程序逻辑问题--实验吧

原创

Gunther17 于 2017-09-01 10:09:04 发布

程序逻辑问题

题目提示是绕过,本题考点：sql语句注入

```
<html>
<head>
welcome to simplexue
</head>
<body>
<form method=post action=index.php>
<input type=text name=user value="Username">
<input type=password name=pass value="Password">
<input type=submit>
</form>
</body>
<a href="index.txt">
</html>
```

```php
<?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>");

  }


}

?>
```

初了解（可略）：
mysql_fetch_array() 中可选的第二个参数 result_type 是一个常量，可以接受以下值：MYSQL_ASSOC，MYSQL_NUM 和 MYSQL_BOTH。本特性是 PHP 3.0.7 起新加的。
本参数的默认值是 MYSQL_BOTH。如果用了 MYSQL_BOTH，将得到一个同时包含关联和数字索引的数组。用 MYSQL_ASSOC 只得到关联索引（如同 mysql_fetch_assoc() 那样），
用 MYSQL_NUM 只得到数字索引（如同 mysql_fetch_row() 那样）。它仅仅返回关联数组。
mysql_connect — 打开一个到 MySQL 服务器的连接
strcasecmp($pass, $row[pw])二进制安全比较字符串（不区分大小写）。本题要求也就是pass==row[pw]

分析本题：
一、漏洞点$sql = "select pw from php where user='$user'"; 因为前面是post所以就是钥匙式注入
跟'程序员的问题'不同，这里用户和密码分开判了,所以注释掉pw不可行,只要让row[pw]的值与pass经过md5之后的值相等即可 而$pass经过md5之后的值是我们可以通过正常输入控制的
同时，row[pw]的值是从$sql提取出来的 目标就一句话：只要我们能够修改$sql的值，此题解决。再次审视注入点：$sql = "select pw from php where user='$user'";
在这里我们可以利用sql语句，直接给$sql返回一个值。
也就是说，不需要访问题里的数据库，只要我们修改了$sql的值，此题解决。
二、剩下的就是猜用户名了，试了试admin，不对，然后又试了默认username 成了，防止发生短路，确保后面union执行。
解释：
1. 最前面的单引号：闭合原文的where user='
2. AND 0=1:为了使前面的表达式返回值为空.
3. 接着我们使用UNION SELECT MD5(2)，直接把MD5值作为返回值retuen给$sql，这样在查询的时候$query就会有值.
4. 最后的#用来注释掉后面没用的东西

username:username' union select md5(1)#

password:1

welcome to simplexue

Logged in! Key: SimCTF{[illegible]ing}

提交