【攻防世界】十一 --- PHP2

原创

通地塔 于 2020-12-25 18:31:14 发布 31 收藏

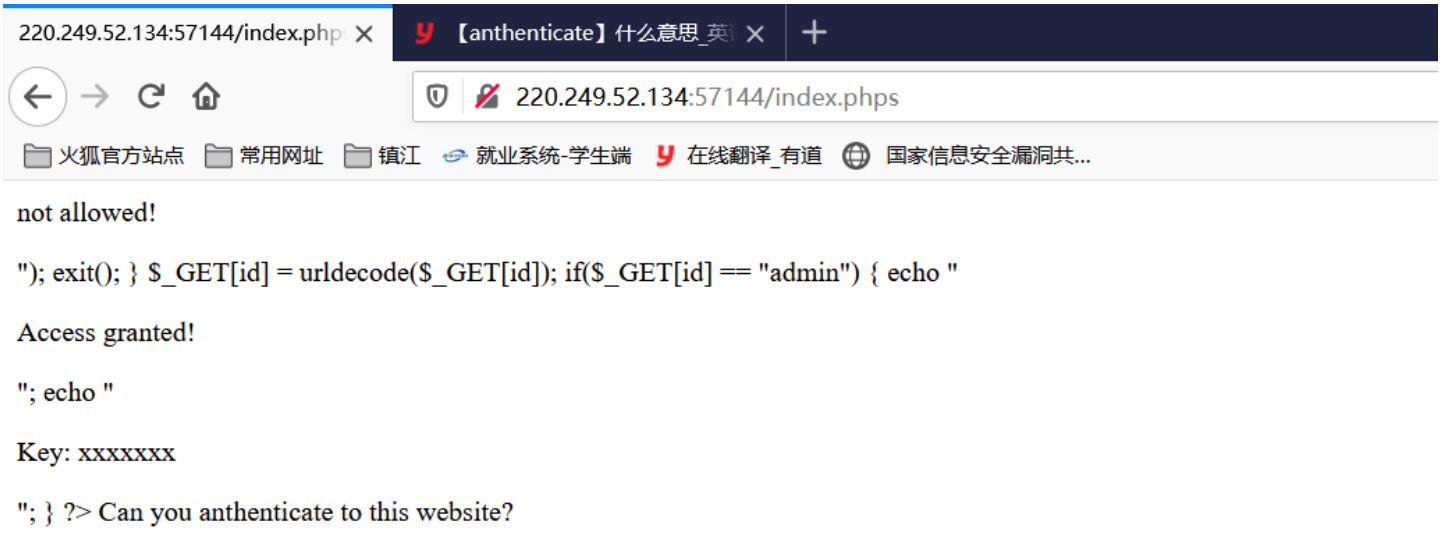
分类专栏： 攻防世界 文章标签： ctf 网络安全

题目 — PHP2

一、writeup

主页回显：你是否可以鉴定这个网站

这里有一个坑点，需要你的字典中有`index.phps`目录，访问`index.phps`目录，可得代码



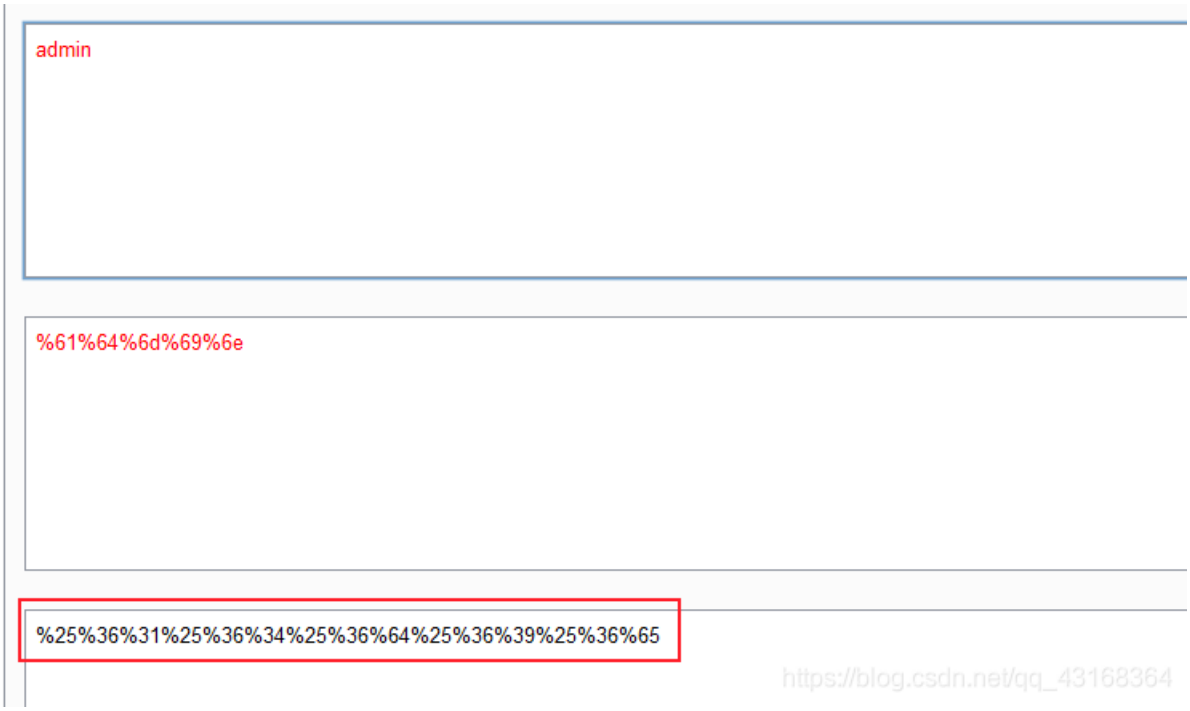
这里用firefox抓到得到代码有点显示不完全，chrome可以完整显示

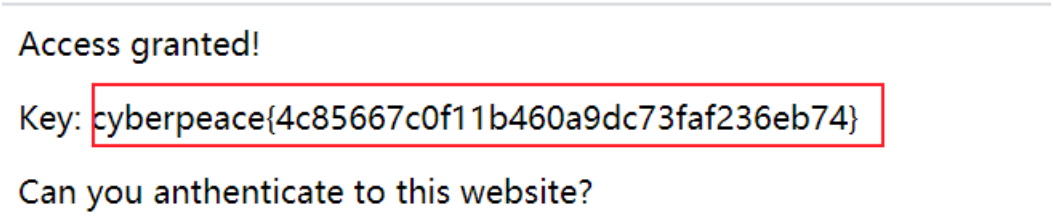
```
<?php
if("admin"===$_GET[id]) {
  echo("<p>not allowed!</p>");
  exit();
}

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

Can you anthenticate to this website?
```


关键点

- 1、查询字符串名为 id
- 2、id 不能直接等于 admin
- 3、id 经过url 解码之后等于admin即可回显出flag

那就很清晰了，将admin进行`两次url编码`，即可得到flag。注意这里还有一个坑点：id 应该跟在 `index.php` 的后面，而不是 `index.phps` 的后面。这里index.phps显示的是index.php的源代码。so，payload为：`/index.php?id=%25%36%31%25%36%34%25%36%64%25%36%39%25%36%65`





二、知识点

- php代码审计