Acunetix
by Invicti

# Affected Items Report

Acunetix Security Audit

2024-11-01

Generated by Acunetix

# Scan of pj.ftis.org.tw

## Scan details

| Scan information | |
|---|---|
| Start time | 2024-11-01T11:34:18.535039+08:00 |
| Start url | https://pj.ftis.org.tw/CFCv2/ |
| Host | pj.ftis.org.tw |
| Scan time | 77 minutes, 30 seconds |
| Profile | Full Scan |
| Server information | Microsoft-IIS/10.0 |
| Responsive | True |
| Server OS | Windows |
| Application build | 24.9.241025109 |

### Threat level

#### Acunetix Threat Level 4

One or more critical-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.

### Alerts distribution

| Total alerts found | 30 |
|---|---|
| Critical | 4 |
| High | 4 |
| Medium | 13 |
| Low | 0 |
| Informational | 9 |

## Affected items

| | |
|---|---|
| **Web Server** | |
| **Alert group** | **Handlebars CVE-2021-23369 Vulnerability** |
| Severity | Critical |
| Description | The package handlebars before 4.7.7 are vulnerable to Remote Code Execution (RCE) when selecting certain compiling options to compile templates coming from an untrusted source. |
| Recommendations | |
| Alert variants | |
| Details | handlebars.js v4.0.5-4.0.5 |

| | |
|---|---|
| **Web Server** | |
| **Alert group** | **Handlebars Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection') Vulnerability** |
| Severity | Critical |
| Description | Versions of handlebars prior to 4.3.0 are vulnerable to Prototype Pollution leading to Remote Code Execution. Templates may alter an Object's __proto__ and __defineGetter__ properties, which may allow an attacker to execute arbitrary code through crafted payloads. |
| Recommendations | |
| Alert variants | |
| Details | handlebars.js v4.0.5-4.0.5 |

| | |
|---|---|
| **Web Server** | |
| **Alert group** | **Handlebars Other Vulnerability** |
| Severity | Critical |
| Description | The package handlebars before 4.7.7 are vulnerable to Prototype Pollution when selecting certain compiling options to compile templates coming from an untrusted source. |
| Recommendations | |
| Alert variants | |
| Details | handlebars.js v4.0.5-4.0.5 |

| | |
|---|---|
| **Web Server** | |
| **Alert group** | **Lodash Other Vulnerability** |
| Severity | Critical |
| Description | Versions of lodash lower than 4.17.12 are vulnerable to Prototype Pollution. The function defaultsDeep could be tricked into adding or modifying properties of Object.prototype using a constructor payload. |
| Recommendations | |
| Alert variants | |
| Details | lodash v3.10.1-3.10.1 |

| | |
|---|---|
| **Web Server** | |
| **Alert group** | **Handlebars Improper Control of Generation of Code ('Code Injection') Vulnerability** |
| Severity | High |

| | |
|---|---|
| Description | Handlebars before 3.0.8 and 4.x before 4.5.3 is vulnerable to Arbitrary Code Execution. The lookup helper fails to properly validate templates, allowing attackers to submit templates that execute arbitrary JavaScript. This can be used to run arbitrary code on a server processing Handlebars templates or in a victim's browser (effectively serving as XSS). |
| Recommendations | |
| Alert variants | |
| Details | handlebars.js v4.0.5-4.0.5 |

| | |
|---|---|
| **Web Server** | |
| **Alert group** | **Handlebars Loop with Unreachable Exit Condition ('Infinite Loop') Vulnerability** |
| Severity | High |
| Description | Handlebars before 4.4.5 allows Regular Expression Denial of Service (ReDoS) because of eager matching. The parser may be forced into an endless loop while processing crafted templates. This may allow attackers to exhaust system resources. |
| Recommendations | |
| Alert variants | |
| Details | handlebars.js v4.0.5-4.0.5 |

| | |
|---|---|
| **Web Server** | |
| **Alert group** | **Lodash Improper Neutralization of Special Elements used in a Command ('Command Injection') Vulnerability** |
| Severity | High |
| Description | Lodash versions prior to 4.17.21 are vulnerable to Command Injection via the template function. |
| Recommendations | |
| Alert variants | |
| Details | lodash v3.10.1-3.10.1 |

| | |
|---|---|
| **Web Server** | |
| **Alert group** | **Lodash Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution') Vulnerability** |
| Severity | High |
| Description | Prototype pollution attack when using _.zipObjectDeep in lodash before 4.17.20. |
| Recommendations | |
| Alert variants | |
| Details | lodash v3.10.1-3.10.1 |

| | |
|---|---|
| **Web Server** | |
| **Alert group** | **jQuery Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability** |
| Severity | Medium |

| | |
|---|---|
| Description | jQuery before 1.9.0 is vulnerable to Cross-site Scripting (XSS) attacks. The jQuery(strInput) function does not differentiate selectors from HTML in a reliable fashion. In vulnerable versions, jQuery determined whether the input was HTML by looking for the '<' character anywhere in the string, giving attackers more flexibility when attempting to construct a malicious payload. In fixed versions, jQuery only deems the input to be HTML if it explicitly starts with the '<' character, limiting exploitability only to attackers who can control the beginning of a string, which is far less common. |
| Recommendations | |
| Alert variants | |
| Details | jquery v1.8.0-1.8.0 |

| | |
|---|---|
| **Web Server** | |
| **Alert group** | **jQuery Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability** |
| Severity | Medium |
| Description | jquery prior to 1.9.0 allows Cross-site Scripting attacks via the load method. The load method fails to recognize and remove "<script>" HTML tags that contain a whitespace character, i.e: "</script >", which results in the enclosed script logic to be executed. |
| Recommendations | |
| Alert variants | |
| Details | jquery v1.8.0-1.8.0 |

| | |
|---|---|
| **Web Server** | |
| **Alert group** | **jQuery Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability** |
| Severity | Medium |
| Description | jQuery before 3.0.0 is vulnerable to Cross-site Scripting (XSS) attacks when a cross-domain Ajax request is performed without the dataType option, causing text/javascript responses to be executed. |
| Recommendations | |
| Alert variants | |
| Details | jquery v1.8.0-1.8.0 |

| | |
|---|---|
| **Web Server** | |
| **Alert group** | **jQuery Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability** |
| Severity | Medium |
| Description | 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. |
| Recommendations | |
| Alert variants | |
| Details | jquery v1.8.0-1.8.0 |

| | |
|---|---|
| **Web Server** | |

| | |
|---|---|
| **Alert group** | **jQuery Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability** |
| Severity | Medium |
| 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. |
| Recommendations | |
| Alert variants | |
| Details | jquery v1.8.0-1.8.0 |

| | |
|---|---|
| **Web Server** | |
| **Alert group** | **jQuery Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution') Vulnerability** |
| Severity | Medium |
| Description | jQuery before 3.4.0, as used in Drupal, Backdrop CMS, and other products, 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. |
| Recommendations | |
| Alert variants | |
| Details | jquery v1.8.0-1.8.0 |

| | |
|---|---|
| **Web Server** | |
| **Alert group** | **Lodash Allocation of Resources Without Limits or Throttling Vulnerability** |
| Severity | Medium |
| Description | lodash prior to 4.17.11 is affected by: CWE-400: Uncontrolled Resource Consumption. The impact is: Denial of service. The component is: Date handler. The attack vector is: Attacker provides very long strings, which the library attempts to match using a regular expression. The fixed version is: 4.17.11. |
| Recommendations | |
| Alert variants | |
| Details | lodash v3.10.1-3.10.1 |

| | |
|---|---|
| **Web Server** | |
| **Alert group** | **Lodash CVE-2018-16487 Vulnerability** |
| Severity | Medium |
| Description | A prototype pollution vulnerability was found in lodash <4.17.11 where the functions merge, mergeWith, and defaultsDeep can be tricked into adding or modifying properties of Object.prototype. |
| Recommendations | |
| Alert variants | |
| Details | lodash v3.10.1-3.10.1 |

| | |
|---|---|
| **Web Server** | |
| **Alert group** | **Lodash CVE-2018-3721 Vulnerability** |

| | |
|---|---|
| Severity | Medium |
| Description | lodash node module before 4.17.5 suffers from a Modification of Assumed-Immutable Data (MAID) vulnerability via defaultsDeep, merge, and mergeWith functions, which allows a malicious user to modify the prototype of "Object" via __proto__, causing the addition or modification of an existing property that will exist on all objects. |
| Recommendations | |
| Alert variants | |
| Details | lodash v3.10.1-3.10.1 |

| | |
|---|---|
| **Web Server** | |
| **Alert group** | **Lodash Other Vulnerability** |
| Severity | Medium |
| Description | Lodash versions prior to 4.17.21 are vulnerable to Regular Expression Denial of Service (ReDoS) via the toNumber, trim and trimEnd functions. |
| Recommendations | |
| Alert variants | |
| Details | lodash v3.10.1-3.10.1 |

| | |
|---|---|
| **Web Server** | |
| **Alert group** | **Vulnerable JavaScript libraries** |
| Severity | Medium |
| Description | 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. |
| Recommendations | Upgrade to the latest version. |
| Alert variants | |

| | |
|---|---|
| Details | • **jQuery 1.8.0**<br>◦ URL: https://pj.ftis.org.tw/CFCv2/swagger/ui/index<br>◦ Detection method: The library's name and version were determined based on its dynamic behavior.<br>◦ CVE-ID: CVE-2015-9251, CVE-2020-11022, CVE-2020-11023<br>◦ Description: Selector interpreted as HTML / Possible Cross Site Scripting via third-party text/javascript responses / 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.<br>◦ References:<br>▪ http://bugs.jquery.com/ticket/11290<br>▪ http://research.insecurelabs.org/jquery/test/<br>▪ https://github.com/jquery/jquery/issues/2432<br>▪ http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/<br>▪ https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/<br>▪ https://mksben.l0.cm/2020/05/jquery3.5.0-xss.html<br>▪ https://jquery.com/upgrade-guide/3.5/<br>▪ https://api.jquery.com/jQuery.htmlPrefilter/<br>▪ https://www.cvedetails.com/cve/CVE-2020-11022/<br>▪ https://github.com/advisories/GHSA-gxr4-xjj5-5px2<br>▪ https://www.cvedetails.com/cve/CVE-2020-11023/<br>▪ https://github.com/advisories/GHSA-jpcq-cgw6-v4j6 |

```
GET /CFCv2/swagger/ui/index?apiKey=1&baseUrl=http://www.example.com 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** | **Vulnerable JavaScript libraries** |
| Severity | Medium |
| Description | 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. |
| Recommendations | Upgrade to the latest version. |
| Alert variants | |

| | |
|---|---|
| Details | • **handlebars.js 4.0.5**<br>◦ URL: https://pj.ftis.org.tw/CFCv2/swagger/ui/index<br>◦ Detection method: The library's name and version were determined based on its dynamic behavior.<br>◦ CVE-ID: N/A<br>◦ Description: Unsafe direct call of helperMissing and blockHelperMissing / Prototype pollution<br>◦ References:<br>▪ https://github.com/wycats/handlebars.js/blob/master/release-notes.md#v430---september-24th-2019<br>▪ https://github.com/wycats/handlebars.js/blob/master/release-notes.md#v453---november-18th-2019 |

```
GET /CFCv2/swagger/ui/index?apiKey=1&baseUrl=http://www.example.com 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** | **Vulnerable JavaScript libraries** |
| Severity | Medium |
| Description | 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. |
| Recommendations | Upgrade to the latest version. |
| Alert variants | |

| | |
|---|---|
| Details | • **Lodash 3.10.1**<br>◦ URL: https://pj.ftis.org.tw/CFCv2/swagger/ui/index<br>◦ Detection method: The library's name and version were determined based on its dynamic behavior.<br>◦ CVE-ID: CVE-2021-23337, CVE-2020-8203, CVE-2020-28500, CVE-2019-10744, CVE-2018-16487, CVE-2019-1010266<br>◦ Description: Lodash versions prior to 4.17.21 are vulnerable to Command Injection via the template function. / Prototype pollution attack when using _.zipObjectDeep in lodash before 4.17.20. / Lodash versions prior to 4.17.21 are vulnerable to Regular Expression Denial of Service (ReDoS) via the toNumber, trim and trimEnd functions. / Versions of lodash lower than 4.17.12 are vulnerable to Prototype Pollution. The function defaultsDeep could be tricked into adding or modifying properties of Object.prototype using a constructor payload. / A prototype pollution vulnerability was found in lodash <4.17.11 where the functions merge, mergeWith, and defaultsDeep can be tricked into adding or modifying properties of Object.prototype. / lodash prior to 4.17.11 is affected by: CWE-400: Uncontrolled Resource Consumption. The impact is: Denial of service. The component is: Date handler. The attack vector is: Attacker provides very long strings, which the library attempts to match using a regular expression. The fixed version is: 4.17.11.<br>◦ References:<br>▪ https://nvd.nist.gov/vuln/detail/CVE-2021-23337<br>▪ https://nvd.nist.gov/vuln/detail/CVE-2020-8203<br>▪ https://nvd.nist.gov/vuln/detail/CVE-2020-28500<br>▪ https://nvd.nist.gov/vuln/detail/CVE-2019-10744<br>▪ https://nvd.nist.gov/vuln/detail/CVE-2018-16487<br>▪ https://nvd.nist.gov/vuln/detail/CVE-2019-1010266 |

```
GET /CFCv2/swagger/ui/index?apiKey=1&baseUrl=http://www.example.com 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** | **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.<br><br>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):<br><br>• /<br>• /CFCv2/<br>• /CFCv2/Content/prj/images/<br>• /CFCv2/CFC/Login/guest<br>• /CFCv2/Scripts/<br>• /CFCv2/swagger/ui/index<br>• /CFCv2/CFC/<br>• /CFCv2/swagger/<br>• /CFCv2/Content/<br>• /CFCv2/CFC/GetCompanyProperties<br>• /CFCv2/error.html<br>• /CFCv2/CFC/Guest<br>• /CFCv2/Content/prj/<br>• /CFCv2/swagger/docs/v1<br>• /CFCv2/api/<br>• /CFCv2/api/CFCData<br>• /CFCv2/api/cfc/cal<br>• /CFCv2/api/DataPrint<br>• /CFCv2/CFC/Index<br>• /CFCv2/Images/<br>• /CFCv2/CFC/Logoff |

```
GET / HTTP/1.1

Origin: https://pj.ftis.org.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/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.<br><br>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:<br><br>`Content-Security-Policy:`<br>`default-src 'self';`<br>`script-src 'self' https://code.jquery.com;`<br><br>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:<br>• https://pj.ftis.org.tw/CFCv2/CFC/Login/guest<br>• https://pj.ftis.org.tw/CFCv2/<br>• https://pj.ftis.org.tw/CFCv2/swagger/ui/index<br>• https://pj.ftis.org.tw/CFCv2/error.html<br>• https://pj.ftis.org.tw/CFCv2/CFC/<br>• https://pj.ftis.org.tw/CFCv2/CFC/Index<br>• https://pj.ftis.org.tw/CFCv2/CFC/Login/ |

```
GET /CFCv2/CFC/Login/guest 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:<br>• https://pj.ftis.org.tw/CFCv2/<br>**pol78917@ftis.org.tw**<br>• https://pj.ftis.org.tw/CFCv2/CFC/Login/guest<br>**pol78917@ftis.org.tw**<br>• https://pj.ftis.org.tw/CFCv2/CFC/<br>**pol78917@ftis.org.tw**<br>• https://pj.ftis.org.tw/CFCv2/CFC/Index<br>**pol78917@ftis.org.tw**<br>• https://pj.ftis.org.tw/CFCv2/CFC/Login/<br>**pol78917@ftis.org.tw** |

```
POST /CFCv2/?login=True HTTP/1.1

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

Content-Type: application/x-www-form-urlencoded

Content-Length: 26

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



Id=1&Pass=u]H[ww6KrA9F.x-F
```

| | |
|---|---|
| **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:<br><br>• https://pj.ftis.org.tw/CFCv2/ - No includeSubDomains directive<br>• https://pj.ftis.org.tw/CFCv2/CFC/Login/guest - No includeSubDomains directive<br>• https://pj.ftis.org.tw/CFCv2/swagger/ui/index - No includeSubDomains directive<br>• https://pj.ftis.org.tw/CFCv2/error.html - No includeSubDomains directive<br>• https://pj.ftis.org.tw/CFCv2/CFC/ - No includeSubDomains directive<br>• https://pj.ftis.org.tw/CFCv2/CFC/Index - No includeSubDomains directive<br>• https://pj.ftis.org.tw/CFCv2/CFC/Login/ - No includeSubDomains directive |

```
POST /CFCv2/?login=True HTTP/1.1

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

Content-Type: application/x-www-form-urlencoded

Content-Length: 26

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



Id=1&Pass=u]H[ww6KrA9F.x-F
```

| | |
|---|---|
| **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**<br>  ◦ URL: https://pj.ftis.org.tw/CFCv2/Scripts/modernizr-2.8.3.js<br>  ◦ Detection method: The library's name and version were determined based on the file's name.<br>  ◦ References:<br>  ▪ https://github.com/Modernizr/Modernizr/releases |

```
GET /CFCv2/Scripts/modernizr-2.8.3.js 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
```

| **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**<br>◦ URL: https://pj.ftis.org.tw/CFCv2/<br>◦ Detection method: The library's name and version were determined based on its dynamic behavior.<br>◦ References:<br>▪ https://github.com/aFarkas/html5shiv/tags |

```
POST /CFCv2/?login=True HTTP/1.1

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

Content-Type: application/x-www-form-urlencoded

Content-Length: 26

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



Id=1&Pass=u]H[ww6KrA9F.x-F
```

| **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 | • **Backbone.js 1.1.2**<br>◦ URL: https://pj.ftis.org.tw/CFCv2/swagger/ui/index<br>◦ Detection method: The library's name and version were determined based on its dynamic behavior.<br>◦ References:<br>▪ https://backbonejs.org/#changelog |

```
GET /CFCv2/swagger/ui/index?apiKey=1&baseUrl=http://www.example.com 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:<br>• https://pj.ftis.org.tw/CFCv2/<br>• https://pj.ftis.org.tw/CFCv2/CFC/Login/guest<br>• https://pj.ftis.org.tw/CFCv2/swagger/ui/index<br>• https://pj.ftis.org.tw/CFCv2/error.html<br>• https://pj.ftis.org.tw/CFCv2/CFC/<br>• https://pj.ftis.org.tw/CFCv2/CFC/Index<br>• https://pj.ftis.org.tw/CFCv2/CFC/Login/ |

```
POST /CFCv2/?login=True HTTP/1.1

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

Content-Type: application/x-www-form-urlencoded

Content-Length: 26

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



Id=1&Pass=u]H[ww6KrA9F.x-F
```

| **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:<br>`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/api/
https://pj.ftis.org.tw/CFCv2/api/cfc/
https://pj.ftis.org.tw/CFCv2/api/cfc/cal
https://pj.ftis.org.tw/CFCv2/api/cfc/cal2
https://pj.ftis.org.tw/CFCv2/api/CFCData
https://pj.ftis.org.tw/CFCv2/api/DataPrint
https://pj.ftis.org.tw/CFCv2/CFC/
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/modernizr-2.8.3.js
https://pj.ftis.org.tw/CFCv2/Scripts/prj/
https://pj.ftis.org.tw/CFCv2/Scripts/prj/cfc_n.js
https://pj.ftis.org.tw/CFCv2/swagger/
https://pj.ftis.org.tw/CFCv2/swagger/docs/
https://pj.ftis.org.tw/CFCv2/swagger/docs/v1
https://pj.ftis.org.tw/CFCv2/swagger/ui/
https://pj.ftis.org.tw/CFCv2/swagger/ui/css/
https://pj.ftis.org.tw/CFCv2/swagger/ui/css/print-css
https://pj.ftis.org.tw/CFCv2/swagger/ui/css/reset-css
https://pj.ftis.org.tw/CFCv2/swagger/ui/css/screen-css
https://pj.ftis.org.tw/CFCv2/swagger/ui/css/typography-css
https://pj.ftis.org.tw/CFCv2/swagger/ui/fonts/
https://pj.ftis.org.tw/CFCv2/swagger/ui/fonts/DroidSans-Bold-ttf
https://pj.ftis.org.tw/CFCv2/swagger/ui/fonts/DroidSans-ttf
https://pj.ftis.org.tw/CFCv2/swagger/ui/images/
https://pj.ftis.org.tw/CFCv2/swagger/ui/images/explorer_icons-png
https://pj.ftis.org.tw/CFCv2/swagger/ui/images/favicon-16x16-png
https://pj.ftis.org.tw/CFCv2/swagger/ui/images/favicon-32x32-png
https://pj.ftis.org.tw/CFCv2/swagger/ui/images/logo_small-png
https://pj.ftis.org.tw/CFCv2/swagger/ui/images/throbber-gif
https://pj.ftis.org.tw/CFCv2/swagger/ui/index
https://pj.ftis.org.tw/CFCv2/swagger/ui/lib/
https://pj.ftis.org.tw/CFCv2/swagger/ui/lib/backbone-min-js
https://pj.ftis.org.tw/CFCv2/swagger/ui/lib/handlebars-4-0-5-js
https://pj.ftis.org.tw/CFCv2/swagger/ui/lib/highlight-9-1-0-pack-js
https://pj.ftis.org.tw/CFCv2/swagger/ui/lib/highlight-9-1-0-pack_extended-js
https://pj.ftis.org.tw/CFCv2/swagger/ui/lib/jquery-1-8-0-min-js
https://pj.ftis.org.tw/CFCv2/swagger/ui/lib/jquery-ba-bbq-min-js
https://pj.ftis.org.tw/CFCv2/swagger/ui/lib/jquery-slideto-min-js
https://pj.ftis.org.tw/CFCv2/swagger/ui/lib/jquery-wiggle-min-js
https://pj.ftis.org.tw/CFCv2/swagger/ui/lib/jsoneditor-min-js
https://pj.ftis.org.tw/CFCv2/swagger/ui/lib/lodash-min-js
https://pj.ftis.org.tw/CFCv2/swagger/ui/lib/marked-js
https://pj.ftis.org.tw/CFCv2/swagger/ui/lib/object-assign-pollyfill-js
https://pj.ftis.org.tw/CFCv2/swagger/ui/lib/swagger-oauth-js
https://pj.ftis.org.tw/CFCv2/swagger/ui/swagger-ui-min-js