eml 企业通讯录管理系统 v5.0 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 登录页面 username 参数 过滤不严导致 sql 注入。

漏洞分析

WWW/action/action.user.php 文件 第 23 行

```
//验证登录
if($do=="loginok"){
    $name=$_POST[username];
    $pwd=md5($_POST[password]);

    $validate_arr=array($name,$pwd);
    Ifvalidate($validate_arr);

    $sql = "SELECT * from eml_users WHERE username = '$name' AND
password = '$pwd' limit 1 ";
    $db->query($sql);

    if ($record = $db->fetchRow()){ //登录成功
        $_SESSION['isLogin']    = true;
        $_SESSION['userid']     = $record['id'];
        $_SESSION['uid']        = $record['uid'];
        $_SESSION['username']   = $record['username'];
        $_SESSION['roleid']     = $record['roleid'];
        exit($lang_cn['rabc_login_ok']);
    }
    else
        exit($lang_cn['rabc_login_error']);
    exit;
}
```

username 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：

用户名输入 ：admin’ or 1=1# 造成万能密码登录。