# 系统安全和权限设计

## 系统安全

### 前后端数据传输

前后端接口我们使用https协议，该协议会在传输层对传输的数据进行加密，可以防止一些抓包工具获取明文数据。主要优点有：内容采用混合加密技术，中间者无法直接查看明文内容；通过证书验证客户端访问的是自己的服务端；数据进行签名加密，可以防止数据被冒充或篡改。

### 传输数据进行过滤

为了防止XSS攻击、SQL注入攻击，后端会先对传输的数据进行过滤，然后再处理过滤后的数据。

### 数据库加密存储

为了防止数据库泄露或其它情况造成的用户私密信息（如登录密码等信息）泄露，所有存储在数据库中的私密数据都是加密后再存储的。用户登录密码会进行 md5（加盐）加密后存储在数据库中。

### 前端使用验证码

前端发送验证码的按钮设置两次的间隔时间为60s，防止被恶意刷按钮造成后端大量请求阻塞。

### 密码安全等级

用户注册的时候对密码的安全等级进行要求，必须达到一定的安全等级才能注册成功。

### 密码防爆破

用户连续输错密码三次后需要等待5分钟才能再次输入，用户连续输错密码5次后将发送邮件给用户示警。

### 接口防爆破

后端使用拦截器拦截用户的每次请求，如果某个用户在短时间内频繁大量访问同一个接口，该请求将会被拦截。

### token验证身份

为了防止CSRF攻击，我们将会使用jwt机制，每一次后端请求将会检查经过签名后的token数据，如果非法将禁止访问。

### 唯一登录

每个用户在同一时间段仅能维护一个登录的客户端，用户最新一次的登录将会把用户上次的登录踢下线。

## 权限设计

本系统采用Sa-Token框架进行权限管理，不同于shiro、Spring Security等权限管理框架，这框架较新，更加轻量级，且支持RESTful规范接口。

### 游客、封禁用户

仅支持博客、评论、各个板块的查询功能

### 普通用户

博客、评论、板块的增加、删除、修改、查询

收藏、举报博客

接收公告

树洞功能

### 管理员

用户、博客的封禁

用户统计数据

博客统计数据