

Developer Report

Acunetix Security Audit

2024-03-15

Scan of www.apeccbn.org

Scan details





Scan information	
Start time	2024-03-15T10:17:46.280045+08:00
Start url	http://www.apeccbn.org/
Host	www.apeccbn.org
Scan time	3 minutes, 54 seconds
Profile	Full Scan
Server information	nginx
Responsive	True
Server OS	Unknown
Server technologies	PHP
Scan status	failed
Application build	15.2.221208162

Threat level

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.

Alerts distribution

Total alerts found	9
 High	1
 Medium	2
 Low	4
 Informational	2

Alerts summary

! TLS/SSL certificate invalid date

Classification	
CVSS3	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L Base Score: 5.3 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: None Integrity Impact: None Availability Impact: Low
CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: Partial Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-298
Affected items	Variation
Web Server	1

! TLS/SSL Sweet32 attack

Classification	
CVSS3	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None

CVSS2	Base Score: 4.3 Access Vector: Network_accessible Access Complexity: Medium Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVE	CVE-2016-2183
CVE	CVE-2016-6329
CWE	CWE-310
Affected items	Variation
Web Server	1

TLS/SSL Weak Cipher Suites

Classification	
CVSS3	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N Base Score: 6.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: Low Integrity Impact: Low Availability Impact: None
CVSS2	Base Score: 3.3 Access Vector: Local_access Access Complexity: Medium Authentication: None Confidentiality Impact: Partial Integrity Impact: Partial Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-310
Affected items	Variation
Web Server	1

Cookies with missing, inconsistent or contradictory properties

Classification

CVSS3	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:N Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Required Scope: Unchanged Confidentiality Impact: None Integrity Impact: None Availability Impact: None
CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-284
Affected items	Variation
Web Server	1

 **Cookies without HttpOnly flag set**

Classification	
CVSS3	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:N Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Required Scope: Unchanged Confidentiality Impact: None Integrity Impact: None Availability Impact: None
CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined

CWE	CWE-1004
Affected items	Variation
Web Server	1

ⓘ Cookies without Secure flag set

Classification	
CVSS3	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N Base Score: 3.1 Attack Vector: Network Attack Complexity: High Privileges Required: None User Interaction: Required Scope: Unchanged Confidentiality Impact: Low Integrity Impact: None Availability Impact: None
CVSS2	Base Score: 2.6 Access Vector: Network_accessible Access Complexity: High Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-614
Affected items	Variation
Web Server	1

ⓘ HTTP Strict Transport Security (HSTS) not implemented

Classification	
CVSS3	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:N/A:N Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Required Scope: Changed Confidentiality Impact: None Integrity Impact: None Availability Impact: None

CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-16
Affected items	Variation
Web Server	1

Content Security Policy (CSP) not implemented

Classification	
CVSS3	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:N/A:N Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Required Scope: Changed Confidentiality Impact: None Integrity Impact: None Availability Impact: None
CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-1021
Affected items	Variation
Web Server	1

Permissions-Policy header not implemented

Classification

CVSS3	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:N/A:N Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Required Scope: Changed Confidentiality Impact: None Integrity Impact: None Availability Impact: None
CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-1021
Affected items	Variation
Web Server	1

Alerts details

TLS/SSL certificate invalid date

Severity	High
Reported by module	/Scripts/PerServer/SSL_Audit.script

Description

One of the TLS/SSL certificates sent by your server has either expired or is not yet valid.

Most web browsers will present end-users with a security warning, asking them to manually confirm the authenticity of your certificate chain. Software or automated systems may silently refuse to connect to the server.

This alert is not necessarily caused by the server (leaf) certificate, but may have been triggered by an intermediate certificate. Please refer to the certificate serial number in the alert details to identify the affected certificate.

Impact

This SSL certificate is not valid.

Recommendation

Verify Start Date and/or End Dates of your SSL Certificate.

Affected items

Web Server
Details
Error: could not render details.
Request headers

TLS/SSL Sweet32 attack

Severity	Medium
Reported by module	/Scripts/PerServer/SSL_Audit.script

Description

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.

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/)

[CVE-2016-2183](http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2183) (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2183)

[CVE-2016-6329](http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6329) (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6329)

Affected items

Web Server

Details

Cipher suites susceptible to Sweet32 attack (TLS1.2 on port 443):

- TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_RSA_WITH_3DES_EDE_CBC_SHA

Request headers

! TLS/SSL Weak Cipher Suites

Severity

Medium

Reported by module

/Scripts/PerServer/SSL_Audit.script

Description

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

Impact

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)

Affected items

Web Server

Details

Weak TLS/SSL Cipher Suites: (offered via TLS1.2 on port 443):

- TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (Medium strength encryption algorithm (3DES).)
- TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (Medium strength encryption algorithm (3DES).)
- TLS_RSA_WITH_3DES_EDE_CBC_SHA (Medium strength encryption algorithm (3DES).)

🔔 Cookies with missing, inconsistent or contradictory properties

Severity	Low
Reported by module	/RPA/Cookie_Validator.js

Description

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.

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)

Affected items

Web Server

Verified vulnerability

Details

List of cookies with missing, inconsistent or contradictory properties:

- https://www.apeccbn.org/

Cookie was set with:

```
Set-Cookie: PHPSESSID=pltsnfr2g5r4v8s08qd82bp077; path=/
```

This cookie has the following issues:

```
- Cookie without SameSite attribute.  
When cookies lack the SameSite attribute, Web browsers may apply different and someti
```

Request headers

GET / HTTP/1.1

Referer: https://www.apeccbn.org/

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

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36

Host: www.apeccbn.org

Connection: Keep-alive

🚩 Cookies without HttpOnly flag set

Severity	Low
Reported by module	/RPA/Cookie_Without_HttpOnly.js

Description

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.

Recommendation

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

Affected items

Web Server

Verified vulnerability

Details

Cookies without HttpOnly flag set:

- https://www.apeccbn.org/

```
Set-Cookie: PHPSESSID=pltsnfr2g5r4v8s08qd82bp077; path=/
```

Request headers

GET / HTTP/1.1

Referer: https://www.apeccbn.org/

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

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36

Host: www.apeccbn.org

Connection: Keep-alive

🔔 Cookies without Secure flag set

Severity	Low
Reported by module	/RPA/Cookie_Without_Secure.js

Description

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.

Recommendation

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

Affected items

Web Server

Verified vulnerability

Details

Cookies without Secure flag set:

- https://www.apeccbn.org/

```
Set-Cookie: PHPSESSID=pltsnfr2g5r4v8s08qd82bp077; path=/
```

Request headers

GET / HTTP/1.1

Referer: https://www.apeccbn.org/

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

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36

Host: www.apeccbn.org

Connection: Keep-alive

ⓘ HTTP Strict Transport Security (HSTS) not implemented

Severity	Low
Reported by module	/httpdata/HSTS_not_implemented.js

Description

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

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>)

Affected items

Web Server

Details

URLs where HSTS is not enabled:

- <https://www.apeccbn.org/>
- https://www.apeccbn.org/activity_detail.php
- <https://www.apeccbn.org/search.php>

Request headers

```
GET / HTTP/1.1
```

```
Referer: https://www.apeccbn.org/
```

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

```
Accept-Encoding: gzip,deflate,br
```

```
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
```

```
Host: www.apeccbn.org
```

```
Connection: Keep-alive
```

Content Security Policy (CSP) not implemented

Severity	Informational
Reported by module	/httpdata/CSP_not_implemented.js

Description

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.

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/)

Affected items

Web Server

Details

Paths without CSP header:

- <https://www.apeccbn.org/>
- https://www.apeccbn.org/activity_detail.php

Request headers

GET / HTTP/1.1

Referer: <https://www.apeccbn.org/>

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

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36

Host: www.apeccbn.org

Connection: Keep-alive

Permissions-Policy header not implemented

Severity	Informational
Reported by module	/httpdata/permissions_policy.js

Description

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

Impact

Recommendation

References

[Permissions-Policy / Feature-Policy \(MDN\)](https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Feature-Policy) (https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Feature-Policy)
[Permissions Policy \(W3C\)](https://www.w3.org/TR/permissions-policy-1/) (https://www.w3.org/TR/permissions-policy-1/)

Affected items

Web Server

Details

Locations without Permissions-Policy header:

- <https://www.apeccbn.org/>
- https://www.apeccbn.org/activity_detail.php
- <https://www.apeccbn.org/search.php>

Request headers

GET / HTTP/1.1

Referer: <https://www.apeccbn.org/>

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

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36

Host: www.apeccbn.org

Connection: Keep-alive

Scanned items (coverage report)

<https://www.apeccbn.org/>
<https://www.apeccbn.org/@webadmin/>
<https://www.apeccbn.org/about.php>
<https://www.apeccbn.org/activity.php>
https://www.apeccbn.org/activity_detail.php
https://www.apeccbn.org/activity_documents.php
https://www.apeccbn.org/activity_photo.php
https://www.apeccbn.org/calendar_detail.php
<https://www.apeccbn.org/css/>
<https://www.apeccbn.org/css/flexslider.css>
<https://www.apeccbn.org/css/pagenumbers.css>
<https://www.apeccbn.org/css/pagestyle.css>
<https://www.apeccbn.org/css/style.css>
<https://www.apeccbn.org/default.js>
<https://www.apeccbn.org/error.html>
<https://www.apeccbn.org/eventscalendar.php>
<https://www.apeccbn.org/follow.php>
<https://www.apeccbn.org/images/>
<https://www.apeccbn.org/index.php>
<https://www.apeccbn.org/js/>
<https://www.apeccbn.org/js/jquery.flexslider.js>
<https://www.apeccbn.org/js/scripts.js>
<https://www.apeccbn.org/link.php>
<https://www.apeccbn.org/news.php>
https://www.apeccbn.org/news_detail.php
<https://www.apeccbn.org/robots.txt>
<https://www.apeccbn.org/search.php>