WLP course learning system v1.0.0 permission verification bypass vulnerability

[Entity Description]

By obtaining online learning capabilities through the WLP online learning platform, it can assist enterprises in offline training or place enterprise training courseware in the system, making it convenient for users to learn online anytime, anywhere.

[Vulnerability Description]

Not filtering the URL path submitted by the user, resulting in API// Accessing functions that require permission verification.

[Impact Description]

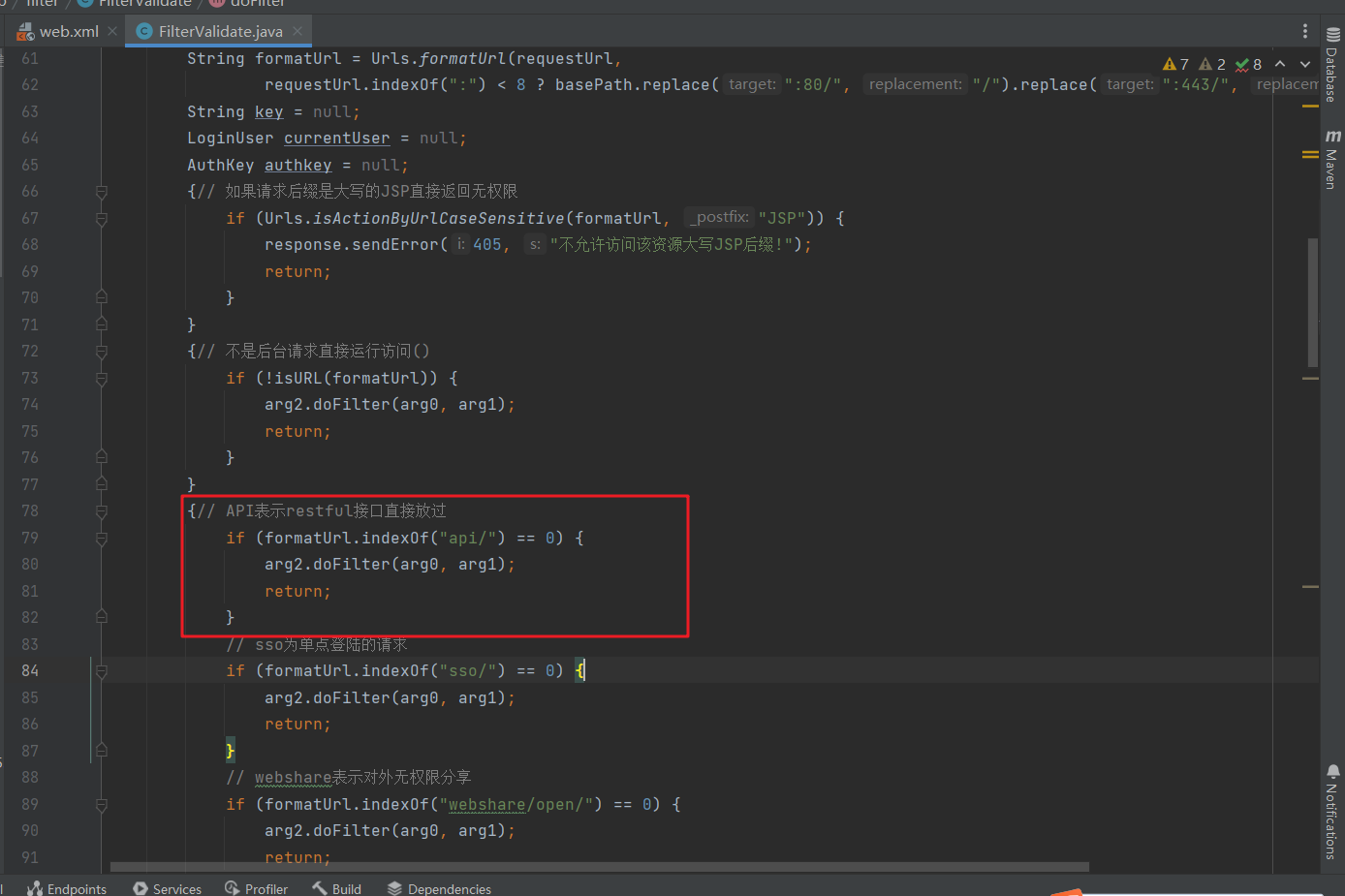
Attackers can bypass the permission verification of the application and access restricted resources, functions, or data. Obtain access privileges higher than its normal permission level, such as executing operations with administrator privileges.

[Physical download address]

https://gitee.com/macplus/WLP

Vulnerability code:

src/main/java/com/farm/web/filter/FilterValidate.java



Unconditional triggering

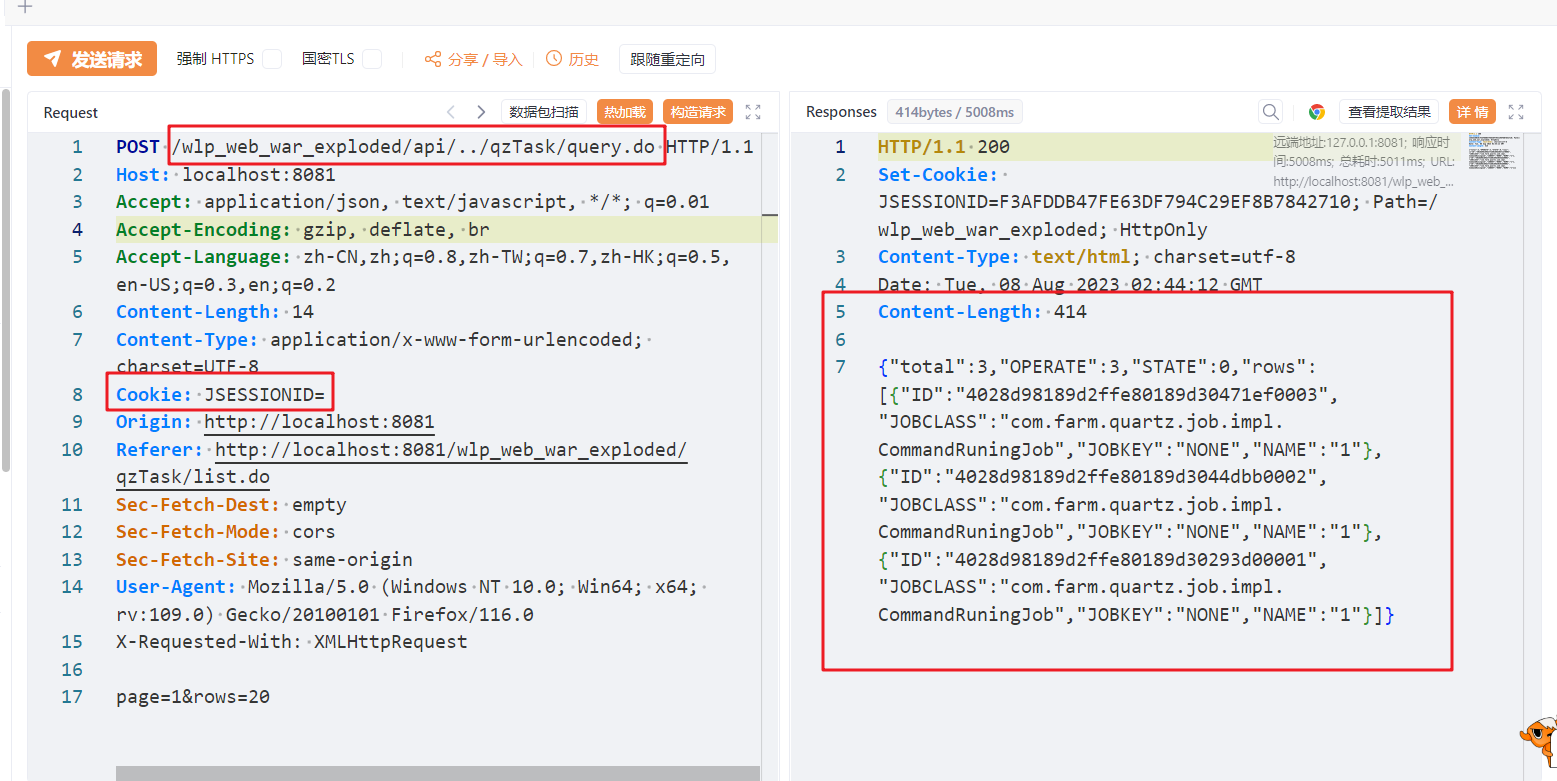
Vulnerability location:

Position 1: Management Console ->System Configuration ->Task Scheduling ->Task Definition

After deleting the cookie, accessing the link will redirect you to the login page



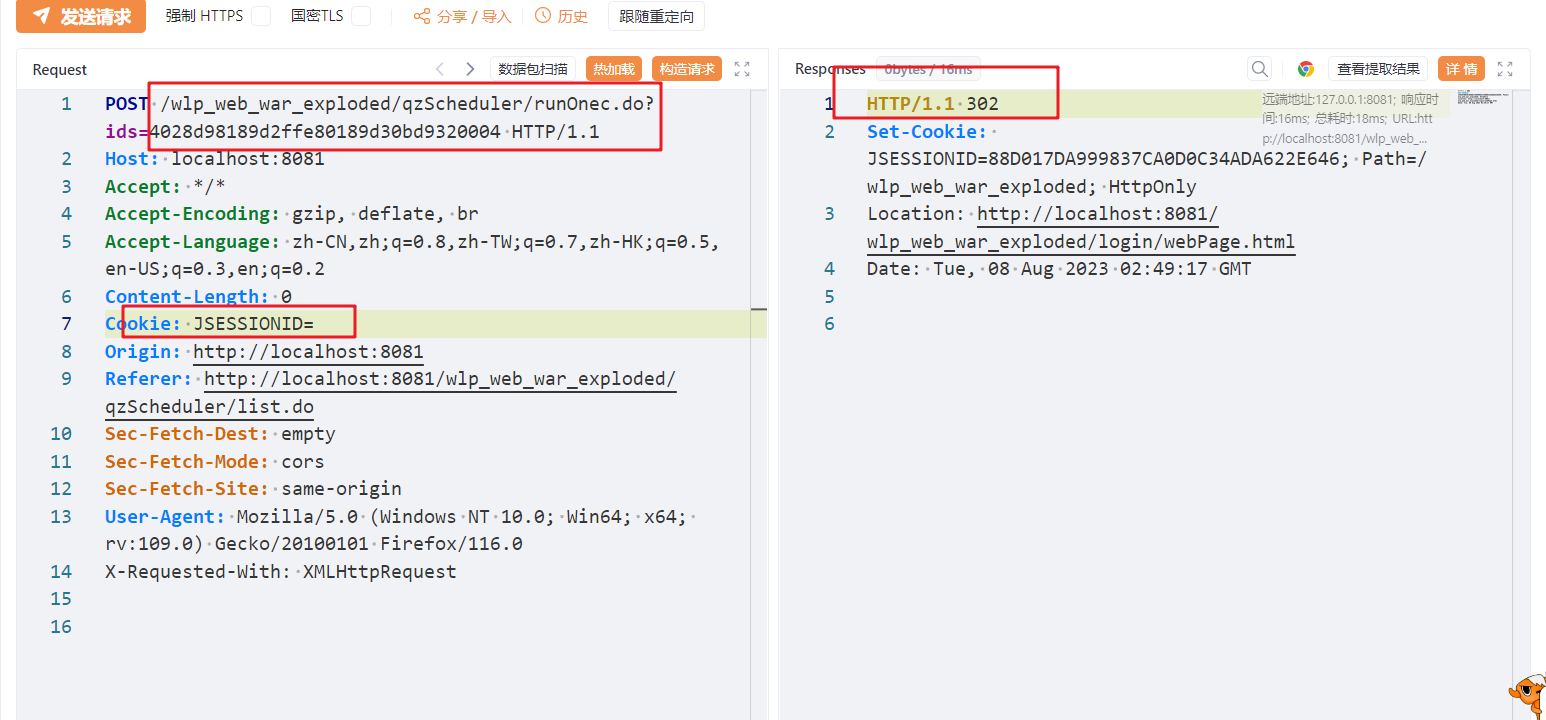
Using API// Accessing the page can request data normally



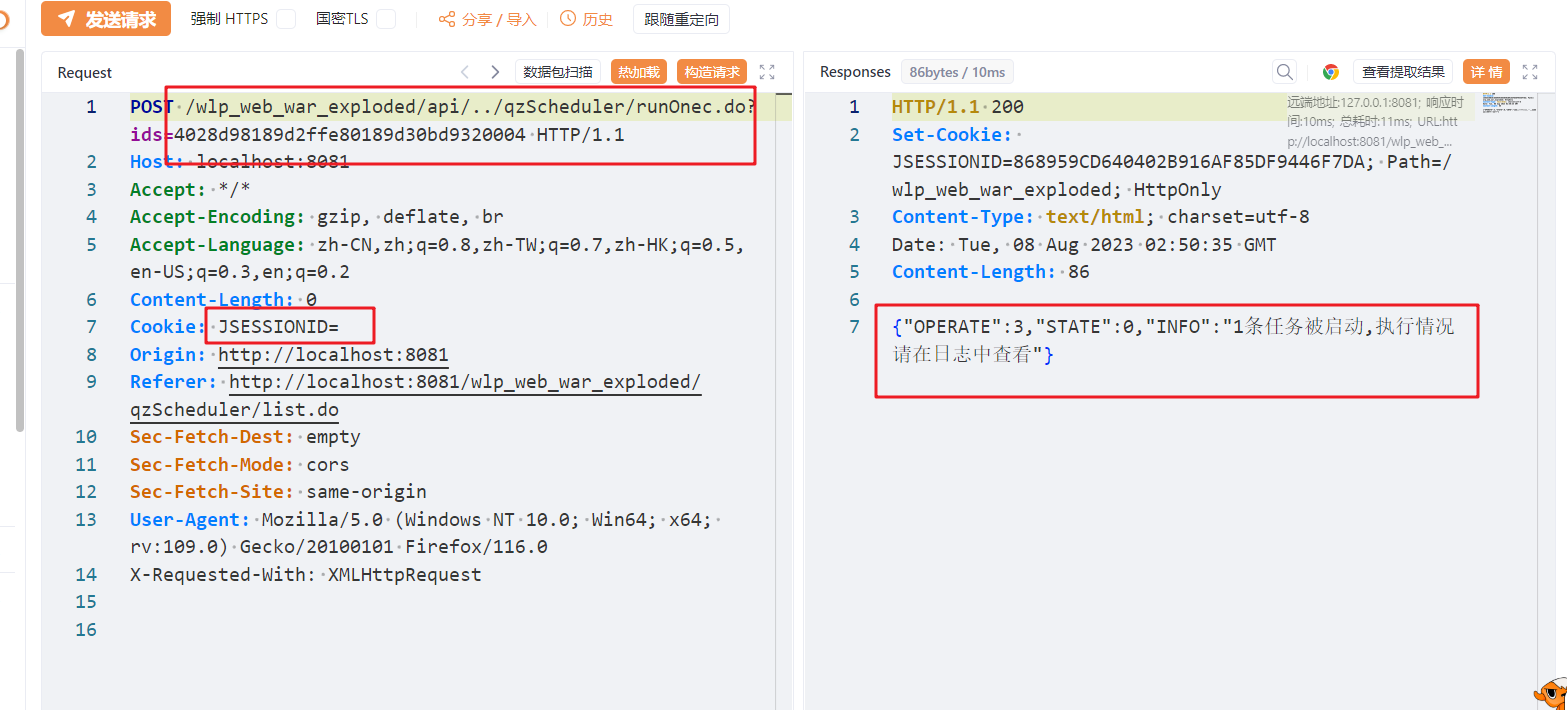
Position 2:

Management Console ->System Configuration ->Task Scheduling ->Scheduling Instances ->Execute Once

Deleting cookies to execute tasks will redirect you to the login page



Using/app// Can execute scheduling tasks normally, task ID can be obtained through location 1



Other login required functions can also be bypassed through this method