教育部
Ministry of Education

教育體系資通安全防護巡迴研討會

教育體系資安威脅與重要政策說明

111年5月

(公開用版本)

大綱

1. 教育體系資通安全威脅趨勢
2. 本部重要資通安全政策說明
3. 教育體系重大資通安全事件案例分享
4. 結論與建議

1.教育體系資通安全威脅趨勢

1.1 教育體系資安威脅現況

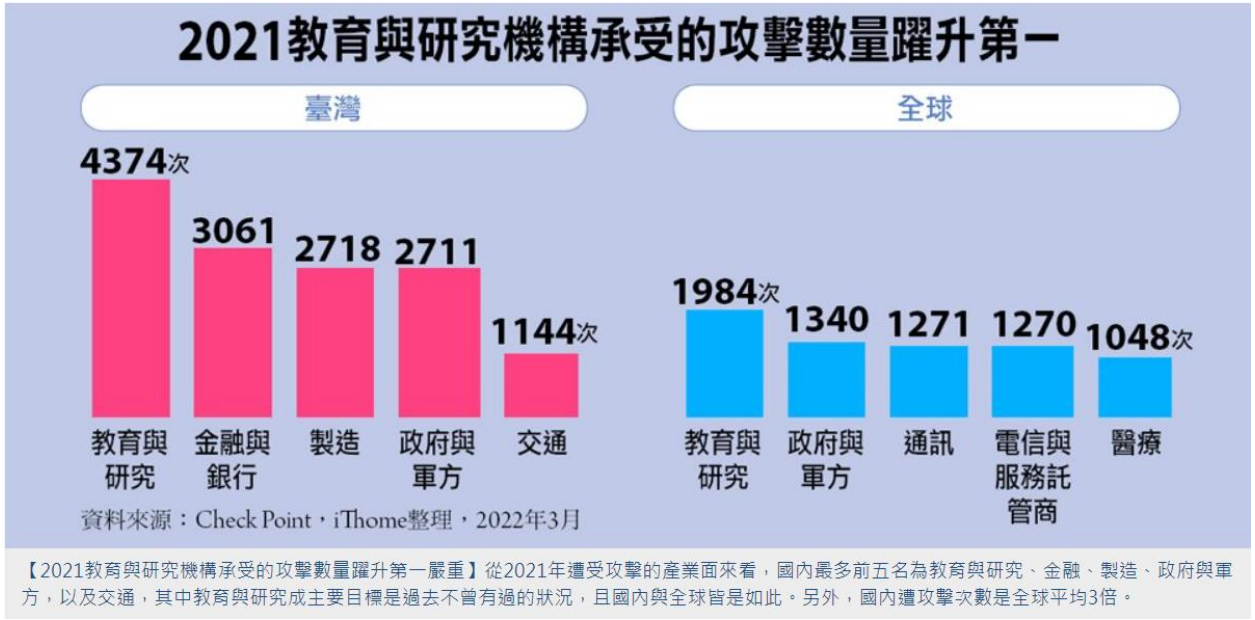
1.2 教育體系資安事件趨勢

1.1 教育體系資安威脅現況

- 教育體系資安威脅持續上升
- 重大資安漏洞頻傳

教育體系資安威脅持續上升(1/2)

- 依據資安業者統計：(Check Point 110年全球威脅趨勢回顧報告)
  - ➢**臺灣110年每週平均遭受攻擊**次數，依產業別，以**教育與研究機構最多**(4,374次)。
  - ➢**全球110年**亦同(教育與研究機構最多)，且**比前一年度增長75%**。



【2021教育與研究機構承受的攻擊數量躍升第一嚴重】從2021年遭受攻擊的產業面來看，國內最多前五名為教育與研究、金融、製造、政府與軍方，以及交通，其中教育與研究成主要目標是過去不曾有過的狀況，且國內與全球皆是如此。另外，國內遭攻擊次數是全球平均3倍。

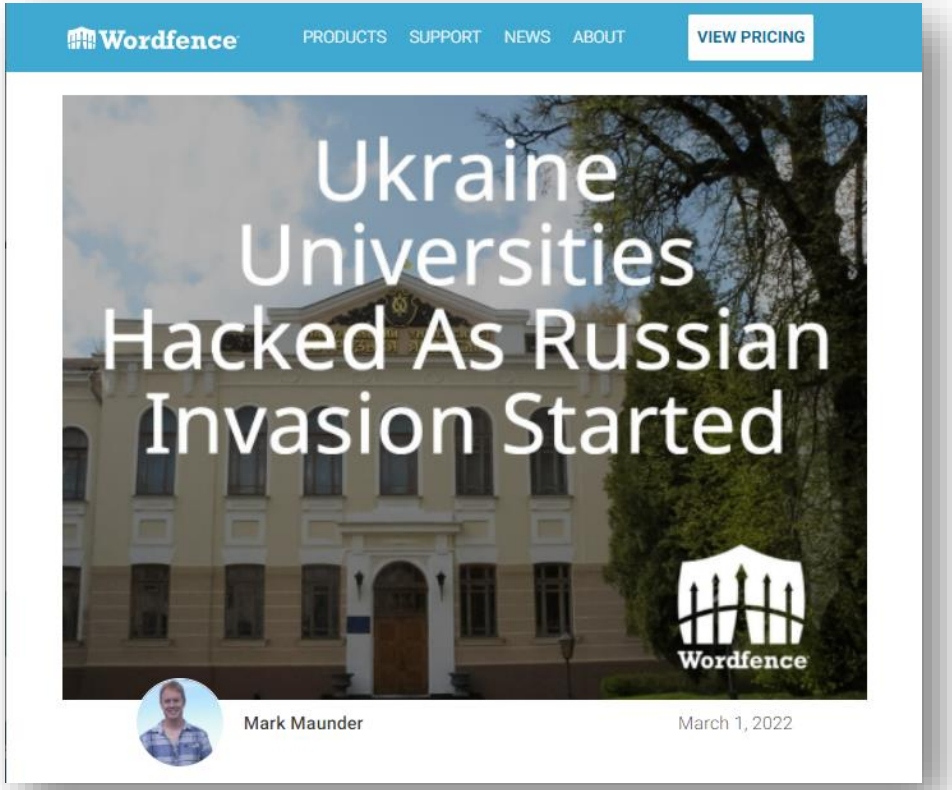
資料來源: iThome 111/3/16 報導，
https://www.ithome.com.tw/news/149919

教育體系資安威脅持續上升(2/2)

- 國家/地區間發生衝突時，教育機構經常**首當其衝**。
  - ➢**俄烏戰爭**爆發後，至少30所烏克蘭**大學網站**遭到駭客**入侵**，包含網頁被惡置換(插旗)情形。

Date	Notifier	H	M	R	L	★	Domain	OS
2022/03/10	theMx0nday	H	M				vstup.oa.edu.ua	FreeBSD
2022/03/10	theMx0nday	H	M				consulting.vbs.oa.edu.ua	FreeBSD
2022/03/10	theMx0nday	H	M				db.lib.oa.edu.ua	FreeBSD
2022/03/10	theMx0nday	H	M				events.oa.edu.ua	FreeBSD
2022/03/10	theMx0nday	H	M				gw.oa.edu.ua	FreeBSD
2022/03/10	theMx0nday	H	M				handbook.oa.edu.ua	FreeBSD
2022/03/10	theMx0nday	H	M				hrampfo.oa.edu.ua	FreeBSD
2022/03/10	theMx0nday	H	M				igsu.oa.edu.ua	FreeBSD
2022/03/10	theMx0nday	H	M				iirns.oa.edu.ua	FreeBSD
2022/03/10	theMx0nday	H	M				incgc.oa.edu.ua	FreeBSD

資料來源: http://www.zone-h.org/archive



資料來源: https://reurl.cc/anlZV7

重大資安漏洞頻傳(1/2)

(情資發布編號：NCCST-ANA-2021-0000411、TACERT-ANA-2021091503093939)

- **CVE-2021-40444**
  (CVSS 3.0評分8.8分)
  - 微軟Windows之**瀏覽器排版引擎MSHTML存在安全漏洞**，攻擊者可誘騙使用者開啟含有**惡意ActiveX之Office文件**，進而載入瀏覽器引擎並瀏覽惡意網頁，利用此漏洞**遠端執行任意程式碼**(RCE)。
  - 駭客可藉由搭配**社交工程**信件開採此弱點。

資料來源: iThome 110/9/17 報導，
https://www.ithome.com.tw/news/146764，

重大資安漏洞頻傳(2/2)

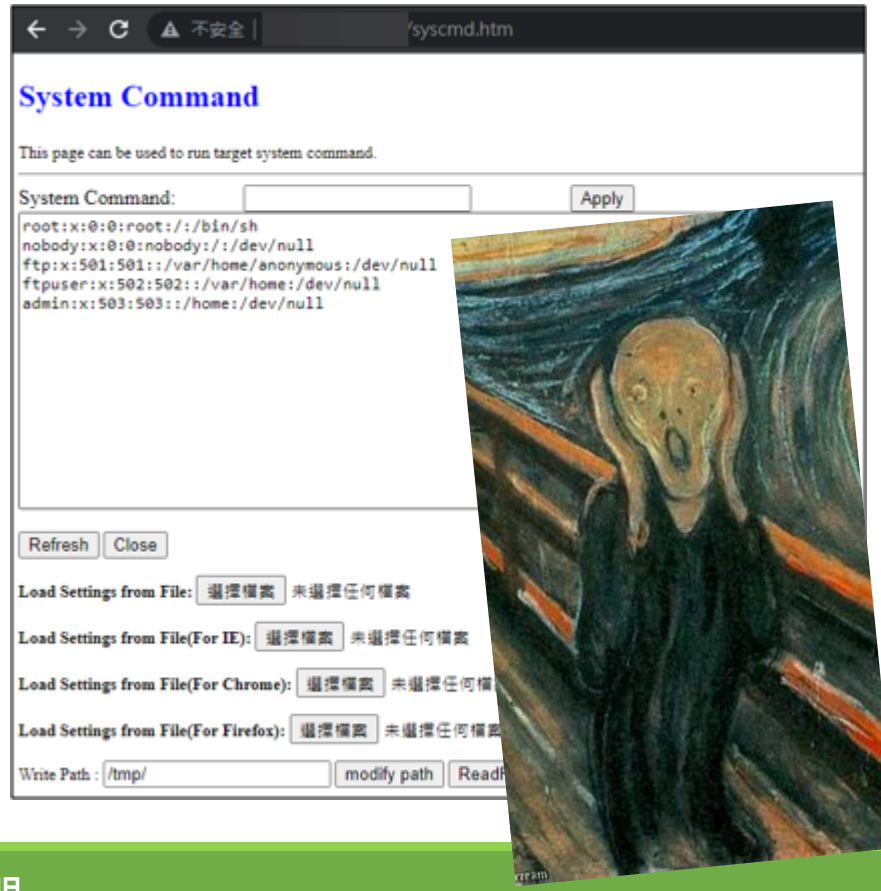
(情資發布編號：NCCST-ANA-2021-0000637、TACERT-ANA-2021091503093939)

- Log4Shell(CVE-2021-44228等)
  (CVSS 3.0評分10.0分)
  - Apache Log4j(Java日誌記錄工具)存在安全漏洞，攻擊者可藉由發送特製 JNDI lookup 訊息，利用漏洞進而遠端執行任意程式碼(RCE)或洩露資訊。
  - 相關弱點已被中國網軍運用於實戰，用以入侵政府網路(如圖)。

資料來源: iThome 111/3/9 報導，
https://www.ithome.com.tw/news/146654

但古老的資安漏洞也仍未處理...

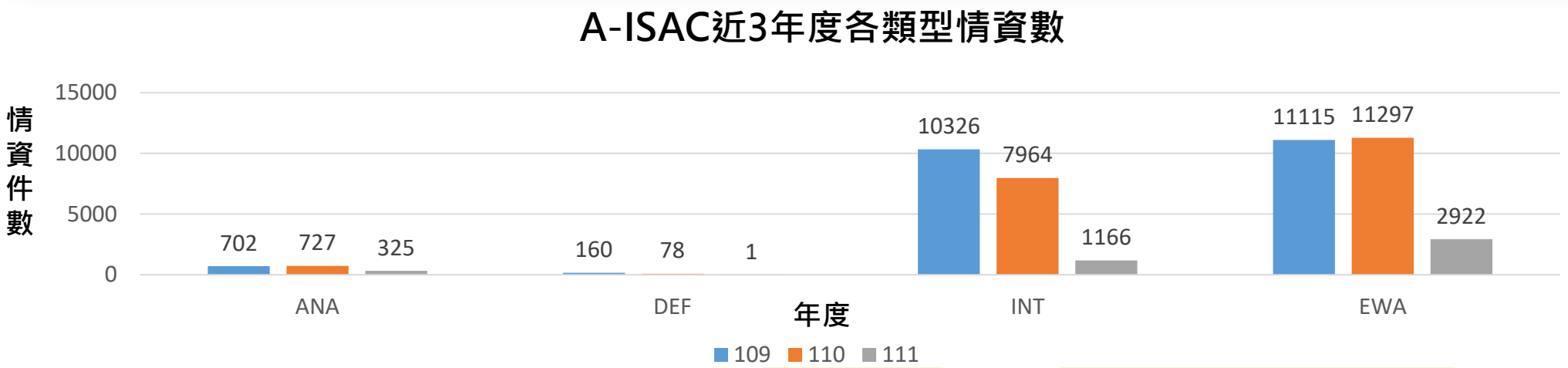
- 教育機構針對部分系統、設備**古老且重大**的資安**漏洞仍未處理**，且其**曝露於外網**。
- **CVE-2019-19822~19823**
  (CVSS 3.0評分7.5分)
  - 行政院國家資通安全會報技術服務中心於110年12月使用 Shodan 掃描臺灣 Sapido(傻多)系列AP無線分享器產品，發現**教育領域**有**40臺**設備具**遠端程式碼執行漏洞**或**預設密碼弱點**。



1.2 教育體系資安事件趨勢

- A-ISAC通報教育體系資安情資數量
- A-ISAC通報教育體系資安事件類型
- 外部單位通報資安威脅情資
- 教育體系重大資安事件激增

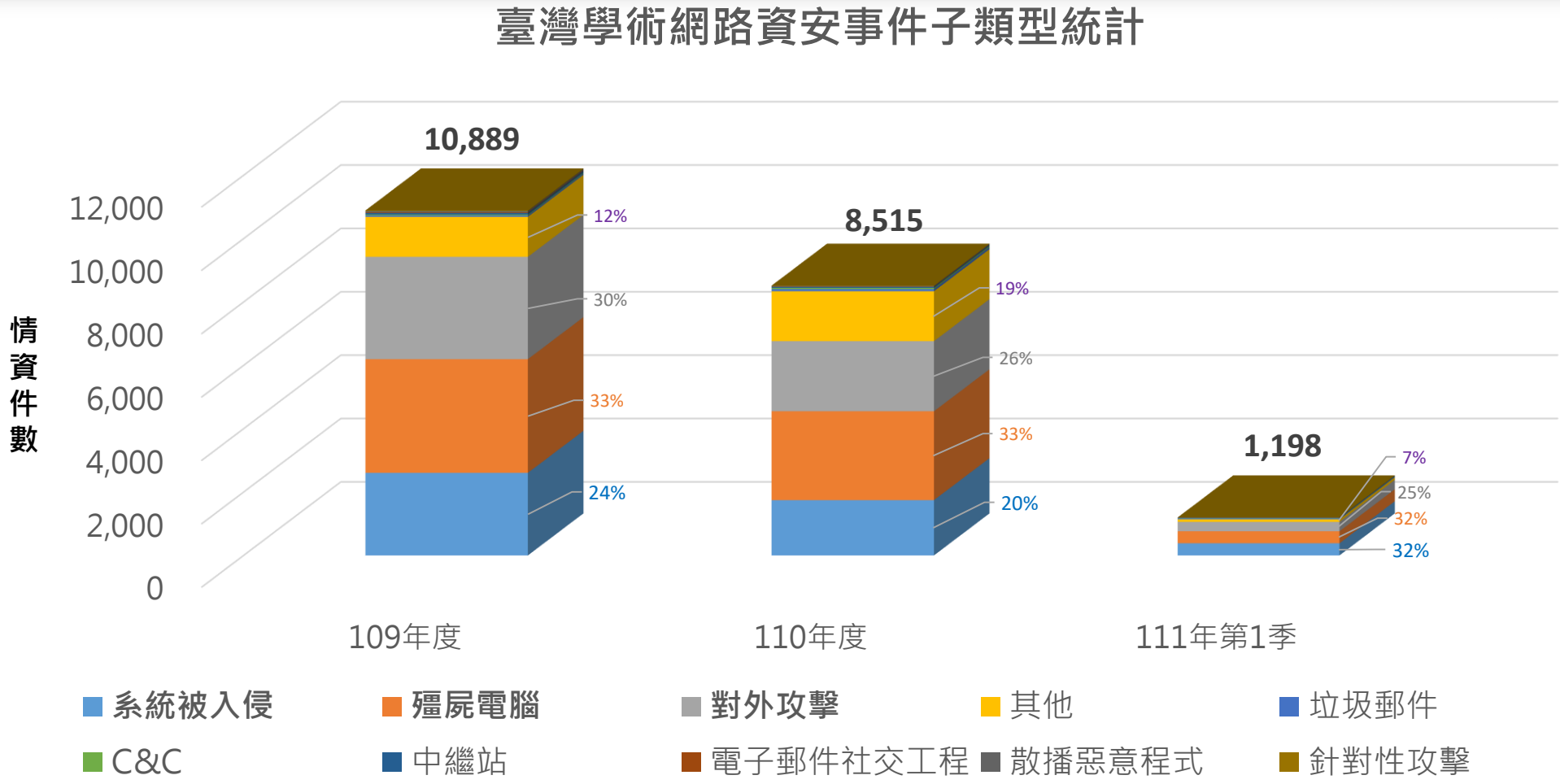
A-ISAC通報教育體系資安情資數量



資安事件　　疑似資安事件(需確認)

情資類型 / 年度	ANA	DEF	INT	EWA	件數合計
109年	702	160	10326	11115	22303
110年	727	78	7964	11297	20066
111年第1季	325	1	1166	1430	2922

A-ISAC通報教育體系資安事件類型



外部單位通報資安威脅情資(1/2)

- 法務部**調查局**資安**威脅情資**通報

➢法務部調查局為執行安全防護工作，**110年起至今**針對**教育體系**已通報**36件**資安情資威脅，包含下列型態：

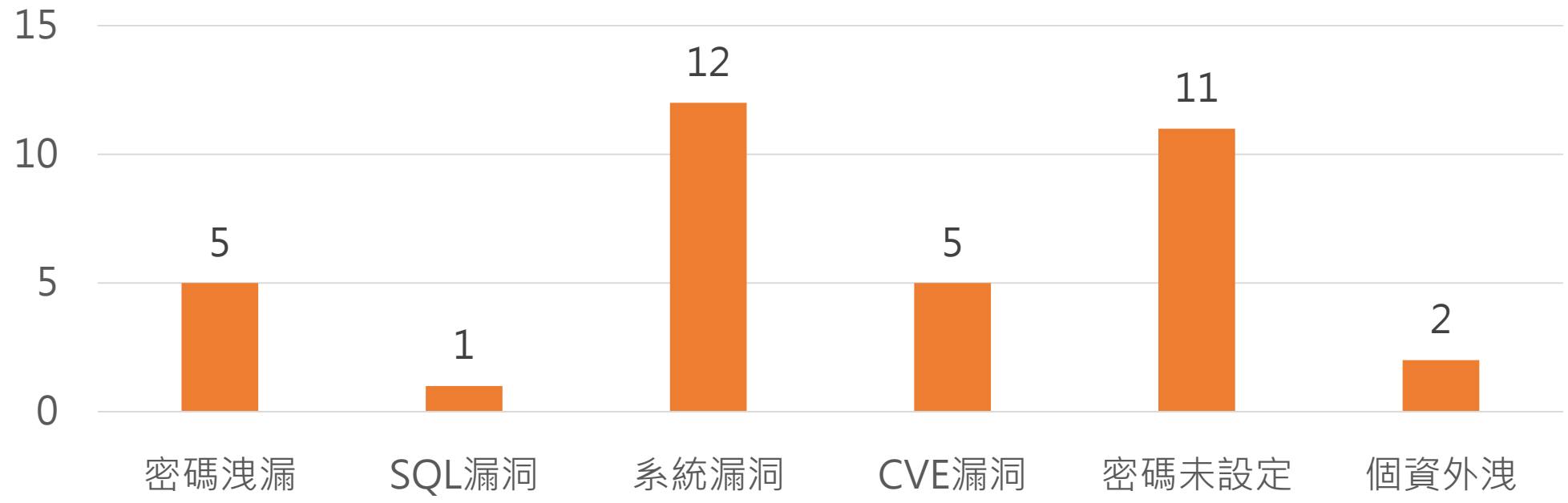
■**網站遭駭**。

■**網站設計漏洞**。

■物聯網(**IoT**)設備安全問題，且通報數量以**網路印表機**、**網路攝影機**數量最多(**管理員**權限帳號的**密碼未設定**)。

外部單位通報資安威脅情資(2/2)

➢調查局提供威脅情資，依其**弱點分類**如下：

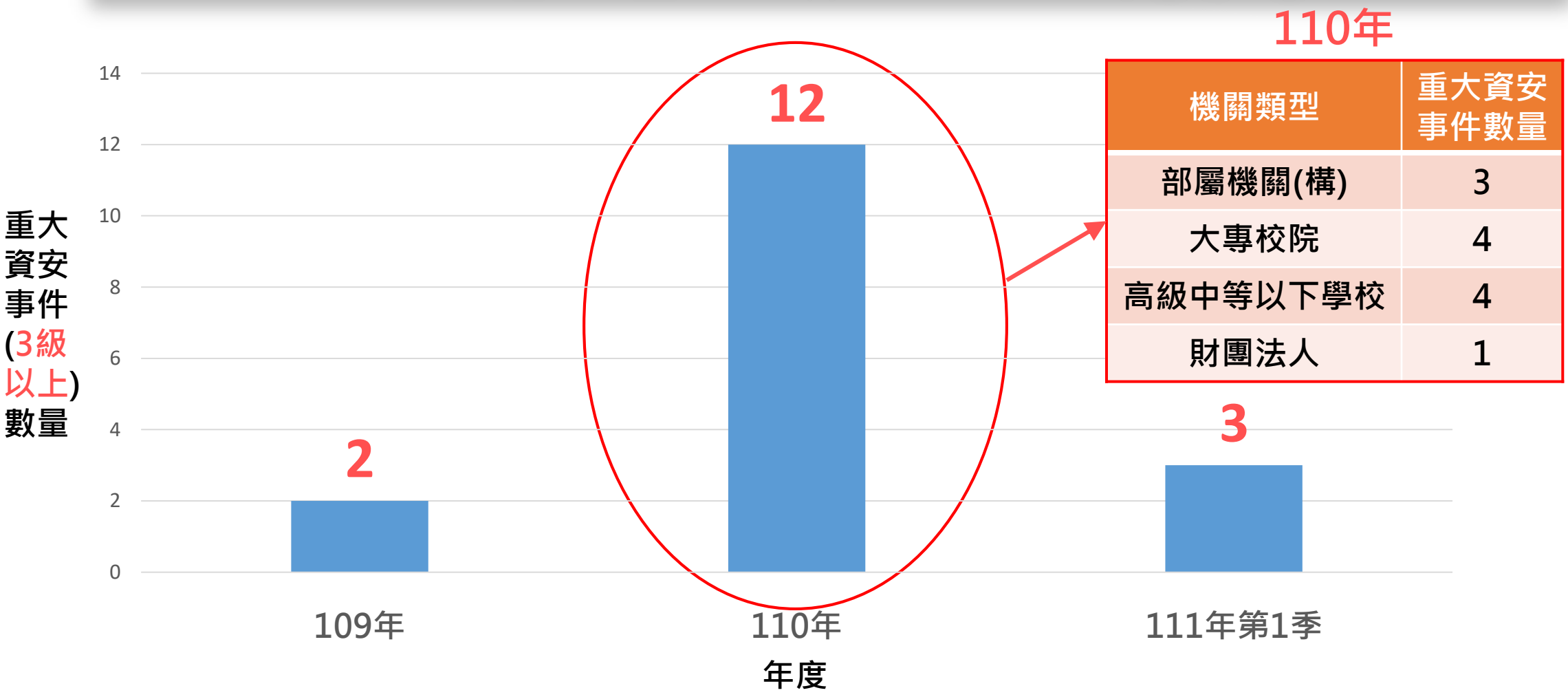


教育體系重大資安事件激增(1/2)

- 行政院資安處針對**近年政府機關**資安現況揭露：
  - ➢**重大資安事件通報**，以**教育體系最多**。
  - ➢有15件與**人為疏失**有關，突顯最大的問題是在資安**管理與落實面**。另有2件是駭客入侵。

資料來源: iThome 110/12/17 報導，
https://www.ithome.com.tw/news/148431

教育體系重大資安事件激增(2/2)



110年

機關類型	重大資安事件數量
部屬機關(構)	3
大專校院	4
高級中等以下學校	4
財團法人	1

2.教育體系重要資通安全政策說明

2.1 推動全校導入資安管理制度
2.2 訂定資安相關作業指引
2.3 加強教育體系獎懲機制
2.4 其他相關政策規範

2.1 推動全校導入資安管理制度

- 學校應落實資通系統及資訊之盤點
- 國立大專校院資通安全維護作業指引

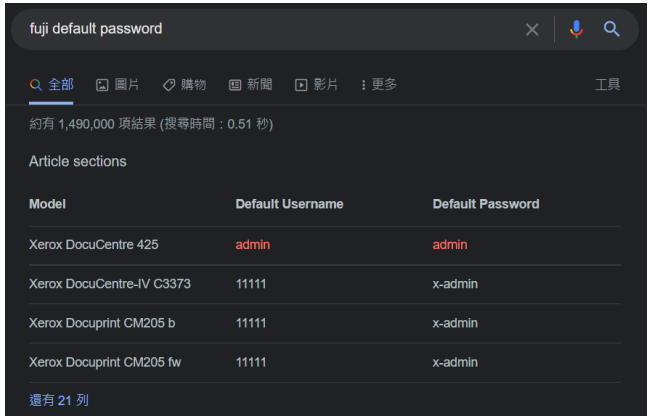
學校應落實資通系統及資訊之盤點(1/3)

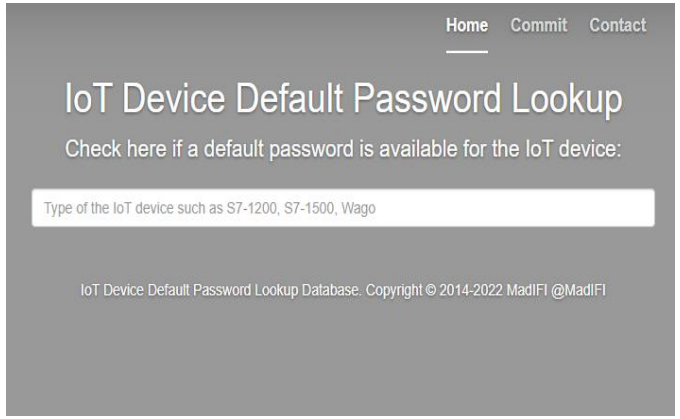
- 各校應依資安法相關規定，辦理下列安全防護及控制措施：
  - ➢落實**全校資通系統及資訊之盤點**。盤點範圍至少包含：
    - ■**行政、教學單位**自行或委外開發之資通系統。
    - ■**學校採購及公務使用之物聯網設備**(如網路印表機、網路攝影機、門禁設備、環控系統、無線網路基地台/無線路由器等)。

教育部110年9月22日臺教資(四)字第1100128345號函

學校應落實資通系統及資訊之盤點(2/3)

- 各校應依資安法相關規定，辦理下列安全防護及控制措施(續)：
  - ➢落實**全校資通安全風險評估**、資通安全防護及控制措施。
    - ■**不得使用弱密碼及廠商預設密碼**，並符合規範之**密碼複雜度要求**。
    - ■依業務需求設定適當網路**存取限制**。



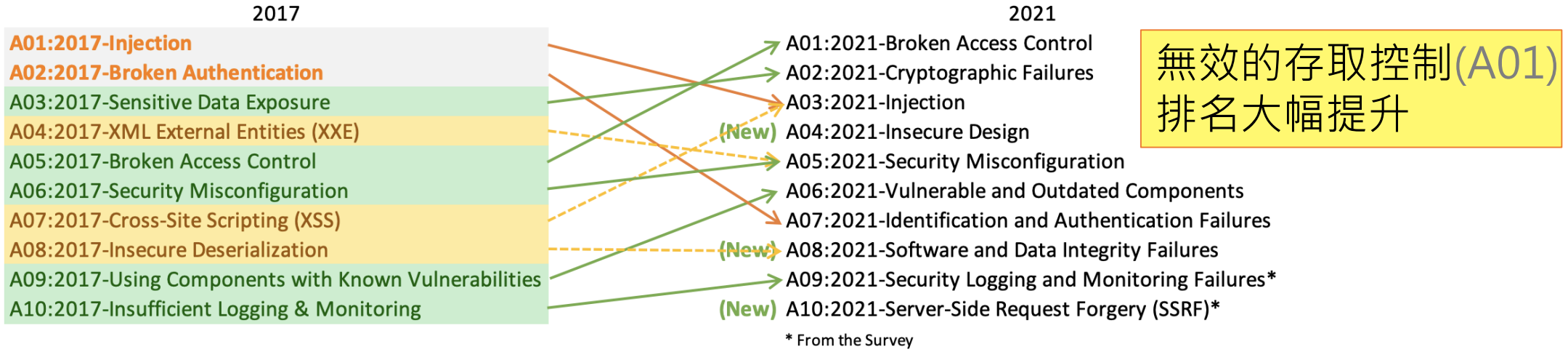


曝露在外網且使用廠商預設密碼 (Google等網站能輕易查找) 的IoT設備，幾乎等同沒有存取限制。

教育部110年9月22日臺教資(四)字第1100128345號函

學校應落實資通系統及資訊之盤點(3/3)

- 各校應依資安法相關規定，辦理下列安全防護及控制措施(續)：
  - 資通系統**避免軟體常見漏洞**(如Injection、XSS等OWASP Top 10安全弱點)，落實漏洞修復並定期更新。



無效的存取控制(A01)排名大幅提升

資料來源: https://owasp.org/Top10/zh_TW/

教育部110年9月22日臺教資(四)字第1100128345號函

國立大專校院資通安全維護作業指引(1/3)

- 鑒於近期教育體系發生多起**重大資安事件**，**根因分析**顯示各校資通安全維護計畫**施行範圍未涵蓋全校**。
  - ➢為強化教育體系資安環境，並推動全校落實資安法相關規定，訂定**國立大專校院資通安全維護作業指引**。
- 自111年起，前述作業指引之各款注意事項，列入資通安全維護計畫**實施情形審查重點**，各校執行成果納入次年度本部**績效型補助款**衡量指標計算。

教育部110年12月30日臺教資(四)字第1100179797號函

國立大專校院資通安全維護作業指引(2/3)

- 各校資通安全維護計畫**適用範圍應涵蓋全校**(各系、院、所教學單位及各行政單位)，並注意下列事項。

資安長之配置

宜指派**主任秘書以上人員**兼任。

資安推動組織

宜由**資通安全長**召集全校各單位主管或副主管組成，**每年至少召開會議1次**。

資通系統盤點

盤點範圍應包含**全校各單位**。

內部資安稽核

稽核範圍應包含**全校各單位**。

教育部110年12月30日臺教資(四)字第1100179797號函

國立大專校院資通安全維護作業指引(3/3)

資通系統盤點

- 各校每年提交之「**資通系統資產清冊**」**至少應包含**落於**各校IP網段內**、或使用**各校網域名稱**之資通系統。

內部資安稽核

- 各校得就資通系統(保有個人資料)風險高低、教學單位特性**評估訂定推動先後順序**，**分年分階段**規劃辦理，並**明訂於**各校資通安全**維護計畫**。

教育部110年12月30日臺教資(四)字第1100179797號函

2.2 訂定資安相關作業指引

- 資安管理相關作業指引

資安管理相關作業指引(1/2)

各級學校使用資通系統或服務蒐集及使用個人資料注意事項

教育部110年9月8日臺教資(四)字第1100122001號函

【 Google表單蒐集個人資料使用原則】
https://sites.google.com/email.nchu.edu.tw/g-form

蒐集最小化

蒐集個資**不得逾越**特定目的**必要範圍**，並應具有**合理關聯**。

最小授權

檔案存取權限，應採**最小權限原則**。依目的指派任務所需最小授權存取。

設定檢查

使用雲端資通服務，應**避免允許顯示其他使用者內容**，發布前應確實檢查相關設定。

加密傳輸

網路傳輸應採用HTTPS(TLS 1.2以上版本)加密傳輸。

加密儲存

特種個資或**敏感資料**，應以**加密方式儲存**。

資料銷毀

應訂個資保存期限，並於**期限或業務終止後刪除或銷毀**，避免個資外洩。

資安管理相關作業指引(2/2)

- **教育機構資安驗證中心**(ISCB)建置之**規範指引**

全校落實資通安全管理之優先執行策略

https://sites.google.com/email.nchu.edu.tw/isms-strategy/

安全系統發展生命週期

https://sites.google.com/email.nchu.edu.tw/ssdlc

2.3 加強教育體系獎懲機制

- 獎勵機制
- 處罰機制

獎勵機制(1/2)

- 針對資安**辦理成效優良**之學校**給予獎勵**

  ➢將資安辦理成效**納入**學校**獎補助衡量指標**，指標項目包含但不限於：

  ■**全校導入ISMS**：指ISMS**適用範圍**，至少包含全校範圍內之**核心資通系統**、**保有個資或防護需求中等級以上之資通系統**，及其相關網路與資訊機房活動。

  ■**無重大資安事件**：指**未發生重大(3級以上)**資安事件(含個資外洩事件)。惟若發生資安事件的原因係**非可歸責於學校**且學校無管理不當之情事，則**不列入此項**。

獎勵機制(2/2)

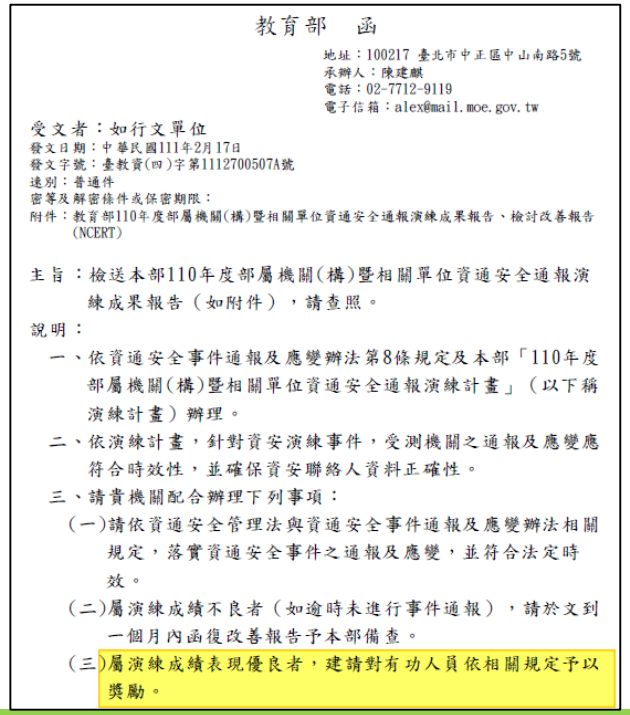
- 針對資安**辦理成效優良**之學校**給予獎勵**(續)
  - ➢學校資安**作業事項**(如社交工程演練、資安事件通報演練)成績優良者，建請學校對相關人員**行政獎勵**。

教育部　函

地址：100217 臺北市中正區中山南路5號
承辦人：林鉦烜
電話：02-7712-9078
電子信箱：esora@mail.moe.gov.tw

受文者：如行文單位
發文日期：中華民國111年1月25日
發文字號：臺教資(四)字第1112700267B號
速別：普通件
密等及解密條件或保密期限：
附件：無附件

主旨：本部辦理110年度教育部、所屬公務機關及臺灣學術網路防範惡意電子郵件社交工程演練，貴機關演練成績表現優良，建請對有功人員依相關規定予以獎勵，請查照。



教育部　函

地址：100217 臺北市中正區中山南路5號
承辦人：陳建麒
電話：02-7712-9119
電子信箱：alex@mail.moe.gov.tw

受文者：如行文單位
發文日期：中華民國111年2月17日
發文字號：臺教資(四)字第1112700507A號
速別：普通件
密等及解密條件或保密期限：
附件：教育部110年度部屬機關(構)暨相關單位資通安全通報演練成果報告、檢討改善報告(NCERT)

主旨：檢送本部110年度部屬機關(構)暨相關單位資通安全通報演練成果報告（如附件），請查照。

說明：
一、依資通安全事件通報及應變辦法第8條規定及本部「110年度部屬機關(構)暨相關單位資通安全通報演練計畫」（以下稱演練計畫）辦理。
二、依演練計畫，針對資安演練事件，受測機關之通報及應變應符合時效性，並確保資安聯絡人資料正確性。
三、請貴機關配合辦理下列事項：
(一)請依資通安全管理法與資通安全事件通報及應變辦法相關規定，落實資通安全事件之通報及應變，並符合法定時效。
(二)屬演練成績不良者（如逾時未進行事件通報），請於文到一個月內函復改善報告予本部備查。
(三)屬演練成績表現優良者，建請對有功人員依相關規定予以獎勵。

處罰機制(1/2)

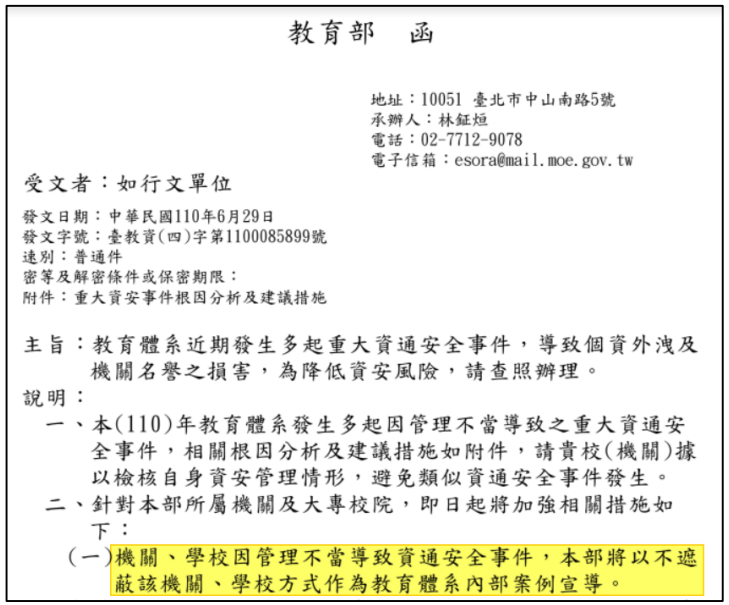
- 針對**因管理不當**導致資安事件之學校**加重處罰**
  - ➢發生**重大資安事件**，**且未落實**本部專案稽核之缺失**改善**者：
    - ■循相關機制**提報懲處**。
    - ■**專案評估扣減**對該校之獎補助款。
  - ➢**管理人員**因**設置弱密碼**而導致資安事件。
    - ■本部將正式請機關評估**予以懲處**。

非技術問題，
而是管理上的怠惰

教育部110年6月29日臺教資(四)字第1100085899號函
教育部110年6月29日臺教資(四)字第1100085899A號函

處罰機制(2/2)

- 針對**因管理不當**導致資安事件之學校**加重處罰**(續)
  - ➢如因管理不當導致**資安事件**，以**不遮蔽**該學校方式作為教育體系**內部案例宣導**。



教育部　函

地址：10051 臺北市中山南路5號
承辦人：林鉦垣
電話：02-7712-9078
電子信箱：esora@mail.moe.gov.tw

受文者：如行文單位

發文日期：中華民國110年6月29日
發文字號：臺教資(四)字第1100085899號
速別：普通件
密等及解密條件或保密期限：
附件：重大資安事件根因分析及建議措施

主旨：教育體系近期發生多起重大資通安全事件，導致個資外洩及機關名譽之損害，為降低資安風險，請查照辦理。

說明：

一、本(110)年教育體系發生多起因管理不當導致之重大資通安全事件，相關根因分析及建議措施如附件，請貴校(機關)據以檢核自身資安管理情形，避免類似資通安全事件發生。

二、針對本部所屬機關及大專校院，即日起將加強相關措施如下：

(一)機關、學校因管理不當導致資通安全事件，本部將以不遮蔽該機關、學校方式作為教育體系內部案例宣導。

自110年6月29日起實施

教育部110年6月29日臺教資(四)字第1100085899號函
教育部110年6月29日臺教資(四)字第1100085899A號函

2.4 其他相關政策規範

- 教育機構資通安全通報事件演練規劃
- 個資侵害事故通報機制

教育機構資通安全通報事件演練規劃

- 本部辦理之**111年度**教育機構**資通安全事件通報演練**規劃
  - ➢將新增下列評分項目：
    - ■將**資通安全長的聯繫方式**納入評分項目，且前述聯繫資訊未來將用於重大資安事件及重要資安政策之傳達。
    - ■將**通報演練之內容正確性**納入評分項目。

個資侵害事故通報機制

- 個人資料侵害**事故通報**
  - ➢本部110年12月8日修正**私立專科以上學校及私立學術研究機構個人資料檔案**安全維護計畫實施辦法。
    - ■學校應自事故**發現時起72小時內**，填具個人資料侵害事故**通報與紀錄表**，通報主管機關。

第八條附件

個人資料侵害事故通報與紀錄表		
非公務機關名稱 通報機關	通報時間：　年　月　日　時　分 通報人：　簽名（核章） 職稱： 電話： E-mail： 地址：	
事故發現時間		
事故發生種類	□竊取 □洩漏 □竄改 □毀損 □滅失 □其他侵害事故	個資侵害之總筆數（大約） □一般個資＿＿＿＿筆 □特種個資＿＿＿＿筆
發生原因及事故摘要		
損害狀況		
個資侵害可能結果		
擬採取之因應措施		
擬採通知當事人之時間及方式		
是否於發現個資外洩後72小時通報	□是　□否，理由：	

3.教育體系重大資安事件案例分享

3.1 教育體系重大資安事件分類說明
3.2 弱密碼及身分驗證缺失
3.3 個資檔案未受適當保護
3.4 雲端服務使用不當
3.5 未落實SSDLC要求
3.6 重大變更管理失控

3.1 教育體系重大資安事件分類說明

教育體系重大資安事件分類說明

- 為方便案例說明，依事件發生原因粗略分類如下：

項次	發生原因	事件數量	備註
1	弱密碼及身分驗證缺失	1	
2	個資檔案未受適當保護	6	如:網頁公開內容含有敏感資訊
3	雲端服務使用不當	2	如:Google表單管理設定錯誤
4	未落實SSDLC要求	4	如:第三方元件漏洞未更新、身分認/驗證管理機制未考量安全需求、系統版本控制失當等。
5	重大變更管理失控	1	如:缺乏重大變更驗證及複核機制

~~要命的~~

3.2 弱密碼及身分驗證缺失

- 教育體系重大資安事件案例分享
- 建議改善事項

教育體系重大資安事件案例分享1

- **事件說明**
  - ➢OO署委託A大學建置維運**學生業務**相關網站， A大學網站維運團隊於查看**網站日誌紀錄**(log)時，發現AP**管理者帳號**有來自**陌生國外IP成功登入**的紀錄，且疑似上百筆**個資遭到非授權的存取**。
- **發生原因**
  - ➢AP**管理者帳號**存在**弱密碼**問題，且管理後臺並**未限制存取來源**。
  - ➢什麼樣的弱密碼？
    - ■管理者帳號：[學校縮寫]+流水號，密碼：123456789
  - ➢**帳密設定**功能頁面，遺漏將**管理者**納入**密碼複雜度限制**要求範圍。

補充：教育體系資安技術檢測案例分享A (1/2)

- **檢測發現**
  - ➢OO大學的**人事業務**相關系統，**測試機**曝露於外網，檢測作業時發現有**弱密碼**問題，且測試機疑似使用正式資料，導致可非授權取得上萬筆職員的**個人資訊**。
- **風險說明**
  - ➢AP**管理者帳號**存在**弱密碼**問題，且管理後臺並**未限制存取來源**。
  - ➢什麼樣的弱密碼？
    - ■管理者帳號：admin，密碼：admin
  - ➢測試環境直接**使用正式資料**，且未有相關**配套保護**措施。

補充：教育體系資安技術檢測案例分享A (2/2)

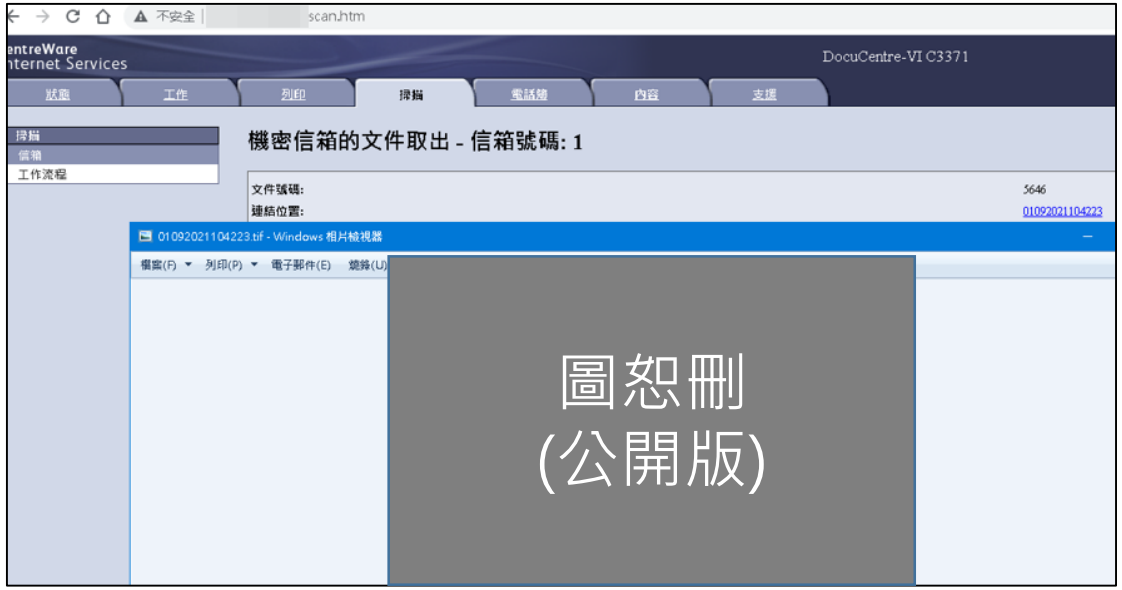
透過外網可連線至人事業務相關系統測試站，嘗試使用admin/admin登入成功。

相關功能存在SQLi弱點可利用。

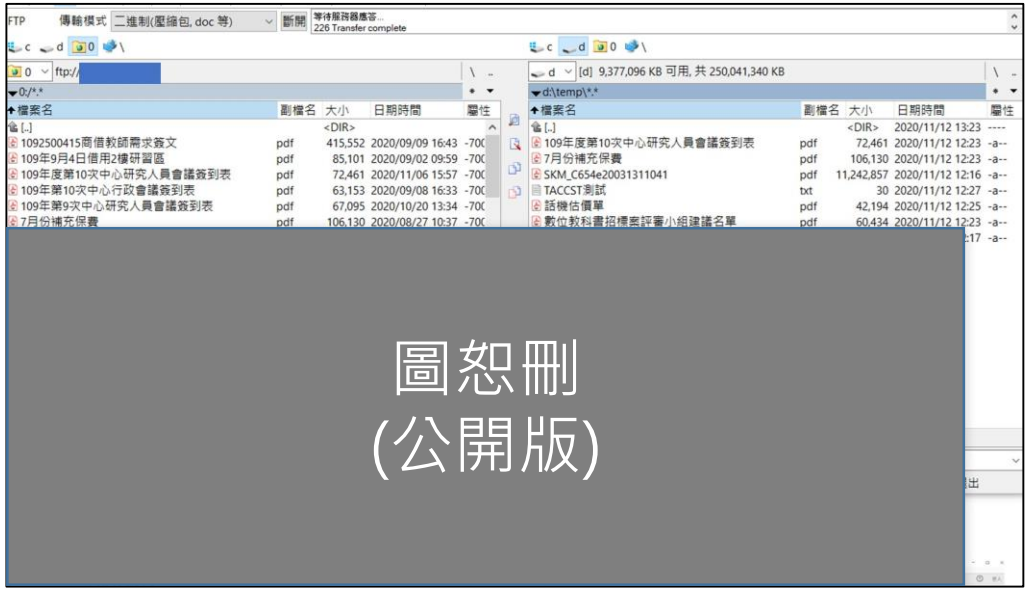
補充：教育體系資安技術檢測案例分享B (1/2)

- **檢測發現**
  - 多間機關、學校的**網路印表機**(多功能事務機)使用**廠商預設帳密**，或其檔案伺服器(**FTP**)可**匿名登入**，且因**曝露於外網**，外界可輕易以未授權方式存取。進一步發現疑似**敏感資訊洩漏**。
- **風險說明**
  - **未變更**廠商**預設帳密**，亦**未實施其他存取控管**(如限制IP存取來源)。
  - 設備具有掃描功能，**掃描後檔案**存放於設備本身或**可匿名登入之FTP**，導致敏感資訊外洩。

補充：教育體系資安技術檢測案例分享B (2/2)



上圖為機關 Xerox DocuCentre 系列網路印表機，自外網可使用廠商預設帳密 11111/x-admin 成功登入，並發現部分掃描檔案具有敏感資訊。



上圖為於機關IP範圍內，發現可自外網匿名登入之FTP(網路印表機於個人電腦安裝之客戶端)，並發現FTP資料夾內保有具敏感資訊檔案。

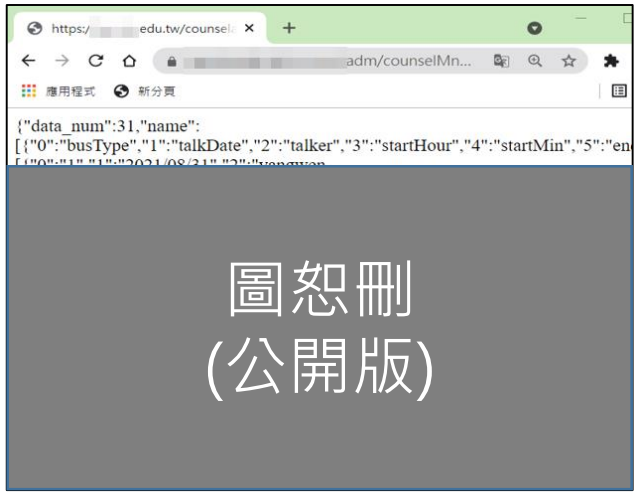
補充：教育體系資安技術檢測案例分享C (1/2)

- **檢測發現**
  - ➢OO大學**學生輔導**相關系統，開放外網連線使用，檢測作業時發現老師端登入頁面、重要系統API皆有**身份驗證繞過**問題，導致可非授權取得所有學生**輔導歷程**、**個資**等敏感資訊。
- **風險說明**
  - ➢**登入頁面**系統身分**驗證僅依賴前端 Javascript 檢查**，如使用 Proxy 等工具攔截網路封包進行修改，即**可繞過**(bypass)身分驗證機制。
  - ➢重要**系統API之請求**存取，忽略進行**身分驗證**或其他存取控管機制。

補充：教育體系資安技術檢測案例分享C (2/2)

```
success: function (result) {
    var response = jQuery.parseJSON(result)
    if (response.staffName == "" || response.staffIdentity == "") {
        alert("尚未登入成功");
        document.location.href = "index.html";
    }
```

身份驗證僅依賴前端Javascript檢查，可攔截封包修改後，繞過(bypass)身份驗證功能進入系統。



系統針對後端網頁(API)請求無安全保護機制，未經驗證之使用者可取得所有受輔導學生個資。

建議改善事項(1/3)

- **弱密碼及身分驗證缺失**
  - ➢落實資通系統及其帳號權限(應涵括作業系統、應用系統、資料庫等各類帳號)的**盤點清查**，並加強**特權帳號之管理**。
  - ➢資通系統應依其防護需求等級，落實防護基準之**身分驗證管理控制措施**相關要求。

構面	類別	項次編號	適用等級	安全控制措施
識別與鑑別	身分驗證管理	37	普	使用預設密碼登入系統時，應於登入後要求立即變更。
		38	普	身分驗證相關資訊不以明文傳輸。
		39	普	具備帳戶鎖定機制，帳號登入進行身分驗證失敗達5次後，至少15分鐘內不允許該帳號繼續嘗試登入或使用機關自建之失敗驗證機制。
		40	普	使用密碼進行驗證時，應強制最低密碼複雜度；強制密碼最短及最長之效期限制。(對非內部使用者，可依機關自行規範辦理)
		41	普	密碼變更時，至少不可以與前3次使用過之密碼相同。(對非內部使用者，可依機關自行規範辦理)
		42	普	上述兩點所定措施，對非內部使用者，可依機關自行規範辦理。
		43	中	身分驗證機制應防範自動化程式之登入或密碼更換嘗試。
		44	中	密碼重設機制對使用者重新身分確認後，發送一次性及具有時效性符記。

建議改善事項(2/3)

- **弱密碼及身分驗證缺失**(續)
  - ➢加強帳戶防護機制：
    - ■資通系統使用密碼進行驗證時，應強制**最低密碼複雜度**。
    - ■密碼複雜度**規範對象**，應包含**所有具管理權限之帳號**。
    - ■密碼**複雜度檢查**程序，應被納入**所有密碼變更功能**。
    - ■建議啟用**多因子認證**，並減少管理者帳號數量。
  - ➢機關宜訂定**密碼複雜度共通規範**，如禁止使用**與帳號名稱相同**、身分證字號、**學校/機關代碼**、易猜測之**弱密碼**、**廠商預設密碼**或其他公開資訊等。

建議改善事項(3/3)

- **弱密碼及身分驗證缺失**(續)
  - ➢網站**管理後臺**及機關內部使用之**物聯網(IoT)設備**，存取控制應以**限制IP來源範圍**為原則。
  - ➢身分驗證功能應使用**伺服器後端程式驗證**，切勿依賴前端驗證。
  - ➢所有前端**向後端API請求功能**，須加入**身分驗證機制**，並依人員身分或業務需求**授予最小權限**，以防止未授權存取敏感功能。
  - ➢弱密碼及身分驗證缺失問題，建議**納入機關安全性檢測項目**。

3.3 個資檔案未受適當保護

- 教育體系重大資安事件案例分享
- 建議改善事項

教育體系重大資安事件案例分享2

- **事件說明**
  - 調查局通知某**2所公立高中**將保有**學生個人資料**的檔案直接**公開於學校官網**，且未進行加密或遮蔽，並**可透過Google搜尋引擎發現**，可能洩漏**上百筆**個人資訊。
- **發生原因**
  - 學校承辦人**缺乏個資保護意識**，針對敏感資訊安全處理亦**未具有相關知能**。

教育體系重大資安事件案例分享3

- **事件說明**
  - ➢OO署主辦某競賽業務，該競賽**申請處理案**原應採書面回復結果，惟委辦之B高中採網站公告方式處理，且**個資未去識別化**，經**當事人主動通報**後緊急下架，可能洩漏**1筆**個人資訊。
- **發生原因**
  - ➢未依規定方式辦理申請處理案結果回復。且**因人為疏忽**，公佈資訊時**未覆核是否包含敏感資訊**。

教育體系重大資安事件案例分享4

- **事件說明**
  - ➢**OO高級中等學校**收到民眾反映，**可透過Google搜尋引擎發現**學校具有**上千筆**個人資訊之相關Excel檔，查係該校**學習登錄**相關系統供轉存資料庫暫存使用。
- **發生原因**
  - ➢網站針對**敏感資訊檔案存取控制**失當。
  - ➢**蒐集個資未作小化**。系統僅供預約登錄用途，惟新建資料時要求上傳個人敏感資訊。

教育體系重大資安事件案例分享5

- **事件說明**
  - ➢OO大學收到外部人員通報，該校OO學系**碩士班招生報名表**曝露於外網，且**內含考生個資**，並**可透過Google搜尋引擎發現**，可能洩漏數筆個人資訊。
- **發生原因**
  - ➢OO學系承辦人於網站建置考古題專區時，**因人為疏忽誤上傳**碩士班招生報名表，且原檔案亦未加密。

圖恕刪
(公開版)

教育體系重大資安事件案例分享6

- **事件說明**
  - ➢調查局通知**OO大學**OO系網站公開之**會議資料**，內含學生之重要個資(如重要證件影本)，並**可透過Google搜尋引擎發現**，可能洩漏**1筆**個人資訊。
- **發生原因**
  - ➢OO學系承辦人於OO系網站上傳會議資料，**因人為疏忽**未針對敏感資訊進行**遮罩處理或移除**。

補充：教育體系資安技術檢測案例分享D

- **檢測發現**
  - ➢OO機關因應**活動業務**建置OO網站，該網站提供使用者上傳**申請表**(包含申請人個人資訊)，檢測作業時發現數十份申請表**可透過Google搜尋引擎發現**取得。
- **風險說明**
  - ➢網站針對**敏感資訊檔案存取控制**失當。

圖恕刪
(公開版)

建議改善事項(1/2)

- **個資檔案未受適當保護**(續)
  - **敏感性或機密資料**應以**加密方式**進行**儲存及傳輸**。
  - **全面清查網站**包含**個資檔案**，確認有無保留之必要，並針對需保留之部分，確認已實施**存取控制**或進行適當**遮罩處理**。
  - **網站更新或上傳檔案**時應具備**覆核機制**，以確認內容應不包含敏感資訊(如個人資料、網站帳密等)。
  - 強化個資檔案**生命週期安全管理**，落實重要個資檔案使用前之**申請審核**，及保存期限或業務終止後之**確認刪除**等管理措施。
  - 使用者**寄送郵件**時，應謹慎檢查**收文者正確性**。

建議改善事項(2/2)

- **個資檔案未受適當保護**
  - 依資通安全責任等級分級辦法第11條規定，機關人員應依所屬人員類型(一般使用者及主管、資通安全專職人員、資通安全專職人員以外之資訊人員)完成對應之**資安教育訓練法定時數要求**。
  - **落實全體人員**(包含工讀生)**個資保護教育訓練**，且應要求**新進人員**盡速完成，以提升人員個資保護意識及知能，避免因不熟悉相關規範或個資安全處理方式造成資安事件。
  - 機關、學校**各單位**主管應**積極督促所轄**人員完成上述教育訓練，建議由專責單位(如人事單位)**定期追蹤管考**以確保成效。

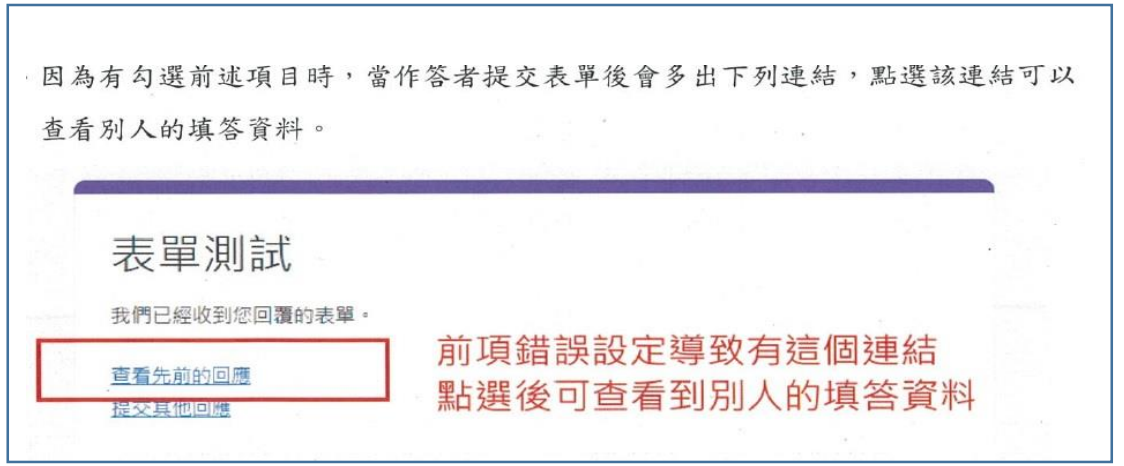
3.4 雲端服務使用不當

- 教育體系重大資安事件案例分享
- 建議改善事項

教育體系重大資安事件案例分享7 (1/2)

- **事件說明**
  - ➢OO高級中學OO室以Google表單蒐集學生資料，因表單管理設定失當，致使填報人可查看其他已填人員之填寫資訊(包含個人資料)，可能造成個資外洩。
- **發生原因**
  - ➢承辦人於設計Google表單時，因對於其管理設定功能不熟悉，錯誤勾選允許檢視其他回應選項。

教育體系重大資安事件案例分享7 (2/2)



於建置Google表單過程，因管理設定錯誤勾選「顯示摘要圖表和其他作答內容」，導致表單填寫人可查看到其他填寫人之填寫資料(包含敏感資訊)。

教育體系重大資安事件案例分享8

- **事件說明**
  - OO署委託C高中辦理OO會議，該校以Google表單蒐集參加人員資料時，因表單管理設定失當，致使填報人可查看其他已填人員之填寫資訊(包含個人資料)，可能造成個資外洩。
- **發生原因**
  - 承辦人於設計Google表單時，因對於其管理設定功能不熟悉，錯誤勾選允許檢視其他回應選項。

成因跟前案都一樣

建議改善事項

- **建議改善事項**
  - ➢依**各級學校使用資通系統或服務蒐集及使用個人資料注意事項**：
    - ■應加強並**留意表單設計所開啟的功能，是否會造成機敏資料或個人資料外洩**情事發生。
    - ■以Google表單為例，於**製作完成發送前**，應確實做好相關**設定檢查，並實際操作檢驗**，確認無風險疑慮再行送出。
  - ➢針對雲端服務之使用，加強人員教育訓練與**安全宣導**。

SSDLC (Secure Software Development Life Cycle)

即安全軟體發展生命週期

3.5 未落實SSDLC要求

- 教育體系重大資安事件案例分享
- 建議改善事項

教育體系重大資安事件案例分享9

- **事件說明**
  - ➢OO大學**活動報名**相關系統，因系統老舊遭駭客利用其**元件漏洞**上傳程式，取得系統執行權限後**植入惡意程式**，並連結學校Portal進而**竊取教職員工個資**。
- **發生原因**
  - ➢系統版本老舊，且**未修補第三方元件安全漏洞**。
  - ➢**重要資料庫未最小授權**，系統具備完整讀取校務資料庫之介接權限。
  - ➢系統處理敏感資訊，惟**未被納入**學校**資安規範適用範圍**。

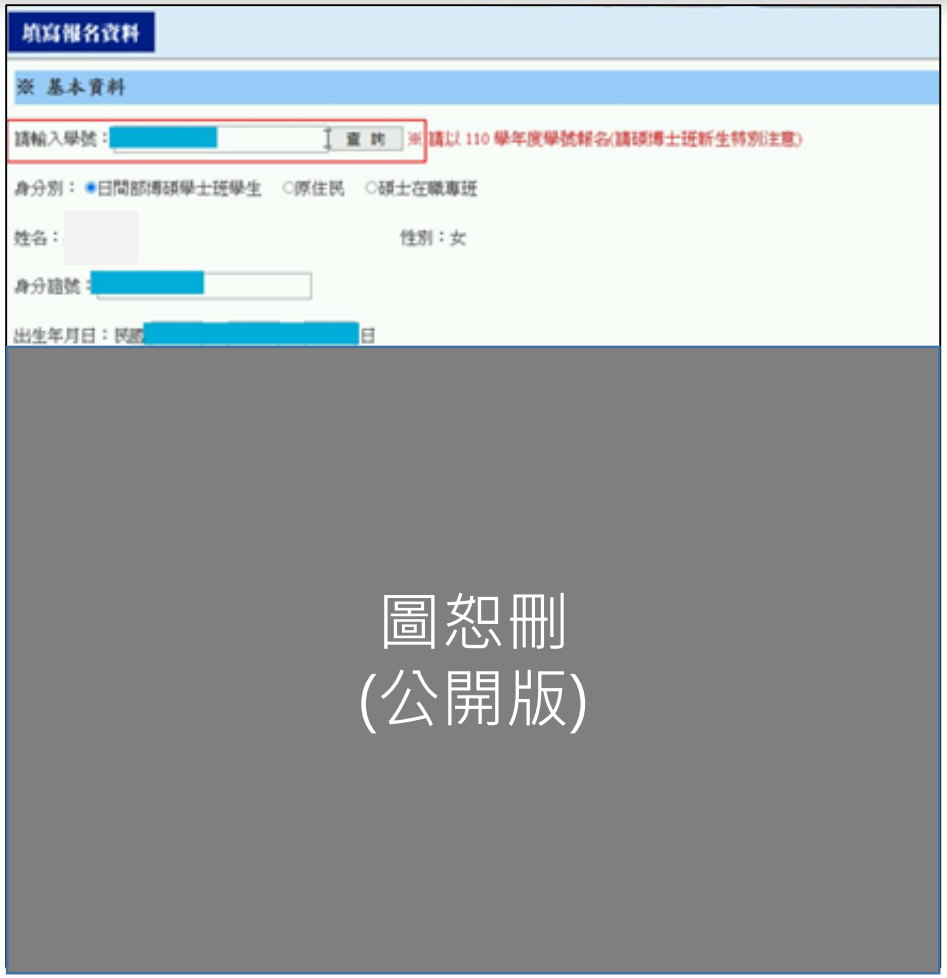
教育體系重大資安事件案例分享10

- **事件說明**
  - ➢OO機關**考招業務**相關系統，其**密碼重設功能**具有**安全邏輯漏洞**，致被外界不當利用，並發現學校端帳號有**未授權登入**之紀錄，可能洩漏多筆個人資料。
- **發生原因**
  - ➢密碼重設功能**未能確實檢驗使用者身分**，致遭惡意濫用。
  - ➢**需求及設計階段**未完整考量**安全需求**，且**測試階段**未能發現**重要功能之安全邏輯問題**。

教育體系重大資安事件案例分享11 (1/2)

- **事件說明**
  - ➢OO大學**考試報名**相關系統，**經長官交辦因應疫情緊急開發上線**，系統提供自動帶入申請人資料之便利功能，惟**僅使用學號作為身分驗證條件**，經學生通報問題後緊急下線，可能洩漏個人資訊。
- **發生原因**
  - ➢系統身分**驗證機制過於簡陋**，僅依賴學號(容易猜測或公開取得)進行身分確認，忽略可能被使用者濫用之風險。
  - ➢開發**時程過於倉促**，設計時僅考量便利性而**未納入安全需求**。
  - ➢系統處理敏感資訊，惟**未被納入**學校**資安規範適用範圍**。

教育體系重大資安事件案例分享11 (2/2)



輸入任意學生學號後(為固定格式，學年度+系所代碼+流水號)，可顯示當事人之戶籍地址、電話、Email等資訊。

教育體系重大資安事件案例分享12 (1/2)

- **事件說明**
  - ➢OO大學OO單位**跨校服務**相關系統，其網站管理後臺以**任意帳密皆可登入**，且具備查看敏感資訊權限，可能洩漏多筆個人資訊。
- **發生原因**
  - ➢網站管理後臺**驗證機制完全失效**(輸入任意帳密皆可通過驗證)，且並**未限制存取來源**。
  - ➢網站**版本控制失當**，開發人員將測試用版本之程式上傳至正式網站，而該版本無需使用者身分驗證即可登入。

教育體系重大資安事件案例分享12 (2/2)

修正前的版本

login.php

```php
<?php
include '../security/cache_expire.php';
include '../security/user_security.php';
include '../security/xss_security.php';
include './checklogin.php';


cache_expire();

$err_msg = '';

if (isset($_POST['RNO']) && isset($_POST['PASSWD'])) {
    $RNO = $_POST['RNO'];
    $PASSWD = $_POST['PASSWD'];
    $RNO = quotes($RNO);
    $PASSWD = quotes($PASSWD);

    if (check_login($RNO, $PASSWD)) {

        setcookie('rno', $RNO);
        setcookie('passwd', $PASSWD);
        setcookie('auth', get_auth_str());
        header('Location: index.php');
        exit(0);
    }
    // else
    //  $err_msg = '您的帳號或密碼不正確';

}
?>
```

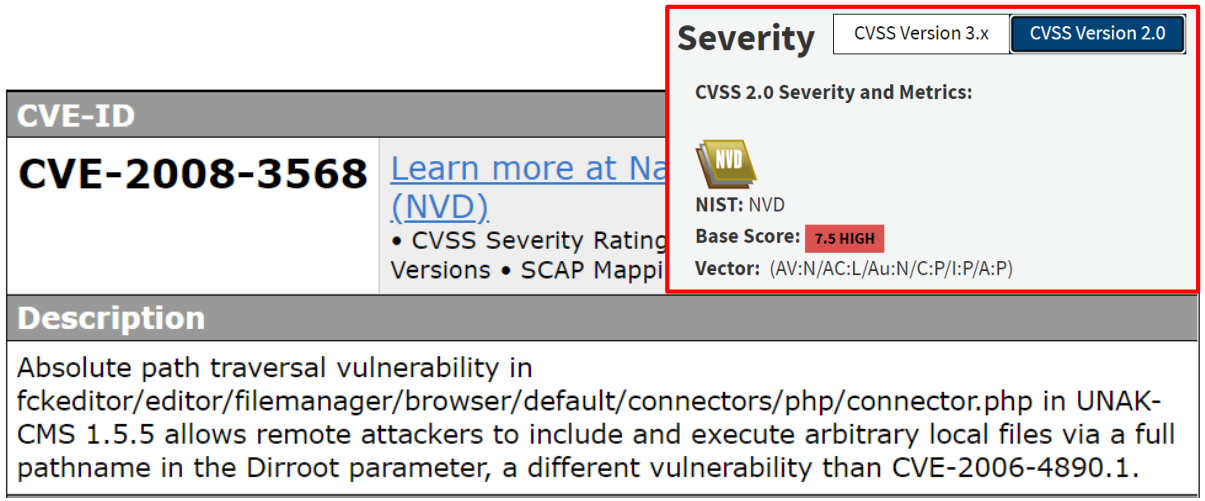
修正後的版本

login.php

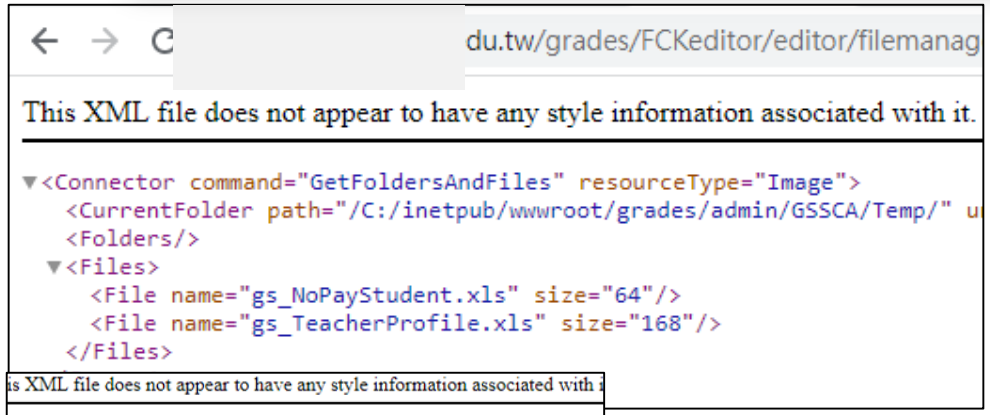
```php
<?php
include '../security/cache_expire.php';
include '../security/user_security.php';

if (1) {

    setcookie('rno', $RNO);
    setcookie('passwd', $PASSWD);
    setcookie('auth', get_auth_str());
    header('Location: index.php');
    exit(0);
}
// else
//  $err_msg = '您的帳號或密碼不正確';
```

補充：教育體系資安技術檢測案例分享E (1/2)

- **檢測發現**
  - ➢OO大學**校務**相關系統，開放外網連線使用，檢測作業時發現系統所使用之第三方元件具有**目錄遍歷**(directory traversal)弱點，進一步找到多個敏感檔案，可非授權取得全體教職員生的**個人資訊**。
- **風險說明**
  - ➢系統版本老舊，且**未修補第三方元件安全漏洞**。



補充：教育體系資安技術檢測案例分享E (2/2)



特定版本 FCKeditor 具有目錄遍歷弱點，導致網站目錄內敏感檔案曝露。

圖恕刪
(公開版)

建議改善事項(1/3)

- **未落實SSDLC要求**
  - 資通系統應依其防護需求等級，落實防護基準之**系統發展生命週期**的**需求**、**設計**、**開發**、**測試**、**部署與維運**、**委外**等各階段之**控制措施**相關要求。
    - ■需求或設計階段，應建立**安全需求檢核項目**。如身分驗證機制，除考量使用者之便利性，亦應注意被濫用之安全風險。
    - ■測試階段應進行**弱點掃描安全檢測**，並進行**中、高風險弱點修補**。針對**系統重要功能**(如忘記密碼功能)建立**安全檢核機制**，以避免安全邏輯造成資安問題。亦建議納入盲測或惡意行為測試。

建議改善事項(2/3)

- **未落實SSDLC要求**(續)
  - ➢如因應業務需求**緊急上線**，**仍應保留安全性檢測及弱點修補所需時間**，避免因重大安全漏洞被利用，導致機關嚴重損失。
  - ➢盤點系統**第三方元件使用情形**，注意相關弱點**情資通報**(如行政院技服中心、TACERT之ANA情資)，並落實**弱點修補**或實施相當之風險管理措施。
  - ➢爭取相關預算經費，加速更新與**升級老舊系統**。
  - ➢**系統開發維運團隊**人員應參與**SSDLC相關專業訓練課程**。

建議改善事項(3/3)

- **系統處理敏感資訊惟未被納入資安規範適用範圍**
  - ➢落實資通安全維護計畫，全面盤點資通系統及評估核心/重要業務，將**涉及敏感資訊者**納入**重點實施**範圍，並執行相對應之**防護基準**。
- **重要資料庫未最小授權**
  - ➢機關應建立**系統介接**作業之權限**審核機制**。
  - ➢**重要資料庫**應以**最小權限原則**進行存取授權，依介接系統之**業務功能**，提供**所需資料表及資料欄位**。

3.6 重大變更管理失控

- 教育體系重大資安事件案例分享
- 建議改善事項

教育體系重大資通安全事件案例分享13 (1/2)

- **事件說明**
  - ➢OO署委託D大學辦理**學習歷程**相關系統，該系統由D大學維運人員因應集中需求**搬遷**至OO機房，於O月O日因應**更新重新開機**，隨後發現因**虛擬主機設定錯誤**導致**硬碟資料被還原**，且因無相關備份，造成**使用者資料遺失**。


即時 要聞 娛樂 運動 全球 社會 地方 產經 股市 房市 生活 健康

學習歷程檔案遺失 蘇揆：即刻補救、專案團隊全面體檢

2021-09-26 13:48 聯合報 / 記者鄭煒／即時報導

學習歷程檔案是新課綱重頭戲，卻因廠商疏失，導致近八千位學生的學習歷程檔案消失。示意圖。本報資料照片

資料來源: https://udn.com/news/story/122472/5772658

教育體系重大資通安全事件案例分享13 (2/2)

- **發生原因**
  - ➢**備份機制失效**，搬遷後機房環境僅啟用虛擬主機層級備份。
    - ■查因系統搬遷過程，操作人員建立虛擬磁碟時**誤選「暫時性磁碟」選項**，致使系統重開機後磁碟資料被還原，且因備份系統不包含「暫時性磁碟」，故後續無法救回資料。
  - ➢針對系統搬遷等**重大變更**過程及結果，**缺乏驗證及複核**機制。
  - ➢委外團隊管理**專業能量不足**。

建議參考資訊：2.5萬件學習歷程資料遺失追追追(iThome 110/10/8報導)，
https://www.ithome.com.tw/news/147155

建議改善事項

- **重大變更管理失控**
  - ➢落實資通系統**變更管理**。
    - ■針對系統重大變更之過程，應建立**多重驗證及複核**機制，並**訂定標準作業程序(SOP)**，據以執行並檢核應辦理事項。
  - ➢落實**監控系統備份運作狀態**，並**定期辦理還原演練**，以確認備份資訊的有效性。

4. 結論與建議

結論與建議(1/3)

- 教育體系資安威脅持續提升，重大資安事件激增，為保護教職員生、民眾資料安全及各項權益，除**落實資安事件通報**應變程序外，亦應確實**落實日常資安管理**相關作業。
- **落實日常資安管理**
  - ➢應依資通安全管理法、國立大專校院資通安全維護作業指引等規定
    - ■落實**各單位(非僅資訊單位)**資通系統與資訊之**盤點**及內部資安**稽核**。
    - ■將**各單位(非僅資訊單位)**納入資安推動組織，**共同參與**重要資安議題之討論與管理審查，**訂定資安規範**、**告知資安風險**及**釐清資安責任**，並透過資安長督導落實推動。

結論與建議(2/3)

- **落實日常資安管理**(續)
  - 資通系統應依其防護需求等級，**落實防護基準各項控制措施**(涵蓋身分驗證管理、SSDLC等)相關要求。
  - **不可使用弱密碼**、廠商預設密碼等容易猜測之密碼。
  - **全面清查**網站包含個資檔案，針對需保留之部分**實施存取控制**或進行**遮罩處理**。網站**更新或上傳**檔案時應具備**覆核**機制。
  - 妥善使用雲端服務。製作線上表單時應**留意表單設計所開啟的功能**，**做好設定檢查**，確認無風險疑慮再行送出。

結論與建議(3/3)

- **落實日常資安管理**(續)
  - ➢測試階段應進行**弱點掃描安全檢測**，並進行**中、高風險弱點修補**。針對**系統重要功能**(如忘記密碼功能)建立**安全檢核**機制。
  - ➢盤點系統**第三方元件使用情形**，注意相關弱點**情資通報**，並落實**弱點修補**或實施相當之風險管理措施。
  - ➢針對系統**重大變更**應建立**多重驗證及複核**機制，並訂定**SOP**。
  - ➢落實**監控系統備份運作狀態**，並**定期辦理還原演練**。

您辛苦了
讓我們一同加油

共同提升教育體系資安環境
保障教職員生及民眾資料安全

報告完畢