


國立臺灣師範大學伺服器弱點處理報告單

填表日期：2025 年 11 月 24 日

IP					
Domain Name				掃描時間	2025 年 11 月 21 日
項次	等級	弱點名稱	修補情形	修補日期	未修補原因說明 與防禦因應方法
1	中	在 CSP 中允許的不安全的內聯腳本回退	<input type="checkbox"/> 已修補 <input checked="" type="checkbox"/> 暫不修補		經 Google CSP Evaluator 檢查，已符合資訊安全。佐證如附。
2	中	繞過腳本允許清單的配置	<input type="checkbox"/> 已修補 <input checked="" type="checkbox"/> 暫不修補		經 Google CSP Evaluator 檢查，已符合資訊安全。佐證如附。
3	低	在 CSP 中未強制執行腳本中的可信類型	<input checked="" type="checkbox"/> 已修補 <input type="checkbox"/> 暫不修補		已於末端加上 trusted-types default; require-trusted-types-for 'script'; 佐證如附。
4	低	遺漏「Content-Security-Policy」標頭	<input checked="" type="checkbox"/> 已修補 <input type="checkbox"/> 暫不修補		Web.config 補上 HTTP 回應標頭，新增最安全的互通版本(主程式之 CSP 建立於 index.php 中) Content-Security-Policy: default-src 'none'; style-src 'self' 'unsafe-inline'; img-src 'self' data:; font-src 'self'; media-src 'self'; object-src 'none'; frame-ancestors 'self'; base-uri 'self'; ，佐證如附
5					
申請掃描單位					
承辦人簽章				主管簽章	

備註：主管簽章完畢後，請將本文件掃描電子檔或正本傳送至和平校區 II 資訊中心吳京剛備存，電話：

序號 1 佐證資料：在 CSP 中允許的不安全的內聯腳本回退

檢測結果：

```
Server:
Content-Security-Policy: default-src 'none'; script-src 'self' 'nonce-tAEgwiAUYE5wogzm8LjPog='; style-src 'self' 'unsafe-inline'; img-src 'self' data: blob;; connect-src 'self'; font-src 'self'; frame-src 'self'; frame-ancestors 'self'; form-action 'self'; media-src 'self'; object-src 'none'; base-uri 'self'; manifest-src 'self'; worker-src 'self'; script-src-attr 'none';
```

說明及佐證：

CSP 設定為最新第三版要求

```
Content-Security-Policy: default-src 'none'; script-src 'nonce-gbLTli57SZHUK4H1boVt4g==' 'strict-dynamic' https;; style-src 'self' 'unsafe-inline'; img-src 'self' data: blob;; connect-src 'self'; font-src 'self'; frame-src 'self'; frame-ancestors 'self'; form-action 'self'; media-src 'self'; object-src 'none'; base-uri 'self'; manifest-src 'self'; worker-src 'self'; script-src-attr 'none';
```

預設全部為 none，script 僅開放 nonce 與 strict-dynamic(嚴格)，依據 Google CSP Evaluator 檢查，符合最新第三版的資安檢查，如下圖。

The screenshot shows the Google CSP Evaluator interface. At the top, there are links for "Sample unsafe policy" and "Sample safe policy". The main area displays the CSP configuration: `Content-Security-Policy: default-src 'none'; script-src 'nonce-gbLTli57SZHUK4H1boVt4g==' 'strict-dynamic' https;; style-src 'self' 'unsafe-inline'; img-src 'self' data: blob;; connect-src 'self'; font-src 'self'; frame-src 'self'; frame-ancestors 'self'; form-action 'self'; media-src 'self'; object-src 'none'; base-uri 'self'; manifest-src 'self'; worker-src 'self'; script-src-attr 'none';`. Below this, a dropdown menu is set to "CSP Version 3" and a "CHECK CSP" button is visible. The evaluation results section, titled "Evaluated CSP as seen by a browser supporting CSP Version 3", shows a list of 14 CSP directives, each with a green checkmark and a dropdown arrow. The directives are: default-src, script-src, style-src, img-src, connect-src, font-src, frame-src, frame-ancestors, form-action, media-src, object-src, base-uri, manifest-src, worker-src, and script-src-attr. A link "expand/collapse all" is located at the top right of the results list.

```

C:\Users\confl>
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 0
Content-Type: text/html; charset=utf-8
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server:
Content-Security-Policy: default-src 'none'; script-src 'nonce-gbLTli57SZHUK4H1boVt4g==' 'strict-dynamic' https;; style
-src 'self' 'unsafe-inline'; img-src 'self' data: blob;; connect-src 'self'; font-src 'self'; frame-src 'self'; frame-an
cestors 'self'; form-action 'self'; media-src 'self'; object-src 'none'; base-uri 'self'; manifest-src 'self'; worker-sr
c 'self'; script-src-attr 'none';
Set-Cookie: PHPSESSID=cith0iki55uf6aui9fbonqgp2o; path=/; samesite=Strict; secure; HttpOnly
X-Frame-Options: DENY
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Referrer-Policy: Strict-origin-when-cross-origin
Permissions-Policy: accelerometer=(self), camera=(self), geolocation=(self), gyroscope=(self), magnetometer=(self), micr
ophone=(self), payment=(self), usb=(self)
Date: Mon, 24 Nov 2025 04:43:06 GMT

```

序號 2 佐證資料：繞過腳本允許清單的配置

檢測結果：

```

Content-Type: text/html; charset=utf-8
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server:
Content-Security-Policy: default-src 'none'; script-src 'self' 'nonce-ClRuref1W43fgfYiUnzAGA==' 'strict-dynamic' https;; style-src 'self' 'unsafe-inline'; img-src 'self' data: blob;; connect-src
'self'; font-src 'self'; frame-src 'self'; frame-ancestors 'self'; form-action 'self'; media-src 'self'; object-src 'none'; base-uri 'self'; manifest-src 'self'; worker-src
'self'; script-src-attr 'none';
X-Frame-Options: DENY
X-XSS-Protection: 1; mode=block

```

說明及佐證：

CSP 設定為最新第三版要求

```

Content-Security-Policy: default-src 'none'; script-src 'nonce-gbLTli57SZHUK4H1boVt4g==' 'strict-
dynamic' https;; style-src 'self' 'unsafe-inline'; img-src 'self' data: blob;; connect-src
'self'; font-src 'self'; frame-src 'self'; frame-ancestors 'self'; form-action 'self'; media-src 'self'; object-src 'none';
base-uri 'self'; manifest-src 'self'; worker-src 'self'; script-src-attr 'none';

```

預設全部為 none，script 僅開放 nonce 與 strict-dynamic(嚴格)，依據 Google CSP Evaluator 檢查，符合最新第三版的資安檢查，如下圖。

csp-evaluator.withgoogle.com

Content Security Policy

[Sample unsafe policy](#) [Sample safe policy](#)

```
Content-Security-Policy: default-src 'none'; script-src
'nonce-gbLTli57SZHUK4H1boVt4g==' 'strict-dynamic' https;; style-src
'self' 'unsafe-inline'; img-src 'self' data: blob;; connect-src
'self'; font-src 'self'; frame-src 'self'; frame-ancestors 'self';
form-action 'self'; media-src 'self'; object-src 'none'; base-uri
'self'; manifest-src 'self'; worker-src 'self'; script-src-attr
'none';
```

CSP Version 3

CHECK CSP

Evaluated CSP as seen by a browser supporting CSP Version 3

[expand/collapse all](#)

- ✓ default-src
- ✓ script-src
- ✓ style-src
- ✓ img-src
- ✓ connect-src
- ✓ font-src
- ✓ frame-src
- ✓ frame-ancestors
- ✓ form-action
- ✓ media-src
- ✓ object-src
- ✓ base-uri
- ✓ manifest-src
- ✓ worker-src
- ✓ script-src-attr

```
C:\Users\confl>curl -I [redacted]
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 0
Content-Type: text/html; charset=utf-8
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server:
Content-Security-Policy: default-src 'none'; script-src 'nonce-83blmrJ0RHWgce3eOntPFg==' 'strict-dynamic' https;; style
-src 'self' 'unsafe-inline'; img-src 'self' data: blob;; connect-src 'self'; font-src 'self'; frame-src 'self'; frame-an
cestors 'self'; form-action 'self'; media-src 'self'; object-src 'none'; base-uri 'self'; manifest-src 'self'; worker-sr
c 'self'; script-src-attr 'none';
Set-Cookie: PHPSESSID=leu7ov9jt9ek0nsjtpq7mlg9c8; path=/; samesite=Strict; secure; HttpOnly
X-Frame-Options: DENY
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Referrer-Policy: Strict-origin-when-cross-origin
Permissions-Policy: accelerometer=(self), camera=(self), geolocation=(self), gyroscope=(self), magnetometer=(self), micr
ophone=(self), payment=(self), usb=(self)
Date: Mon, 24 Nov 2025 04:43:22 GMT
```

序號 3 佐證資料：在 CSP 中未強制執行腳本中的可信類型

檢測結果：

```
Server:
Content-Security-Policy: default-src 'none'; script-src 'self' 'nonce-Ea+CKr0gQ65c6DH9T8BtVA='; style-src 'self' 'unsafe-inline'; img-src 'self' data: blob;; connect-src
'self'; font-src 'self'; frame-src 'self'; frame-ancestors 'self'; form-action 'self'; media-src 'self'; object-src 'none'; base-uri 'self'; manifest-src 'self'; worker-src
'self'; script-src-attr 'none';
```

說明及佐證：

CSP 設定為最新第三版要求

```
default-src 'none'; script-src 'nonce-BhPnNPLNO1gIjKucUGGLlw==' 'strict-dynamic' https:; style-src 'self'
'unsafe-inline'; img-src 'self' data: blob;; connect-src 'self'; font-src 'self'; frame-src 'self'; frame-
ancestors 'self'; form-action 'self'; media-src 'self'; object-src 'none'; base-uri 'self'; manifest-src 'self';
worker-src 'self'; script-src-attr 'none'; trusted-types default; require-trusted-types-for 'script';
```

預設全部為 none，script 僅開放 nonce 與 strict-dynamic(嚴格)，並加上可信類型 trusted-types default; require-trusted-types-for 'script';，依據 Google CSP Evaluator 檢查，符合最新第三版的資安檢查，如下圖。

csp-evaluator.withgoogle.com

Content Security Policy

[Sample unsafe policy](#) [Sample safe policy](#)

```
default-src 'none'; script-src 'nonce-BhPnNPLNO1gIjKucUGGLlw=='
'strict-dynamic' https;; style-src 'self' 'unsafe-inline'; img-src
'self' data: blob;; connect-src 'self'; font-src 'self'; frame-src
'self'; frame-ancestors 'self'; form-action 'self'; media-src
'self'; object-src 'none'; base-uri 'self'; manifest-src 'self';
worker-src 'self'; script-src-attr 'none'; trusted-types default;
require-trusted-types-for 'script';
```

CSP Version 3

CHECK CSP

Evaluated CSP as seen by a browser supporting CSP Version 3

[expand/collapse all](#)

- ✓ default-src
- ✓ script-src
- ✓ style-src
- ✓ img-src
- ✓ connect-src
- ✓ font-src
- ✓ frame-src
- ✓ frame-ancestors
- ✓ form-action
- ✓ media-src
- ✓ object-src
- ✓ base-uri
- ✓ manifest-src
- ✓ worker-src
- ✓ script-src-attr
- ✓ trusted-types
- ✓ require-trusted-types-for

```
C:\Users\confl>curl -I h[redacted]
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 0
Content-Type: text/html; charset=utf-8
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server:
Content-Security-Policy: default-src 'none'; script-src 'nonce-gbLTli57SZHUK4H1boVt4g==' 'strict-dynamic' https;; style
-src 'self' 'unsafe-inline'; img-src 'self' data: blob;; connect-src 'self'; font-src 'self'; frame-src 'self'; frame-an
cestors 'self'; form-action 'self'; media-src 'self'; object-src 'none'; base-uri 'self'; manifest-src 'self'; worker-sr
c 'self'; script-src-attr 'none';
Set-Cookie: PHPSESSID=cith0iki55uf6au19fbonggp2o; path=/; samesite=Strict; secure; HttpOnly
X-Frame-Options: DENY
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Referrer-Policy: Strict-origin-when-cross-origin
Permissions-Policy: accelerometer=(self), camera=(self), geolocation=(self), gyroscope=(self), magnetometer=(self), micr
ophone=(self), payment=(self), usb=(self)
Date: Mon, 24 Nov 2025 04:43:06 GMT
```

序號 4 佐證資料：遺漏「Content-Security-Policy」標頭

檢測結果：

```
GET /plugins/jquery-ui/jquery-ui.min.js HTTP/1.1
Host: [REDACTED]
Connection: [REDACTED]
sec-ch-ua: [REDACTED]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessChrome/138.0.0.0 Safari/537.36
sec-ch-ua: "(Not)A;Brand";v="8", "Chromium";v="138"
sec-ch-ua-mobile: ?0
Accept: */*
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Referer: [REDACTED]
Accept-Language: [REDACTED]
Cookie: [REDACTED]
Content-Length: 0

HTTP/1.1 200 OK
Content-Type: application/javascript
Last-Modified: Mon, 26 Sep 2022 01:51:44 GMT
Accept-Ranges: bytes
ETag: "07896874ad1d81:0"
Server:
X-Frame-Options: DENY
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Referrer-Policy: Strict-origin-when-cross-origin
Permissions-Policy: accelerometer=(self), camera=(self), geolocation=(self), gyroscope=(self), magnetometer=(self), microphone=(self), payment=(self), usb=(self)
Date: Fri, 21 Nov 2025 09:27:00 GMT
Content-Length: 255079
```

說明及佐證：

Web.config 補上 HTTP 回應標頭，新增最安全的互通版本(主程式之 CSP 建立於 index.php 中)

```
Content-Security-Policy: default-src 'none';style-src 'self' 'unsafe-inline';img-src 'self' data:;font-src 'self';media-src 'self';object-src 'none';frame-ancestors 'self';base-uri 'self';
```

預設全部為 none，依據 Google CSP Evaluator 檢查，符合最新第三版的資安檢查，如下圖。

Content Security Policy

[Sample unsafe policy](#)

[Sample safe policy](#)

```
Content-Security-Policy: default-src 'none'; style-src 'self'
'unsafe-inline'; img-src 'self' data:; font-src 'self'; media-src
'self'; object-src 'none'; frame-ancestors 'self'; base-uri 'self';
```

CSP Version 3 ▼ ?

CHECK CSP

Evaluated CSP as seen by a browser supporting CSP Version 3

[expand/collapse all](#)

- ✓ **default-src** ▼

- ✓ **style-src** ▼

- ✓ **img-src** ▼

- ✓ **font-src** ▼

- ✓ **media-src** ▼

- ✓ **object-src** ▼

- ✓ **frame-ancestors** ▼

- ✓ **base-uri** ▼

```
C:\Users\confl>curl -I https://[redacted]/jquery-ui.min.js
HTTP/1.1 200 OK
Content-Length: 255079
Content-Type: application/javascript
Last-Modified: Mon, 26 Sep 2022 01:51:44 GMT
Accept-Ranges: bytes
ETag: "07896874ad1d81:0"
Server:
Content-Security-Policy: default-src 'none'; style-src 'self' 'unsafe-inline';
img-src 'self' data:; font-src 'self'; media-src 'self';
object-src 'none'; frame-ancestors 'self'; base-uri 'self';
X-Frame-Options: DENY
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Referrer-Policy: Strict-origin-when-cross-origin
Permissions-Policy: accelerometer=(self), camera=(self), geolocation=(self), gyroscope=(self), magnetometer=(self), microphone=(self), payment=(self), usb=(self)
Date: Mon, 24 Nov 2025 08:24:18 GMT
```