攻防世界web进阶PHP2详解

原创

無名之涟 于 2020-07-17 00:30:20 发布 350 收藏

分类专栏： CTF

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/hxhxhxhxx/article/details/107398307

版权

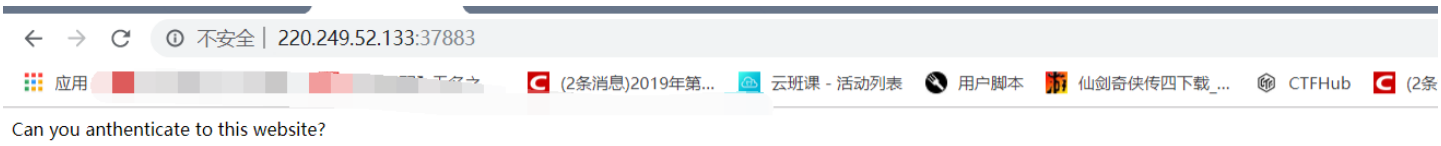
CTF 专栏收录该内容

37 篇文章 0 订阅

订阅专栏

攻防世界web进阶PHP2详解

题目

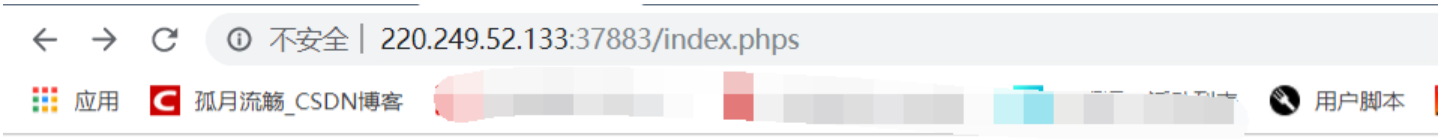


https://blog.csdn.net/hxhxhxhxx

解法

我们发现index.phps存在源码泄露，他只问了原页面在那儿里

（我觉得这里应该给提示）



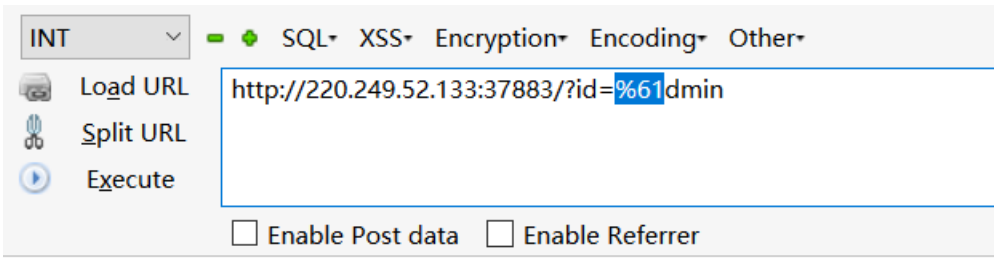

```php
<?php
if("admin"===$_GET[id]) {
  echo("<p>not allowed!</p>");
  exit();
}

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

Can you anthenticate to this website?

https://blog.csdn.net/hxhxhxhxx

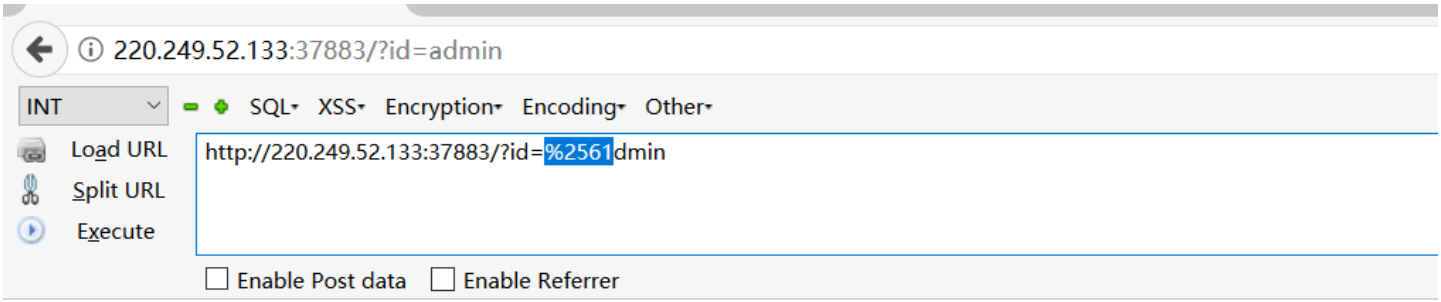
首先我们得admin不能恒等于get获得的id的值
我们需要跳过第一个
接下来get id的值经过一次url解码
然后要恒等于admin
那么我们就将adminurl编码即可，



not allowed!

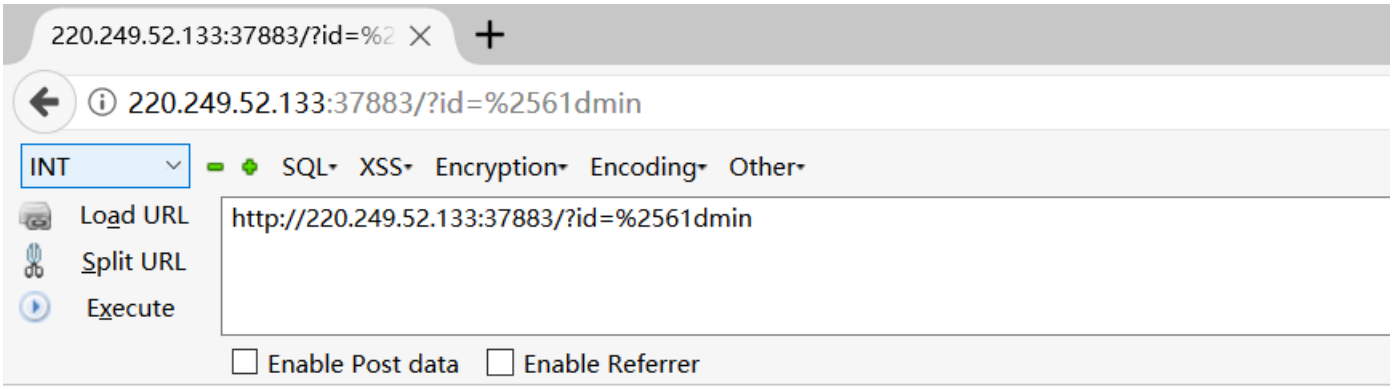
https://blog.csdn.net/hxhxhxhxx

因为第一次经过了get，那么我们就需要两次url编码



not allowed!

https://blog.csdn.net/hxhxhxhxx



Access granted!

Key: cyberpeace{988cbb807818baed7230c4cc03217e72}

Can you anthenticate to this website?

https://blog.csdn.net/hxhxhxhxx

字母的url编码

字符的url编码就是：
字符的十六进制前面加了个百分号