Acunetix by Invicti

Comprehensive Report

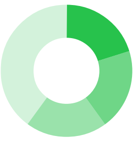
Acunetix Threat Level 3

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.

17	2	11	5
High	Medium	Low	Informational

Severity	Vulnerabilities	Instances
High	17	17
Medium	2	2
Low	11	11
Informational	5	5
Total	35	35

Informational

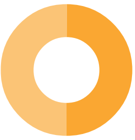


	Instances
🟩 Content Security Policy (CSP) not implemented	1
🟩 PHP Version Disclosure	1
🟩 Reverse proxy detected	1
🟩 Others	2

Low Severity

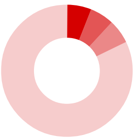
	Instances
🟦 Clickjacking: X-Frame-Options header	1
🟦 Cookies with missing, inconsistent or contrad…	1
🟦 Cookies without HttpOnly flag set	1
🟦 Others	8

Medium Severity



	Instances
🟧 Folder backup	1
🟧 WordPress XML-RPC authentication brute force	1

High Severity



	Instances
🟥 Server directory traversal	1
🟥 WordPress 5.0 Multiple Vulnerabilities (5.0 - 5.0)	1
🟥 WordPress 5.0 Multiple Vulnerabilities (5.0 - 5.0)	1
🟥 Others	14

Impacts

SEVERITY	IMPACT	
High	1	Server directory traversal
High	1	WordPress 5.0 Multiple Vulnerabilities (5.0 - 5.0)
High	1	WordPress 5.0 Multiple Vulnerabilities (5.0 - 5.0)
High	1	WordPress 5.0.x Cross-Site Request Forgery (5.0 - 5.0.3)
High	1	WordPress 5.0.x Multiple Vulnerabilities (5.0 - 5.0.10)
High	1	WordPress 5.0.x Multiple Vulnerabilities (5.0 - 5.0.11)
High	1	WordPress 5.0.x Multiple Vulnerabilities (5.0 - 5.0.13)
High	1	WordPress 5.0.x Multiple Vulnerabilities (5.0 - 5.0.14)
High	1	WordPress 5.0.x Multiple Vulnerabilities (5.0 - 5.0.4)
High	1	WordPress 5.0.x Multiple Vulnerabilities (5.0 - 5.0.6)
High	1	WordPress 5.0.x Multiple Vulnerabilities (5.0 - 5.0.7)
High	1	WordPress 5.0.x Multiple Vulnerabilities (5.0 - 5.0.8)
High	1	WordPress 5.0.x Multiple Vulnerabilities (5.0 - 5.0.9)
High	1	WordPress 5.0.x PHP Object Injection (5.0 - 5.0.12)
High	1	WordPress 5.0.x Prototype Pollution (5.0 - 5.0.15)
High	1	WordPress Directory Traversal (3.7 - 5.0.3)
High	1	WordPress Plugin MailPoet-emails and newsletters in WordPress Cross-Site Scripting (3.23.1)
Medium	1	Folder backup
Medium	1	WordPress XML-RPC authentication brute force
Low	1	Clickjacking: X-Frame-Options header
Low	1	Cookies with missing, inconsistent or contradictory properties
Low	1	Cookies without HttpOnly flag set
Low	1	Cookies without Secure flag set
Low	1	Documentation files
Low	1	HTTP Strict Transport Security (HSTS) not implemented
Low	1	Possible sensitive directories
Low	1	Sensitive pages could be cached
Low	1	Session cookies scoped to parent domain
Low	1	WordPress default administrator account
Low	1	WordPress REST API User Enumeration

SEVERITY	IMPACT	
ⓘ Informational	1	Content Security Policy (CSP) not implemented
ⓘ Informational	1	PHP Version Disclosure
ⓘ Informational	1	Reverse proxy detected
ⓘ Informational	1	Subresource Integrity (SRI) not implemented
ⓘ Informational	1	Web Application Firewall detected

Server directory traversal

This script is possibly vulnerable to directory traversal attacks.

Directory Traversal is a vulnerability which allows attackers to access restricted directories and read files outside of the web server's root directory.

Impact

By exploiting directory traversal vulnerabilities, attackers step out of the root directory and access files in other directories. As a result, attackers might view restricted files or execute commands, leading to a full compromise of the Web server.

---

https://shb.fpt-software.com/wp-content/themes/twentynineteen/js/

This file was found using the payload **/wp-content/themes/twentynineteen/js/%2e%2e%2fpackage.json**.
Original directory: **/wp-content/themes/twentynineteen/js/**
Pattern found:

```
"devDependencies"
```

In the same time, the pattern was not found without the directory traversal payload: https://shb.fpt-software.com/wp-content/themes/twentynineteen/package.json.

Request

```
GET /wp-content/themes/twentynineteen/js/%2e%2e%2fpackage.json HTTP/1.1
Cookie: __cf_bm=QO5ofzz3dC5qwZ83BOZ5SiRtmskbLAS1w0a2_liBl5M-1672912472-0-
Aa15IVpahAl1yhwOJvsC5Uikv5OsGYk1jzeDmBYTlWReOs8VjOOr2qvRDofl3zJfaCIftRZOG1nomxHZyoMUGStVEU8nA6lrqE3SZnI4TVsV; cf_chl_2=ff566390659d71b;
cf_chl_rc_ni=3
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: shb.fpt-software.com
Connection: Keep-alive
```

Recommendation

Your script should filter metacharacters from user input.

References

Acunetix Directory Traversal Attacks
https://www.acunetix.com/websitesecurity/directory-traversal/

WordPress 5.0 Multiple Vulnerabilities (5.0 - 5.0)

WordPress is prone to multiple vulnerabilities, including cross-site scripting, security bypass, information disclosure 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 perform otherwise restricted actions and subsequently delete files that they weren't authorized to or create posts of unauthorized post types, to obtain sensitive information, or to possibly execute arbitrary PHP code within the context of the affected webserver process. WordPress version 5.0 is vulnerable.

Impact

---

https://shb.fpt-software.com/

Current WordPress version: 5.0.
WordPress version 5.0 is affected.

Request

```
GET / HTTP/1.1
Cookie: __cf_bm=069JkpR1BoL3r4KqpJMpzOwAU9RhUU7PCIvGz4Kn.6U-1672211005-0-
ATwsAjwXtbyH+Zp1i5zeg/8SHQBXDD4k+oQCy576YcQw2AEOMVelZAbOixiCobuoQ1AmmutqYU6MqbjEffeqn3MFAnKaioiTAhOF6TGFGovHd8R5L6v2AAzsRGH0TRgQSTnk9nCSazw
W0/a73GwWA0s=; cf_chl_rc_m=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: shb.fpt-software.com
Connection: Keep-alive
```

Recommendation

Update to WordPress version 5.0.1 or latest

References

https://cdn2.hubspot.net/hubfs/3853213/us-18-Thomas-It's-A-PHP-Unserialization-Vulnerability-Jim-But-Not-As-We-....pdf?
https://cdn2.hubspot.net/hubfs/3853213/us-18-Thomas-It's-A-PHP-Unserialization-Vulnerability-Jim-But-Not-As-We-....pdf?

https://blog.ripstech.com/2018/wordpress-post-type-privilege-escalation/
https://blog.ripstech.com/2018/wordpress-post-type-privilege-escalation/

https://blog.ripstech.com/2019/wordpress-image-remote-code-execution/
https://blog.ripstech.com/2019/wordpress-image-remote-code-execution/

http://foreversong.cn/archives/1364
http://foreversong.cn/archives/1364

https://wordpress.org/news/2018/12/wordpress-5-0-1-security-release/
https://wordpress.org/news/2018/12/wordpress-5-0-1-security-release/

WordPress 5.0 Multiple Vulnerabilities (5.0 - 5.0)

WordPress is prone to multiple vulnerabilities, including directory traversal and remote code execution vulnerabilities. Exploiting these issues could allow an attacker to obtain sensitive information that could aid in further attacks, or to execute arbitrary code with the privileges of the user running the application, to compromise the application or the underlying database, to access or modify data or to compromise a vulnerable system. WordPress version 5.0 is vulnerable.

Impact

https://shb.fpt-software.com/

Current WordPress version: 5.0.
WordPress version 5.0 is affected.

Request

```
GET / HTTP/1.1
Cookie: __cf_bm=069JkpR1BoL3r4KqpJMpzOwAU9RhUU7PCIvGz4Kn.6U-1672211005-0-
ATwsAjwXtbyH+Zp1i5zeg/8SHQBXDD4k+oQCy576YcQw2AEOMVelZAbOixiCobuoQ1AmmutqYU6MqbjEffeqn3MFAnKaioiTAhOF6TGFGovHd8R5L6v2AAzsRGH0TRgQSTnk9nCSazw
W0/a73GwWA0s=; cf_chl_rc_m=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: shb.fpt-software.com
Connection: Keep-alive
```

Recommendation

Update to WordPress version 5.0.1 or latest

References

https://blog.ripstech.com/2019/wordpress-image-remote-code-execution/
https://blog.ripstech.com/2019/wordpress-image-remote-code-execution/

http://foreversong.cn/archives/1364
http://foreversong.cn/archives/1364

https://gist.github.com/allyshka/f159c0b43f1374f87f2c3817d6401fd6
https://gist.github.com/allyshka/f159c0b43f1374f87f2c3817d6401fd6

WordPress 5.0.x Cross-Site Request Forgery (5.0 - 5.0.3)

WordPress is prone to a cross-site request forgery vulnerability. Exploiting this issue may allow a remote attacker to perform certain administrative actions and gain unauthorized access to the affected application; other attacks are also possible. WordPress versions 5.0.x ranging from 5.0 and up to (and including) 5.0.3 are vulnerable.

Impact

https://shb.fpt-software.com/

Current WordPress version: 5.0.
WordPress versions between 5.0 and 5.0.3 are affected.

Request

```
GET / HTTP/1.1
Cookie: __cf_bm=069JkpR1BoL3r4KqpJMpzOwAU9RhUU7PCIvGz4Kn.6U-1672211005-0-
ATwsAjwXtbyH+Zp1i5zeg/8SHQBXDD4k+oQCy576YcQw2AEOMVelZAbOixiCobuoQ1AmmutqYU6MqbjEffeqn3MFAnKaioiTAhOF6TGFGovHd8R5L6v2AAzsRGH0TRgQSTnk9nCSazw
W0/a73GwWA0s=; cf_chl_rc_m=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: shb.fpt-software.com
Connection: Keep-alive
```

Recommendation

Update to WordPress version 5.0.4 or latest

References

https://blog.ripstech.com/2019/wordpress-csrf-to-rce/
https://blog.ripstech.com/2019/wordpress-csrf-to-rce/

https://cert.360.cn/warning/detail?id=149a32b8f582ee5e0cbd5f1c1b4a61de
https://cert.360.cn/warning/detail?id=149a32b8f582ee5e0cbd5f1c1b4a61de

https://wordpress.org/support/wordpress-version/version-5-0-4/
https://wordpress.org/support/wordpress-version/version-5-0-4/

WordPress 5.0.x Multiple Vulnerabilities (5.0 - 5.0.10)

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 5.0.x ranging from 5.0 and up to (and including) 5.0.10 are vulnerable.

Impact

https://shb.fpt-software.com/

Current WordPress version: 5.0.

WordPress versions between 5.0 and 5.0.10 are affected.

Request

```
GET / HTTP/1.1
Cookie: __cf_bm=069JkpR1BoL3r4KqpJMpzOwAU9RhUU7PCIvGz4Kn.6U-1672211005-0-
ATwsAjwXtbyH+Zp1i5zeg/8SHQBXDD4k+oQCy576YcQw2AEOMVelZAbOixiCobuoQ1AmmutqYU6MqbjEffeqn3MFAnKaioiTAhOF6TGFGovHd8R5L6v2AAzsRGH0TRgQSTnk9nCSazw
W0/a73GwWA0s=; cf_chl_rc_m=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: shb.fpt-software.com
Connection: Keep-alive
```

Recommendation

Update to WordPress version 5.0.11 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-5-0-11/
https://wordpress.org/support/wordpress-version/version-5-0-11/

WordPress 5.0.x Multiple Vulnerabilities (5.0 - 5.0.11)

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 5.0.x ranging from 5.0 and up to (and including) 5.0.11 are vulnerable.

Impact

https://shb.fpt-software.com/

Current WordPress version: 5.0.

WordPress versions between 5.0 and 5.0.11 are affected.

Request

```
GET / HTTP/1.1
Cookie: __cf_bm=069JkpR1BoL3r4KqpJMpzOwAU9RhUU7PCIvGz4Kn.6U-1672211005-0-
ATwsAjwXtbyH+Zp1i5zeg/8SHQBXDD4k+oQCy576YcQw2AEOMVelZAbOixiCobuoQ1AmmutqYU6MqbjEffeqn3MFAnKaioiTAhOF6TGFGovHd8R5L6v2AAzsRGH0TRgQSTnk9nCSazw
W0/a73GwWA0s=; cf_chl_rc_m=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: shb.fpt-software.com
Connection: Keep-alive
```

Recommendation

Update to WordPress version 5.0.12 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-5-0-12/
https://wordpress.org/support/wordpress-version/version-5-0-12/

WordPress 5.0.x Multiple Vulnerabilities (5.0 - 5.0.13)

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 5.0.x ranging from 5.0 and up to (and including) 5.0.13 are vulnerable.

Impact

https://shb.fpt-software.com/

Current WordPress version: 5.0.
WordPress versions between 5.0 and 5.0.13 are affected.

Request

```
GET / HTTP/1.1
Cookie: __cf_bm=069JkpR1BoL3r4KqpJMpzOwAU9RhUU7PCIvGz4Kn.6U-1672211005-0-
ATwsAjwXtbyH+Zp1i5zeg/8SHQBXDD4k+oQCy576YcQw2AEOMVelZAbOixiCobuoQ1AmmutqYU6MqbjEffeqn3MFAnKaioiTAhOF6TGFGovHd8R5L6v2AAzsRGH0TRgQSTnk9nCSazw
W0/a73GwWA0s=; cf_chl_rc_m=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: shb.fpt-software.com
Connection: Keep-alive
```

Recommendation

Update to WordPress version 5.0.14 or latest

References

https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-wh69-25hr-h94v
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/WordPress/wordpress-develop/security/advisories/GHSA-m9hc-7v5q-x8q5

https://github.com/lodash/lodash/wiki/Changelog#v41721
https://github.com/lodash/lodash/wiki/Changelog#v41721

https://wordpress.org/support/wordpress-version/version-5-0-14/
https://wordpress.org/support/wordpress-version/version-5-0-14/

WordPress 5.0.x Multiple Vulnerabilities (5.0 - 5.0.14)

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 5.0.x ranging from 5.0 and up to (and including) 5.0.14 are vulnerable.

Impact

https://shb.fpt-software.com/

Current WordPress version: 5.0.
WordPress versions between 5.0 and 5.0.14 are affected.

Request

```
GET / HTTP/1.1
Cookie: __cf_bm=069JkpR1BoL3r4KqpJMpzOwAU9RhUU7PCIvGz4Kn.6U-1672211005-0-
ATwsAjwXtbyH+Zp1i5zeg/8SHQBXDD4k+oQCy576YcQw2AEOMVelZAbOixiCobuoQ1AmmutqYU6MqbjEffeqn3MFAnKaioiTAhOF6TGFGovHd8R5L6v2AAzsRGH0TRgQSTnk9nCSazw
W0/a73GwWA0s=; cf_chl_rc_m=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: shb.fpt-software.com
Connection: Keep-alive
```

Recommendation

Update to WordPress version 5.0.15 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-5-0-15/
https://wordpress.org/support/wordpress-version/version-5-0-15/

WordPress 5.0.x Multiple Vulnerabilities (5.0 - 5.0.4)

WordPress is prone to multiple vulnerabilities, including cross-site scripting and open redirect vulnerabilities. An attacker may leverage these issues 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 redirect users to arbitrary web sites and conduct phishing attacks. WordPress versions 5.0.x ranging from 5.0 and up to (and including) 5.0.4 are vulnerable.

Impact

https://shb.fpt-software.com/

Current WordPress version: 5.0.

WordPress versions between 5.0 and 5.0.4 are affected.

Request

```
GET / HTTP/1.1
Cookie: __cf_bm=069JkpR1BoL3r4KqpJMpzOwAU9RhUU7PCIvGz4Kn.6U-1672211005-0-
ATwsAjwXtbyH+Zp1i5zeg/8SHQBXDD4k+oQCy576YcQw2AEOMVelZAbOixiCobuoQ1AmmutqYU6MqbjEffeqn3MFAnKaioiTAhOF6TGFGovHd8R5L6v2AAzsRGH0TRgQSTnk9nCSazw
W0/a73GwWA0s=; cf_chl_rc_m=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: shb.fpt-software.com
Connection: Keep-alive
```

Recommendation

Update to WordPress version 5.0.6 or latest

References

https://www.fortinet.com/blog/threat-research/wordpress-core-stored-xss-vulnerability.html
https://www.fortinet.com/blog/threat-research/wordpress-core-stored-xss-vulnerability.html

https://www.wordfence.com/blog/2019/09/the-wordpress-5-2-3-security-release-unpacked/
https://www.wordfence.com/blog/2019/09/the-wordpress-5-2-3-security-release-unpacked/

https://www.exploit-db.com/exploits/49338
https://www.exploit-db.com/exploits/49338

https://packetstormsecurity.com/files/160745/WordPress-Core-5.2.2-Cross-Site-Scripting.html
https://packetstormsecurity.com/files/160745/WordPress-Core-5.2.2-Cross-Site-Scripting.html

https://wordpress.org/support/wordpress-version/version-5-0-6/
https://wordpress.org/support/wordpress-version/version-5-0-6/

WordPress 5.0.x Multiple Vulnerabilities (5.0 - 5.0.6)

WordPress is prone to multiple vulnerabilities, including cross-site scripting, security bypass, or server-side request forgery 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 bypass certain security restrictions and perform unauthorized actions, or to make the vulnerable server perform port scanning of hosts in internal or external networks. WordPress versions 5.0.x ranging from 5.0 and up to (and including) 5.0.6 are vulnerable.

Impact

https://shb.fpt-software.com/

Current WordPress version: 5.0.

WordPress versions between 5.0 and 5.0.6 are affected.

Request

```
GET / HTTP/1.1
Cookie: __cf_bm=069JkpR1BoL3r4KqpJMpzOwAU9RhUU7PCIvGz4Kn.6U-1672211005-0-
ATwsAjwXtbyH+Zp1i5zeg/8SHQBXDD4k+oQCy576YcQw2AEOMVelZAbOixiCobuoQ1AmmutqYU6MqbjEffeqn3MFAnKaioiTAhOF6TGFGovHd8R5L6v2AAzsRGH0TRgQSTnk9nCSazw
W0/a73GwWA0s=; cf_chl_rc_m=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: shb.fpt-software.com
Connection: Keep-alive
```

Recommendation

Update to WordPress version 5.0.7 or latest

References

https://blog.wpscan.org/wordpress/security/release/2019/10/15/wordpress-524-security-release-breakdown.html
https://blog.wpscan.org/wordpress/security/release/2019/10/15/wordpress-524-security-release-breakdown.html

https://0day.work/proof-of-concept-for-wordpress-5-2-3-viewing-unauthenticated-posts/
https://0day.work/proof-of-concept-for-wordpress-5-2-3-viewing-unauthenticated-posts/

https://blog.ripstech.com/2020/wordpress-hardening-bypass/
https://blog.ripstech.com/2020/wordpress-hardening-bypass/

https://wordpress.org/support/wordpress-version/version-5-0-7/
https://wordpress.org/support/wordpress-version/version-5-0-7/

https://wordpress.org/news/2019/11/wordpress-5-2-4-update/
https://wordpress.org/news/2019/11/wordpress-5-2-4-update/

WordPress 5.0.x Multiple Vulnerabilities (5.0 - 5.0.7)

WordPress is prone to multiple vulnerabilities, including cross-site scripting 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, or to bypass certain security restrictions and perform unauthorized actions. WordPress versions 5.0.x ranging from 5.0 and up to (and including) 5.0.7 are vulnerable.

Impact

https://shb.fpt-software.com/

Current WordPress version: 5.0.

WordPress versions between 5.0 and 5.0.7 are affected.

Request

```
GET / HTTP/1.1
Cookie: __cf_bm=069JkpR1BoL3r4KqpJMpzOwAU9RhUU7PCIvGz4Kn.6U-1672211005-0-
ATwsAjwXtbyH+Zp1i5zeg/8SHQBXDD4k+oQCy576YcQw2AEOMVelZAbOixiCobuoQ1AmmutqYU6MqbjEffeqn3MFAnKaioiTAhOF6TGFGovHd8R5L6v2AAzsRGH0TRgQSTnk9nCSazw
W0/a73GwWA0s=; cf_chl_rc_m=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: shb.fpt-software.com
Connection: Keep-alive
```

Recommendation

Update to WordPress version 5.0.8 or latest

References

https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-g7rg-hchx-c2gw
https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-g7rg-hchx-c2gw

https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-pg4x-64rh-3c9v
https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-pg4x-64rh-3c9v

https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-x3wp-h3qx-9w94
https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-x3wp-h3qx-9w94

https://wordpress.org/support/wordpress-version/version-5-0-8/
https://wordpress.org/support/wordpress-version/version-5-0-8/

WordPress 5.0.x Multiple Vulnerabilities (5.0 - 5.0.8)

WordPress is prone to multiple vulnerabilities, including cross-site scripting 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, or to bypass certain security restrictions and perform unauthorized actions. WordPress versions 5.0.x ranging from 5.0 and up to (and including) 5.0.8 are vulnerable.

Impact

https://shb.fpt-software.com/

Current WordPress version: 5.0.

WordPress versions between 5.0 and 5.0.8 are affected.

Request

```
GET / HTTP/1.1
Cookie: __cf_bm=069JkpR1BoL3r4KqpJMpzOwAU9RhUU7PCIvGz4Kn.6U-1672211005-0-
ATwsAjwXtbyH+Zp1i5zeg/8SHQBXDD4k+oQCy576YcQw2AEOMVelZAbOixiCobuoQ1AmmutqYU6MqbjEffeqn3MFAnKaioiTAhOF6TGFGovHd8R5L6v2AAzsRGH0TRgQSTnk9nCSazw
W0/a73GwWA0s=; cf_chl_rc_m=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: shb.fpt-software.com
Connection: Keep-alive
```

Recommendation

Update to WordPress version 5.0.9 or latest

References

https://www.wordfence.com/blog/2020/04/unpacking-the-7-vulnerabilities-fixed-in-todays-wordpress-5-4-1-security-update/
https://www.wordfence.com/blog/2020/04/unpacking-the-7-vulnerabilities-fixed-in-todays-wordpress-5-4-1-security-update/

https://wordpress.org/support/wordpress-version/version-5-0-9/
https://wordpress.org/support/wordpress-version/version-5-0-9/

WordPress 5.0.x Multiple Vulnerabilities (5.0 - 5.0.9)

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 5.0.x ranging from 5.0 and up to (and including) 5.0.9 are vulnerable.

Impact

https://shb.fpt-software.com/

Current WordPress version: 5.0.
WordPress versions between 5.0 and 5.0.9 are affected.

Request

```
GET / HTTP/1.1
Cookie: __cf_bm=069JkpR1BoL3r4KqpJMpzOwAU9RhUU7PCIvGz4Kn.6U-1672211005-0-
ATwsAjwXtbyH+Zp1i5zeg/8SHQBXDD4k+oQCy576YcQw2AEOMVelZAbOixiCobuoQ1AmmutqYU6MqbjEffeqn3MFAnKaioiTAhOF6TGFGovHd8R5L6v2AAzsRGH0TRgQSTnk9nCSazw
W0/a73GwWA0s=; cf_chl_rc_m=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: shb.fpt-software.com
Connection: Keep-alive
```

Recommendation

Update to WordPress version 5.0.10 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/support/wordpress-version/version-5-0-10/
https://wordpress.org/support/wordpress-version/version-5-0-10/

WordPress 5.0.x PHP Object Injection (5.0 - 5.0.12)

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 5.0.x ranging from 5.0 and up to (and including) 5.0.12 are vulnerable.

Impact

https://shb.fpt-software.com/

Current WordPress version: 5.0.
WordPress versions between 5.0 and 5.0.12 are affected.

Request

```
GET / HTTP/1.1
Cookie: __cf_bm=069JkpR1BoL3r4KqpJMpzOwAU9RhUU7PCIvGz4Kn.6U-1672211005-0-
ATwsAjwXtbyH+Zp1i5zeg/8SHQBXDD4k+oQCy576YcQw2AEOMVelZAbOixiCobuoQ1AmmutqYU6MqbjEffeqn3MFAnKaioiTAhOF6TGFGovHd8R5L6v2AAzsRGH0TRgQSTnk9nCSazw
W0/a73GwWA0s=; cf_chl_rc_m=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: shb.fpt-software.com
Connection: Keep-alive
```

Recommendation

Update to WordPress version 5.0.13 or latest

References

https://github.com/JamesGeee/CVE-2020-36326

https://github.com/JamesGeee/CVE-2020-36326

https://wordpress.org/support/wordpress-version/version-5-0-13/

https://wordpress.org/support/wordpress-version/version-5-0-13/

WordPress 5.0.x Prototype Pollution (5.0 - 5.0.15)

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 5.0.x ranging from 5.0 and up to (and including) 5.0.15 are vulnerable.

Impact

https://shb.fpt-software.com/

Current WordPress version: 5.0.

WordPress versions between 5.0 and 5.0.15 are affected.

Request

```
GET / HTTP/1.1
Cookie: __cf_bm=069JkpR1BoL3r4KqpJMpzOwAU9RhUU7PCIvGz4Kn.6U-1672211005-0-
ATwsAjwXtbyH+Zp1i5zeg/8SHQBXDD4k+oQCy576YcQw2AEOMVelZAbOixiCobuoQ1AmmutqYU6MqbjEffeqn3MFAnKaioiTAhOF6TGFGovHd8R5L6v2AAzsRGH0TRgQSTnk9nCSazw
W0/a73GwWA0s=; cf_chl_rc_m=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: shb.fpt-software.com
Connection: Keep-alive
```

Recommendation

Update to WordPress version 5.0.16 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-5-0-16/

https://wordpress.org/support/wordpress-version/version-5-0-16/

WordPress Directory Traversal (3.7 - 5.0.3)

WordPress is prone to a directory traversal vulnerability because it fails to sufficiently verify user-supplied input data. Exploiting this issue may allow an attacker to access sensitive information that could aid in further attacks. WordPress versions ranging from 3.7 and up to (and including) 5.0.3 are vulnerable.

Impact

https://shb.fpt-software.com/

Current WordPress version: 5.0.

WordPress versions between 3.7 and 5.0.3 are affected.

Request

```
GET / HTTP/1.1
Cookie: __cf_bm=069JkpR1BoL3r4KqpJMpzOwAU9RhUU7PCIvGz4Kn.6U-1672211005-0-
ATwsAjwXtbyH+Zp1i5zeg/8SHQBXDD4k+oQCy576YcQw2AEOMVelZAbOixiCobuoQ1AmmutqYU6MqbjEffeqn3MFAnKaioiTAhOF6TGFGovHd8R5L6v2AAzsRGH0TRgQSTnk9nCSazw
W0/a73GwWA0s=; cf_chl_rc_m=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: shb.fpt-software.com
Connection: Keep-alive
```

Recommendation

Edit the source code to ensure that input is properly verified, or apply a fix when available

References

https://blog.ripstech.com/2019/wordpress-image-remote-code-execution/

https://blog.ripstech.com/2019/wordpress-image-remote-code-execution/

http://foreversong.cn/archives/1364

http://foreversong.cn/archives/1364

WordPress Plugin MailPoet-emails and newsletters in WordPress Cross-Site Scripting (3.23.1)

WordPress Plugin MailPoet-emails and newsletters in WordPress is prone to a cross-site scripting vulnerability because it fails to properly sanitize user-supplied input. An attacker may leverage this issue to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site. This can allow the attacker to steal cookie-based authentication credentials and launch other attacks. WordPress Plugin MailPoet-emails and newsletters in WordPress version 3.23.1 is vulnerable; prior versions may also be affected.

Impact

https://shb.fpt-software.com/wp-content/plugins/mailpoet/

Current plugin version: 3.17.1.

Latest plugin version: 4.3.0.

Plugin versions lower (or equal) to 3.23.1 are affected.

Request

```
GET /wp-content/plugins/mailpoet/readme.txt HTTP/1.1
Cookie: __cf_bm=069JkpR1BoL3r4KqpJMpzOwAU9RhUU7PCIvGz4Kn.6U-1672211005-0-
ATwsAjwXtbyH+Zp1i5zeg/8SHQBXDD4k+oQCy576YcQw2AEOMVelZAbOixiCobuoQ1AmmutqYU6MqbjEffeqn3MFAnKaioiTAhOF6TGFGovHd8R5L6v2AAzsRGH0TRgQSTnk9nCSazw
W0/a73GwWA0s=; cf_chl_rc_m=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: shb.fpt-software.com
Connection: Keep-alive
```

Recommendation

Update to plugin version 3.23.2 or latest

References

https://plugins.svn.wordpress.org/mailpoet/trunk/readme.txt
https://plugins.svn.wordpress.org/mailpoet/trunk/readme.txt

Folder backup

A possible backup copy of a directory was found on your web server. These files are usually created by developers to backup their work.

Impact

Backup files can contain script sources, configuration files or other sensitive information that may help an malicious user to prepare more advanced attacks.

---

https://shb.fpt-software.com/wp-content/plugins/Copy%20of%20google-map-generator/ Confidence: 80%

This object was found using the pattern **Copy of ${dirName}**/.
Original directory name: **google-map-generator**

Request

```
GET /wp-content/plugins/Copy%20of%20google-map-generator/ HTTP/1.1
Range: bytes=0-99999
Cookie: __cf_bm=rJ6LFYwjNvjAVVc9wFZXp_UVDMB84k5doTA.B4noGUg-1672982332-0-
AXRtNKHEIwCloXsD+B7nRuzU/CuFrzVWYzKd/QPKGBESkAHMwQyHx6ZFqgWSgj3FRI66S8DZYJj/oyeYfhPcu+AK/BH9sBtOEhXw1OUcvrLz; cf_chl_2=734663a696d391d
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: shb.fpt-software.com
Connection: Keep-alive
```

Recommendation

Remove the file(s) if they are not required on your website. As an additional step, it is recommended to implement a security policy within your organization to disallow creation of backup files in directories accessible from the web.

References

Testing for Old, Backup and Unreferenced Files (OWASP-CM-006)
https://www.owasp.org/index.php/Review_Old,_Backup_and_Unreferenced_Files_for_Sensitive_Information_(OTG-CONFIG-004)

Security Tips for Server Configuration
https://httpd.apache.org/docs/2.4/misc/security_tips.html

Protecting Confidential Documents at Your Site
http://www.w3.org/Security/Faq/wwwsf5.html

WordPress XML-RPC authentication brute force

WordPress provides an XML-RPC interface via the xmlrpc.php script. XML-RPC is remote procedure calling using HTTP as the transport and XML as the encoding. An attacker can abuse this interface to brute force authentication credentials using API calls such as **wp.getUsersBlogs**.

Impact

An attacker can brute force the authentication credentials for your WordPress blog.

https://shb.fpt-software.com/xmlrpc.php

Pattern found:

```
<value><string>Incorrect username or password.</string></value>
```

Request

```
POST //xmlrpc.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Cookie: __cf_bm=Y4EwOBc2T2uCg1.ouf7F3CEioOv22imytliTczzKF8A-1672902855-0-
AUxNzP2WMoDH8u5WAIMtsdYq99n4wbB8IiPV/jNBfGemjGcQ4h87uL5+z4KC1ARpemyRCAzeveA3uFwAqPt84rgw9YcODMJJCo8p0Iw6tmF5; cf_chl_2=ff566390659d71b;
cf_chl_rc_ni=1
Content-Length: 264
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: shb.fpt-software.com
Connection: Keep-alive

<?xml version="1.0" encoding="iso-8859-1"?>
<methodCall>
<methodName>wp.getUsersBlogs</methodName>
<params>
<param><value><string>admin</string></value></param>
<param><value><string>89475895437895437534987</string></value>
</param>
</params>
</methodCall>
```

Recommendation

It is possible to disable the XML-RPC script if you do not want to use it. Consult references for a WordPress plugin that does that. If you don't want to disable XML-RPC you can monitor for XML-RPC authentication failures with a Web Application Firewall like ModSecurity.

References

WordPress XML-RPC Brute Force Scanning
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/honeypot-alert-wordpress-xml-rpc-brute-force-scanning/

Prevent XMLRPC
https://wordpress.org/plugins/prevent-xmlrpc/

WordPress brute force attack via wp.getUsersBlogs
https://isc.sans.edu/diary/+WordPress+brute+force+attack+via+wp.getUsersBlogs/18427

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://shb.fpt-software.com/

Paths without secure XFO header:

- https://shb.fpt-software.com/ubb_threads/invoker/_test/user_uploads/
- https://shb.fpt-software.com/ubb_threads/invoker/user_uploads/
- https://shb.fpt-software.com/buddypress/cmd/wizards/
- https://shb.fpt-software.com/buddypress/cmd/userfiles/
- https://shb.fpt-software.com/buddypress/amcharts/tag/
- https://shb.fpt-software.com/ubb_threads/invoker/nusoap/
- https://shb.fpt-software.com/wp-content/plugins/alipay/includes/api_tenpay/inc.tenpay_notify.php
- https://shb.fpt-software.com/ubb_threads/utf8/
- https://shb.fpt-software.com/buddypress/amcharts/oauth/
- https://shb.fpt-software.com/ubb_threads/invoker/_test/_tests/
- https://shb.fpt-software.com/wp-content/plugins/zelist-directory/
- https://shb.fpt-software.com/ubb_threads/axis2/
- https://shb.fpt-software.com/ubb_threads/invoker/_test/uploader/
- https://shb.fpt-software.com/wp-content/plugins/wpsnapapp/
- https://shb.fpt-software.com/buddypress/amcharts/Install/
- https://shb.fpt-software.com/ubb_threads/invoker/admin0/
- https://shb.fpt-software.com/buddypress/amcharts/developers/
- https://shb.fpt-software.com/buddypress/cmd/bugs/
- https://shb.fpt-software.com/buddypress/amcharts/database/
- https://shb.fpt-software.com/ubb_threads/invoker/_test/RestApi/!test/
- https://shb.fpt-software.com/wp-content/plugins/wp-easy-gallery/

Request

```
POST /?__cf_chl_f_tk=CQ4e_CDM8lP3qzrTKzVq35kt51UD3ZlnaHcweZvVKxM-1672902270-0-gaNycGzNEqU HTTP/1.1
Host: shb.fpt-software.com
Content-Length: 5629
accept-language: en-US
content-type: multipart/form-data; boundary=----WebKitFormBoundaryJEhUnltYpHyBob07
accept: */*
origin: https://shb.fpt-software.com
cookie: __cf_bm=R0Shmnp8yajW6EOFCB8aRSR_Yg3ZdIgYeZjYJerXv94-1672902302-0-
```

```
AXs1ef3FT6/CLewdNzCV8KwF/ha4+Vcval7HqVZad3QtqJKWW3wonNdopw2A/6MS871c1FmiDSk22/PIS8DphNNTZkBUiPTr9bNe3eC5X/gE
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://shb.fpt-software.com/?__cf_chl_f_tk=Amb0jlgNivJtAZIENs6KgOk78RHbMTRk_pTywEmCkic-1672902138-0-gaNycGzNBz0
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

------WebKitFormBoundaryJEhUnltYpHyBobO7
Content-Disposition: form-data; name="md"

EwBiEcSsUlzjg_8rL4Ul8JhUE4efVXYE0nmW6rT5Da8-1672902270-0-
AZ2dfH_NSvoWiEcDMjhfjqeoefgdnSQJk09KkzlUZWAEs0KUICZd_0V0uXHH4uDsXAStuftCA_hpqpw3mlO7e60SLgEYsh4XCF9KqDofIOpdTllyairoQVaV8qa0RLv7uEY7jhebI0I
3uMcj1eFipY4zrDQMUZstlkpaKrOABsTubMbhoeZM_z1JJeXxCYUiuJD7YcH93NYFYYXrn2Ld7pPXyTzNKAVEl15OJp0MYpvXEhv9N2f6SJbtGpqrFB7EUX1mjjyWRZ3OCL6rcPTAQI
cQYTPmeX7nJ5jovq0XXGNq9eImrYBrufB_8zhXtm3zfmelaORGGSQT5x7xutkKmW3JBUkIENCFN3s1HjSIloqwWUVrm9_RNnR1QVrXTh5xKFNbX4JAYtcHyU8ZTWBn4Xr8tHFxk2gUr
B2qcbPnxCDQOT-
RKOFoxBdmi69C7NtwtcUruZQ0Q94TOppRJpflYtvs1JFwjIrJc_pQizfkrTNq06aMwCAzp0uRFsi4FVIaTbCqQHC0hrn2lbAWQlICpNY4xwlUdYGphH5Q_wXjknXgkxEvcHncgz7sZz
wQ_l90-A
------WebKitFormBoundaryJEhUnltYpHyBobO7
Content-Disposition: form-data; name="r"

DNGR_9VFO4yyWOfwLJNtkoPf2ho3ckwKYYm6_wDXwKw-1672902270-0-
ATzgxvELl282ZC5iV+sZiJbKMnM2h973Hxen5qGrd28qTElhomrK+HOJz8s8sOKPV7Yr33fTqm62VXGImHm8HDMA6BgaN35BD8+gZQcCmxDHOytqeOtNE3aJTUlmXj7YxKdJeP/bX/A
W6GGICPJB06Kr71VWfg4kewfSPChTfahiAVkiUSIpo6B+WgMQKxxOp6X3neeQnD8QeQc/WHBWf/IC1/7NOct2H7WN+wzoOvSrvy+hIZ9c4JB5mDXEtAhk08TKyN88+z/uUssPgynKNG
Xtg31B9F++cffdBGIRHMPvrFn6yo2EHFnDy7O1mIBHiU1FSCBO2JxKWne8dv/ueaQRym2Gh5Nlg0V0OHvQAvSbzA7JhUvR6ikUE+Q8XyHa0OUU1zl42OqZwOLDVg4U8oqGdC/8a2FTg
+JLx8fKg/AMoqUZvU2jco+3tkROgNByL4ytohcR36+yZD+G++aXyc6CSeNr5ZNkrEEcBhrxazWc8256T45UKhjVlXP6Klcq7bWmf0WQl5a89cHC1+xsHNGyAemvrvch39tz5en1ViAw
PvVb3OJ5GCfC0G3dRwSRTfcQTSZz7v9Unxo1eQvqpdwjPyB0l5aQFjDzZdpliszRx8MauX2HtYahftVUM2GU0+zCWQjASjew6ZqxeSO1RtUT6q3ukIPHCuotBy+X5qlz9LVpDDG2lk7
56gFb54PQLA0BBE+jgdhbpOBm97eeENzLsSi7SI94R0Gs5FyfV2XKoVD+EhW4YeVI2bCYfW7EQIrnN7nTQF1QGxOm1M8o27NWiQwQ5uU+uk1ezZzmTVi8aGAfn5/BHEEwZnSR3DEDFa
+N1O8Jth0Txz9tc1aboM+5/VKjBJJJmPTTMMYKx6mMo80FX1deXGTlWfW+9dkc2UvTTVBrRZ/YXTQ+hVMHiVu5bklkHXFB2nzFf5/tpjxVxlIjjXVyrbMHK4+pghVhmS/DClUwPICLN
/89qe1FMX9bPjNhbWPLpDJgud3ngs9eYISTmu+6xAfGZBnVyfRiYUGes4Pe8VUx13RF2qdYwzUlq78ZjKaCw8utTLjosd6mU9wEqyTQCpU5nie2gPGJ9IoDqN01hS2sIqQuEIh4Tw3I
boNpnGstJMDe0snwB89+s4/t6RVwhmzjouEZh2+w1+7fT/kZ1nSdFqXeaXFi+PUhOfFE6mSBLanjFBB/3i2nl1Rmp1WT1O12E5vxyhKyETtpgwa56fwf+wHPIJrUXic0sli976i5xBW
YPB107xhlwDlGyBcLy009KQzqejOQ1ZLA9coGdp5zf2ckRyRYVdw0MHwSq0VC02ySH5iXoLPXYrf4Fpqs1/Mki9pAVVlXd19tin5Ud5+JNVNq0CuN1f8ScfYblGmXBD9S4Mt0rC+O1w
KyOY4afv2O7JZbKs2TQbCHj1c+0URpDpGw24omhJo6SuOri1P2kTlyDCTEWbnQSN0zN3EbPzxEzCpeMoGuGfIB44NQtkY0ueTDlskxgS/N64IFlVneLrfcXg6FdcqKbNUFKkOa6pX2S
8M0VTaZ2Ld1TnnQW4e42jFj8Eyi26XVauB5xRhwr2Umv/4IAlrSPq4S72N1nv2PF7pqvRaYiNIRrQKFZrdXJsF2WoBL93SPt1hqG4/vcjHPkbVvfRLNS5dm5YVB+olNtoQ+uUtl9Atj
fzbROPJLp7IVroiJBVXrYLfFcm5YoBTUylO3I4b10aBOAXFptCY8ZOayCs0syC49JOZ7yZDg0z3oqg4WveyRhPOHkkUXgqr7fhgoVc4NzGc+ZF59s1AeBzX1KKp+SDe3tJ9w7+yRAFj
Ktk3X/kPhILeVP53fn0c5VtHDeGt6HHSybNoz0mU1jzEizAIK6W+LJK1RIefsQeZ75CdPcqPC4tXA7Gplm13ILXOxwjcj2a4g651VehDlZOcIEdxysoYUylRFBmKZHvfBR4XP2YCLx6
Qj36DyvI8T2YhFlBnVHIyckLKujvBdf/OBcMd2HHEHh08ly/FfjC8DZmbe3CYQXrpJWRgD1LOEZ5Vt8vHmU70q9R2rdanAJcu3SAz7+Rmo1dF6iF67g2fQQV9MRBze4HI6p+LOG/hbf
m2h4z+qTkCTZyJe28L8E47fQIk4Hcsn7bSI5Ufp2RcUFjnWxwrfkX32Sk1nrcvGnLF6DO28FZUszLfuA0uRiEtfcdzZRUKCLCgP6EZTKLEyso6PmDVGeMRcI3jqlxqHNJRQvVxA6jBV
7TYzxQb3EnU7SUzLkkY28eKu49oMT+RB2vN9x9GnfAo1EW7pPE/GsgA6bICs9/v5QgnRZO2s1F43yBVR0XCfSPV+MOiQIT5AH6/deFTlSjmcXC8mWLyylEMptTvaOoRKttYmTlgUGBQ
+X2YQQ1AtMQPKJmmNqTT8cXQjl2LQihCwsBkDG8KTE8SedN0WNLnTQq0vb+qqy/OwHTkGllyEMyu8VEVYbGNjyGKKhsbtuGUhH6IZXjVKe+NPStFO+MBQL7tD+FFSRpAUlUMQw6p7NA
1kleojhrEhpPOCCwKQTsLcYggqaVBgu4AEHBDnzrqlbS4Eoo43bQr+KJZiFDlz8aSWQ4kJDh9cT4VJ18S/jKUvpQ/jnaku6PWnE5s+x2szZcxs6Swn0g58e0VfB7O8ue2kCl8LNmcDn
xS5ZHfJrek04yDlAqVltRvtRERQUY+4TWvIXRMwFeEnyUkTU+8S/ybj71RyIr/QvASBuxyYouqj4FKVsKRrwqxzDA2Euzyfk4kOdqqBzu2SCiPL6nCxhkuX7UbMfahcPYKfXYfLC/UF
ke8GRZ4Ql3a7LMtO990tOmMvtIH1Spo7KvDhrxzYnPaoibp+nmFOeCY0tdhVEpCxnJWK0xoYQbvOmDN60vnoZVWBSFE18FshoPsZNsseug2HQJ890rLv+Use3s4PhpuybI+aEOTUZ10
0IU8TvKpehD3k+w+7JQOgn5Hjb9g74tM82z9rLKW512C/b0jKCQZ8CxXlNdpHbgF8T+yMUWklYHXaHlx8ImadK+ZOVoxRgo9MadXD0vQJy/O2LS3nQn4VJuxBkfadti+8e2lVk6aahv
+YNipUI3YGdDNOw/ytvVUFNgCx8SHK/qEqPERo1LA1Etgq020weQ1tBEWLExYLZErS7C+EzZlSIkxMBlka7ds9qmo7irRMo15NqMQteh7gYMXWm+Lgpu5WYmsgc5T7nqav3qQUXmntf
eLxNKK5btY6ShtdPgYFV9V7rimP24+p4viKKe7lLxHrLLyYqqDNTR0Tb394M12HlC/bEdWZaIQVvOj4GGIi3B9QQLWADMRj6l2OYjMdOH7QSdk5T5vhpWX9f/Ey/8ThIQeQQRWZ5E7/
wux7nctyuHxI+iju4V8CGwB4YtRnbRS6XZ4ykvljdUflhHbo70W7rh5GzsM3vj4zI8xVMegNPEsMnmFE24EgvIKCgfsgOL0oNIzbzkXh9zFFERob/1kKVW2WFC3Anvl9acgoJ3AYS9r
kRVsZmuee3jggRtkJnaz4im1RDf+n1Kj3qzdfASK3gfVaRdc+ttVv5yZszav6dktRkvfoLnvEbdBbpQjw0H5YybILmy8pRWaWtP0RNenRW6N4cnLH2YJZ87lq1D1hq9ibk9vWRiPLdV
+JT7Wh3hiqV+0QEFK0U8pyXLOl0jJjYjqSU1CRxCiGuodb2nlgq6KIAIwZ69S9M11SWOJMFJ2zM/Np9uOI+RHmcm2e+Y1P8RZVEZy/CVFpJNyjZd5BiO2AhCFICGOR5kjl9DZ6H5g1D
nWtMhCShGVARGcyjSfBb5GbwOqiz+uihzrSdQsZb/zY8M9f9HXZEoMdX0dRWp+qcdp/Q6Iuf0fN4FPGbM8VYFnPZsARnGzKh6xB/kcB2oBKPgnqaPfLykkFgJ+8NJ1RLl3krYCTrtN/
CobPqqfcMgVlOL994VkJBnWvpz0h6pQl3VJEmEXbUYpKSdKN8Kb1CylevnDyqSupBXfoP+KObTouo+v1Frb3i8gZMxhRTd8uo+djpM+EXu65bCLAFrE5xwuGUrWkHpBklRtkcVJ2W8y
bAc1SYM1vVhPVRc9W2IlDmdPup0e0nMaFf1xjNhRcMW4+YGi3zRVI9cGYZHuf/UMisK551x5+qzPHp3fecL6rDbeIFn1rbBjnTxyPFJSftH+wI9nMWvi6XYRHG7a2GZqw39zdn0Qjqm
sir8X5xtFcGWQRXi7ZewO7hwuDJQecvUwPpBJKrfcUlupeWf0NZs10la6wiRgDT2vuyHyY1n/OUoef90oJBOWltBhlXkoU4YfWMsGKOCODV1rqLrcseNnlZMGbWUEz+ZIClu5jeI6G4
ZnTGAQkRtt5sqG+XG9bFrvJZH8UtYr3dazwkxOUKYeDBCvGjBMX8Z4LBvJWyle9eCGZ+xCKnMysoWVU3Z3Sa9GkZIyKTgmdmdzbWR6Mt3g6vmq3fGxJLHpkucVqPArwfVIKtOYk8GRk
/Njh2gCPvAzTZ7pag/WmcTFi2lly+foi8wlpDSoZ3D8TO2jUDCEU0PKdB3BrvD4IyI8net1/CCIqgvM1/mwCboB2LPNVnxxg31F5x3cxuboqPeXnohLuhk6nMLg8uN1BBXRMTt4eKQ6
g/U0w3VXSNq0WtNE52g1UJyFthTVteecIJHzmFYeAf0RZKOUqnWl5SRGqMJy/GSYO67pwZbCQgNm7Dx7YYeSDg16C+NoEP1jlhzwQl8l8IJCBJCCFrWl5iHyUmnI0Sn+C
------WebKitFormBoundaryJEhUnltYpHyBobO7--
```

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

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

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

Frame Buster Buster
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://shb.fpt-software.com/ Verified

List of cookies with missing, inconsistent or contradictory properties:

- https://shb.fpt-software.com/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://shb.fpt-software.com/
Cookie: __cf_bm=FnUUevfrLmkiyZL1JuFCdB4oEhy40SaDcLLQNQyivuk-1672215725-0-
Af8TJCE4a4nChTkLCsfImzNcPSjCn7vjVqvCqL07UN4pNMsdBiTGrSIiwlHAq6VPl+RTMLaTixWJst3R4/VKyTLmNDlS4HPINboOg2s/7EQXZ7yuCIp15iCuVhMysr9QXYPsix82oX1
QG+vM4bYRiu8=; cf_chl_2=815b105252d1bcd; cf_chl_rc_m=3
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: shb.fpt-software.com
Connection: Keep-alive

log=admin&pwd=acunetixtest&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

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.

Impact

Cookies can be accessed by client-side scripts.

https://shb.fpt-software.com/ Verified

Cookies without HttpOnly flag set:

- https://shb.fpt-software.com/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://shb.fpt-software.com/
Cookie: __cf_bm=FnUUevfrLmkiyZL1JuFCdB4oEhy40SaDcLLQNQyivuk-1672215725-0-
Af8TJCE4a4nChTkLCsfImzNcPSjCn7vjVqvCqL07UN4pNMsdBiTGrSIiwlHAq6VPl+RTMLaTixWJst3R4/VKyTLmNDlS4HPINboOg2s/7EQXZ7yuCIp15iCuVhMysr9QXYPsix82oX1
QG+vM4bYRiu8=; cf_chl_2=815b105252d1bcd; cf_chl_rc_m=3
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: shb.fpt-software.com
Connection: Keep-alive

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

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://shb.fpt-software.com/ Verified

Cookies without Secure flag set:

- https://shb.fpt-software.com/wp-comments-post.php

```
Set-Cookie: comment_author_f8bce339782a23aa7365909d28c7d5fd=+; expires=Wed, 29-Dec-2021 01:34:20 GMT; Max-Age=0;
path=/
```

- https://shb.fpt-software.com/wp-comments-post.php

```
Set-Cookie: comment_author_email_f8bce339782a23aa7365909d28c7d5fd=+; expires=Wed, 29-Dec-2021 01:34:20 GMT; Max-
Age=0; path=/
```

- https://shb.fpt-software.com/wp-comments-post.php

```
Set-Cookie: comment_author_url_f8bce339782a23aa7365909d28c7d5fd=+; expires=Wed, 29-Dec-2021 01:34:20 GMT; Max-Age=0;
path=/
```

Request

```
POST /wp-comments-post.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Referer: https://shb.fpt-software.com/
Content-Length: 136
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: shb.fpt-software.com
Connection: Keep-alive

author=MmzHrrdb&comment=555&comment_parent=0&comment_post_ID=1&email=sample%40email.tst&submit=Post%20Comment&url=http://www.vulnweb.com
```

Recommendation

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

Documentation files

One or more documentation files (e.g. readme.txt, changelog.txt, ...) were found. The information contained in these files could help an attacker identify the web application you are using and sometimes the version of the application. It's recommended to remove these files from production systems.

Impact

These files may disclose sensitive information. This information can be used to launch further attacks.

https://shb.fpt-software.com/

Documentation files:

- https://shb.fpt-software.com/**readme.html**
  File contents (first 100 characters):

```
<!DOCTYPE html>
<html>
<head>
<meta name="viewport" content="width=device-width" />
<meta http-equiv ...
```

- https://shb.fpt-software.com/**license.txt**
  File contents (first 100 characters):

  ```
  WordPress - Web publishing software

  Copyright 2011-2018 by the contributors

  This program is fr ...
  ```

Request

```
GET /readme.html HTTP/1.1
Cookie: __cf_bm=z2WtbX5MZ66atl8JO3nuzRavuo6GiExZWyi45XbjMn0-1672210599-0-
AYWEfAKOgrki+UxixBEfcL9BALS76V8DwTKimTo48vPzGvvgg812v7S3ODyrwZTF/TcJ/+wtJwNy+XTtEhSEg3pkTFn6RrASPQXtRwsz+9zy; cf_chl_rc_m=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: shb.fpt-software.com
Connection: Keep-alive
```

Recommendation

Remove or restrict access to all documentation file acessible from internet.

HTTP Strict Transport Security (HSTS) not implemented

HTTP Strict Transport Security (HSTS) tells a browser that a web site is only accessable 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://shb.fpt-software.com/

URLs where HSTS is not enabled:

- https://shb.fpt-software.com/ubb_threads/invoker/_test/user_uploads/
- https://shb.fpt-software.com/ubb_threads/invoker/user_uploads/
- https://shb.fpt-software.com/buddypress/cmd/wizards/
- https://shb.fpt-software.com/buddypress/cmd/userfiles/
- https://shb.fpt-software.com/buddypress/amcharts/tag/
- https://shb.fpt-software.com/ubb_threads/invoker/nusoap/
- https://shb.fpt-software.com/wp-content/plugins/alipay/includes/api_tenpay/inc.tenpay_notify.php
- https://shb.fpt-software.com/ubb_threads/utf8/
- https://shb.fpt-software.com/buddypress/amcharts/oauth/
- https://shb.fpt-software.com/ubb_threads/invoker/_test/_tests/
- https://shb.fpt-software.com/wp-content/plugins/zelist-directory/
- https://shb.fpt-software.com/ubb_threads/axis2/
- https://shb.fpt-software.com/ubb_threads/invoker/_test/uploader/
- https://shb.fpt-software.com/wp-content/plugins/wpsnapapp/
- https://shb.fpt-software.com/buddypress/amcharts/Install/
- https://shb.fpt-software.com/ubb_threads/invoker/admin0/

- https://shb.fpt-software.com/buddypress/amcharts/developers/
- https://shb.fpt-software.com/buddypress/cmd/bugs/
- https://shb.fpt-software.com/buddypress/amcharts/database/
- https://shb.fpt-software.com/ubb_threads/invoker/_test/RestApi/!test/
- https://shb.fpt-software.com/wp-content/plugins/wp-easy-gallery/

Request

```
POST /?__cf_chl_f_tk=CQ4e_CDM8lP3qzrTKzVq35kt51UD3ZlnaHcweZvVKxM-1672902270-0-gaNycGzNEqU HTTP/1.1
Host: shb.fpt-software.com
Content-Length: 5629
accept-language: en-US
content-type: multipart/form-data; boundary=----WebKitFormBoundaryJEhUnltYpHyBobO7
accept: */*
origin: https://shb.fpt-software.com
cookie: __cf_bm=R0Shmnp8yajW6EOFCB8aRSR_Yg3ZdIgYeZjYJerXv94-1672902302-0-
AXs1ef3FT6/CLewdNzCV8KwF/ha4+Vcval7HqVZad3QtqJKWW3wonNdopw2A/6MS871c1FmiDSk22/PIS8DphNNTZkBUiPTr9bNe3eC5X/gE
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://shb.fpt-software.com/?__cf_chl_f_tk=Amb0jlgNivJtAZIENs6KgOk78RHbMTRk_pTywEmCkic-1672902138-0-gaNycGzNBz0
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

------WebKitFormBoundaryJEhUnltYpHyBobO7
Content-Disposition: form-data; name="md"

EwBiEcSsUlzjg_8rL4Ul8JhUE4efVXYE0nmW6rT5Da8-1672902270-0-
AZ2dfH_NSvoWiEcDMjhfjqeoefgdnSQJk09KkzlUZWAEs0KUICZd_0V0uXHH4uDsXAStuftCA_hpqpw3mlO7e60SLgEYsh4XCF9KqDofIOpdTllyairoQVaV8qa0RLv7uEY7jhebI0I
3uMcj1eFipY4zrDQMUZstlkpaKrOABsTubMbhoeZM_z1JJeXxCYUiuJD7YcH93NYFYYXrn2Ld7pPXyTzNKAVEl15OJp0MYpvXEhv9N2f6SJbtGpqrFB7EUX1mjjyWRZ3OCL6rcPTAQI
cQYTPmeX7nJ5jovq0XXGNq9eImrYBrufB_8zhXtm3zfmelaORGGSQT5x7xutkKmW3JBUkIENCFN3s1HjSIloqwWUVrm9_RNnR1QVrXTh5xKFNbX4JAYtcHyU8ZTWBn4Xr8tHFxk2gUr
B2qcbPnxCDQOT-
RKOFoxBdmi69C7NtwtcUruZQ0Q94TOppRJpflYtvs1JFwjIrJc_pQizfkrTNq06aMwCAzp0uRFsi4FVIaTbCqQHC0hrn2lbAWQlICpNY4xwlUdYGphH5Q_wXjknXgkxEvcHncgz7sZz
wQ_l90-A
------WebKitFormBoundaryJEhUnltYpHyBobO7
Content-Disposition: form-data; name="r"

DNGR_9VFO4yyWOfwLJNtkoPf2ho3ckwKYYm6_wDXwKw-1672902270-0-
ATzgxvELl282ZC5iV+sZiJbKMnM2h973Hxen5qGrd28qTElhomrK+HOJz8s8sOKPV7Yr33fTqm62VXGImHm8HDMA6BgaN35BD8+gZQcCmxDHOytqeOtNE3aJTUlmXj7YxKdJeP/bX/A
W6GGICPJB06Kr71VWfg4kewfSPChTfahiAVkiUSIpo6B+WgMQKxxOp6X3neeQnD8QeQc/WHBWf/IC1/7NOct2H7WN+wzoOvSrvy+hIZ9c4JB5mDXEtAhk08TKyN88+z/uUssPgynKNG
Xtg31B9F++cffdBGIRHMPvrFn6yo2EHFnDy7O1mIBHiU1FSCBO2JxKWne8dv/ueaQRym2Gh5Nlg0V0OHvQAvSbzA7JhUvR6ikUE+Q8XyHa0OUU1zl42OqZwOLDVg4U8oqGdC/8a2FTg
+JLx8fKg/AMoqUZvU2jco+3tkROgNByL4ytohcR36+yZD+G++aXyc6CSeNr5ZNkrEEcBhrxazWc8256T45UKhjVlXP6Klcq7bWmf0WQl5a89cHC1+xsHNGyAemvrvch39tz5en1ViAw
PvVb3OJ5GCfC0G3dRwSRTfcQTSZz7v9Unxo1eQvqpdwjPyB0l5aQFjDzZdpliszRx8MauX2HtYahftVUM2GU0+zCWQjASjew6ZqxeSO1RtUT6q3ukIPHCuotBy+X5qlz9LVpDDG2lk7
56gFb54PQLA0BBE+jgdhbpOBm97eeENzLsSi7SI94R0Gs5FyfV2XKoVD+EhW4YeVI2bCYfW7EQIrnN7nTQF1QGxOm1M8o27NWiQwQ5uU+uk1ezZzmTVi8aGAfn5/BHEEwZnSR3DEDFa
+N1O8Jth0Txz9tc1aboM+5/VKjBJJJmPTTMMYKx6mMo80FX1deXGTlWfW+9dkc2UvTTVBrRZ/YXTQ+hVMHiVu5bklkHXFB2nzFf5/tpjxVxlIjjXVyrbMHK4+pghVhmS/DClUwPICLN
/89qe1FMX9bPjNhbWPLpDJgud3ngs9eYISTmu+6xAfGZBnVyfRiYUGes4Pe8VUx13RF2qdYwzUlq78ZjKaCw8utTLjosd6mU9wEqyTQCpU5nie2gPGJ9IoDqN01hS2sIqQuEIh4Tw3I
boNpnGstJMDe0snwB89+s4/t6RVwhmzjouEZh2+w1+7fT/kZ1nSdFqXeaXFi+PUhOfFE6mSBLanjFBB/3i2nl1Rmp1WT1O12E5vxyhKyETtpgwa56fwf+wHPIJrUXic0sli976i5xBW
YPB107xhlwDlGyBcLy009KQzqejOQ1ZLA9coGdp5zf2ckRyRYVdw0MHwSq0VC02ySH5iXoLPXYrf4Fpqs1/Mki9pAVVlXd19tin5Ud5+JNVNq0CuN1f8ScfYblGmXBD9S4Mt0rC+O1w
KyOY4afv2O7JZbKs2TQbCHj1c+0URpDpGw24omhJo6SuOri1P2kTlyDCTEWbnQSN0zN3EbPzxEzCpeMoGuGfIB44NQtkY0ueTDlskxgS/N64IFlVneLrfcXg6FdcqKbNUFKkOa6pX2S
8M0VTaZ2Ld1TnnQW4e42jFj8Eyi26XVauB5xRhwr2Umv/4IAlrSPq4S72N1nv2PF7pqvRaYiNIRrQKFZrdXJsF2WoBL93SPt1hqG4/vcjHPkbVvfRLNS5dm5YVB+olNtoQ+uUtl9Atj
fzbROPJLp7IVroiJBVXrYLfFcm5YoBTUylO3I4b10aBOAXFptCY8ZOayCs0syC49JOZ7yZDg0z3oqg4WveyRhPOHkkUXgqr7fhgoVc4NzGc+ZF59s1AeBzX1KKp+SDe3tJ9w7+yRAFj
Ktk3X/kPhILeVP53fn0c5VtHDeGt6HHSybNoz0mU1jzEizAIK6W+LJK1RIefsQeZ75CdPcqPC4tXA7Gplm13ILXOxwjcj2a4g651VehDlZOcIEdxysoYUylRFBmKZHvfBR4XP2YCLx6
Qj36DyvI8T2YhFlBnVHIyckLKujvBdf/OBcMd2HHEHh08ly/FfjC8DZmbe3CYQXrpJWRgD1LOEZ5Vt8vHmU70q9R2rdanAJcu3SAz7+Rmo1dF6iF67g2fQQV9MRBze4HI6p+LOG/hbf
m2h4z+qTkCTZyJe28L8E47fQIk4Hcsn7bSI5Ufp2RcUFjnWxwrfkX32Sk1nrcvGnLF6DO28FZUszLfuA0uRiEtfcdzZRUKCLCgP6EZTKLEyso6PmDVGeMRcI3jqlxqHNJRQvVxA6jBV
7TYzxQb3EnU7SUzLkkY28eKu49oMT+RB2vN9x9GnfAo1EW7pPE/GsgA6bICs9/v5QgnRZO2s1F43yBVR0XCfSPV+MOiQIT5AH6/deFTlSjmcXC8mWLyylEMptTvaOoRKttYmTlgUGBQ
+X2YQQ1AtMQPKJmmNqTT8cXQjl2LQihCwsBkDG8KTE8SedN0WNLnTQq0vb+qqy/OwHTkGllyEMyu8VEVYbGNjyGKKhsbtuGUhH6IZXjVKe+NPStFO+MBQL7tD+FFSRpAUlUMQw6p7NA
1kleojhrEhpPOCCwKQTsLcYggqaVBgu4AEHBDnzrqlbS4Eoo43bQr+KJZiFDlz8aSWQ4kJDh9cT4VJ18S/jKUvpQ/jnaku6PWnE5s+x2szZcxs6Swn0g58e0VfB7O8ue2kCl8LNmcDn
xS5ZHfJrek04yDlAqVltRvtRERQUY+4TWvIXRMwFeEnyUkTU+8S/ybj71RyIr/QvASBuxyYouqj4FKVsKRrwqxzDA2Euzyfk4kOdqqBzu2SCiPL6nCxhkuX7UbMfahcPYKfXYfLC/UF
ke8GRZ4Ql3a7LMtO990tOmMvtIH1Spo7KvDhrxzYnPaoibp+nmFOeCY0tdhVEpCxnJWK0xoYQbvOmDN60vnoZVWBSFE18FshoPsZNsseug2HQJ890rLv+Use3s4PhpuybI+aEOTUZ10
0IU8TvKpehD3k+w+7JQOgn5Hjb9g74tM82z9rLKW512C/b0jKCQZ8CxXlNdpHbgF8T+yMUWklYHXaHlx8ImadK+ZOVoxRgo9MadXD0vQJy/O2LS3nQn4VJuxBkfadti+8e2lVk6aahv
+YNipUI3YGdDNOw/ytvVUFNgCx8SHK/qEqPERo1LA1Etgq020weQ1tBEWLExYLZErS7C+EzZlSIkxMBlka7ds9qmo7irRMo15NqMQteh7gYMXWm+Lgpu5WYmsgc5T7nqav3qQUXmntf
eLxNKK5btY6ShtdPgYFV9V7rimP24+p4viKKe7lLxHrLLyYqqDNTR0Tb394M12HlC/bEdWZaIQVvOj4GGIi3B9QQLWADMRj6l2OYjMdOH7QSdk5T5vhpWX9f/Ey/8ThIQeQQRWZ5E7/
wux7nctyuHxI+iju4V8CGwB4YtRnbRS6XZ4ykvljdUflhHbo70W7rh5GzsM3vj4zI8xVMegNPEsMnmFE24EgvIKCgfsgOL0oNIzbzkXh9zFFERob/1kKVW2WFC3Anvl9acgoJ3AYS9r
kRVsZmuee3jggRtkJnaz4im1RDf+n1Kj3qzdfASK3gfVaRdc+ttVv5yZszav6dktRkvfoLnvEbdBbpQjw0H5YybILmy8pRWaWtP0RNenRW6N4cnLH2YJZ87lq1D1hq9ibk9vWRiPLdV
+JT7Wh3hiqV+0QEFK0U8pyXLOl0jJjYjqSU1CRxCiGuodb2nlgq6KIAIwZ69S9M11SWOJMFJ2zM/Np9uOI+RHmcm2e+Y1P8RZVEZy/CVFpJNyjZd5BiO2AhCFICGOR5kjl9DZ6H5g1D
nWtMhCShGVARGcyjSfBb5GbwOqiz+uihzrSdQsZb/zY8M9f9HXZEoMdX0dRWp+qcdp/Q6Iuf0fN4FPGbM8VYFnPZsARnGzKh6xB/kcB2oBKPgnqaPfLykkFgJ+8NJ1RLl3krYCTrtN/
CobPqqfcMgVlOL994VkJBnWvpz0h6pQl3VJEmEXbUYpKSdKN8Kb1CylevnDyqSupBXfoP+KObTouo+v1Frb3i8gZMxhRTd8uo+djpM+EXu65bCLAFrE5xwuGUrWkHpBklRtkcVJ2W8y
bAc1SYM1vVhPVRc9W2IlDmdPup0e0nMaFf1xjNhRcMW4+YGi3zRVI9cGYZHuf/UMisK551x5+qzPHp3fecL6rDbeIFn1rbBjnTxyPFJSftH+wI9nMWvi6XYRHG7a2GZqw39zdn0Qjqm
sir8X5xtFcGWQRXi7ZewO7hwuDJQecvUwPpBJKrfcUlupeWf0NZs10la6wiRgDT2vuyHyY1n/OUoef90oJBOWltBhlXkoU4YfWMsGKOCODV1rqLrcseNnlZMGbWUEz+ZIClu5jeI6G4
```

```
ZnTGAQkRtt5sqG+XG9bFrvJZH8UtYr3dazwkxOUKYeDBCvGjBMX8Z4LBvJWyle9eCGZ+xCKnMysoWVU3Z3Sa9GkZIyKTgmdmdzbWR6Mt3g6vmq3fGxJLHpkucVqPArwfVIKtOYk8GRk
/Njh2gCPvAzTZ7pag/WmcTFi2lly+foi8wlpDSoZ3D8TO2jUDCEU0PKdB3BrvD4IyI8net1/CCIqgvM1/mwCboB2LPNVnxxg31F5x3cxuboqPeXnohLuhk6nMLg8uN1BBXRMTt4eKQ6
g/U0w3VXSNq0WtNE52g1UJyFthTVteecIJHzmFYeAf0RZKOUqnWl5SRGqMJy/GSYO67pwZbCQgNm7Dx7YYeSDg16C+NoEP1jlhzwQl8l8IJCBJCCFrWl5iHyUmnI0Sn+C
------WebKitFormBoundaryJEhUnltYpHyBobO7--
```

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

Possible sensitive directories

One or more possibly sensitive directories were found. These resources are not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

Impact

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

https://shb.fpt-software.com/

Possible sensitive directories:

- https://shb.fpt-software.com/buddypress/amcharts/fck/**crm**
- https://shb.fpt-software.com/ubb_threads/invoker/_test/admin0/**manager**

Request

```
GET /ubb_threads/index_files/admin-console/ HTTP/1.1
Cookie: __cf_bm=XXYCcHO6Y4Gzbl7KMePQ0sNN1X_LTjFKo8qx8RgFc7E-1672909865-0-
Acg1vDLjho657H7oNjHK6bbauc2bHZr6Q5RhGireEBLe1hbxnbsi/uuc5Cma6AcClzNsx+5Hs+7IrFFTqASZAJWz1ceLLypuKnDLS84CTf9D; cf_chl_2=ff566390659d71b;
cf_chl_rc_ni=3
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: shb.fpt-software.com
Connection: Keep-alive
```

Recommendation

Restrict access to these directories or remove them from the website.

References

Web Server Security and Database Server Security
https://www.acunetix.com/websitesecurity/webserver-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://shb.fpt-software.com/

List of pages that could be cached:

- https://shb.fpt-software.com/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://shb.fpt-software.com/
Cookie: __cf_bm=IMtAYKdX6PYPKpcotzvmUVX6zfxS_RG7Kxqx74GRdeQ-1672904700-0-
AR0KikR2inxvcBOG5Xc/mHtcZvrJUb2dY9IYOfbpb0qg2KDJ9rBjNwvkTAyhJ68teMwZt8nKZqG5x8gsRq+dE1VNGBHlT79KEtKOhzz/VSGO; cf_chl_2=ff566390659d71b;
cf_chl_rc_ni=3
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: shb.fpt-software.com
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://shb.fpt-software.com/ Verified

Session cookies scoped to parent domain:

- https://shb.fpt-software.com/buddypress/amcharts/_tests/

```
Set-Cookie: __cf_bm=sXr5b3AdtlCZzf1JJ7X9dwQgdRiBpfSjnV7qKFoOuHc-1672972098-0-
AZb53+o65HmazuHVfizKO6hQvhLKMDdp9lXcHrJ1Zdesep5mBNksC9GPuICtHPinn0sYe5HYzpH2Rx0vkZF8HM6id+fsr9nFA4iBhkfbGS9s;
path=/; expires=Fri, 06-Jan-23 02:58:18 GMT; domain=.fpt-software.com; HttpOnly; Secure; SameSite=None
```

- https://shb.fpt-software.com/ubb_threads/invoker/_test/wp-includes/

```
Set-Cookie: __cf_bm=UHNIdgToAwhKhlZ5cz3f4M_0GML0cmG6n3zCiRs.CYY-1672972104-0-
AZJr7BcoQahr1h1wAo+snpftutzlYW2xXboGzMyCN5JYQHYX4KcRiIT+ojtAk8TP67mQoMIBm1GV/Dh8SjZI+H17ntZVJW3wF4qS3MkafFw1;
path=/; expires=Fri, 06-Jan-23 02:58:24 GMT; domain=.fpt-software.com; HttpOnly; Secure; SameSite=None
```

- https://shb.fpt-software.com/buddypress/cmd/_files/

```
Set-Cookie: __cf_bm=DWAebz5ozH6zqX6M3U6GZMZzmEKDLJWCEXiwce0YDRU-1672972109-0-
AZReovBiiBw1XdgvPPeJN8bfygqkk1dThlvMW8MrByjtB3kgS22ZA6LEsJfkl2SSzIK/k6mt9oMUPFUsF9kKmwGGhUdl4Gg+YvEQDDqBm0XR;
path=/; expires=Fri, 06-Jan-23 02:58:29 GMT; domain=.fpt-software.com; HttpOnly; Secure; SameSite=None
```

- https://shb.fpt-software.com/ubb_threads/invoker/_test/user_uploads/

```
Set-Cookie: __cf_bm=X8SbLijUGOd5iodqN8MMhV1i6bT8nfyJI_.A9A5tbbM-1672972112-0-
Adj/fx06bB2kHyLgccXdxus5lFxL+NlzHVdZH0DkdVmhRZbfr3hYOl5t4gWWG/ucVYQEGyNLHJGU+83kCJE2S0rJPR6Cefg3nZ8SaC+Xzsq+;
path=/; expires=Fri, 06-Jan-23 02:58:32 GMT; domain=.fpt-software.com; HttpOnly; Secure; SameSite=None
```

- https://shb.fpt-software.com/buddypress/amcharts/_src/

```
Set-Cookie: __cf_bm=.Vm22lMps7iO5ojhQobJEBwM89hIV8Hdt2MHf5O9p1s-1672972125-0-
AVAbbwtVjRYw/Aljec73KXron2EuMLFPnKLYTxculR1HHMKUz5VSVJUsR8ExH7zAilpYwl299U4kFa0sZ7Ughz5KTCLA8xjiTCuOggQBE9H7;
path=/; expires=Fri, 06-Jan-23 02:58:45 GMT; domain=.fpt-software.com; HttpOnly; Secure; SameSite=None
```

- https://shb.fpt-software.com/buddypress/wp-includes/

```
Set-Cookie: __cf_bm=YNm8NEOOM3.Qs_xG0IMA6iPP6lVdtKszMLBBoTef_lE-1672972129-0-
AXDEdXNWRfsjgWv3qN7l0gtXUKWGiHrCF7TP16MPNfWMwJi/NT5kN5F0MKq/rdwwL35OvApalPhRdoZ4IHGiRNMKdDi9FpqrBKH2udpCTdpK;
path=/; expires=Fri, 06-Jan-23 02:58:49 GMT; domain=.fpt-software.com; HttpOnly; Secure; SameSite=None
```

- https://shb.fpt-software.com/cdn-cgi/challenge-platform/h/b/orchestrate/jsch/v1

```
Set-Cookie: __cf_bm=vjKLIGhfPQbLGDkVQ67l.CJpFoEpzXT8xEccSdKORJY-1672972098-0-
Ac8w9Hq1+SygvtL3DasmDDdjvX0VVrX+Y8T/g8dbHnsJNbzKTrtZTWwPtfX+vaFbuYaG91euxmUzmgKAjTXz3VcpCh8reIR7l6H+RixglbbJ;
path=/; expires=Fri, 06-Jan-23 02:58:18 GMT; domain=.fpt-software.com; HttpOnly; Secure; SameSite=None
```

- https://shb.fpt-software.com/cdn-cgi/challenge-platform/h/b/orchestrate/managed/v1

```
Set-Cookie: __cf_bm=561IOGAjvSOcqsxkzE_0iDkbJSb98OOHRTmZEsZs83Q-1672972097-0-
ARYUhNS4Qb7Ueb9kGX4xP3jsRHez5G+neSFjZkCexLxZZCAtSXEoOCWsEXhQ51O0e55S9zoXTrdSucOIgly/zUQOs68gUFd0ouIy+B08941c;
path=/; expires=Fri, 06-Jan-23 02:58:17 GMT; domain=.fpt-software.com; HttpOnly; Secure; SameSite=None
```

- https://shb.fpt-software.com/buddypress/webadmin/

```
Set-Cookie: __cf_bm=rD_RSiI0EPm4.Hc_ueNe7Yaf16.ggM.j9dzYW.z03zQ-1672972149-0-
AbVtwuGHR4s+SIiDZNtRHjgvKUaXF0yNbHDASdIlf5EvJJ0SvZ0CZuPBN3uU8Okk5oCp09zq7pRtOm06xJ1xd8hvjMXLMN0lgk1nM5RUE6Ic;
path=/; expires=Fri, 06-Jan-23 02:59:09 GMT; domain=.fpt-software.com; HttpOnly; Secure; SameSite=None
```

- https://shb.fpt-software.com/buddypress/user_uploads/

```
Set-Cookie: __cf_bm=D50CeT1ROo9HMaCQdMhPZYZu0ionjODPFfqw7W6K3so-1672972173-0-
AXKjnaSTzXJnbd0M4ART9ZoTgoAEiXt1t/P1VtIXcx5DFJgs7wN1T2sCtX4TpWCzs8vkmXfuomUIRDBIBqe1l8bNC2aVjUgffi6xkZBxYb5o;
path=/; expires=Fri, 06-Jan-23 02:59:33 GMT; domain=.fpt-software.com; HttpOnly; Secure; SameSite=None
```

- https://shb.fpt-software.com/cdn-cgi/challenge-platform/h/b/orchestrate/jsch/v1

```
Set-Cookie: __cf_bm=urzqsCmzKNLWJY8ROkEG397Fbhce4gjCB7LdeQ_2dhw-1672972107-0-
ARmGh/973O/K5/M8HIPaKVhwXpw8ieACRLfBBfLDYnz2KpmY4cfBadPhTCAoeaNE4nYMGJTxYsPYmb7stCnqOJ6tkTiPE2DobERE6y10e6uK;
```

```
path=/; expires=Fri, 06-Jan-23 02:58:27 GMT; domain=.fpt-software.com; HttpOnly; Secure; SameSite=None
```

- https://shb.fpt-software.com/buddypress/user_guide/

```
Set-Cookie: __cf_bm=7gvr65rVWdnIVoVnW7d8hE0thNB.HLfGbywid6PSNEg-1672972181-0-
AdTsofMWvy5v86mwi9VGV5Rrp3JEYm8+SOzXnQDsqeuYNIdDlHaooDb9ACaog9XCNA+Mx969bjdSJVA3wpGhRyndkRciHjc7cfEwcbZe2PTN;
path=/; expires=Fri, 06-Jan-23 02:59:41 GMT; domain=.fpt-software.com; HttpOnly; Secure; SameSite=None
```

- https://shb.fpt-software.com/cdn-cgi/challenge-platform/h/b/orchestrate/managed/v1

```
Set-Cookie: __cf_bm=uTEDmW7exW3WqPVMSl0m_Xmt6PbwIBhvrH6FyhdQCy4-1672972108-0-
ATIVjOddXcwB2E+FL3ZTwKvAxiJMaULETBi930KzNGDhrT4nww1Yv9nRAI+uzPAGlEuzmeR7fXau6vq0HSmbogZN4pc2T3Dy4szsZhh0HsSM;
path=/; expires=Fri, 06-Jan-23 02:58:28 GMT; domain=.fpt-software.com; HttpOnly; Secure; SameSite=None
```

- https://shb.fpt-software.com/cdn-cgi/challenge-platform/h/b/orchestrate/jsch/v1

```
Set-Cookie: __cf_bm=QzHCXpun9SIiNTQ7lTpkRjR7X2o4By5nELSw.FLH4NM-1672972149-0-
AeRwo6MSKzM1YdQDCqxHKEjh0cJEQwoDngbdiyBCwSeCj39CRvJIh1759KnD/ZNcAOohFKBzb+cv1S4JnC+zSzYvrCX53vC7leDQuya1tXOh;
path=/; expires=Fri, 06-Jan-23 02:59:09 GMT; domain=.fpt-software.com; HttpOnly; Secure; SameSite=None
```

- https://shb.fpt-software.com/ubb_threads/invoker/_test/user_uploads/

```
Set-Cookie: __cf_bm=ZdNlZJZuw5mwHwjgr2KdXO.iZfBB2dWFpS31RWOAE54-1672972167-0-
AflYRxjgOUOfK7wVO/rG98xOBwOj1W5RxZt+kcbE+VbUHg8mhvVltR/QamLk2VdncXJ2+uFjS+Rhg0suZWbMMhSlaFhXKjTheI/A//n3QjE2;
path=/; expires=Fri, 06-Jan-23 02:59:27 GMT; domain=.fpt-software.com; HttpOnly; Secure; SameSite=None
```

- https://shb.fpt-software.com/cdn-cgi/challenge-platform/h/b/orchestrate/jsch/v1

```
Set-Cookie: __cf_bm=MwC.cQSTq4IePdaS8TnWow3YncxG5kIDZCtBWL66ldo-1672972173-0-
AaZoFjd6nxO17KO+Zp/nlM7e7oYl5trcYozI3loH9vIOCP0KMC0t41Rb/Vt+Fq5FIBOJOZfs+B4py6MPPi2Am4yahZh09/KTrEQq+l+Jm/q1;
path=/; expires=Fri, 06-Jan-23 02:59:33 GMT; domain=.fpt-software.com; HttpOnly; Secure; SameSite=None
```

- https://shb.fpt-software.com/cdn-cgi/challenge-platform/h/b/orchestrate/jsch/v1

```
Set-Cookie: __cf_bm=qyk1b7F8pCedJfcIuqhdMVvpDxd9vh51bZuNbteTi1I-1672972155-0-
AZFrKnptCQBbbigNc/Bt/2x6J4aO0LtsGMINcYfNItY+FZq/ZpEzIVyNUd3cTqqawBcw0dE9OsGhJ+7wRAJJFg4mb+zdynncp8vWtUf3SNmw;
path=/; expires=Fri, 06-Jan-23 02:59:15 GMT; domain=.fpt-software.com; HttpOnly; Secure; SameSite=None
```

- https://shb.fpt-software.com/cdn-cgi/challenge-platform/h/b/orchestrate/jsch/v1

```
Set-Cookie: __cf_bm=1AZrCclc85d0ClQbIAHwdFQ3_F_zCQXrARiDbDt6lBg-1672972202-0-
AZzbQzFtEOMt91+pauVOx1uIcgQqmHcKGI9gODJO13tVA86DeX0wVcr9o6d2zg4BfVwESMMS9EWMQHB+R3Nu75RWI06EXcSlbPEYxND2EJtu;
path=/; expires=Fri, 06-Jan-23 03:00:02 GMT; domain=.fpt-software.com; HttpOnly; Secure; SameSite=None
```

- https://shb.fpt-software.com/cdn-cgi/challenge-platform/h/b/orchestrate/managed/v1

```
Set-Cookie: __cf_bm=zRUIBOG6by.YiD_htV4w7f9Qir6z4GNwcXVtmc9gtGQ-1672972207-0-
AXmH3ftvZbmZrdKQ5ADhQBMzXIs7z/meudexBeV278Ac41vlwPlMSVSz025h8ipfNq3RNvS4eh/QPmpTmbt0F5il4mziTDYFEUI4GdEwv6N3;
path=/; expires=Fri, 06-Jan-23 03:00:07 GMT; domain=.fpt-software.com; HttpOnly; Secure; SameSite=None
```

- https://shb.fpt-software.com/cdn-cgi/challenge-platform/h/b/orchestrate/managed/v1

```
Set-Cookie: __cf_bm=COgNSqetnM7XfA5sQOAytZ1EwHJJwBNdIbaUAf1tIfo-1672972149-0-
AQo7+DjvkzYn+A8R9CQddAw4IUr+nU4ItSD6I73v8uzMpWcj3bRwEdfIe9D7DbyXkTFdocGedtsAn5918nJnNXMnfz63bUG1cgm/XJJ+A4GR;
path=/; expires=Fri, 06-Jan-23 02:59:09 GMT; domain=.fpt-software.com; HttpOnly; Secure; SameSite=None
```

- https://shb.fpt-software.com/

```
Set-Cookie: __cf_bm=2l22Ue0RKLbaMbAnv2lnvINJWoWdsnj3O3SVIsGTVjE-1672972287-0-
AfhscM1VBr8VmBBRGSX2fE8qdMIkYb9w624EZy6pOVcsjl6IqMMhWKv+derxcZWOaq0G6qMSCwyLIutEaWqLCI+SZ19XqpXMvW0YkCiZaXZT;
path=/; expires=Fri, 06-Jan-23 03:01:27 GMT; domain=.fpt-software.com; HttpOnly; Secure; SameSite=None
```

Request

```
GET / HTTP/1.1
Referer: https://shb.fpt-software.com/
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: shb.fpt-software.com
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://shb.fpt-software.com/wp-login.php

Request

```
POST //wp-login.php HTTP/1.1
Content-type: application/x-www-form-urlencoded
Cookie: __cf_bm=9fG6TYMi8jqtWwN7LsOrO5Ue4Ow6xcz3MUORz3gym2o-1672214147-0-
AUTCIlwSzAqH2Znzph7bfoTb6mNJXO/6UEfxi7fWQHq58mGc3R6lpdWStyqDzqCvfrJl8U80NPSe1vDkO/GFGM2QuR0o/2YuIXNHC48UxwJZchvVlVGYOn2aXYNUW+hpOHjVDAKifij
vkjAPkhYpDDE=
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: shb.fpt-software.com
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

Your WordPress Installation Is Using the 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

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://shb.fpt-software.com/

Request

```
GET /?rest_route=/wp/v2/users HTTP/1.1
Cookie: __cf_bm=069JkpR1BoL3r4KqpJMpzOwAU9RhUU7PCIvGz4Kn.6U-1672211005-0-
ATwsAjwXtbyH+Zp1i5zeg/8SHQBXDD4k+oQCy576YcQw2AEOMVelZAbOixiCobuoQ1AmmutqYU6MqbjEffeqn3MFAnKaioiTAhOF6TGFGovHd8R5L6v2AAzsRGH0TRgQSTnk9nCSazw
W0/a73GwWA0s=; cf_chl_rc_m=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: shb.fpt-software.com
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/

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://shb.fpt-software.com/

Paths without CSP header:

- https://shb.fpt-software.com/ubb_threads/invoker/user_uploads/
- https://shb.fpt-software.com/buddypress/cmd/wizards/
- https://shb.fpt-software.com/buddypress/cmd/userfiles/
- https://shb.fpt-software.com/buddypress/amcharts/tag/
- https://shb.fpt-software.com/ubb_threads/invoker/nusoap/
- https://shb.fpt-software.com/wp-content/plugins/alipay/includes/api_tenpay/inc.tenpay_notify.php
- https://shb.fpt-software.com/ubb_threads/utf8/
- https://shb.fpt-software.com/ubb_threads/invoker/_test/user_uploads/
- https://shb.fpt-software.com/buddypress/amcharts/oauth/
- https://shb.fpt-software.com/wp-content/plugins/zelist-directory/
- https://shb.fpt-software.com/ubb_threads/axis2/
- https://shb.fpt-software.com/ubb_threads/invoker/_test/uploader/
- https://shb.fpt-software.com/wp-content/plugins/wpsnapapp/
- https://shb.fpt-software.com/buddypress/amcharts/Install/
- https://shb.fpt-software.com/ubb_threads/invoker/admin0/
- https://shb.fpt-software.com/buddypress/amcharts/developers/
- https://shb.fpt-software.com/buddypress/cmd/bugs/
- https://shb.fpt-software.com/buddypress/amcharts/database/
- https://shb.fpt-software.com/ubb_threads/invoker/_test/RestApi/!test/
- https://shb.fpt-software.com/wp-content/plugins/wp-easy-gallery/
- https://shb.fpt-software.com/wp-content/plugins/wp-display-users/

Request

```
GET /?__cf_chl_rt_tk=DWAhYZSPR4UHqsHBI1ob402assQVQr6MFS3ulOiK2Ho-1672903034-0-gaNycGzNCD0&p=1 HTTP/1.1
Referer: https://shb.fpt-software.com/
Cookie: __cf_bm=whtcydEqSK.vpWqb2bcwk2nU1lO7auvYzg76zlzT3cI-1672904792-0-
ASKt5/hMTDxZG0tuX8SZmEE1xbBg0TwE4zMPtQo7zym/HK7IKAqMlQleSFPtllhFy9xt1fSUJzDQRpQzyDlfsIKRfNjrM/b9ts01xwWhw7/7; cf_chl_2=ff566390659d71b;
cf_chl_rc_ni=3
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: shb.fpt-software.com
Connection: Keep-alive
```

Recommendation

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

References

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

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

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://shb.fpt-software.com/

Version detected: **PHP/7.0.32**.

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://shb.fpt-software.com/

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: shb.fpt-software.com
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://shb.fpt-software.com/cdn-cgi/rum

Pages where SRI is not implemented:

- https://shb.fpt-software.com/cdn-cgi/rum
  Script SRC: **https://performance.radar.cloudflare.com/beacon.js**

Request

```
POST /cdn-cgi/rum? HTTP/1.1
Host: shb.fpt-software.com
Content-Length: 3879
accept-language: en-US
content-type: application/json
accept: */*
origin: https://shb.fpt-software.com
cookie: cf_chl_2=ff566390659d71b; cf_chl_rc_ni=1; __cf_bm=tc0iBeqy3ppplZK8MZDiCvQiaJca5c4fWlwRtDIMOXs-1672903016-0-
AfhxR44drfSUuXWSp/z0a69l5KLlXgSjX5P07th7pBR5d/WDDb3L/EfkIKKrO9IjbyZc0j5epBE/D23alg7B+2ow/KSkynHzuJHO6NHosocc
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://shb.fpt-software.com/wp-includes/css/dist/block-library/undefined
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://shb.fpt-
software.com/wp-includes/css/dist/block-library/style.min.css?
ver=5.0","s":94.3,"d":603.5,"i":"link","p":"http/1.1","rs":0,"re":0,"fs":94.3,"ds":94.3,"de":94.3,"cs":94.3,"ce":94.3,"qs":99.9,"ps":692.1,
"pe":697.8,"ws":0,"ss":94.3,"ts":299,"ec":18446744073709552000,"dc":0},{"n":"https://shb.fpt-software.com/wp-includes/css/dist/block-
library/theme.min.css?
ver=5.0","s":94.9,"d":800.6,"i":"link","p":"http/1.1","rs":0,"re":0,"fs":94.9,"ds":94.9,"de":94.9,"cs":113.5,"ce":120.1,"qs":121,"ps":890,"
pe":895.5,"ws":0,"ss":118,"ts":299,"ec":18446744073709552000,"dc":0},{"n":"https://shb.fpt-software.com/wp-
content/themes/twentynineteen/style.css?
ver=1.0","s":95.5,"d":881,"i":"link","p":"http/1.1","rs":0,"re":0,"fs":95.5,"ds":95.5,"de":95.5,"cs":112.9,"ce":120.5,"qs":121.4,"ps":972.7
,"pe":976.5,"ws":0,"ss":118.7,"ts":299,"ec":18446744073709552000,"dc":0},{"n":"https://shb.fpt-software.com/wp-
content/themes/twentynineteen/js/skip-link-focus-fix.js?
ver=20151215","s":95.9,"d":843.9,"i":"script","p":"http/1.1","rs":0,"re":0,"fs":95.9,"ds":95.9,"de":95.9,"cs":115.3,"ce":123,"qs":123.1,"ps
":930.8,"pe":939.8,"ws":0,"ss":120.5,"ts":299,"ec":18446744073709552000,"dc":0},{"n":"https://shb.fpt-software.com/wp-includes/js/wp-
embed.min.js?
ver=5.0","s":96.5,"d":732,"i":"script","p":"http/1.1","rs":0,"re":0,"fs":96.5,"ds":96.5,"de":96.5,"cs":114.2,"ce":124.7,"qs":124.9,"ps":824
.1,"pe":828.5,"ws":0,"ss":120.8,"ts":299,"ec":18446744073709552000,"dc":0},
{"n":"https://static.cloudflareinsights.com/beacon.min.js/vaafb692b2aea4879b33c060e79fe94621666317369993","s":96.9,"d":202.8,"i":"script","
p":"","rs":0,"re":0,"fs":96.9,"ds":0,"de":0,"cs":0,"ce":0,"qs":0,"ps":0,"pe":299.7,"ws":0,"ss":0,"ts":0,"ec":0,"dc":0},
{"n":"https://shb.fpt-software.com/wp-includes/js/wp-emoji-release.min.js?
ver=5.0","s":207,"d":1086,"i":"script","p":"http/1.1","rs":0,"re":0,"fs":207,"ds":207,"de":207,"cs":243.6,"ce":245.6,"qs":245.7,"ps":1287.8
,"pe":1293,"ws":0,"ss":244.2,"ts":299,"ec":18446744073709552000,"dc":0},{"n":"https://shb.fpt-software.com/wp-
content/themes/twentynineteen/print.css?
ver=1.0","s":209.1,"d":1251,"i":"link","p":"","rs":0,"re":0,"fs":209.1,"ds":209.1,"de":209.1,"cs":209.1,"ce":209.1,"qs":0,"ps":1460.1,"pe":
1460.1,"ws":0,"ss":209.1,"ts":4269,"ec":3969,"dc":3969}],"referrer":"","documentWriteIntervention":false,"errorCount":0,"eventType":1,"firs
tPaint":1064.3000000044703,"firstContentfulPaint":1064.3000000044703,"si":100,"startTime":1672903011402.5,"versions":
{"fl":"2022.11.3","js":"2022.10.1","timings":2},"pageloadId":"79496bd3-677f-410f-8258-4a3a3b3d9b51","location":"https://shb.fpt-
software.com/wp-includes/css/dist/block-library/undefined","wd":true,"timingsV2":
{"unloadEventStart":0,"unloadEventEnd":0,"domInteractive":1142.2000000029802,"domContentLoadedEventStart":1166.3000000044703,"domContentLoa
dedEventEnd":1171.1000000014901,"domComplete":1461.7000000029802,"loadEventStart":1461.8999999985099,"loadEventEnd":1462.6000000014901,"typ
e":"navigate","redirectCount":0,"initiatorType":"navigation","nextHopProtocol":"","workerStart":0,"redirectStart":0,"redirectEnd":0,"fetchS
tart":2.8000000044703484,"domainLookupStart":2.8000000044703484,"domainLookupEnd":2.8000000044703484,"connectStart":2.8000000044703484,"con
nectEnd":2.8000000044703484,"secureConnectionStart":2.8000000044703484,"requestStart":0,"responseStart":22.399999998509884,"responseEnd":22
.399999998509884,"transferSize":12287,"encodedBodySize":11987,"decodedBodySize":11987,"serverTiming":[{"name":"cf-q-
config","duration":0.0000079999999798019,"description":""}],"name":"https://shb.fpt-software.com/wp-includes/css/dist/block-
library/undefined","entryType":"navigation","startTime":0,"duration":1462.6000000014901},"siteToken":"3738ecc515634f0897fdf687e0a6b45c","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.

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

References

Subresource Integrity
https://developer.mozilla.org/en-US/docs/Web/Security/Subresource_Integrity

SRI Hash Generator
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://shb.fpt-software.com/

Detected Cloudflare WAF from the headers.

Request

```
GET /9500453 HTTP/1.1
Cookie: __cf_bm=26KLWDlW4RM6a8enjC5EXwwglRZfyzDhaiDmyB3KFXY-1672902151-0-
AYIl0NYaHS6uVTsBqdW1Xq4O/KHcP+F+1km8YplfDu9YCSmsIUnDY9iWmbYo8JNsxk+rnhnHnHBIoGtEyUJgVNOfYLIzdF6nCtPrIf823sYM
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: shb.fpt-software.com
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://shb.fpt-software.com/

https://shb.fpt-software.com/cdn-cgi/rum

https://shb.fpt-software.com/wp-content/plugins/Copy%20of%20google-map-generator/

https://shb.fpt-software.com/wp-content/plugins/mailpoet/

https://shb.fpt-software.com/wp-content/themes/twentynineteen/js/

https://shb.fpt-software.com/wp-login.php

https://shb.fpt-software.com/xmlrpc.php