Acunetix
by Invicti

Affected Items Report

Acunetix Security Audit

2024-11-27

Scan of eslc.ftis.org.tw

Scan details

Scan information	
Start time	2024-11-25T14:00:35.503978+08:00
Start url	https://eslc.ftis.org.tw/
Host	eslc.ftis.org.tw
Scan time	149 minutes, 27 seconds
Profile	Full Scan
Server information	Microsoft-IIS/10.0
Responsive	True
Server OS	Windows
Server technologies	ASP.NET
Application build	24.10.241106172

Threat level

Acunetix Threat Level 0

No vulnerabilities have been discovered by the scanner.

Alerts distribution

Total alerts found	9
⚠ Critical	0
⚠ High	0
⌃ Medium	0
⌄ Low	0
ⓘ Informational	9

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://eslc.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://eslc.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: eslc.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://eslc.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://eslc.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: eslc.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://eslc.ftis.org.tw/
	  jimi@ftis.org.tw
	- https://eslc.ftis.org.tw/
	  wenhsiung@ftis.org.tw
	- https://eslc.ftis.org.tw/link
	  jimi@ftis.org.tw
	- https://eslc.ftis.org.tw/link
	  wenhsiung@ftis.org.tw
	- https://eslc.ftis.org.tw/profile
	  jimi@ftis.org.tw
	- https://eslc.ftis.org.tw/profile
	  melody0320@ftis.org.tw
	- https://eslc.ftis.org.tw/profile
	  pupss93326@ftis.org.tw
	- https://eslc.ftis.org.tw/profile
	  jackywu@ftis.org.tw
	- https://eslc.ftis.org.tw/profile
	  rb26dett@ftis.org.tw
	- https://eslc.ftis.org.tw/profile
	  coco000902@ftis.org.tw
	- https://eslc.ftis.org.tw/profile
	  danny@ftis.org.tw
	- https://eslc.ftis.org.tw/profile
	  jackyyang@ftis.org.tw
	- https://eslc.ftis.org.tw/profile
	  jackyang@ftis.org.tw
	- https://eslc.ftis.org.tw/profile
	  wenhsiung@ftis.org.tw
	- https://eslc.ftis.org.tw/index
	  jimi@ftis.org.tw
	- https://eslc.ftis.org.tw/index
	  wenhsiung@ftis.org.tw
	- https://eslc.ftis.org.tw/industry
	  jimi@ftis.org.tw
	- https://eslc.ftis.org.tw/industry
	  neighbor@ftis.org.tw
	- https://eslc.ftis.org.tw/industry
	  wenhsiung@ftis.org.tw
	- https://eslc.ftis.org.tw/news_in
	  jimi@ftis.org.tw
	- https://eslc.ftis.org.tw/news_in
	  wenhsiung@ftis.org.tw

```
GET / HTTP/1.1

Referer: https://eslc.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: eslc.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://eslc.ftis.org.tw/ - No includeSubDomains directive • https://eslc.ftis.org.tw/link - No includeSubDomains directive • https://eslc.ftis.org.tw/profile - No includeSubDomains directive • https://eslc.ftis.org.tw/index - No includeSubDomains directive • https://eslc.ftis.org.tw/industry - No includeSubDomains directive • https://eslc.ftis.org.tw/news_in - No includeSubDomains directive • https://eslc.ftis.org.tw/industry3 - No includeSubDomains directive • https://eslc.ftis.org.tw/news - No includeSubDomains directive • https://eslc.ftis.org.tw/sitemap - No includeSubDomains directive • https://eslc.ftis.org.tw/index.html - No includeSubDomains directive • https://eslc.ftis.org.tw/login - No includeSubDomains directive • https://eslc.ftis.org.tw/login.html - No includeSubDomains directive • https://eslc.ftis.org.tw/results - No includeSubDomains directive • https://eslc.ftis.org.tw/industry.html - No includeSubDomains directive • https://eslc.ftis.org.tw/link.html - No includeSubDomains directive • https://eslc.ftis.org.tw/results_in - No includeSubDomains directive • https://eslc.ftis.org.tw/news.html - No includeSubDomains directive • https://eslc.ftis.org.tw/news2_in.html - No includeSubDomains directive • https://eslc.ftis.org.tw/news3_in.html - No includeSubDomains directive • https://eslc.ftis.org.tw/news_in.html - No includeSubDomains directive • https://eslc.ftis.org.tw/profile.html - No includeSubDomains directive

```
GET / HTTP/1.1

Referer: https://eslc.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: eslc.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://eslc.ftis.org.tw/Scripts/bootstrap/js/bootstrap.min.js

```
GET /Scripts/bootstrap/js/bootstrap.min.js HTTP/1.1

Referer: https://eslc.ftis.org.tw/industry2

Cookie: ASP.NET_SessionId=tyutb5zdes42ytbgwplyhaxi

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: eslc.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://eslc.ftis.org.tw/ • https://eslc.ftis.org.tw/link • https://eslc.ftis.org.tw/profile • https://eslc.ftis.org.tw/index • https://eslc.ftis.org.tw/industry • https://eslc.ftis.org.tw/news_in • https://eslc.ftis.org.tw/industry3 • https://eslc.ftis.org.tw/news • https://eslc.ftis.org.tw/sitemap • https://eslc.ftis.org.tw/index.html • https://eslc.ftis.org.tw/login • https://eslc.ftis.org.tw/login.html • https://eslc.ftis.org.tw/results • https://eslc.ftis.org.tw/industry.html • https://eslc.ftis.org.tw/link.html • https://eslc.ftis.org.tw/results_in • https://eslc.ftis.org.tw/news.html • https://eslc.ftis.org.tw/news2_in.html • https://eslc.ftis.org.tw/news3_in.html • https://eslc.ftis.org.tw/news_in.html • https://eslc.ftis.org.tw/profile.html

```
GET / HTTP/1.1

Referer: https://eslc.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: eslc.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.
	
	<pre><script src="https://example.com/example-framework.js"
	        integrity="sha384-oqVuAfXRKap7fdgcCY5uykM6+R9GqQ8K/uxy9rx7HN
	        crossorigin="anonymous"></script></pre>

Alert variants	
Details	Pages where SRI is not implemented: • https://eslc.ftis.org.tw/login Script SRC: **https://www.google.com/recaptcha/api.js**

```
GET /login HTTP/1.1

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

Cookie: ASP.NET_SessionId=tyutb5zdes42ytbgwplyhaxi

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: eslc.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: eslc.ftis.org.tw

Connection: Keep-alive
```

Web Server	
Alert group	**Web Application Firewall Detected**
Severity	Informational
Description	This server is protected by an IPS (Intrusion Prevention System), IDS (Intrusion Detection System) or an WAF (Web Application Firewall). Acunetix detected this by sending various malicious payloads and detecting changes in the response code, headers and body.
Recommendations	If possible, it's recommended to scan an internal (development) version of the web application where the WAF is not active.
Alert variants	
Details	Detected ASP.NET RequestValidation from the response body.

```
GET /?search=<script>alert(1)</script> HTTP/1.1

Cookie: ASP.NET_SessionId=tyutb5zdes42ytbgwplyhaxi

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: eslc.ftis.org.tw

Connection: Keep-alive
```

Scanned items (coverage report)

https://eslc.ftis.org.tw/
https://eslc.ftis.org.tw/bak/
https://eslc.ftis.org.tw/Case.aspx
https://eslc.ftis.org.tw/change.html
https://eslc.ftis.org.tw/contact/
https://eslc.ftis.org.tw/content/
https://eslc.ftis.org.tw/forget
https://eslc.ftis.org.tw/forget.aspx
https://eslc.ftis.org.tw/forget.html
https://eslc.ftis.org.tw/images/
https://eslc.ftis.org.tw/img/
https://eslc.ftis.org.tw/index
https://eslc.ftis.org.tw/index.aspx
https://eslc.ftis.org.tw/index.html
https://eslc.ftis.org.tw/industry
https://eslc.ftis.org.tw/industry.aspx
https://eslc.ftis.org.tw/industry.html
https://eslc.ftis.org.tw/industry2
https://eslc.ftis.org.tw/industry2.aspx
https://eslc.ftis.org.tw/industry2.html
https://eslc.ftis.org.tw/industry3
https://eslc.ftis.org.tw/industry3.aspx
https://eslc.ftis.org.tw/industry3.html
https://eslc.ftis.org.tw/industry3_in
https://eslc.ftis.org.tw/industry3_in.aspx
https://eslc.ftis.org.tw/industry3_in.html
https://eslc.ftis.org.tw/industry4
https://eslc.ftis.org.tw/industry4.aspx
https://eslc.ftis.org.tw/industry4.html
https://eslc.ftis.org.tw/industry5
https://eslc.ftis.org.tw/industry5.aspx
https://eslc.ftis.org.tw/industry5.html
https://eslc.ftis.org.tw/industry5_A
https://eslc.ftis.org.tw/industry5_A.aspx
https://eslc.ftis.org.tw/industry5_B
https://eslc.ftis.org.tw/industry5_B.aspx
https://eslc.ftis.org.tw/industry5_in
https://eslc.ftis.org.tw/industry5_in.aspx
https://eslc.ftis.org.tw/industry6
https://eslc.ftis.org.tw/industry6.aspx
https://eslc.ftis.org.tw/industry6.html
https://eslc.ftis.org.tw/link
https://eslc.ftis.org.tw/link.aspx
https://eslc.ftis.org.tw/link.html
https://eslc.ftis.org.tw/login
https://eslc.ftis.org.tw/login.aspx
https://eslc.ftis.org.tw/login.html
https://eslc.ftis.org.tw/logs/
https://eslc.ftis.org.tw/news
https://eslc.ftis.org.tw/news.aspx
https://eslc.ftis.org.tw/news.html
https://eslc.ftis.org.tw/news_in
https://eslc.ftis.org.tw/news_in.aspx
https://eslc.ftis.org.tw/news_in.html
https://eslc.ftis.org.tw/news2.html
https://eslc.ftis.org.tw/news2_in.html
https://eslc.ftis.org.tw/news3.html
https://eslc.ftis.org.tw/news3_in.html
https://eslc.ftis.org.tw/Personalized.html

https://eslc.ftis.org.tw/profile
https://eslc.ftis.org.tw/profile.aspx
https://eslc.ftis.org.tw/profile.html
https://eslc.ftis.org.tw/profile2.html
https://eslc.ftis.org.tw/resources.html
https://eslc.ftis.org.tw/resources_in.html
https://eslc.ftis.org.tw/resources2
https://eslc.ftis.org.tw/resources2.aspx
https://eslc.ftis.org.tw/resources2.html
https://eslc.ftis.org.tw/resources3
https://eslc.ftis.org.tw/resources3.aspx
https://eslc.ftis.org.tw/results
https://eslc.ftis.org.tw/results.aspx
https://eslc.ftis.org.tw/results.html
https://eslc.ftis.org.tw/results_in
https://eslc.ftis.org.tw/results_in.aspx
https://eslc.ftis.org.tw/results_in.html
https://eslc.ftis.org.tw/results2
https://eslc.ftis.org.tw/results2.aspx
https://eslc.ftis.org.tw/results2.html
https://eslc.ftis.org.tw/results2_in
https://eslc.ftis.org.tw/results2_in.aspx
https://eslc.ftis.org.tw/scripts/
https://eslc.ftis.org.tw/Scripts/bootstrap/
https://eslc.ftis.org.tw/Scripts/bootstrap/css/
https://eslc.ftis.org.tw/Scripts/bootstrap/css/bootstrap.min.css
https://eslc.ftis.org.tw/scripts/bootstrap/fonts/
https://eslc.ftis.org.tw/Scripts/bootstrap/js/
https://eslc.ftis.org.tw/Scripts/bootstrap/js/bootstrap.min.js
https://eslc.ftis.org.tw/Scripts/bootstrap/js/validator.min.js
https://eslc.ftis.org.tw/Scripts/jquery-3.3.1.min.js
https://eslc.ftis.org.tw/scripts/plugins/
https://eslc.ftis.org.tw/Scripts/WebForms/
https://eslc.ftis.org.tw/Scripts/WebForms/MsAjax/
https://eslc.ftis.org.tw/Scripts/WebForms/MsAjax/MicrosoftAjax.js
https://eslc.ftis.org.tw/Scripts/WebForms/MsAjax/MicrosoftAjaxWebForms.js
https://eslc.ftis.org.tw/sitemap
https://eslc.ftis.org.tw/sitemap.aspx
https://eslc.ftis.org.tw/sitemap.html
https://eslc.ftis.org.tw/style/
https://eslc.ftis.org.tw/style/style.css
https://eslc.ftis.org.tw/WebPhoto/
https://eslc.ftis.org.tw/WebPhoto/MUploads/
https://eslc.ftis.org.tw/WebResource.axd