XCTF攻防世界 Web高手进阶区 PHP2 writeup

原创

Senimo_ 于 2020-03-30 14:51:51 发布 358 收藏

分类专栏： 各CTF平台 Writeup 文章标签： php web XCTF攻防世界 writeup Web高手进阶区

本文链接：https://blog.csdn.net/weixin_44037296/article/details/105198912

XCTF攻防世界 Web高手进阶区 PHP2 writeup

PHP2

难度系数： 2.0

题目来源： 暂无

题目描述：暂无

启动靶机，打开环境：

Can you anthenticate to this website?

你能浏览这个网站嘛？

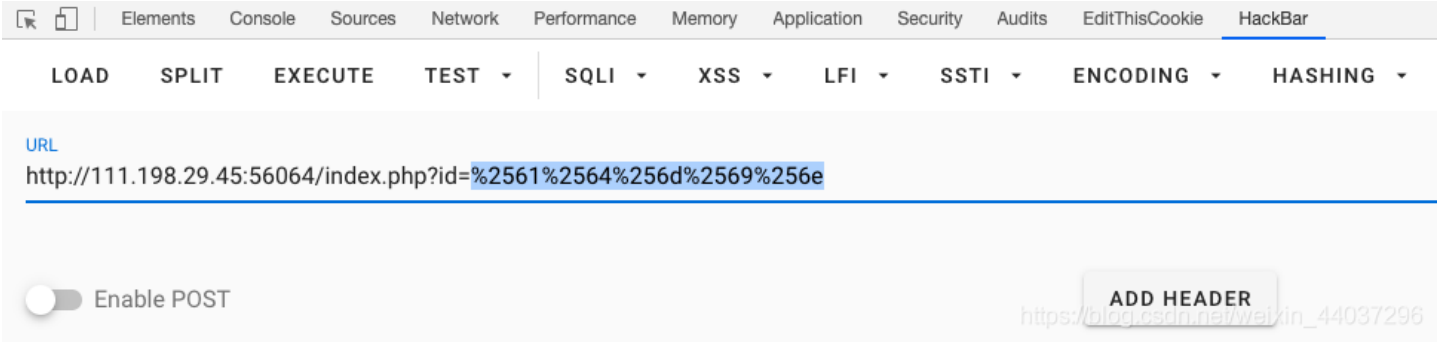
首先访问`index.php`，可以正常访问，尝试查看`index.phps`文件（`.phps`文件就是`php`的源代码文件，通常用于提供给访问者查看`php`代码）：

```
<?php
if("admin"===$_GET[id]) {
  echo("<p>not allowed!</p>");
  exit();
}

$_GET[id] = urldecode($_GET[id]);
if($_GET[id] == "admin")
{
  echo "<p>Access granted!</p>";
  echo "<p>Key: xxxxxxx </p>";
}
?>

Can you anthenticate to this website?
```

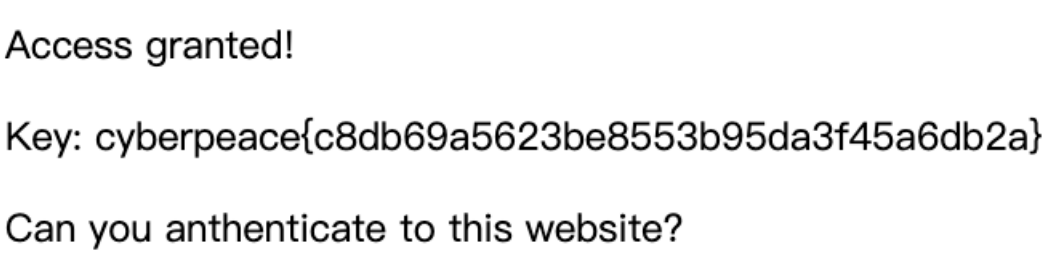

得到网页的源代码，分析代码：
需要传入变量`id`的值，不能等于`admin`，经过`URL`解码后等于`admin`将输出`key`，因为服务器会进行一次`URL`解码，所以我们将`admin`进行二次编码：



得到最后的传输值为：

```
?id=%2561%2564%256d%2569%256e
```

传输数据得到`flag`：


Access granted!
Key: cyberpeace{c8db69a5623be8553b95da3f45a6db2a}
Can you anthenticate to this website?