Acunetix
by Invicti

Developer Report

Acunetix Security Audit

2023-02-16

Generated by Acunetix

Scan of acad.hhsh.tn.edu.tw

Scan details

Scan information	
Start time	2023-02-16T00:05:49.198612+08:00
Start url	https://acad.hhsh.tn.edu.tw/
Host	acad.hhsh.tn.edu.tw
Scan time	2 minutes, 54 seconds
Profile	Full Scan
Server information	Microsoft-IIS/7.5
Responsive	True
Server OS	Windows
Server technologies	ASP.NET
Application build	15.2.221208162

Threat level

Acunetix Threat Level 1

One or more low-severity type vulnerabilities have been discovered by the scanner.

Alerts distribution

Total alerts found	8
High	0
Medium	0
Low	3
Informational	5

Alerts summary

ASP.NET version disclosure

Classification	
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 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-200

Affected items	Variation
Web Server	1

Clickjacking: X-Frame-Options header

Classification	
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 Impact: None Integrity Impact: Low Availability Impact: None

CVSS2	Base Score: 4.3 Access Vector: Network_accessible Access Complexity: Medium Authentication: None Confidentiality Impact: None 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-1021

Affected items	Variation
Web Server	1

HTTP Strict Transport Security (HSTS) not implemented

Classification	
CVSS3	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:N/A:N Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Required Scope: Changed Confidentiality Impact: None Integrity Impact: None Availability Impact: None
CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-16

Affected items	Variation
Web Server	1

Content Security Policy (CSP) not implemented

Classification

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

Affected items	Variation
Web Server	1

ⓘ Microsoft IIS version disclosure

Classification	
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 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-200

Affected items	Variation
Web Server	1

Permissions-Policy header not implemented

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

Affected items	Variation
Web Server	1

TLS/SSL (EC)DHE Key Reuse

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

CVSS2	Base Score: 1.9 Access Vector: Local_access Access Complexity: Medium Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-310

Affected items	Variation
Web Server	1

ⓘ Web server default welcome page

Classification	
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 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-200

Affected items	Variation
Web Server	1

Alerts details

ASP.NET version disclosure

Severity	**Low**
Reported by module	/Scripts/PerServer/ASP_NET_Error_Message.script

Description

The HTTP responses returned by this web application include anheader named **X-AspNet-Version**. The value of this header is used by Visual Studio to determine which version of ASP.NET is in use. It is not necessary for production sites and should be disabled.

Impact

The HTTP header may disclose sensitive information. This information can be used to launch further attacks.

Recommendation

Apply the following changes to the web.config file to prevent ASP.NET version disclosure:

```
<System.Web>

 <httpRuntime enableVersionHeader="false" />

</System.Web>
```

References

HttpRuntimeSection.EnableVersionHeader Property (https://docs.microsoft.com/en-us/dotnet/api/system.web.configuration.httpruntimesection.enableversionheader?redirectedfrom=MSDN&view=netframework-4.8#System_Web_Configuration_HttpRuntimeSection_EnableVersionHeader)

Affected items

Web Server

Details

Version information found:

```
2.0.50727
```

Request headers

```
GET /|~.aspx HTTP/1.1

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

Accept-Encoding: gzip,deflate,br

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

Host: acad.hhsh.tn.edu.tw

Connection: Keep-alive
```

Clickjacking: X-Frame-Options header

Severity	**Low**
Reported by module	/httpdata/X_Frame_Options_not_implemented.js

Description

Clickjacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages.

The server did not return an **X-Frame-Options** header with the value DENY or SAMEORIGIN, which means that this website could be at risk of a clickjacking attack. The X-Frame-Options HTTP response header can be used to indicate whether or not a browser should be allowed to render a page inside a frame or iframe. Sites can use this to avoid clickjacking attacks, by ensuring that their content is not embedded into untrusted sites.

Impact

The impact depends on the affected web application.

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)

Affected items

Web Server
Details
Paths without secure XFO header: • https://acad.hhsh.tn.edu.tw/

Request headers

```
GET / HTTP/1.1

Referer: https://acad.hhsh.tn.edu.tw/

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

Accept-Encoding: gzip,deflate,br

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

Host: acad.hhsh.tn.edu.tw

Connection: Keep-alive
```

HTTP Strict Transport Security (HSTS) not implemented

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

Description

HTTP Strict Transport Security (HSTS) tells a browser that a web site is only 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://acad.hhsh.tn.edu.tw/

Request headers

```
GET / HTTP/1.1

Referer: https://acad.hhsh.tn.edu.tw/

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

Accept-Encoding: gzip,deflate,br

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

Host: acad.hhsh.tn.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)(https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP)
[Implementing Content Security Policy](https://hacks.mozilla.org/2016/02/implementing-content-security-policy/)(https://hacks.mozilla.org/2016/02/implementing-content-security-policy/)

Affected items

Web Server

Details

Paths without CSP header:

- https://acad.hhsh.tn.edu.tw/

Request headers

```
GET / HTTP/1.1

Referer: https://acad.hhsh.tn.edu.tw/

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

Accept-Encoding: gzip,deflate,br

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

Host: acad.hhsh.tn.edu.tw

Connection: Keep-alive
```

Microsoft IIS version disclosure

Severity	**Informational**
Reported by module	/Scripts/PerServer/ASP_NET_Error_Message.script

Description

The HTTP responses returned by this web application include a header named **Server**. The value of this header includes the version of Microsoft IIS server.

Impact

The HTTP header may disclose sensitive information. This information can be used to launch further attacks.

Recommendation

Microsoft IIS should be configured to remove unwanted HTTP response headers from the response. Consult web references for more information.

References

[Remove Unwanted HTTP Response Headers](https://blogs.msdn.microsoft.com/varunm/2013/04/23/remove-unwanted-http-response-headers/)(https://blogs.msdn.microsoft.com/varunm/2013/04/23/remove-unwanted-http-response-headers/)

Affected items

Web Server

Details

Version information found:

```
Microsoft-IIS/7.5
```

Request headers

```
GET /|~.aspx HTTP/1.1

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

Accept-Encoding: gzip,deflate,br

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

Host: acad.hhsh.tn.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://acad.hhsh.tn.edu.tw/

Request headers

```
GET / HTTP/1.1

Referer: https://acad.hhsh.tn.edu.tw/

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

Accept-Encoding: gzip,deflate,br

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

Host: acad.hhsh.tn.edu.tw

Connection: Keep-alive
```

TLS/SSL (EC)DHE Key Reuse

Severity	**Informational**
Reported by module	/Scripts/PerServer/SSL_Audit.script

Description

The remote host reuses Diffie-Hellman Ephemeral public server keys with (EC)DHE cipher suites.

Impact

Recommendation

Reconfigure the affected application to always generate new keys when using tmp_dh/tmp_ecdh parameters.

References

Raccoon Attack (https://raccoon-attack.com/)
Raccoon Attack (Technical Paper, PDF) (https://raccoon-attack.com/RacoonAttack.pdf)
Logjam Attack (https://weakdh.org/)
Logjam Attack (Technical Paper, PDF) (https://weakdh.org/imperfect-forward-secrecy-ccs15.pdf)
List of SSL OP Flags (see: SSL_OP_SINGLE_DH_USE, SSL_OP_SINGLE_ECDH_USE)
(https://wiki.openssl.org/index.php/List_of_SSL_OP_Flags)

Affected items

Web Server

Details

Diffie-Hellman Public Key Reuse:

- ECDHE public server key reuse: 04 00 86 04 2b 54 9b d9 bf 9f 14 35 40 25 d0 13 18 70 da 77 c3 06 de 2f 7c be 0b 1a 2e bd 19 44 88 04 e9 fe ae 97 1d 71 07 b3 5e 29 40 cd 84 7a fe 6d 3d 9f 5f 3c 4d 60 21 5b 16 1f 5e 70 3d af be 4e 6c 01 dc c0 24 1a 56 07 14 24 78 19 15 2e 0c 27 e5 84 96 8c 9f 50 cb 04 1f 1b a5 2b 36 a8 22 05 4f e0 fe d3 50 c5 44 32 50 a0 d6 3d 9b 21 56 44 f7 da dc cf 97 bc 12 64 71 59 95 c4 91 a3 ea af 40 5c 97 (with TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384)

Request headers

ⓘ Web server default welcome page

Severity	**Informational**
Reported by module	/Scripts/PerServer/Web_Server_Default_Welcome_Page.script

Description

This web server has a default welcome page. If you are not using this web server, it should be disabled because it may pose a security threat.

Impact

No impact is associated with this vulnerability.

Recommendation

If this server is not used, it is recommended to disable it.

References

[Web Server Default Welcome Page](https://www.thesitewizard.com/apache/change-default-page-for-domain.shtml)(https://www.thesitewizard.com/apache/change-default-page-for-domain.shtml)

Affected items

Web Server

Details

Request headers

```
GET / HTTP/1.1

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

Accept-Encoding: gzip,deflate,br

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

Host: acad.hhsh.tn.edu.tw

Connection: Keep-alive
```

Scanned items (coverage report)

https://acad.hhsh.tn.edu.tw/