Acunetix
by Invicti

Affected Items Report

Acunetix Security Audit

2024-11-27

Generated by Acunetix

Scan of pj.ftis.org.tw

Scan details

Scan information	
Start time	2024-11-25T14:02:00.348041+08:00
Start url	https://pj.ftis.org.tw/CFCv2/
Host	pj.ftis.org.tw
Scan time	18 minutes, 57 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	6
Critical	0
High	0
Medium	0
Low	0
Informational	6

Affected items

Web Server	
Alert group	**Access-Control-Allow-Origin header with wildcard (*) value**
Severity	Informational
Description	Cross-origin resource sharing (CORS) is a mechanism that allows restricted resources (e.g. fonts) on a web page to be requested from another domain outside the domain from which the resource originated. The Access-Control-Allow-Origin header indicates whether a resource can be shared based on the value of the Origin request header, "*", or "null" in the response. If a website responds with Access-Control-Allow-Origin: * the requested resource allows sharing with every origin. Therefore, any website can make XHR (XMLHTTPRequest) requests to the site and access the responses.
Recommendations	Check whether Access-Control-Allow-Origin: * is appropriate for the resource/response.
Alert variants	
Details	Affected paths (max. 25): • /CFCv2/ • / • /CFCv2/CFC/CreateUser • /CFCv2/CFC/ • /CFCv2/Scripts/ • /CFCv2/CFC/GetCompanyProperties • /CFCv2/Content/ • /CFCv2/error.html • /CFCv2/CFC/Guest • /CFCv2/CFC/Login/guest • /CFCv2/CFC/Index • /CFCv2/Content/prj/images/ • /CFCv2/Images/ • /CFCv2/CFC/GetFactoriesByUser • /CFCv2/cfc/cal • /CFCv2/CFC/Logoff • /CFCv2/Content/font-awesome-4.7.0/fonts/ • /CFCv2/Content/prj/ • /CFCv2/CFC/Login/ • /CFCv2/Scripts/gis/bootstraptable/extensions/mobile/ • /CFCv2/Content/font-awesome-4.7.0/

```
GET /CFCv2/ HTTP/1.1

Referer: https://pj.ftis.org.tw/CFCv2/

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: pj.ftis.org.tw

Connection: Keep-alive
```

Web Server	
Alert group	**Content Security Policy (CSP) Not Implemented**
Severity	Informational

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.

Recommendations	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.
Alert variants	
Details	Paths without CSP header: • https://pj.ftis.org.tw/CFCv2/ • https://pj.ftis.org.tw/CFCv2/error.html • https://pj.ftis.org.tw/CFCv2/CFC/ • https://pj.ftis.org.tw/CFCv2/CFC/Index • https://pj.ftis.org.tw/CFCv2/CFC/Login/ • https://pj.ftis.org.tw/CFCv2/CFC/Login/guest

```
GET /CFCv2/ HTTP/1.1

Referer: https://pj.ftis.org.tw/CFCv2/

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: pj.ftis.org.tw

Connection: Keep-alive
```

Web Server	
Alert group	**Generic Email Address Disclosure**
Severity	Informational
Description	One or more email addresses have been found on this website. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.
Recommendations	Check references for details on how to solve this problem.
Alert variants	
Details	Emails found: • https://pj.ftis.org.tw/CFCv2/ **pol78917@ftis.org.tw** • https://pj.ftis.org.tw/CFCv2/CFC/ **pol78917@ftis.org.tw** • https://pj.ftis.org.tw/CFCv2/CFC/Index **pol78917@ftis.org.tw** • https://pj.ftis.org.tw/CFCv2/CFC/Login/ **pol78917@ftis.org.tw** • https://pj.ftis.org.tw/CFCv2/CFC/Login/guest **pol78917@ftis.org.tw**

```
GET /CFCv2/ HTTP/1.1

Referer: https://pj.ftis.org.tw/CFCv2/

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: pj.ftis.org.tw

Connection: Keep-alive
```

Web Server	
Alert group	**HTTP Strict Transport Security (HSTS) Errors and Warnings**
Severity	Informational
Description	HTTP Strict Transport Security (HSTS) instructs a web browser to only connect to a web site using HTTPS. It was detected that your web application's HTTP Strict Transport Security (HSTS) implementation is not as strict as is typically advisable.
Recommendations	It is recommended to implement best practices of HTTP Strict Transport Security (HSTS) in your web application. Consult web references for more information.
Alert variants	
Details	URLs where HSTS configuration is not according to best practices: • https://pj.ftis.org.tw/CFCv2/ - No includeSubDomains directive • https://pj.ftis.org.tw/CFCv2/error.html - No includeSubDomains directive • https://pj.ftis.org.tw/CFCv2/CFC/ - No includeSubDomains directive • https://pj.ftis.org.tw/CFCv2/CFC/Index - No includeSubDomains directive • https://pj.ftis.org.tw/CFCv2/CFC/Login/ - No includeSubDomains directive • https://pj.ftis.org.tw/CFCv2/CFC/Login/guest - No includeSubDomains directive

```
GET /CFCv2/ HTTP/1.1

Referer: https://pj.ftis.org.tw/CFCv2/

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: pj.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://pj.ftis.org.tw/CFCv2/ • https://pj.ftis.org.tw/CFCv2/error.html • https://pj.ftis.org.tw/CFCv2/CFC/ • https://pj.ftis.org.tw/CFCv2/CFC/Index • https://pj.ftis.org.tw/CFCv2/CFC/Login/ • https://pj.ftis.org.tw/CFCv2/CFC/Login/guest

```
GET /CFCv2/ HTTP/1.1

Referer: https://pj.ftis.org.tw/CFCv2/

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: pj.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: pj.ftis.org.tw

Connection: Keep-alive
```

Scanned items (coverage report)

https://pj.ftis.org.tw/
https://pj.ftis.org.tw/CFCv2/
https://pj.ftis.org.tw/CFCv2/CFC/
https://pj.ftis.org.tw/CFCv2/cfc/cal
https://pj.ftis.org.tw/CFCv2/CFC/CreateUser
https://pj.ftis.org.tw/CFCv2/CFC/GetCompanyProperties
https://pj.ftis.org.tw/CFCv2/CFC/GetFactoriesByUser
https://pj.ftis.org.tw/CFCv2/CFC/Guest
https://pj.ftis.org.tw/CFCv2/CFC/Index
https://pj.ftis.org.tw/CFCv2/CFC/Login/
https://pj.ftis.org.tw/CFCv2/CFC/Login/guest
https://pj.ftis.org.tw/CFCv2/CFC/Logoff
https://pj.ftis.org.tw/CFCv2/Content/
https://pj.ftis.org.tw/CFCv2/Content/bootstrap.css
https://pj.ftis.org.tw/CFCv2/Content/font-awesome-4.7.0/
https://pj.ftis.org.tw/CFCv2/Content/font-awesome-4.7.0/css/
https://pj.ftis.org.tw/CFCv2/Content/font-awesome-4.7.0/css/font-awesome.css
https://pj.ftis.org.tw/CFCv2/Content/font-awesome-4.7.0/fonts/
https://pj.ftis.org.tw/CFCv2/Content/prj/
https://pj.ftis.org.tw/CFCv2/Content/prj/css/
https://pj.ftis.org.tw/CFCv2/Content/prj/css/style.css
https://pj.ftis.org.tw/CFCv2/Content/prj/images/
https://pj.ftis.org.tw/CFCv2/Content/prj/site.css
https://pj.ftis.org.tw/CFCv2/error.html
https://pj.ftis.org.tw/CFCv2/Images/
https://pj.ftis.org.tw/CFCv2/Scripts/
https://pj.ftis.org.tw/CFCv2/Scripts/bootstrap.bundle.min.js
https://pj.ftis.org.tw/CFCv2/Scripts/Dou/
https://pj.ftis.org.tw/CFCv2/Scripts/Dou/datetimepicker/
https://pj.ftis.org.tw/CFCv2/Scripts/Dou/datetimepicker/css/
https://pj.ftis.org.tw/CFCv2/Scripts/Dou/datetimepicker/css/tempusdominus-bootstrap-4.min.css
https://pj.ftis.org.tw/CFCv2/Scripts/Dou/datetimepicker/js/
https://pj.ftis.org.tw/CFCv2/Scripts/Dou/datetimepicker/js/moment.js
https://pj.ftis.org.tw/CFCv2/Scripts/Dou/datetimepicker/js/tempusdominus-bootstrap-4.min.js
https://pj.ftis.org.tw/CFCv2/Scripts/Dou/Dou.css
https://pj.ftis.org.tw/CFCv2/Scripts/Dou/Dou.js
https://pj.ftis.org.tw/CFCv2/Scripts/gis/
https://pj.ftis.org.tw/CFCv2/Scripts/gis/b3/
https://pj.ftis.org.tw/CFCv2/Scripts/gis/b3/css/
https://pj.ftis.org.tw/CFCv2/Scripts/gis/b3/css/bootstrap.css
https://pj.ftis.org.tw/CFCv2/Scripts/gis/b3/fonts/
https://pj.ftis.org.tw/CFCv2/Scripts/gis/bootstraptable/
https://pj.ftis.org.tw/CFCv2/Scripts/gis/bootstraptable/bootstrap-table.css
https://pj.ftis.org.tw/CFCv2/Scripts/gis/bootstraptable/bootstrap-table.js
https://pj.ftis.org.tw/CFCv2/Scripts/gis/bootstraptable/extensions/
https://pj.ftis.org.tw/CFCv2/Scripts/gis/bootstraptable/extensions/mobile/
https://pj.ftis.org.tw/CFCv2/Scripts/gis/bootstraptable/extensions/mobile/bootstrap-table-mobile.js
https://pj.ftis.org.tw/CFCv2/Scripts/gis/helper.js
https://pj.ftis.org.tw/CFCv2/Scripts/gis/images/
https://pj.ftis.org.tw/CFCv2/Scripts/gis/Main.css
https://pj.ftis.org.tw/CFCv2/Scripts/gis/Main.js
https://pj.ftis.org.tw/CFCv2/Scripts/gis/select/
https://pj.ftis.org.tw/CFCv2/Scripts/gis/select/bselect/
https://pj.ftis.org.tw/CFCv2/Scripts/gis/select/bselect/bootstrap-select.min.css
https://pj.ftis.org.tw/CFCv2/Scripts/jquery-3.6.4.js
https://pj.ftis.org.tw/CFCv2/Scripts/prj/
https://pj.ftis.org.tw/CFCv2/Scripts/prj/cfc_n.js