doi:10.16104/j.issn.1673-1891.2018.03.022

# 基于Shiro框架的政协提案系统安全性研究与设计

陈 波,刘 星,兰全祥*
(攀枝花学院,四川 攀枝花 617000)

**摘要**:针对政协提案系统存在的安全性问题,提出基于Shiro框架的政协提案系统的安全性设计与研究。首先对政协提案系统的安全性需求进行分析,并指出系统普遍存在的安全性问题。经过政协提案系统的安全性研究与分析,提出了一些安全性设计措施与手段。实际应用表明基于Shiro框架的政协提案系统具有很好的抗攻击性和安全性。

**关键词**:政协提案系统;安全性;Shiro框架
**中图分类号**:TP311.522 **文献标志码**:A **文章编号**:1673-1891(2018)03-0094-04

# Research and Design of System Security of CPPCC Proposal System Based on Shiro Framework

CHEN Bo,LIU Xing, LAN Quan-xiang
(School of Mathematics and Computer Science, Panzhihua University, Panzhihua 617000)

**Abstract**: In view of the security problems existing in CPPCC proposal system, the security design and research of CPPCC proposal system based on Shiro framework are proposed. This paper first analyzes the security requirements of the CPPCC proposal system and points out the common security issue in the system. After the CPPCC proposal system security research and analysis, it puts forward some safety design measures and means. The practical application shows that the CPPCC proposal system based on the Shiro framework has good anti-attack and security.

**Keywords**: CPPCC proposal system; security; Shiro framework

## 0 引言

随着信息时代的飞速发展,政协提案方式从传统的文档形式转换到现有的基于网络的政协提案系统。传统的方式在人力物力上开销很大,并且文档的收集和提交受到区域和时间的限制,不能及时处理和流转提案信息。但基于网络的政协提案系统能很好地解决这些弊端,大大提升政协提案的处理周期,被大多数政府部门所运用。另外,政协提案系统中可能存在涉及国家机密的文件,因此系统在安全性上要求非常高。目前,一般的信息系统在安全性方面存在诸多的漏洞和问题,这些漏洞常被黑客利用并窃取系统信息。为了满足政协提案系统对安全性的高要求,本文提出了基于Shiro框架的政协提案系统,并针对系统的安全性问题进行研究与设计。

## 1 政协提案系统安全性需求分析

政协提案系统对于安全性的要求高于其他一般系统。在系统安全需求设计中,不仅需要有登录认证、请求拦截、权限细化、防SQL注入以及防暴力破解等功能,而且需要满足系统的保密性、完整性、可用性和抗毁性[1]。

### 1.1 用户登录认证需求

政协提案系统首先应具备用户登录认证、授权以及账户异常处理等功能。由于政协提案系统为非公共信息处理系统,因此需要进行用户登录认证,只有使用正确口令进行认证后才能进行系统操作。游客只能浏览首页面的公告信息。

用户在登录政协提案系统时,除了输入密码错误或用户名错误导致登录认证失败外,账号可能处于异常状态,如账户未激活、由于人员离职引起的账户注销或休眠等情况。其次,异地登录、多次认证失败将引起系统安全机制对账户的主动冻结和休眠。对于账号正常认证成功的用户,通过Shiro安全框架确定用户的角色并授权。政协提案系统的登录认证用例图如图1所示。

**收稿日期**:2018-01-02
**基金项目**:教育部高等教育司产学合作协同育人项目(201701048010);攀枝花学院科研项目(2016YB016)。
**作者简介**:陈波(1995— ),男,四川眉山人,本科,研究方向:网络工程专业。*为通信作者:兰全祥(1990— ),男,四川攀枝花人,助教,硕士,研究方向:计算机应用、软件开发技术。

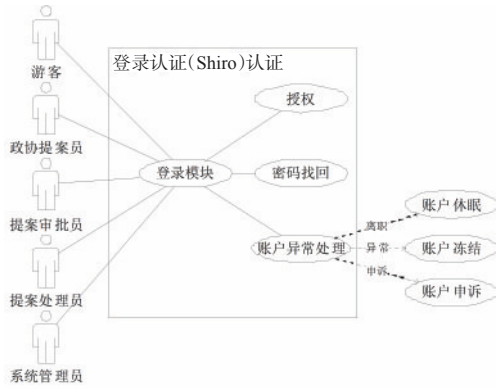


图1　政协提案系统的登录认证用例图

### 1.2 浏览器请求拦截

政协提案系统应具备请求拦截功能，拦截用户的非法访问和未授权请求。对于公共访问页面的信息，访问者不需要授权就可以直接进行访问浏览。但对于提案系统内部信息则需要授权认证之后才能访问。系统应具备URL直接访问拦截、登录超时下的授权销毁等功能。政协提案系统请求拦截流程图如图2所示。

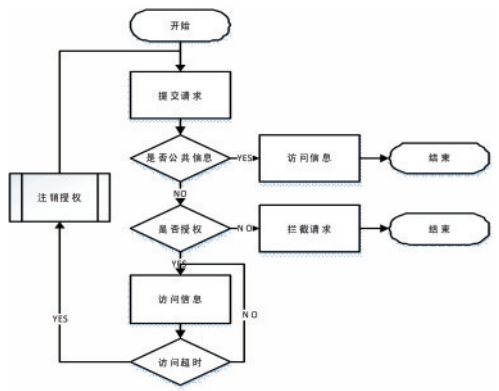


图2　政协提案系统请求拦截流程图

### 1.3 用户权限细化

政协提案系统应具备权限细化功能，可以为不同的用户进行不同的权限设定。该系统将包含多个模块，如个人信息模块、公告信息模块、提案模块、提案审核模块以及提案处理模块等。不同职务的人员应具备不同的权限，这就要求系统应具备权限细化功能，能够灵活、可变的处理所有用户的权限。

### 1.4 预防黑客攻击和非法入侵

除上述安全需求外，政协提案系统还应具备一般信息系统预防黑客攻击和非法入侵的功能。

（1）防止SQL注入式攻击。SQL注入式攻击是普遍存在于信息系统中的攻击方式。该攻击通过欺骗服务器执行恶意的SQL命令，使得数据库暴露或非法认证登录成功。

（2）防止暴力破解。暴力破解是一种基于穷举法的密码破译方法，IBM为美国军方制造的“飓风”超级计算机就是为了提高密码的破译效率而专门其制造的。因此防止暴力破解是信息系统必不可少的安全防护手段。

（3）MD5混合加密机制。Message Digest Algorithm MD5（消息摘要算法第五版）是计算机安全领域广泛使用的一种散列函数，用以提供消息的完整性保护和密码加密。虽然MD5是一种不可逆算法，但随着信息技术的不断发展，MD5库已经得到了极大的完善，简单的MD5加密已经不再安全。

（4）防止网络监听。网络监听是黑客最常使用、最有效的网络攻击方法之一。通过监视网络状态、截获网络传输信息可以有效地截获用户登录认证的关键数据。也就是说，当黑客伪造登录页面并将截获的信息发送至主机将轻易的获得授权。

## 2 政协提案系统的安全性设计

通过对政协提案系统的安全性需求进行分析，为了实现用户登录认证、权限细化、请求拦截以及一些常规黑客攻击和非法入侵防护，提出基于Shiro安全框架的政协提案系统，具体安全性功能设计如下。

### 2.1 Shiro框架实现用户身份认证和权限分配

Apache Shiro是一个功能强大、灵活性较好的Java开源安全框架，提供了身份认证、访问授权、数据加密和会话管理等功能，它能够为任何应用提供安全认证及身份控制，支持命令行应用、移动应用、企业应用和大型网络应用等不同环境下的安全保障[2]。

政协提案系统采用Shiro框架处理用户登录认证以及权限细化问题，能够很好地满足安全性需求。其次，Shiro提供了对WEB应用的强大支持，并且能很好的与第三方框架进行集成，方便系统开发[3]。

### 2.2 使用预编译SQL以及正则实现防SQL注入

SQL注入式攻击一般是通过传输特殊字符给服务器，使得原本的SQL命令发生改变，从而欺骗服务器执行恶意的SQL命令。因此，针对这一攻击手段可以采用java.sql中的PreparedStatement接口来预编译SQL语句，使SQL命令固化，不因传输的参数而发生改变。其次，采用正则表达式(又称规则表达式Regular Expression)限制用户输入特殊字符也能有效的避免SQL命令发生异常，防止SQL注入式攻击[4-5]。

政协提案系统采用预编译SQL以及正则表达式处理系统中SQL语句，能很好的预防SQL注入式

攻击。保证系统数据库中的数据不被非法访问者获取。

### 2.3 基于验证码以及复杂密码防止暴力破解

针对暴力破解这种基于穷举法的密码破译方法,验证码是非常简单、有效的方法。通过添加验证码,能大大降低黑客的攻击次数和频率[6]。另外,简单的密码非常容易被穷举法破译,因此为了增加黑客穷举攻击代价,在设置密码时要求包含大小写、数字及特殊字符,并且密码长度在规定范围之内,保证密码足够复杂,不易被破解。

政协提案系统采用验证码以及复杂的密码将能够很好的防止暴力破解。

### 2.4 使用MD5混合加密对数据库进行加密

MD5混合加密是基于MD5技术,通过设计特定的公式对数据进行加密。这样的加密方法是为了防止黑客通过查询MD5密码库来获得明文的有效手段。政协提案系统采用MD5混合加密能够有效的满足系统的保密性。即使数据被黑客获取后,真实数据也很难被破译。

### 2.5 使用时间令牌防止网络监听

用户关键数据在传输过程中很难避免被黑客截获,这就意味着黑客可以伪装成用户向服务器发送二次请求,并获得新的授权。政协提案系统可采用由系统产生一个基于系统时间的密文,客户端和服务端各持一份。用户的每次访问都具有不同的时间令牌,防止黑客进行模拟登陆。其次,将用户关键数据与时间令牌进行加密操作得到一个含有时间令牌的密文数据,即使监听到关键数据也是无效的[7-8]。

政协提案系统采用时间令牌加密关键数据,能很好地避免网络监听导致的数据泄漏和伪装请求。

## 3 系统实现

通过对政协提案系统的安全性分析与设计,该系统采用Shiro安全框架实现用户登录认证和权限细化,使用预编译SQL、MD5混合加密以及时间令牌加密关键数据,防止常规黑客攻击,具体实现如下。

### 3.1 Shiro框架的配置

首先在Java Web工程的web.xml文件中声明一个Shiro Servlet过滤器以实现Shiro与Web应用的集成[9]。

```
<filter>  <filter-name>shiroFilter</filter-name>
    <filter-class>org.springframework.web.
filter.DelegatingFilterProxy</filter-class>
</filter>
<filter-mapping>
<filter-name>shiroFilter</filter-name>
<url-pattern>/*</url-pattern>
</filter-mapping>
```

其次,在与Shiro集成的Spring配置文件ApplicationContext.xml中配置不同用户的访问权限。

```
/login.jsp* = anon
.....
/page_base_staff.action = perms["staff"]
/* = authc
```

其中anon表示允许用户匿名访问以/login.jsp开头的URL,perms表示需要特定用户认证才能使用,如/page_base_staff.action= perms["staff"]表示仅当认证用户为stuff才能访问此路径。authc表示主要用户通过认证即可访问以/* 开头的URL。

### 3.2 采用预编译SQL命令以及正则约束

基于Shiro框架的政协提案系统采用预编译SQL命令以及正则约束来实现SQL注入式攻击的防范。下面分别介绍两种方式在系统中的使用:

(1)在用户登录过程中,采用预编译SQL语句来实现,使攻击者无法改变SQL的结构。用户传递的参数采用“?”占位。

```
String sql = “select * from user where uid = ?”;
PreparedStatement ps = conn.prepareStatement
(sql);
ps.setString(1,id);
```

ps对象包含语句“select * from t_user where uid = ?”,它已发送给DBMS,并为执行作好了准备。在执行PreparedStatement对象之前,必须设置每个?参数的值。无论参数值为什么,此SQL命令不会发生变化。

(2)使用正则表达式来过滤传入的参数,首先需要创建正则表达式String CHECKSQL = “^(.+)\\sand\\s(.+)|(.+)\\sor(.+)\\s$”;再进行判断是否匹配Pattern.matches(CHECKSQL,targerStr)。其中targerStr表示传入的参数,CHECKSQL表示约束条件,当判断为true时传入的参数无效,页面提示用户输入不合法。

### 3.3 验证码

基于Shiro框架的政协提案系统的验证码实现主要包含对验证码字符的随机生成、干扰线的随机添加以及关键字符的拉伸变形。

首先随机生成n位验证码字符,代码如下:

```
for(int I =0;i<n;i++){
```

```
intindex=random.nextInt(ele.length);
codes=codes+ele[index];
}
```

其中,n为生成验证码字符个数;ele为验证码可选字符数组。然后对验证码图片进行随机线条干扰和旋转拉伸:

```
// 将文字旋转指定角度
Graphics2D g2d_word = (Graphics2D) g;
AffineTransform trans = new AffineTransform();
trans.rotate(random.nextInt(45)*3.14 / 180, 15 * i + 8, 7);
// 拉伸文字
float scaleSize = random.nextFloat() +0.8f;
if (scaleSize > 1f)  scaleSize = 1f;
trans.scale(scaleSize, scaleSize);
g2d_word.setTransform(trans);
```

### 3.4 MD5对数据库加密

为了提高政协提案系统的安全性,在密码方面采用了MD5混合加密算法,防止单一MD5加密被查表攻破,具体实现代码如下:

```
String password = MD5.GetMD5Code(string_left + MD5.GetMD5Code(password).substring(m, n) + string_right);
```

其中m,n取值范围在0-32之间,且m<n。string_left、string_right为系统默认提供的前置字符串和后置字符串。

### 3.5 时间令牌

为了防止数据在网络传输过程中被截获破译,政协提案系统采用了时间令牌来防止网络监听。

首先,在用户发起请求时,由服务器生成一个包含时间的认证令牌,并将该令牌放入session容器中以便于识别用户是否为正常认证。

```
String secret=Conver2MD5.getMD5(new Date().getTime()+"");
request.getSession(true).setAttribute("secret", secret);
```

当用户进行登录认证时,系统自动将密码与时间令牌进行组合并使用MD5进行加密再发送服务端进行认证。

```
var user_pwd = md5(md5($("#password").val())+$("#secret").val());
```

服务端在接受到客户端的认证数据后,系统自动从session域中获得请求用户的时间令牌,从数据库中获取用户信息,并将两组数据按照与客户端相同的加密方法进行加密,得到密文db_pwd。比对服务器密文db_pwd与用户提交密文user_pwd是否匹配并将时间令牌进行销毁,匹配成功则认证通过,反之认证失败。

```
String user_pwd= request.getParameter("password");//获得用户提交密文
String db_pwd=Conver2MD5.getMD5(user.getPassword()//构造服务器认证密文
+request.getSession().getAttribute("secret"));
request.getSession().setAttribute("secret","");//销毁时间令牌
password.equals(db_pwd); //判断密码匹配
```

## 4 结语

本文通过对政协提案系统的安全性进行了详细的分析和设计,并提出了基于Shiro安全框架的政协提案系统,使程序授权更加灵活,权限控制更加严格,系统更加安全。针对普通系统存在的SQL注入漏洞、明文密码以及网络监听,系统采用了预编译SQL、验证码、MD5混合加密以及时间令牌等技术。经验证系统很好地防范了上述安全问题,提高了系统的安全性。

**参考文献:**

[1] 赵俊杰.政协提案管理系统的设计与实现[D].成都:电子科技大学,2015.
[2] 黄经赢.基于Shiro框架的细粒度权限控制系统的设计与实现[J].广东技术师范学院学报,2013,34(7):20-23+26.
[3] 翁云翔. Java安全框架Shiro在Web中的研究与应用[D].武汉:武汉邮电科学研究院,2016.
[4] 金鑫,卫文学.SQL注入的攻与防[J].电脑知识与技术,2015,11(20):4-5+10.
[5] 李少峰.防止SQL注入方法攻击的研究与探讨[J].鄖阳师范高等专科学校学报,2014,34(3):17-19.
[6] 王斌君,王靖亚,杜凯选,等.验证码技术的攻防对策研究[J].计算机应用研究,2013,30(9):2776-2779.
[7] 柳鑫瑶.网络监听的防范措施[J].电子制作,2017(20):88-89+85.
[8] 过玉清.网络安全中网络监听与防范技术探析[J].数字技术与应用,2016(1):224.
[9] 徐孝成.基于Shiro的Web应用安全框架的设计与实现[J].电脑知识与技术,2015,11(16):93-95.

(责任编辑:曲继鹏)