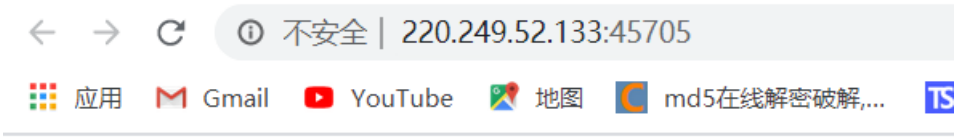
攻防世界 PHP2 解题思路

原创

「已注销」 于 2020-07-12 22:13:10 发布 564 收藏
分类专栏： 攻防世界_web篇

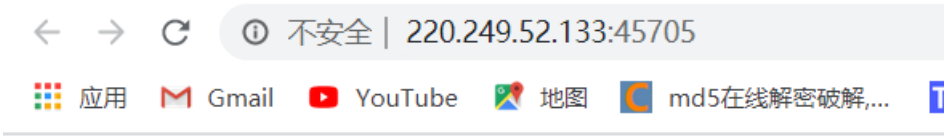
本文链接：https://blog.csdn.net/xj28555/article/details/107306373

进入题目



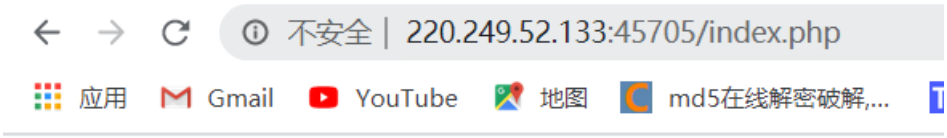
Can you anthenticate to this website?

英语学渣的我只能谷歌翻译



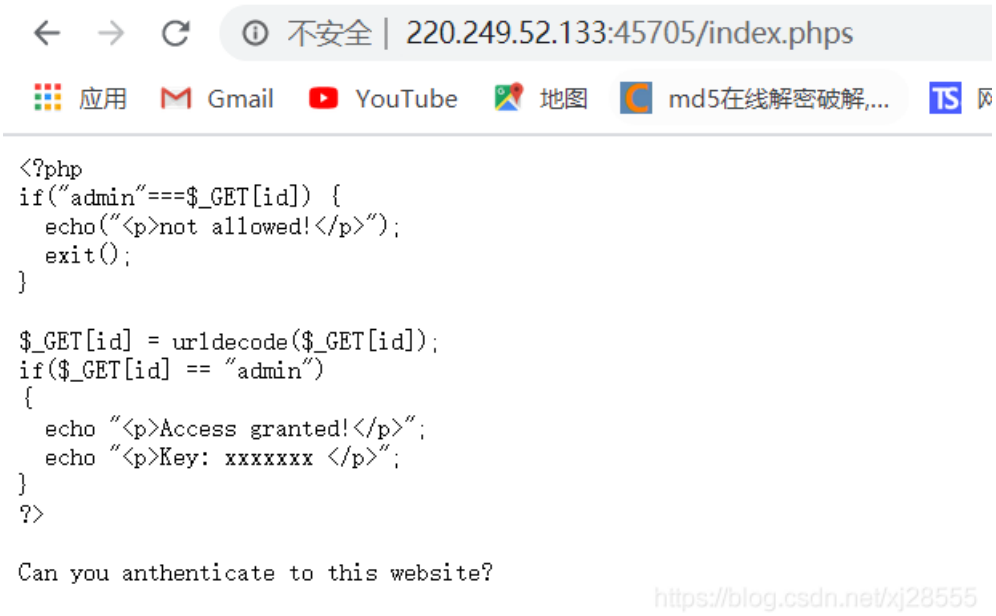
您可以访问该网站吗?

他问我们能访问到该网站吗，我输入了index.php试了试。



Can you anthenticate to this website?

没有结果，然后我上bp用spider模块爬行了下，也没爬出来什么东西。既然爬不到那我们就上御剑跑了下看有什么目录。然后发现了个index.phps这个目录。访问一下。




```
<?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?
```


这里就是一个条件判断，用get的方式传入id这个参数判断是否等于admin，等于就不让访问，等于admin的url编码才让访问。

这里呢我们要进行两次url编码才能成功，因为浏览器会自动解码一次，假如只编码一次，那么还是会被判断到等于admin。

构造payload

?id=%25%36%31%25%36%34%25%36%64%25%36%39%25%36%65

Access granted!

Key: cyberpeace{302082a4f33bd10efdc82e4b0899cd75}

Can you anthenticate to this website?

得到flag！