

112年教育體系資安攻防 演練成果報告

網路系統組
邱惠隆



背景

- 教育部於112年底對**全國國立47所大專院校網頁**進行資安攻防演練，以了解演練機關的**資安防護與應變處理能力**。

- 演練實施時間:

- **第一階段:112/11/27~112/12/29(僅上班日)**
- **第二階段(複測):113/1/8-113/1/26 (針對有中
高以上風險，進行複測)**



112年教育體系資安攻防演練成果

- 此次本校繳交網站清冊共計有**572筆** (各單位提供)
 - 共計有發現**44筆網站漏洞**。
 - 其中**2筆**不是已繳交清冊的網站。
- 全國總共有**741件**漏洞，平均每所大學**15.8件**。
 - 本校的數量大約是其他學校的**2.8倍**!

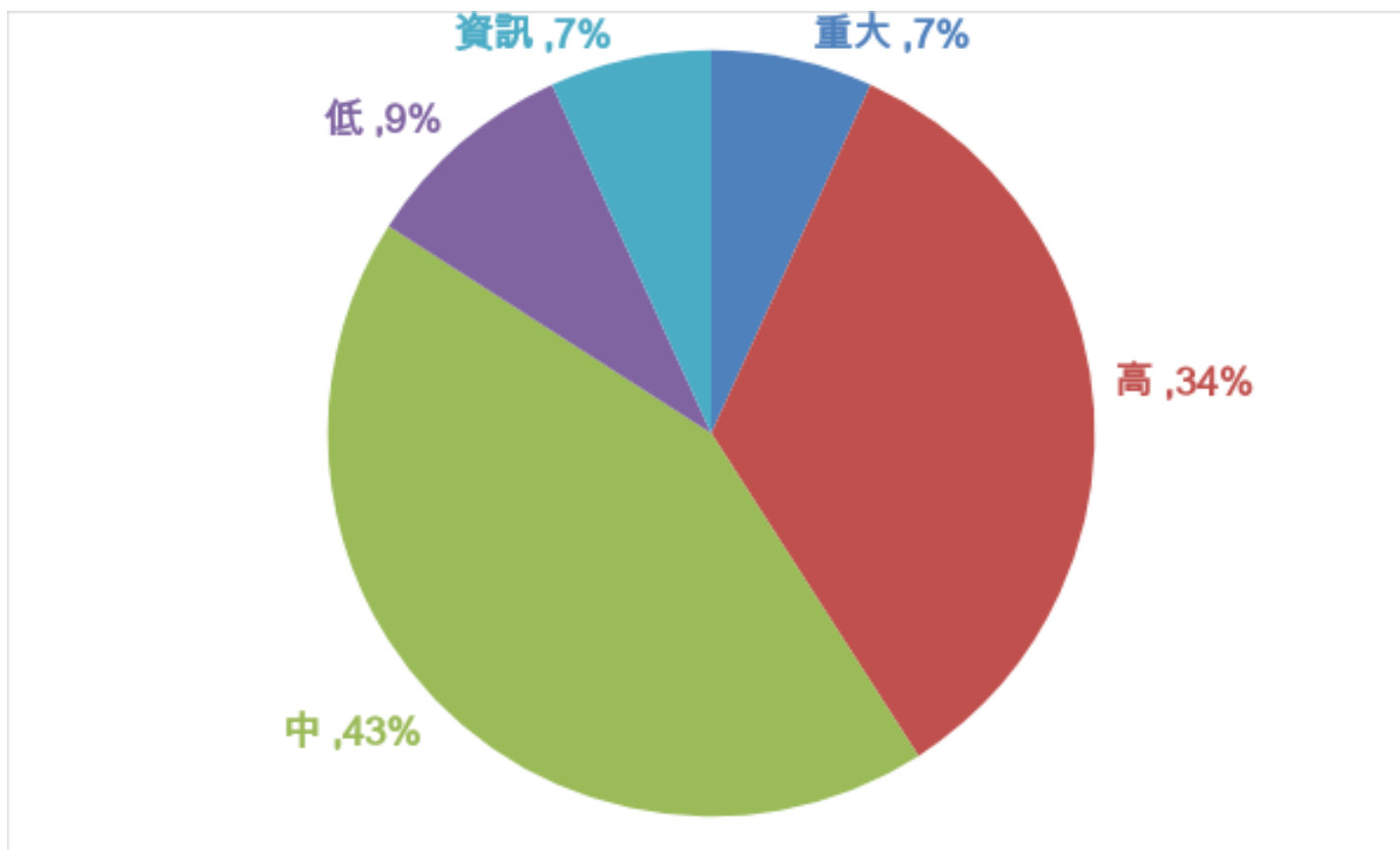


中大漏洞統計

弱點名稱	衝擊性	弱點數量	百分比	小計
伺服器請求偽造	中	14	31.82%	14
SQL Injection	重大	2	4.55%	11
	高	4	9.09%	
	中	5	11.36%	
權限控制失效	重大	1	2.27%	9
	高	7	15.91%	
	低	1	2.27%	
安全設定缺陷	低	1	2.27%	4
	資訊	3	6.82%	
XSS	高	2	4.55%	4
	低	2	4.55%	
命令注入	高	1	2.27%	1
認證及驗證機制失效	高	1	2.27%	1
合計			100%	44



中大漏洞衝擊性比例統計





xmlrpc SSRF 弱點(伺服器請求偽造)

- ❑ [XML-RPC](#) 是 [WordPress](#) 提供對外遠端程式呼叫 (Remote Procedure Call ; RPC) 的 API 接口，可提供外部系統透過 XML-RPC API 執行遠端發文管理。
- ❑ 常用外部服務例如 Blogger, metaWeblog, Movable Type 或是 Pingback 等等，可與 XML-RPC 串接服務。
- ❑ [XML-RPC](#) 使用 [http](#) 協定作為傳送機制，串接頁面為 [/xmlrpc.php](#)，在 3.5 版開始，預設會啟用此功能。
- ❑ WordPress 預設開啟對外 API 服務，同時也[潛藏著資安風險](#)，在 2014 年曾經發生過一次大規模的攻擊事件，是由 [XML-RPC](#) 漏洞所引起，[如果你的網站並沒有使用 XML-RPC 服務](#)，建議關閉 XML-RPC 服務以避免資安風險。



xmlrpc SSRF 弱點(伺服器請求偽造)

- Wordpress 版本過舊未更新

建議

- 定期更新Wordpress版本，並在.htaccess設定禁止對xmlrpc.php檔的訪問
 - protect xmlrpc Order Deny,Allow Deny from all
- 或刪除根目錄下的xmlrpc.php。



SQL injection案例(資料庫資料)

```
Parameter: cid (GET)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: cid=62' AND 8236=8236 AND 'FBTZ'='FBTZ

  Type: stacked queries
  Title: MySQL ≥ 5.0.12 stacked queries (comment)
  Payload: cid=62';SELECT SLEEP(5)#

  Type: time-based blind
  Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
  Payload: cid=62' AND (SELECT 4393 FROM (SELECT(SLEEP(5)))UHXu) AND 'xJkU'='xJkU

  Type: UNION query
  Title: Generic UNION query (NULL) - 10 columns
  Payload: cid=-9586' UNION ALL SELECT NULL,CONCAT(0x71706b7171,0x6e56426264597a5773504d7267871),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL-- -

[13:24:44] [INFO] the back-end DBMS is MySQL
web server operating system: Windows 10 or 11 or 2016 or 2019 or 2022
web application technology: Microsoft IIS 10.0, ASP.NET 4.0.30319, ASP.NET
back-end DBMS: MySQL ≥ 5.0.12
[13:24:51] [INFO] fetching current database
current database: 'a[REDACTED]nt'
[13:24:52] [INFO] fetched data logged to text files under '/home/code/.local/share/sqlmap/out'
```




SQL injection防護措施參考

➤ Defense in Depth (縱深防禦)

- 輸入淨化 (input sanitization)
- 輸入驗證 (input validation)
- 參數化查詢 (prepared statement)
- 最小權限原則 (Principle of Least Privilege)
- 使用 WAF (Web Application Firewall) 防護
- 安全程式設計及開發 (SSDLC)

建議:

• 系統開發者

- 對使用者輸入內容進行嚴格過濾，或採用白名單機制過濾使用者輸入內容。
- 改以參數化形式傳值，避免SQL語句被竄改或截斷。



XSS防護參考

➤ Output Encoding (輸出前先做編碼)

Character	Entity Encoding
"	"
&	&
'	'
<	<
>	>

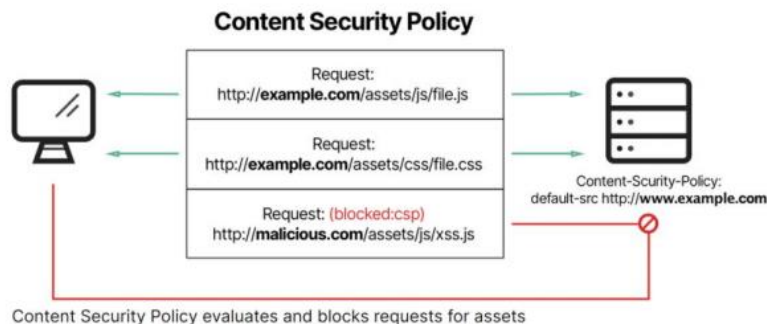
```
<div class="comment">  
<script>alert("XSS")</script>  
</div>
```



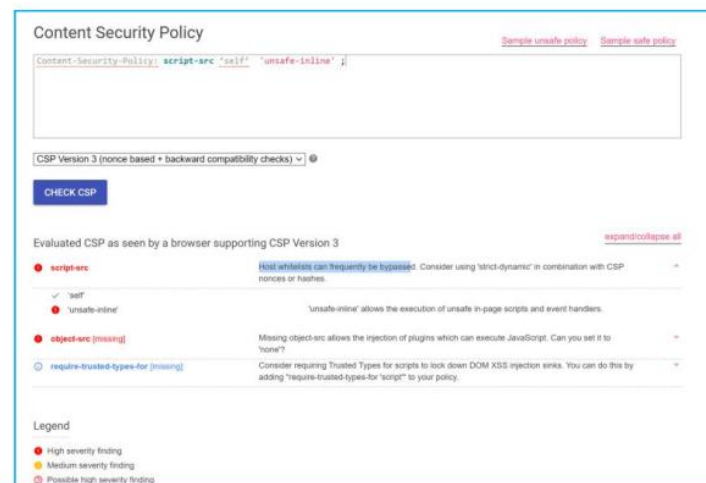
```
<div class="comment">  
&lt;script&gt;alert(&quot;XSS&quot;)&lt;/script&gt;  
</div>
```

XSS防護參考

- **Cookie設定HttpOnly屬性**
 - 無法以JavaScript讀取Cookie值
- **設定Content Security Policy**
 - <https://content-security-policy.com/>

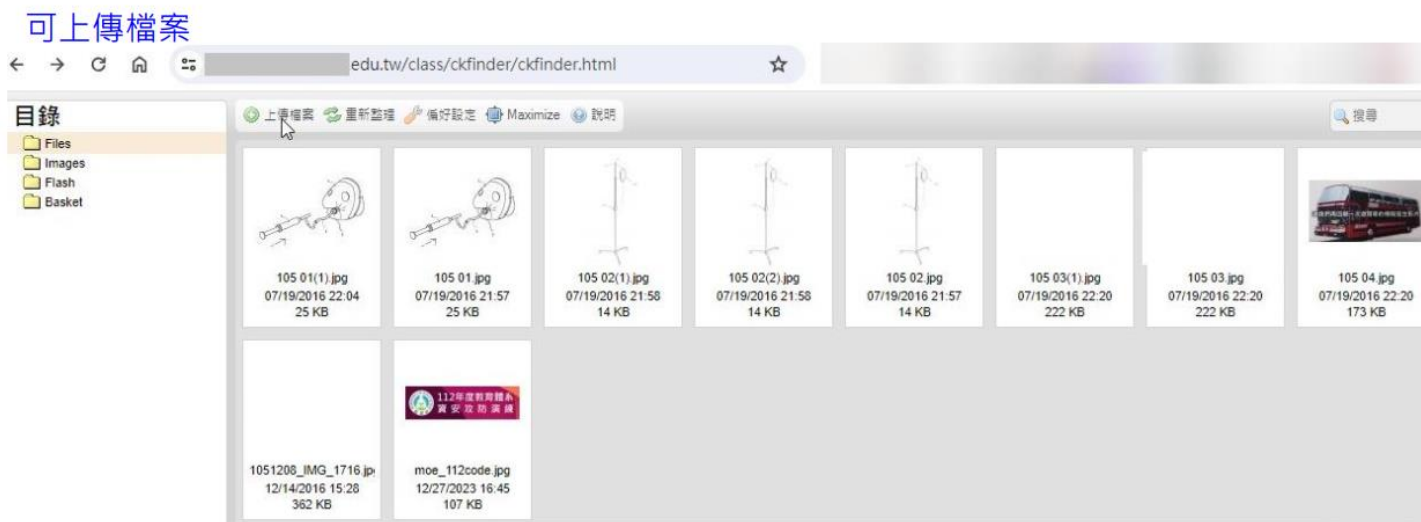


- **CSP 設定不正確，存在可能被繞過風險**
- <https://csp-evaluator.withgoogle.com/>





通過CKFinder漏洞獲取敏感信息



建議:

- **系統開發者**
 - 針對網頁套件之預設路徑進行更改，避免攻擊者可輕易猜測路徑進行存取。
- **系統管理者**
 - 應限制功能頁面之存取來源，若為外部使用者不需使用之功能，應禁止由外部存取該頁面。
 - 應避免直接由外網存取系統管理介面，應統一透過內網或透過VPN連線後，進行系統管理介面操作。



其他相關改善方法

建議:

- **檢視已存在弱密碼問題之系統帳號並定期變更機制**
 - 系統管理權限之帳號須立即變更密碼，且強度至少8碼以上，須符合大小寫英文、數字與符號，四種達成3種以上之高強度密碼。
 - 從系統面重新設計，每180天要求使用者變更密碼，於30至5天前發送系統信件通知且不得符合前3次密碼內容。
- **檢視已存在注入攻擊的程式**
 - 採用參數化 (Parameterized) 查詢語法並且加強對用戶輸入資料的檢核與驗證；使用最小權限原則 (Principle of Least Privilege)存取資料庫。
- **檢視已存在XSS的程式並使用工具加強檢查注入及XSS等漏洞**
 - 採取輸出前先做編碼，Cookie設定HttpOnly屬性及設定Content Security Policy原則
 - 使用專業的程式碼弱點掃描工具來尋找應用系統所隱含的漏洞，重要系統使用 WAF (Web Application Firewall) 防護。。



其他相關改善方法(續)

建議:

- 伺服器請求偽造點、權限控制失效及安全設定缺陷排除
 - 檢查系統，移除敏感個資或惡意程式並設定資料夾瀏覽權限及存取來源，關閉不需要的檔案(如phpinfo)與顯示模式，減少資訊暴露的風險。
- 採用SSDLC開發系統
 - 使用安全的軟體發展生命週期開發系統。
- 進行系統清點
 - 針對不需要存在的網站及系統，建議將其關閉下線。
- 進行教育訓練
 - 針對管理及開發人員進行網站建置的安全觀念宣導，隨時進行資安防護，定期更新系統及相關套件。



資安攻防演練分數

□ 112年資安攻防演練中大的分數如下:

類別	項目	結果	分數
系統盤點能力(10%)	調查表正確率	$[572/(572+2)]*5$	5
	調查表回復時間	提早 1 日 16 時 33 分	5
通報應變作業(30%)	應變處置時間	事件應變處置時間： 2 日 3 時 6 分	30
防護能力(50%)	重大衝擊性弱點比例	$[1 - (3 / 572)] * 20$	19.9
	高衝擊性弱點比例	$[1 - (15 / 572)] * 15$	14.6
	中衝擊性弱點比例	$[1 - (14 / 572)] * 10$	9.8
	低衝擊性弱點比例	$[1 - (3 / 572)] * 5$	5
弱點複測(10%)	複測通過率		10
總計			99.3



113年資安攻防演練時程

113年資安攻防演練:

- 預計於今年(113)7月~9月施實，敬請各單位提早準備。(詳情以教育部來文為主)



感謝演練期間“ SNMG成員” 及“
各單位網頁管理員” 等相關人員的即
時處理與回覆。

資安防護並非一人、二人就可以達成!
需要您/我/他，大家一起努力。



Computer Center, National Central University.



Thank You!