

TeamViewer能夠在NAT伺服器後面成功進行遠端控制的NAT穿透技術：

**原理**

收集候選傳輸位址：Caller和Callee各自收集能提供IP流量的位址（Transport Candidates）

交換候選傳輸位址：利用SIP協定結合Offer/Answer模式交換收集到的Transport Candidates

配對候選傳輸位址：根據收集到的Transport Candidates，整合出可能的候選配對組（Candidate Pair）

連線測試：進行點對點連線測試，確定最佳的連線

建立實際連線：選擇一條成功的連線作為實際傳輸路徑

**操作流程**

收集Transport Candidates：Caller和Callee各自收集自己的Transport Candidates

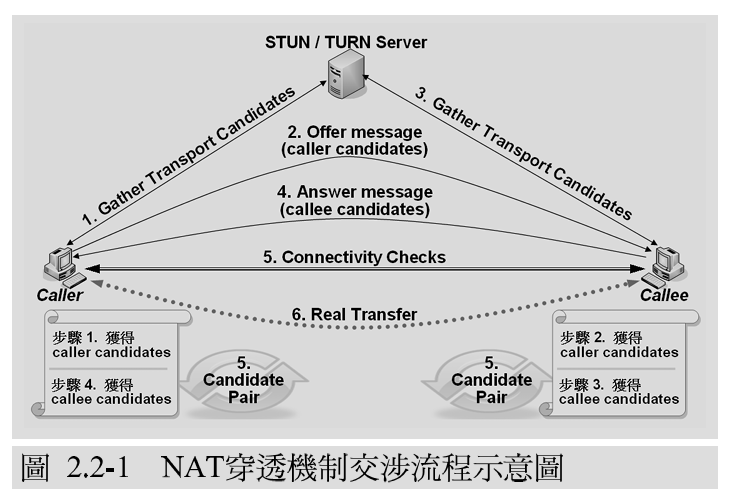
發送Offer訊息：Caller使用SDP協定描述Transport Candidates後，將訊息發送給Callee

Callee收集Transport Candidates：Callee同意通訊後，收集自己的Transport Candidates

回應Answer訊息：Callee使用SDP協定描述自己的Transport Candidates後，回傳給Caller

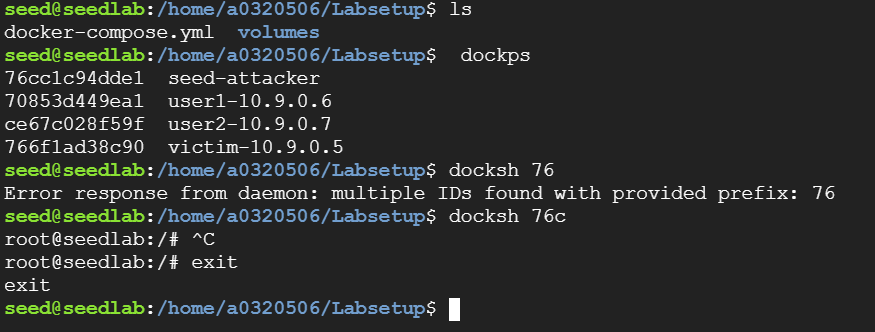
進行互連測試：Caller和Callee各自根據Candidate Pair進行點對點互連測試

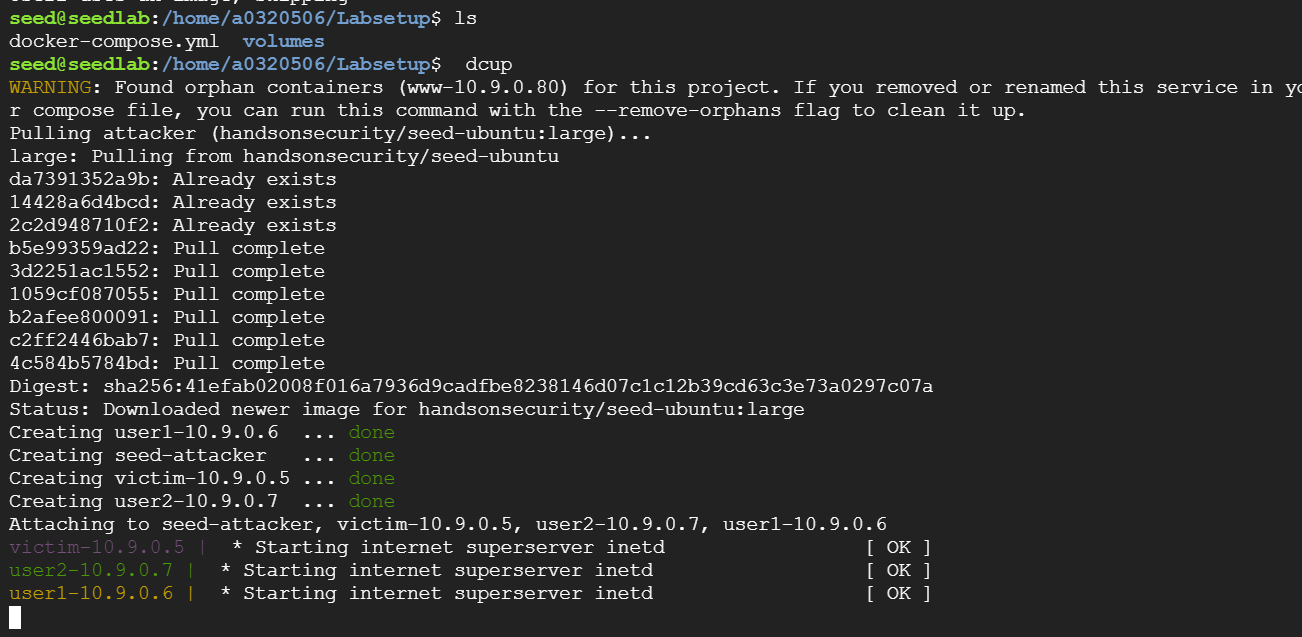
建立實際連線：選擇一條成功的連線作為實際傳輸路徑

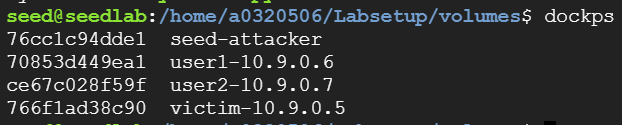


賴靜瑛（2009）。互動式連線建立之NAT穿透整合技術。電腦與通訊，(129)，99-108。<https://doi.org/10.29917/CCLTJ.200909.0014>

Docker相關



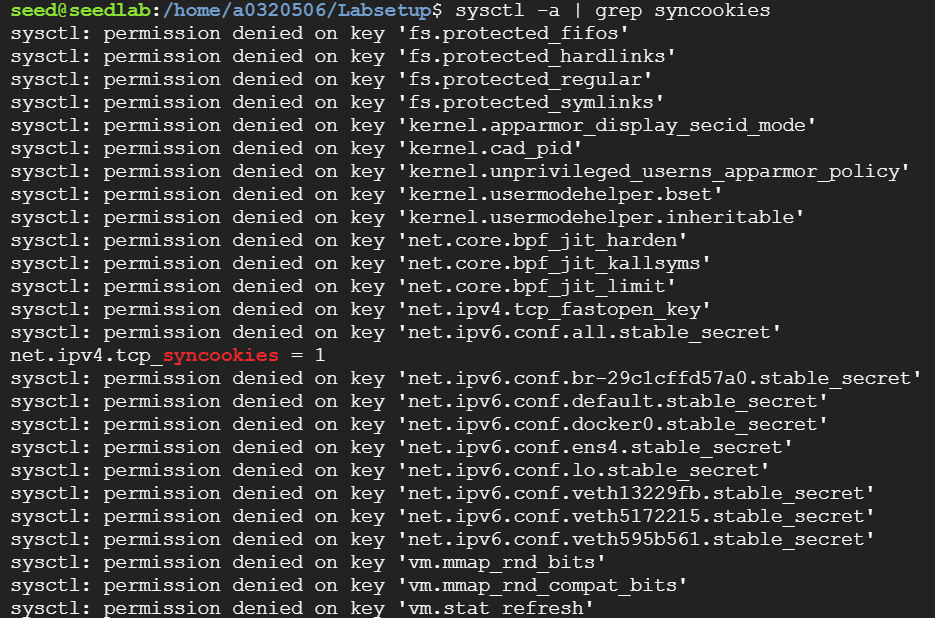


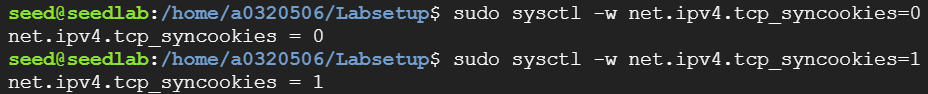


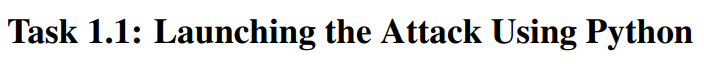




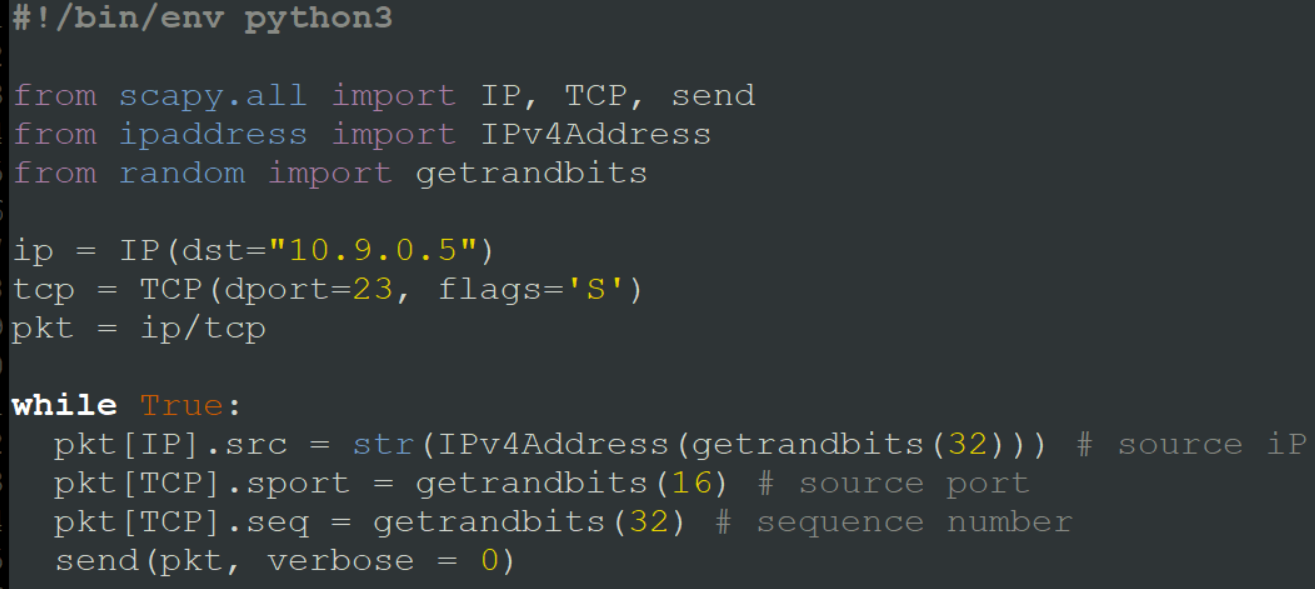




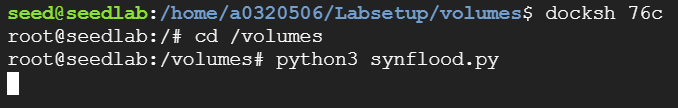




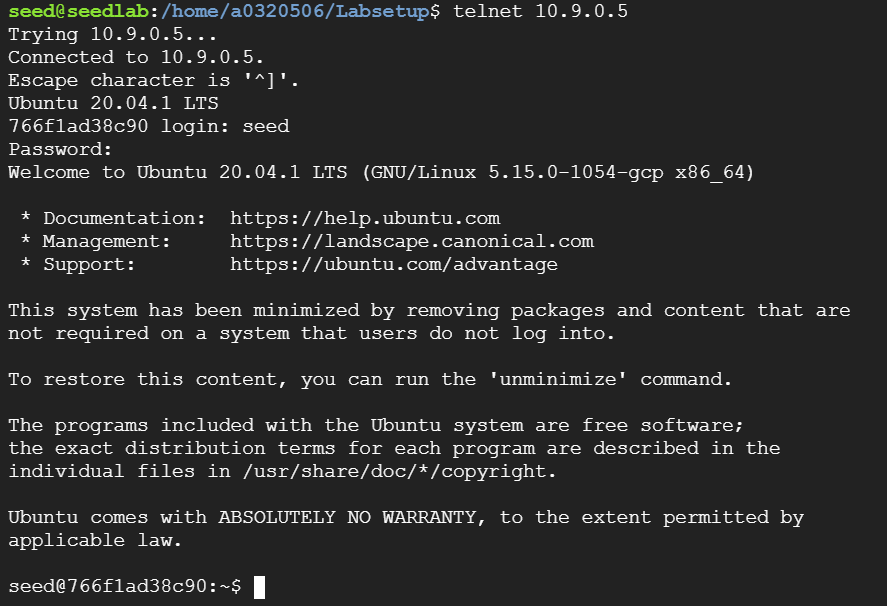
synflood.py



在seed-attacker執行攻擊

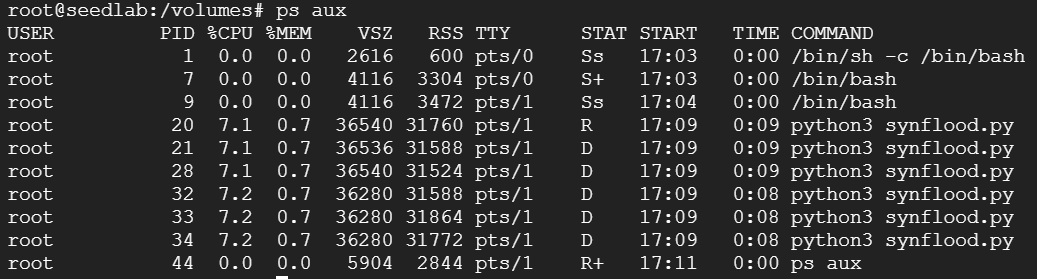


可以登入victim：攻擊失敗

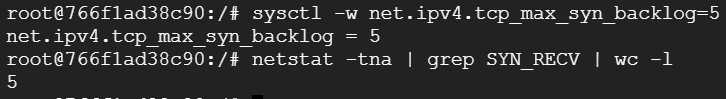


**【為了讓攻擊成功】**

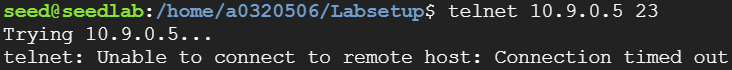
1. 強化攻擊：在seed-attacker同時執行6個攻擊程式



2. 削弱防禦：將victim-10.9.0.5的半開區間減到5



攻擊成功：無法連線至victim-10.9.0.5

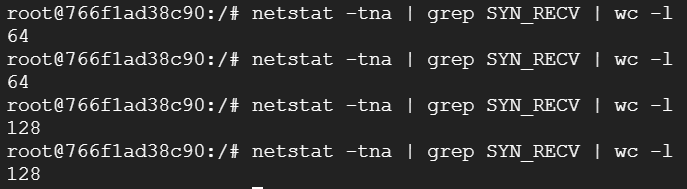




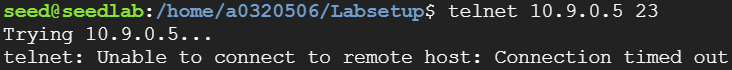




攻擊前64 攻擊後128



攻擊成功



**比較：**和python相比，用C語言攻擊一次就成功，不需要增加攻擊程式執行次數或調整半開區間

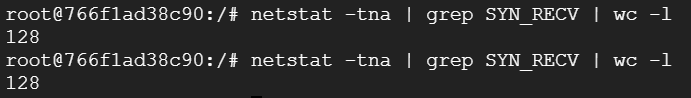
**可能的原因：**

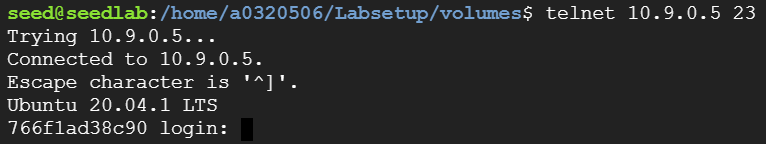
1. 攻擊速度：C語言的程式比Python程式更快速，能夠以更快的速度發送大量的攻擊封包，導致目標機器的半開連接隊列迅速被填滿

2. 封包生成和發送效率：C語言通常比Python更靠近硬體層，能夠更有效地生成和發送封包，從而降低攻擊的延遲和效率損失





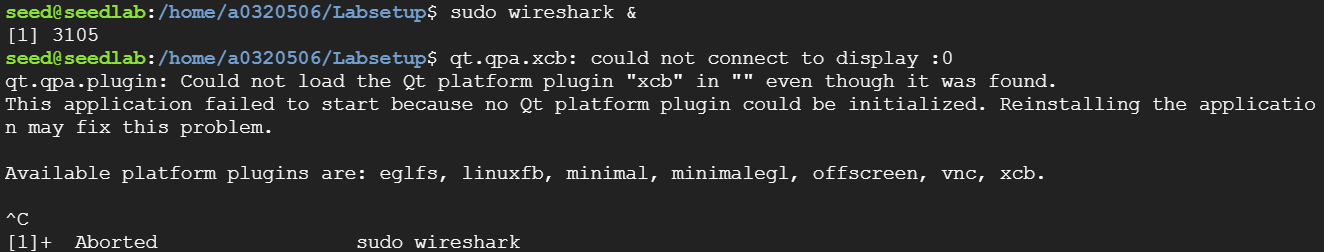


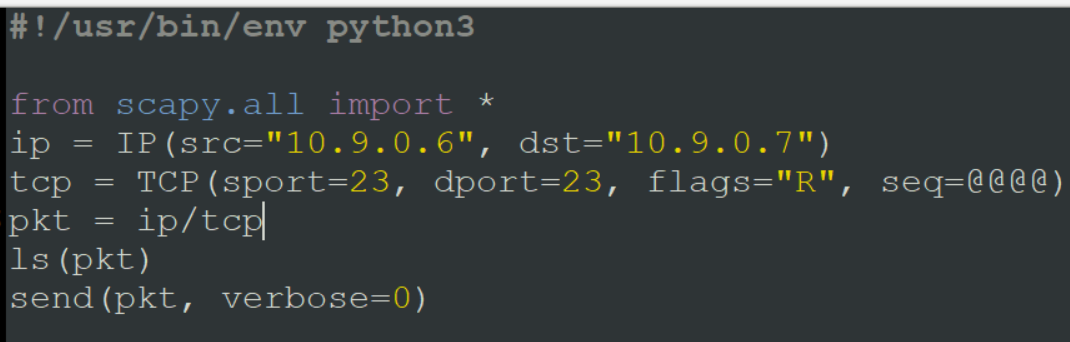


SYN cookie機制允許狀態資訊作為SYN-ACK和ACK封包的一部分儲存在cookie中，而不是儲存在victim的flow table中，由於流程表沒有被填滿，因此當發生SYN洪氾攻擊時，flow table不會出現緩衝區溢位問題，因此victim將能夠服務更多請求



使用SSH連線進VM，無法開啟Wireshark，故無法得知seq，無法執行程式

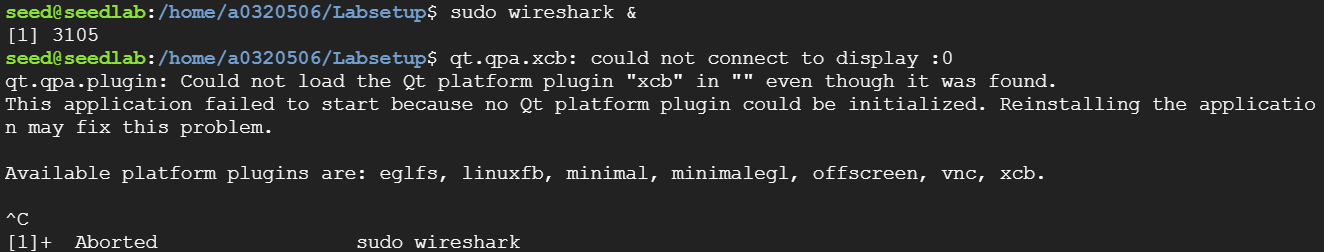




理論上發送攻擊後會讓A telnet連線到B 的連線斷掉



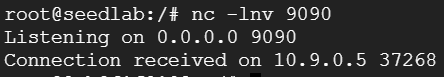
使用SSH連線進VM，無法開啟Wireshark，故無法得知seq，無法執行程式



理論上因為被劫持了，並將惡意命令注入到telnet，Telnet服務器會執行攻擊者所發送的惡意命令



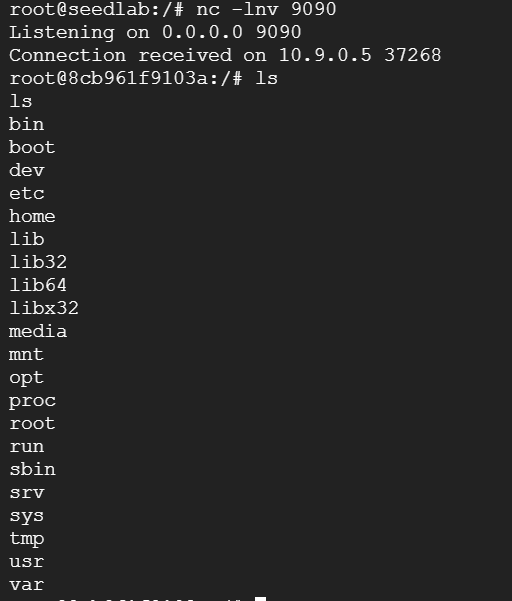
seed-attacker



victim

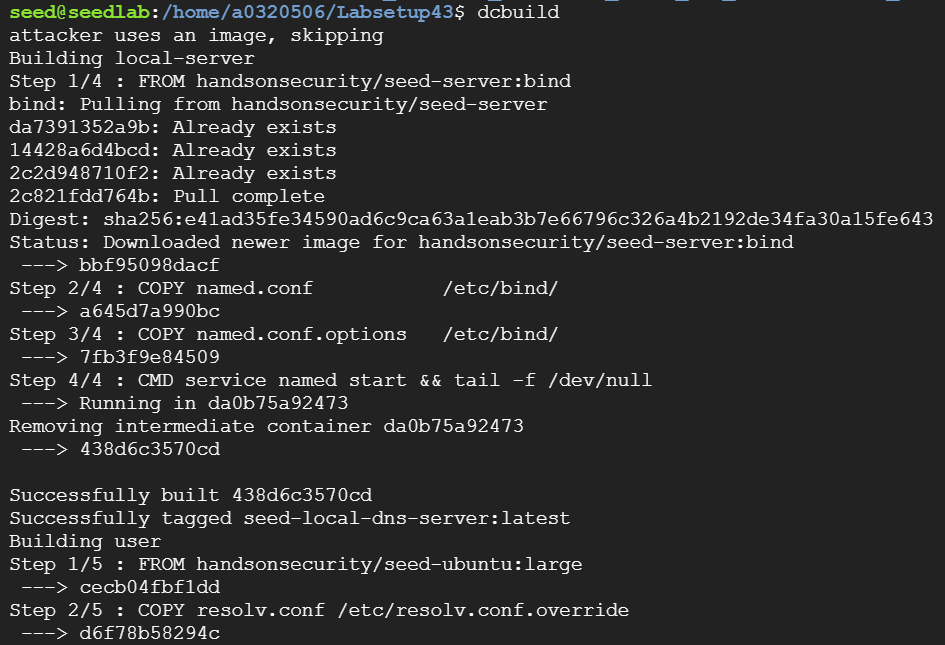


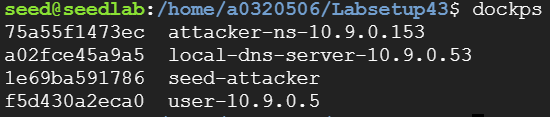
成功遠程執行命令



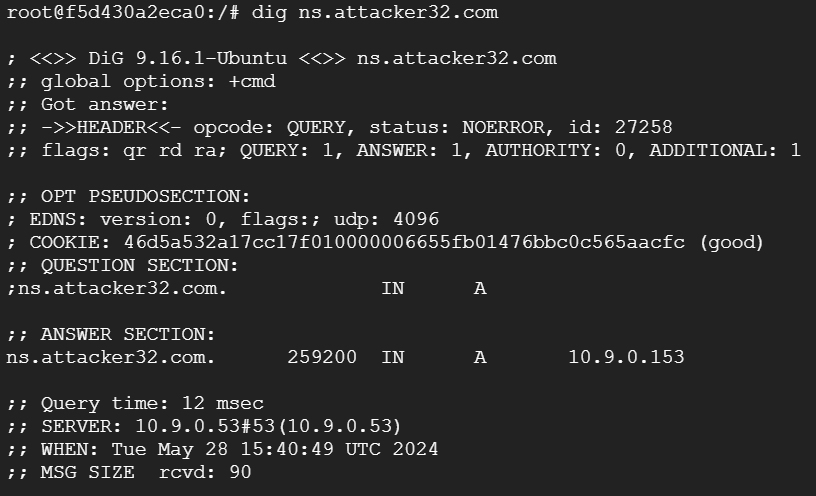








dig ns.attacker32.com 表示查詢域名 ns.attacker32.com 的 DNS 記錄



**查詢結果：**

HEADER：查詢成功返回，狀態是 NOERROR，表示查詢沒有錯誤

QUESTION SECTION：顯示查詢的問題，即 ns.attacker32.com 的 A 記錄

ANSWER SECTION：提供答案，ns.attacker32.com 對應的 IP 地址是 10.9.0.153

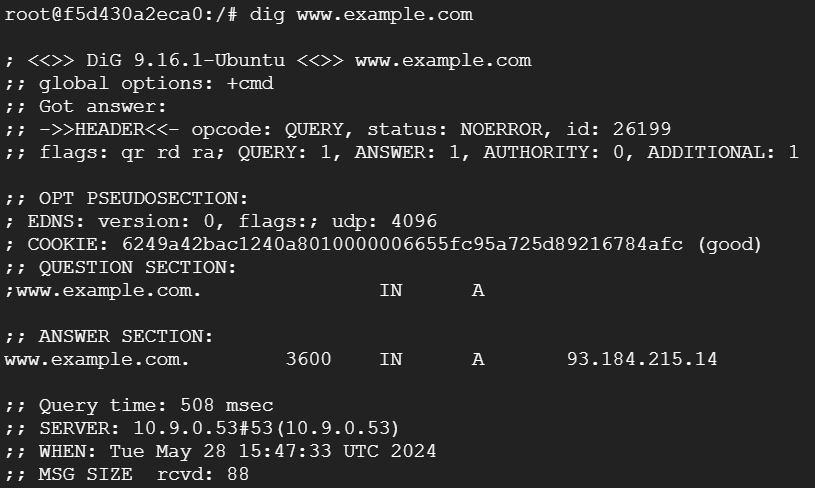
**附加資訊：**

Query time：查詢耗時 12 毫秒。

SERVER：使用的 DNS 伺服器是 10.9.0.53

EDNS：顯示擴展 DNS 資訊，包含 cookie

dig www.example.com 表示查詢域名 www.example.com 的 DNS 記錄



**查詢結果：**

HEADER：查詢成功返回，狀態是 NOERROR，表示查詢沒有錯誤

QUESTION SECTION：顯示查詢的問題，即 www.example.com 的 A 記錄

ANSWER SECTION：提供答案，www.example.com 對應的 IP 地址是 93.184.215.14

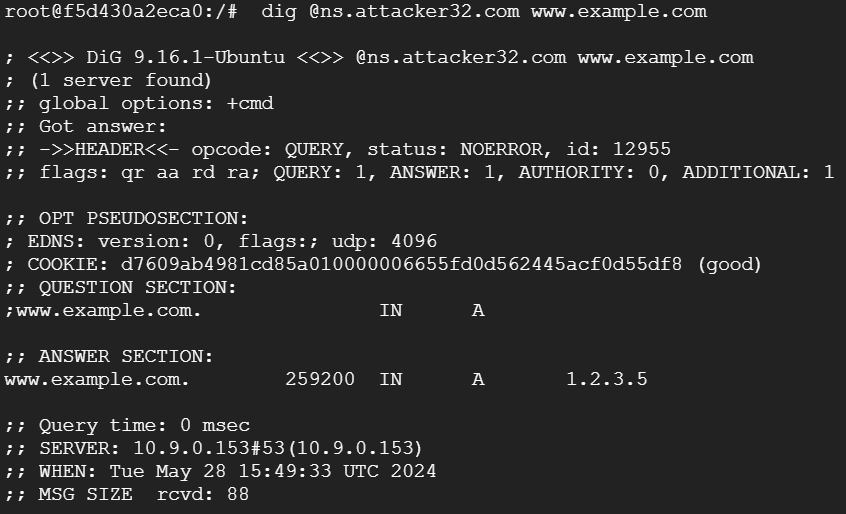
**附加資訊：**

Query time：查詢耗時 508 毫秒

SERVER：使用的 DNS 伺服器是 10.9.0.53

EDNS：顯示擴展 DNS 資訊，包含 cookie

dig @ns.attacker32.com www.example.com表示查詢www.example.com的A記錄，並指定使用 ns.attacker32.com這個DNS伺服器



**查詢結果：**

HEADER：查詢成功返回，狀態是 NOERROR，表示查詢沒有錯誤

QUESTION SECTION：顯示查詢的問題，即 www.example.com 的 A 記錄

ANSWER SECTION：提供答案，www.example.com 對應的 IP 地址是 1.2.3.5

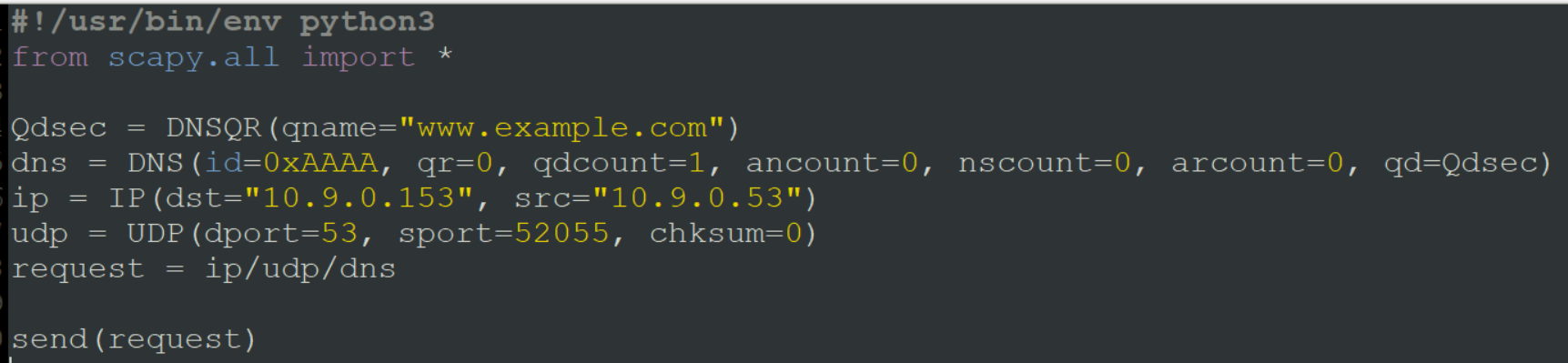
**附加資訊：**

Query time：查詢耗時 0 毫秒。

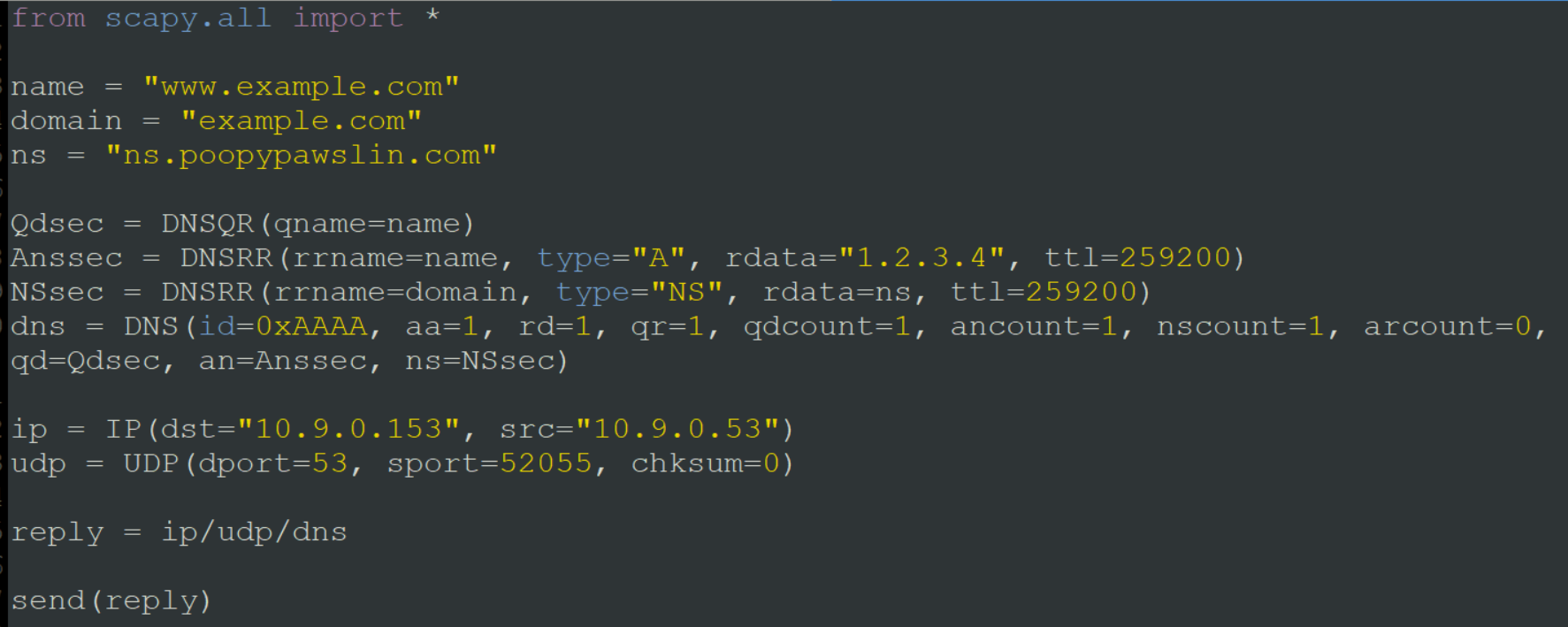
SERVER：使用的 DNS 伺服器是 10.9.0.153

EDNS：顯示擴展 DNS 資訊，包含 cookie





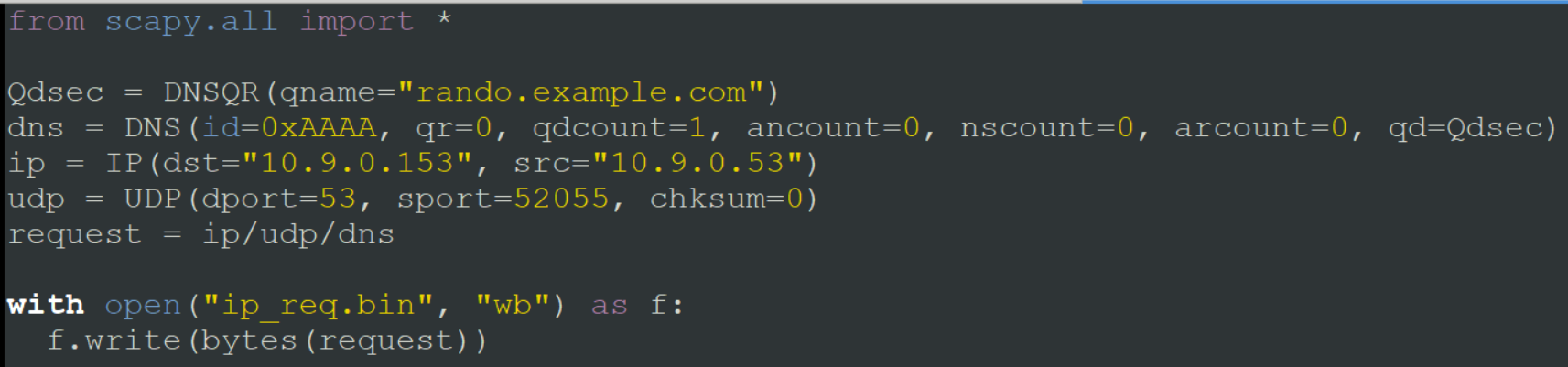
使用SSH連線進VM，無法開啟Wireshark，但理論上這支程式會觸發一系列封包的發送和接收



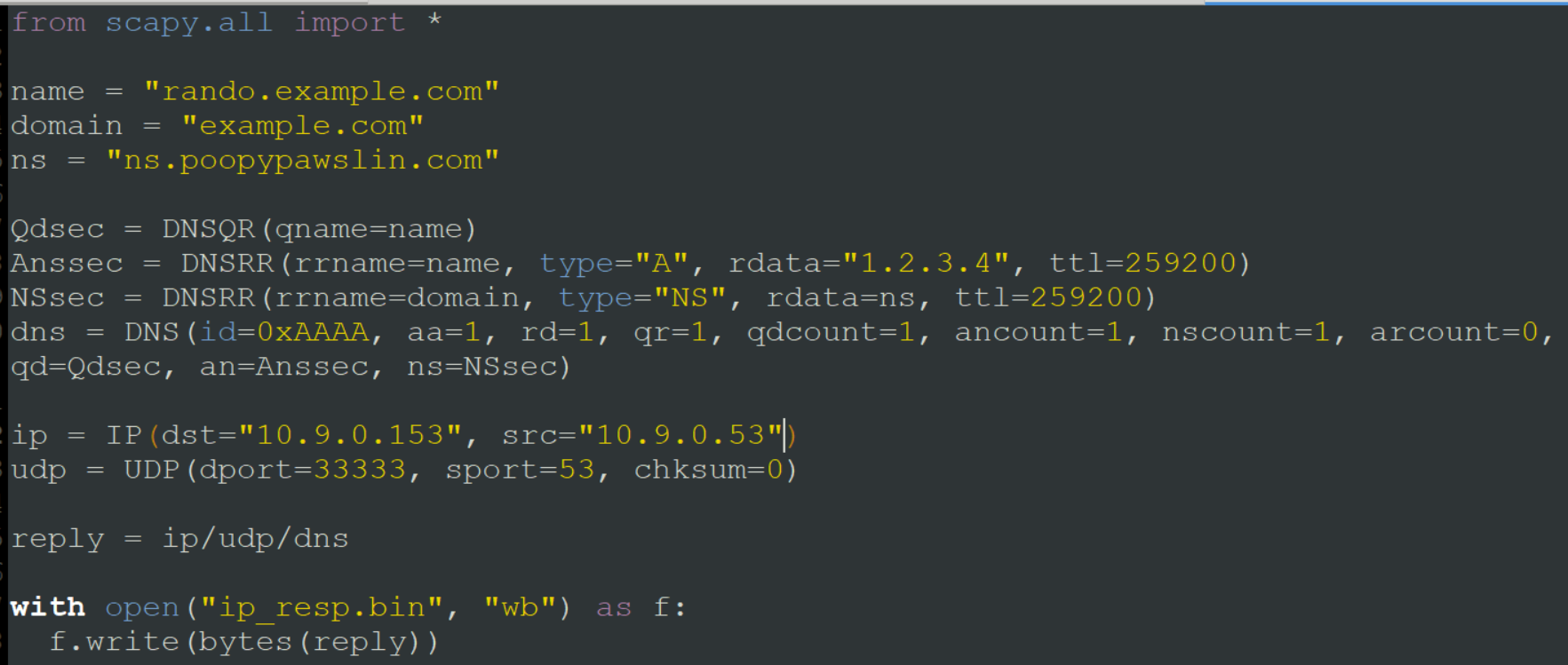
使用SSH連線進VM，無法開啟Wireshark，但理論上會接收到修改後的UDP封包



建立DNS請求的封包模板 template-DNS-request-packet.py



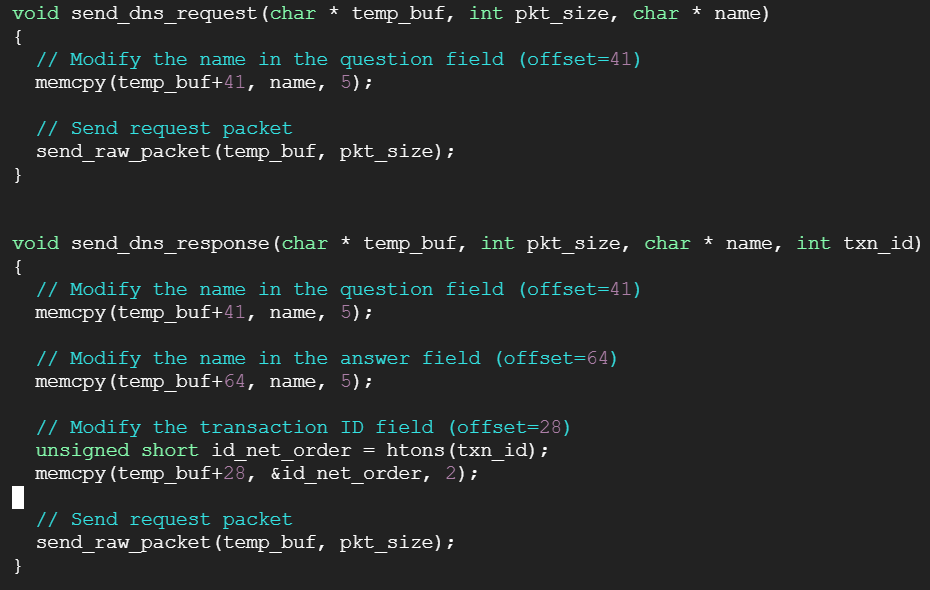
建立DNS回應的封包模板 template-DNS-response-packet.py



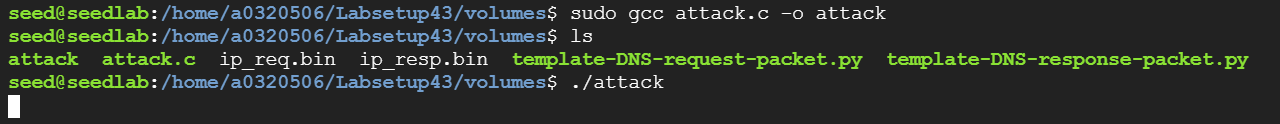
執行上面兩個程式



補完attack.c



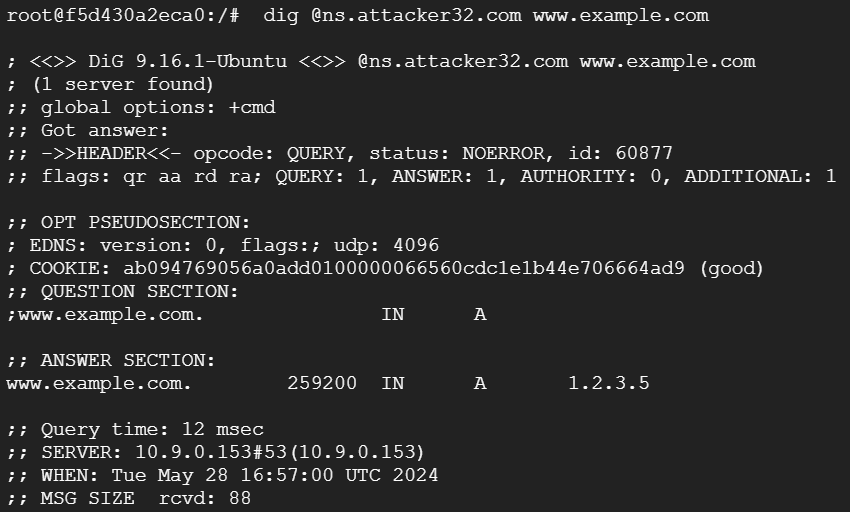
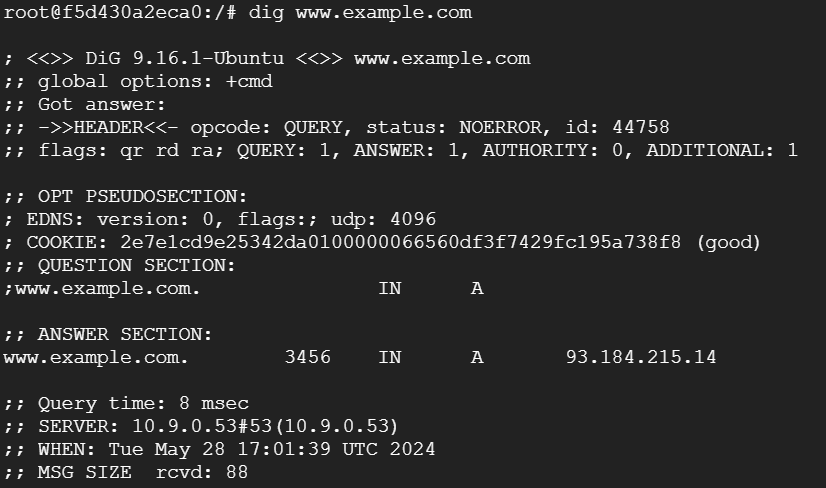
編譯+執行



在local-dns-server-10.9.0.53檢查DNS cache



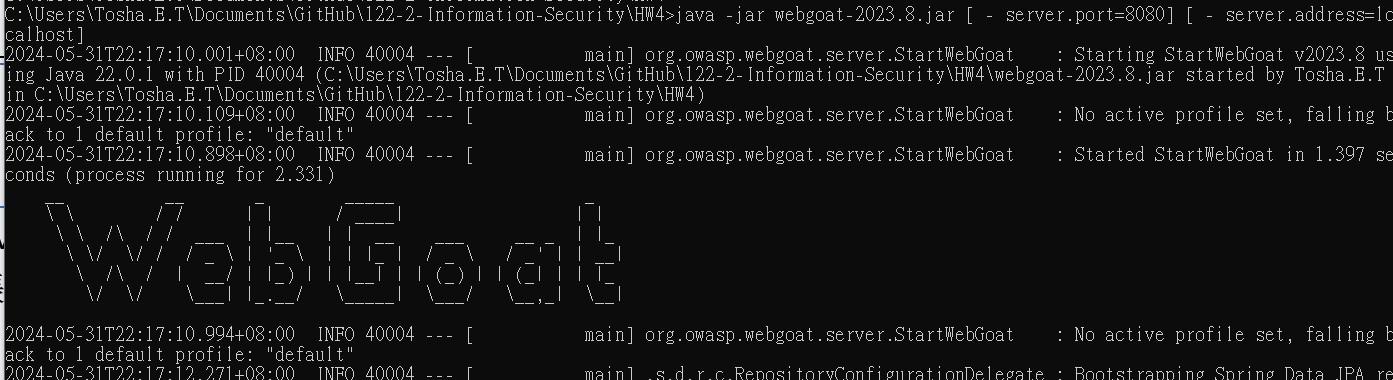




看起來沒有，但理論上本地DNS伺服器要直接向10.9.0.153的惡意伺服器ns.poopypawslin.com查詢答案，而不是執行遞歸DNS查詢，因為惡意伺服器已被快取為名稱伺服器

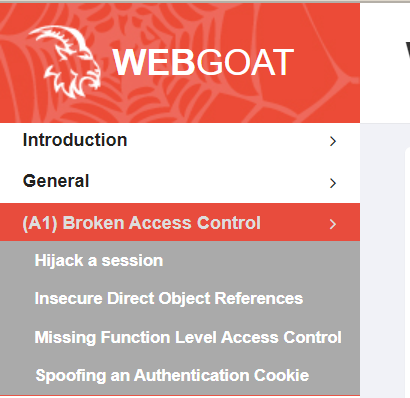


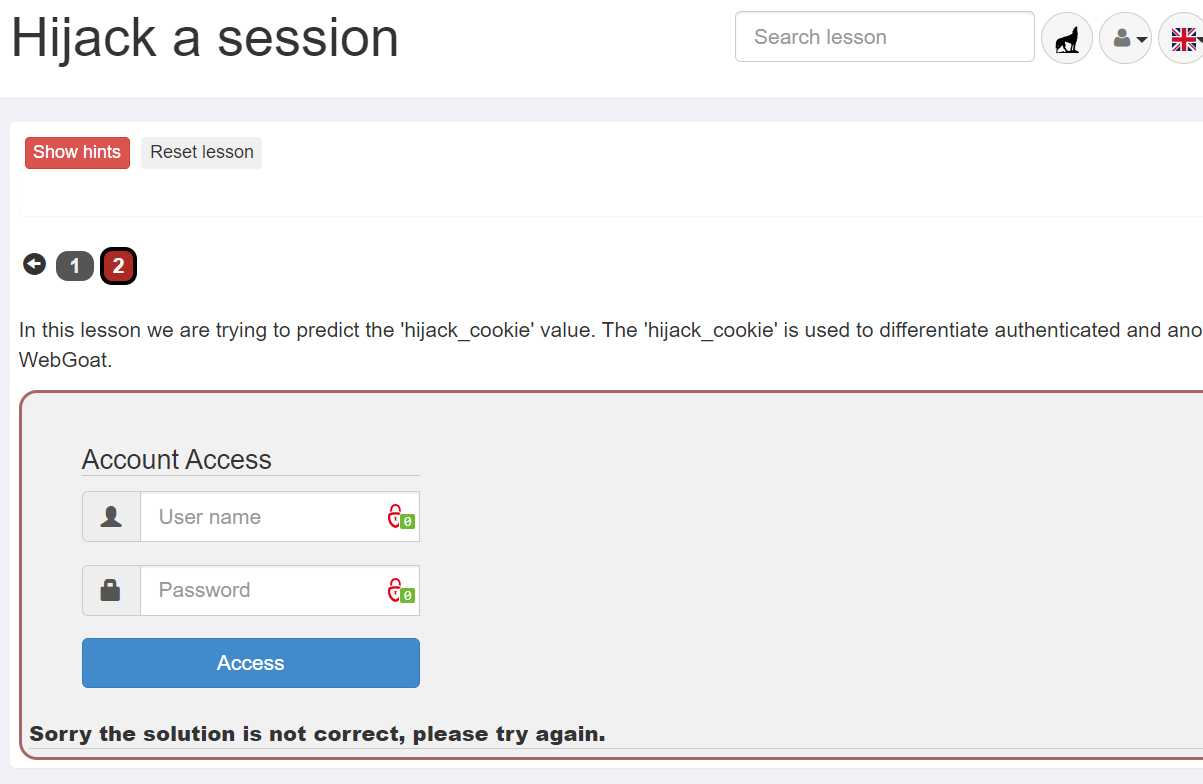
java -jar webgoat-2023.8.jar [ — server.port=8080] [ — server.address=localhost]



帳號: 40923129l 密碼: 40923129l

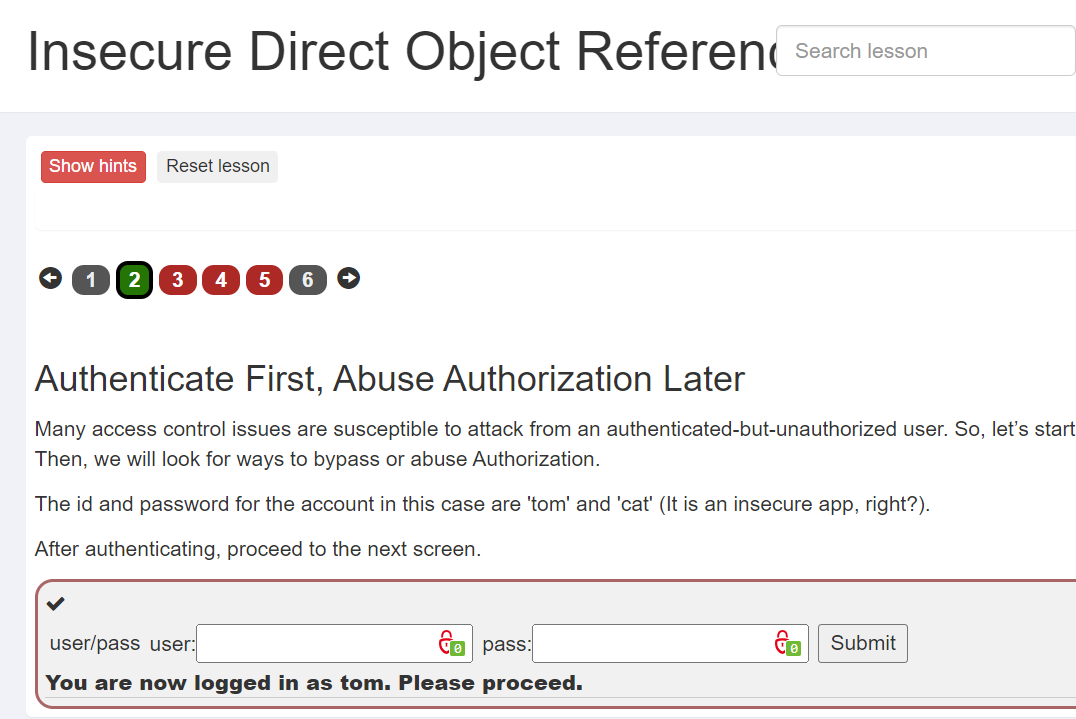
不知道為什麼沒辦法用封包抓取工具，所以有的不能直接做，所以有些改成參考網路資料進行學習

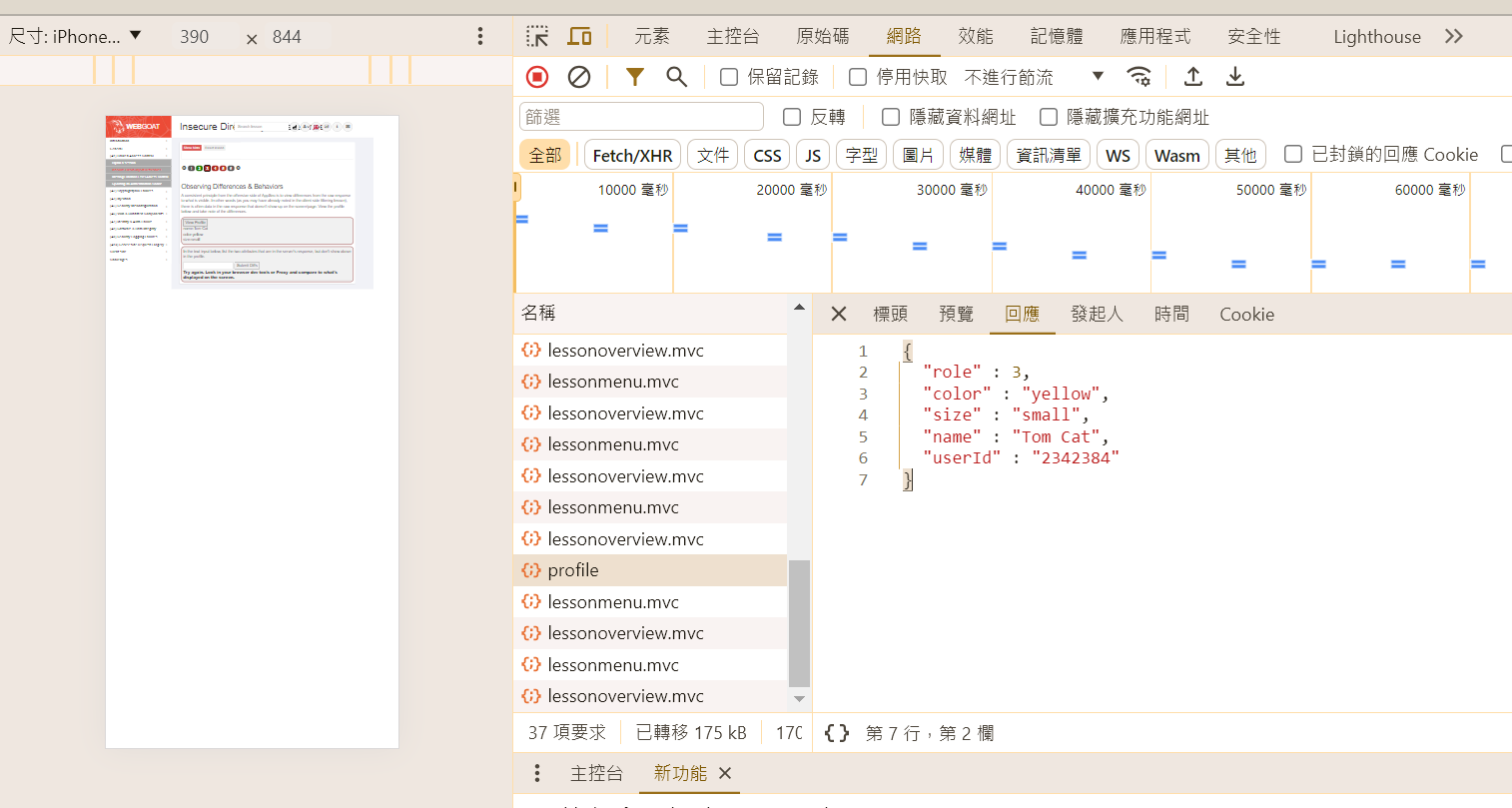




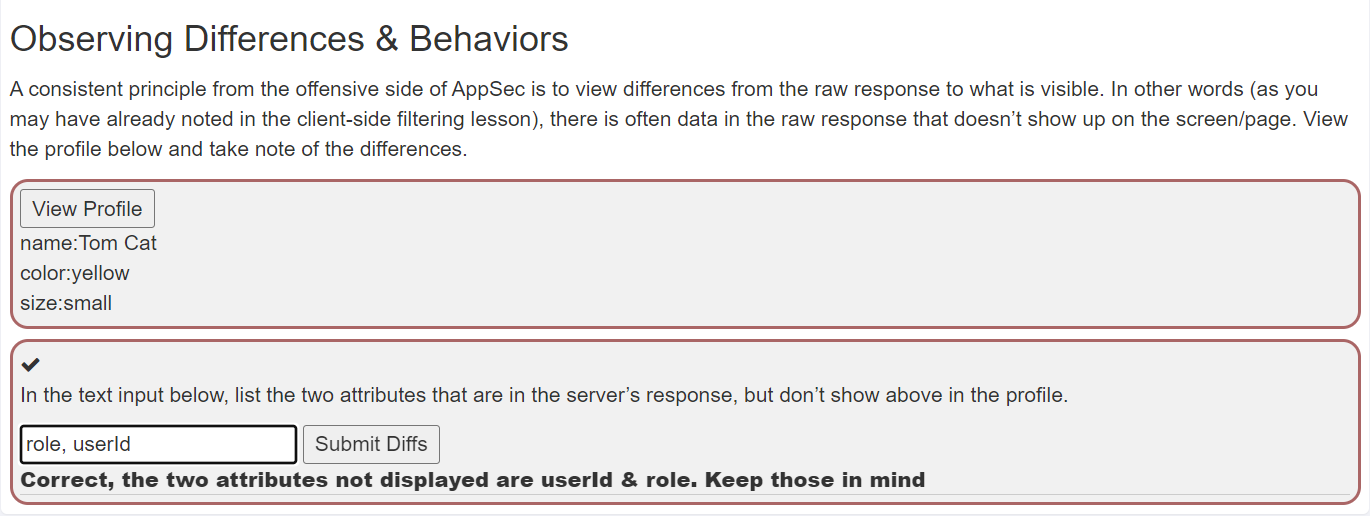
沒辦法處理封包

參考<https://blog.csdn.net/weixin_43639512/article/details/132621320>進行學習

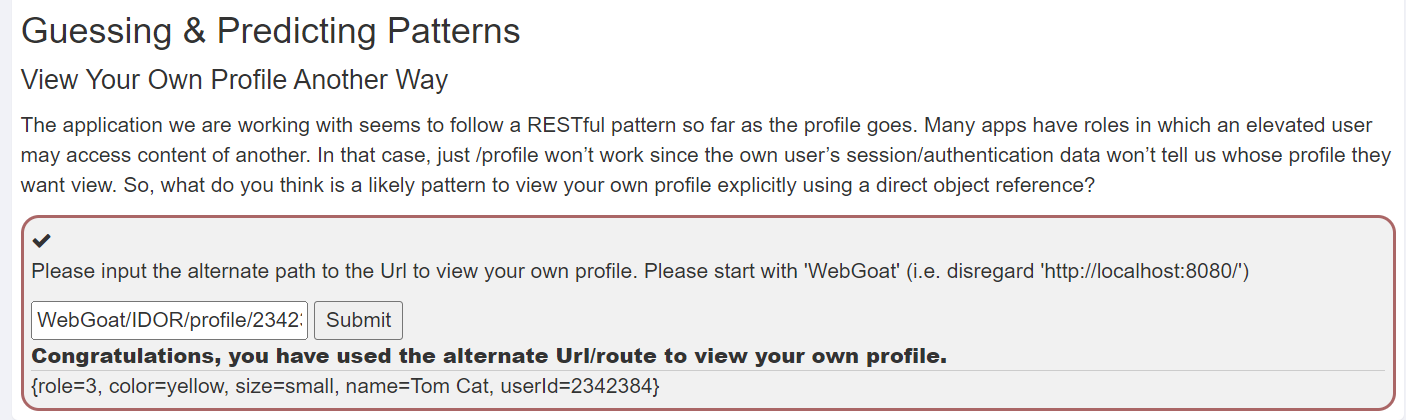


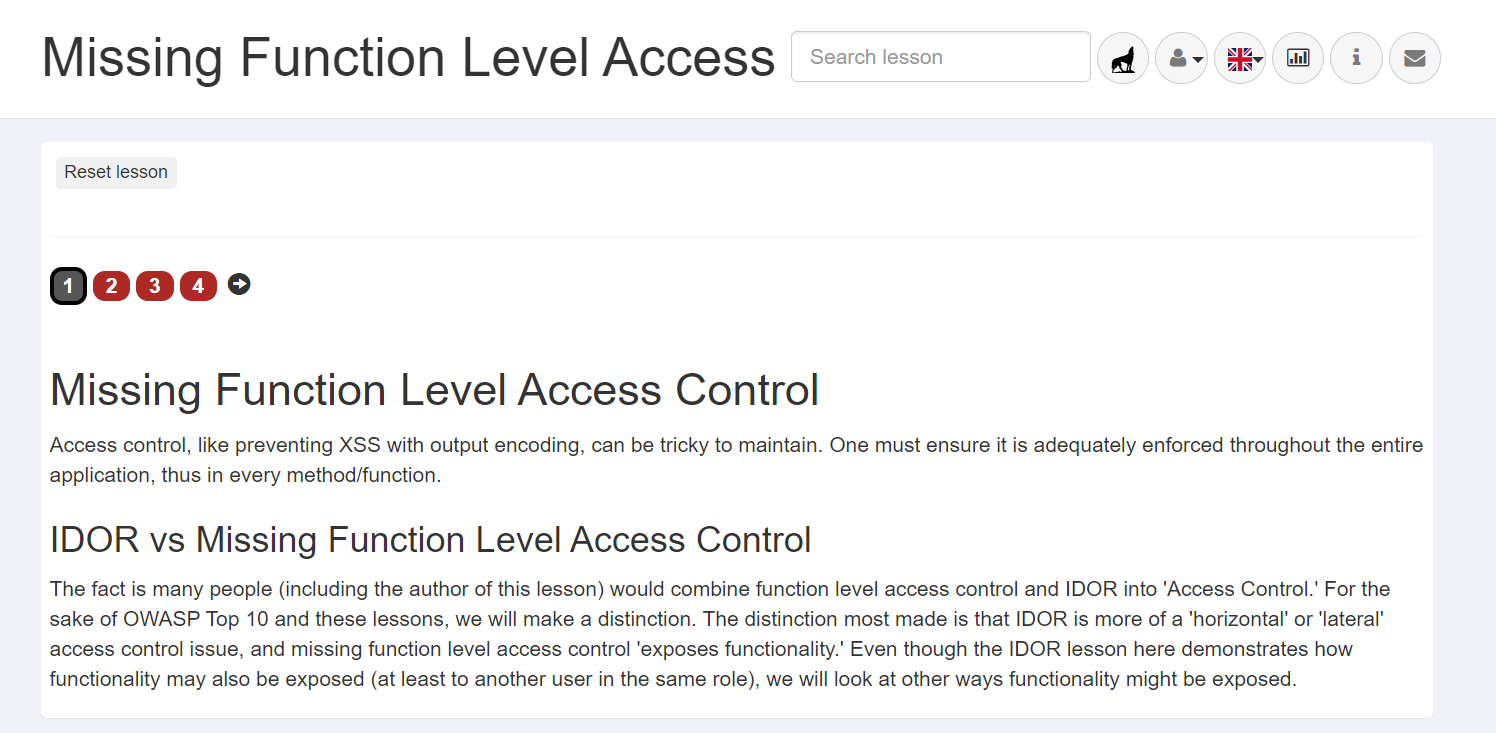


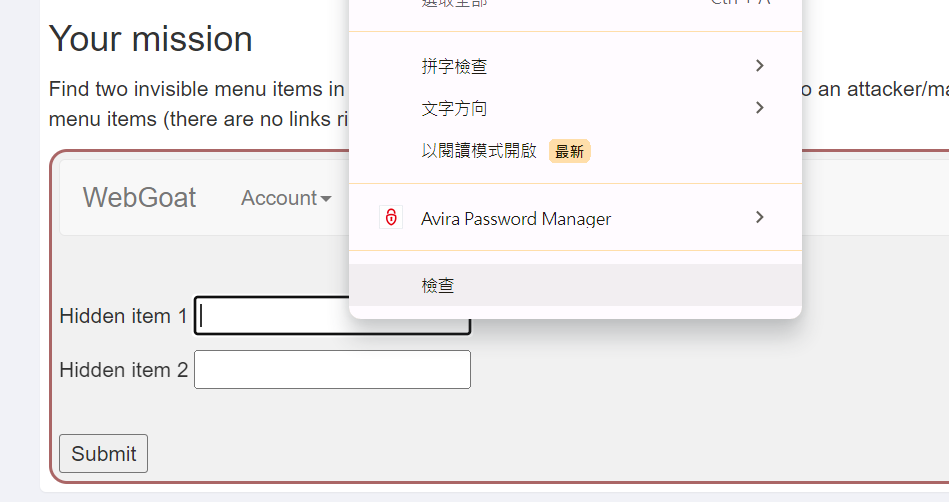
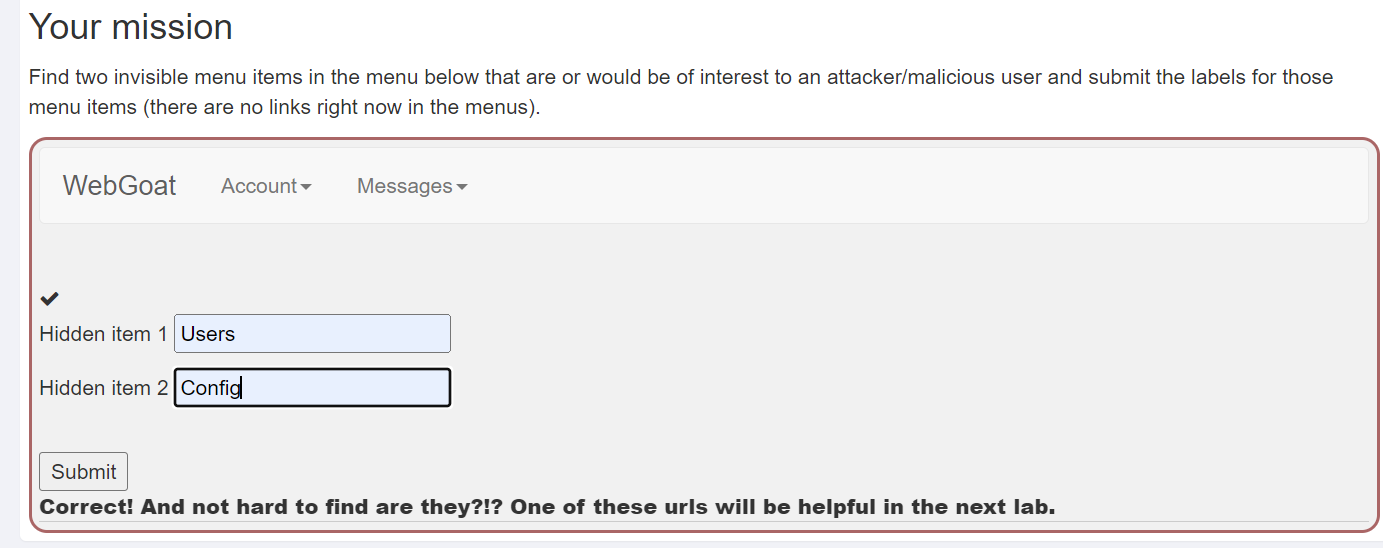
比對後發現role, userId不在網頁上

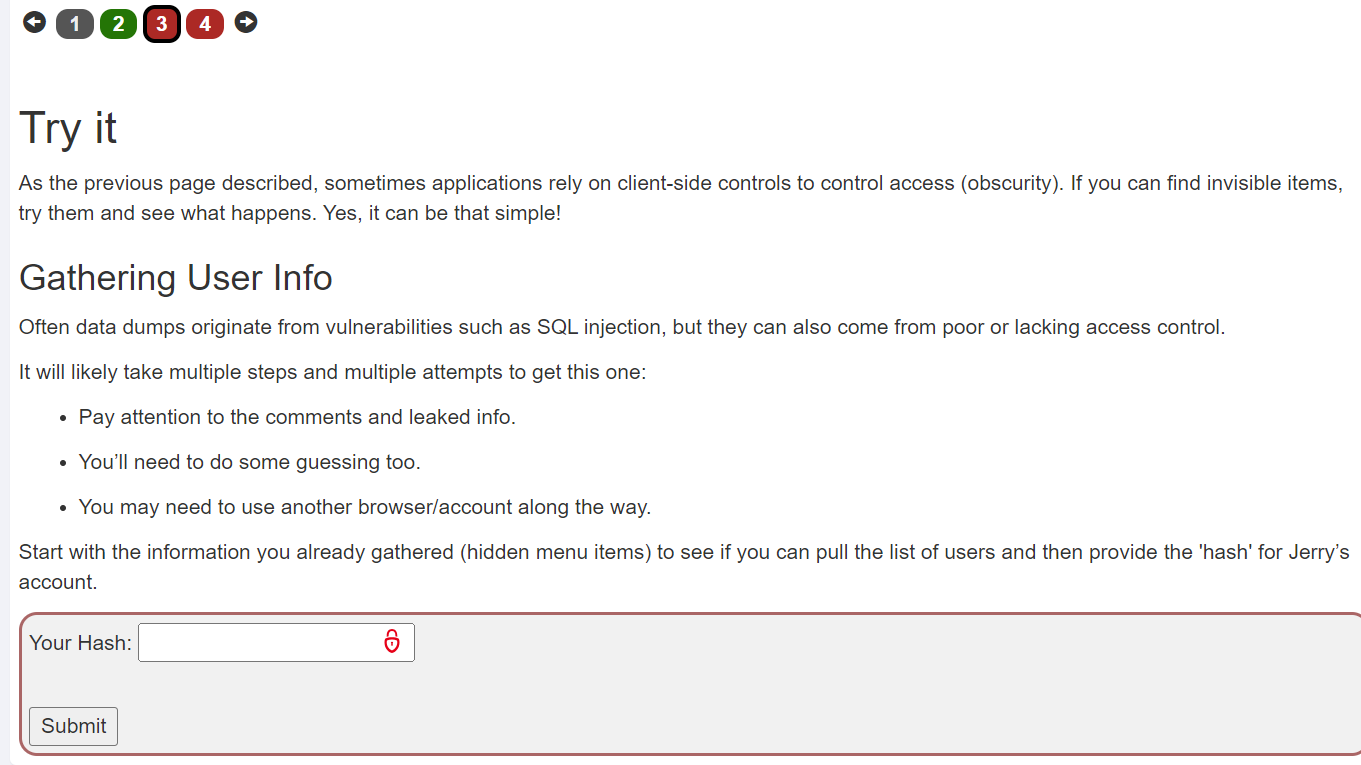


WebGoat/IDOR/profile/2342384



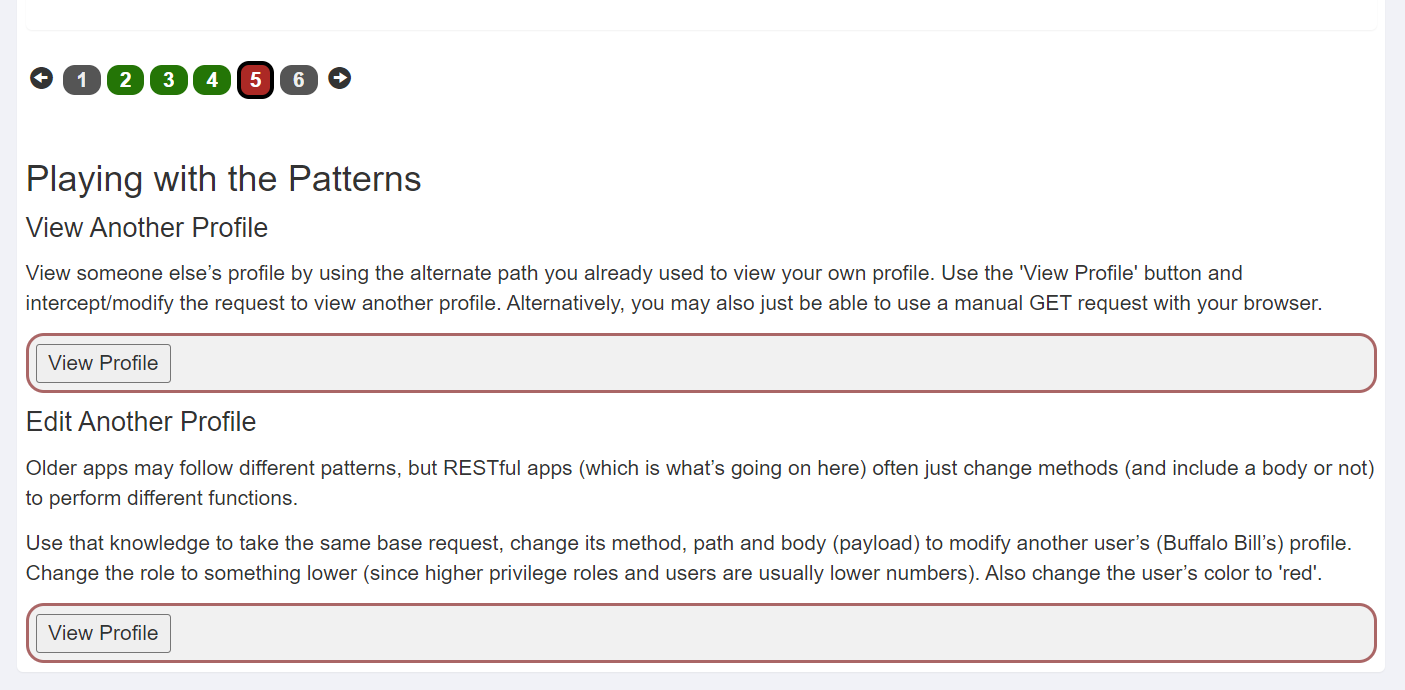




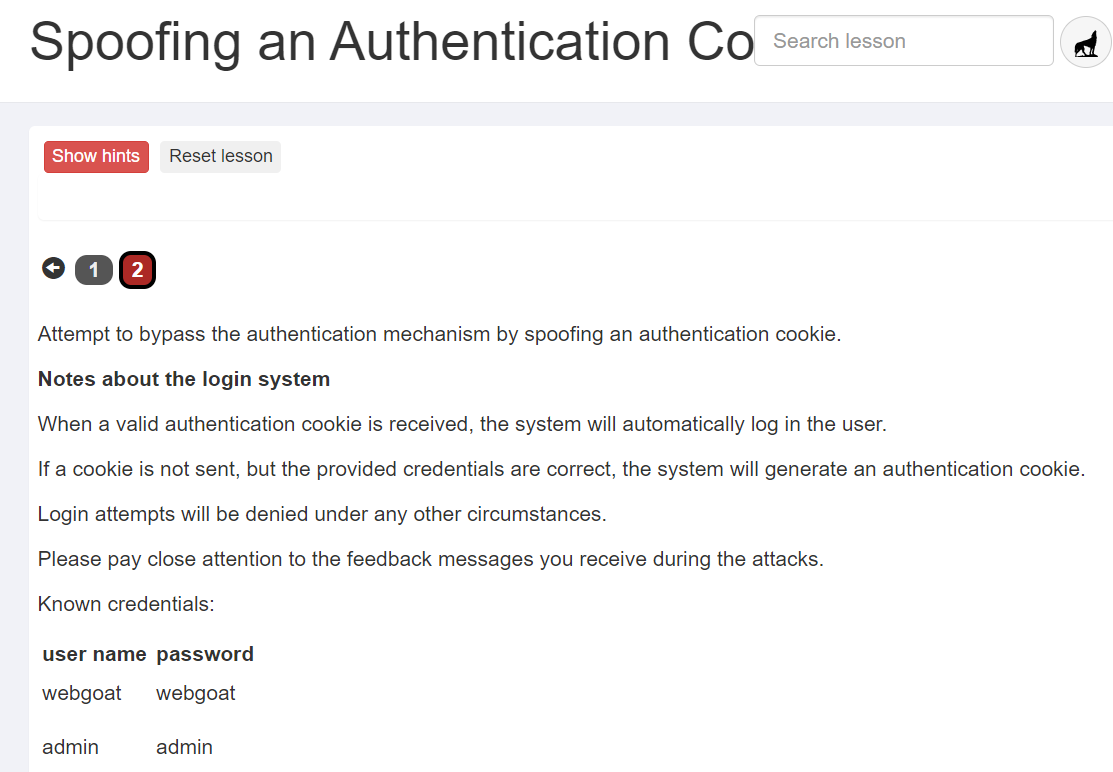
沒辦法處理封包

參考<https://blog.csdn.net/elephantxiang/article/details/114947393>進行學習



沒辦法處理封包

參考<https://blog.csdn.net/elephantxiang/article/details/114855007>進行學習



沒辦法處理封包

參考<https://www.youtube.com/watch?v=-n4OmhUN3vA&t=207s>進行學習