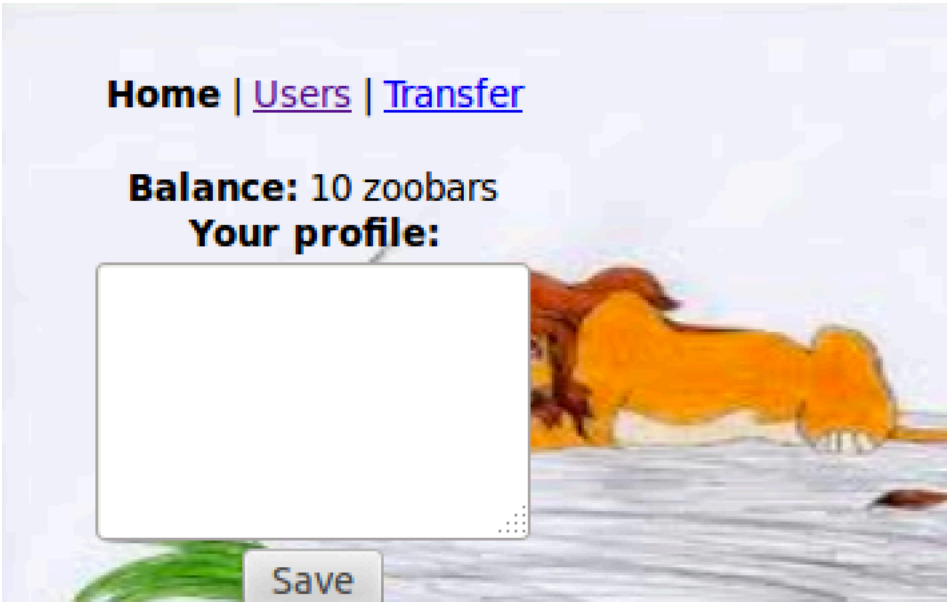
Lab2：修改 zoobar 显示数量
实验要求：在上节课搭建的 zoobar 网站上，如图所示：



在不修改网站源代码的情况下使得 zoobar 显示的数量有 1000 个，而事实上每个人默认的 zoobar 数量只有 10 个，然后以下是四种方法：

方法一：by 小强

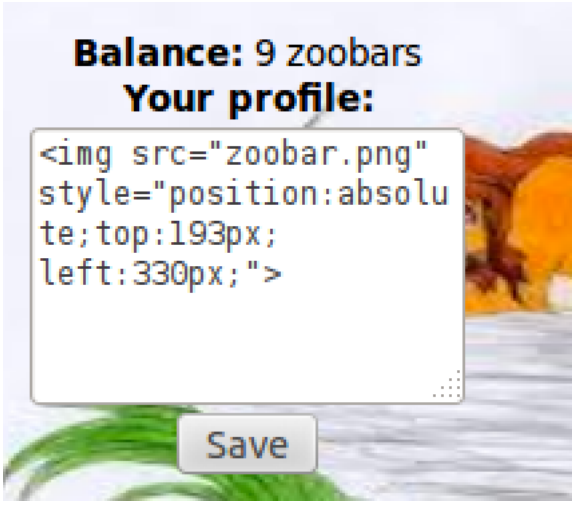
这种方法是修改数据库的方法，略微有点违规（个人意见哈，但小强依然是大腿~），首先打开 index.php 的源代码

```
<?php
  if($_POST['profile_submit']) {  // Check for profile submission
    $profile = $_POST['profile_update'];
    $sql = "UPDATE Person SET Profile='$profile' ".
           "WHERE PersonID=$user->id";
    $db->executeQuery($sql);  // Overwrite profile in database
  }
  $sql = "SELECT Profile FROM Person WHERE PersonID=$user->id";
  $rs = $db->executeQuery($sql);
  $rs = mysql_fetch_array($rs);
  echo $rs["Profile"];
?>
```

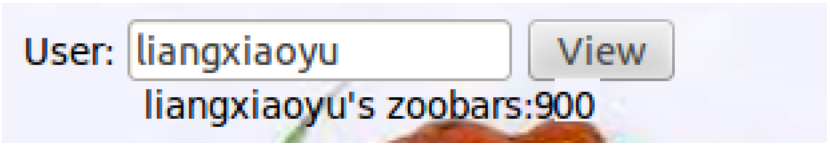
可以看到在这一段中，这个$profile就是上图所示网站用户用来提交的 profile_submit，$sql 变量里是数据库查询语句,会作为参数交给executeQuery 函数(在 database.class.php中)去执行相应的数据库操作。
那么我们要修改数据库中 Zoobars 的数量就可以这样写 profile: 00',Zoobars=1000,Profile='zoobars is 1000 now
此时,$sql 就是”UPDATE Pserson SET Profile='00',Zoobars=1000,Profile='zoobars is 1000 now' “.” WHERE PersonID=$user->id”,就起到了修改数据库中 Zoobars 的 作用,其效果就是把 Zoobars 设为 1000,Pprofile 设为 zoobars is 1000 now.00'是为了把之前=后面的但引号匹配掉。 点击 save 可以看到 zoobars 数量变了!

方法二:使用CSS修改法

这种方法很简单，具体思路就是在数字10后面插入图片，使得从视觉上看上去像是用户的zoobar看上去为1000,具体实现方法如下：



直接插入‘00’的图片形式，然而该图片放在网页源代码的根目录下，建议最好自建一个网站，例如在佳爷的电脑上，用apache建立了另一个网站localhost:8080端口，然后在这个自建网站上插入图片，所以此时img的src为 http://localhost:8080/zoobar.png，然后点击save保存，出来的效果是：



当然还可以调一下透明度，我没调的原因是因为我懒233333。

方法三：

这个方法是从别的大神那里学到的，是这四种方法中我觉得最聪明的方法，具体实现如下，首先我们仔细观察在user界面下的网页源代码，我们会发现有以下内容：

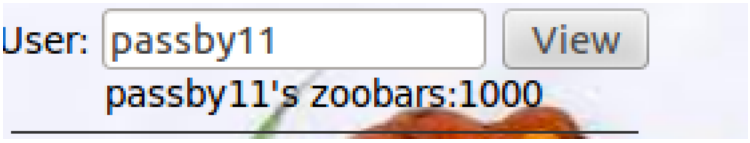
```
<div id="profileheader"><!-- user data appears here --></div>
<div class=profilecontainer><b>Profile</b><p id=profile></p></div><span id='zoobars' class='10'/><script type="text/javascript">
  var total = eval(document.getElementById('zoobars').className);
  function showZoobars(zoobars) {
    document.getElementById("profileheader").innerHTML =
      "passbyll's zoobars:" + zoobars;
    if (zoobars < total) {
      setTimeout("showZoobars(" + (zoobars + 1) + ")", 100);
    }
  }
  if (total > 0) showZoobars(0);  // count up to total
</script>
```

在这段代码里我们发现，zoobar显示的数量与total有关，因此我们的思路就是只要改变total的值，就可以显示我们想要的结果，然而这段代码也给了我们修改total值的机会：

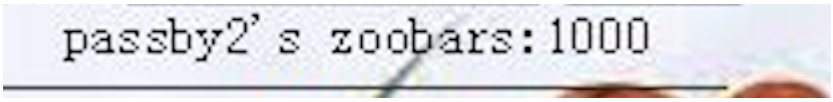
var total = eval(document.getElementById('zoobars').className);

这句js代码的含义是：total的值等于id为zoobars的class属性的值，因此我们只需再构造一个标签，使得id=zoobars,class=1000，便可以完成目标；
基于此我们在profile内提交的语句如下：

提交之后，显示的结果如下所示：



修改成功。
方法四：使用javascript
同样是请教了js大神，也是感到了震撼，这种成果我不敢一个人独吞，所以希望和大家分享，在之前，我也试图注入js代码，然而总是失败，今天实验课上特地向老师请教了这个问题，老师表示是因为在源代码中过滤掉了<script>标签，本着不修改代码（事实是我懒）的原则，结果看到大神的结果的时候，跪了，好了，下面是分享内容
好的既然过滤掉了<script>标签，那么大神的做法是
利用从而达到注入的目的
javascript的编码转换后的结果为（百度上很多在线16进制编码转换器）
&#x6a&#x61&#x76&#x61&#x73&#x63&#x72&#x69&#x70&#x74
<a
href=&#x6a&#x61&#x76&#x61&#x73&#x63&#x72&#x69&#x70&#x74:alert(document.getElementById('profileheader').innerHTML="passby2\'s%20zoobars:1000")>df
其中我的用户名在这里是passby2，\’是一个转义字符，%20是空格，然后提交后，首先出来的会有一个df的链接，点击进去之后就会出现下面的情况：



（然而，在我的ubuntu12.04上，提交这段代码始终有问题，原创大神的电脑上一切ok，如果有和我一样问题的朋友，欢迎大家讨论啊，交个朋友啊！）