实验吧-PHP大法 Writeup

原创

baynk 于 2019-08-24 02:23:50 发布 129 收藏 1

分类专栏： # 实验吧 Writeup 文章标签： CTF 实验吧 PHP大法

本文链接：https://blog.csdn.net/u014029795/article/details/100048117

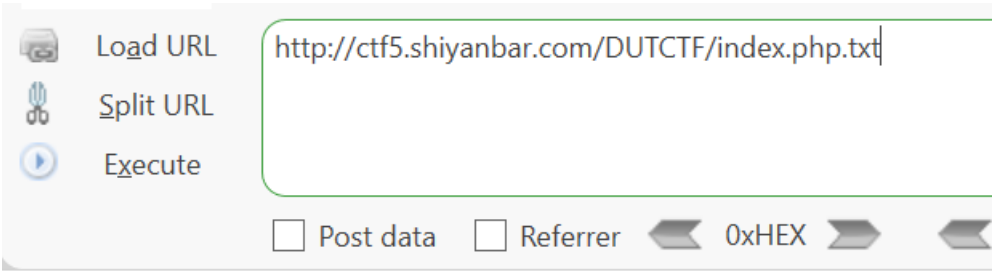
写这个东西真是有点上隐。。。

过程

- 链接：http://ctf5.shiyanbar.com/DUTCTF/index.php
- 一进去就看到提示

Can you authenticate to this website? index.php.txt

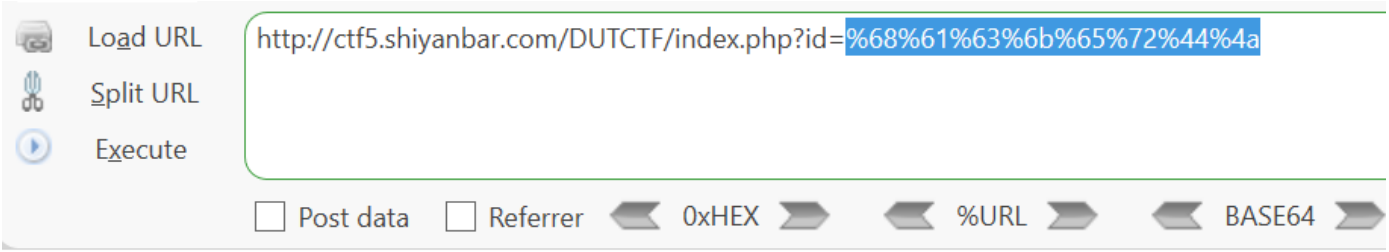
- 接着去访问源码文件




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

$_GET[id] = urldecode($_GET[id]);
if($_GET[id] == "hackerDJ")
{
  echo "<p>Access granted!</p>";
  echo "<p>flag: ****************} </p>";
}
```

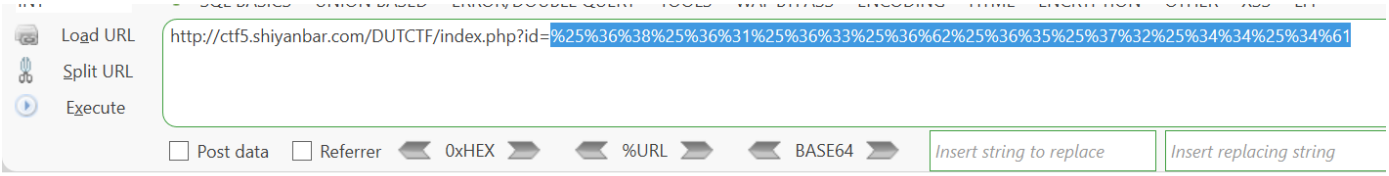
```
?>


<br><br>
Can you authenticate to this website?
```

- 拿flag条件简单，id不能包含hackerDJ，并且要求通过urldecode解密后的id和hackerDJ相等。
- 先尝试将hackerDJ进行urlencode进行提交。



not allowed!

- 结果不行，这是因为url在用Get方式获取参数时会自动解码，于是想到了既然多解码了一次，那我就再多编码一次不就行了，再来一次。



Access granted!

flag: DUTCTF{PHP_is_the_best_program_language}

Can you authenticate to this website? index.php.txt

- 搞定，拿到Flag。

总结

1. 除了-._三个字符、大小写字母、数字，其它字符串都会被urlencode处理
2. 通过浏览器在URL后面带GET参数的时候都是经过encode处理的，PHP在后台接收参数的时候无需经过urldecode的处理了：
   Warning: 超全局变量 $_GET 和 $_REQUEST 已经被解码了。
3. POST传递和接受参数都不需要经过encode和decode处理，$_POST接收的参数也不会进行解码操作
4. 在使用fsockopen等函数，通过凭借header信息字符串的方式添加进去的参数，如果经过eneode，需要自己调用urldecode方法
5. encode之后的字符串还会可以再次被encode，%会被编码为%25，但是如果在浏览器上带上encode之后的字符串，字符串不会被再次编码

6. PHP的urlencode函数被把空格替换成+,rawurlencode函数会空格编码成%20