RtXC9FOEluZ2hac1NPblJlIiwibWFjIjo1
ZTBjMzdjZTVmMDViMTY3NTk0YWY0MjZjNmNjYjdhZjRmZjk1Yzg3MGY4NmJ1MjQ1ZGZkM2U0NzJiMTIzY
mJlZiJ9; expires=Thu, 05-Jan-2023 07:05:17 GMT; Max-Age=7200; path=/

- Cookie without SameSite attribute.

When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It is therefore recommended to add a SameSite attribute with an appropriate value of either "Strict", "Lax", or "None".

- Cookie was set with:

workplace_bot_ticket_session=eyJpdiI6IkNSN3k4NE1TTEFaYWhCU2JwNDVHeXc9PSIsInZhbnV1IjoisSDB2cTNPNWExbjVcLzcrbTM0UnpWSGI0Mmt4Y0tWYTU1OWpyR1VcL3ZSaHRJMFJ1djMrU29wVm9MZ
XZtQXI4WGV3IiwibWFjIjoieYWQzMtA5MTJjYzllZjJjZDI3MmQ5MjNmYzM5ZGU5MzFjNTMxM2I0NmYzNT
QyOWIwNjg5Mzc0ZWEmMTEyZjI4NiJ9; expires=Thu, 05-Jan-2023 07:05:17 GMT; Max-
Age=7200; path=/; httponly

14

- Cookie without SameSite attribute.

When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It is therefore recommended to add a SameSite attribute with an appropriate value of either "Strict", "Lax", or "None".

- <https://it-support-tag-aws.fpt-software.it/login>

Cookie was set with:

Set-Cookie:

workplace_bot_ticket_session=eyJpdjI6Ik93bmYxdlhuVVBEdUNNSkNoaWU1RFE9PSIsInZhbnVlIjoISWxabWg5VXhFNjZkXC9rSlVtTTFqdXVhMVMxUWFObXdjRENRRVg5djNjR3lFcnhsazVNRjIxTjN2XC8rU1FvNU1GIiwibWFjIjoiodY1ZDElNWQyMGFiMTQyYzJlY2ZjMGU2OWI4ZWNiYTklZjQ3MzRiZDQxNzEwMjc5YjYwMzQ0MTQwM2MzYTZhZCJ9; expires=Thu, 05-Jan-2023 07:05:16 GMT; Max-Age=7200; path=/; httponly

This cookie has the following issues:

- Cookie without SameSite attribute.

When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It is therefore recommended to add a SameSite attribute with an appropriate value of either "Strict", "Lax", or "None".

- <https://it-support-tag-aws.fpt-software.it/login>

Cookie was set with:

Set-Cookie: XSRF-

TOKEN=eyJpdjI6Iis3azF2bGhlZ3hMazM5OTQxZ0NpOGc9PSIsInZhbnVlIjoiveJHUVQzcmZGUis1SnB3a2xvclVzc0tGYUdJKzZuYVdcLzlTM2lpQjdQSHZvUGRwdk1wK2UzaVRZalc4Zk5xN1EiLCJtYWMiOiJlZmMzMzQ2N2M0NGJhNGY5M2VjOTU1MTIwMGE1OWQ0NDEwZDdkYjIwMzRmYmExNDUyNDZhNGNiOWU2OGViN2YwIn0%3D; expires=Thu, 05-Jan-2023 07:05:18 GMT; Max-Age=7200; path=/

This cookie has the following issues:

- Cookie without SameSite attribute.

When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It is therefore recommended to add a SameSite attribute with an appropriate value of either "Strict", "Lax", or "None".

- <https://it-support-tag-aws.fpt-software.it/login>

Cookie was set with:

Set-Cookie:

```
workplace_bot_ticket_session=eyJpdiI6Im1CVlFXUzhQKz1YdU1aclldzanJzU2c9PSIsInZhbmHV1Ijo1WHFFYk1SMHZ2b2pGQmRsSDBuM2VlSHA4WHQ5WkxuOVNkcitaUTlUTDdiNERPWDRYRkp1Rm1MRkFNN1VcLzNnVFYiLCJtYWMiOiIzZDdlMDQ2NWZjNGYzYTcxMzYxMzYzMDcyNWUwNDcyNTM3ZGJhNzAzNGI2MWQ1YTFlMzA5Mzg4MDFjZDM5NmY3In0%3D; expires=Thu, 05-Jan-2023 07:05:18 GMT; Max-Age=7200; path=/; httponly
```

This cookie has the following issues:

- Cookie without SameSite attribute.

When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It is therefore recommended to add a SameSite attribute with an appropriate value of either "Strict", "Lax", or "None".

- <https://it-support-tag-aws.fpt-software.it/login>

Cookie was set with:

Set-Cookie: XSRF-

```
TOKEN=eyJpdiI6I1pIMUVSbXVod3N6a0lubnJTRGtRWGc9PSIsInZhbmHV1Ijoic3ZiMEDqbDJKYjVUUTRwWTBub2VNdlpPN2t6NWVpOGZcL2V2RlFQYytwSlQ3SDVJZzVSZFFvYkswaEhQczZWXC9YIiwibWFjIjo1M2EyN2Q2MTRmMzRhYjJiMGZmZDY1OGFiMmE0M2E1NzQ2YjA5YTE3NzJmMTEwNjE3N2Q4MTgyN2YzMjQ1Y2QwZCJ9; expires=Thu, 05-Jan-2023 07:08:41 GMT; Max-Age=7200; path=
```

This cookie has the following issues:

- Cookie without SameSite attribute.

When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It is therefore recommended to add a SameSite attribute with an appropriate value of either "Strict", "Lax", or "None".

- <https://it-support-tag-aws.fpt-software.it/login>

Cookie was set with:

Set-Cookie:

```
workplace_bot_ticket_session=eyJpdiI6IkR3U1dhduFzUVJDDGtzQlRFVmNwMHc9PSIsInZhbmHV1Ijo1U2FWNjBCY1Q0aU1STWtjMTlvWlgydkh4N1JoUWQwR0JyWUV1cTl5ZHJXQnVxSHozNzM4Um84bkdGN3liTm16eSIsIm1hYyI6ImY4ZTdmdDdlNDlmNGZhYWY5MTZlMzcyY2RmZjYyNDM3MzEwMjJlNmYyNDc0OTdmMDY2ZDRlN2YyMThjYWI3ZWUifQ%3D%3D; expires=Thu, 05-Jan-2023 07:08:41 GMT; Max-Age=7200; path=/; httponly
```

This cookie has the following issues:

- Cookie without SameSite attribute.

When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It is therefore recommended to add a SameSite attribute with an appropriate value of either "Strict", "Lax", or "None".

Request

```
GET / HTTP/1.1
Referer: https://it-support-tag-aws.fpt-software.it/
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/99.0.4844.0 Safari/537.36
Host: it-support-tag-aws.fpt-software.it
Connection: Keep-alive
```

Recommendation

Ensure that the cookies configuration complies with the applicable standards.

References

[MDN | Set-Cookie](#)

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

[Securing cookies with cookie prefixes](#)

<https://www.sjoerdlangkemper.nl/2017/02/09/cookie-prefixes/>

[Cookies: HTTP State Management Mechanism](#)

<https://tools.ietf.org/html/draft-ietf-httpbis-rfc6265bis-05>

[SameSite Updates - The Chromium Projects](#)

<https://www.chromium.org/updates/same-site>

[draft-west-first-party-cookies-07: Same-site Cookies](#)

<https://tools.ietf.org/html/draft-west-first-party-cookies-07>

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.

<https://it-support-tag-aws.fpt-software.it/>

Verified

Cookies without HttpOnly flag set:

- <https://it-support-tag-aws.fpt-software.it/>

```
Set-Cookie: XSRF-  
TOKEN=eyJpdii6Ijd5QURRUldQRVg2QytYclFwUlBseVE9PSIsInZhbnHVlIjoiNVdXbjd4Q3JKc0RxRE5  
EVnNyVE56Q1RKK3FyZEYxSmphVE0ydU5qajdpWnp3TzhhQWszV2ZsV0ltU1RPy05TbyIsImlhYyI6IjI5  
NjU3ZTdiZjY5ZTQzYjYyNmUzODI2ZWlwODIwYjQxYjYzZDZmNGFhYTliNTkyMTRmYjUxZDczMjRjMmY5Z  
DAifQ%3D%3D; expires=Thu, 05-Jan-2023 06:40:06 GMT; Max-Age=7200; path=/  

```

- <https://it-support-tag-aws.fpt-software.it/login>

```
Set-Cookie: XSRF-  
TOKEN=eyJpdii6IkhFQWV6MFNGaDB0XC92d0M5MlZCNU5nPT0iLCJ2YWx1ZSI6ImtPREQ5R3pXTXlIQjl  
XRWhZNEZOTFl3bXpta0JYaW9Va2xVaGo4aDJLTnVTRHJNqzVxYWJDQlwwYkZcL1JEOThiaiIsImlhYyI6  
IjM2ODM2ZDk3YmI0NmJmNzRjMWUyOTlhZTZmZDk5ZGZlZTUxZTYyYWQ5ZDc5NzVmYzcyZTBjODliOTgxZ  
mRmYzQifQ%3D%3D; expires=Thu, 05-Jan-2023 06:42:11 GMT; Max-Age=7200; path=/  

```

- <https://it-support-tag-aws.fpt-software.it/login>

```
Set-Cookie: XSRF-  
TOKEN=eyJpdii6IjhEODdocDFQT3RcL1htc0N4N3UxN1hnPT0iLCJ2YWx1ZSI6IkZsYVwvUGJFNElJdDY  
2dGFiznhua2hyejNjemFGR1FUK0huN25hV3hsQ09idEEySTFYOVd1XC9vYVhsYTd2bElINyIsImlhYyI6  
ImVjYzBlNWRjY2RmYzIxM2QxNjdlYzA0ZWZiYWE2ZjE4ZTUxOWEwNTNhM2NlM2RiYTU2MzQzZjkwNzMyN  
2Q2MGIifQ%3D%3D; expires=Thu, 05-Jan-2023 06:43:07 GMT; Max-Age=7200; path=/  

```

- <https://it-support-tag-aws.fpt-software.it/login>

```
Set-Cookie: XSRF-  
TOKEN=eyJpdii6IjhZbEJxMHFheVZuSDY5Y1BaVURSaXc9PSIsInZhbnHVlIjoiZDRUN2g0cnlxRXhEY01  
BM0hoV0dUMlg1YnpTa205KzlhV2w3MTdma2VkaJhcL0tWaFhwU0pFUEdpckV3ejFqUUMiLCJtYWMiOiIw  
NDBmMjcwMzdhYWVmZWJmYjM0NmUwZGUxZmQwNjIxMWRhYjllhOGZiY2NiNjY1Mzg1OTIzY2ZhYjgwMTkyY  
2ExIn0%3D; expires=Thu, 05-Jan-2023 06:47:57 GMT; Max-Age=7200; path=/  

```

- <https://it-support-tag-aws.fpt-software.it/>

```
Set-Cookie: XSRF-  
TOKEN=eyJpdiI6ImRcLzdoQXJObFFiYnVSWGxyNHhQVjBBPT0iLCJ2YWx1ZSI6IjhpD0JqbGR3MEYwaFR  
CRmJQY0ZsTCTDaFlIeTRHeDBlSWhkdGFwY05xT0p2cHJsZ2RtXC9FOEluZ2hac1NPblJlIiwibWFjIjo  
ZTBjMzdjZTVmMDViMTY3NTk0YWY0MjZjNmNjYjdhZjRmZjk1Yzg3MGY4NjM1MjQ1ZGZkM2U0NzJiMTIzY  
mJlZiJ9; expires=Thu, 05-Jan-2023 07:05:17 GMT; Max-Age=7200; path=/  

```

- <https://it-support-tag-aws.fpt-software.it/login>

```
Set-Cookie: XSRF-  
TOKEN=eyJpdiI6Iis3azF2bG1hZ3hMazM5OTQxZ0NpOGc9PSIsInZhbnHVlIjoieVEJHUVQzcmZGUis1SnB  
3a2xvclVzc0tGYUdJKzZuYVdcLz1TM2lpQjdQSHZvUGRwdk1wK2UzaVRZa1c4Zk5xN1EiLCJtYWMiOiJl  
ZmMzMzQ2N2M0NGJhNGY5M2VjOTU1MTIwMGE1OWQ0NDEwZDdkYjIwMzRmYmExNDUyNDZhNGNiOWU2OGViN  
2YwIn0%3D; expires=Thu, 05-Jan-2023 07:05:18 GMT; Max-Age=7200; path=/  

```

- <https://it-support-tag-aws.fpt-software.it/login>

```
Set-Cookie: XSRF-  
TOKEN=eyJpdiI6IlpIMUVSbXVod3N6a0lubnJTRGtRWGc9PSIsInZhbnHVlIjoic3ZiMEDqbDJKYjVUUTR  
wWTBub2VNd1pPN2t6NWVpOGZcL2V2R1FQYytWslQ3SDVJZzVSZFFvYkswaEhQczZWXC9YIiwibWFjIjo  
iM2EyN2Q2MTRmMzRhYjJiMGZmZDY1OGFiMmE0M2E1NzQ2YjA5YTE3NzJmMTEwNjE3N2Q4MTgyN2YzMjQ1Y  
2QwZCJ9; expires=Thu, 05-Jan-2023 07:08:41 GMT; Max-Age=7200; path=/  

```

Request

```
GET / HTTP/1.1  
Referer: https://it-support-tag-aws.fpt-software.it/  
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/99.0.4844.0 Safari/537.36  
Host: it-support-tag-aws.fpt-software.it  
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.

<https://it-support-tag-aws.fpt-software.it/>

Verified

Cookies without Secure flag set:

- <https://it-support-tag-aws.fpt-software.it/>

```
Set-Cookie: XSRF-  
TOKEN=eyJpdii6Ijd5QURRUldQRVg2QytYclFwUlBseVE9PSIsInZhbnVlIjoianVdXbjd4Q3JKc0RxRE5  
EVnNyVE56Q1RKK3FyZEYxSmphVE0ydU5qaJdpWnp3TzhhQWszV2ZsV0ltU1RPY05TbyIsIm1hYyI6IjI5  
NjU3ZTdiZjY5ZTQzYjYyNmUzODI2ZWlWODIwYjQxYjYzZDZmNGFhYTliNTkyMTRmYjUxZDczMjRjMmY5Z  
DAifQ%3D%3D; expires=Thu, 05-Jan-2023 06:40:06 GMT; Max-Age=7200; path=/  

```

- <https://it-support-tag-aws.fpt-software.it/>

```
Set-Cookie:  
workplace_bot_ticket_session=eyJpdii6Im9sR3BvRzVONE9HOG9RbjNQWGUycWc9PSIsInZhbnVlIjoiaGFuMkxkS3lRbzk1K0tkVGhRHZBUDdYQ1RiSFpid3hxU01tNFdNVWpHd2tMaDZ6cjdZbk9oRm5lX  
C9MMkl0a1IiLCJtYWMiOiI4NDA2MjQ3OTMOMzA0NDA5Njk3YjI4OTRiMWQ2MzI1NDZlNzI1OTc4YmZlMT  
I5OWJhYWRLZDhkNmI2ZTAzOWY3In0%3D; expires=Thu, 05-Jan-2023 06:40:06 GMT; Max-  
Age=7200; path=/; httponly
```

- <https://it-support-tag-aws.fpt-software.it/login>

```
Set-Cookie: XSRF-  
TOKEN=eyJpdii6IkhFQWV6MFNGaDB0XC92d0M5M1ZCNU5nPT0iLCJ2YWx1ZSI6ImtPREQ5R3pXTXlIQjl  
XRWhZNEZOTFl3bXpta0JYaW9Va2xVaGo4aDJLTnVTRHJNqzVxYWJDQ1wvYkZcL1JEOThiaiIsIm1hYyI6  
IjM2ODM2ZDk3YmI0NmJmNzRjMWUyOTlhZTZmZDk5ZGZlZTUxZTYyYWQ5ZDc5NzVmYzcyZTBjODliOTgxZ  
mRmYzQifQ%3D%3D; expires=Thu, 05-Jan-2023 06:42:11 GMT; Max-Age=7200; path=/  

```

- <https://it-support-tag-aws.fpt-software.it/login>

Set-Cookie:

```
workplace_bot_ticket_session=eyJpdiI6ImFpQ2hDTUxJOUFTWlg0cWw5Rjd5TlE9PSIsInZhbmHV1IjoicXJwQjd5Z01qbFhjCHR4N0crYXpZDdYNTThGQnpUdFljK256OXdqU1lyTGo2UXQ4OUlSYjFvNjZlbzQ3WlFndiIsIm1hYyI6IjIyNGM1N2Q3NzIxOTIyNGY0YzEyMjU5ZjI3ODk1YzZwMDQ4MzBiNzBlYjJjNzVjNGI2NGVMTG0Yjk4YmVhNGIifQ%3D%3D; expires=Thu, 05-Jan-2023 06:42:11 GMT; Max-Age=7200; path=/; httponly
```

- <https://it-support-tag-aws.fpt-software.it/login>

Set-Cookie: XSRF-

```
TOKEN=eyJpdiI6IjhEODdocDFQT3RcLlhtc0N4N3UxN1hnPT0iLCJ2YWx1ZSI6IkJzYVwvUGJFNElJdDY2dGFiznhua2hyejNjemFGR1FUK0huN25hV3hsQ09idEEySTFYOVd1XC9vYVhsYTd2bElINyIsIm1hYyI6ImVjYzBlNWRjY2RmYzIxM2QxNjdlYzA0ZWZiYWE2ZjE4ZTUxOWEwNTNhM2NlM2RiYTU2MzQzZjkwNzMyN2Q2MGIifQ%3D%3D; expires=Thu, 05-Jan-2023 06:43:07 GMT; Max-Age=7200; path=
```

- <https://it-support-tag-aws.fpt-software.it/login>

Set-Cookie:

```
workplace_bot_ticket_session=eyJpdiI6IjE2c0V5YzJGWXZ4aUh5azdwdWdwTFE9PSIsInZhbmHV1IjoiUWhqcGlkQVxkK0o4Um9SeTJOaWo0T29wTEF0ejlrSnZQdUVhMFJlNFpOc1p0WU53UVduejdKSytSK1EyRmZacyIsIm1hYyI6IjhmODQ0NWQ1MGIzZTVmN2NiYWU5ZTlkYzExMTA2MDI3NDk0MWQ2ZGQ3OWYwZjNiNDc5NjY0NmMyNTM4N2E4ZjUifQ%3D%3D; expires=Thu, 05-Jan-2023 06:43:07 GMT; Max-Age=7200; path=/; httponly
```

- <https://it-support-tag-aws.fpt-software.it/login>

Set-Cookie: XSRF-

```
TOKEN=eyJpdiI6IjhzBEJxMHFheVZuSDY5YlBaVURSaXc9PSIsInZhbmHV1IjoiZDRUN2g0cnlxRXhEY01BM0hoV0dUMlg1YnpTa205KzlhV2w3MTdma2VkaJhcL0tWaFhwU0pFUEdpckV3ejFqUUMiLCJtYWMiOiIwNDBmMjcwMzdhYWVmZWJmYjM0NmUwZGUxZmQwNjIxMWRhYjllhOGZiY2NiNjY1MzgzOTIzY2ZhYjgwMTkyY2ExIn0%3D; expires=Thu, 05-Jan-2023 06:47:57 GMT; Max-Age=7200; path=
```

- <https://it-support-tag-aws.fpt-software.it/login>

Set-Cookie:

```
workplace_bot_ticket_session=eyJpdiI6IjhxXcWt4djBHWjRaazF2eWlyOUx0dGc9PSIsInZhbmHV1IjoiVktGSXdwOHJEc2EzVDBTdExwR01VWlQ5Q2srOEEZJVTNXT3IwalpQZytvZmdrREYwRGpBZDhxSTdaR
```


- <https://it-support-tag-aws.fpt-software.it/login>

Set-Cookie:

```
workplace_bot_ticket_session=eyJpdiI6ImlCVlFXUzhQKzlydUlaclldzanJzU2c9PSIsInZhbmHVlIjoic3ZiMEDqbDJKYjVUUTRwWTBub2VNdlpPN2t6NWVpOGZcL2V2RlFQYytWslQ3SDVJZzVSZFFvYksEhQczZWXC9YIiwibWFjIjoic2E2Y2Q2MTRmMzRhYjJiMGZmZDY1OGFiMmE0M2E1NzQ2YjA5YTE3NzJmMTE3NzQ2MTgyN2YzMjQ1Y2QwZCJ9; expires=Thu, 05-Jan-2023 07:05:18 GMT; Max-Age=7200; path=/; httponly
```

- <https://it-support-tag-aws.fpt-software.it/login>

Set-Cookie: XSRF-

```
TOKEN=eyJpdiI6ImlpIMUVSbXVod3N6a0lubnJTRGtRWGc9PSIsInZhbmHVlIjoic3ZiMEDqbDJKYjVUUTRwWTBub2VNdlpPN2t6NWVpOGZcL2V2RlFQYytWslQ3SDVJZzVSZFFvYksEhQczZWXC9YIiwibWFjIjoic2E2Y2Q2MTRmMzRhYjJiMGZmZDY1OGFiMmE0M2E1NzQ2YjA5YTE3NzJmMTE3NzQ2MTgyN2YzMjQ1Y2QwZCJ9; expires=Thu, 05-Jan-2023 07:08:41 GMT; Max-Age=7200; path=
```

- <https://it-support-tag-aws.fpt-software.it/login>

Set-Cookie:

```
workplace_bot_ticket_session=eyJpdiI6IkR3UldhdUFzUVJDDGtzQlRFVmNwMHc9PSIsInZhbmHVlIjoic3ZiMEDqbDJKYjVUUTRwWTBub2VNdlpPN2t6NWVpOGZcL2V2RlFQYytWslQ3SDVJZzVSZFFvYksEhQczZWXC9YIiwibWFjIjoic2E2Y2Q2MTRmMzRhYjJiMGZmZDY1OGFiMmE0M2E1NzQ2YjA5YTE3NzJmMTE3NzQ2MTgyN2YzMjQ1Y2QwZCJ9; expires=Thu, 05-Jan-2023 07:08:41 GMT; Max-Age=7200; path=/; httponly
```

Request

```
GET / HTTP/1.1
Referer: https://it-support-tag-aws.fpt-software.it/
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/99.0.4844.0 Safari/537.36
Host: it-support-tag-aws.fpt-software.it
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://it-support-tag-aws.fpt-software.it/>

URLs where HSTS is not enabled:

- <https://it-support-tag-aws.fpt-software.it/9389881>

Request

```
GET /9389881 HTTP/1.1
Referer: https://it-support-tag-aws.fpt-software.it/
Cookie: XSRF-
TOKEN=eyJpdiI6Ijd5QURRUldQRVg2QytYclFwU1BseVE9PSIsInZhbnVlIjoInVdXbjd4Q3JKc0RxRE5EVnNyVE56Q1RKK3FyZE
YxSmphVE0ydU5qajdpWnp3TzhhQWszV2ZsV01tU1RPy05TbyIsIm1hYyI6IjI5NjU3ZTdiZjY5ZTQzYjYyNmUzODI2ZWwODIwYj
QxYjYzZDZmNGFhYTliNTkyMTRmYjUxZDczMjRjMmY5ZDAifQ%3D%3D;
workplace_bot_ticket_session=eyJpdiI6Im9sR3BvRzVONE9HOG9RbjNQWGUycWc9PSIsInZhbnVlIjoiaGFuMkxS3lRbzk
1K0tkVGlhRHZBUddYQ1RisFpid3hxU01tNFdNVWpHd2tMaDZ6cjZbk9oRm5lXC9MMk10a1IiLCJtYWMiOiI4NDA2MjQ3OTM0MzA
0NDA5Njk3YjI4OTRiMQw2MzIiNDZlNzI1OTc4YmZlMTI5OWJhYWRlZDhkNmI2ZTAzOWY3In0%3D;
__cf_bm=TxK272th_zOIvWKtwgDKeWcrhLrMncVRqn4XMDfwESk-1672893606-0-
AYjl0HhQKwhyWWH2Xxl/hYe+r9G98Lq7AbFz4yJl46qXDUuvGqjhJ+/Cs+c2LmP/ZPJdnLyyg5kU1R5paGyuEfo=
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/99.0.4844.0 Safari/537.36
Host: it-support-tag-aws.fpt-software.it
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

<httpspreload.org>

Session cookies scoped to parent domain

One or more session cookies are scoped to the parent domain instead of a sub-domain. If a cookie is scoped to a parent domain, then this cookie will be accessible by the parent domain and also by any other sub-domains of the parent domain. This could lead to security problems.

Impact

None

<https://it-support-tag-aws.fpt-software.it/>

Verified

Session cookies scoped to parent domain:

- <https://it-support-tag-aws.fpt-software.it/>

```
Set-Cookie: __cf_bm=TxK272th_zOIvWKtwgDKeWcrhLrMncVRqn4XMDfwESk-1672893606-0-AYjlOHhqKwhyWWH2Xxl/hYe+r9G98Lq7AbFz4yJl46qXDUuvGqjhJ+/Cs+c2LmP/ZPJdnLyyg5kU1R5paGyuEFo; path=/; expires=Thu, 05-Jan-23 05:10:06 GMT; domain=.fpt-software.it; HttpOnly; Secure; SameSite=None
```

- <https://it-support-tag-aws.fpt-software.it/9389881>

```
Set-Cookie: __cf_bm=aEl.uJ84x__jp43lJwvKYihGWsdj_rsGuCWUXJ284Gw-1672893707-0-AVlF6yoGtKy6Wb05dd3qkqkLY4e3awM3o2wQZzmOr4FZ4EqV+dmcHnsnbJMfeb50Ck4B4yN5kNz/fwYOf/iqLIk=; path=/; expires=Thu, 05-Jan-23 05:11:47 GMT; domain=.fpt-software.it; HttpOnly; Secure; SameSite=None
```

- <https://it-support-tag-aws.fpt-software.it/login>

```
Set-Cookie: __cf_bm=exxT3b1IPg00Ln1W7BHbOEbc88MV7pMWYXTR.SCqE04-1672893731-0-AZ+qmFX326BE6QB109/cuD2DQ+njolCJS9/3wTEMVz6voilxtabsrPzMqLOqJRX4UWr3bbkbq8D9JBmmc
```

f83mdo=; path=/; expires=Thu, 05-Jan-23 05:12:11 GMT; domain=.fpt-software.it;
HttpOnly; Secure; SameSite=None

- <https://it-support-tag-aws.fpt-software.it/login>

Set-Cookie: __cf_bm=SzSv7txAnjiDGvdRKTe64WU3vVqu4rjq8KwrW.grVog-1672893787-0-
AXcIn/WOd3JWyT6ROcJdPERKOog7N4Zzpa8ATxV7lCQwMGW4Is9nvQMyQKnM/Sny0PjFdQW0+aAxpSz+d
t699zs=; path=/; expires=Thu, 05-Jan-23 05:13:07 GMT; domain=.fpt-software.it;
HttpOnly; Secure; SameSite=None

- <https://it-support-tag-aws.fpt-software.it/js/jquery.letterpic.min.js>

Set-Cookie: __cf_bm=UGI_7v3lQVONrHh3457F1IeAsp.wc.WprwdEsjtQK1Q-1672894172-0-
AcDqk5A5GLU9evKIdVlBUdYmkQLktec7YhCTn8E7pJz+nI43A5ub138b3uFPDPku0CgWEhF882dWWMZA/
jhcZnk=; path=/; expires=Thu, 05-Jan-23 05:19:32 GMT; domain=.fpt-software.it;
HttpOnly; Secure; SameSite=None

- <https://it-support-tag-aws.fpt-software.it/assets/vendors/base/vendors.bundle.css>

Set-Cookie: __cf_bm=TF.1BPFLY2BhUutuJEuesNrQk5Fc1PW.9N2Mk.0OPSQ-1672894195-0-
AWV4reEEuFV77DSFkX8RKuJEB/x2E2gdVrsZMt802hx4EcyBEmjrYu1Xg3bEq30Jyyjedyf63x+LzMn98
Ryoy9c=; path=/; expires=Thu, 05-Jan-23 05:19:55 GMT; domain=.fpt-software.it;
HttpOnly; Secure; SameSite=None

- <https://it-support-tag-aws.fpt-software.it/vendor/>

Set-Cookie: __cf_bm=08aHTi4XRKm8aE6l3dvUv0oe7yCTsU6EG43MVp_dtng-1672894212-0-
AZJrxwIAkPkvzZUjKT0pCi4qt9udc0yTMjUuHEO5we3NomNXgyVvpUzgsW2xnM/pfbBeq2CAFG/FjO9Wk
K7YRjo=; path=/; expires=Thu, 05-Jan-23 05:20:12 GMT; domain=.fpt-software.it;
HttpOnly; Secure; SameSite=None

- <https://it-support-tag-aws.fpt-software.it/assets/vendors/base/fonts/flaticon/>

Set-Cookie: __cf_bm=_do.KJqp6DEtj7fpss27Exofz9QS1fOTx0ceGcACxxY-1672894314-0-
AVy+bikNNeUPtChMXK50lbZgrx882d09dQfmbDRl37dbBK2UVQXt+a+TwN2KTuobsuiF8CnV2MKzJD4bL
2BKilIo=; path=/; expires=Thu, 05-Jan-23 05:21:54 GMT; domain=.fpt-software.it;
HttpOnly; Secure; SameSite=None

- <https://it-support-tag-aws.fpt-software.it/js/jquery.loading.min.js>

```
Set-Cookie: __cf_bm=P3FGulTB6QLk13LcbwaEUrGXUThx_dgGMb753A7Qjmk-1672894327-0-AcXuVugolG/BamQVuI/1d1KQdAbPCLLMgSBI+h8j0uh9668nqZjfTRkXBeIWA9e06YoH8xds82FLY4m5Vpd9b14=; path=/; expires=Thu, 05-Jan-23 05:22:07 GMT; domain=.fpt-software.it; HttpOnly; Secure; SameSite=None
```

- <https://it-support-tag-aws.fpt-software.it/assets/app/js/app.js>

```
Set-Cookie: __cf_bm=HqZZkT9TiwG1lzFwdKGyOBLivXAMznHQsmACoG5j9V4-1672894425-0-AQC9cygitFZuW/ecIqrrJGzOb7kxallG9VVawx3id/7pG1MvpAxe+zE3yheO/wGLFZ0iuvtv3CJ1+SyTnbOLbOw=; path=/; expires=Thu, 05-Jan-23 05:23:45 GMT; domain=.fpt-software.it; HttpOnly; Secure; SameSite=None
```

- <https://it-support-tag-aws.fpt-software.it/assets/>

```
Set-Cookie: __cf_bm=MsIpGhP3Ciidt5diJsaRjuNYKEClN0.yUi6FV41owPA-1672894339-0-AXlBKKsHJt7NvyBO2y/NGe3dPwKKPR4Rqh4EOXJ/OMWem7KRkQx5iFaz59eTZvJgnyAQNJWeIsSvBChDP3QrEO0=; path=/; expires=Thu, 05-Jan-23 05:22:19 GMT; domain=.fpt-software.it; HttpOnly; Secure; SameSite=None
```

- <https://it-support-tag-aws.fpt-software.it/assets/app/>

```
Set-Cookie: __cf_bm=1SR07Fw3ffmt6Lsolw_dUVzTZpq9smgygZTv3viWiCc-1672894437-0-AUwU4Rm+0alleXoIFXjbLKf7E6gDvJfeLAISA6iAivXb7NzU11cTHgnGDQfUDD0C9gTCFygssEdaR/YYdgc7KLo=; path=/; expires=Thu, 05-Jan-23 05:23:57 GMT; domain=.fpt-software.it; HttpOnly; Secure; SameSite=None
```

- <https://it-support-tag-aws.fpt-software.it/assets/vendors/>

```
Set-Cookie: __cf_bm=zcMgjcg9CX9YPRLrl8HCh1x6ppIpcJMgnXb3dgixO8-1672894437-0-Adm27qb4kGhA54OwzZhSbmX0NaMSZwQtrdlft9zY6tIFUXP0flyqte0bCL0suy+dDh5mdQAj+dq+8LMsAmCL8Lw=; path=/; expires=Thu, 05-Jan-23 05:23:57 GMT; domain=.fpt-software.it; HttpOnly; Secure; SameSite=None
```

- <https://it-support-tag-aws.fpt-software.it/assets/demo/default/media/>

Set-Cookie: __cf_bm=AixjXSJdwlUHN7vevz5TTzo4JlRdpi86.307Z4o2pk0-1672894439-0-AW2lFqOEHDJWZNff5rZW3WXC1RPLQiPh8ToxNpn5eYiafVwlowX05tXJWPViweDT419Gpfp073w/gtLMBWPsbTw=; path=/; expires=Thu, 05-Jan-23 05:23:59 GMT; domain=.fpt-software.it; HttpOnly; Secure; SameSite=None

- <https://it-support-tag-aws.fpt-software.it/assets/app/js/>

Set-Cookie: __cf_bm=PyadKSHSmYRjR8zwTd2OKXapdwzHo4PDBZyaXmZ.IiU-1672894537-0-ASNz1slbfLavfpMNMZ+vBt61tZP/veEe3mVKVcC8LuavdA3kkQ+p1MGJw4tYfOqS2vNouME8c2mt6WzWREGa+TY=; path=/; expires=Thu, 05-Jan-23 05:25:37 GMT; domain=.fpt-software.it; HttpOnly; Secure; SameSite=None

- <https://it-support-tag-aws.fpt-software.it/assets/vendors/base/fonts/fontawesome5/>

Set-Cookie: __cf_bm=0XjFWB2QYXyz_Nw5.MB4GOF0LCZY82xVrCykj3weIkg-1672894539-0-Aegy8c4b6Cf+b8oNbH8PX321R8DPkkicnAwPlKM+/+G39VZJurxLYaM6KpnOZOxXewb75SJquFZmXkdSg0VUOrQ=; path=/; expires=Thu, 05-Jan-23 05:25:39 GMT; domain=.fpt-software.it; HttpOnly; Secure; SameSite=None

- <https://it-support-tag-aws.fpt-software.it/assets/demo/default/>

Set-Cookie: __cf_bm=lbUwZWH16_wbflFiCB.iHTdbUIXHXBy7pOinZv.gZWI-1672894568-0-AdIpGFcR+TmNHNJGsfPn6U8PuhNOFEIrNdjKGXnG6uWBgQhotNR6wUAHxkNXEUh+soOkuSPANnSCzqD/B1MPW4=; path=/; expires=Thu, 05-Jan-23 05:26:08 GMT; domain=.fpt-software.it; HttpOnly; Secure; SameSite=None

- <https://it-support-tag-aws.fpt-software.it/assets/app/media/img/files/>

Set-Cookie: __cf_bm=DV34fbWNGWNPIw3UkZVUwDgwVBmF0U24GqoCHJt8MkY-1672894571-0-AX+tmVKHMvhkGyNfrQZCs3rVZXpOrrE9Ef01ErMt28jpBMhTwvxgA8x42pe+v7qkvzvSCgqw+EyC9IE9T2YxX9w=; path=/; expires=Thu, 05-Jan-23 05:26:11 GMT; domain=.fpt-software.it; HttpOnly; Secure; SameSite=None

- <https://it-support-tag-aws.fpt-software.it/assets/demo/default/base/>

Set-Cookie: __cf_bm=_WLvxTBA9dg5MliUZH6q4TbmJzE8B.faz7B0arNMbIk-1672894638-0-AYkuNiTPAYFJs4kmvLSiR1M20YHtwZhGAsUtW37spE9eHCd7BkbCa1sVz34wK5YE7dsFzNmqmDpipiLGS

```
nJ62sI=; path=/; expires=Thu, 05-Jan-23 05:27:18 GMT; domain=.fpt-software.it;
HttpOnly; Secure; SameSite=None
```

- <https://it-support-tag-aws.fpt-software.it/assets/app/media/img/misc/>

```
Set-Cookie: __cf_bm=sdFY4VhWWUb2jMLf4zeEr0nFHQbnm08xI6Lc_OUlhv8-1672894685-0-
AbAfCYCDpkJWd3fkiNDS/cyYqW3fbLAN4Wy8lpdVECF1+oJA1093YrETqkxHdgXanHz+vglzCYuG2NJnN
YjpN/0=; path=/; expires=Thu, 05-Jan-23 05:28:05 GMT; domain=.fpt-software.it;
HttpOnly; Secure; SameSite=None
```

- <https://it-support-tag-aws.fpt-software.it/assets/vendors/base/vendors.bundle.js>

```
Set-Cookie: __cf_bm=LdExBZ2effJn48Ub_TTw.duLYeL7idiswCE_0GvEXj8-1672894708-0-
AQY2EfQ+GUWAeX00D4tOrYEpeqkTnCzCwYDTjwvcvHXkGJH1Y2U5pkQUERA0c0STg2uDnQiSxGhiSul54
lEryo8=; path=/; expires=Thu, 05-Jan-23 05:28:28 GMT; domain=.fpt-software.it;
HttpOnly; Secure; SameSite=None
```

Request

```
GET / HTTP/1.1
Referer: https://it-support-tag-aws.fpt-software.it/
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/99.0.4844.0 Safari/537.36
Host: it-support-tag-aws.fpt-software.it
Connection: Keep-alive
```

Recommendation

If possible, the session cookies should be scoped strictly to a sub-domain.

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://it-support-tag-aws.fpt-software.it/>

Paths without CSP header:

- <https://it-support-tag-aws.fpt-software.it/9389881>
- <https://it-support-tag-aws.fpt-software.it/login>

Request

```
GET /9389881 HTTP/1.1
Referer: https://it-support-tag-aws.fpt-software.it/
Cookie: XSRF-
TOKEN=eyJpdiI6Ijd5QURRU1dQRVg2QytYclFwU1BseVE9PSIsInZhbnVlIjoInVdXbJd4Q3JKc0RxE5EVnNyVE56Q1RKK3FyZEYxSmphVE0ydU5qajdpWnp3TzhhQWszV2ZsV0ltU1RPy05TbyIsIm1hYyI6IjI5NjU3ZTdZjY5ZTQzYjYyNmUzODI2ZWlWODIwYjQxYjYzZDZmNGFhYTliNTkyMTRmYjUxZDczMjRjMmY5ZDAifQ%3D%3D;
workplace_bot_ticket_session=eyJpdiI6Im9sR3BvRzVONE9HOG9RbjNQWGUycWc9PSIsInZhbnVlIjoiaGFuMkkxS3lRbzk1K0tkVG1hRHZBUddYQ1RiSFpid3hxU0ltNFdNVWpHd2tMaDZ6cjZbk9oRm5lXC9MMk10a1IiLCJtYWMiOiI4NDA2MjQ3OTM0MzA0NDA5Njk3YjI4OTRiMWQ2MzI1NDZlNzI1OTc4YmZlMTI5OWJhYWRLZDhkNmI2ZTAzOWY3In0%3D;
__cf_bm=TxK272th_z0IvWKtwgDKeWcrhLrMncVRqn4XMDfwESk-1672893606-0-
AYj10HhqKwhyWWH2Xxl/hYe+r9G98Lq7AbFz4yJl46qXDUuvGqjhJ+/Cs+c2LmP/ZPJdnLyyg5kU1R5paGyuEFo=
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/99.0.4844.0 Safari/537.36
Host: it-support-tag-aws.fpt-software.it
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)

<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/>

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.

<https://it-support-tag-aws.fpt-software.it/>

Version detected: PHP/7.3.33.

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

Reverse proxy detected

This server uses a reverse proxy, a load balancer or a CDN (Content Delivery Network) or it's hosted in a cloud provider. Acunetix detected this by sending various payloads and detecting changes in headers and body.

Impact

No impact is associated with this vulnerability.

<https://it-support-tag-aws.fpt-software.it/>

Detected reverse proxy: CloudFlare

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/99.0.4844.0 Safari/537.36
Host: it-support-tag-aws.fpt-software.it
Connection: Keep-alive
```

Recommendation

None

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.

<https://it-support-tag-aws.fpt-software.it/login>

Pages where SRI is not implemented:

- <https://it-support-tag-aws.fpt-software.it/login>
Script SRC: <https://ajax.googleapis.com/ajax/libs/webfont/1.6.16/webfont.js>

Request

```
GET /login HTTP/1.1
Referer: https://it-support-tag-aws.fpt-software.it/
Cookie: XSRF-
TOKEN=eyJpdiI6Ijd5QURRUldQRVg2QytYclFwU1BseVE9PSIsInZhbnVlIjoibVdXbjd4Q3JKc0RxeRE5EVnNyVE56Q1RKK3FyZEYxSmphVE0ydU5qajdpWnp3TzhhQWszV2ZsV0ltU1RlPy05TbyIsIm1hYyI6IjI5NjU3ZTdidiZjY5ZTQzYjYyNmUzODI2ZWlWODIwYjQxYjYzZDZmNGFhYTliNTkyMTRmYjUxZDczMjRjMmY5ZDAifQ%3D%3D;
workplace_bot_ticket_session=eyJpdiI6Im9sR3BvRzVONE9HOG9RbjNQWGUycWc9PSIsInZhbnVlIjoiaGFuMkkxS3lRbzk1K0tkVG1hRHZBUddYQ1RiSFpid3hxU0ltNFdNVWpHd2tMaDZ6cjdZbk9oRm5lXC9MMk10a1IiLCJtYWMiOiI4NDA2MjQ3OTM0MzA0NDA5Njk3YjI4OTRiMWQ2MzI1NDZlNzI1OTc4YmZlMTI5OWJhYWRLZDhkNmI2ZTAzOWY3In0%3D;
__cf_bm=aEl.uJ84x__jp431JwvKYihGWsdj_rsGuCWUXJ284Gw-1672893707-0-
AV1F6yoGtKy6Wb05dd3qkqkLY4e3awM3o2wQZzmOr4FZ4EqV+dmCHnsnbJMfeb50Ck4B4yN5kNz/fwYOf/iqLIk=
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/99.0.4844.0 Safari/537.36
Host: it-support-tag-aws.fpt-software.it
Connection: Keep-alive
```

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/uxy9rx7HNQ1GY11kPzQh01wx4JwY8wC"
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

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

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

Web Application Firewall detected

This server is protected by an IPS (Intrusion Prevention System), IDS (Intrusion Detection System) or an WAF (Web Application Firewall). Acunetix detected this by sending various malicious payloads and detecting changes in the response code, headers and body.

Impact

You may receive incorrect/incomplete results when scanning a server protected by an IPS/IDS/WAF. Also, if the WAF detects a number of attacks coming from the scanner, the IP address can be blocked after a few attempts.

<https://it-support-tag-aws.fpt-software.it/>

Detected Cloudflare WAF from the headers.

Request

```
GET /9389881 HTTP/1.1
Cookie: XSRF-
TOKEN=eyJpdiI6Ijd5QUURRU1dQRVg2QytYclFwU1BseVE9PSIsInZhbnVlIjoiaWVdXWJkd4Q3JKc0RxE5EVnNyVE56Q1RKK3FyZEYxSmphVE0ydU5qajdpWnp3TzhhQWszV2ZsV0ltU1RPU05TbyIsIm1hYyI6IjI5NjU3ZTdZjY5ZTQzYjYyNmUzODI2ZWlWODIwYjQxYjYzZDZmNGFhYTliNTkyMTRmYjUxZDczMjRjMmY5ZDAifQ%3D%3D;
workplace_bot_ticket_session=eyJpdiI6Im9sR3BvRzVONE9HOG9RbjNQWGUycWc9PSIsInZhbnVlIjoiaGFuMkxS3lRbzk1K0tkVG1hRHZBUddYQlRiSFpid3hxU0ltNFdNVWpHd2tMaDZ6cjdZbk9oRm5lXC9MMk10a1IiLCJtYWMiOiI4NDA2MjQ3OTM0MzA0NDA5Njk3YjI4OTRiMWQ2MzI1NDZlNzI1OTc4YmZlMTI5OWJhYWRLZDhkNmI2ZTAzOWY3In0%3D;
__cf_bm=TxK272th_zOIvWKtwgDKeWcrhLrMncVRqn4XMDfwESk-1672893606-0-AYjlOHhqKwhyWWH2Xxl/hYe+r9G98Lq7AbFz4yJl46qXDUuvGqjhJ+/Cs+c2LmP/ZPJdnLyyg5kU1R5paGyuEFo=
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/99.0.4844.0 Safari/537.36
Host: it-support-tag-aws.fpt-software.it
Connection: Keep-alive
```

Recommendation

If possible, it's recommended to scan an internal (development) version of the web application where the WAF is not active.

Coverage

<https://it-support-tag-aws.fpt-software.it/>

<https://it-support-tag-aws.fpt-software.it/login>