

第二屆產品資安漏洞獵捕活動

漏洞類型中英文對照表

| 序號 | 中文 | 英文 |
|----|-------------|---|
| 1 | 任意檔案讀取 | Arbitrary File Read |
| 2 | 任意檔案上傳 | Arbitrary File Upload |
| 3 | 任意檔案寫入 | Arbitrary File Write |
| 4 | 任意使用者密碼變更 | Arbitrary User Password Change |
| 5 | 引數注入 | Argument Injection |
| 6 | 驗證機制濫用 | Authentication Abuse |
| 7 | 身分鑑別繞過 | Authentication Bypass |
| 8 | 緩衝區溢位 | Buffer Overflow |
| 9 | 程式碼注入 | Code Injection |
| 10 | 指令注入 | Command Injection |
| 11 | 跨網站腳本攻擊 | Cross-Site Scripting |
| 12 | 阻斷服務 | Denial of Service |
| 13 | 權限提升 | Privilege Escalation |
| 14 | 原型鏈汙染 | Prototype Pollution |
| 15 | 敏感資訊洩露 | Exposure of Sensitive Information |
| 16 | 堆積型緩衝區溢位 | Heap-based Buffer Overflow |
| 17 | 不當存取控制 | Improper Access Control |
| 18 | 不當驗證 | Improper Authentication |
| 19 | 不當憑證驗證 | Improper Certificate Validation |
| 20 | 不當輸入驗證 | Improper Input Validation |
| 21 | 不當處理長度不一致參數 | Improper Handling of Length Parameter Inconsistency |
| 22 | 權限管理不當 | Improper Privilege Management |
| 23 | 不安全之反序列化 | Insecure Deserialization |
| 24 | 不安全之物件參照 | Insecure Direct Object Reference |
| 25 | 更新完整性驗證不足 | Insufficient Update Integrity Verification |
| 26 | 整數溢位 | Integer Overflow |
| 27 | 連結追蹤 | Link Following |
| 28 | 本機提權 | Local Privilege Escalation |
| 29 | 記憶體毀損 | Memory Corruption |
| 30 | 記憶體溢位 | Memory Overflow |

| 序號 | 中文 | 英文 |
|----|--------------|--|
| 31 | 缺乏身分鑑別 | Missing Authentication |
| 32 | NTLM 反射 | NTLM Reflection |
| 33 | 作業系統指令注入 | OS Command Injection |
| 34 | 越界讀取 | Out-of-Bounds Read |
| 35 | 越界寫入 | Out-of-Bounds Write |
| 36 | 路徑遍歷 | Path Traversal |
| 37 | PHP 本機檔案包含 | PHP Local File Inclusion |
| 38 | 保護機制失效 | Protection Mechanism Failure |
| 39 | 競爭條件 | Race Condition |
| 40 | 相對路徑遍歷 | Relative Path Traversal |
| 41 | 遠端執行程式碼 | Remote Code Execution |
| 42 | 沙箱逃逸 | Sandbox Escape |
| 43 | 安全功能繞過 | Security Feature Bypass |
| 44 | 伺服器請求偽造 | Server-side Request Forgery |
| 45 | SQL 注入 | SQL Injection |
| 46 | 堆疊型緩衝區溢位 | Stack-based Buffer Overflow |
| 47 | 類型混淆 | Type Confusion |
| 48 | 不帶引號搜尋路徑 | Unquoted Search Path |
| 49 | 未設置父指標 | Unset Parent Pointer |
| 50 | 未驗證之通行碼變更 | Unverified Password Change |
| 51 | 使用釋放後記憶體 | Use After Free |
| 52 | 使用用戶端驗證 | Use of Client-Side Authentication |
| 53 | 使用外部控制之格式化字串 | Use of Externally-Controlled Format String |
| 54 | 使用硬刻之帳號通行碼 | Use of Hard-coded Credentials |
| 55 | 使用未初始化變數 | Use of Uninitialized Variable |
| 56 | 驗證機制不足 | Weak Authentication |
| 57 | 弱密碼回復機制 | Weak Password Recovery Mechanism |
| 58 | XML 注入 | XML Injection |
| 59 | 其他 | Others |