2025 年【科學探究競賽-這樣教我就懂】

技高組 成果報告格式

題目名稱： 咖啡廳的免費陷阱：你知道一杯咖啡的時間，你的個資可能就暴露了嗎？

一、摘要

本研究聚焦於公共 Wi-Fi 環境中的資安風險，透過模擬 Wi-Fi 嗅探與會話劫持等攻擊手法，實證未加密 HTTP 網站在 Cookie 傳輸上的漏洞。結果顯示，使用 HTTP 傳輸協定的網站極易使敏感資訊遭攔截，進而造成使用者身分被冒用的風險。相對地，透過 HTTPS 加密與妥善的 Cookie 安全設定，能有效降低此類威脅。研究同時提出具體的實驗數據與實務建議，以提升社會大眾對免費 Wi-Fi 背後潛藏風險的警覺與防護意識。

二、探究題目與動機

(一.) 題目： 公共 Wi-Fi 環境下的資安風險——從 Wi-Fi 嗅探到會話劫持的實證研究

(二.) 動機：

1. 公共 Wi-Fi 普及性：現代社會大量依賴免費 Wi-Fi，尤其是年輕族群與自由工作者，但這些網路多數未加密，可能成為駭客攻擊的溫床。

2. 資安風險增加：駭客可利用中間人攻擊 (MITM) 攔截數據流量，竊取帳號密碼、Cookie 等敏感資訊。

3. 資安宣導不足：多數資安教育以理論為主，缺乏具體的攻擊示範。本研究希望透過實驗設計，提高大眾對資安風險的認識，並促進資安防護意識。

三、探究目的與假設

(一.) 目的：

透過駭客攻擊模擬，揭示公共 Wi-Fi 如何成為中間人攻擊 (MITM) 與會話劫持 (Session Hijacking) 的管道。

透過實驗數據分析，驗證 HTTP 網站的 Cookie 傳輸風險，並比較 HTTPS 加密的安全性。

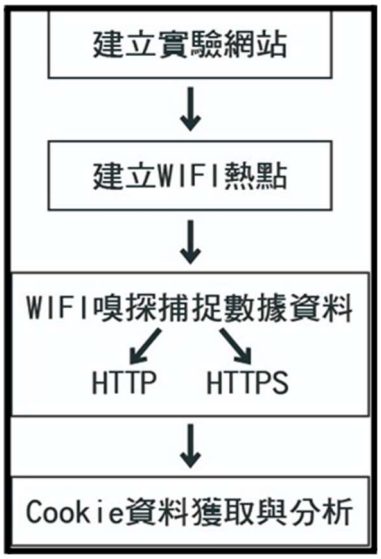
提供具體建議，讓用戶、企業與開發者提高無線網路的資安防護措施。

(二.) 假設：

公共 Wi-Fi 環境下，未加密的 HTTP 網站會導致 Cookie 容易被竊取。

攻擊者可透過 Wi-Fi 嗅探技術，輕易取得用戶的登入憑證並進行身分冒充。

HTTPS 加密機制能有效降低 Cookie 被竊取的風險。



圖一：研究流程圖

圖一資料來源：研究者自繪

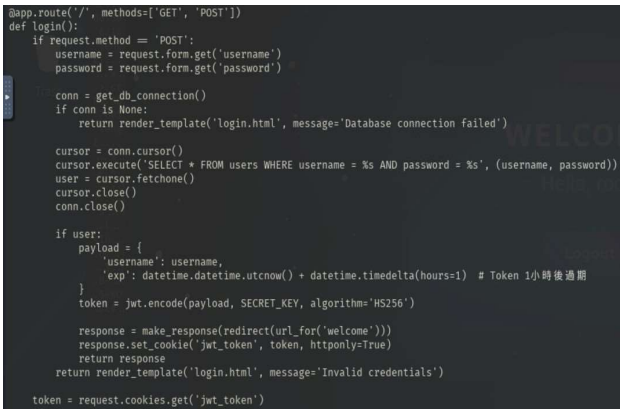
四、探究方法與驗證步驟

(一.) 建立實驗網站

使用 Flask 建立 Web 服務，整合 MySQL 驗證登入機制，模擬 HTTP 與 HTTPS 版本網站。設定 JWT Cookie，測試其在不同網路環境下的安全性。

圖二：網站檔案

資料來源：研究者截圖



```
@app.route('/', methods=['GET', 'POST'])
def login():
    if request.method == 'POST':
        username = request.form.get('username')
        password = request.form.get('password')

        conn = get_db_connection()
        if conn is None:
            return render_template('login.html', message='Database connection failed')

        cursor = conn.cursor()
        cursor.execute('SELECT * FROM users WHERE username = %s AND password = %s', (username, password))
        user = cursor.fetchone()
        cursor.close()
        conn.close()

        if user:
            payload = {
                'username': username,
                'exp': datetime.datetime.utcnow() + datetime.timedelta(hours=1)  # Token 1小時後過期
            }
            token = jwt.encode(payload, SECRET_KEY, algorithm='HS256')

            response = make_response(redirect(url_for('welcome')))
            response.set_cookie('jwt_token', token, httponly=True)
            return response
        return render_template('login.html', message='Invalid credentials')

    token = request.cookies.get('jwt_token')
```

圖三：cookie 設定程式

資料來源：研究者截圖

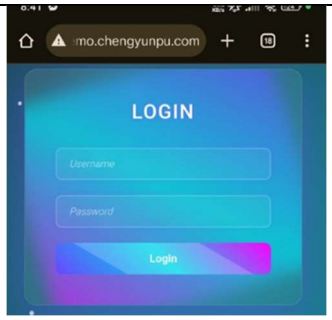
```
ubuntu@ubuntu:~/tmp/web3$ docker-compose up -d
Creating network "web3_default" with the default driver
Creating web3_web_1 ... done
ubuntu@ubuntu:~/tmp/web3$ cat /etc/nginx/sites-available/default | grep demo -B 2 -A 9
server {
    listen 80;
    server_name demo.chengyunpu.com;

    location / {
        proxy_pass http://127.0.0.1:9011/;
        proxy_set_header Host $host;
        proxy_set_header X-Real-IP $remote_addr;
        proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
        proxy_set_header X-Forwarded-Proto $scheme;
    }

ubuntu@ubuntu:~/tmp/web3$
```

圖四：伺服器配置

資料來源：研究者截圖



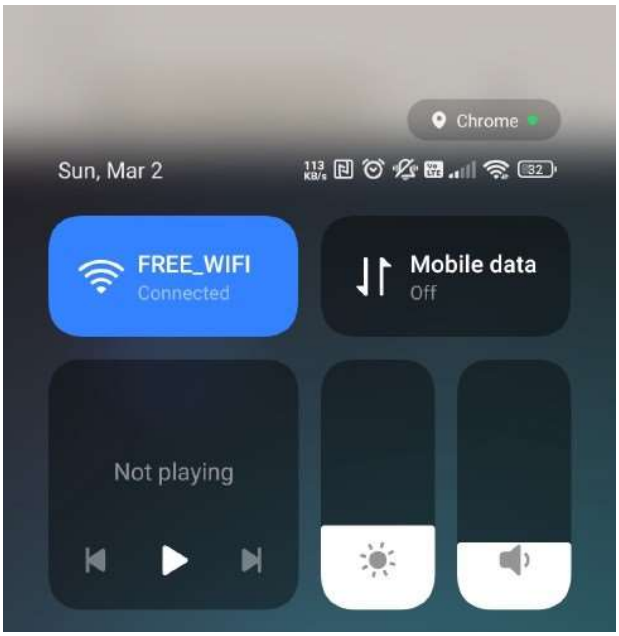
圖五：使用 WIFI 透過網際網路連到模擬網站

資料來源：研究者截圖

(二.) 架設 Wi-Fi 熱點

使用 Kali Linux 設置無加密 Wi-Fi (SSID: FREE_WIFI)，並允許設備連線。

設定 IP 轉發與 NAT，使設備可透過此熱點存取網際網路。



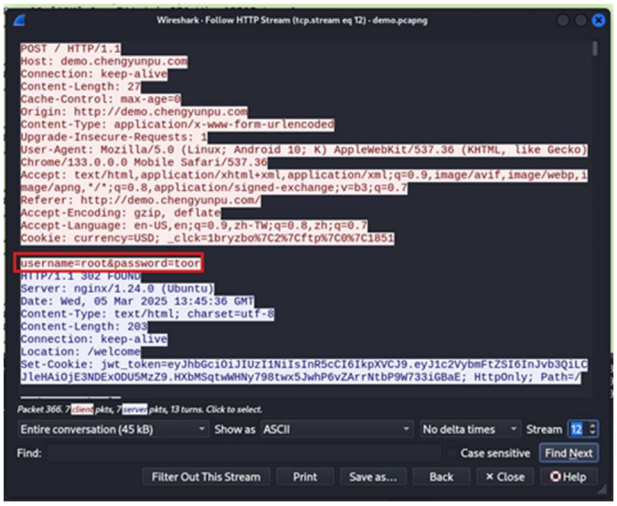
圖七：成功建立 WIFI 熱點並連接

資料來源：研究者截圖

(三.) Wi-Fi 嗅探攻擊模擬

使用 Wireshark 監控 Wi-Fi 熱點的數據流量，分析 HTTP 與 HTTPS Cookie 的傳輸情況。

設定封包過濾條件，篩選出 HTTP Cookie 並記錄可被攔截的數據。

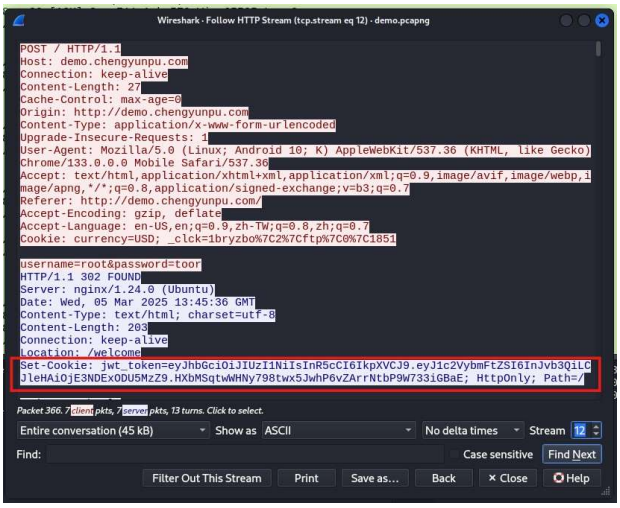


圖八：登入憑證

(四.) Cookie 竊取與分析

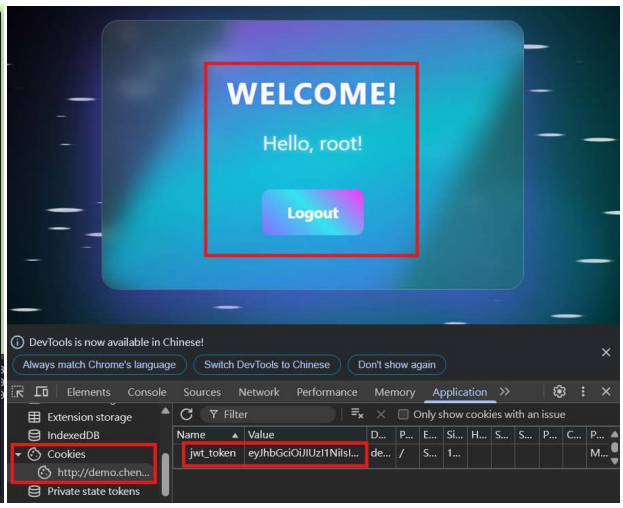
嘗試使用攔截到的 Cookie 在不同裝置上進行身份冒充，驗證 Session Hijacking 的可行性。

比較 HTTP 與 HTTPS 在 Cookie 保護上的差異，分析 HTTPS 的防禦效果。



圖九：捕獲 cookie

資料來源：研究者截圖



圖十：透過獲捕到的 cookie 進行登入

資料來源：研究者截圖

五、 結論與生活應用

(一.) 結論：

1. HTTP 連線 Cookie 泄露風險高：當使用者透過未加密的 HTTP 網站傳送資料時，其

Cookie 極可能被惡意攔截者取得，進而進行會話劫持等攻擊。

2. HTTPS 可有效保護用戶數據：透過 SSL/TLS 加密協議，HTTPS 能有效防止 Cookie 在傳輸過程中外洩，大幅提升用戶資料的保密性與完整性
3. Wi-Fi 嗅探攻擊容易實施：攻擊者僅需設置無加密熱點與基本工具，即可實施攔截行為。若使用者未加警覺，便可能在日常中無意洩露個資。

(二.) 生活應用與建議：

1. 避免連接來路不明的 Wi-Fi：若需使用，應搭配 VPN 進行流量加密。
2. 檢查網站是否為 HTTPS：登入前確認網址是否有鎖頭標誌，避免在 HTTP 網站輸入敏感資訊。
3. 定期清除 Cookie，避免長時間登入：減少 Session Hijacking 風險
4. 開發者應使用 HttpOnly 與 Secure 屬性保護 Cookie，避免被 JavaScript 或未加密連線存取。

參考資料

張文奕（2023 年 7 月 12 日）。無線網路之中間人攻擊手法與防護研究。國立屏東大學資訊學院電腦科學與人工智慧學系：碩士論文。https://hdl.handle.net/11296/yt954d

中華電信資訊技術分公司 (2024 年 5 月 9 日)。Wi-Fi 無線網路安全與防護新知。https://reurl.cc/86KZxd

台灣電腦網路危機處理中心 TWCERT（2019 年 3 月 13 日）。免費的最貴，公用 Wi-Fi 背後的真相。https://www.twcert.org.tw/tw/cp-15-50-e49ce-1.html

台灣電腦網路危機處理中心 TWCERT（2023 年 11 月 28 日）。十大常見的資安不安全設定。 https://www.twcert.org.tw/tw/cp-14-7555-68615-1.html

美國國土安全部資安機構 CISA（2023 年 10 月 5 日）。 AA23-278A 資安通報 NSA and CISA Red and Blue Teams Share Top Ten Cybersecurity Misconfigurations 。https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-278a

Kaspersky（2020 年 10 月 8 日）。什麼是 Cookie？。https://reurl.cc/Y42rMX