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;
    }
```

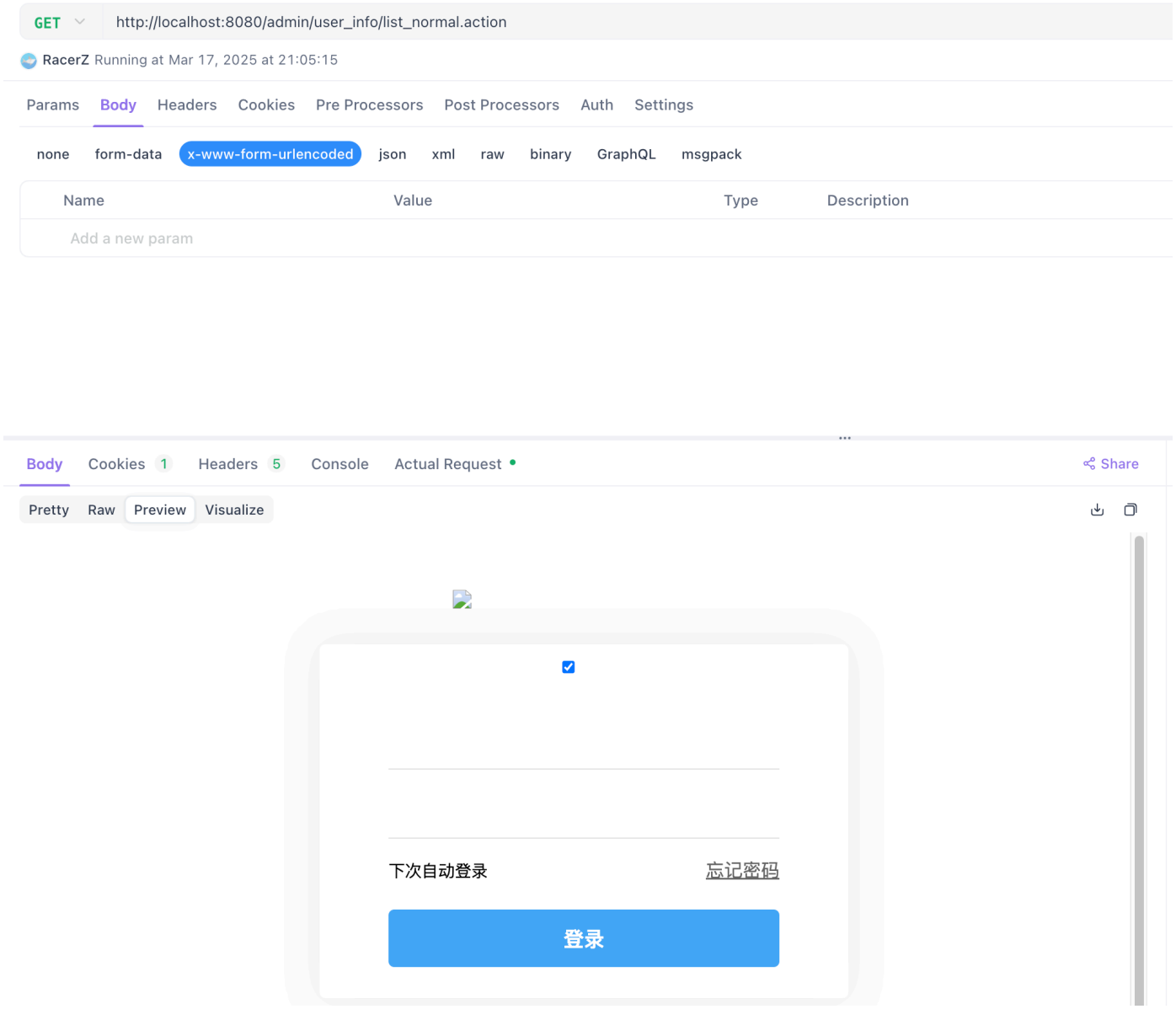
and then determine whether the `url` contains `login` . If the condition is met, it will execute `return true;` to bypass the Filter. Otherwise, it will block the current request and redirect to the login page.

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.

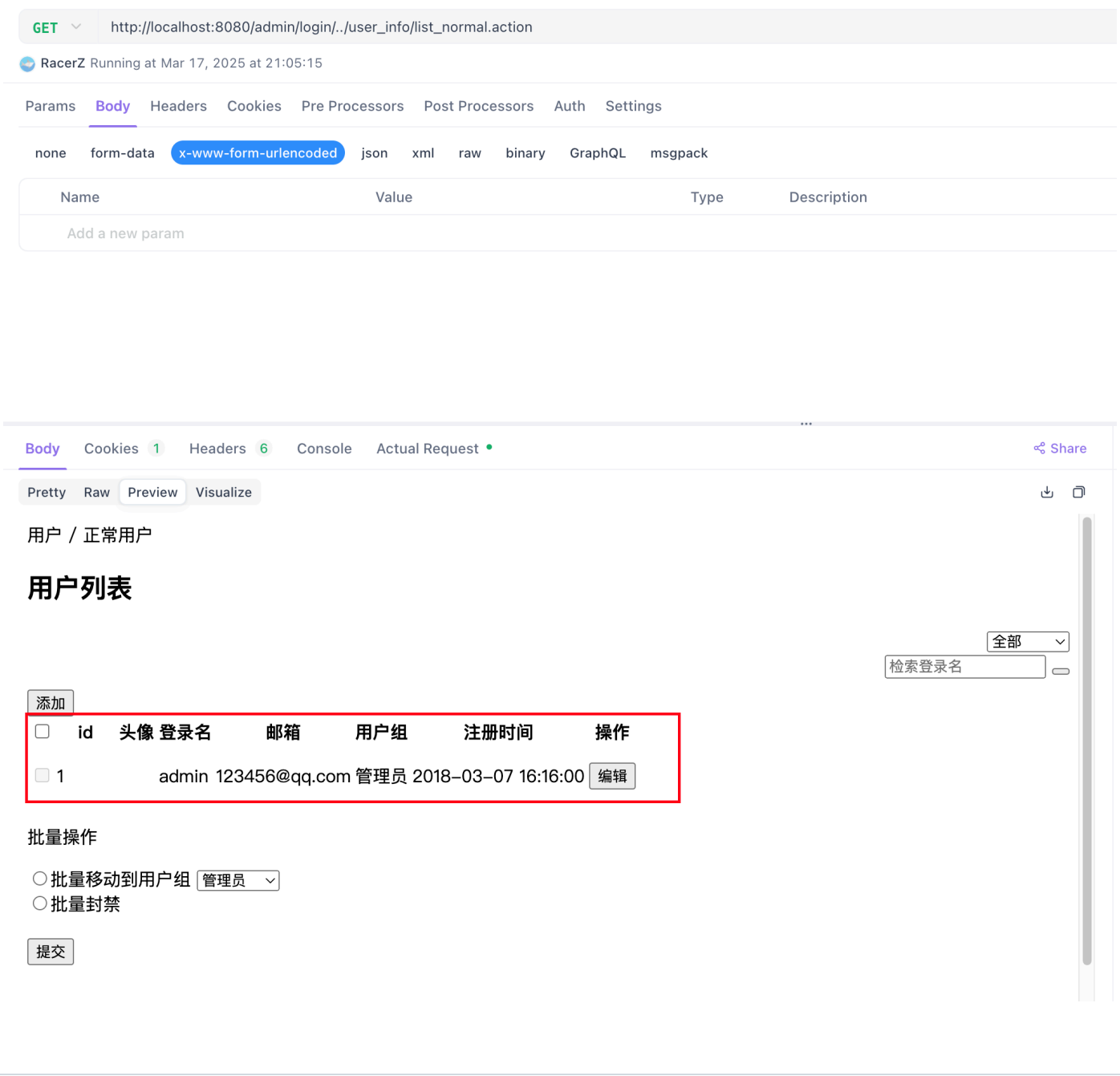
Take the backend interface `/admin/user_info/list_normal.action` as an example. By using `admin/login/../user_info/list_normal.action`, it can bypass the `QingInterceptor`, allowing access to any user's information.

Reproduce the vulnerablitity

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.



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