# Purpose

The purpose of this document is to understand role based access control and open forward. Later on, we use open forward vulnerability in the application to bypass access control.

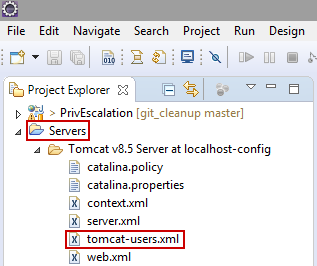
# Role Based Access Control

This application has proper access control in place. It does not allow user role (lower role) to access admin role pages.

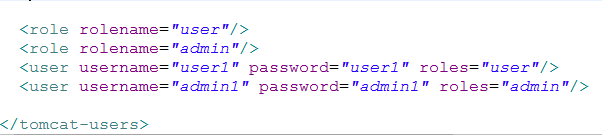
## How to test?

Set up two user roles in Tomcat Server

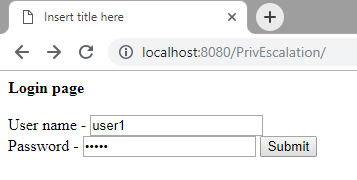
1. User
2. Admin

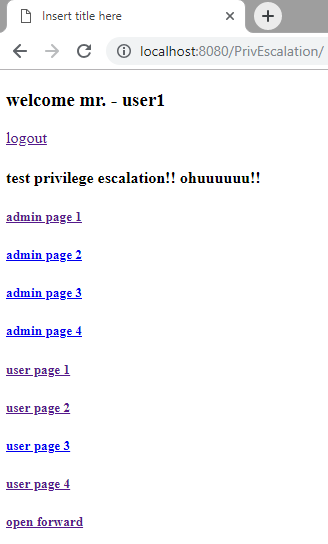


Edit tomcat-users.xml

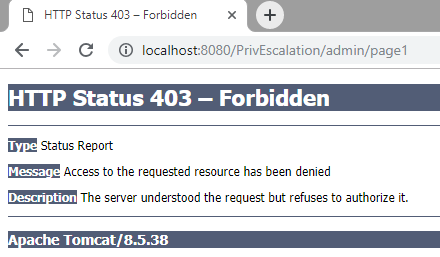


Login with user role - user1/user1





Go ahead and try to access admin pages



## Observation

A person with user role cant access pages meant for the admin role.

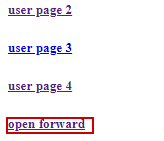
## Code(/WEB-INF/web.xml)

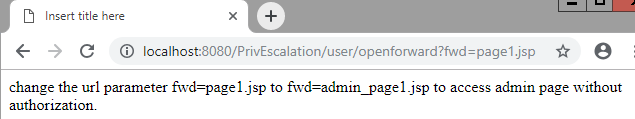


# Open Forward

## How to Test

Login with user role and click on ‘open forward’ link located at the bottom of page.





Change the url parameter to fwd=admin\_page1.jsp

## Observation

We have exploited open forward vulnerability to access admin page without being authorized to do so.

## Code(/PrivEscalation/src/OpenForward.java)

