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 httpServletRequest = (HttpServletRequest) request;
    HttpServletResponse httpServletResponse = (HttpServletResponse) response;
    try {
        String uri = httpServletRequest.getRequestURI();
        boolean noAuth = noAuth(uri);
        User user = null;
        if (!noAuth) {
            User currentUser = UserThreadLocal.currentUser();
            if (null == currentUser) {
                String xtoken = httpServletRequest.getHeader(XTOKEN);
                if (StringUtils.isBlank(xtoken)) {
                    xtoken = httpServletRequest.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.

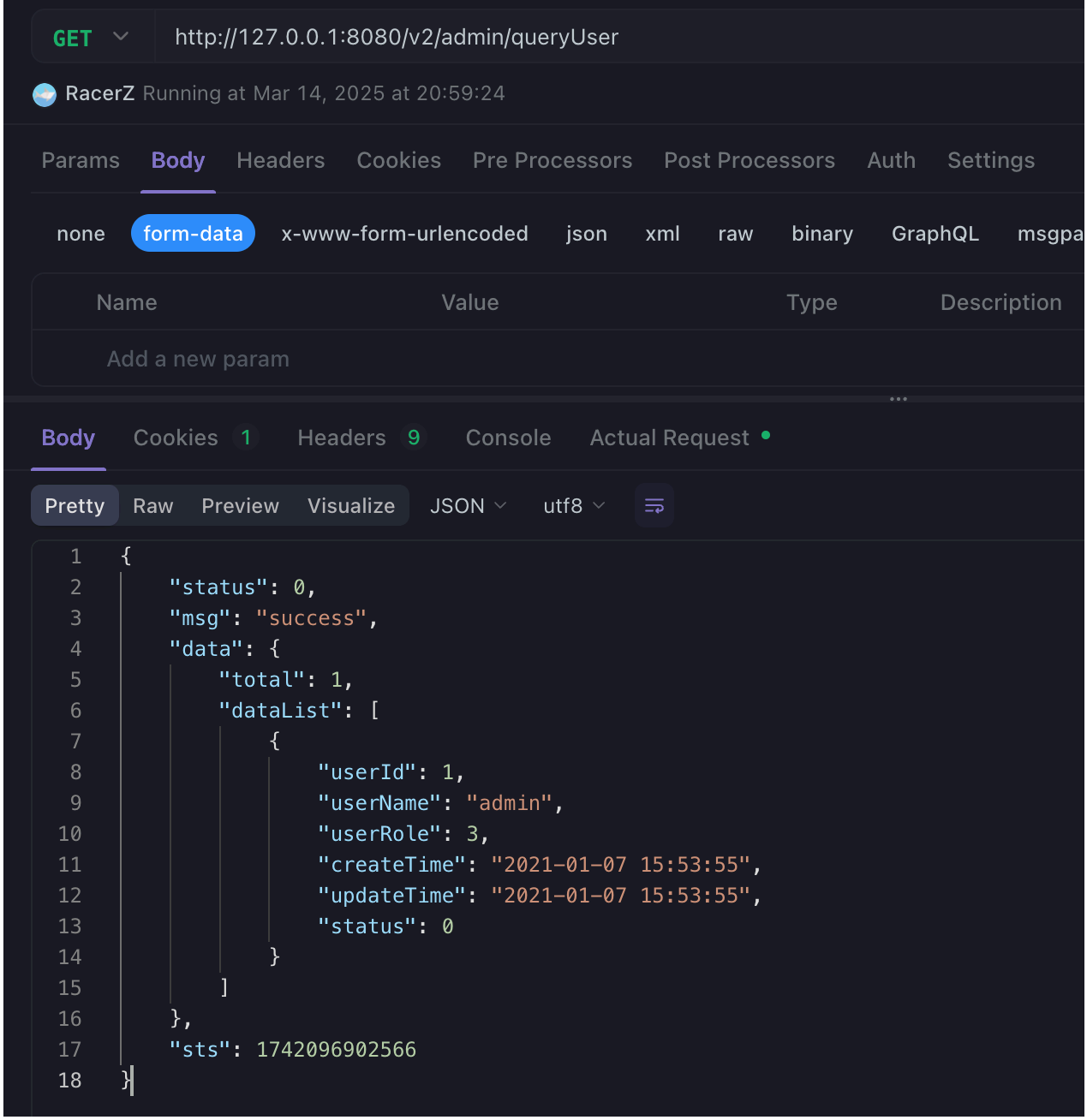

2. The problem lies in using `request.getRequestURI()` to obtain the request path. The path obtained by this function will not parse special symbols, but will be passed on directly. **If an application developer mistakenly configures the servlet `contextPath` as a prefix included in `noAuths`, such as `/v2`, it will lead to an authorization bypass.**

## Reproduce the vulnerablitity

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`.

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

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






**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**