# 实验吧CTF刷题记录（web篇二）

原创

Tools-only 于 2017-03-11 10:18:51 发布 14431 收藏 3


8.上传绕过

解题链接： http://ctf5.shiyanbar.com/web/upload

直接上传.php会被拦截。尝试上传图片马，能上传但不符合题目要求。

尝试bp抓包改后缀名无果，并非在客户端javascript验证。

尝试截断路径绕过，上传1.jpg文件，bp抓包，路径upload后添加1.php空格，将hex中空格20改为00，forward，成功绕过。

9.FALSE

PHP代码审计
hint：sha1函数你有认真了解过吗？听说也有人用md5碰撞o(╯□╰)o

格式：CTF{}

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

源码：

```
<?php
if (isset($_GET['name']) and isset($_GET['password'])) {
   if ($_GET['name'] == $_GET['password'])
      echo '<p>Your password can not be your name!</p>';
   else if (sha1($_GET['name']) === sha1($_GET['password']))
     die('Flag: '.$flag);
   else
      echo '<p>Invalid password.</p>';
}
else{
echo '<p>Login first!</p>';

 ?>
```

按代码中的思路非常难找出碰撞，但是sha1()函数默认的传入参数类型是字符串型。加上题目标题false可以想到构造FALSE===FALSE拿到flag

地址栏修改name[]=xxx,password[]=zzz;

**10.Guess Next Session**

写个算法没准就算出来了，23333

hint：你确定你有认真看判断条件？

格式：CTF{}

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

```
<?php

session_start();

if (isset ($_GET['password'])) {

   if ($_GET['password'] == $_SESSION['password'])
```

```
    die ('Flag: '.$flag);
  else
    print '<p>Wrong guess.</p>';
}
```

session在判断时是没有值的，构造第二个if语句左右均为空值。

bp抓包，将PHPSESSID删除，并将输入的密码置空，拿到flag。

**11.Once More**

hint：ereg()函数有漏洞哩；从小老师就说要用科学的方法来算数。

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

```
if (isset ($_GET['password'])) {
if (ereg ("^[a-zA-Z0-9]+$", $_GET['password']) === FALSE)
{
echo '<p>You password must be alphanumeric</p>';
}
else if (strlen($_GET['password']) < 8 && $_GET['password'] > 9999999)
{
if (strpos ($_GET['password'], '*-*') !== FALSE)
{
die('Flag: ' . $flag);
}
else
{
echo('<p>*-* have not been found</p>');
}
}
else
{
echo '<p>Invalid password</p>';
}
}
```

需要通过两个if语句，题目提示1 ereg()函数存在漏洞，ereg()限制password的格式，只能是数字或者字母。但ereg()函数存在NULL截断漏洞，可以使用%00绕过验证。

题目提示2 科学记数法，由于要使密码长度小于8或值大于9999999，可以使用1e8或1e9满足条件。

正确pass：1e9%00*-* 得到flag。

## 12.忘记密码了

找回密码

解题链接： http://ctf5.shiyanbar.com/10/upload/

首先还是先查看源代码，可以发现两个重要信息点：

```
<meta name="admin" content="admin@simplexue.com" />
<meta name="editor" content="Vim" />
```

管理员邮箱以及使用的是vim编辑器。

看了大神writeup，得知读取.submit.php.swp （看评论说burpsuite抓包可以看到submit - - 无奈我没找到。）

访问http://ctf5.shiyanbar.com/10/upload/.submit.php.swp

```
if(!empty($token)&&!empty($emailAddress)){
 if(strlen($token)!=10) die('fail');
 if($token!='0') die('fail');
 $sql = "SELECT count(*) as num from `user` where token='$token' AND email='$emailAddress'";
 $r = mysql_query($sql) or die('db error');
 $r = mysql_fetch_assoc($r);
 $r = $r['num'];
 if($r>0){
  echo $flag;
 }else{
  echo "谴辫触浜喟慈";
 }
}
```

可以看到token需要满足长度为10且==‘0’ 构造弱类型0000000000

http://ctf5.shiyanbar.com/10/upload/submit.php?emailAddress=admin@simplexue.com&token=0000000000 得到flag。