OurPHP会员中心 xss漏洞

复现环境：

OurPHP v1.7.1

漏洞简介：

OurPHP会员中心>收货地址 存在xss漏洞，可获取管理员cookie。

漏洞分析:

在client/user/ourphp_play.class.php 文件 320行 `OP_Add`。

```
$query = $db -> insert("`ourphp_usershopadd`","`OP_Addname` =
'".$_POST["OP_Addname"]."',`OP_Addtel` = '".$_POST["OP_Addtel"]."',`OP_Add` =
'".$add."',`OP_Addindex` = 0,`OP_Adduser` = '".$_SESSION['username']."',`time` =
'".date("Y-m-d H:i:s")."'","");
echo @ourphp_pcwapurl($_GET['type'],'?'.$_GET["lang"].'-
usershopadd.html','?'.$_GET["lang"].'-usershopadd.html',0,'');
```

从代码里可以看到 `OP_Add` 参数 没有然和过滤 直接带入sql语句，导致xss漏洞

漏洞复现

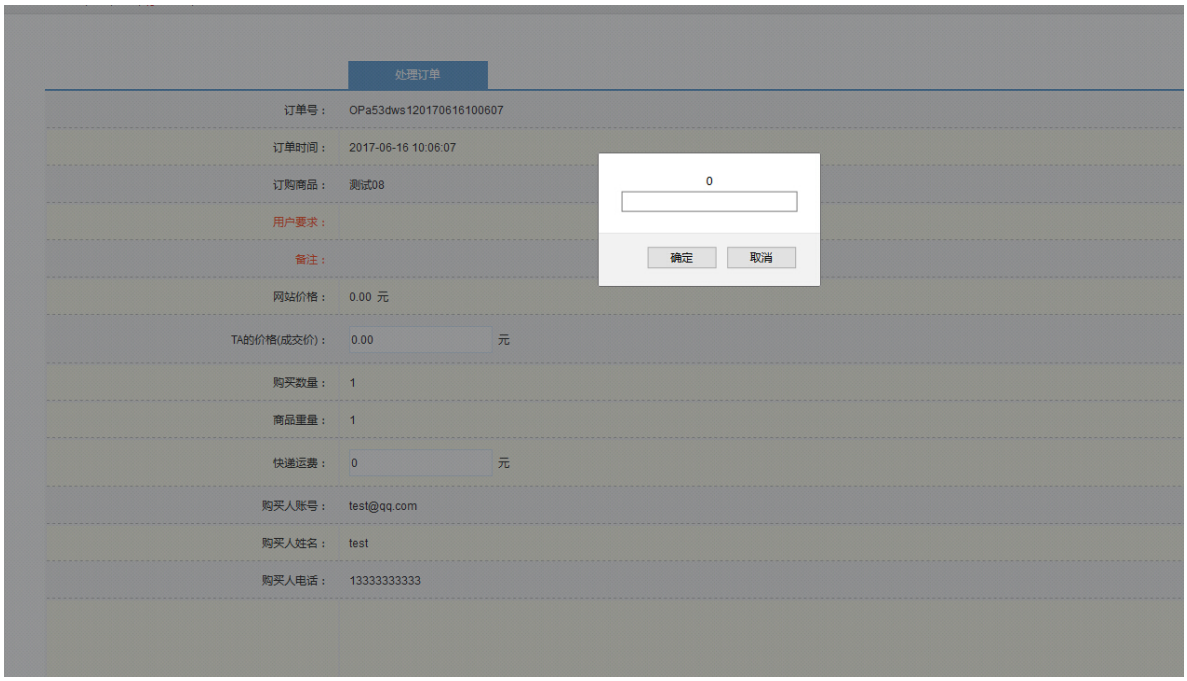
前台注册会员，然后登陆到会员中心>收货地址页面。 在创建新的收货地址中填写payload
收货地址： `<svg/onload=prompt(0)>`

然后点击提交，即可触发xss漏洞。

前台购买商品选择地址触发xss漏洞。

然后点击提交，即可触发xss漏洞。

后台管理员订单管理，查看订单，触发xss漏洞。



##漏洞修复：## 对参数进行 xss过滤。比如：用 `htmlspecialchars($str)` 函数进行过滤。