i春秋 “百度杯”CTF比赛 十月场 Vld

原创

「已注销」 于 2018-09-27 20:45:46 发布 1111 收藏

分类专栏： i春秋

友链：https://cutt.ly/7777aaaa

本文链接：https://blog.csdn.net/include_heqile/article/details/82873125

https://www.ichunqiu.com/battalion?t=1&r=0

`opcode`中的 `BEGIN_SILENCE`就是`@`，不显示报错信息

猜测`opcode`中的 `EXT_STMT`就是`;`，表示一个语句的结束

`opcode`中的`FETCH_R`意思是**从某个变量中取出值并把这个值赋给另一个变量**

详细信息参考php opcode

`JMPZ`，若比较结果为`false`，则跳转到指定地址处的代码

JMPZ

PHP code

```
<?php
/*
 * Jump to the address if the value is zero
 * opcode number: 43
 */
if($a != 0) echo "foo";
?>
```

PHP opcodes

如果比较结果为false，就会跳转到编号为4的opcode，执行RETURN

Function name: (null)

Compiled variables: !0=$a

line	#	op	fetch	ext	return	operands
6	0	IS_NOT_EQUAL			~0	!0,0
	1	JMPZ				~0,->4
	2	ECHO				'foo'
	3	JMP				->4
7	4	RETURN				1

对`vld`输出结果的分析如下：

```
<?php

echo 'do+you+know+Vulcan+Logic+Dumper%3F%3Cbr%3E';

$a = @$_GET['flag1'];
$b = @$_GET['flag2'];
$c = @$_GET['flag3'];

比较 $a 和 'fvhjjihfcv'是否相等
 如果不相等，跳转至38
 继续执行39，输出  'false%3Cbr%3E'

比较 $b 和 'gfuyiyhioyf'是否相等
 如果不相等，跳转至35
 继续执行36，输出  'false%3Cbr%3E'

比较 $c 和 'yugoiiyhi'是否相等
 如果不相等，跳转至32
 继续执行33，输出  'false%3Cbr%3E'

如果以上三个判断都为true，就会执行30
ECHO  'the+next+step+is+xxx.zip'
```

所以我们要向`index.php`提交三个参数，`flag1、flag2、flag3`，值分别为：`fvhjjihfcv、gfuyiyhioyf、yugoiiyhi`

这是返回结果

```
do you know Vulcan Logic Dumper?
the next step is 1chunqiu.zip
```

直接使用`URL`访问`1chunqiu.zip`，我们就可以得到一份源代码

审计源代码，发现存在`SQL`注入漏洞

```
    $username = $db->safe_data($_POST['username']);
    $password = $db->my_md5($_POST['password']);
    $number = is_numeric($_POST['number']) ? $_POST['number'] : 1;
    $username = trim(str_replace($number, '', $username));
```

`$username`变量中与`$number`相等的字符串会被替换为`""`，我们可以结合`dbmysql.class.php`中的`safe_data`成员方法中的`addslashes`函数来进行`'`的绕过

PHP的一个语言特性，PHP中的addslashes函数除了会对`' " \`进行转义之外，还会对`url`编码为`%00`的字符进行转义，转义结果为`\0`，因为在ascii码中，`0`对应的字符为`\0`，是没有办法直接输出的，但是使用`addslashes`函数之后，就可以显示了，`\\0`输出就是`\0`

这一点我们可以通过在本地环境中验证来得到

然后我们就可以在`burp suite`这样来构造我们的`$number`和`$username`：

```
$number = 0
$username = %00'
```

`$username`的处理结果为`\0\'`，因为我们构造的`$number`为`0`，因此最终的`$username`为`\\'`，前面的`\`被转义失效，这样就成功绕过了`'`的过滤，接下来执行报错注入即可