不可不知的資訊安全

國立成功大學電機系 網際網路實驗室

楊竹星教授

大綱

- 資安現況與威脅
- 業務單位應具備的資安措施與程序
- 成大團隊 資安弱點掃描防護服務計畫

資安現況與威脅

資安攻擊事件頻傳

一銀ATM

發動大量連線的系統是倫敦分行的電話錄音伺服器。但是，一銀這家倫敦分行沒有ATM業務，不需連線回臺灣ATM，不應出現任何連線記錄，

Yahoo 有史以來規模最大駭客入侵事件

Yahoo 稍早宣布，確認駭客曾經入侵 Yahoo，並導致旗下約 10 億用戶的帳號遭駭，可能是 Yahoo 有史以來規模最龐大的帳號入侵事件，甚至比 2014 年駭客攻擊並偷走 5 億用戶資料的狀況還要嚴重

遠東商銀遭駭

金融監督管理委員會表示，遠銀遭駭有三大缺失，一是未落實資安控管SOP，沒有遵循最小授權原則；二是未依規定進行網段隔離；以及第三、事後檢視稽核未落實。

2016/2017

MIRAI

美國網路效能管理公司Dyn所管理的DNS服務系統上周五（10/21）遭到大規模的分散式阻斷服務（DDoS）攻擊，影響了包括Twitter、Amazon、Spotify及Netflix等使用該公司服務的網路公司。

駭客竊取民眾電腦「挖礦」

駭客將特殊的程式碼植入各大熱門網站，像是學校、社福機構，甚至是雲端服務網站；只要民眾造訪這些網站，駭客就能悄悄地用民眾的電腦來賺取虛擬貨幣，不過他們並非竊走民眾的虛擬貨幣，而是利用他們的電腦來協助挖礦。

資料來源：中央社
http://www.cna.com.tw/news/afe/201710120379-1.aspx

資料來源：自由時報
http://3c.ltn.com.tw/news/27822
http://news.ltn.com.tw/news/world/breakingnews/2218283

資料來源：iThome
https://www.ithome.com.tw/news/107294
https://www.ithome.com.tw/news/109225

資安簡介

- 資訊安全之基本為保護資料之C.I.A
  - Confidentiality(機密性)
    - 提供資訊內容的保密
  - Integrity(完整性)
    - 傳輸中的封包/資料不會被任何人修改、刪除及增加
  - Availability(可用性)
    - 資訊或功能讓其資訊保持可用的狀態，亦即無論何時均可正常提供服務

為什麼網站弱點難以根除？

- 網站是活的
- 程式設計人員缺乏資安觀念
- 網站管理人為疏失
- 技術日新月異，新弱點持續被公布

考試作業系統的資安事件

冒名填志願 恐遭退學

同學交惡報復「受害者將加額錄取」

2009年08月09日蘋果日報

訂閱 列印(43) 轉寄(0) 引用(1) 書籤

【楊勝裕、林師民、楊惠琪/連線報導】大學考試入學分發前天放榜，明星高中新竹高中畢業生彭琮淳冒用同班同學盛維康的身分上網填志願，且只填一個台灣大學醫學系，害原本可上台大的盛生高分落榜，冒名的彭生則錄取長庚大學。大學考試入學分發委員會昨決定，將以外加名額方式讓盛維康重新分發；長庚大學說，將開會討論對彭琮淳懲處，最重可能退學。

國中基測考生資料外洩案 高中生駭客涉案

【打印機版】 【字號】大 中 小

【大紀元6月25日報導】（中央社記者程啟峰高雄二十五日電）檢警偵辦國中基測考生資料外洩案，昨天展開第二波大搜索，查出高雄市楊姓高中生兩年多來受補教業者教唆，擔任駭客侵入全台十多所國中網站，竊取學生個人資料轉賣補教業者賺外快，近兩年來獲利近新台幣三十萬元。

資料來源：大紀元
http://www.epochtimes.com/b5/8/6/25/n2168156.htm

資料來源：蘋果日報
http://tw.nextmedia.com/applenews/article/art_id/31849258/IssueID/20090809

考試人員疏失的資安事件

國立變私立 桃連區放榜鬧烏龍

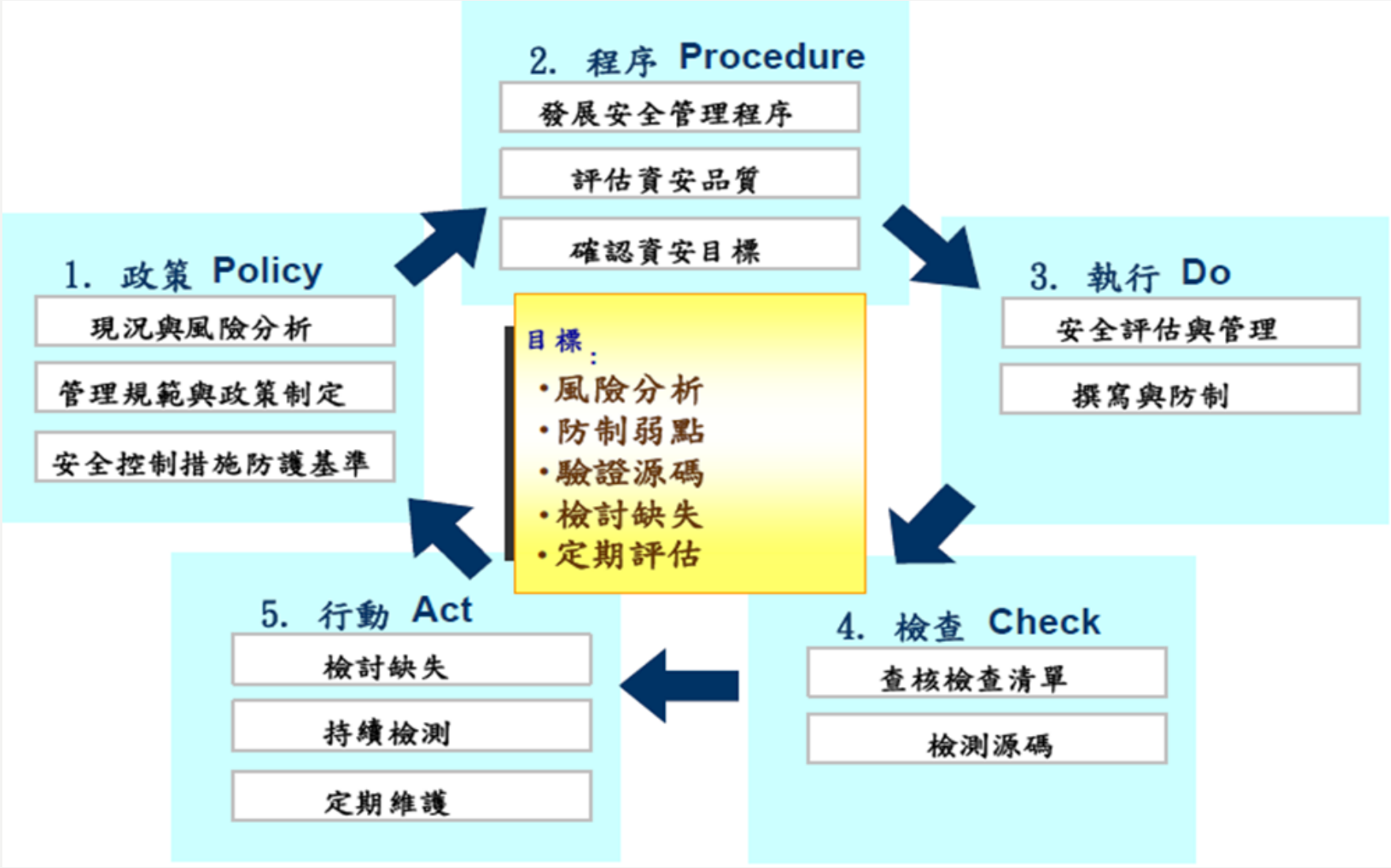
2015-07-01 09:25:36 聯合報 記者鄭國棟、呂筱嬋、張錦弘／報導 存新聞

高中職免試入學昨天放榜，桃連區官網卻擺烏龍，重新燒錄官網放榜資料時，竟誤取今年三月模擬分發結果，不少學生和家長發現錄取落差大，直呼「怎麼可能」，負責分發作業的中壢高商發現錯誤，放榜不到半小時隨即關閉官網、重新輸入資料，中午十二點半恢復查榜。

資料來源：聯合新聞網
http://udn.com/news/story/6916/1027174

資安措施與程序

管理程序



資料來源：資策會，Web應用程式安全參考指引

系統層面安全

人員管理安全


人員管理
資訊安全組織
安全政策
資訊資產分類管制
人員安全管理教育訓練
資訊安全事件之反應及處理
業務永續運作管理

學術機構資安責任等級區分

	學術機構屬性
A級	1.凡涉及各相關機關委託研究具國家安全機密性或敏感性之學校 2.辦理大學、技專校院及高級中等學校等入學考試、甄選、招生等工作之 常設試務機構
B級	1. 各大學 2. 臺灣學術網路各區域網路中心 暨各直轄市、縣（市）教育網路中心 3.辦理專科學校、十二年國教入學考試、甄選、招生工作等輪流辦理之試務機構與學校、各項評鑑工作之評鑑機構。
C級	1. 各學院、專科學校及各高中職（含）以下學校 2. 教育部所屬研究機構

資料來源：
行政院國家資通安全會報 技術服務中心
「政府機關（構）資通安全責任等級分級作業規定」(104年3月)

資安責任等級應辦事項

	安全性檢測
A級	每年至少辦理2次網站安全弱點檢測 每年至少辦理1次系統滲透測試 每年至少辦理1次資安健診
B級	每年至少辦理1次網站安全弱點檢測 每2年至少辦理1次系統滲透測試 每2年至少辦理1次資安健診
C級	依各主管機關規定教育部所屬研究機構

資料來源：
行政院國家資通安全會報 技術服務中心
「政府機關（構）資通安全責任等級分級作業規定」(104年3月)

弱點掃描防護服務計畫

成大團隊

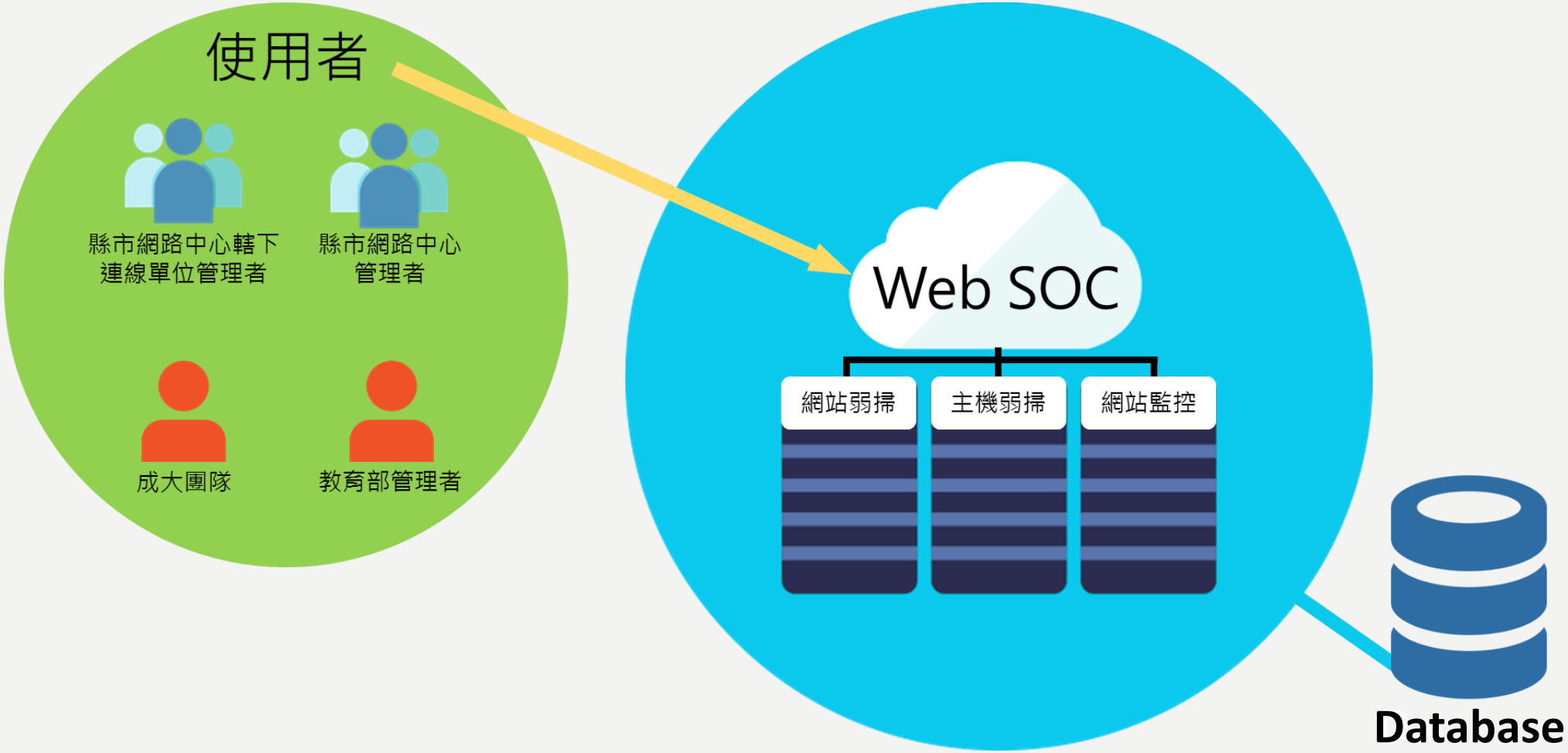
提供服務內容

- 成大團隊建置之**教育單位網站資安監控中心**

  現階段可提供以下服務

  1. 網站應用程式弱點掃描服務
  2. 網站主機弱點檢測服務
  3. 網站運作與內容監控服務
- 今日課程將說明各項服務內容

教育單位網站資安監控中心服務架構



網站應用程式弱點掃描服務

項次	弱點名稱
A1	注入攻擊(SQL Injection)
A2	無效身分認證和Session管理(Broken Authentication and Session Management，BASM)
A3	跨站腳本攻擊(Cross-Site Scripting，XSS)
A4	無效的存取控管(Broken Access Control)
A5	不安全的組態設定(Security Misconfiguration)
A6	敏感資料外洩(Sensitive Data Exposure)
A7	API攻擊防護不足(Insufficient Attack Protection)
A8	跨站請求偽造(Cross-Site Request Forgery，CSRF)
A9	使用已有漏洞的元件(Using Components with Known Vulnerabilities)
A10	API未受防護(Underprotected APIs)

網站應用程式弱點掃描服務

危險層級	資安項目
High **高風險**	OWASP TOP10資安議題、已知著名資料庫系統嚴重漏洞
Medium **中風險**	更舊版資料庫系統漏洞 (與High之差別為版本太過老舊，較無人使用) 較無立即資安危機但仍需注意
Low **低風險**	敏感資料未加密、網頁暫存Cookie安全、 網站原始碼洩漏檔案路徑、未使用之服務未關閉等
Informational **訊息提示**	錯誤顯示、網站連結失效、可能洩漏之帳號密碼、 洩漏網站、資料庫環境版本等

網站主機弱點檢測服務

Scan Report

September 21, 2017

Summary

This document reports on the results of an automatic security scan. All dates are displayed using the timezone "Coordinated Universal Time", which is abbreviated "UTC". The task was "Immediate scan of IP 120.114.234.108". The scan started at Wed Sep 20 08:32:25 2017 UTC and ended at Wed Sep 20 08:47:10 2017 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

Contents

Result Overview

Host	High	Medium	Low	Log	False Positive
[redacted]	0	1	0	10	0
Total: 1	0	1	0	10	0

Vendor security updates are not trusted.
Overrides are on. When a result has an override, this report uses the threat of the override.
Notes are included in the report.
This report might not show details of all issues that were found.
It only lists hosts that produced issues.
Issues with the threat level "Debug" are not shown.
Issues with the threat level "False Positive" are not shown.

This report contains all 11 results selected by the filtering described above. Before filtering there were 12 results.

Results per Host

[redacted]

Host scan start Wed Sep 20 08:32:37 2017 UTC
Host scan end Wed Sep 20 08:47:10 2017 UTC

Service (Port)	Threat Level
80/tcp	Medium
80/tcp	Log
111/tcp	Log
general/tcp	Log
general/CPE-T	Log

Medium 80/tcp

Medium (CVSS: 5.0)
NVT: Missing 'httpOnly' Cookie Attribute

Summary
The application is missing the 'httpOnly' cookie attribute

Vulnerability Detection Result
The cookies:
Set-Cookie: locale=***replaced***; expires=Tue, 20-Sep-2016 08:34:17 GMT; path=/

. . . continues on next page . . .

Log (CVSS: 0.0)
NVT: CGI Scanning Consolidation

Summary
The script consolidates various information for CGI scanning.
This information is based on the following scripts / settings:
- HTTP-Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100034)
- No 404 check (OID: 1.3.6.1.4.1.25623.1.0.10386)
- Web mirroring / webmirror.nasl (OID: 1.3.6.1.4.1.25623.1.0.10662)

If you think any of these are wrong please report openvas-plugins@wald.intevation.org

Vulnerability Detection Result
Requests to this service are done via HTTP/1.1.
This service seems to be able to host PHP scripts.
This service seems to be NOT able to host ASP scripts.
The following directories were used for CGI scanning:
[redacted]edu.tw/
edu.tw/certificate
edu.tw/cgi-bin
edu.tw/email
edu.tw/error
edu.tw/poll
edu.tw/report
edu.tw/res/1d3b/sys/modules/mod_fileUpload
edu.tw/res/1d3b/sys/templates/default
edu.tw/res/1d3b/sysdata/templates/default
edu.tw/scripts
edu.tw/service
edu.tw/share
edu.tw/site
edu.tw/sys
edu.tw/sys/libs/class/capcha
edu.tw/sys/modules/mod_fileUpload
edu.tw/sys/templates/default
edu.tw/sysdata/attach/mgr.service
edu.tw/sysdata/course/100
edu.tw/sysdata/course/105

. . . continues on next page . . .

網站運作與內容監控服務

弱點掃描資安素養課程

HTTP://PORTAL2.K12MOOCS.EDU.TW/COURSE/129/SECTION/LECTURE

課程大綱	課程章節
弱點掃描簡介	• 弱點掃描簡介 • 弱點掃描的標準與結果分析
OWASP Top10	• OWASP Top 10簡介 • OWASP Top 10 A1~A10 實作：攻防演練
弱點掃描工具介紹	• 弱掃工具介紹(NMAP、SQLMAP、Superscan、Getif、OpenVAS、W3AF) • 弱掃工具掃描實作
物聯網安全	• 網路印表機的資訊安全 • 網路攝影機的資訊安全
平台使用介紹	• 個人與學校資料維護 • 弱掃登錄與排程 • 報表與查詢

弱點掃描資安素養課程

HTTP://PORTAL2.K12MOOCS.EDU.TW/COURSE/129/SECTION/LECTURE

謝謝聆聽