



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



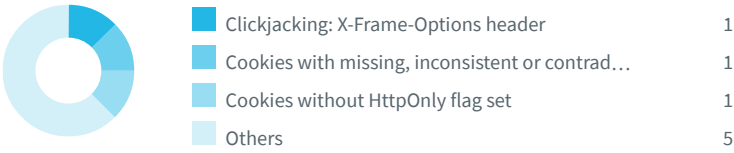
Informational

Severity	Vulnerabilities	Instances
 High	8	8
 Medium	3	3
 Low	8	8
 Informational	6	6
Total	25	25

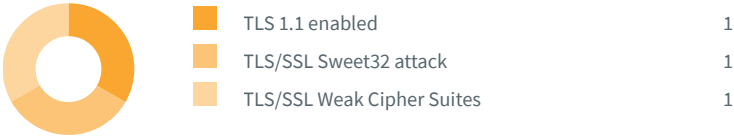
Informational



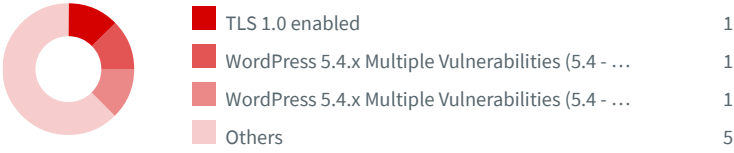
Low Severity





















































Medium Severity



High Severity



Impacts

SEVERITY	IMPACT
 High	 TLS 1.0 enabled
 High	 WordPress 5.4.x Multiple Vulnerabilities (5.4 - 5.4.1)
 High	 WordPress 5.4.x Multiple Vulnerabilities (5.4 - 5.4.2)
 High	 WordPress 5.4.x Multiple Vulnerabilities (5.4 - 5.4.4)
 High	 WordPress 5.4.x Multiple Vulnerabilities (5.4 - 5.4.6)
 High	 WordPress 5.4.x Multiple Vulnerabilities (5.4 - 5.4.8)
 High	 WordPress 5.4.x PHP Object Injection (5.4 - 5.4.5)
 High	 WordPress 5.4.x Prototype Pollution (5.4 - 5.4.9)
 Medium	 TLS 1.1 enabled
 Medium	 TLS/SSL Sweet32 attack
 Medium	 TLS/SSL Weak Cipher Suites
 Low	 Clickjacking: X-Frame-Options header
 Low	 Cookies with missing, inconsistent or contradictory properties
 Low	 Cookies without HttpOnly flag set
 Low	 HTTP Strict Transport Security (HSTS) not implemented
 Low	 Sensitive pages could be cached
 Low	 Session cookies scoped to parent domain
 Low	 WordPress default administrator account
 Low	 WordPress REST API User Enumeration
 Informational	 Content Security Policy (CSP) not implemented
 Informational	 Outdated JavaScript libraries
 Informational	 PHP Version Disclosure
 Informational	 Reverse proxy detected
 Informational	 Subresource Integrity (SRI) not implemented
 Informational	 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://fsoftacademy.fsoft.com.vn/>

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)

<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>

WordPress 5.4.x Multiple Vulnerabilities (5.4 - 5.4.1)

WordPress is prone to multiple vulnerabilities, including cross-site scripting, open redirect and security bypass vulnerabilities. Exploiting these issues could allow an attacker to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site, allowing the attacker to steal cookie-based authentication credentials, to redirect users to arbitrary web sites and conduct phishing attacks, or to bypass certain security restrictions and perform unauthorized actions. WordPress versions 5.4.x ranging from 5.4 and up to (and including) 5.4.1 are vulnerable.

Impact

<https://fsoftacademy.fsoft.com.vn/>

Current WordPress version: 5.4.1.

WordPress versions between 5.4 and 5.4.1 are affected.

Request

GET / HTTP/1.1

Cookie: __cf_bm=pNPvfQKABoWcLfGPC6BrOna7AC0Kv4faSBYj7wH0Yhc-1672902422-0-

AZLK5QgH5eYQ8idxArcxHGucb5JfJIDSr54vN3Dyt2EIDLDTI5yhAoWk3tYJi23nF3rVqC0ef8u4ldgaX9C4CG89U5GX/DdAzWlcPOVOA9vfwQX2BUvNbzNwdFQuZXsVrNnVoQWwX1P+s2bVSBnVfnHvmiMlcugX2h5xlgzWjaoDyAXlh7vLorvis6ge5brpHEn2qeLzFXueYGCwDdPHI=; cf_chl_rc_ni=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: fsoftacademy.fsoft.com.vn
Connection: Keep-alive

Recommendation

Update to WordPress version 5.4.2 or latest

References

<https://pentest.co.uk/labs/research/subtle-stored-xss-wordpress-core/>

<https://pentest.co.uk/labs/research/subtle-stored-xss-wordpress-core/>

<https://www.youtube.com/watch?v=tCh7Y8z8fb4>

<https://www.youtube.com/watch?v=tCh7Y8z8fb4>

<https://wordpress.org/news/2020/06/wordpress-5-4-2-security-and-maintenance-release/>

<https://wordpress.org/news/2020/06/wordpress-5-4-2-security-and-maintenance-release/>

WordPress 5.4.x Multiple Vulnerabilities (5.4 - 5.4.2)

WordPress is prone to multiple vulnerabilities, including cross-site scripting, privilege escalation, security bypass, Denial of Service and PHP object injection vulnerabilities. Exploiting these issues could allow an attacker to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site, allowing the attacker to steal cookie-based authentication credentials and launch other attacks, to bypass the expected capabilities check, to perform otherwise restricted actions and subsequently delete arbitrary files, to deny service to legitimate users, or to possibly execute arbitrary PHP code within the context of the affected webserver process. WordPress versions 5.4.x ranging from 5.4 and up to (and including) 5.4.2 are vulnerable.

Impact

<https://fsoftacademy.fsoft.com.vn/>

Current WordPress version: 5.4.1.

WordPress versions between 5.4 and 5.4.2 are affected.

Request

GET / HTTP/1.1
Cookie: __cf_bm=pNPvfQKABoWcLfGPC6Br0na7AC0Kv4faSBYj7wH0Yhc-1672902422-0-AZLK5QgH5eYQ8idxARcxHGGuicb5JfJIDSr54vN3Dyt2EIDLDOTI5yhAoWk3tYJiZ3nF3rVqC0ef8u41dgaX9C4CG89U5GX/DdAzW1cPOVOA9vfwQX2BUvNbZNwdFQuZXsVrNnVoQWwX1P+s2bVSBnvfnHvMiMlcugX2h5xlgzWjaoDyAXlh7vLorvis6ge5brpHEN2qeLzFXueYGCwDdPHI=; cf_chl_rc_ni=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: fsoftacademy.fsoft.com.vn
Connection: Keep-alive

Recommendation

Update to WordPress version 5.4.3 or latest

References

<https://blog.sucuri.net/2020/10/reflected-xss-in-wordpress-v5-5-1-and-lower.html>

<https://blog.sucuri.net/2020/10/reflected-xss-in-wordpress-v5-5-1-and-lower.html>

<https://blog.wpscan.com/2020/10/30/wordpress-5.5.2-security-release.html>

<https://blog.wpscan.com/2020/10/30/wordpress-5.5.2-security-release.html>

<https://threatpost.com/wordpress-patches-rce-bug/160812/>

<https://threatpost.com/wordpress-patches-rce-bug/160812/>

<https://wordpress.org/support/wordpress-version/version-5-4-3/>
<https://wordpress.org/support/wordpress-version/version-5-4-3/>

WordPress 5.4.x Multiple Vulnerabilities (5.4 - 5.4.4)

WordPress is prone to multiple vulnerabilities, including XML External Entity injection and information disclosure vulnerabilities. Exploiting these issues could allow an attacker to obtain sensitive information which could be used to launch further attacks. WordPress versions 5.4.x ranging from 5.4 and up to (and including) 5.4.4 are vulnerable.

Impact

<https://fsoftacademy.fsoft.com.vn/>

Current WordPress version: 5.4.1.

WordPress versions between 5.4 and 5.4.4 are affected.

Request

```
GET / HTTP/1.1
Cookie: __cf_bm=pNPvfQKABoWcLfgpc6BrOna7AC0Kv4faSBYj7wH0Yhc-1672902422-0-AZLK5QgH5eYQ8idxARcxHGuicb5JfJIDSr54vN3Dyt2EIDLDOTI5yhAoWk3tYJi23nF3rVqC0ef8u41dgaX9C4CG89U5GX/DdAzW1cPOVOA9vfwQX2BUvNbznWdFQuZXsVrNnVoQWwX1P+s2bVSBNvfnHvmiMlcugX2h5xlgzWjaoDyAXlh7vLorvis6ge5brpHEn2qeLzFXueYGCwDdPHI=; cf_chl_rc_ni=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: fsoftacademy.fsoft.com.vn
Connection: Keep-alive
```

Recommendation

Update to WordPress version 5.4.5 or latest

References

<https://blog.sonarsource.com/wordpress-xxe-security-vulnerability/>

<https://blog.sonarsource.com/wordpress-xxe-security-vulnerability/>

<https://github.com/motikan2010/CVE-2021-29447>

<https://github.com/motikan2010/CVE-2021-29447>

<https://wordpress.org/support/wordpress-version/version-5-4-5/>

<https://wordpress.org/support/wordpress-version/version-5-4-5/>

WordPress 5.4.x Multiple Vulnerabilities (5.4 - 5.4.6)

WordPress is prone to multiple vulnerabilities, including cross-site scripting and information disclosure vulnerabilities. Exploiting these issues could allow an attacker to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site, allowing the attacker to steal cookie-based authentication credentials, or to obtain potentially sensitive information that may aid in other attacks. WordPress versions 5.4.x ranging from 5.4 and up to (and including) 5.4.6 are vulnerable.

Impact

<https://fsoftacademy.fsoft.com.vn/>

Current WordPress version: 5.4.1.
WordPress versions between 5.4 and 5.4.6 are affected.

Request

```
GET / HTTP/1.1
Cookie: __cf_bm=pNPvfQKABoWcLfGPC6BrOna7AC0Kv4faSBYj7wH0Yhc-1672902422-0-AZLK5QgH5eYQ8idxArcxHGuicb5JfJIDsr54vN3Dyt2EIDLdotI5yhAoWk3tYJiZ3nF3rVqC0ef8u4ldgaX9C4CG89U5GX/DdAzW1cPOVOA9vfwQX2BUvNbZNwdFQuZXsVrNnVoQWwX1P+s2bVSBNvfnHvMiMlcugX2h5xlgzWjaoDyAXlh7vLorvis6ge5brpHEn2qeLzFXueYGCwDdPHI=; cf_chl_rc_ni=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: fsoftacademy.fsoft.com.vn
Connection: Keep-alive
```

Recommendation

Update to WordPress version 5.4.7 or latest

References

- <https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-wh69-25hr-h94v>
- <https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-m9hc-7v5q-x8q5>
- <https://github.com/lodash/lodash/wiki/Changelog#v41721>
- <https://wordpress.org/support/wordpress-version/version-5-4-7/>

WordPress 5.4.x Multiple Vulnerabilities (5.4 - 5.4.8)

WordPress is prone to multiple vulnerabilities, including cross-site scripting, SQL injection and PHP object injection vulnerabilities. Exploiting these issues could allow an attacker to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site, allowing the attacker to steal cookie-based authentication credentials, to compromise the application, access or modify data, or exploit latent vulnerabilities in the underlying database, or to possibly execute arbitrary PHP code within the context of the affected webserver process. WordPress versions 5.4.x ranging from 5.4 and up to (and including) 5.4.8 are vulnerable.

Impact

<https://fsoftacademy.fsoft.com.vn/>

Current WordPress version: 5.4.1.
WordPress versions between 5.4 and 5.4.8 are affected.

Request

```
GET / HTTP/1.1
Cookie: __cf_bm=pNPvfQKABoWcLfGPC6BrOna7AC0Kv4faSBYj7wH0Yhc-1672902422-0-AZLK5QgH5eYQ8idxArcxHGuicb5JfJIDsr54vN3Dyt2EIDLdotI5yhAoWk3tYJiZ3nF3rVqC0ef8u4ldgaX9C4CG89U5GX/DdAzW1cPOVOA9vfwQX2BUvNbZNwdFQuZXsVrNnVoQWwX1P+s2bVSBNvfnHvMiMlcugX2h5xlgzWjaoDyAXlh7vLorvis6ge5brpHEn2qeLzFXueYGCwDdPHI=; cf_chl_rc_ni=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: fsoftacademy.fsoft.com.vn
Connection: Keep-alive
```

Recommendation

Update to WordPress version 5.4.9 or latest

References

<https://blog.sonarsource.com/wordpress-stored-xss-vulnerability>
<https://blog.sonarsource.com/wordpress-stored-xss-vulnerability>
<https://www.wordfence.com/blog/2022/01/wordpress-5-8-3-security-release/>
<https://www.wordfence.com/blog/2022/01/wordpress-5-8-3-security-release/>
<https://www.zerodayinitiative.com/advisories/ZDI-22-020/>
<https://www.zerodayinitiative.com/advisories/ZDI-22-020/>
<https://www.exploit-db.com/exploits/50663>
<https://www.exploit-db.com/exploits/50663>
<https://wordpress.org/support/wordpress-version/version-5-4-9/>
<https://wordpress.org/support/wordpress-version/version-5-4-9/>

WordPress 5.4.x PHP Object Injection (5.4 - 5.4.5)

WordPress is prone to a vulnerability that lets remote attackers inject and execute arbitrary code because the application fails to sanitize user-supplied input before being passed to the unserialize() PHP function. Attackers can possibly exploit this issue to execute arbitrary PHP code within the context of the affected webserver process. WordPress versions 5.4.x ranging from 5.4 and up to (and including) 5.4.5 are vulnerable.

Impact

<https://fsoftacademy.fsoft.com.vn/>

Current WordPress version: 5.4.1.

WordPress versions between 5.4 and 5.4.5 are affected.

Request

```
GET / HTTP/1.1
Cookie: __cf_bm=pNPvfQKABoWcLfGPC6BrOna7AC0Kv4faSBYj7wH0Yhc-1672902422-0-AZLK5QgH5eYQ8idXARcxHGuicb5JfJIDSr54vN3Dyt2EIDLDTI5yhAoWk3tYJi23nF3rVqC0ef8u4ldgaX9C4CG89U5GX/DdAzWlcPOVOA9vfwQX2BUvNbZNwdFQuZXsVrNnVoQWwX1P+s2bVSBnvfnHvmiMlcugX2h5xlgzWjaoDyAXlh7vLorvis6ge5brpHEn2qeLzFXueYGCwDdPHI=; cf_chl_rc_ni=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: fsoftacademy.fsoft.com.vn
Connection: Keep-alive
```

Recommendation

Update to WordPress version 5.4.6 or latest

References

<https://github.com/JamesGeee/CVE-2020-36326>
<https://github.com/JamesGeee/CVE-2020-36326>
<https://wordpress.org/support/wordpress-version/version-5-4-6/>
<https://wordpress.org/support/wordpress-version/version-5-4-6/>

WordPress 5.4.x Prototype Pollution (5.4 - 5.4.9)

WordPress is prone to a prototype pollution vulnerability. Exploiting this issue could allow an attacker to inject key/value properties into JavaScript objects, potentially allowing for execution of arbitrary JavaScript in a user's session if they can trick that user into clicking a link. WordPress versions 5.4.x ranging from 5.4 and up to (and including) 5.4.9 are vulnerable.

Impact

<https://fsoftacademy.fsoft.com.vn/>

Current WordPress version: 5.4.1.
WordPress versions between 5.4 and 5.4.9 are affected.

Request

```
GET / HTTP/1.1
Cookie: __cf_bm=pNPvfQKABoWcLfgpc6BrOna7AC0Kv4faSBYj7wH0Yhc-1672902422-0-AZLK5QgH5eYQ8idxArcxHGuicb5JfJIDSr54vN3Dyt2EIDLDOTI5yhAoWk3tYJi23nF3rVqC0ef8u41dgaX9C4CG89U5GX/DdAzW1cPOVOA9vfwQX2BUvNbznWdFQuZXsVrNnVoQWwX1P+s2bVSBNvfnHvmiMlcugX2h5xlqzWjaoDyAXlh7vLorvis6ge5brpHEn2qeLzFXueYGCwDdPHI=; cf_chl_rc_ni=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: fsoftacademy.fsoft.com.vn
Connection: Keep-alive
```

Recommendation

Update to WordPress version 5.4.10 or latest

References

- <https://github.com/BlackFan/client-side-prototype-pollution/blob/master/pp/jquery-query-object.md>
- <https://github.com/BlackFan/client-side-prototype-pollution/blob/master/pp/jquery-query-object.md>
- <https://wordpress.org/support/wordpress-version/version-5-4-10/>
- <https://wordpress.org/support/wordpress-version/version-5-4-10/>

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://fsoftacademy.fsoft.com.vn/>

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>

[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://fsoftacademy.fsoft.com.vn/>

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://fsoftacademy.fsoft.com.vn/>

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>

[RFC 9155: Deprecating MD5 and SHA-1 Signature Hashes in TLS 1.2 and DTLS 1.2](https://datatracker.ietf.org/doc/html/rfc9155)

<https://datatracker.ietf.org/doc/html/rfc9155>

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://fsoftacademy.fsoft.com.vn/>

Paths without secure XFO header:

- <https://fsoftacademy.fsoft.com.vn/wp-content/plugins/activehelper-livehelp/server/offline.php>
- <https://fsoftacademy.fsoft.com.vn/wp-content/plugins/topquark/lib/js/fancyupload/showcase/batch/script.php>
- <https://fsoftacademy.fsoft.com.vn/wp-content/plugins/ss-downloads/templates/emailsent.php>
- https://fsoftacademy.fsoft.com.vn/wp-content/plugins/spider-calendar/front_end/spidercalendarbig_seemore.php
- https://fsoftacademy.fsoft.com.vn/wp-content/plugins/wp-football/football_matches_load.php
- <https://fsoftacademy.fsoft.com.vn/wp-content/plugins/compfight/compfight-search.php>
- <https://fsoftacademy.fsoft.com.vn/wp-content/plugins/zotpress/zotpress.rss.php>
- <https://fsoftacademy.fsoft.com.vn/wp-content/plugins/forum-server/wpf-insert.php>
- <https://fsoftacademy.fsoft.com.vn/wp-content/plugins/spotlightyour/library/includes/payment/paypalexpress/DoDirectPayment.php>
- <https://fsoftacademy.fsoft.com.vn/wp-content/plugins/wpforum/wp-forum-manage.php>
- <https://fsoftacademy.fsoft.com.vn/wp-content/plugins/thecartpress/checkout/CheckoutEditor.php>
- <https://fsoftacademy.fsoft.com.vn/wp-content/plugins/fbpromotions/admin/swarm-settings.php>
- <https://fsoftacademy.fsoft.com.vn/wp-content/plugins/wp-auctions/admin.php>
- <https://fsoftacademy.fsoft.com.vn/wp-content/plugins/firestats/php/ajax-handler.php>
- <https://fsoftacademy.fsoft.com.vn/wp-content/plugins/thecartpress/admin/OptionsPostsList.php>

- <https://fsoftacademy.fsoft.com.vn/wp-content/plugins/eventify/php/ajax/fetcheventdetails.php>
- https://fsoftacademy.fsoft.com.vn/wp-content/plugins/wp-bannerize/ajax_sorter.php
- <https://fsoftacademy.fsoft.com.vn/wp-content/plugins/immopress/sdk/Oauth/example/index.php>
- <https://fsoftacademy.fsoft.com.vn/wp-content/plugins/dm-albums/dm-albums.php>
- https://fsoftacademy.fsoft.com.vn/wp-content/plugins/wp-football/football_groups_list.php
- <https://fsoftacademy.fsoft.com.vn/wp-content/plugins/pure-html/alter.php>

Request

```
POST /undefined HTTP/1.1
Host: fsoftacademy.fsoft.com.vn
Content-Length: 1890
accept-language: en-US
cf-challenge: e10c8dd650f4ae9
content-type: application/x-www-form-urlencoded
accept: */*
origin: https://fsoftacademy.fsoft.com.vn
cookie: __cf_bm=BkGBYTrCm8F8UXDR5LDny6Lx_HrIf65Fk6H3k5XQPYw-1672902248-0-AQeGwYsUCha24PzMkhdQ5PSxfr9Vn2x32Id9BA08jfK1L/Tx03PuHH+Bk+6//yTMB0ZIK+TfvcEo5SV8TV6gWXrNnHt+k2T9VChhr4wS1Hr
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://fsoftacademy.fsoft.com.vn/
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.0 Safari/537.36

v_784a5b362cd04aad=hLuV-VeVwVOV2nrtarcVm-PWV3zjaLXE0rq69KVJLVrgLrB6V5LO2tuES9r2rEXaBKBEpawrQvPvRFQdVEq3rrzi8VuuE$3tFFrD3h-
ZPQnyuwGFnrawn5X$VIuBrdVQR4rWxEwTzV0ur-raSrFPED5rrNradrCPEo3VrKe9j57uEe36CYTaByp5z1r9Brtq5qQMMreZC4C63PvR8r71CDt6L1PhyrBXEOHxQrEv2f5rj-
rJ7s9bbuR3ss5Ky6mXrp7Oic5Pn6mMCgV9zpw-
iOm2ML1YwzVaQnbh8cJdFPVAm1zq2gn1jb4g6ttSyqQBVVFLy%2bnVHxMppi2XnqQwi$US$mRQuypBZfwyVVInny6LQwBra8LVEWIjomqo9b5aLren5u18RrVntB+qB-
9Gf9SOIrbD3Xt5c5QusMMhggreyqE3MJAibwmVrxpjryFXBCWFPClrr81DJGQOIAT5brw3faAIdQzQ-
PoSfVEBpNfdrGDFEPbhZ53QwbelSU5QaaEN2zTolzuiYOCujyhid$XRNyRtfRrDYc-eauyL2EcurEyyfQweEPi1BdEnBeaI2GI2rqaM+qgI2Mb-1-NX01j-G5H2Ln$L-
eUPxiyeaTwBF1wdS0Gg3bO11CVVtSJOV5QSynB2dulomTWvr9O3feuwL7GFQ2OPMzrSDP$ZJFOgdDe5onxDcJg7FQp3SanP3+xE$2FVhL42XJuD$33-
uQSaunnb9pWl53eCParz98wXza50rtZr2VCy0JyXEBc-iJr4jvQGrGJJXaMoMpFB1rDpOmCPCyXEQarpEBcpJtLm-
6xMTjzEQer69BpQ7pZquAEcHXxXjwXhwzh74Qa9jACQdEe2iJ3UCVm-DEP5uhwVzVtYatJcWze-HrnCyCy7a3Zp$hrOQOWL197egnMwNV8JaarOJWtXurh5uxD3auLrV0Pu$am-
aEBdPn1LJEm9Syuhtw0FJFWH-
n9LtyxfOy362Ty2ZtB0rOaVdeZEQp3ZeZPLtPhe8qVDQP7wVCqeQ7cuCZZWAP2reDZZZPLqcCZerhHX0eLwXArdqFng0uz0EiNrjCP356azdEJqVh7DCacoDJuTO62MjyqM6d8XrOH
-JyGTjD2dv-ATjtqVdS2pUe85P-QSPA2QwmXq2P3-meay3iazu7eeUpuyh8TruVnaqDJGTr-Qaartt+NEIEgCq3M6PV8Q7PAY1MR-
DQ6mqzwbC$fazaEaJIQR3$LPu8CnTLCZydEDE0CE4avdpZCTc3J24No+JGc3mCXPq1-prX1aT5rcCT5jjeLEvb1RJ3rg75PCwbw-
rxQz3sEQCqQM0TOP1B0pf9LaMtFVWAg2PcuatZP7pPyMta10puUj4-nlLdpdY117orqBcuwHPJ3SJIHX6Egwz-CXtXACTJZr6z2qIaYtu7FeQr8QM37V66PuLn5m-
r6QVDpu79U4sWZpW8$7r1rLTjgSaa3Sa5e-QywuPutpNZynlBaMDFmWan9Wauz$3Zy-
rOyux1VhLtQwm$W4XNq3QaJuJaD03QMyCytWICzfJXwzPyab2rQLd8Q89LvJPIcpPiVznvnbhVhzz$YunQauM3XyPjE-
9wJyPuOuuawa5hzd8lapCe$Zai552p4aqeJaimViPXasrTPZPeE+ryJXJVPLbOHr$Zya5yuHpgqvKXeOuJu63JPSQ6uvEu7LzrBEn3dar6DHC8JXTLwzOuxvQJL9QhLG-Vq-
ab5bJrjPcr+989gpuGEWLPQUBvAufEaa89yIhNrXpjjabJrwrTPvYrJeyd8tOsa5eyCjzGou5FhEB3Pzu7AUCTp$eueUurra4cESCSJLuvN3bjMab6uEQ7jdriIrIWGQyM07wd$rr
```

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](#)

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://fsoftacademy.fsoft.com.vn/>

Verified

List of cookies with missing, inconsistent or contradictory properties:

- <https://fsoftacademy.fsoft.com.vn/wp-comments-post.php>

Cookie was set with:

```
Set-Cookie: comment_author_9e4a81fe01e040a3e779d6c0e0806a09=tsSLAueP; expires=Tue, 19-Dec-2023 08:04:07 GMT; Max-Age=30000000; path=/; secure
```

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://fsoftacademy.fsoft.com.vn/wp-comments-post.php>

Cookie was set with:

```
Set-Cookie: comment_author_email_9e4a81fe01e040a3e779d6c0e0806a09=sample%40email.tst; expires=Tue, 19-Dec-2023 08:04:07 GMT; Max-Age=30000000; path=/; secure
```

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://fsoftacademy.fsoft.com.vn/wp-comments-post.php>

Cookie was set with:

```
Set-Cookie: comment_author_url_9e4a81fe01e040a3e779d6c0e0806a09=http%3A%2F%2Fwww.vulnweb.com; expires=Tue, 19-Dec-2023 08:04:07 GMT; Max-Age=30000000; path=/; secure
```

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://fsoftacademy.fsoft.com.vn/wp-comments-post.php>

Cookie was set with:

```
Set-Cookie: comment_author_9e4a81fe01e040a3e779d6c0e0806a09=tsSLAueP; expires=Tue, 19-Dec-2023 08:50:33 GMT; Max-Age=30000000; path=/; secure
```

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://fsoftacademy.fsoft.com.vn/wp-comments-post.php>

Cookie was set with:

```
Set-Cookie: comment_author_email_9e4a81fe01e040a3e779d6c0e0806a09=sample%40email.tst; expires=Tue, 19-Dec-2023 08:50:33 GMT; Max-Age=30000000; path=/; secure
```

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://fsoftacademy.fsoft.com.vn/wp-comments-post.php>

Cookie was set with:

```
Set-Cookie: comment_author_url_9e4a81fe01e040a3e779d6c0e0806a09=http%3A%2F%2Fwww.vulnweb.com; expires=Tue, 19-Dec-2023 08:50:33 GMT; Max-Age=30000000; path=/; secure
```

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://fsoftacademy.fsoft.com.vn/wp-login.php>

Cookie was set with:

```
Set-Cookie: wordpress_test_cookie=WP+Cookie+check; path=/; secure
```

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

```
POST /wp-login.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Referer: https://fsoftacademy.fsoft.com.vn/
Cookie: __cf_bm=_kRm3_B8gMA6I38JXa_t8wWgpRlGQVqf1IZsDOIT7A4-1672907005-0-AeK3kxF2e7SNUzmPb/bIz76pckXWxlJ1WKvWPWMBDf8g6PE0ioAWRgvqXptFxxqSqBmFi8u8+caeT5znVwfwAeCeufCZDwY4YAe/jxbgxN; cf_chl_rc_ni=2;
```

```
cf_chl_2=6bbd62a16768ad4
Content-Length: 42
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: fsoftacademy.fsoft.com.vn
Connection: Keep-alive
```

```
log=admin&pwd=acunetix&wp-submit=Login
```

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)

<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/)

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

[Cookies: HTTP State Management Mechanism](https://tools.ietf.org/html/draft-ietf-httpbis-rfc6265bis-05)

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

[SameSite Updates - The Chromium Projects](https://www.chromium.org/updates/same-site)

<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)

<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.

Impact

Cookies can be accessed by client-side scripts.

<https://fsoftacademy.fsoft.com.vn/>

Verified

Cookies without HttpOnly flag set:

- <https://fsoftacademy.fsoft.com.vn/wp-comments-post.php>

```
Set-Cookie: comment_author_9e4a81fe01e040a3e779d6c0e0806a09=tsSLAueP; expires=Tue, 19-Dec-2023 08:04:07 GMT; Max-Age=30000000; path=/; secure
```

- <https://fsoftacademy.fsoft.com.vn/wp-comments-post.php>

```
Set-Cookie: comment_author_email_9e4a81fe01e040a3e779d6c0e0806a09=sample%40email.tst; expires=Tue, 19-Dec-2023 08:04:07 GMT; Max-Age=30000000; path=/; secure
```

- <https://fsoftacademy.fsoft.com.vn/wp-comments-post.php>

```
Set-Cookie: comment_author_url_9e4a81fe01e040a3e779d6c0e0806a09=http%3A%2F%2Fwww.vulnweb.com; expires=Tue, 19-Dec-2023 08:04:07 GMT; Max-Age=30000000; path=/; secure
```


- <https://fsoftacademy.fsoft.com.vn/wp-comments-post.php>

```
Set-Cookie: comment_author_9e4a81fe01e040a3e779d6c0e0806a09=tsSLAueP; expires=Tue, 19-Dec-2023 08:50:33 GMT; Max-Age=30000000; path=/; secure
```

- <https://fsoftacademy.fsoft.com.vn/wp-comments-post.php>

```
Set-Cookie: comment_author_email_9e4a81fe01e040a3e779d6c0e0806a09=sample%40email.tst; expires=Tue, 19-Dec-2023 08:50:33 GMT; Max-Age=30000000; path=/; secure
```

- <https://fsoftacademy.fsoft.com.vn/wp-comments-post.php>

```
Set-Cookie: comment_author_url_9e4a81fe01e040a3e779d6c0e0806a09=http%3A%2F%2Fwww.vulnweb.com; expires=Tue, 19-Dec-2023 08:50:33 GMT; Max-Age=30000000; path=/; secure
```

- <https://fsoftacademy.fsoft.com.vn/wp-login.php>

```
Set-Cookie: wordpress_test_cookie=WP+Cookie+check; path=/; secure
```

Request

```
POST /wp-login.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Referer: https://fsoftacademy.fsoft.com.vn/
Cookie: __cf_bm=_kRm3_B8gMA6I38JXa_t8wWgpRlGQVqf1IZsDOIT7A4-1672907005-0-AeK3kxF2e7SNUzmPb/bIz76pckXWhx1J1WKvWPWmBDf8g6PE0ioAWRGvqXptFxxqSqBmFi8u8+caeT5znVwfWoAeCeufCZDwY4YAe/jxbgxN; cf_chl_rc_ni=2; cf_chl_2=6bbd62a16768ad4
Content-Length: 42
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: fsoftacademy.fsoft.com.vn
Connection: Keep-alive

log=admin&pwd=acunetixtest&wp-submit=Login
```

Recommendation

If possible, you should set the HttpOnly 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://fsoftacademy.fsoft.com.vn/>

URLs where HSTS is not enabled:

- <https://fsoftacademy.fsoft.com.vn/wp-content/plugins/activehelper-livehelp/server/offline.php>
- <https://fsoftacademy.fsoft.com.vn/wp-content/plugins/topquark/lib/js/fancyupload/showcase/batch/script.php>
- <https://fsoftacademy.fsoft.com.vn/wp-content/plugins/ss-downloads/templates/emailsent.php>
- https://fsoftacademy.fsoft.com.vn/wp-content/plugins/spider-calendar/front_end/spidercalendarbig_seemore.php
- https://fsoftacademy.fsoft.com.vn/wp-content/plugins/wp-football/football_matches_load.php
- <https://fsoftacademy.fsoft.com.vn/wp-content/plugins/compfight/compfight-search.php>
- <https://fsoftacademy.fsoft.com.vn/wp-content/plugins/zotpress/zotpress.rss.php>
- <https://fsoftacademy.fsoft.com.vn/wp-content/plugins/forum-server/wpf-insert.php>
- <https://fsoftacademy.fsoft.com.vn/wp-content/plugins/spotlightyour/library/includes/payment/paypalexpress/DoDirectPayment.php>
- <https://fsoftacademy.fsoft.com.vn/wp-content/plugins/wpforum/wp-forum-manage.php>
- <https://fsoftacademy.fsoft.com.vn/wp-content/plugins/thecartpress/checkout/CheckoutEditor.php>
- <https://fsoftacademy.fsoft.com.vn/wp-content/plugins/fbpromotions/admin/swarm-settings.php>
- <https://fsoftacademy.fsoft.com.vn/wp-content/plugins/wp-auctions/admin.php>
- <https://fsoftacademy.fsoft.com.vn/wp-content/plugins/firestats/php/ajax-handler.php>
- <https://fsoftacademy.fsoft.com.vn/wp-content/plugins/thecartpress/admin/OptionsPostsList.php>
- <https://fsoftacademy.fsoft.com.vn/wp-content/plugins/eventify/php/ajax/fetcheventdetails.php>
- https://fsoftacademy.fsoft.com.vn/wp-content/plugins/wp-bannerize/ajax_sorter.php
- <https://fsoftacademy.fsoft.com.vn/wp-content/plugins/immopress/sdk/Oauth/example/index.php>
- https://fsoftacademy.fsoft.com.vn/wp-content/plugins/wp-football/football_groups_list.php
- <https://fsoftacademy.fsoft.com.vn/wp-content/plugins/dm-albums/dm-albums.php>
- <https://fsoftacademy.fsoft.com.vn/wp-content/plugins/pure-html/alter.php>

Request

```
POST /undefined HTTP/1.1
Host: fsoftacademy.fsoft.com.vn
Content-Length: 1890
accept-language: en-US
cf-challenge: e10c8dd650f4ae9
content-type: application/x-www-form-urlencoded
accept: */*
origin: https://fsoftacademy.fsoft.com.vn
cookie: __cf_bm=BkGBYTrCm8F8UXDR5LDny6Lx_HrIf65Fk6H3k5XQPYw-1672902248-0-AQeGwYsUCha24PzMkhdQ5PSxfr9Vn2x32Id9BA08jfk1L/Tx03PuHH+Bk+6//yTMB0ZIK+TfvcEo5SV8TV6gWXrNnHt+k2T9VChhr4wS1Hr
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://fsoftacademy.fsoft.com.vn/
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.0 Safari/537.36

v_784a5b362cd04aad=hLuV-VeVwVOV2nrtarcVm-PWV3zjaLXE0rq69KVJLVrgLrB6V5LO2tuES9r2rEXaBKBEpawrQvPvRFQdVEq3rrzi8VuuE$3tFFrD3h-
ZPQnyuwGFnrawn5X$VIuBrdVQR4rWxEwTzV0ur-raSrFPED5rrNradrCPeO3VrKe9j57uEe36CYTaByp5z1r9Brtq5qMMreZC4C63PvR8r7lCDt6L1PhyrBXEOHxQrEv2f5rj-
rJ7s9bbuR3ss5Ky6mXrp7Oic5Pn6mMCgV9zpw-
iOm2ML1YwzVaQnbh8cJdFPVaM1zq2gn1jb4g6ttSyqQBvVf1y%2bnVHXmPpi2XnqQwi$US$mRQuypBZfwyVVInny6LQwBra8LVEWIjomoq9b5aLren5ul8RrVntB+qB-
9Gf9SOIrbD3Xt5cQusMMhggreyqE3MJAibwmVrxpjryFXBCWFcPlrr81DJGQOIAI5brw3faAIdQzQ-
PoSfVEbPnFdrGDFEpbhz53QwbelSU5QaaEN2zTolzuiYOCujyhid$XRNyRtfrRDYc-eauyL2EcurEyyfQweEPilBdEnBeaI2GI2rqaM+qgI2Mb-1-NX01j-G5HZLn$L-
eUPxiyaeTaWbFlwdSOGg3b01lCVvtSJJOVSQSynB2dulomTWvr9O3feuwL7GFQ2OPMzrSDP$ZJFOgdDe5onxDCjg7FQp3SanP3+xPe$ZFVhL42XJuD$33-
uQSaunnb9pwWI53eCParz98wXza50rtZr2VCy0JyXEBc-iJr4jvQGrGXXaMoMpFB1rDpOmCPCyXEQarpEBcpJtLm-
6xMTjzEQR69BpQ7pQzuAEcHxxXjwXhwzh74Qa9jACQdEe2iJ3UCVm-DEP5uhwVzVtYaTjCwze-HrnCyCy7a3Zp$hrOQ0WL197egnMwNV8JaarOJWtXurh5uxD3auLrV0Pu$am-
aEBdPn1LJEm9Syuhtw0FJFWH-
n9Ltyxf0y362Ty2ZtB0rOaVdZEQp3ZeZPLtPhe8qVDQP7wVCqeQ7cuCZZWAP2reDZZZZPLqcCZerhHX0eLwXArdqFng0uz0EiNrjCP356azdEJqVh7DCacoDJuTO62MJyqM6d8XrOH-
~JyGTjD2dv-ATjtqVdSZpUe85P-QSPA2QwmXq2P3-meay3iazu7eeUpuyh8TruVnaqDJGTr-Qaartt+NEIEGcQ3M6PV8Q7PAY1MR-
DQ6mqZwbC$faZaEaJlQR3$LPu8CnTLCZydeDE0CE4avdpZCTc3J24No+JGc3mCXPql-pRXlaT5rcCT5jjeLEvb1RJ3rg75PCwbw-
rxQz3sEQCqQM0TOP1B0pf9LaMtFVWAg2PcuuatZP7pPyMta10puUj4-nlLdpdY17orqBcuwHPJ3SJIHX6EgWz-CXtXACTJZr6z2qIaYTu7FeQR8QM37V66PuLn5m-
r6QVDpu79U4sWZpW8$7r1rLTJtgSaa3Sa5e-QywuPtNZyn1BaMDFmWan9Wauz$3Zy-
rOyux1VhLtQwm$W4XNq3QaJuJaD03QMqCytWICZfJXwxPyab2rQLd8Q89LvJPicpPiVznvnbhVhz$YunQauM3XyPjE-
9wJyuPOuuawa5hzd8lapCe$Zai552p4aqeJaimViPXasrnTFZPeE+ryJXJVPLbOHr$2ya5yuHpgvKXeOuJu63JPSQ6uvEu7LzrBen3dar6DHC8JXTLwzOuxvQJL9qhLG-Vq-
ab5bJrjPcr+989gpuGEWLPQuBvaufEaa89yIhNrXpqjjabJrwzTprVyJIEydh2Osa5eyCjzGou5FhEB3Pzu7AUCTp$eueUurra4cESCSJLuvN3bjMab6uEQ7jdrirIWGQyMO7wd$rr
```

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/>

[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>

Sensitive pages could be cached

One or more pages contain possible sensitive information (e.g. a password parameter) and could be potentially cached. Even in secure SSL channels sensitive data could be stored by intermediary proxies and SSL terminators. To prevent this, a Cache-Control header should be specified.

Impact

Possible sensitive information disclosure.

<https://fsoftacademy.fsoft.com.vn/>

List of pages that could be cached:

- <https://fsoftacademy.fsoft.com.vn/wp-content/plugins/wpforum/wp-forum-manage.php?editgroupsbmit=true&group=1&groupname=acunetix&passwd=acunetix>
- <https://fsoftacademy.fsoft.com.vn/wp-content/plugins/wpforum/sendmail.php?user=1>

Request

```
GET /wp-content/plugins/mailz/lists/dl.php?id=0&user=root&wpdb=test&wph=localhost&wpp=root HTTP/1.1
Referer: https://fsoftacademy.fsoft.com.vn/
Cookie: __cf_bm=hPwTs9QwsYnY9KgZICV9J__1SYx1ecqVuLgzeRIRJ2o-1672912978-0-
AduaKXykzhtAVA8BmP/PinmtEGNXtejzXuWemb0/D0WA8tK2l77YF0RzUvQNpZO5PyjZPjc6oJl1De9nFhVYrgopQdo9iMRtD9Tgs+3yQbet;
wordpress_test_cookie=WP+Cookie+check; cf_chl_2=d20267b70c0835b; cf_chl_rc_ni=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: fsoftacademy.fsoft.com.vn
Connection: Keep-alive
```

Recommendation

Prevent caching by adding "Cache Control: No-store" and "Pragma: no-cache" to the HTTP response header.

Session cookies scoped to parent domain

One ore 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://fsoftacademy.fsoft.com.vn/>

Verified

Session cookies scoped to parent domain:

- <https://fsoftacademy.fsoft.com.vn/wp-content/plugins/activehelper-livehelp/server/offline.php>

Set-Cookie: __cf_bm=dz.Ldben996D9IBqn44Xb2UrEqt6mSowwekHOpmWR.s-1672972044-0-
AbzK+LR4qB2VBi4jw68UGfGBmsyXLZu+dnni61M6y6+cEdT439jJ/JZmfcp0heEG6MxAfZ/sQdREZ3izieldKmJ0LGil4iBkxprA9FLXDiP;
path=/; expires=Fri, 06-Jan-23 02:57:24 GMT; domain=.fsoft.com.vn; HttpOnly; Secure; SameSite=None

- <https://fsoftacademy.fsoft.com.vn/wp-content/plugins/activehelper-livehelp/server/offline.php>

Set-Cookie: __cf_bm=N0gERy6fXgffGZw.rGHppnQ7wRjw19CwMjS.8S634g0-1672972112-0-
Af+Xf1cUJUOD/Grdj4U+KR8IBJZ15f0UWOzyYED/dHjiLMF5D3HUHES65+vdwyPFnlYSCgvD+7yB53rHR0PPOzHiSjN3ihYiwGfKYrriS3DL;
path=/; expires=Fri, 06-Jan-23 02:58:32 GMT; domain=.fsoft.com.vn; HttpOnly; Secure; SameSite=None

- <https://fsoftacademy.fsoft.com.vn/wp-content/plugins/activehelper-livehelp/server/offline.php>

Set-Cookie: __cf_bm=dYd5bsep09tTAYF6lcKL7X8gIQoKFLbXwTKgiAvH6e4-1672972177-0-
AWti6LL+9pbkBlH6w7Dk403G6SlGBX5NiiLoQ3uc9ODyRcNcfXyLjaZ0q5zEy2ccDTbFFJ3fvKRhn4gf918XBK4BF+MDMc1893ixoYJ2L1d;
path=/; expires=Fri, 06-Jan-23 02:59:37 GMT; domain=.fsoft.com.vn; HttpOnly; Secure; SameSite=None

- https://fsoftacademy.fsoft.com.vn/wp-content/plugins/spider-calendar/front_end/spidercalendarbig_seemore.php

Set-Cookie: __cf_bm=TmiwS5c38q4JaIzh49yVXYGdRL.gjGChRtJBCMtGjcQ-1672972284-0-
AWxLl/bIT98J9Z1GP3F/sDVLuwcc6xWRbLhQ/bwebirAdZ5LMfehZ4FnIHk5fXXjmmgHb1JAmb8X2GPFCKw3m+qMBFbCR1VWEKkFnrit600j;
path=/; expires=Fri, 06-Jan-23 03:01:24 GMT; domain=.fsoft.com.vn; HttpOnly; Secure; SameSite=None

- https://fsoftacademy.fsoft.com.vn/wp-content/plugins/wp-football/football_matches_load.php

Set-Cookie: __cf_bm=JBGFYYo4RUo275BtGeU0UQ5zssyEOvyA6apcq.szk4E-1672972285-0-
AbdnSM/T4HRZVZTqz4n+WzXs2kcjjeItYmN9Ho2wkbTOG/7Rjlcwx4GT8J4dZ+w9JZATPFwtrO4dr72bStRY14B+OAb1k0UT/jBZj5ArqHRP;
path=/; expires=Fri, 06-Jan-23 03:01:25 GMT; domain=.fsoft.com.vn; HttpOnly; Secure; SameSite=None

- <https://fsoftacademy.fsoft.com.vn/wp-content/plugins/zotpress/zotpress.rss.php>

Set-Cookie: __cf_bm=vOXA1fqz6BVnPQMsw4U6nNB9kvuSonVgI6YBDeIzyXM-1672972360-0-
AcgTRL6DMz5i/dcLFxflwmDMO7FauwVjifVs7BRjSDVB90YtZIZfDOWH+lvXun2U5ROASfdNgLbewN6sG0A4joitWt8Phhyf2aTZipZiEGk;
path=/; expires=Fri, 06-Jan-23 03:02:40 GMT; domain=.fsoft.com.vn; HttpOnly; Secure; SameSite=None

- https://fsoftacademy.fsoft.com.vn/cdn-cgi/challenge-platform/h/b/beacon/ov1/0.5806607074855685:1672909551:lQVQM55JIRbDm_VUptOPldfuWOqkJyVzUPOxcfSSshA/784b5d03ec2da132/97751d8e34c075e/non-interactive

Set-Cookie: __cf_bm=IRR4gl2JmQJYqEQdP77xZ51CcREOZ11JdRMMOivY250-1672972449-0-
AZFwSpXjrIiYUk2FlzxJodTv+aCQIrV4Z4YWCrBZqpbPERDjRFEnTusjlFH8OciFqgcPZ3nNxvXEqSPKzvbJJ+RwXXyhSXG1ddZUvrAnthHT;
path=/; expires=Fri, 06-Jan-23 03:04:09 GMT; domain=.fsoft.com.vn; HttpOnly; Secure; SameSite=None

- <https://fsoftacademy.fsoft.com.vn/wp-content/plugins/thecartpress/checkout/CheckoutEditor.php>

Set-Cookie: __cf_bm=QFDSVnYxAn7dFOtLEJgSQrBjmuSlM3h00qPlDBcUEQ-1672972466-0-
ATt2fKiaVP+BeGKAXu/O9u9NQ8zm5Q88Yx6i2A+yfWTG4f+2ybJFc10xA65VvQ4UzDDQ1SpplSECMsrxaflq7iFjpMkGqzaUAdhYx+BNUwzU;
path=/; expires=Fri, 06-Jan-23 03:04:26 GMT; domain=.fsoft.com.vn; HttpOnly; Secure; SameSite=None

- <https://fsoftacademy.fsoft.com.vn/wp-content/plugins/firestats/php/ajax-handler.php>

Set-Cookie: __cf_bm=R86KvKL41367RB2sK26ItpnD7ns7nusmuaQxShc5kFE-1672972506-0-AwLrLRNmGUA5AXg9EkKPG2OuZbvwxFb7mxcqYIMYyk3vvALxN4LfOl6pdFfuNGPnLE7TlWdD2B98pM7DBRjESdNin7Yn/8MXS48QsLlGqjQQU; path=/; expires=Fri, 06-Jan-23 03:05:06 GMT; domain=.fsoft.com.vn; HttpOnly; Secure; SameSite=None

- <https://fsoftacademy.fsoft.com.vn/wp-content/plugins/thecartpress/admin/OptionsPostsList.php>

Set-Cookie: __cf_bm=ipMadWf7DqBTqy5C8.HLYEOz27e56Z.ZECjrkobfJts-1672972516-0-AcNSdz/C7IkExoWw+ZK5WWUMPP1BkQ0nIlpTDVgUzU1cg7FmGyZ7XRaxYn27HRRc2WQ2aGeagEOX/IXo+jW6igidNmT0zdI8c5TAMtxWAs4Q; path=/; expires=Fri, 06-Jan-23 03:05:16 GMT; domain=.fsoft.com.vn; HttpOnly; Secure; SameSite=None

- <https://fsoftacademy.fsoft.com.vn/wp-content/plugins/eventify/php/ajax/fetcheventdetails.php>

Set-Cookie: __cf_bm=pdH5CBxgKEEJvvyUzP5lGX6ap21IOpHRcymbkcvVkvVw-1672972530-0-AfFw86ZRxG/jaj6FAhom6cTxjMbG+rHuv8qRJu9aYmwhigKMuuMs4MMoUHJo/fb5dwV4IB3A4M2bCIT4tc413xjZBUrvycAls54yvOaZENP; path=/; expires=Fri, 06-Jan-23 03:05:30 GMT; domain=.fsoft.com.vn; HttpOnly; Secure; SameSite=None

- <https://fsoftacademy.fsoft.com.vn/cdn-cgi/challenge-platform/h/b/beacon/ov1/0.44402211295220734:1672909558:5PtflHU12TYZRhIqx1yU1tOLTxDK8iiRwdNFUq2Ms/784b5d041d6cab5f/d20267b70c0835b/non-interactive>

Set-Cookie: __cf_bm=USXzjAJy3MphAjFt7TMn8TO7CAjv68nBn_xZckhYjuA-1672972545-0-AUITTQLlmjDVcvI8pyyTmyOVSXF9RDJffU1/Lbn5R/DXb5JZQpBg+xb0Ocao0ZGZogWwmKa57ViZ0K4OkkyXzmrXzxpjnHr0/jd5oIXo7H3y; path=/; expires=Fri, 06-Jan-23 03:05:45 GMT; domain=.fsoft.com.vn; HttpOnly; Secure; SameSite=None

- <https://fsoftacademy.fsoft.com.vn/wp-content/plugins/editormonkey/fckeditor/editor/filemanager/upload/test.html>

Set-Cookie: __cf_bm=4zsBZriMo06pzmt7scKRIF9VER1Q8LnoUAMy7gfwsHc-1672972579-0-AbuifZNdzjUHjRu0ilcfrbTohIIfLRV1xe9baXMM4MT4159LH3aheqexng2YzMovWO4X8JbTJZzyJtb/aSq7zSWh4OX5nNURHYgg0Yy+OhB9; path=/; expires=Fri, 06-Jan-23 03:06:19 GMT; domain=.fsoft.com.vn; HttpOnly; Secure; SameSite=None

- <https://fsoftacademy.fsoft.com.vn/wp-content/plugins/pure-html/alter.php>

Set-Cookie: __cf_bm=dx6xm_lsA4AfwmdZOTJTAFkkGlllsZzeqqlnmOrc9o-1672972594-0-Afssqn8v0x6tliPK0imtE+9vmtujItltOqiSgGATxC0uuvnMBGpQiUyJrtm/QFCg25U6bVmF9oKjIKA6L8Iu8cyHckaCBIRj04i4ejL7s50my; path=/; expires=Fri, 06-Jan-23 03:06:34 GMT; domain=.fsoft.com.vn; HttpOnly; Secure; SameSite=None

- https://fsoftacademy.fsoft.com.vn/wp-content/plugins/wp-realty/index_ext.php

Set-Cookie: __cf_bm=.3cnAkuKVkinSrS.1YXsNXlhGF40lQygzv0QRt60Y7s-1672972596-0-Ab3ooEtMDUvJx4Vcilwqq9pfO3H2Rgq37pLieKjiHiA4Tg2LgtkBCEySlyXrTI/sMOcPXDi8ZSQvfklz51IhqOF9V2+yQe09k9MJJRv/w4Eg; path=/; expires=Fri, 06-Jan-23 03:06:36 GMT; domain=.fsoft.com.vn; HttpOnly; Secure; SameSite=None

- <https://fsoftacademy.fsoft.com.vn/wp-content/plugins/wp-filebase/wpfb-ajax.php>

Set-Cookie: __cf_bm=G5CjfKJlJtvXR.n.7ePUDm9FQVYPTljjyWHvqwJZA4dw-1672972610-0-ASom4iqpHUkj0h8IASoTAGxKQpI44bsUcAQrM6s+AEbGKM816XQt9ndf947dGRZge9AHiP2RbAfEyxiAuqX1Lc2uv2QJrdTbooICsc50DbDx; path=/; expires=Fri, 06-Jan-23 03:06:50 GMT; domain=.fsoft.com.vn; HttpOnly; Secure; SameSite=None

- <https://fsoftacademy.fsoft.com.vn/wp-content/plugins/ss-downloads/templates/emailform.php>

```
Set-Cookie: __cf_bm=VtznQRP2AccRaYASAnPhVfXW_JapIJJHfQosnGkZE-1672972639-0-
AToojXEfvwUiDfVRG5OF/mIC77JPdkuk9aC24u7107cSkyQgYN2hIfs3tlHleYBVbaDh61GmAtjRbht1lfsYkYbKxXIEcHMMOk8gsNXLMUQM;
path=/; expires=Fri, 06-Jan-23 03:07:19 GMT; domain=.fsoft.com.vn; HttpOnly; Secure; SameSite=None
```

- <https://fsoftacademy.fsoft.com.vn/cdn-cgi/challenge-platform/h/b/cv/result/7851122dfed0502>

```
Set-Cookie: __cf_bm=vfS5n.hBnOBvXYkblYz8nBzqodxc0VyrzohHnjf3H4s-1672972643-0-
Aetn3N3sCwBOiaew5GUjWlk9yfVqAv7ElIJROTL/g22IjO8k3o15nClOikrTlwG/Z8XlJUA2MXUGVzUssLOA7gBOqemFXzpxlY8IOVuRLw+aaJBkpfnf
pirGkCbERtL/UsF2gbLrL9A9IKpaFm3anpI=; path=/; expires=Fri, 06-Jan-23 03:07:23 GMT; domain=.fsoft.com.vn; HttpOnly;
Secure; SameSite=None
```

- <https://fsoftacademy.fsoft.com.vn/cdn-cgi/challenge-platform/h/b/cv/result/785112d79d1b6baa>

```
Set-Cookie: __cf_bm=QUzyLl9hPS5ylYU.8EnlX4M0hUtMO9MyFg9lc7UdIQY-1672972679-0-
AfrUtEGcIGjwruvUcDXblCBmhC3zQHCNfZJHi9Yqt5GaI/hfWcOYatZXwgTtua1ZmH+UrMxLWXltEw7vzz6WwqZSK4iN4RA0VPzliy4gYr4JVq5MiOH
4WtWMyBcBv4HGxlcHkd1/wy/HQYRhpB+94M=; path=/; expires=Fri, 06-Jan-23 03:07:59 GMT; domain=.fsoft.com.vn; HttpOnly;
Secure; SameSite=None
```

- <https://fsoftacademy.fsoft.com.vn/>

```
Set-Cookie: __cf_bm=UbdWeMkkrKxIVMvddGmlB8wMnr19Rdr_QT7BR1G.9Y-1672973001-0-
AZFL2z7PZavZla3ONvd4ST/J0VCj8WEGk08WDgiuaN92kN/ykkSzzrIeC8oTirWAD6/sj/sr79tpukldL7I2aAdgMJydZI/JslD8MKD1z30bt;
path=/; expires=Fri, 06-Jan-23 03:13:21 GMT; domain=.fsoft.com.vn; HttpOnly; Secure; SameSite=None
```

- <https://fsoftacademy.fsoft.com.vn/>

```
Set-Cookie: __cf_bm=RICE1uLpUeRcTEkOp_Fcu3PBYFV5rMiAM9qUkfZuuX8-1672973002-0-
AQ07FRk/D428Xro8XBe+KuzhF6ZYSM7whLNWk46eUbQxFRcesNCuPw5YAQQfnWeioUwb7pH022/MgGHebKgLi7U5RrqzLqWmC/wkoBBL7gBQ;
path=/; expires=Fri, 06-Jan-23 03:13:22 GMT; domain=.fsoft.com.vn; HttpOnly; Secure; SameSite=None
```

Request

```
GET / HTTP/1.1
Referer: https://fsoftacademy.fsoft.com.vn/
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: fsoftacademy.fsoft.com.vn
Connection: Keep-alive
```

Recommendation

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

WordPress default administrator account

By default WordPress creates an administrator user account named **admin**. Using the default Admin WordPress Account, hackers can easily launch a brute force attack against it. In order to help deter this type of attack, you should change your default WordPress administrator username to something more difficult to guess.

Impact

No impact is associated with this vulnerability.

<https://fsoftacademy.fsoft.com.vn/wp-login.php>

Request

```
POST //wp-login.php HTTP/1.1
Content-type: application/x-www-form-urlencoded
Cookie: __cf_bm=pNPvfQKABoWcLfGPC6BrOna7AC0Kv4faSBYj7wH0Yhc-1672902422-0-AZLK5QgH5eYQ8idxARcxHGuicb5JfJIDSr54vN3Dyt2EIDLDOTI5yhAoWk3tYJiZ3nF3rVqC0ef8u4ldgaX9C4CG89U5GX/DdAzW1cPOVOA9vfwQX2BUvNbznWdFQuZXsVrNnVoQWwX1P+s2bVSBnvfnHvmiMlcugX2h5xlgzWjaoDyAXlh7vLorvis6ge5brpHEn2qeLzFXueYGCwDdPHI=; cf_chl_rc_ni=1
Content-Length: 42
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: fsoftacademy.fsoft.com.vn
Connection: Keep-alive

log=admin&pwd=acunetixtest&wp-submit=Login
```

Recommendation

Change the default WordPress administrator username to something more difficult to guess. Consult web references for more information.

References

[OWASP Wordpress Security Implementation Guideline](https://www.owasp.org/index.php/OWASP_Wordpress_Security_Implementation_Guideline#Remove_or_change_the_default_administrator_account)

https://www.owasp.org/index.php/OWASP_Wordpress_Security_Implementation_Guideline#Remove_or_change_the_default_administrator_account

[Your WordPress Installation Is Using the Default Admin Account](https://www.acunetix.com/blog/wordpress-security/wordpress-default-admin-account/)

<https://www.acunetix.com/blog/wordpress-security/wordpress-default-admin-account/>

[Change WordPress admin username for security](https://www.inmotionhosting.com/support/website/wordpress/change-wordpress-admin-username-for-security)

<https://www.inmotionhosting.com/support/website/wordpress/change-wordpress-admin-username-for-security>

WordPress REST API User Enumeration

WordPress includes a REST API that can be used to list the information about the registered users on a WordPress installation. The REST API exposed user data for all users who had authored a post of a public post type. WordPress 4.7.1 limits this to only post types which have specified that they should be shown within the REST API.

Impact

An unauthenticated attacker can gain access to the list of users on a WordPress installation. This can be exploited by bots that are launching brute-force password guessing attacks on WordPress websites.

<https://fsoftacademy.fsoft.com.vn/>

Request

```
GET /?rest_route=/wp/v2/users HTTP/1.1
Cookie: __cf_bm=pNPvfQKABoWcLfGPC6BrOna7AC0Kv4faSBYj7wH0Yhc-1672902422-0-AZLK5QgH5eYQ8idxARcxHGuicb5JfJIDSr54vN3Dyt2EIDLDOTI5yhAoWk3tYJiZ3nF3rVqC0ef8u4ldgaX9C4CG89U5GX/DdAzW1cPOVOA9vfwQX2BUvNbznWdFQuZXsVrNnVoQWwX1P+s2bVSBnvfnHvmiMlcugX2h5xlgzWjaoDyAXlh7vLorvis6ge5brpHEn2qeLzFXueYGCwDdPHI=; cf_chl_rc_ni=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: fsoftacademy.fsoft.com.vn
Connection: Keep-alive
```

Recommendation

Install a WordPress plugin such as Stop User Enumeration. Stop User Enumeration is a security plugin designed to detect and prevent hackers scanning your site for user names.

References

[Stop User Enumeration](https://wordpress.org/plugins/stop-user-enumeration/)

<https://wordpress.org/plugins/stop-user-enumeration/>

[WordPress 4.7.1 Security and Maintenance Release](https://wordpress.org/news/2017/01/wordpress-4-7-1-security-and-maintenance-release/)

<https://wordpress.org/news/2017/01/wordpress-4-7-1-security-and-maintenance-release/>

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://fsoftacademy.fsoft.com.vn/>

Paths without CSP header:

- <https://fsoftacademy.fsoft.com.vn/wp-content/plugins/activehelper-livehelp/server/offline.php>
- <https://fsoftacademy.fsoft.com.vn/wp-content/plugins/topquark/lib/js/fancyupload/showcase/batch/script.php>
- <https://fsoftacademy.fsoft.com.vn/wp-content/plugins/ss-downloads/templates/emailsent.php>
- https://fsoftacademy.fsoft.com.vn/wp-content/plugins/spider-calendar/front_end/spidercalendarbig_seemore.php
- https://fsoftacademy.fsoft.com.vn/wp-content/plugins/wp-football/football_matches_load.php
- <https://fsoftacademy.fsoft.com.vn/wp-content/plugins/zotpress/zotpress.rss.php>
- <https://fsoftacademy.fsoft.com.vn/wp-content/plugins/spotlightyour/library/includes/payment/paypalexpress/DoDirectPayment.php>
- <https://fsoftacademy.fsoft.com.vn/wp-content/plugins/wpforum/wp-forum-manage.php>
- <https://fsoftacademy.fsoft.com.vn/wp-content/plugins/thecartpress/checkout/CheckoutEditor.php>
- <https://fsoftacademy.fsoft.com.vn/wp-content/plugins/fbpromotions/admin/swarm-settings.php>

- <https://fsoftacademy.fsoft.com.vn/wp-content/plugins/wp-auctions/admin.php>
- <https://fsoftacademy.fsoft.com.vn/wp-content/plugins/thecartpress/admin/OptionsPostsList.php>
- <https://fsoftacademy.fsoft.com.vn/wp-content/plugins/immopress/sdk/Oauth/example/index.php>
- https://fsoftacademy.fsoft.com.vn/wp-content/plugins/wp-football/football_groups_list.php
- <https://fsoftacademy.fsoft.com.vn/wp-content/plugins/dm-albums/dm-albums.php>
- https://fsoftacademy.fsoft.com.vn/wp-content/plugins/flog/silex-plugin-themes/flash-theme/silex_server/cgi/scripts/proxy.php
- https://fsoftacademy.fsoft.com.vn/wp-content/plugins/wp-realty/index_ext.php
- <https://fsoftacademy.fsoft.com.vn/wp-content/plugins/wp-filebase/wpfb-ajax.php>
- <https://fsoftacademy.fsoft.com.vn/wp-content/plugins/wpsnapapp/js/button-snapapp.php>
- <https://fsoftacademy.fsoft.com.vn/wp-content/plugins/ss-downloads/templates/emailform.php>
- <https://fsoftacademy.fsoft.com.vn/wp-content/plugins/js-multihotel/includes/refreshDate.php>

Request

```
GET /?forum=all&page_id=4/&search=1&searchpage=2&type=9&value=1 HTTP/1.1
Referer: https://fsoftacademy.fsoft.com.vn/
Cookie: __cf_bm=zcg7fjP8o7kmTxS9puY7nO3_S6DJ8iK9KFaf4Ov2MI-1672904220-0-AZtBrjNQ+8vBNwJcGQOiaYjX3qSgrAEmrbVoaiAOpuWOqw8FObfExHLzU100BN0981nZwDcpnBTFY7Y84n9RK9MVgQMz4Ss8xie81ZF6nt3ZdnUya31LhulEZ54s1SU4gdCzTGrZerqCEBGgxTCL1YY=; cf_chl_rc_ni=2; cf_chl_2=6bbd62a16768ad4
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: fsoftacademy.fsoft.com.vn
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/>

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.

<https://fsoftacademy.fsoft.com.vn/>

- **jQuery Migrate 1.4.1**
 - URL: <https://fsoftacademy.fsoft.com.vn/wp-includes/js/jquery/jquery-migrate.min.js>
 - Detection method: The library's name and version were determined based on the file's syntax fingerprint.
 - References:
 - <https://github.com/jquery/jquery-migrate/releases>

Request

```
GET /wp-includes/js/jquery/jquery-migrate.min.js?ver=1.4.1 HTTP/1.1
Host: fsoftacademy.fsoft.com.vn
accept-language: en-US
accept: */*
cookie: cf_chl_rc_ni=3; cf_chl_2=6bbd62a16768ad4; wordpress_test_cookie=WP+Cookie+check;
__cf_bm=LFZz4jU5PvN2H5Q19Eam900iX_xcMz_72LwZHITPzt4-1672907009-0-
AQoj6FyH/IKuL6iqzJ/o9y3Evvs7m/i5PQnXEs/Ix89FWeabyhmhfF68vNIHEbzszHXkhTrC+SoSndQq5/7K3tcRtgPta8C1j7qMMUaKtJ/
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Referer: https://fsoftacademy.fsoft.com.vn/wp-login.php
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.0 Safari/537.36
```

Recommendation

Upgrade to the latest version.

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://fsoftacademy.fsoft.com.vn/>

Version detected: PHP/7.2.30.

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>

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://fsoftacademy.fsoft.com.vn/>

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: fsoftacademy.fsoft.com.vn
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://fsoftacademy.fsoft.com.vn/cdn-cgi/rum>

Pages where SRI is not implemented:

- <https://fsoftacademy.fsoft.com.vn/cdn-cgi/rum>
Script SRC: <https://performance.radar.cloudflare.com/beacon.js>

Request

```
POST /cdn-cgi/rum? HTTP/1.1
Host: fsoftacademy.fsoft.com.vn
Content-Length: 3782
accept-language: en-US
content-type: application/json
accept: */*
origin: https://fsoftacademy.fsoft.com.vn
cookie: cf_chl_rc_ni=2; cf_chl_2=6bbd62a16768ad4; __cf_bm=A0F4eio06RdzWNErSaY5nZ04k4YGU8z3bXw83nsIMac-1672905412-0-AVePRE9GuKv0JtqP1MP3KvYO4lqM+48JokEl2ksiQt3fuZzQFStFbWNNpgexWKdT/c0z54oWCv00EtKmRMXYeg2tGSRT1UrrkVftv09KhM+m
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://fsoftacademy.fsoft.com.vn/?forum=all&page_id=4/&search=1&searchpage=2&type=9&value=1
Accept-Encoding: gzip,deflate,br
```

```
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.0 Safari/537.36

{"memory":{"totalJSHeapSize":10000000,"usedJSHeapSize":10000000,"jsHeapSizeLimit":2190000000},"resources":
[{"n":"https://fsoftacademy.fsoft.com.vn/wp-includes/css/dist/block-library/style.min.css?
ver=5.4.1","s":126.2,"d":572.6,"i":"link","p":"","rs":0,"re":0,"fs":126.2,"ds":126.2,"de":126.2,"cs":126.2,"ce":126.2,"qs":0,"ps":698.8,"pe
":698.8,"ws":0,"ss":126.2,"ts":53893,"ec":53593,"dc":53593},{n":"https://fsoftacademy.fsoft.com.vn/wp-
content/themes/twentytwenty/style.css?
ver=1.2","s":126.9,"d":1783.1,"i":"link","p":"","rs":0,"re":0,"fs":126.9,"ds":126.9,"de":126.9,"cs":126.9,"ce":126.9,"qs":0,"ps":1910,"pe":
1910,"ws":0,"ss":126.9,"ts":88392,"ec":88092,"dc":88092},{n":"https://fsoftacademy.fsoft.com.vn/wp-
content/themes/twentytwenty/assets/js/index.js?
ver=1.2","s":128,"d":1971.3,"i":"script","p":"","rs":0,"re":0,"fs":128,"ds":128,"de":128,"cs":128,"ce":128,"qs":0,"ps":2099.3,"pe":2099.3,"
ws":0,"ss":128,"ts":66061,"ec":65761,"dc":65761},{n":"https://fsoftacademy.fsoft.com.vn/wp-includes/js/wp-embed.min.js?
ver=5.4.1","s":128.3,"d":1091.9,"i":"script","p":"","rs":0,"re":0,"fs":128.3,"ds":128.3,"de":128.3,"cs":128.3,"ce":128.3,"qs":0,"ps":1220.2
,"pe":1220.2,"ws":0,"ss":128.3,"ts":4792,"ec":4492,"dc":4492},
{"n":"https://static.cloudflareinsights.com/beacon.min.js/vaafb692b2aea4879b33c060e79fe94621666317369993","s":128.9,"d":1834.1,"i":"script"
,"p":"","rs":0,"re":0,"fs":128.9,"ds":0,"de":0,"cs":0,"ce":0,"qs":0,"ps":0,"pe":1963,"ws":0,"ss":0,"ts":0,"ec":0,"dc":0},
{"n":"https://fsoftacademy.fsoft.com.vn/wp-includes/js/wp-emoji-release.min.js?
ver=5.4.1","s":322.4,"d":2349.7,"i":"script","p":"","rs":0,"re":0,"fs":322.4,"ds":322.4,"de":322.4,"cs":322.4,"ce":322.4,"qs":0,"ps":2672.1
,"pe":2672.1,"ws":0,"ss":322.4,"ts":40914,"ec":40614,"dc":40614},{n":"https://fsoftacademy.fsoft.com.vn/wp-
content/themes/twentytwenty/print.css?
ver=1.2","s":324.9,"d":2425.8,"i":"link","p":"","rs":0,"re":0,"fs":324.9,"ds":324.9,"de":324.9,"cs":324.9,"ce":324.9,"qs":0,"ps":2750.7,"pe
":2750.7,"ws":0,"ss":324.9,"ts":1756,"ec":1456,"dc":1456},{n":"https://fsoftacademy.fsoft.com.vn/wp-
content/themes/twentytwenty/assets/fonts/inter/Inter-upright-
var.woff2","s":1949,"d":340.3,"i":"css","p":"","rs":0,"re":0,"fs":1949,"ds":1949,"de":1949,"cs":1949,"ce":1949,"qs":0,"ps":2289.3,"pe":2289
.3,"ws":0,"ss":1949,"ts":224192,"ec":223892,"dc":223892}],{"referrer":"","documentWriteIntervention":false,"errorCount":0,"eventType":1,"fir
stPaint":2018.9000000059605,"firstContentfulPaint":2018.9000000059605,"si":100,"startTime":1672905410294.6,"versions":
{"fl":"2022.11.3","js":"2022.10.1","timings":2},"pageloadId":"4d3b3480-1fb6-49b2-9d7c-
703f735a6704","location":"https://fsoftacademy.fsoft.com.vn/","wd":true,"timingsV2":
{"unloadEventStart":0,"unloadEventEnd":0,"domInteractive":2140,"domContentLoadedEventStart":2162.8000000044703,"domContentLoadedEventEnd":2
166,"domComplete":2753.2000000029802,"loadEventStart":2753.4000000059605,"loadEventEnd":2754.9000000059605,"type":"navigate","redirectCount
":0,"initiatorType":"navigation","nextHopProtocol":"","workerStart":0,"redirectStart":0,"redirectEnd":0,"fetchStart":0.7000000029802322,"do
mainLookupStart":0.7000000029802322,"domainLookupEnd":0.7000000029802322,"connectStart":0.7000000029802322,"connectEnd":0.7000000029802322,
"secureConnectionStart":0.7000000029802322,"requestStart":0,"responseStart":52.600000001490116,"responseEnd":52.600000001490116,"transferSi
ze":21280,"encodedBodySize":20980,"decodedBodySize":20980,"serverTiming":[{"name":"cf-q-
config","duration":0.0000070000005507609,"description":""}],{"name":"https://fsoftacademy.fsoft.com.vn/?
forum=all&page_id=4/&search=1&searchpage=2&type=9&value=1","entryType":"navigation","startTime":0,"duration":2754.9000000059605},"siteToken
":"42ef590a44e848a8a25df7f6ec3a8293","st":2}
```

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.

```
&ltscript src="https://example.com/example-framework.js"
integrity="sha384-oqVuAfXRKap7fdgcCY5uykM6+R9GqQ8K/uxy9rx7HNQlGY11kPzQh01wx4JwY8wC"
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://fsoftacademy.fsoft.com.vn/>

Detected Cloudflare WAF from the headers.

Request

```
GET /9963403 HTTP/1.1
Cookie: __cf_bm=euPqv6hiJ2GBylpONld89jXlxBiVe429Zh5TfTTj_oM-1672902254-0-
AWSZrj69UJJ3T9aPKzIz+dtbNX+V/BOsHqLlsN9JEWp9azGV0tHm+Jt6rzCinK7bTZGzoWy5xdhLAt2gnNrZojYU9RbJIeNMVfx+iTPuw0HR; cf_chl_rc_ni=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: fsoftacademy.fsoft.com.vn
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://fsoftacademy.fsoft.com.vn/>

<https://fsoftacademy.fsoft.com.vn/cdn-cgi/rum>

<https://fsoftacademy.fsoft.com.vn/wp-login.php>