網站應用程式常見弱點解析

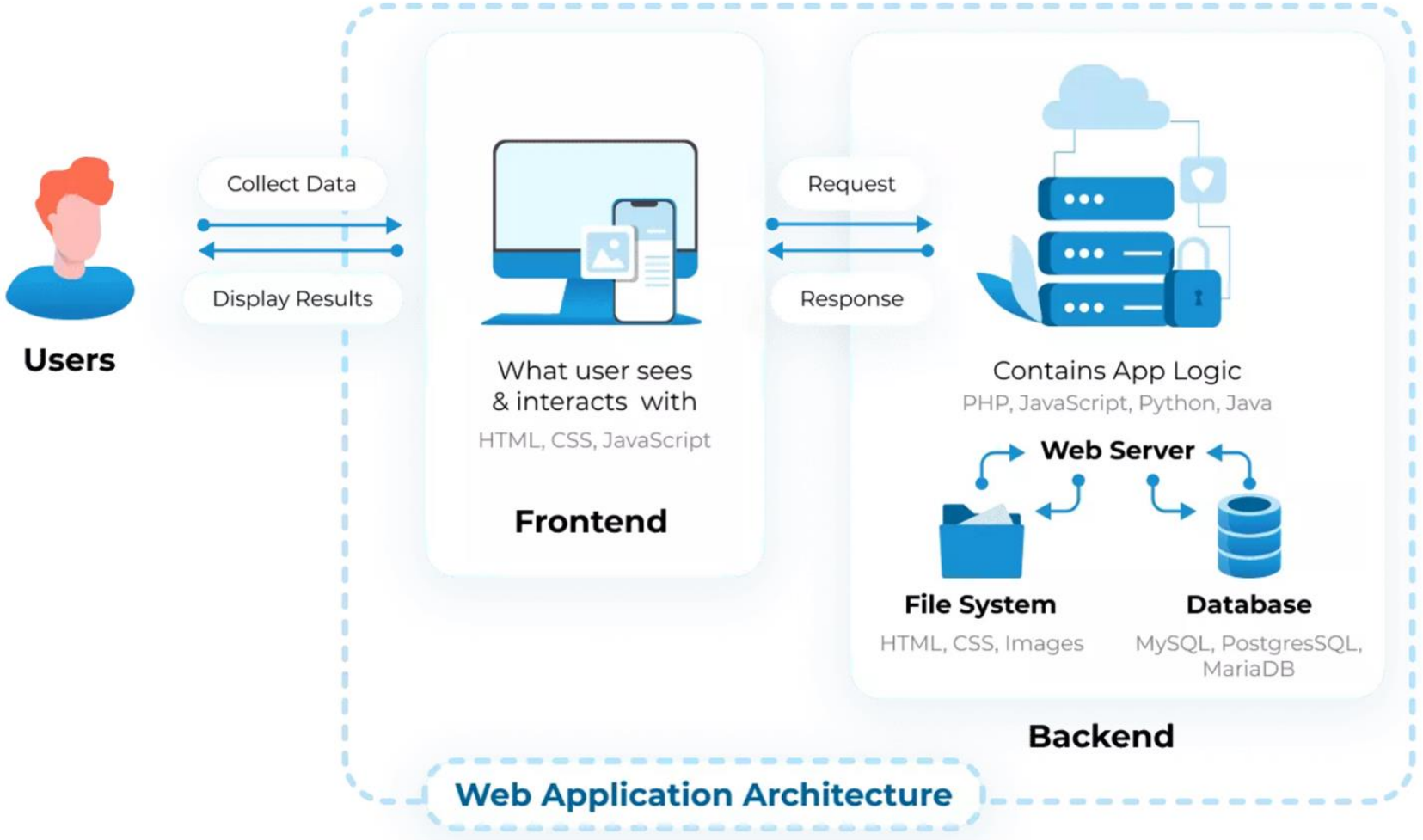
國立中山大學王聖全

2023/2/23

Agenda

- 網站架構與基礎簡介
- OWASP TOP 10 風險介紹
- 網站應用程式常見弱點實務解析
- 問題討論

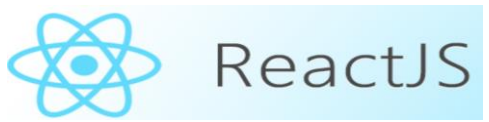
網站架構示意圖



source: https://litslink.com/blog/web-application-architecture

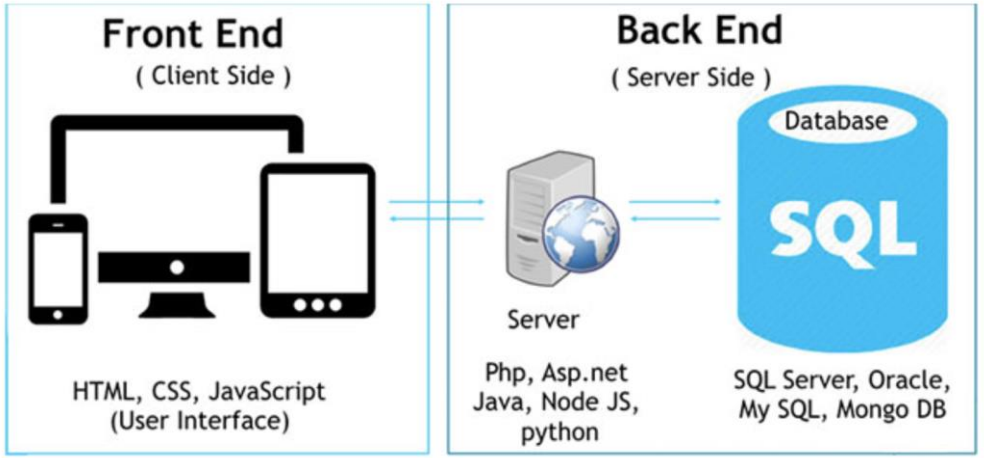
前端(Front-end)

- HTML
- CSS
- JavaScript
- Bootstrap
- jQuery
- Front-end Frameworks
  - AngularJS
  - ReactJS
  - Vue.js



後端(Backend)

- 程式語言
  - PHP, ASP.NET, Python, Java, Ruby
- 開發框架
  - Laravel, Django, Spring, Ruby on Rails
- 資料庫
  - MySQL, SQL Server, Oracle, Mongodb, Redis
- 網站伺服器
  - Apache, Nginx, IIS



https://t2conline.com/choosing-a-web-development-stack-for-your-startup/

常見網站系統技術

- JavaScript
- JSON, XML
- SPA (Single Page application) 框架
- 網站伺服器
- 負載平衡器
- 資料庫
- 身份驗證及授權系統
- 用戶端的本機資料儲存 (cookies, web storage, IndexedDB)

XML

```xml
<employees>
  <employee>
    <firstName>John</firstName> <lastName>Doe</lastName>
  </employee>
  <employee>
    <firstName>Anna</firstName> <lastName>Smith</lastName>
  </employee>
  <employee>
    <firstName>Peter</firstName> <lastName>Jones</lastName>
  </employee>
</employees>
```

Json

```json
{"employees":[
  { "firstName":"John", "lastName":"Doe" },
  { "firstName":"Anna", "lastName":"Smith" },
  { "firstName":"Peter", "lastName":"Jones" }
]}
```

HTTP常見method

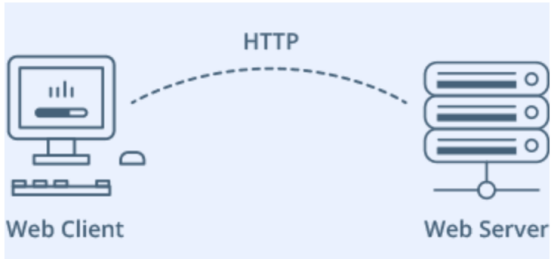
- GET
  - request data from a specified resource
  - E.g.

```
/test/demo_form.php?name1=value1&name2=value2
```

- POST
  - send data to a server to create/update a resource
  - E.g.

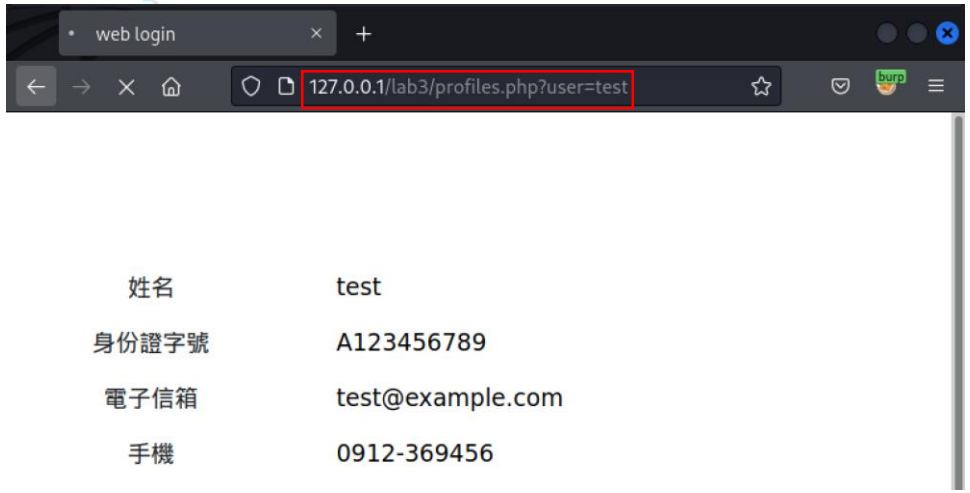
```
POST /test/demo_form.php HTTP/1.1
Host: w3schools.com

name1=value1&name2=value2
```



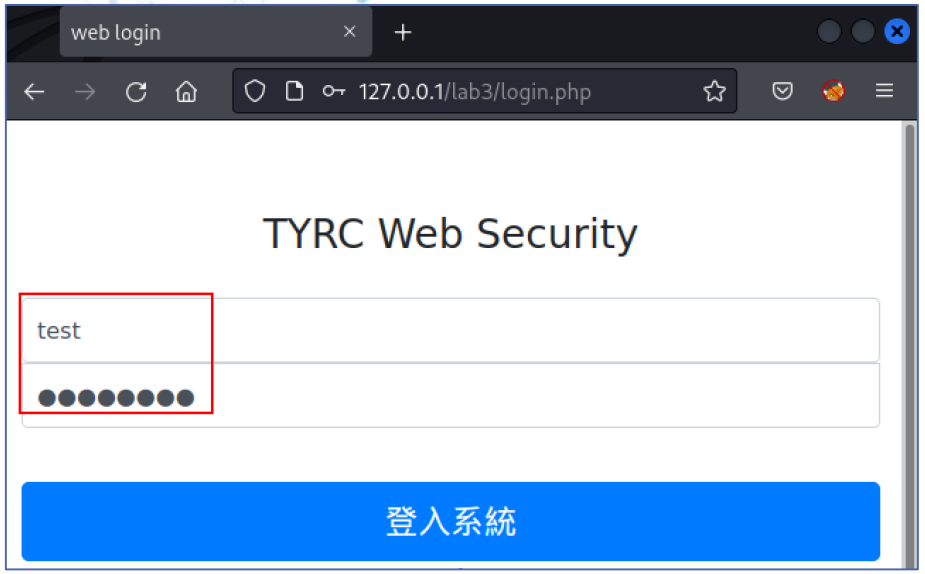
https://www.electrorules.com/webserver-how-it-work/

GET method實例




```
GET /lab3/profiles.php?user=test HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: PHPSESSID=hlp1slrmo5ven1fms2cbrk1vi7
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
```

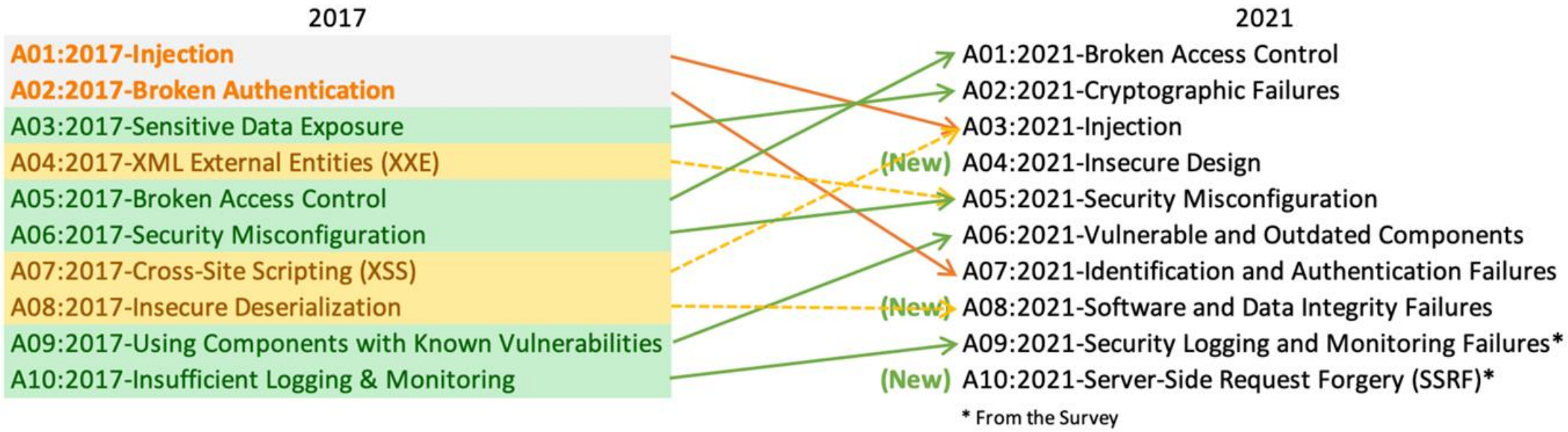
POST method實例




```
1  POST /lab3/login.php HTTP/1.1
2  Host: 127.0.0.1
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
4  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate
7  Content-Type: application/x-www-form-urlencoded
8  Content-Length: 23
9  Origin: http://127.0.0.1
10 Connection: close
11 Referer: http://127.0.0.1/lab3/login.php
12 Cookie: PHPSESSID=hlp1slrmo5ven1fms2cbrk1vi7
13 Upgrade-Insecure-Requests: 1
14 Sec-Fetch-Dest: document
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-Site: same-origin
17 Sec-Fetch-User: ?1
18
19 user=test&pass=test1234
```

OWASP TOP 10:2021 弱點風險

OWASP Top 10 2021 介紹



Source: https://owasp.org/Top10/zh_TW/

CWEs弱點 (1/2)

- https://owasp.org/Top10/A01_2021-Broken_Access_Control/

List of Mapped CWEs

CWE-22 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

CWE-23 Relative Path Traversal

CWE-35 Path Traversal: '.../...//'

CWE-59 Improper Link Resolution Before File Access ('Link Following')

CWE-200 Exposure of Sensitive Information to an Unauthorized Actor

CWE-201 Exposure of Sensitive Information Through Sent Data

CWE-219 Storage of File with Sensitive Data Under Web Root

CWE-264 Permissions, Privileges, and Access Controls (should no longer be used)

CWE-275 Permission Issues

CWE-276 Incorrect Default Permissions

CWE-284 Improper Access Control

CWE-285 Improper Authorization

CWE-352 Cross-Site Request Forgery (CSRF)

CWEs弱點 (2/2)

- https://cwe.mitre.org/data/definitions/284.html

CWE-284: Improper Access Control

Weakness ID: 284
Abstraction: Pillar
Structure: Simple

Memberships

Nature	Type	ID	Name
MemberOf	C	254	7PK - Security Features
MemberOf	C	723	OWASP Top Ten 2004 Category A2 - Broken Access Control
MemberOf	C	944	SFP Secondary Cluster: Access Management
MemberOf	C	1031	OWASP Top Ten 2017 Category A5 - Broken Access Control
MemberOf	V	1340	CISQ Data Protection Measures
MemberOf	C	1345	OWASP Top Ten 2021 Category A01:2021 - Broken Access Control
MemberOf	C	1369	ICS Supply Chain: IT/OT Convergence/Expansion

A01:2021 – 權限控制失效 (Broken Access Control)

- 執行帳號預期權限之外的事
  - 未經授權的資訊洩露、修改或損壞所有資料
  - 執行超出用戶權限的業務功能
- 可對應CWE列表
  - CWE-22 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
  - CWE-200 Exposure of Sensitive Information to an Unauthorized Actor
  - CWE-284 Improper Access Control
- Example
  - IDOR (Insecure direct object references ，不安全的直接物件參考)
  - LFI (Local File Inclusion，本機檔案包含)

Source: https://owasp.org/Top10/zh_TW/A01_2021-Broken_Access_Control/#cwe

A02:2021 –加密機制失效(Cryptographic Failures)

- 聚焦於密碼學相關的失效(或缺乏加密)，導致敏感資料的洩漏
- 可對應CWE列表
  - CWE-261 Weak Encoding for Password
  - CWE-319 Cleartext Transmission of Sensitive Information
- Example
  - Weak Hashing
  - HTTP / FTP / TELNET (明文傳輸)
  - 弱加密演算法

Source: https://owasp.org/Top10/zh_TW/A02_2021-Cryptographic_Failures/

A03:2021 –注入式攻擊(Injection)

- 注入攻擊 (injection attack)
- 可對應CWE列表
  - CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
  - CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
- Example
  - SQL injection
  - Cross Site Scripting (XSS)

Source: https://owasp.org/Top10/zh_TW/A03_2021-Injection/

A04:2021 –不安全設計(Insecure Design)

- 應用程式設計缺陷與架構中的風險
- 2021年新增類別
- 可對應CWE列表
  - CWE-209 Generation of Error Message Containing Sensitive Information
  - CWE-434 Unrestricted Upload of File with Dangerous Type
- Example
  - 可上傳惡意程式

Source: https://owasp.org/Top10/zh_TW/A04_2021-Insecure_Design/

A05:2021 –安全設定缺陷(Security Misconfiguration)

- 不必要的功能啟用或是安裝 (如Debug功能)
- 系統發生錯誤時揭露過多錯誤訊息 (如stack traces)
- 可對應CWE列表
  - CWE-260 Password in Configuration File
  - CWE-611 Improper Restriction of XML External Entity Reference
- Example
  - 系統Debug模式未關閉，顯示過多詳細資訊
  - XXE (XML External Entity)

Source: https://owasp.org/Top10/zh_TW/A03_2021-Injection/

A06:2021 –易受攻擊和已淘汰的組件 (Vulnerable and Outdated Components)

- 容易受到攻擊、已不支援或已淘汰的軟體
  - 作業系統、網頁/應用程式伺服器、資料庫、應用程式、 API 以及所有組件、Library。
- 可對應CWE列表
  - CWE-937 OWASP Top 10 2013: Using Components with Known Vulnerabilities
  - CWE-1035 2017 Top 10 A9: Using Components with Known Vulnerabilities
- Example
  - Apache版本過舊
  - Log4j

Source: https://owasp.org/Top10/zh_TW/A06_2021-Vulnerable_and_Outdated_Components/

A07:2021 –認證及驗證機制失效 (Identification and Authentication Failures)

- 與身份識別失效相關
  - 允許暴力或其他自動化攻擊
  - 無效的多因素認證
- 可對應CWE列表
  - CWE-287 Improper Authentication
  - CWE-384 Session Fixation
    - 登入後的Session ID仍一樣
- Example
  - 認證機制繞過弱點

Source: https://owasp.org/Top10/zh_TW/A07_2021-Identification_and_Authentication_Failures/

A08:2021 –軟體及資料完整性失效 (Software and Data Integrity Failures)

- 程式碼或基礎架構未能保護軟體及資料之完整性受到破壞
  - 物件或資料經編碼或序列化到一個對攻擊者可讀寫之結構中將導致**不安全的反序列化**
  - 應用程式依賴來自於不受信任來源，典藏庫及內容遞送網路之外掛，函式庫或模組
- 可對應CWE列表
  - CWE-502 Deserialization of Untrusted Data
- Example
  - **反序列化 (Deserialization)**

Source: https://owasp.org/Top10/zh_TW/A08_2021-Software_and_Data_Integrity_Failures/

A09:2021 –資安紀錄及監控失效 (Security Logging and Monitoring Failures)

- 缺乏記錄及監控，無法偵測資安事件發生
  - Auditable events, such as logins, failed logins, and high-value transactions, are not logged.
  - Logs of applications and APIs are not monitored for suspicious activity.
- 可對應CWE列表
  - CWE-778 Insufficient Logging
- Example
  - 登入失敗未紀錄log

Source: https://owasp.org/Top10/zh_TW/A09_2021-Security_Logging_and_Monitoring_Failures/

A10:2021 –伺服器請求偽造 (Server-Side Request Forgery)

- 網頁應用程式正在取得遠端資源，卻未驗證由使用者提供的網址
- 2021年新類別
- **Send a crafted request to an unexpected destination**
  - protected by a firewall, VPN, or another type of network access control list (ACL)
- 可對應CWE列表
  - CWE-918 Server-Side Request Forgery (SSRF)
- Example
  - SSRF attack

Source: https://owasp.org/Top10/zh_TW/A09_2021-Security_Logging_and_Monitoring_Failures/

網站弱點原理介紹及解析

網站弱點原理介紹及解析

- XSS (Cross Site Scripting)
- SQL injection (SQLi)
- LFI / RFI
- File upload
- Command injection
- SSRF (Server-side request forgery)
- Access Control

問題討論

THANK YOU
FOR
YOUR ATTENTION