

Xss vulnerability exists in DedeBIZ v6.2.10

[Suggested description]

DedeBIZ v6.2.10 was discovered to contain css 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

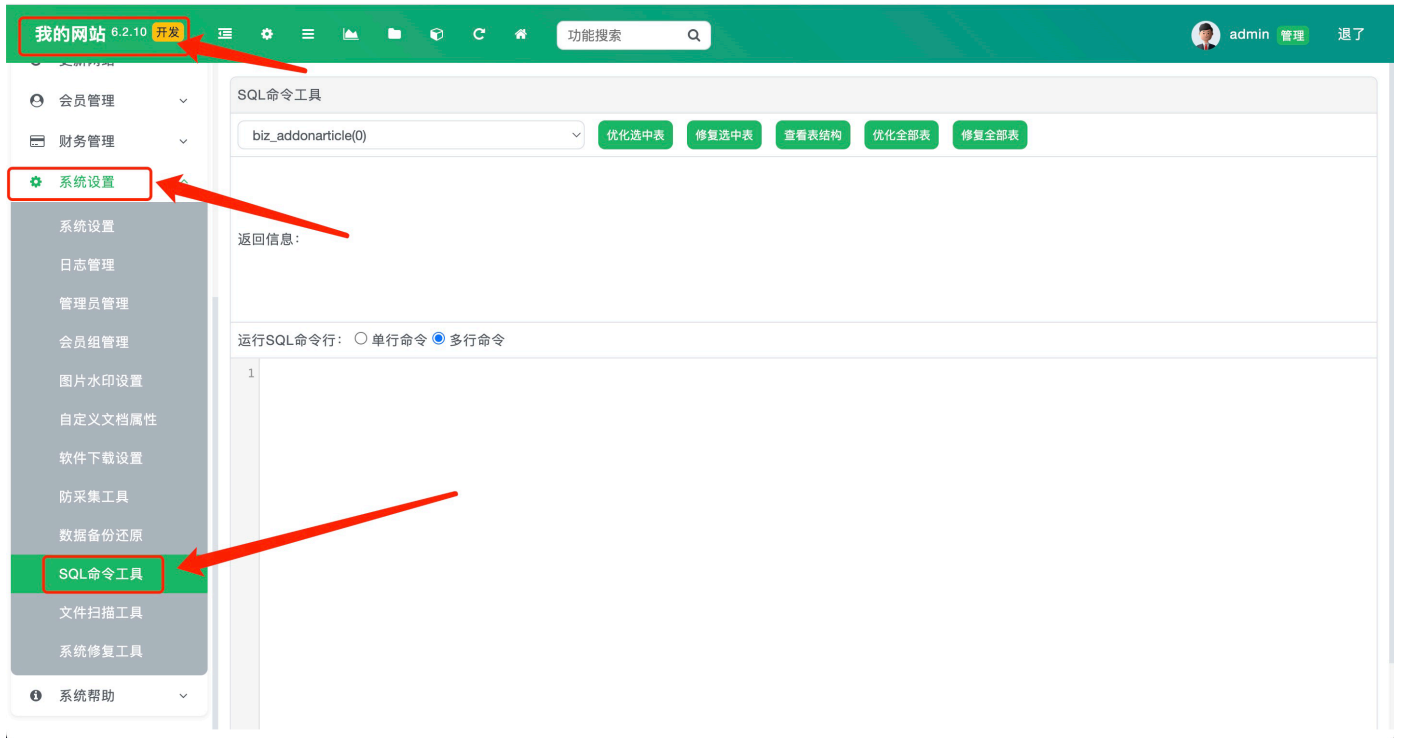
```
POST /admin/sys_sql_query.php HTTP/1.1
.....
dopost=query&_csrf_token=cefb8cd300e4ef8c92a9334d18640faf&querytype=2&sqlquery=%3Cscript%3Ealert%28document.cookie%29%3C%2Fscript%3E
```

[Attack Type]

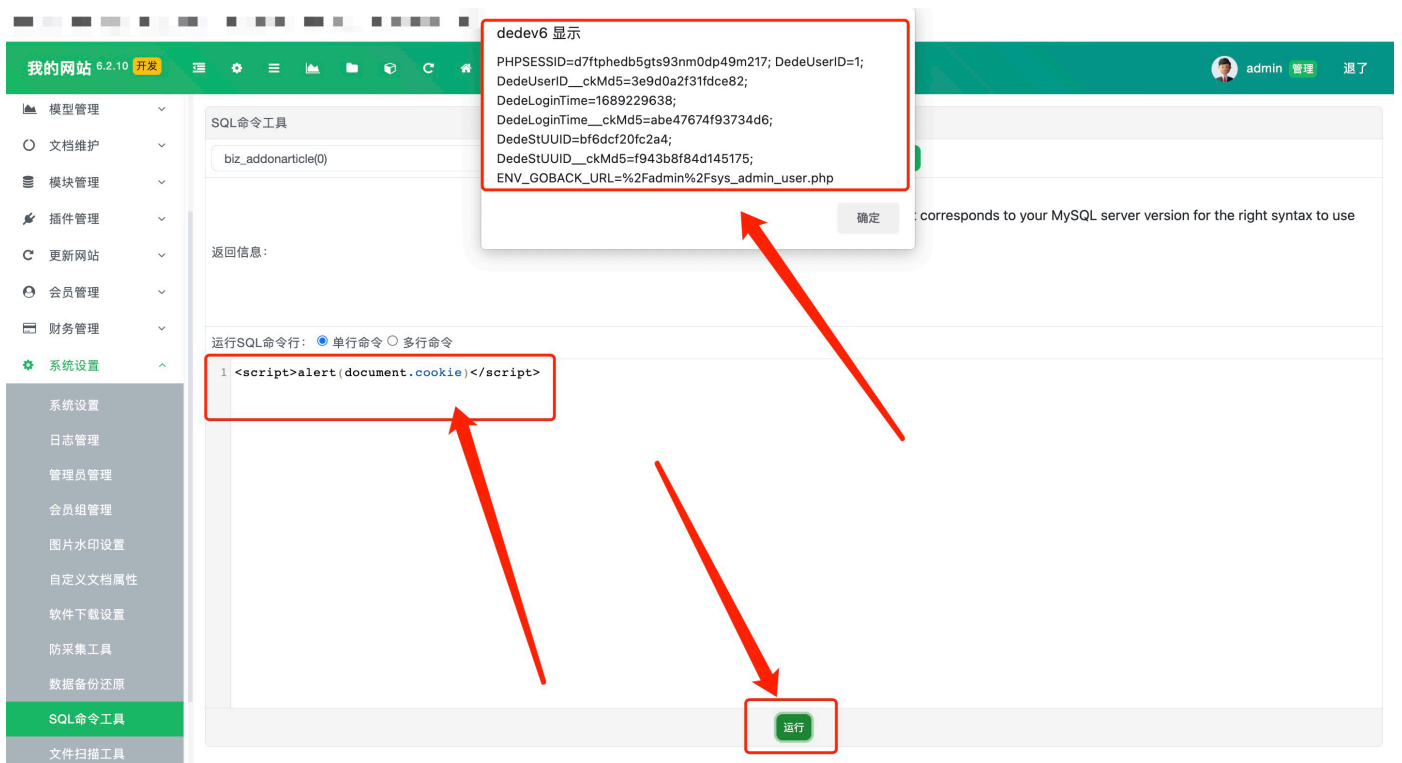
Remote

[Vulnerability demonstration]

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



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



[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#i", $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)) {
        $dsql->SetQuery($sqlquery);
        $dsql->Execute();
        if ($dsql->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'>".$dsql->GetTotalRow()."<
        }
    }
    $j = 0;
}

```



[Repair suggestions]

Filter the output SQL statement content.