

Web Security

Ian



Who am I?

- ◆ Name : Ian
- ◆ Department : 東華大學資管系(NDHU IM)
- ◆ Grade : 大四(Senior)



Pre Security



資安概論



Linux



網路基礎



網站基礎

資安概論 Keywords

- ◆ 攻擊、檢測：資安檢測、弱點掃描、滲透測試、紅隊演練
- ◆ 防禦、偵測：資安鑑識、資安防禦、資安健診、資安規劃

Linux

- ❖ 鳥哥的Linux 私房菜
- ❖ dywang 呆王老師
- ❖ Linux 線上練習 jsLinux : <https://bellard.org/jslinux/>
- ❖ Linux 線上練習 copy.sh : <https://copy.sh/v86/?profile=linux26>
- ❖ Linux WarGame : <https://overthewire.org/wargames/bandit/>
- ❖ Linux 線上練習 webminal : <https://www.webminal.org/register/>
- ❖ Linux 線上練習 linuxcontainers :
<https://linuxcontainers.org/lxd/try-it/>

Network

- ❖ HTTP 概論：<https://www.tutorialspoint.com/http/>
- ❖ HTTP 規範：<https://httpwg.org/specs/>
- ❖ HTTP 請求與回應練習：<https://httpbin.org/>
- ❖ Lidemy HTTP Challenge：<https://lidemy-http-challenge.herokuapp.com/>

Web

- ◆ 練習操作資料庫：<https://sqlbolt.com/>
- ◆ Web 入門：https://developer.mozilla.org/zh-TW/docs/Learn/Getting_started_with_the_web

Web 網站安全漏洞/弱點

- ◆ OWASP TOP 10: https://owasp.org/Top10/zh_TW/
- ◆ 常見注入型弱點： XSS 、 SQL injection 、 Command injection 、 Code injection (Local File Inclusion)
- ◆ Session 相關弱點： Session 劫持 、 Session 固定
- ◆ 前端相關弱點： CSRF 、 點擊劫持 、 DOM base 、
- ◆ 進階弱點： SSRF 、 XXE 、 Insecure Deserialization 、 WebSockets

Prerequest

- ❖ Kali
- ❖ Docker
- ❖ Browser

Tool

- ❖ OWASP WebScarab / OWASP ZAP
- ❖ Burp Suite
- ❖ Git
- ❖ <https://github.com/ianyang66/WebAttackDemo>

工具 > 選項 > Local Proxies > 端口(8180)

XSS?

Cross-Site Scripting

跨站腳本攻擊 - XSS

- ◆ XSS攻擊是利用動態網頁的特性、程式開發者未嚴格限制使用者輸入與未過濾特殊字串，讓惡意的Script (如Java Script或VB Script等)得以在使用者的瀏覽器上執行
- ◆ 影響：控制瀏覽器，進而竊取資料

跨站腳本攻擊 - XSS

◆ 種類

種類	說明
反射型XSS	來自當前的HTTP請求
儲存型XSS	儲存於受害者資料庫等處
DOM型XSS	來自瀏覽器中的程式碼非伺服器中的程式碼

跨站腳本攻擊 - XSS



◆ Source: <https://ithelp.ithome.com.tw/m/articles/10243967>

跨站腳本攻擊 - XSS

手法

攻擊者於具有弱點的網站輸入惡意 HTML 語法或 JavaScript 程式碼

成因

因網站後端未進行過濾惡意語法於瀏覽的頁面執行受害者瀏覽具有弱點的頁面

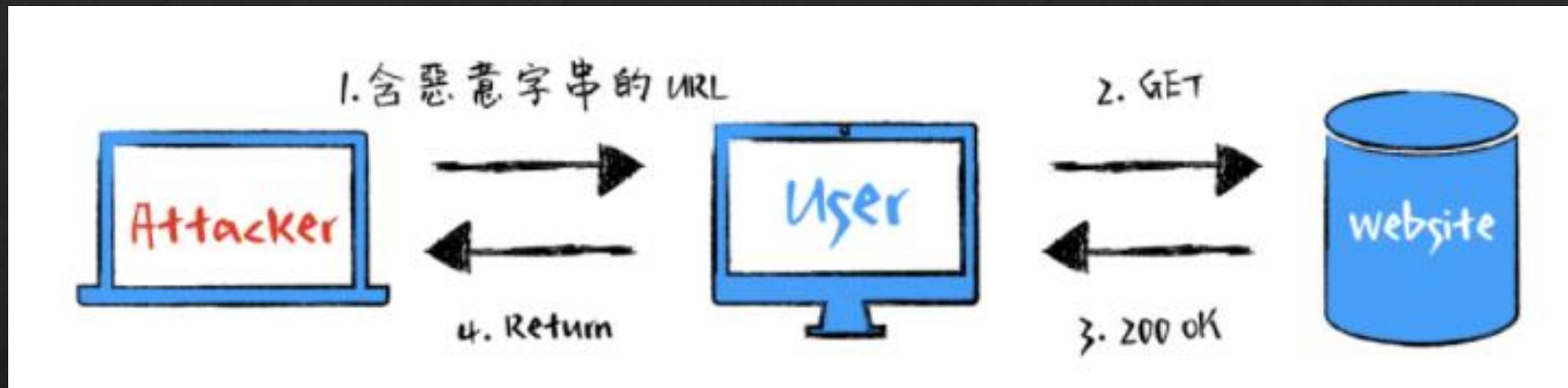
影響

導致釣魚攻擊、網頁置換
Cookie 資料被竊取
Session 劫持

瀏覽器

可解析執行 Javascript 等腳本語言
但只會執行不會判別是否為惡意

反射型XSS

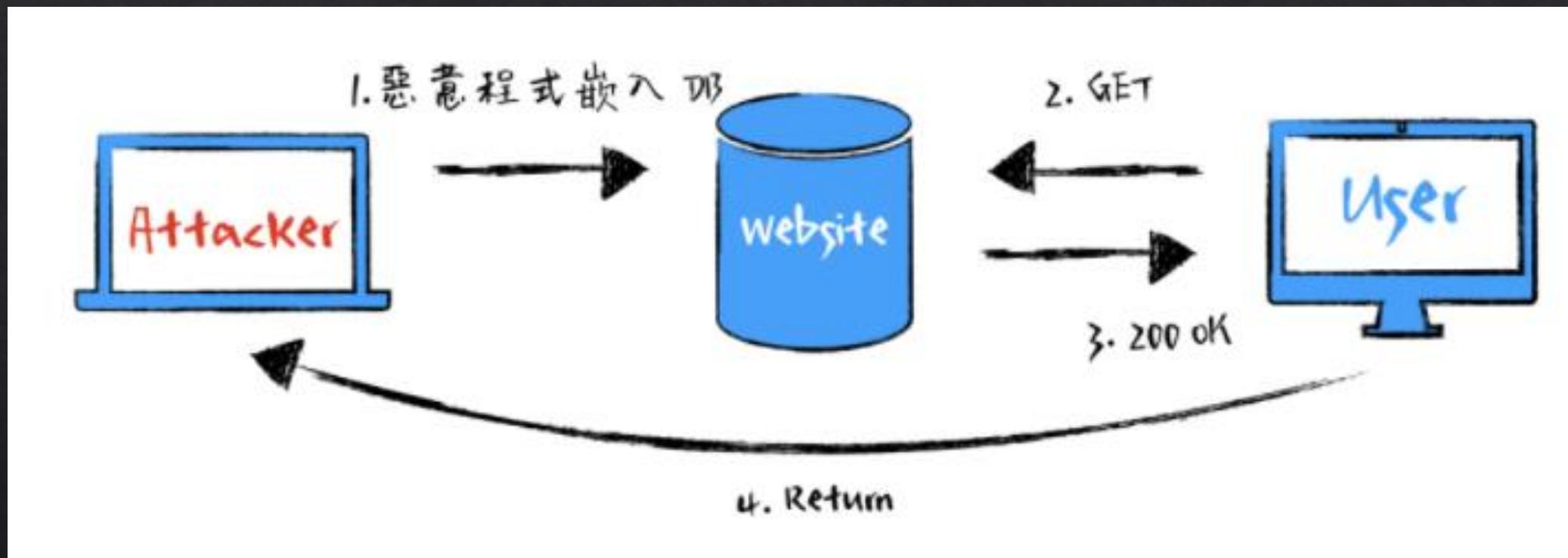


`http://localhost:8080/?a=%3Cscript%3Ealert(%22xss%22)%3C/script%3E`

15

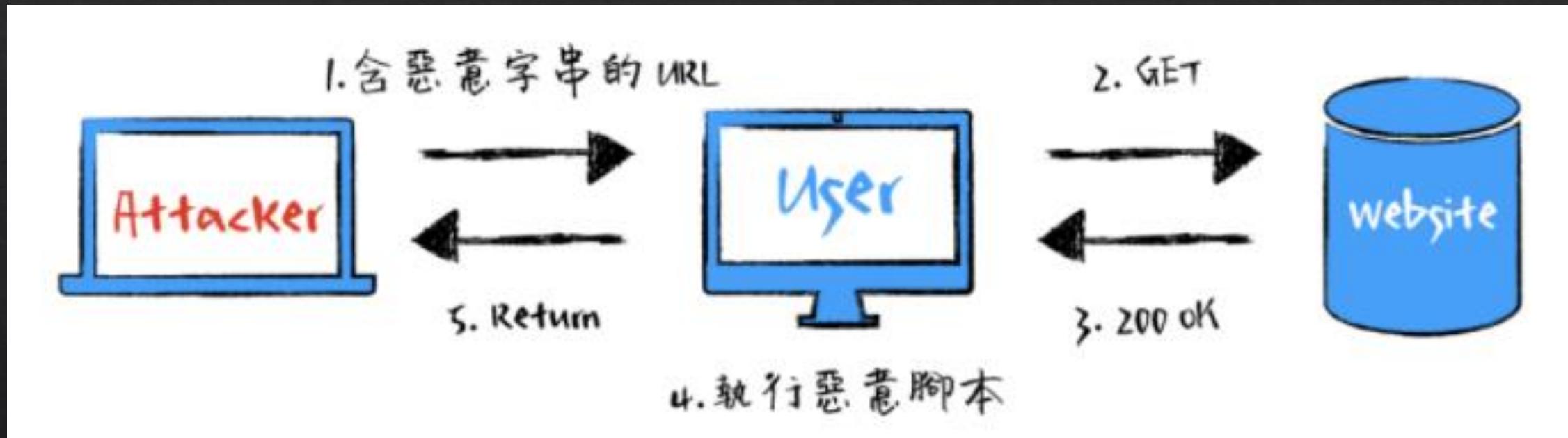
❖ Source: <https://ithelp.ithome.com.tw/articles/10218476>

儲存型XSS



◆ Source: <https://ithelp.ithome.com.tw/articles/10218476>

DOM型XSS



◆ Source: <https://ithelp.ithome.com.tw/articles/10218476>

Play Time ☺☺☺

- ❖ 請對127.0.0.1:9080 做XSS

防禦手法

- ❖ 驗證使用者輸入資訊
 - 1. 特殊符號編碼
 - 2. 必須使用的情況下，務必使用白名單
- ❖ Cookie 使用 HttpOnly, Secure
- ❖ Header
 - ❖ Content-Type : media type
 - ❖ Content-Type-Options :防止 Content-Type 被竄改
- ❖ Content Security Policy (CSP)內容安全政策
 - ❖ Content-Security-Policy: frame-ancestors 'self';
 - ❖ Content-Security-Policy: frame-ancestors ian.tw ;

CSRF?

Cross-site request forgery

跨網站請求偽造攻擊(CSRF)



使用者輸入帳號登入網站後
伺服器登入Cookie
SessionID=f236a59b

登入成功



駭客傳送釣魚信件或惡意網站誘使使
用者點擊或瀏覽



使用者輸入帳號登入網站後
伺服器登入Cookie

被登出



@user

GET /logout
host: ian.com
SessionID=f236a59b

跨網站請求偽造攻擊(CSRF)

◆ 影響

- ◆ 惡意攻擊者讓受害者於不知情狀況送出請求
- ◆ 根據功能性而有不同程度上的**風險**

◆ 案例

- ◆ 更改帳號信箱
- ◆ 更改密碼
- ◆ 問卷
- ◆ 轉帳



跨網站請求偽造攻擊(CSRF)

◆ CSRF達成條件



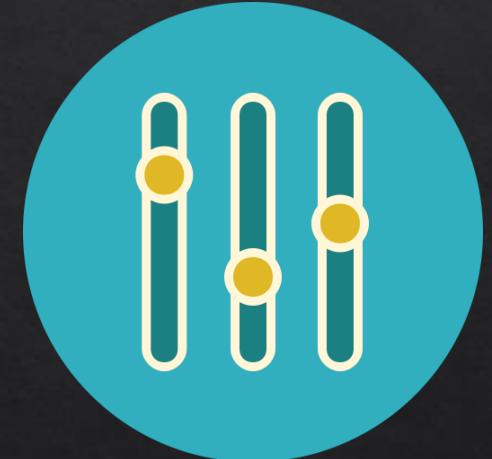
目的

駭客有想達成的目標



Cookie

網站功能驗證缺失



參數

沒有未知的參數

Play Time ☺☺☺

- ❖ 請對127.0.0.1:9080 竊取cookie

防禦手法

- ◆ 不可預測的CSRF Token
 - 1. 特殊符號編碼
 - 2. 必須使用的情況下，務必使用白名單
- ◆ 每次請求都有嚴格的驗證
- ◆ SameSite cookie屬性
 - ◆ Strict: 無法跨站送出
 - ◆ Lax: POST不包含cookie

舉報網站漏洞？

- ❖ HITCON Zero Day
- ❖ HackerOne Bug Bounty

Thank you