# 攻防世界之PHP2

原创

行于其野 于 2020-11-17 12:31:50 发布 290 收藏

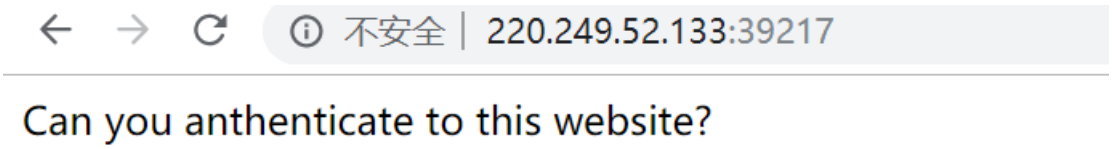
分类专栏： wp



本文链接：https://blog.csdn.net/qq_44111753/article/details/109739973



**题目：**




Can you anthenticate to this website?

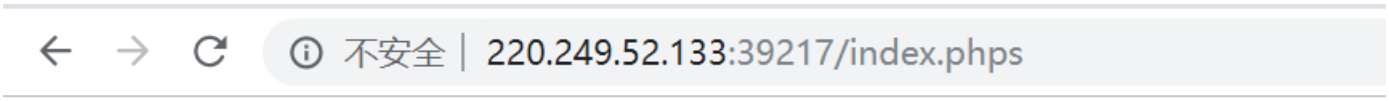


**WP:**

打开题目，查看了源码，~~挺莫名其妙的~~

搜索后发现，可以访问index.phps–index.php的源代码

**php源码文件为phps，url会自动解码一次**




```
<?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?
```

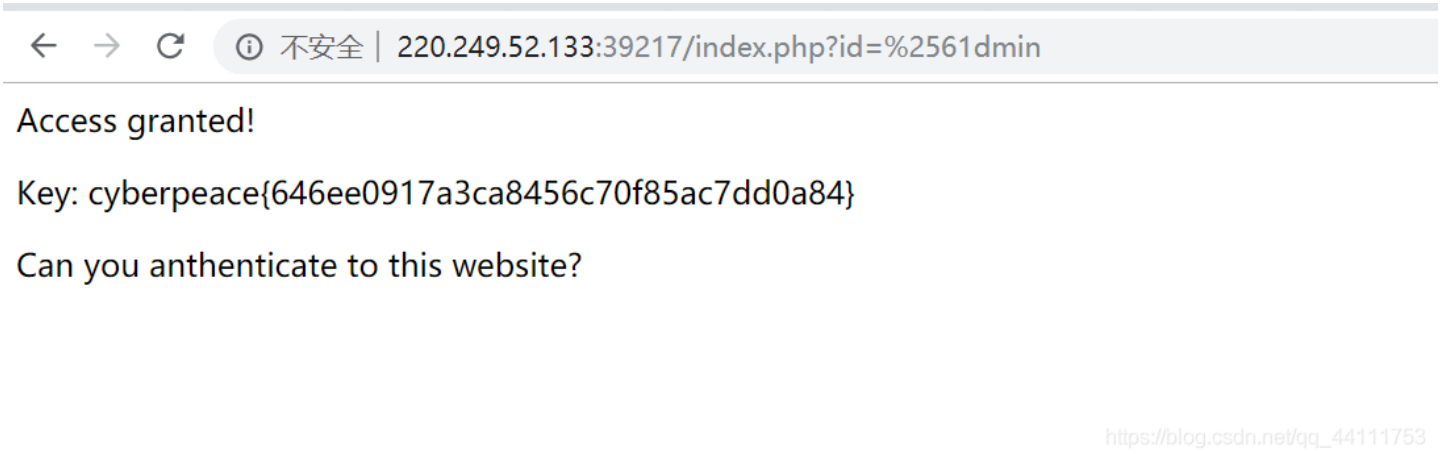


分析代码可知，我们要得到key是第一个if的时候，要使id不等于admin，但经过url解码后，又要等于admin，

提一下url编码：

> %+字符对应的US-ASCII

url中id的值传入后，页面解析时会自动自动进行url解码一次，所以我们可以将
a进行两次编码，第一次编码%61，第二次编码后为%2561，令id=%2561dmin，第一次if比较时将会是admin?=%61dmin，第二次才会是admin






得到flag啦~