CTF题解五 Web PHP大法（实验吧）

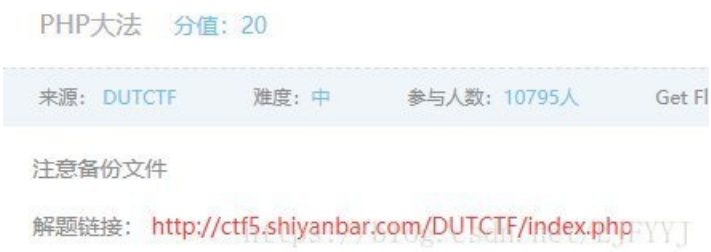
原创

目标是技术宅 于 2018-07-14 20:14:10 发布 1907 收藏

分类专栏： CTF 文章标签： 实验吧 Web CTF 题解

本文链接：https://blog.csdn.net/LJFYYJ/article/details/81047013

实验吧题目链接：http://www.shiyanbar.com/ctf/54



首先，根据题目中提示，要注意备份文件。

点开题目链接后，最后有提示`index.php.txt`。于是进行访问。

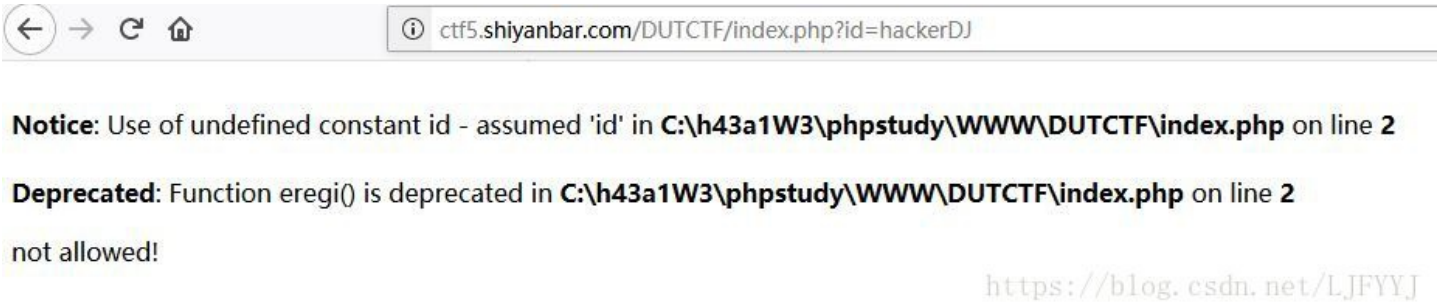
```
<?php
if(eregi("hackerDJ",$_GET[id])) {
  echo("<p>not allowed!</p>");
  exit();
}

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


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


采用的是GET方法，代表着之后可以用`?id=XXX`的方式进行测试。

程序的主要逻辑是，GET方法得到的id的值必须被`hackerDJ`所包含，却又在进行一次url解密后，与其相等。

这里涉及到**PHP中`urldecode`这一函数的特性**。`urldecode`会把字符串中所有带`%`的数字进行解密。

尝试输入`?id=%68ackerDJ`，按下回车键，发现什么也没发生。看一下浏览器的url，发现**浏览器为我们完成了一次url解码**，如图：



所以我们需要对`hackerDJ`进行两次url加密。

看一个例子：

```php
<?php
    $a="%2568ackerDJ";
    $a=urldecode($a);
    echo $a, "</br>";
    $a=urldecode($a);
    echo $a;
?>
```

这里**`%25`对应的符号是`%`**。

所以第一次解密后得到`%68ackerDJ`，再解密一次得到`hackerDJ`。

输入`?id=%2568ackerDJ`，就可以得到flag了：

`flag: DUTCTF{PHP_is_the_best_program_language}`