OWASP TOP 10實務案例

Facebook 資安事件

113EP8012 楊曼翎

用戶資料外洩事件

超過5.33億筆Facebook用戶資料遭駭客透過聯絡人匯入API進行爬蟲蒐集並公開外洩，雖漏洞早已修補，資料仍已廣泛流傳

A01:2021
-Broken Access Control

漏洞描述 →

該功能允許上傳聯絡人並匹配用戶，攻擊者濫用此機制，自動化查詢電話號碼，進行大規模資料蒐集

可能影響 →

- 用戶資料大規模外洩
- 電話號碼被濫用（釣魚、詐騙）

嚴重程度高 →

攻擊門檻低、影響範圍大
資料無法回收、潛在危害高

Facebook陷個資外洩陰霾！5.33億筆個資遭「免費」看，3招自驗帳號是否遭了殃（2021）

“View As” 漏洞事件

利用「View As」功能的設計缺陷，取得用戶的存取權杖（Access Token），進而未經授權登入他人帳號，造成大規模帳戶遭入侵

漏洞描述 → 「View As」與影片上傳模組間的交互問題導致 token 被誤發，攻擊者可連續使用這個漏洞自動化取得其他帳號的存取權

可能影響 →
- 非授權登入帳號
- 嚴重隱私與帳號控制風險

嚴重程度高 → 攻擊者能直接接管用戶帳號，不需任何互動即可執行，造成隱私外洩

A07:2021-Identification and Authentication Failures

50 million Facebook users affected in breach（2018）

RECOMMENDATION

1. 加強**存取權杖**的作用範圍與有效期限、進行**安全程式碼審查**（Secure Code Review），以及避免高風險功能組合使用（View As + 上傳模組）

2. 加強 **API 權限**驗證與查詢速率限制、導入 **OAuth 與 Scope 控管**，以及以 **Zero Trust 思維**重新設計對外功能