

小宁听说php是最好的语言,XCTF攻防世界web新手练习—simple_php

转载

普通网友 于 2021-03-10 14:03:45 发布 149 收藏

文章标签: [小宁听说php是最好的语言](#)

题目

题目为simple_php, 根据题目信息, 判断是关于php代码审计的.

simple_php

92 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: 删除场景

倒计时: 03:51:27 延时

题目附件: 暂无

小宁听说的很对, PHP的最好的语言。

打开题目, 得到一串php代码

```
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;  
}  
?>
```

简单审计下代码，发现需要以get的方式传入两个参数a和b。

a参数的要求 a必须等于0且a为真

b参数的要求 b不能为数字且b大于1234

来看代码

```
if($a==0 and $a){  
echo $flag1;  
}
```

因为php是弱类型语言，当不同类型的值进行==比较的时候会发生类型转换。

所以，只需要使a=0e1

下一段代码

```
if(is_numeric($b)){  
exit();  
}  
if($b>1234){  
echo $flag2;  
}
```

get的b不能是数字，但又必须大于1234，这里可以用b=12345a绕过

结合一下

?a=0e1&b=12345a

得到flag



```
<?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}

本文由 陌涛 发布在 陌涛的记事本，转载此文请保持文章完整性，并请附上文章来源(陌涛的记事本)及本页链接。

原文链接：<https://imotao.com/4068.html>