

# 第14届(2021)CISCN初赛WP（1）——easy\_source

原创

[RangerKnight](#) 于 2021-06-15 14:16:21 发布 98 收藏 1

分类专栏: [CTF练习题目WriteUp](#) 文章标签: [php](#) [信息安全](#) [网络安全](#)

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/InterplanetaryW/article/details/117923513>

版权



[CTF练习题目WriteUp](#) 专栏收录该内容

2 篇文章 0 订阅

订阅专栏

## easy\_source WriteUp

题目打开没发现啥, 就先看看index.php, 还是没有什么变化。这时候想起来前段时间遇到过考敏感文件的。有三种都来试试:

1. robots.txt
2. gedit备份文件, 格式为filename~, 比如index.php~
3. vim备份文件, 格式为.filename.swp 或者 \*.swp

然后发现备份文件/index.php.swp可行



```
}  
  
function p()  
{  
    return ++self::$c;  
}  
  
function q()  
{  
    return ++self::$c;  
}  
  
function r()  
{  
    return ++self::$c;  
}  
  
function s()  
{  
    return ++self::$c;  
}  
  
function t()  
{  
    return ++self::$c;  
}  
  
}  
  
$rc=$_GET["rc"];  
$rb=$_GET["rb"];  
$ra=$_GET["ra"];  
$rd=$_GET["rd"];  
$method= new $rc($ra, $rb);  
var_dump($method->$rd());
```

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

发现了GET传参的要求，构造payload:

```
?rc=ReflectionMethod&ra=User&rb=q&rd=getDocComment
```



```
你能发现我吗string(152) /* ** Increment counter ** @final * @static * @access publicCISCN[Gw3An-1yuJ7-L9Ah5-4x2cJ-QLqh-] * @return int */
```

成功爆出flag。



[创作打卡挑战赛](#) >

[赢取流量/现金/CSDN周边激励大奖](#)