Acunetix
by Invicti

Developer Report

Acunetix Security Audit

2024-02-15

Generated by Acunetix

Scan of ap.tnnua.edu.tw

Scan details

Scan information	
Start time	2024-02-15T00:12:46.204057+08:00
Start url	https://ap.tnnua.edu.tw/enrolldept/
Host	ap.tnnua.edu.tw
Scan time	2 minutes, 42 seconds
Profile	Full Scan
Responsive	True
Server OS	Windows
Server technologies	ASP.NET
Application build	24.1.240131143

Threat level

Acunetix Threat Level 2

One or more medium-severity type vulnerabilities have been discovered by the scanner. You should investigate each of these vulnerabilities to ensure they will not escalate to more severe problems.

Alerts distribution

Total alerts found	5
Critical	0
High	0
Medium	2
Low	1
Informational	2

Alerts summary

HTTP Strict Transport Security (HSTS) Policy Not Enabled

Classification	
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 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
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

Unencrypted __VIEWSTATE parameter

Classification

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 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
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: 6.4 Access Vector: Network_accessible Access Complexity: Low 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-200

Affected items	Variation
Web Server	1

Cookies Not Marked as Secure

Classification

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 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
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

Content Security Policy (CSP) Not Implemented

Classification

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 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
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

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 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
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

HTTP Strict Transport Security (HSTS) Policy Not Enabled

Severity	**Medium**
Reported by module	/httpdata/HSTS_not_implemented.js

Description

HTTP Strict Transport Security (HSTS) tells a browser that a web site is only accessable using HTTPS. It was detected that your web application doesn't implement HTTP Strict Transport Security (HSTS) as the Strict Transport Security header is missing from the response.

Impact

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

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)

Affected items

Web Server

Details

URLs where HSTS is not enabled:

- https://ap.tnnua.edu.tw/enrolldept/
- https://ap.tnnua.edu.tw/enrolldept/login.aspx

Request headers

```
GET /enrolldept/ HTTP/1.1

Referer: https://ap.tnnua.edu.tw/enrolldept/

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: ap.tnnua.edu.tw

Connection: Keep-alive
```

Unencrypted __VIEWSTATE parameter

Severity	**Medium**
Reported by module	/RPA/Unencrypted_VIEWSTATE.js

Description

The __VIEWSTATE parameter is not encrypted for one or more pages. To reduce the chance of someone intercepting the information stored in the ViewState, it is good design to encrypt the ViewState.

Impact

Possible sensitive information disclosure.

Recommendation

Turn on the encryption mode for the view state. Consult web references for more information, taking into consideration ASP.NET version

References

Page.ViewStateEncryptionMode Property (https://docs.microsoft.com/en-us/dotnet/api/system.web.ui.page.viewstateencryptionmode?redirectedfrom=MSDN&view=netframework-4.7.2)
Cryptographic Improvements in ASP.NET 4.5, pt. 2 (https://devblogs.microsoft.com/aspnet/cryptographic-improvements-in-asp-net-4-5-pt-2/)
Working with ViewState (http://appetere.com/post/working-with-viewstate)

Affected items

Web Server
Details

Pages with unencrypted __VIEWSTATE parameter:

- https://ap.tnnua.edu.tw/enrolldept/
  Strings extracted(truncated):

```
167312573

Visiblehddd
```

- https://ap.tnnua.edu.tw/enrolldept/
  Strings extracted(truncated):

```
167312573

Visiblehdd

Texteddd
```

- https://ap.tnnua.edu.tw/enrolldept/login.aspx
  Strings extracted(truncated):

```
167312573

Visiblehddd
```

Request headers

```
GET /enrolldept/ HTTP/1.1

Referer: https://ap.tnnua.edu.tw/enrolldept/

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: ap.tnnua.edu.tw

Connection: Keep-alive
```

Cookies Not Marked as Secure

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://ap.tnnua.edu.tw/enrolldept/

```
Set-Cookie: ASP.NET_SessionId=fdiqkxwxwtjqzzabmshywb2f; path=/; HttpOnly; SameSite=La
```

Request headers

```
GET /enrolldept/ HTTP/1.1

Referer: https://ap.tnnua.edu.tw/enrolldept/

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: ap.tnnua.edu.tw

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

Affected items

Web Server
Details
Paths without CSP header: • https://ap.tnnua.edu.tw/enrolldept/ • https://ap.tnnua.edu.tw/enrolldept/login.aspx
Request headers

```
GET /enrolldept/ HTTP/1.1

Referer: https://ap.tnnua.edu.tw/enrolldept/

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: ap.tnnua.edu.tw

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

Affected items

Web Server
Details

Locations without Permissions-Policy header:

- https://ap.tnnua.edu.tw/enrolldept/
- https://ap.tnnua.edu.tw/enrolldept/image/
- https://ap.tnnua.edu.tw/enrolldept/login.aspx
- https://ap.tnnua.edu.tw/enrolldept/script/
- https://ap.tnnua.edu.tw/enrolldept/Style/

Request headers

```
GET /enrolldept/ HTTP/1.1

Referer: https://ap.tnnua.edu.tw/enrolldept/

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: ap.tnnua.edu.tw

Connection: Keep-alive
```

Scanned items (coverage report)

https://ap.tnnua.edu.tw/
https://ap.tnnua.edu.tw/enrolldept/
https://ap.tnnua.edu.tw/enrolldept/image/
https://ap.tnnua.edu.tw/enrolldept/login.aspx
https://ap.tnnua.edu.tw/enrolldept/script/
https://ap.tnnua.edu.tw/enrolldept/Style/
https://ap.tnnua.edu.tw/enrolldept/Style/Default.css