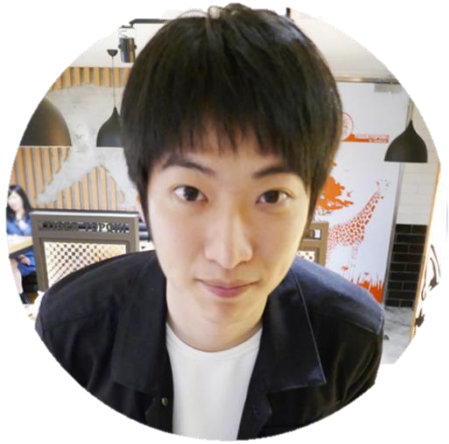

OWASP
神 隱 任 務

OWASP 2017 RC

A1~A10
Introduction

Real World
Hacking Examples

Summary



Bingo

安碁資訊股份有限公司

政大資管系

CEH, CHFI, ISO27001

Luca

安碁資訊股份有限公司

政大資管系，台大資管所

CEH, CHFI, ISO27001

資料來源：Privacy Rights Clearinghouse、Verizon，iThome整理製圖，2017年1月

Owasp 2013 to 2017

OWASP Top 10 – 2013 (Previous)	OWASP Top 10 – 2017 (New)
A1 – Injection	A1 – Injection
A2 – Broken Authentication and Session Management	A2 – Broken Authentication and Session Management
A3 – Cross-Site Scripting (XSS)	A3 – Cross-Site Scripting (XSS)
A4 – Insecure Direct Object References - Merged with A7	A4 – Broken Access Control (Original category in 2003/2004)
A5 – Security Misconfiguration	A5 – Security Misconfiguration
A6 – Sensitive Data Exposure	A6 – Sensitive Data Exposure
A7 – Missing Function Level Access Control - Merged with A4	A7 – Insufficient Attack Protection (NEW)
A8 – Cross-Site Request Forgery (CSRF)	A8 – Cross-Site Request Forgery (CSRF)
A9 – Using Components with Known Vulnerabilities	A9 – Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards - Dropped	A10 – Underprotected APIs (NEW)

Injection A1


1
系統未過濾
user input
2
惡名昭彰
SQL Injection
3
Command Injection,
LDAP Injection,
Xpath Injection
XXE
…
4
資訊遭竊
資訊遭破壞
5
主機接管

某銀行ATM派送系統存在SQL Injection漏洞

若為針對性攻擊 (Targeted Attack)，駭客還會怎麼做？

橫向移動

維持運作

資料外傳

Broken Authentication and Session Management A2


1
Session
控管不當
2
Session Fixation
Session Hijacking
3
Session
未即時更新
4
偽造身分登入
5
使用者帳號遭
竊

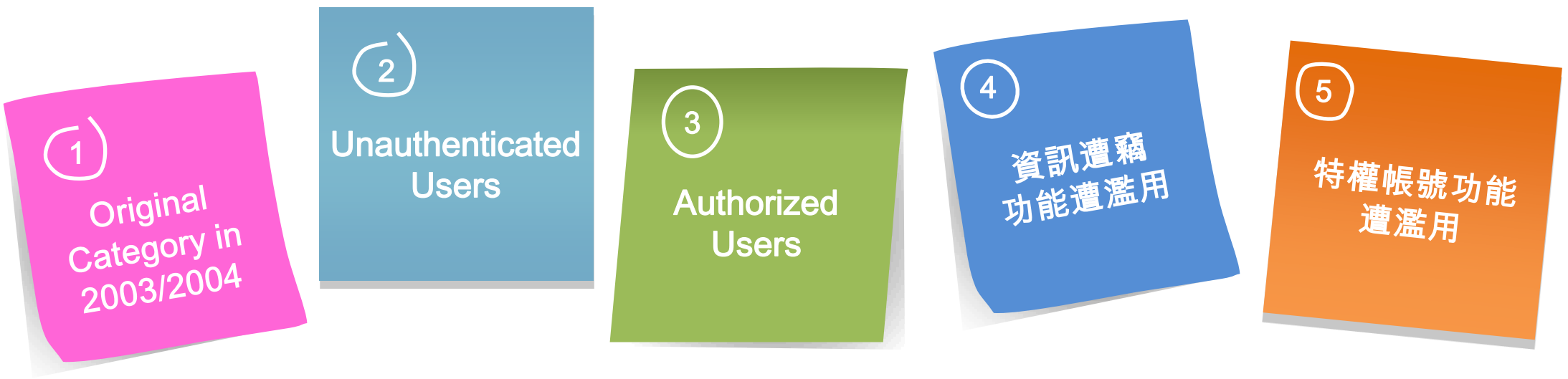
多家銀行存在驗證碼設計瑕疵

Cross-Site Scripting (XSS) A3


1
未妥善處理
user input
2
網站排版遭破壞
3
導向惡意網站
4
竊取Cookie
5
使用者帳號遭
竊

某企業含有XSS弱點

Broken Access Control A4


1
Original Category in 2003/2004
2
Unauthenticated Users
3
Authorized Users
4
資訊遭竊
功能遭濫用
5
特權帳號功能
遭濫用

某企業網路銀行，僅於前端控管頁面權限

Security Misconfiguration A5


1
安全性
設定疏失
2
未更新伺服器
套件版本
3
未妥善
設定伺服器
4
資訊遭竊
資訊遭破壞
5
主機接管

某售票系統目錄權限設定不當
並含有測試頁面

Sensitive Data Exposure A6

1

敏感信息洩漏

2

靜態數據
是否加密儲存

3

傳輸中的數據
是否明文傳遞
MITM

4

敏感數據遭竊

5

帳號、密碼
身分證字號
信用卡卡號

某金融機構以明文方式傳輸機敏資訊

Insufficient Attack Protection(NEW) A7

1. 應用程式是否感知並阻擋手動和自動攻擊
2. 開發者能否快速修補發現的漏洞
3. 幾乎沒有任何應用程序或API具有此類保護
4. 可使用WAF RASP等技術防護
5. 缺乏保護本身不是一個漏洞？

某政府機關應用系統未針對DoS攻擊進行防護

Cross-Site Request Forgery (CSRF) A8


1
使用者執行
非本意操作
2
One Click Attack
3
非本意更改密碼
4
使用者
密碼遭竊
5
使用者匯款
導致金錢損失

某企業網站存在CSRF弱點

Using Components with Known Vulnerabilities A9

1. 使用含有已知漏洞組件
2. 開發者不了解所使用的全部組件版本
3. 開發者未能及時升級至新版本
4. 低到高全系列的漏洞
5. 數據洩漏
主機接管
RCE

某企業存在 Struts2 S2-045 漏洞，可成功造成主機接管

Struts2 使用的 Jakarta Component 存在漏洞
當遠程攻擊者構造惡意的 Content-Type
可導致Remote Command Execution攻擊成功

Underprotected APIs (NEW) A10


1
API設計不良
2
客戶端與API
通訊不安全
3
API被注入攻擊
4
呼叫API
取得大量資料
5
資料庫被攻陷

某電子發票系統API濫用

某交友軟體案例


THANKS