OWASP TOP 10 2017

Description

The primary aim of the OWASP Top 10 is to educate developers, designers, architects, managers, and organizations about the consequences of the most important web application security weaknesses. The Top 10 provides basic techniques to protect against these high risk problem areas - and also provides guidance on where to go from here.

Disclaimer

This document or any of its content cannot account for, or be included in any form of legal advice. The outcome of a vulnerability scan (or security evaluation) should be utilized to ensure that diligent measures are taken to lower the risk of potential exploits carried out to compromise data.

Legal advice must be supplied according to its legal context. All laws and the environments in which they are applied, are constantly changed and revised. Therefore no information provided in this document may ever be used as an alternative to a qualified legal body or representative.

A portion of this report is taken from OWASP's Top Ten 2017 Project document, that can be found at http://www.owasp.org.

Scan Detail

Target	https://www.ashthailand.or.th/
Scan Type	Full Scan
Start Time	Feb 3, 2026, 10:41:08 PM GMT+6
Scan Duration	1 hour, 29 minutes
Requests	3190
Average Response Time	1169ms
Maximum Response Time	23483ms
Application Build	v24.1.240111130
Authentication Profile	-

Compliance at a Glance

CATEGORY	
0	A1 Injection
0	A2 Broken Authentication
13	A3 Sensitive Data Exposure
0	A4 XML External Entity (XXE)
1	A5 Broken Access Control
9	A6 Security Misconfiguration
1	A7 Cross Site Scripting (XSS)
0	A8 Insecure Deserialization
11	A9 Using Components with Known Vulnerabilities
0	A10 Insufficient Logging and Monitoring

Detailed Compliance Report by Category

This section is a detailed report that explains each vulnerability found according to individual compliance categories.

A1 Injection

Injection flaws, such as SQL, NoSQL, OS, and LDAP injection, occur when untrusted data is sent an interpreter as part of a command or query. The attackerâ s hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.

No alerts in this category

A2 Broken Authentication

Application functions related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities.

No alerts in this category

A3 Sensitive Data Exposure

Many web applications and APIs do not properly protect sensitive data, such as financial, healthcare and PII. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data may be compromised without extra protection, such as encryption at rest or in transit, and requires pecial precautions when exchanged with the browser.

HTTP Strict Transport Security (HSTS) Policy Not Enabled

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.

CWE

CWE-16

CVSS2

AV:N/AC:L/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

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	None
Integrity Impact	None
Availability Impact	None

CVSS4

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	Active
Confidentiality Impact to the Vulnerable System	None
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

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

https://www.ashthailand.or.th/

URLs where HSTS is not enabled:

- https://www.ashthailand.or.th/
- https://www.ashthailand.or.th/admin/

Request

```
GET / HTTP/1.1
Referer: https://www.ashthailand.or.th/
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/119.0.0.0 Safari/537.36
Host: www.ashthailand.or.th
Connection: Keep-alive
```

Recommendation

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

References

hstspreload.org
https://hstspreload.org/

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

SSL Certificate Is About To Expire

One of the TLS/SSL certificates used by your server is about to expire.

Once the certificate has expired, 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.

CWE

CWE-298

CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	None
Integrity Impact	Low
Availability Impact	None

CVSS4

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N

Base Score	6.9
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	None
Confidentiality Impact to the Vulnerable System	None
Integrity Impact to the Vulnerable System	Low
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

If an application server detects an expired certificate with a system it is communicating with, the application server may continue processing data as if nothing happened, or the connection may be abruptly terminated.

https://www.ashthailand.or.th/ Confidence: 100%

The TLS/SSL certificate (serial: 05b86f7417bc625694fbb6b89cf3d459d023) will expire in less than **60** days. The certificate validity period is from **Sat Dec 27 2025 17:34:01 GMT+0600 (Bangladesh Standard Time)** to **Fri Mar 27 2026 17:34:00 GMT+0600 (Bangladesh Standard Time)** (51 days left)

Recommendation

Contact your Certificate Authority to renew the SSL certificate.

Cookies Not Marked as Secure

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.

CWE

CWE-614

CVSS2

AV:N/AC:H/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	High
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

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	Low
Integrity Impact	None
Availability Impact	None

CVSS4

CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:A/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N

Base Score	2.1
Attack Vector	Network
Attack Complexity	High
Attack Requirements	None
Privileges Required	None
User Interaction	Active
Confidentiality Impact to the Vulnerable System	Low
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

Cookies could be sent over unencrypted channels.

https://www.ashthailand.or.th/ Verified

Cookies without Secure flag set:

- https://www.ashthailand.or.th/

```
Set-Cookie: ash_sessions=04uugs762832a6af4t6g8e9t2fg4lpd3; expires=Tue, 03-Feb-2026 18:42:34 GMT; Max-Age=7200; path=/;
HttpOnly
```

Request

```
GET / HTTP/1.1
Referer: https://www.ashthailand.or.th/
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/119.0.0.0 Safari/537.36
Host: www.ashthailand.or.th
Connection: Keep-alive
```

Recommendation

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

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.

CWE
CWE-284

CVSS2
AV:N/AC:L/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

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	None
Integrity Impact	None
Availability Impact	None

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	Active
Confidentiality Impact to the Vulnerable System	None
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

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

https://www.ashthailand.or.th/ Verified

List of cookies with missing, inconsistent or contradictory properties:

- https://www.ashthailand.or.th/

  Cookie was set with:

  ```
  Set-Cookie: ash_sessions=04uugs762832a6af4t6g8e9t2fg41pd3; expires=Tue, 03-Feb-2026 18:42:34 GMT; Max-Age=7200; path=/; HttpOnly
  ```

  This cookie has the following issues:

  ```
  - Cookie without SameSite attribute.
  When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It is therefore recommended to add a SameSite attribute with an appropriate value of either "Strict", "Lax", or "None".
  ```

Request

```
GET / HTTP/1.1
Referer: https://www.ashthailand.or.th/
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/119.0.0.0 Safari/537.36
Host: www.ashthailand.or.th
Connection: Keep-alive
```

Recommendation

Ensure that the cookies configuration complies with the applicable standards.

References

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

Securing cookies with cookie prefixes
https://www.sjoerdlangkemper.nl/2017/02/09/cookie-prefixes/

Cookies: HTTP State Management Mechanism

https://tools.ietf.org/html/draft-ietf-httpbis-rfc6265bis-05
SameSite Updates - The Chromium Projects
https://www.chromium.org/updates/same-site

draft-west-first-party-cookies-07: Same-site Cookies
https://tools.ietf.org/html/draft-west-first-party-cookies-07

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.

CWE
CWE-1021

CVSS2
AV:N/AC:L/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

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	None
Integrity Impact	None
Availability Impact	None

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	Active
Confidentiality Impact to the Vulnerable System	None
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

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://www.ashthailand.or.th/

Paths without CSP header:

- https://www.ashthailand.or.th/
- https://www.ashthailand.or.th/admin/

Request

```
GET / HTTP/1.1
Referer: https://www.ashthailand.or.th/
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/119.0.0.0 Safari/537.36
Host: www.ashthailand.or.th
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/

Permissions-Policy header not implemented

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

CWE
CWE-1021

CVSS2
AV:N/AC:L/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

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	None
Integrity Impact	None
Availability Impact	None

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	Active
Confidentiality Impact to the Vulnerable System	None
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

https://www.ashthailand.or.th/

Locations without Permissions-Policy header:

- https://www.ashthailand.or.th/
- https://www.ashthailand.or.th/admin/

Request

```
GET / HTTP/1.1
Referer: https://www.ashthailand.or.th/
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/119.0.0.0 Safari/537.36
Host: www.ashthailand.or.th
Connection: Keep-alive
```

References

Permissions-Policy / Feature-Policy (MDN)
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Feature-Policy

Permissions Policy (W3C)
https://www.w3.org/TR/permissions-policy-1/

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.

CWE
CWE-16

CVSS2
AV:N/AC:L/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS3
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	None
Confidentiality Impact to the Vulnerable System	None
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

No impact is associated with this vulnerability.

https://www.ashthailand.or.th/

Detected reverse proxy: Apache httpd

Request

```
GET / HTTP/1.1
Max-Forwards: 0
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/119.0.0.0 Safari/537.36
Host: www.ashthailand.or.th
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.

CWE
CWE-830

CVSS2
AV:N/AC:L/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS3
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Changed
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N

Base Score	6.9
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	None
Confidentiality Impact to the Vulnerable System	None
Integrity Impact to the Vulnerable System	Low
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

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

https://www.ashthailand.or.th/

Pages where SRI is not implemented:

- https://www.ashthailand.or.th/
  Script SRC: **https://cdn.jsdelivr.net/npm/select2@4.1.0-rc.0/dist/js/select2.min.js**

- https://www.ashthailand.or.th/
  Script SRC: **https://www.statcounter.com/counter/counter.js**

Request

```
GET / HTTP/1.1
Referer: https://www.ashthailand.or.th/
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/119.0.0.0 Safari/537.36
Host: www.ashthailand.or.th
Connection: Keep-alive
```

https://www.ashthailand.or.th/admin/

Pages where SRI is not implemented:

- https://www.ashthailand.or.th/admin/
  Script SRC: **https://www.google.com/recaptcha/api.js**

Request

```
GET /admin/ HTTP/1.1
Referer: https://www.ashthailand.or.th/
Cookie: ash_sessions=q393lt0lic4gnhhd5ac5kd763sot33d3; sc_is_visitor_unique=rx9500380.1770137330.FD71672D9B7F42069CA191F8C0C79A4B.1.1.1.1.1.1.1.1.1
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/119.0.0.0 Safari/537.36
Host: www.ashthailand.or.th
Connection: Keep-alive
```

Recommendation

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

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

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

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.

CWE
CWE-1021

CVSS2
AV:N/AC:M/Au:N/C:N/I:P/A:N

Access Vector	Network
Access Complexity	Medium
Authentication	None
Confidentiality	None
Integrity Impact	Partial
Availability Impact	None

CVSS3
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:L/A:N

Base Score	5.8
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Changed
Confidentiality	None
Integrity Impact	Low
Availability Impact	None

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N

Base Score	5.1
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	Active
Confidentiality Impact to the Vulnerable System	None
Integrity Impact to the Vulnerable System	Low
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

The impact depends on the affected web application.

https://www.ashthailand.or.th/

Paths without secure XFO header:

- https://www.ashthailand.or.th/
- https://www.ashthailand.or.th/admin/

Request

```
GET / HTTP/1.1
Referer: https://www.ashthailand.or.th/
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/119.0.0.0 Safari/537.36
Host: www.ashthailand.or.th
Connection: Keep-alive
```

Recommendation

Configure your web server to include an X-Frame-Options header and a CSP header with frame-ancestors directive. Consult Web references for more information about the possible values for this header.

References

The X-Frame-Options response header
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options

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

Development configuration files

One or more configuration files (e.g. Vagrantfile, Gemfile, Rakefile, ...) were found. These files may expose sensitive information that could help a malicious user to prepare more advanced attacks. It's recommended to remove or restrict access to this type of files from production systems.

CWE
CWE-538

CVSS2
AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

CVSS3
CVSS:3.0/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	Low
Integrity Impact	None
Availability Impact	None

CVSS4
CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:A/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N

Base Score	2.1
Attack Vector	Network
Attack Complexity	High
Attack Requirements	None
Privileges Required	None
User Interaction	Active
Confidentiality Impact to the Vulnerable System	Low
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

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

https://www.ashthailand.or.th/

Development configuration files:

- https://www.ashthailand.or.th/**composer.json**

  ```
  composer.json => Composer configuration file. Composer is a dependency manager for PHP.
  ```

- https://www.ashthailand.or.th/**.gitignore**

  ```
  .gitignore => Git configuration file. Git is a free and open source distributed version control system.
  ```

Request

```
GET /composer.json HTTP/1.1
Cookie: ash_sessions=04uugs762832a6af4t6g8e9t2fg4lpd3; sc_is_visitor_unique=rx9500380.1770137330.FD71672D9B7F42069CA191F8C0C79A4B.1.1.1.1.1.1.1.1.1
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/119.0.0.0 Safari/537.36
Host: www.ashthailand.or.th
Connection: Keep-alive
```

Recommendation

Remove or restrict access to all configuration files acessible from internet.

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.

CWE
CWE-538

CVSS2
AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

CVSS3
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N

Base Score	6.9
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	None
Confidentiality Impact to the Vulnerable System	Low
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

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

https://www.ashthailand.or.th/

Documentation files:

- https://www.ashthailand.or.th/**license.txt**
  File contents (first 100 characters):

```
The MIT License (MIT)

Copyright (c) 2014 - 2019, British Columbia Institute of Technology

Permissi ...
```

Request

```
GET /license.txt HTTP/1.1
Cookie: ash_sessions=q393lt0lic4gnhhd5ac5kd763sot33d3; sc_is_visitor_unique=rx9500380.1770137330.FD71672D9B7F42069CA191F8C0C79A4B.1.1.1.1.1.1.1.1.1
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/119.0.0.0 Safari/537.36
Host: www.ashthailand.or.th
```

```
Connection: Keep-alive
```

Recommendation

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

Version Disclosure (PHP)

The web server is sending the X-Powered-By: response headers, revealing the PHP version.

CVSS2
AV:N/AC:L/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS3
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N/E:P

Base Score	5.5
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	None
Confidentiality Impact to the Vulnerable System	Low
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

An attacker might use the disclosed information to harvest specific security vulnerabilities for the version identified.

https://www.ashthailand.or.th/

Version detected: **PHP/5.6.40**.

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

A4 XML External Entity (XXE)

Many older or poorly configured XML processors evaluate external entity references within XML documents. External entities can be used to disclose internal files using the file URI handler, internal file shares, internal port scanning, remote code execution, and denial of service attacks.

No alerts in this category

A5 Broken Access Control

Restrictions on what authenticated users are allowed to do are often not properly enforced. Attackers can exploit these flaws to access unauthorized functionality and/or data, such as access other users' accounts, view sensitive files, modify other users' data, change access rights, etc.

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.

CWE
CWE-1021

CVSS2
AV:N/AC:M/Au:N/C:N/I:P/A:N

Access Vector	Network
Access Complexity	Medium
Authentication	None
Confidentiality	None
Integrity Impact	Partial
Availability Impact	None

CVSS3
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:L/A:N

Base Score	5.8
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Changed
Confidentiality	None
Integrity Impact	Low
Availability Impact	None

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N

Base Score	5.1
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	Active
Confidentiality Impact to the Vulnerable System	None
Integrity Impact to the Vulnerable System	Low
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

The impact depends on the affected web application.

https://www.ashthailand.or.th/

Paths without secure XFO header:

- https://www.ashthailand.or.th/
- https://www.ashthailand.or.th/admin/

Request

```
GET / HTTP/1.1
Referer: https://www.ashthailand.or.th/
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/119.0.0.0 Safari/537.36
Host: www.ashthailand.or.th
Connection: Keep-alive
```

Recommendation

Configure your web server to include an X-Frame-Options header and a CSP header with frame-ancestors directive. Consult Web references for more information about the possible values for this header.

References

The X-Frame-Options response header
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options

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

A6 Security Misconfiguration

Security misconfiguration is the most commonly seen issue. This is commonly a result of insecure default configurations, incomplete or ad hoc configurations, open cloud storage, misconfigured HTTP headers, and verbose error messages containing sensitive information. Not only must all operating systems, frameworks, libraries, and applications be securly configured, but they must be patched and upgraded in a timely fashion.

HTTP Strict Transport Security (HSTS) Policy Not Enabled

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.

CWE
CWE-16

CVSS2
AV:N/AC:L/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

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	None
Integrity Impact	None
Availability Impact	None

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	Active
Confidentiality Impact to the Vulnerable System	None
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

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

https://www.ashthailand.or.th/
URLs where HSTS is not enabled:

- https://www.ashthailand.or.th/
- https://www.ashthailand.or.th/admin/

Request
```
GET / HTTP/1.1
Referer: https://www.ashthailand.or.th/
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/119.0.0.0 Safari/537.36
Host: www.ashthailand.or.th
Connection: Keep-alive
```

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

References

hstspreload.org
https://hstspreload.org/

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

SSL Certificate Is About To Expire

One of the TLS/SSL certificates used by your server is about to expire.

Once the certificate has expired, 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.

CWE
CWE-298

CVSS2
AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

CVSS3
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	None
Integrity Impact	Low
Availability Impact	None

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N

Base Score	6.9
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	None
Confidentiality Impact to the Vulnerable System	None
Integrity Impact to the Vulnerable System	Low
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

If an application server detects an expired certificate with a system it is communicating with, the application server may continue processing data as if nothing happened, or the connection may be abruptly terminated.

https://www.ashthailand.or.th/ Confidence: 100%

The TLS/SSL certificate (serial: 05b86f7417bc625694fbb6b89cf3d459d023) will expire in less than **60** days. The certificate validity period is from **Sat Dec 27 2025 17:34:01 GMT+0600 (Bangladesh Standard Time)** to **Fri Mar 27 2026 17:34:00 GMT+0600 (Bangladesh Standard Time)** (51 days left)

Recommendation

Contact your Certificate Authority to renew the SSL certificate.

Cookies Not Marked as Secure

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.

CWE
CWE-614

CVSS2
AV:N/AC:H/Au:N/C:P/I:N/A:N

Access Vector	Network

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

CVSS4
CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:A/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N

Base Score	2.1
Attack Vector	Network

Access Complexity	High
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

Attack Complexity	High
Privileges Required	None
User Interaction	Required
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

Attack Complexity	High
Attack Requirements	None
Privileges Required	None
User Interaction	Active
Confidentiality Impact to the Vulnerable System	Low
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

Cookies could be sent over unencrypted channels.

https://www.ashthailand.or.th/ Verified

Cookies without Secure flag set:

- https://www.ashthailand.or.th/

```
Set-Cookie: ash_sessions=04uugs762832a6af4t6g8e9t2fg4lpd3; expires=Tue, 03-Feb-2026 18:42:34 GMT; Max-Age=7200; path=/;
HttpOnly
```

Request

```
GET / HTTP/1.1
Referer: https://www.ashthailand.or.th/
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/119.0.0.0 Safari/537.36
Host: www.ashthailand.or.th
Connection: Keep-alive
```

Recommendation

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

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.

CWE

CWE-284

CVSS2

AV:N/AC:L/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

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	None
Integrity Impact	None

CVSS4

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	Active
Confidentiality Impact to the Vulnerable System	None
Integrity Impact to the Vulnerable System	None

Availability Impact	None

Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

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

https://www.ashthailand.or.th/ Verified

List of cookies with missing, inconsistent or contradictory properties:

- https://www.ashthailand.or.th/

  Cookie was set with:

  ```
  Set-Cookie: ash_sessions=04uugs762832a6af4t6g8e9t2fg41pd3; expires=Tue, 03-Feb-2026 18:42:34 GMT; Max-Age=7200; path=/; HttpOnly
  ```

  This cookie has the following issues:

  ```
  - Cookie without SameSite attribute.
  When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It is therefore recommended to add a SameSite attribute with an appropriate value of either "Strict", "Lax", or "None".
  ```

Request

```
GET / HTTP/1.1
Referer: https://www.ashthailand.or.th/
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/119.0.0.0 Safari/537.36
Host: www.ashthailand.or.th
Connection: Keep-alive
```

Recommendation

Ensure that the cookies configuration complies with the applicable standards.

References

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

Securing cookies with cookie prefixes
https://www.sjoerdlangkemper.nl/2017/02/09/cookie-prefixes/

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

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

draft-west-first-party-cookies-07: Same-site Cookies
https://tools.ietf.org/html/draft-west-first-party-cookies-07

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.

CWE
CWE-1021

CVSS2
AV:N/AC:L/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

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	None
Integrity Impact	None
Availability Impact	None

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	Active
Confidentiality Impact to the Vulnerable System	None
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

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://www.ashthailand.or.th/

Paths without CSP header:

- https://www.ashthailand.or.th/
- https://www.ashthailand.or.th/admin/

Request

```
GET / HTTP/1.1
Referer: https://www.ashthailand.or.th/
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/119.0.0.0 Safari/537.36
Host: www.ashthailand.or.th
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/

Permissions-Policy header not implemented

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

CWE
CWE-1021

CVSS2
AV:N/AC:L/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

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	None
Integrity Impact	None
Availability Impact	None

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	Active
Confidentiality Impact to the Vulnerable System	None
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

https://www.ashthailand.or.th/

Locations without Permissions-Policy header:

- https://www.ashthailand.or.th/
- https://www.ashthailand.or.th/admin/

Request

```
GET / HTTP/1.1
Referer: https://www.ashthailand.or.th/
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/119.0.0.0 Safari/537.36
Host: www.ashthailand.or.th
Connection: Keep-alive
```

References

Permissions-Policy / Feature-Policy (MDN)
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Feature-Policy

Permissions Policy (W3C)
https://www.w3.org/TR/permissions-policy-1/

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.

CWE
CWE-16

CVSS2
AV:N/AC:L/Au:N/C:N/I:N/A:N

CVSS3
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	None
Integrity Impact	None
Availability Impact	None

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	None
Confidentiality Impact to the Vulnerable System	None
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

No impact is associated with this vulnerability.

https://www.ashthailand.or.th/

Detected reverse proxy: Apache httpd

Request

```
GET / HTTP/1.1
Max-Forwards: 0
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/119.0.0.0 Safari/537.36
Host: www.ashthailand.or.th
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.

CWE

CWE-830

CVSS2

AV:N/AC:L/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Changed
Confidentiality	None

CVSS4

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N

Base Score	6.9
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	None
Confidentiality Impact to the Vulnerable System	None

Availability Impact	None

Integrity Impact	None
Availability Impact	None

Integrity Impact to the Vulnerable System	Low
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

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

https://www.ashthailand.or.th/

Pages where SRI is not implemented:

- https://www.ashthailand.or.th/
  Script SRC: **https://cdn.jsdelivr.net/npm/select2@4.1.0-rc.0/dist/js/select2.min.js**

- https://www.ashthailand.or.th/
  Script SRC: **https://www.statcounter.com/counter/counter.js**

Request

```
GET / HTTP/1.1
Referer: https://www.ashthailand.or.th/
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/119.0.0.0 Safari/537.36
Host: www.ashthailand.or.th
Connection: Keep-alive
```

https://www.ashthailand.or.th/admin/

Pages where SRI is not implemented:

- https://www.ashthailand.or.th/admin/
  Script SRC: **https://www.google.com/recaptcha/api.js**

Request

```
GET /admin/ HTTP/1.1
Referer: https://www.ashthailand.or.th/
Cookie: ash_sessions=q393lt0lic4gnhhd5ac5kd763sot33d3; sc_is_visitor_unique=rx9500380.1770137330.FD71672D9B7F42069CA191F8C0C79A4B.1.1.1.1.1.1.1.1.1
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/119.0.0.0 Safari/537.36
Host: www.ashthailand.or.th
Connection: Keep-alive
```

Recommendation

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

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

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

References

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

SRI Hash Generator

A7 Cross Site Scripting (XSS)

XSS flaws occur whenever an application includes untrusted data in a new web page without proper validation or escaping, or updates an existing web page with user-supplied data using a browser API that can create HTML or JavaScript. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.

Cross-site Scripting

Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.

CWE

CWE-79

CVSS2

AV:N/AC:L/Au:N/C:P/I:P/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	Partial
Availability Impact	None

CVSS3

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	None
Integrity Impact	Low
Availability Impact	None

CVSS4

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:L/VA:N/SC:L/SI:L/SA:N

Base Score	5.1
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	Active
Confidentiality Impact to the Vulnerable System	None
Integrity Impact to the Vulnerable System	Low
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	Low
Integrity Impact to the Subsequent System	Low
Availability Impact to the Subsequent System	None

Impact

Malicious JavaScript has access to all the same objects as the rest of the web page, including access to cookies and local storage, which are often used to store session tokens. If an attacker can obtain a user's session cookie, they can then impersonate that user.

Furthermore, JavaScript can read and make arbitrary modifications to the contents of a page being displayed to a user. Therefore, XSS in conjunction with some clever social engineering opens up a lot of possibilities for an attacker.

https://www.ashthailand.or.th/

URI was set to **"onmouseover='ejep(96662)'bad="**
The input is reflected inside a tag parameter between double quotes.

Request

```
GET /?"onmouseover='ejep(96662)'bad=" HTTP/1.1
Referer: https://www.ashthailand.or.th/
Cookie: ash_sessions=04uugs762832a6af4t6g8e9t2fg4lpd3; sc_is_visitor_unique=rx9500380.1770137330.FD71672D9B7F42069CA191F8C0C79A4B.1.1.1.1.1.1.1.1.1
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/119.0.0.0 Safari/537.36
Host: www.ashthailand.or.th
Connection: Keep-alive
```

Recommendation

Apply context-dependent encoding and/or validation to user input rendered on a page

References

Cross-site Scripting (XSS) Attack - Acunetix
https://www.acunetix.com/websitesecurity/cross-site-scripting/

Types of XSS - Acunetix
https://www.acunetix.com/websitesecurity/xss/

XSS Filter Evasion Cheat Sheet
https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet

Excess XSS, a comprehensive tutorial on cross-site scripting
https://excess-xss.com/

Cross site scripting
https://en.wikipedia.org/wiki/Cross-site_scripting

A8 Insecure Deserialization

Insecure deserialization often leads to remote code execution. Even if deserialization flaws do not result in remote code execution, they can be used to perform attacks, including replay attacks, injection attacks, and privilege escalation attacks.

No alerts in this category

A9 Using Components with Known Vulnerabilities

Components, such as libraries, frameworks, and other software modules, almost always run with full privileges. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications using components with known vulnerabilities may undermine application defenses and enable a range of possible attacks and impacts.

HTTP Strict Transport Security (HSTS) Policy Not Enabled

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.

CWE
CWE-16

CVSS2
AV:N/AC:L/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

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	None
Integrity Impact	None
Availability Impact	None

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	Active
Confidentiality Impact to the Vulnerable System	None
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

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

https://www.ashthailand.or.th/

URLs where HSTS is not enabled:

- https://www.ashthailand.or.th/

- https://www.ashthailand.or.th/admin/

Request

```
GET / HTTP/1.1
Referer: https://www.ashthailand.or.th/
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/119.0.0.0 Safari/537.36
Host: www.ashthailand.or.th
Connection: Keep-alive
```

Recommendation

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

References

hstspreload.org
https://hstspreload.org/

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

SSL Certificate Is About To Expire

One of the TLS/SSL certificates used by your server is about to expire.

Once the certificate has expired, 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.

CWE
CWE-298

CVSS2
AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

CVSS3
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	None
Integrity Impact	Low
Availability Impact	None

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N

Base Score	6.9
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	None
Confidentiality Impact to the Vulnerable System	None
Integrity Impact to the Vulnerable System	Low
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

If an application server detects an expired certificate with a system it is communicating with, the application server may continue processing data as if nothing happened, or the connection may be abruptly terminated.

https://www.ashthailand.or.th/ Confidence: 100%

The TLS/SSL certificate (serial: 05b86f7417bc625694fbb6b89cf3d459d023) will expire in less than **60** days. The certificate validity period is from **Sat Dec 27 2025 17:34:01 GMT+0600 (Bangladesh Standard Time)** to **Fri Mar 27 2026 17:34:00 GMT+0600 (Bangladesh Standard Time)** (51 days left)

Recommendation

Contact your Certificate Authority to renew the SSL certificate.

Cookies Not Marked as Secure

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.

CWE
CWE-614

CVSS2
AV:N/AC:H/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	High
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

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	Low
Integrity Impact	None
Availability Impact	None

CVSS4
CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:A/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N

Base Score	2.1
Attack Vector	Network
Attack Complexity	High
Attack Requirements	None
Privileges Required	None
User Interaction	Active
Confidentiality Impact to the Vulnerable System	Low
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

Cookies could be sent over unencrypted channels.

https://www.ashthailand.or.th/ Verified

Cookies without Secure flag set:

- https://www.ashthailand.or.th/

```
Set-Cookie: ash_sessions=04uugs762832a6af4t6g8e9t2fg4lpd3; expires=Tue, 03-Feb-2026 18:42:34 GMT; Max-Age=7200; path=/;
HttpOnly
```

Request

```
GET / HTTP/1.1
Referer: https://www.ashthailand.or.th/
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/119.0.0.0 Safari/537.36
Host: www.ashthailand.or.th
Connection: Keep-alive
```

Recommendation

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

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.

CWE
CWE-284

CVSS2
AV:N/AC:L/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

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	None
Integrity Impact	None
Availability Impact	None

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	Active
Confidentiality Impact to the Vulnerable System	None
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

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

https://www.ashthailand.or.th/ Verified

List of cookies with missing, inconsistent or contradictory properties:

- https://www.ashthailand.or.th/

  Cookie was set with:

  ```
  Set-Cookie: ash_sessions=04uugs762832a6af4t6g8e9t2fg41pd3; expires=Tue, 03-Feb-2026 18:42:34 GMT; Max-Age=7200; path=/; HttpOnly
  ```

  This cookie has the following issues:

  ```
  - Cookie without SameSite attribute.
  When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It is therefore recommended to add a SameSite attribute with an appropriate value of either "Strict", "Lax", or "None".
  ```

Request

```
GET / HTTP/1.1
Referer: https://www.ashthailand.or.th/
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/119.0.0.0 Safari/537.36
Host: www.ashthailand.or.th
Connection: Keep-alive
```

Recommendation

Ensure that the cookies configuration complies with the applicable standards.

References

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

Securing cookies with cookie prefixes
https://www.sjoerdlangkemper.nl/2017/02/09/cookie-prefixes/

Cookies: HTTP State Management Mechanism

https://tools.ietf.org/html/draft-ietf-httpbis-rfc6265bis-05
SameSite Updates - The Chromium Projects
https://www.chromium.org/updates/same-site

draft-west-first-party-cookies-07: Same-site Cookies
https://tools.ietf.org/html/draft-west-first-party-cookies-07

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.

CWE
CWE-1021

CVSS2
AV:N/AC:L/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

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	None
Integrity Impact	None
Availability Impact	None

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	Active
Confidentiality Impact to the Vulnerable System	None
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

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://www.ashthailand.or.th/

Paths without CSP header:

- https://www.ashthailand.or.th/
- https://www.ashthailand.or.th/admin/

Request

```
GET / HTTP/1.1
Referer: https://www.ashthailand.or.th/
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/119.0.0.0 Safari/537.36
Host: www.ashthailand.or.th
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/

Permissions-Policy header not implemented

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

CWE
CWE-1021

CVSS2
AV:N/AC:L/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

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	None
Integrity Impact	None
Availability Impact	None

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	Active
Confidentiality Impact to the Vulnerable System	None
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

https://www.ashthailand.or.th/

Locations without Permissions-Policy header:

- https://www.ashthailand.or.th/
- https://www.ashthailand.or.th/admin/

Request

```
GET / HTTP/1.1
Referer: https://www.ashthailand.or.th/
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/119.0.0.0 Safari/537.36
Host: www.ashthailand.or.th
Connection: Keep-alive
```

References

Permissions-Policy / Feature-Policy (MDN)
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Feature-Policy

Permissions Policy (W3C)
https://www.w3.org/TR/permissions-policy-1/

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.

CWE
CWE-16

CVSS2
AV:N/AC:L/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS3
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	None
Confidentiality Impact to the Vulnerable System	None
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

No impact is associated with this vulnerability.

https://www.ashthailand.or.th/

Detected reverse proxy: Apache httpd

Request

```
GET / HTTP/1.1
Max-Forwards: 0
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/119.0.0.0 Safari/537.36
Host: www.ashthailand.or.th
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.

CWE
CWE-830

CVSS2
AV:N/AC:L/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS3
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Changed
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N

Base Score	6.9
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	None
Confidentiality Impact to the Vulnerable System	None
Integrity Impact to the Vulnerable System	Low
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

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

https://www.ashthailand.or.th/

Pages where SRI is not implemented:

- https://www.ashthailand.or.th/
  Script SRC: **https://cdn.jsdelivr.net/npm/select2@4.1.0-rc.0/dist/js/select2.min.js**

- https://www.ashthailand.or.th/
  Script SRC: **https://www.statcounter.com/counter/counter.js**

Request

```
GET / HTTP/1.1
Referer: https://www.ashthailand.or.th/
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/119.0.0.0 Safari/537.36
Host: www.ashthailand.or.th
Connection: Keep-alive
```

https://www.ashthailand.or.th/admin/

Pages where SRI is not implemented:

- https://www.ashthailand.or.th/admin/
  Script SRC: **https://www.google.com/recaptcha/api.js**

Request

```
GET /admin/ HTTP/1.1
Referer: https://www.ashthailand.or.th/
Cookie: ash_sessions=q393lt0lic4gnhhd5ac5kd763sot33d3; sc_is_visitor_unique=rx9500380.1770137330.FD71672D9B7F42069CA191F8C0C79A4B.1.1.1.1.1.1.1.1.1
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/119.0.0.0 Safari/537.36
Host: www.ashthailand.or.th
Connection: Keep-alive
```

Recommendation

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

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

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

Vulnerable JavaScript libraries

You are using one or more vulnerable JavaScript libraries. One or more vulnerabilities were reported for this version of the library. Consult Attack details and Web References for more information about the affected library and the vulnerabilities that were reported.

CWE
CWE-937

CVSS2
AV:N/AC:L/Au:N/C:P/I:P/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	Partial
Availability Impact	None

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	Low
Integrity Impact	Low
Availability Impact	None

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N

Base Score	6.9
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	None
Confidentiality Impact to the Vulnerable System	Low
Integrity Impact to the Vulnerable System	Low
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

Consult References for more information.

https://www.ashthailand.or.th/ Confidence: 95%

- **jQuery 3.2.1 -ajax,-ajax/jsonp,-ajax/load,-ajax/parseXML,-ajax/script,-ajax/var/location,-ajax/var/nonce,-ajax/var/rquery,-ajax/xhr,-manipulation/_evalUrl,-event/ajax,-effects,-effects/Tween,-effects/animatedSelector**
  - URL: https://www.ashthailand.or.th/
  - Detection method: The library's name and version were determined based on its dynamic behavior.
  - CVE-ID: CVE-2020-11022, CVE-2020-11023, CVE-2019-11358
  - Description: In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0. / In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing option elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0. / jQuery mishandles jQuery.extend(true, {}, ...) because of Object.prototype pollution. If an unsanitized source object contained an enumerable __proto__ property, it could extend the native Object.prototype.
  - References:
    - https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/
    - https://mksben.l0.cm/2020/05/jquery3.5.0-xss.html
    - https://jquery.com/upgrade-guide/3.5/

- https://api.jquery.com/jQuery.htmlPrefilter/
- https://www.cvedetails.com/cve/CVE-2020-11022/
- https://github.com/advisories/GHSA-gxr4-xjj5-5px2
- https://www.cvedetails.com/cve/CVE-2020-11023/
- https://github.com/advisories/GHSA-jpcq-cgw6-v4j6
- https://github.com/jquery/jquery/pull/4333
- https://nvd.nist.gov/vuln/detail/CVE-2019-11358
- https://nvd.nist.gov/vuln/detail/CVE-2019-5428
- https://blog.jquery.com/2019/04/10/jquery-3-4-0-released/

Request

```
GET / HTTP/1.1
Referer: https://www.ashthailand.or.th/
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/119.0.0.0 Safari/537.36
Host: www.ashthailand.or.th
Connection: Keep-alive
```

Recommendation

Upgrade to the latest version.

Outdated JavaScript libraries

You are using an outdated version of one or more JavaScript libraries. A more recent version is available. Although your version was not found to be affected by any security vulnerabilities, it is recommended to keep libraries up to date.

CWE

CWE-937

CVSS2

AV:N/AC:H/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	High
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:N/I:N/A:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	High
Privileges Required	None
User Interaction	Required
Scope	Changed
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS4

CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	High
Attack Requirements	None
Privileges Required	None
User Interaction	Active
Confidentiality Impact to the Vulnerable System	None
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

Consult References for more information.

https://www.ashthailand.or.th/ Confidence: 95%

- bootstrap.js 4.0.0
  - URL: https://www.ashthailand.or.th/
  - Detection method: The library's name and version were determined based on its dynamic behavior.
  - References:
    - https://github.com/twbs/bootstrap/releases

Request

```
GET / HTTP/1.1
Referer: https://www.ashthailand.or.th/
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/119.0.0.0 Safari/537.36
Host: www.ashthailand.or.th
Connection: Keep-alive
```

Recommendation

Upgrade to the latest version.

A10 Insufficient Logging and Monitoring

Insufficient logging and monitoring, coupled with missing or ineffective integration with incident response, allows attackers to further attack systesm, maintain persistence, pivot to more systems, and tamper, extract, or destroy data. Most breach studies show time to detect a breach is over 200 days, typically detected by external parties rathre than inernal processes or monitoring.

No alerts in this category

Coverage

- https://www.ashthailand.or.th
  - about
    - detail
      - 823
        - 13
  - admin
    - user
      - login
  - assets
    - bootstrap
      - dist
        - css
          - bootstrap.min.css
        - js
          - bootstrap.min.js
    - fonts
      - fontawesome
        - css
          - brands.css
          - fontawesome.css
          - solid.css
    - js
      - datatable
        - datatable.min.css
        - datatable.min.js
      - OwlCarousel2-2.3.4
        - dist
          - assets
            - owl.carousel.min.css
            - owl.theme.default.min.css
          - owl.carousel.min.js
      - jquery.js
    - theme
      - theme.css
    - custom.css
    - responsive.css
  - content
    - cat
      - 1
      - 10
      - 11
      - 2
      - 4
      - 5
      - 6
      - 7
      - 9


lists
2
8
gis
home
cat
1
10
11
4
5
6
7
9
lists
2
8
gis
html
dist
css
adminlte.min.css
js
adminlte.min.js
plugins
bootstrap
js
bootstrap.bundle.min.js
fontawesome-free
css
all.min.css
icheck-bootstrap
icheck-bootstrap.min.css
jquery
jquery.min.js
index2.html
images
logo
news
detail
643
10
4
uploads
banner
iconHome
spon
.gitignore

about
composer.json
contact
home
license.txt
news
search