常见功能测试注意事项

**（除了常规的测试以外注意）：**

## 1.登录：

1.1 提示信息是否合理:

例如 如果用户名正确，密码不正确 提示密码错误；用户名不正确，密码正确提示用户名错误，都是不合理的，根据提示信息别人就可以猜测，用户名或者密码，其中一个正确就可以进行另外一个爆破，因此合理的提示信息应该是用户名或者密码错误

1.2 登录的合理性

1.2.1 登录除了用户名和密码以外，应该添加一个动态验证码，防止无限次尝试

1.2.2 除了第一种情况外 或者对登录用户进行登录次数限制，到了指定次数则在指定分钟内不允许尝试登录，或者锁定找回密码

1.2.3 为了更严格的校验 建议用户名，密码+动态验证码+次数限制

1.3 登录加密

为了防止在传输过程中，用户名密码被截获，建议前端先进行加密，调用接口时，传输的是加密的数据

## 2.上传文本数据：

2.1 上传数据转义

上传的数据必须对前端的标签进行转义处理防止xss攻击（所谓xss攻击就是页面执行了攻击者的脚本，只要对标签进行了处理，浏览器无法根据标签来解析执行，问题自然就没有了）

2.2 上传数据添加验证码

上传数据时，必须进行验证码校验 防止用户通过jmeter或者其他并发工具来进行批量提交，造成数据库撑爆

## 3.多用户，多角色操作：

因为是多用户和多角色 这样每个人的权限可能会不一样，能查看或者操作的内容不一样，因此需要注意越权问题，越权分为垂直越权和水平越权

3.1 水平越权.

例如A和B两个用户是拥有同角色的用户，A用户操作或者查看自己的内容，成功执行,如https：//\*\*\*/\*\*\*/\*\*\*?apply\_id=20200931110001,这个id是属于A用户的，理论上B用户是没有权限查看A用户的内容的，此时B用户登录也调用上述接口 如果成功调用则说明存在水平越权，因为B用户能成功操作属于A用户的内容

3.2 垂直越权，

顾名思义 就是能操作比自己权限更大的内容，原理和水平越权类似

## 4.上传文件：

上传文件，除了常规的能上传成功外还要注意：

4.1 上传的格式要求

一定要设置好白名单 如只能上传png，jpg，pdf。。。，只能在有限的格式范围内上传，因为如果不设置好格式，对于一些用户可以上传一些攻击性的脚本，如当前系统如果java编写的可能会上传一些jsp， python编写的上传一些py文件等，能够被本系统的语言解析执行，且上传的格式必须是原来的文件格式而不是经过手动改动的格式

4.2 上传文件大小限制

要进行大小的显示，防止传的文件较大，没有传几个文件将磁盘占满

4.3 上传文件的上传逻辑

再次上传需要确认好需求，确认上传的逻辑，是覆盖，是共存，还是把原来的文件删除掉再次上传，防止可以一直上传许多垃圾文件

4.4 上传文件确认是否存在越权问题

4.5 如果存在多个上传框时，是不是可以继续上传同名文件

4.6 是不是可以上传0kb的文件

4.7 验证在磁盘满的情况下是不是还能继续上传

4.8 验证上传过程中网络较慢，超过一定时长是不是给与提示

4.9 上传过程中 网络中断是否给与正常提示

4.10 上传过程中 服务器挂掉是否给与正常提示

## 5.提交数据：

5.1.对于只读数据：

对于页面的只读数据，通过修改页面此数据的属性进行修改 然后提交，确认是否成功提交，并且提交的数据为修改后的数据，如果成功提交则为bug，如果成功提交，但是提交的数据为未修改之前的数据，则无问题

5.2.对于手机号码：

5.2.1.确认是否存在唯一性限制，因为目前手机都是实名制，有可能隐含条件是唯一的

5.2.2 除了常见的手机网段的手机号输入外，还需要注意最新开通的手机网段是否支持

5.3 对于邮箱号码：

5.3.1 需要注意带下划线的邮箱号，因为除了常见的qq等邮箱外，有的126或者其他的邮箱，允许用户的邮箱中输入下划线等特殊字符，需要注意，不然别人正常的邮箱无法进行输入提交

## 6.下载功能：

1.下载是否需要权限问题，比如我不登录直接调用下载接口是否正常

2.下载是否存在越权问题，比如a用户的能下载的内容，b用户理论上不应该能下载，同样的接口和参数值 b直接进行调用是否能成功调用

3.下载的文件名称是否有格式要求如年月日+特殊要求 等等

4.下载的内容是否正确，如果是excel等文件 内容是否符合需求

5.如果存在查询导出，导出的内容是不是查询后的结果，还是查询选中后的结果

## 7.查询功能

需要做个条件矩阵，对于每种情况进行组合和单个查询，另外需要手动编写sql，来对比开发的检索和自己写的sql查询到的结果是否一致