功能介绍：

登录：

用户名验证：注册的时候有一个验证

注册：

忘记密码：用到具有有效期的一个token、通过guava的缓存来实现

提交问题答案：

重置密码：分为忘记密码的重置密码和登录状态的重置密码

获取用户信息：电商左上角获取用户的信息

更新用户信息：

退出登录：

关键点：横向越权、纵向越权安全漏洞

MD5明文加密及增加salt值

Guava缓存的使用

高复用服务响应对象的设计思想及抽象封装

Mybatis-plugin的使用技巧

session的使用

横向越权：攻击这尝试访问与他拥有相同权限的用户的资源。

纵向越权：低级别攻击者尝试访问高级别用户的资源。

数据表设计：

SET FOREIGN\_KEY\_CHECKS=0;

-- ----------------------------

-- Table structure for mmall\_user

-- ----------------------------

DROP TABLE IF EXISTS `mmall\_user`;

CREATE TABLE `mmall\_user` (

`id` int(11) NOT NULL AUTO\_INCREMENT COMMENT '用户表id',

`username` varchar(50) NOT NULL COMMENT '用户名',

`password` varchar(50) NOT NULL COMMENT '用户密码，MD5加密',

`email` varchar(50) DEFAULT NULL,

`phone` varchar(20) DEFAULT NULL,

`question` varchar(100) DEFAULT NULL COMMENT '找回密码问题',

`answer` varchar(100) DEFAULT NULL COMMENT '找回密码答案',

`role` int(4) NOT NULL COMMENT '角色0-管理员,1-普通用户',

`create\_time` datetime NOT NULL COMMENT '创建时间',

`update\_time` datetime NOT NULL COMMENT '最后一次更新时间',

PRIMARY KEY (`id`),

UNIQUE KEY `user\_name\_unique` (`username`) USING BTREE

) ENGINE=InnoDB AUTO\_INCREMENT=22 DEFAULT CHARSET=utf8;

接口设计

前台用户接口设计：

1. 登录
2. 注册
3. 检查用户名是否有效
4. 获取登录用户信息
5. 忘记密码
6. 提交问题答案
7. 忘记密码时重置密码
8. 登录状态重置密码
9. 登录状态更新个人信息
10. 获取当前登录用户的详细信息，并强制登录
11. 退出登录
12. 登录

/user/login.do post(代码需要post方式请求）开放get，方便调试

request

String username

String password

response

fail

{

“status”:1,

“msg”:”密码错误”

}

success

{

“status”:0,

“data”:{

“id”:12,

“username”:”aaa”,

“email”:”aaa@163.com”,

“phone”:null,

“role”:0,

“createTime”:1479048325000,

“updateTime”:1479048325000

}

}

1. 注册

/user/register.do

request

String username

String password

String email

String phone

String question

String answer

response

success

{

“status”:0,

“msg”:”注册成功”

}

fail

{

“status”:1,

“msg”:”用户已存在”

}

1. 检查用户名是否有效

/user/check\_valid.do

/check\_valid.do?str=admin&type=username 就是检查用户名

request

str,type对应的type是username和email

response

success

{

“status”:0,

“msg”:”校验成功”

}

fail

{

“status”:1,

“msg”:”用户已存在”

}

1. 获取登录用户信息

/user/get\_user\_info.do

request

无参数

response

{

“status”:0,

“data”:{

“id”:12,

“username”:”aaa”,

“email”:”aaa@163.com”,

“phone”:null,

“role”:0,

“createTime”:1479048325000,

“updateTime”:1479048325000

}

fail

{

“status”:1,

“msg”:”用户未登录，无法获取当前用户信息”

}

1. 忘记密码

/user/forget\_get\_question.do

localhost:8080/user/forget\_get\_question.do?username=geely

request

String username

success

{

“status”:0,

“data”:”这里是问题”

}

fail

{

“status”:1,

“msg”:”该用户未设置找回密码问题”

}

1. 提交问题答案

/user/forget\_check\_answer.do

localhost:8080/user/forget\_check\_answer.do?username=aaa&question=aa&answer=sss

request

String username

String question

String answer

response

正确的返回值里有一个token，修改密码 的时候需要用这个。传递给下一个接口

success

{

“status”:0,

“data”:”53lef4b4-966d-9a20-fb56367446a5”

}

fail

{

“status”:1,

“msg”:”问题答案错误”

}

1. 忘记密码时重置密码

/user/forget\_reset\_password.do

localhost:8080/user/forget\_reset\_password.do?username=aaa&passwordNew=xxx&forgetToken=53lef4b4-966d-9a20-fb56367446a5

request

String username

String passwordNew

String forgetToken

response

success

{

“status”:0,

“msg”:”修改密码成功”

}

fail

{

“status”:1,

“msg”:”修改密码操作失效”

}

或

{

“status”:1,

“msg”:”token已经失效”

}

1. 登录状态重置密码

/user/reset\_password.do

request

String passwordOld

String passwordNew

response

success

{

“status”:0,

“msg”:”修改密码成功”

}

fail

{

“status”:1,

“msg”:”旧密码输出错误”

}

1. 登录状态更新个人信息

/user/update\_information.do

request

String email

String phone

String question

String answer

response

success

{

“status”:0,

“msg”:”更新个人信息成功”

}

fail

{

“status”:1,

“msg”:”用户未登录”

}

1. 获取当前登录用户的详细信息，并强制登录

/user/get\_information.do

request

无参数

response

success

{

“status”0,

“data”:{

“id”:1,

“username”:”admin”,

“password”:””,

“email”:”18085459735”,

“phone”:”18085459735”,

“question”:”question”,

“answer”:”answer”,

“role”:1,

“createTime”:1479048325000,

“updateTime”:1479048325000

}

}

fail

{

“status”:10,

“msg”:”用户未登录，无法获取当前用户信息,status=10,转到登录”

}

1. 退出登录

/user/logout.do

request

无参数

response

success

{

“status”:0,

“msg”:”退出成功”

}

fail

{

“status”:0,

“msg”:”退出成功”

}

后台\_用户接口

1. 后台管理员登录
2. 模板
3. 模板
4. 后台管理员登录

/manage/user/login.do

request

String username

String password

response

success

{

“status”:0,

“data”:{

“id”:12,

“username”:”aaa”,

“email”:”aaa@163.com”,

“phone”:null,

“role”:0,

“createTime”:1479048325000

“updateTime”:1479048325000

}

fail

{

“status”:1,

“msg”:”密码错误”

}