Acunetix
by Invicti

Affected Items Report

Acunetix Security Audit

2024-11-27

Generated by Acunetix

Scan of carbonplat.ftis.org.tw

Scan details

Scan information	
Start time	2024-11-25T14:01:05.765096+08:00
Start url	https://carbonplat.ftis.org.tw/
Host	carbonplat.ftis.org.tw
Scan time	39 minutes, 56 seconds
Profile	Full Scan
Server information	Microsoft-IIS/10.0
Responsive	True
Server OS	Windows
Application build	24.10.241106172

Threat level

Acunetix Threat Level 0

No vulnerabilities have been discovered by the scanner.

Alerts distribution

Total alerts found	8
Critical	0
High	0
Medium	0
Low	0
Informational	8

Affected items

Web Server	
Alert group	**An Unsafe Content Security Policy (CSP) Directive in Use (verified)**
Severity	Informational
Description	Acunetix evaluated the scan target's Content Security Policies, checked for misconfigurations and potentially unintended side-effects of otherwise valid configurations, and offers the following suggestions on how to change existing policies for improved security and maximum compatibility.
Recommendations	See alert details for available remediation advice.
Alert variants	
Details	• **An Unsafe Content Security Policy (CSP) Directive in Use** ◦ **First observed on:** https://carbonplat.ftis.org.tw/ ◦ **CSP Value:** default-src 'self'; script-src 'self' 'unsafe-inline'; style-src 'self' 'unsafe-inline'; frame-src 'self'; frame-ancestors 'self'; ◦ **CSP Source:** header ◦ **Summary:** Acunetix detected that one of following CSP directives is used: unsafe-eval, unsafe-inline. By using unsafe-eval, you allow the use of string evaluation functions like eval. By using unsafe-inline, you allow the execution of inline scripts, which almost defeats the purpose of CSP. When this is allowed, it's very easy to successfully exploit a Cross-site Scripting vulnerability on your website. ◦ **Impact:** An attacker can bypass CSP and exploit a Cross-site Scripting vulnerability successfully. ◦ **Remediation:** If possible remove unsafe-eval and unsafe-inline from your CSP directives. ◦ **References:** ▪ N/A

```
GET / HTTP/1.1

Referer: https://carbonplat.ftis.org.tw/

Cookie: 123=1ba4bebc-78af-4d4b-8d3f-4907a41913ff

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/126.0.0.0 Safari/537.36

Host: carbonplat.ftis.org.tw

Connection: Keep-alive
```

Web Server	
Alert group	**default-src Used in Content Security Policy (CSP) (verified)**
Severity	Informational

Description	Acunetix evaluated the scan target's Content Security Policies, checked for misconfigurations and potentially unintended side-effects of otherwise valid configurations, and offers the following suggestions on how to change existing policies for improved security and maximum compatibility.
Recommendations	See alert details for available remediation advice.
Alert variants	
Details	• **default-src Used in Content Security Policy (CSP)** ◦ **First observed on:** https://carbonplat.ftis.org.tw/ ◦ **CSP Value:** default-src 'self'; script-src 'self' 'unsafe-inline'; style-src 'self' 'unsafe-inline'; frame-src 'self'; frame-ancestors 'self'; ◦ **CSP Source:** header ◦ **Summary:** Acunetix detected that you used default-src in CSP directive. It is important to know that default-src cannot be used as a fallback for the functions below: base-uri, form-action, frame-ancestors, plugin-types, report-uri, sandbox ◦ **Impact:** N/A ◦ **Remediation:** N/A ◦ **References:** ▪ N/A

```
GET / HTTP/1.1

Referer: https://carbonplat.ftis.org.tw/

Cookie: 123=1ba4bebc-78af-4d4b-8d3f-4907a41913ff

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/126.0.0.0 Safari/537.36

Host: carbonplat.ftis.org.tw

Connection: Keep-alive
```

Web Server	
Alert group	**Javascript Source map detected**
Severity	Informational
Description	Client side Javascript source code can be combined, minified or compiled. A source map is a file that maps from the transformed source to the original source. Source map may help an attacker to read and debug Javascript.
Recommendations	According to the best practices, source maps should not be accesible for an attacker. Consult web references for more information
Alert variants	

Details	URLs where links to SourceMaps were found: • sourceMappingURL in JS body - https://carbonplat.ftis.org.tw/Scripts/Dou/datetimepicker/js/moment.js • sourceMappingURL in JS body - https://carbonplat.ftis.org.tw/Scripts/bootstrap.bundle.js • sourceMappingURL in JS body - https://carbonplat.ftis.org.tw/Scripts/bootstrap.bundle.min.js • sourceMappingURL in JS body - https://carbonplat.ftis.org.tw/Scripts/bootstrap.js

```
GET /Scripts/Dou/datetimepicker/js/moment.js HTTP/1.1

Referer: https://carbonplat.ftis.org.tw/User/DouLogin

Cookie: 123=1ba4bebc-78af-4d4b-8d3f-4907a41913ff

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/126.0.0.0 Safari/537.36

Host: carbonplat.ftis.org.tw

Connection: Keep-alive
```

Web Server	
Alert group	**Outdated JavaScript libraries**
Severity	Informational
Description	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.
Recommendations	Upgrade to the latest version.
Alert variants	

Details	• **html5shiv 3.7.0**
	  ◦ URL: https://carbonplat.ftis.org.tw/User/DouLogin
	  ◦ Detection method: The library's name and version were determined based on its dynamic behavior.
	  ◦ References:
	  ▪ https://github.com/aFarkas/html5shiv/tags

```
GET /User/DouLogin?redirectLogin=true&returnUrl=/ HTTP/1.1

Referer: https://carbonplat.ftis.org.tw/

Cookie: 123=1ba4bebc-78af-4d4b-8d3f-4907a41913ff

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/126.0.0.0 Safari/537.36

Host: carbonplat.ftis.org.tw

Connection: Keep-alive
```

Web Server	
Alert group	**Outdated JavaScript libraries**
Severity	Informational
Description	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.
Recommendations	Upgrade to the latest version.
Alert variants	
Details	• **Modernizr 2.8.3** ◦ URL: https://carbonplat.ftis.org.tw/User/DouLogin ◦ Detection method: The library's name and version were determined based on its dynamic behavior. ◦ References: ▪ https://github.com/Modernizr/Modernizr/releases

```
GET /User/DouLogin?redirectLogin=true&returnUrl=/ HTTP/1.1

Referer: https://carbonplat.ftis.org.tw/

Cookie: 123=1ba4bebc-78af-4d4b-8d3f-4907a41913ff

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/126.0.0.0 Safari/537.36

Host: carbonplat.ftis.org.tw

Connection: Keep-alive
```

Web Server	

Alert group	Permissions-Policy header not implemented
Severity	Informational
Description	The Permissions-Policy header allows developers to selectively enable and disable use of various browser features and APIs.
Recommendations	
Alert variants	
Details	Locations without Permissions-Policy header: • https://carbonplat.ftis.org.tw/User/DouLogin • https://carbonplat.ftis.org.tw/home

```
GET /User/DouLogin?redirectLogin=true&returnUrl=/ HTTP/1.1

Referer: https://carbonplat.ftis.org.tw/

Cookie: 123=1ba4bebc-78af-4d4b-8d3f-4907a41913ff

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/126.0.0.0 Safari/537.36

Host: carbonplat.ftis.org.tw

Connection: Keep-alive
```

Web Server	
Alert group	**Subresource Integrity (SRI) Not Implemented**
Severity	Informational
Description	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.

Recommendations	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/uxy9rx7HN crossorigin="anonymous"></script>`
Alert variants	
Details	Pages where SRI is not implemented: • https://carbonplat.ftis.org.tw/User/DouLogin Script SRC: **https://cdn.jsdelivr.net/npm/bootstrap@5.3.0-alpha1/dist/js/bootstrap.bundle.min.js**

```
GET /User/DouLogin?redirectLogin=true&returnUrl=/ HTTP/1.1

Referer: https://carbonplat.ftis.org.tw/

Cookie: 123=1ba4bebc-78af-4d4b-8d3f-4907a41913ff

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/126.0.0.0 Safari/537.36

Host: carbonplat.ftis.org.tw

Connection: Keep-alive
```

Web Server	
Alert group	**Version Disclosure (IIS)**
Severity	Informational
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.
Recommendations	Microsoft IIS should be configured to remove unwanted HTTP response headers from the response. Consult web references for more information.
Alert variants	
Details	Version information found: `Microsoft-IIS/10.0`

```
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/126.0.0.0 Safari/537.36

Host: carbonplat.ftis.org.tw

Connection: Keep-alive
```

Scanned items (coverage report)

https://carbonplat.ftis.org.tw/
https://carbonplat.ftis.org.tw/Content/
https://carbonplat.ftis.org.tw/Content/bootstrap.css
https://carbonplat.ftis.org.tw/Content/prj/
https://carbonplat.ftis.org.tw/Content/prj/site.css
https://carbonplat.ftis.org.tw/Content/site.css
https://carbonplat.ftis.org.tw/CounselingRecord/
https://carbonplat.ftis.org.tw/CounselingRecord/Index
https://carbonplat.ftis.org.tw/FactoryBasic/
https://carbonplat.ftis.org.tw/FactoryBasic/Index
https://carbonplat.ftis.org.tw/home
https://carbonplat.ftis.org.tw/image/
https://carbonplat.ftis.org.tw/images/
https://carbonplat.ftis.org.tw/Scripts/
https://carbonplat.ftis.org.tw/Scripts/bootstrap.bundle.js
https://carbonplat.ftis.org.tw/Scripts/bootstrap.bundle.min.js
https://carbonplat.ftis.org.tw/Scripts/bootstrap.js
https://carbonplat.ftis.org.tw/Scripts/Dou/
https://carbonplat.ftis.org.tw/Scripts/Dou/datetimepicker/
https://carbonplat.ftis.org.tw/Scripts/Dou/datetimepicker/css/
https://carbonplat.ftis.org.tw/Scripts/Dou/datetimepicker/css/bootstrap-datetimepicker.css
https://carbonplat.ftis.org.tw/Scripts/Dou/datetimepicker/js/
https://carbonplat.ftis.org.tw/Scripts/Dou/datetimepicker/js/moment.js
https://carbonplat.ftis.org.tw/Scripts/Dou/datetimepicker/js/tempusdominus-bootstrap-4.min.js
https://carbonplat.ftis.org.tw/Scripts/Dou/Dou.css
https://carbonplat.ftis.org.tw/Scripts/Dou/Dou.js
https://carbonplat.ftis.org.tw/Scripts/gis/
https://carbonplat.ftis.org.tw/Scripts/gis/b3/
https://carbonplat.ftis.org.tw/Scripts/gis/b3/css/
https://carbonplat.ftis.org.tw/Scripts/gis/b3/css/bootstrap.css
https://carbonplat.ftis.org.tw/Scripts/gis/b3/fonts/
https://carbonplat.ftis.org.tw/Scripts/gis/bootstraptable/
https://carbonplat.ftis.org.tw/Scripts/gis/bootstraptable/bootstrap-table.css
https://carbonplat.ftis.org.tw/Scripts/gis/bootstraptable/bootstrap-table.js
https://carbonplat.ftis.org.tw/Scripts/gis/bootstraptable/extensions/
https://carbonplat.ftis.org.tw/Scripts/gis/bootstraptable/extensions/export/
https://carbonplat.ftis.org.tw/Scripts/gis/bootstraptable/extensions/mobile/
https://carbonplat.ftis.org.tw/Scripts/gis/bootstraptable/extensions/mobile/bootstrap-table-mobile.js
https://carbonplat.ftis.org.tw/Scripts/gis/bootstraptable/themes/
https://carbonplat.ftis.org.tw/Scripts/gis/helper.js
https://carbonplat.ftis.org.tw/Scripts/gis/images/
https://carbonplat.ftis.org.tw/Scripts/gis/Main.css
https://carbonplat.ftis.org.tw/Scripts/gis/Main.js
https://carbonplat.ftis.org.tw/Scripts/gis/select/
https://carbonplat.ftis.org.tw/Scripts/gis/select/bselect/
https://carbonplat.ftis.org.tw/Scripts/gis/select/bselect/bootstrap-select.min.css
https://carbonplat.ftis.org.tw/Scripts/jquery-3.6.0.js
https://carbonplat.ftis.org.tw/Scripts/modernizr-2.8.3.js
https://carbonplat.ftis.org.tw/Scripts/src/
https://carbonplat.ftis.org.tw/User/
https://carbonplat.ftis.org.tw/User/DouLogin