Writeup

原创

想学python的元气汪 于 2019-11-19 22:45:11 发布 168 收藏

文章标签： 个人学习总结

本文链接：https://blog.csdn.net/qq_43641982/article/details/103074507

十一月份上旬总结

1. 在做这道题目之前下载了虚拟机安装好了Ubuntu
2. 然后弄好共享文件夹（经过百度我在Ubuntu中找到了我创建的share共享文件夹）
3. 然后将此题的附件下载到share文件夹，并且改好名字，因为名字太长不方便使用，我改成了linux
4. 分析题目，需要在linux里面找到关于flag的东西
5. 打开终端，输入以下代码进入root身份（经过百度已经创建好了root身份）

```
su root
```

6. 然后cd到share里面（我直接可以cd share因为我创建了个软连接到home）

```
cd share
```

7.然后开始寻找flag

```
strings linux|grep flag
```

```
.flag.txt.swp
flag.txtt.swx
~root/Desktop/file/O7avZhikgKgbF/flag.txt
.flag.txt.swp
flag.txtt.swx
.flag.txt.swp
flag.txtt.swx
```

发现了flag的位置

8. 将文件挂在Ubuntu上，进入mnt里面通过ls来查看里面的文件

```
mount linux /mnt cd /mnt ls
```

```
root@ater-virtual-machine:/home/ater/share# mount linux /mnt
root@ater-virtual-machine:/home/ater/share# cd /mnt
root@ater-virtual-machine:/mnt# ls
02CdWGSxGPX.bin  0wDq5  3J          7H7geLlS5   8RxQG4bvd  h          i           jj          LO0J8       m9V0lIaElz  Nv          orcA      Q         Raf3SYj    sdb.cramfs  T
0GY1l            0Xs    44aAm       8A2MFawD4   FinD       H          lmgLDPt4BY  KxEQM       lost+found  MlU         o           oSx2p     qkCN8     rhZE1LZ6g  sn          TFGVOSwYd.txt
0h3aS            1      4A          8DQFirm0D   fm         H2Zj8FNbu  lx1EMRHRpIc2  LG6F      LvuGM       Mnuc        O7avZhikgKgbF  OT       QmUY1d    Ruc9       SPaK8l2sYN
0l               2X     6JR3        8HhWfV9nK1  g          hdi7       j6uLMX      Lh          lWIRfzP     n           o8          poiuy7Xdb  QQY3sF63w  RZTOGd     SrZznhSAj
0qsd             3      6wUaZE1vbsW  8nwg       gtj        hYuPvID    jE          LlC6Z0zrgy.bin  m       NgzQPW      OOoOs       px6u      r         scripts    t
```

发现了之前flag.txt所在的目录

9. cd到那个目录里面

```
cd 07avZhikgKgbF
```

```
root@ater-virtual-machine:/mnt# cd O7avZhikgKgbF
root@ater-virtual-machine:/mnt/O7avZhikgKgbF# cat flag.txt
ZmxhZ3tzYWpiY2lienNrampjbmJoc2J2Y2pianN6Y3N6Ymt6an0=
root@ater-virtual-machine:/mnt/O7avZhikgKgbF# base64 -d flag.txt
flag{sajbcibzskjjcnbhsbvcjbjszcszbkzj}root@ater-virtual-machine:/mnt/O7avZhikgKgbF#
```

10. 利用base64解码

```
base64 -d flag.txt
```

找到flag成功

第二题sql注入

本题只找到flag的部分

报错注入？源码审计？

596

实验吧

这题我改变了作者的原意，所以你得到的flag并不是这里要交的flag

你要交的是wctf{flag_user_pw}，例如

simCTF{asdfg}，user=abc，pw=123

提交wctf{asdfg_abc_123}

点此题目链接

View Hint

View Hint

打开网址

welcome to simplexue

Username •••••••• 提交查询

1.查看源代码

```
<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>
```


2. 进入画圈圈的地方

```
<html>
<head>
welcome to simplexue
</head>
<body>
<?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>");

  }


}

?>
<form method=post action=index.php>
```


找到了解题依据，先

一步步来

3. 首先判断是否为注入

1' and 1=1

1' and 1=0

都报错

4.然后判断是什么类型

1"登入失败

1'报错

5.知道了用1'来注入，再次返回刚刚的代码，经过分析

$pass= md5(_POST[pass]);

if ((KaTeX parse error: Expected 'EOF', got '&' at position 10: row[pw]) &&̲ (!strcasecmp(pass, $row[pw]))) {

echo "

Logged in! Key:**********

";

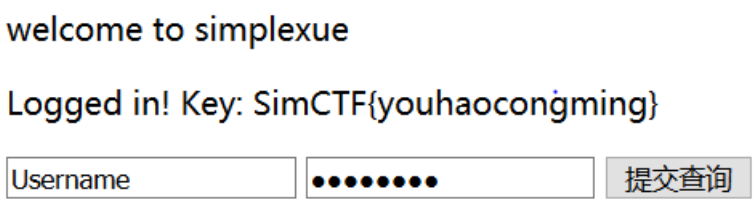
= "*selectpwfromphpwhereuser*= user'";

要使得if成立才能得到flag，所以要在username上加一个union语句

那么我们要把用户名和上方注入语句调成

```
1' union select md5(1) #
```

此时password是1
然后得到flag



*sql*我的能力到这里了