PROJECT DELIVERABLE

PROPOSED BY

RAGHAVENDRAN MUTHUSAMY

**Business Problem**

In today’s business world, every asset of an organization is mostly in digital form. This creates the risk of security threats from hackers stealing the data. Hacking has taken so many new forms that to prevent this, companies need to invest a lot on security tools and providing training to its employees and conducting security audits on a regular basis.

Despite these investments, many companies are being compromised. The main reason is because of unskilled and untrained employees in the organization. For instance, every employee is given a mandatory training to avoid emailing spoofing. Still every company that perform security audit, at least 4/10 employees in an organization are being victims of email spoofing. But the scary thing is all it needs for a hacker is a single victim to get into the organization.

In general, intrusion detection system (IDS) monitors the incoming traffic of an organization. It scans the incoming packets form all the websites visited by the employees in the organization. The firewall generates a log report at the end of the day. These log files are not being used efficiently.

**Proposed Solution**

To prevent such problems, it is better if we get aa complete understanding of the of security tools. Our proposed system is to add an additional functionality to the intrusion detection system(IDS). By the end of day, based on the log generated by the firewall, a warning mail will be sent to the employees who visits malicious websites and an entry will be made. If the employee visits malicious websites for more than three times a month then the employee needs to attend a mandatory security training. By enforcing such rules, employees will be more concerned in type of emails they access and websites they visit. This should be given utmost importance because most organizations are bringing in BYOD (Bring Your Own Device) policy.

Since in real time most organizations will have IDS to their infrastructure sending email to the employees automatically but since we are trying to replicate a prototype for this scenario we are going to send the email to the user’s manually.

**Functionality of the Application**

The application is expected to have the following features

* IT person can track access history of all employees in the organization
* Manager can access his own and access history of his team members
* Employee can access their own access history

The interface will be a Java website. With following facilities

* Login page – Static Page
* Access History Page – Dynamic (Depending on the user)
* Access Device Details – Dynamic page
* Send Email Page – Static Page (only for IT admins)
* Send Alert Page – Static page (only for IT admins)
* Logout Page – Static Page

**Business rules**

1. Every project can have one or more groups.
2. Every group can have one or more employees.
3. Every employee can have one or more devices.
4. Every device can access a website one or more times in a day.
5. Every project can have only one manager.
6. Every group can have only one team lead.
7. Manager can view the access history of the employees in his/her project.
8. Team lead can view the access history of the employees in his/her group.
9. IT admin can view the access history of all the employees.

**Structure of Database**

**GROUP TABLE**

Keys:

PK – Group\_ID

FK – Project\_ID

Dependency:

Every group should be a part of the project in project table corresponding to a project\_id. And every group should have at least one employee taken from the employee table corresponding to Emp\_ID.

**EMPLOYEE TABLE**

Keys:

PK – Emp\_ID

FK – Group\_ID

Dependency:

Each employee might or might not be a part of a project. If the employee is in a project, he/she should be a part of any group in the project.

Each employee can have one or more devices registered. Each device registered by the employee should be entered into device table.

Every group should have a team lead referenced as Emp\_ID derived from employee table.

**PROJECT TABLE**

Keys:

PK – Projet\_ID

Dependency:

Every project can have one or more groups associated with group table.

Every project should have a manager referenced as Emp\_ID derived from employee table.

**DEVICE TABLE**

Keys:

PK – MAC\_ID

FK – Emp\_ID

Dependency:

Every device registered by an employee should be registered by MAC\_ID of the device.

Many devices can be registered by a single employee in employee table.

**ACCESS\_HISTORY TABLE**

Keys:

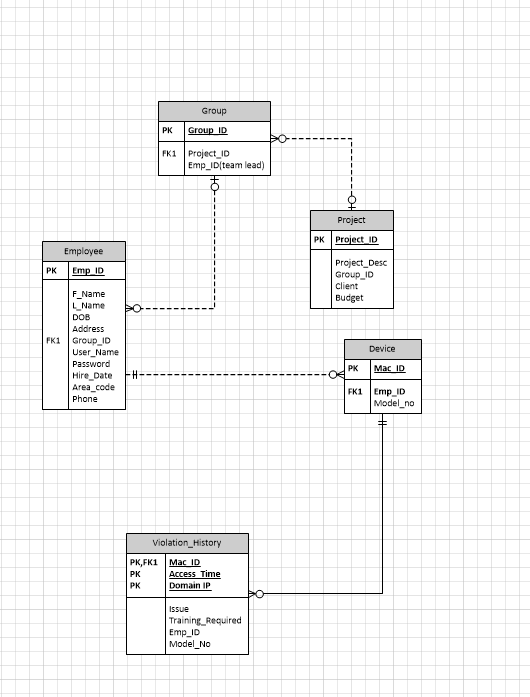
PK – {MAC\_ID, ACCESS\_TIME, DOMAIN\_IP}

Dependency:

For every mail sent by IT ADMIN, a record will be made in Access\_History table for corresponding employee.

* Our database consists of 5 tables namely, employee, group, project, device, access history.
* Employee table contains the following details of the employees – Emp\_ID, Fname, Lname, DOB, Address, Group\_ID, Username, Password.
* Emp\_ID will be the primary key in employee table.
* Group table consists of details about the group like group\_ID, project\_ID, Emp\_ID. Emp\_ID acts as team lead for the group.
* Group\_ID will be primary key in group table.
* Project table consists of details about the project like Project\_ID, roject\_Desc, Emp\_ID. Emp\_ID acts as manager for the project.
* Project\_ID will be primary key in project table.
* Device table consists of MAC ID of the device registered by the employee, Emp\_ID, Model\_no of the device.
* MAC\_ID is the primary key in device table.
* Access\_history table consists of MAC\_ID, Access\_Time, Website visited by the employee, Emp\_ID.
* MAC\_ID, Access\_Time, Domain\_IP acts as composite key in Access\_History table.
* Group table and employee table has 1:M relation between them which states that one group can have one or more employees.
* Project table and group table has 1:M relation between them which states that one project can have one or more groups.
* Employee table and device table has 1:M relation which states that each employee can have one or more devices.
* Device table and Access\_History table has 1:M relation which states that each device can access one or more websites more than once.

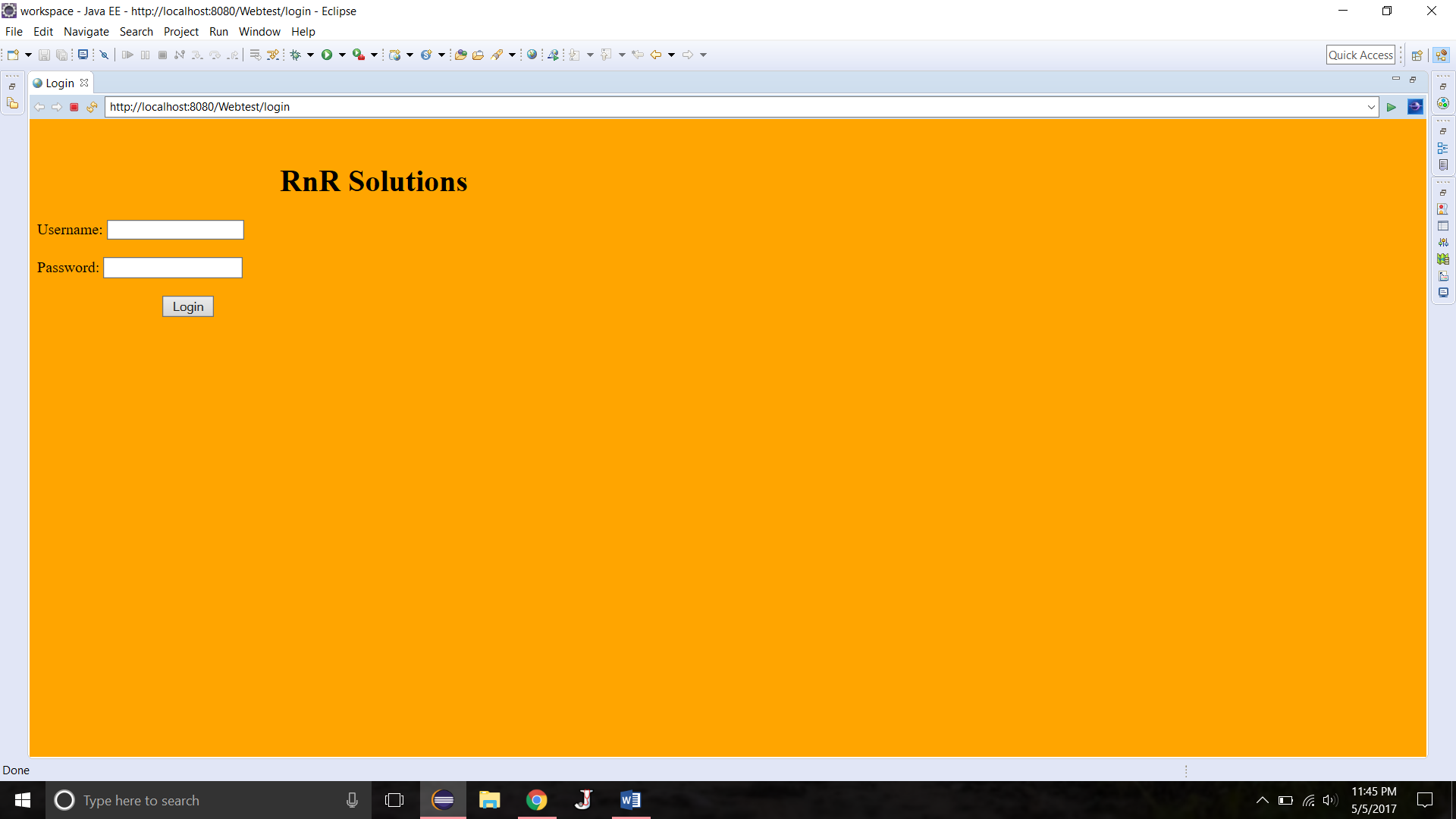
**ERD Diagram**

****

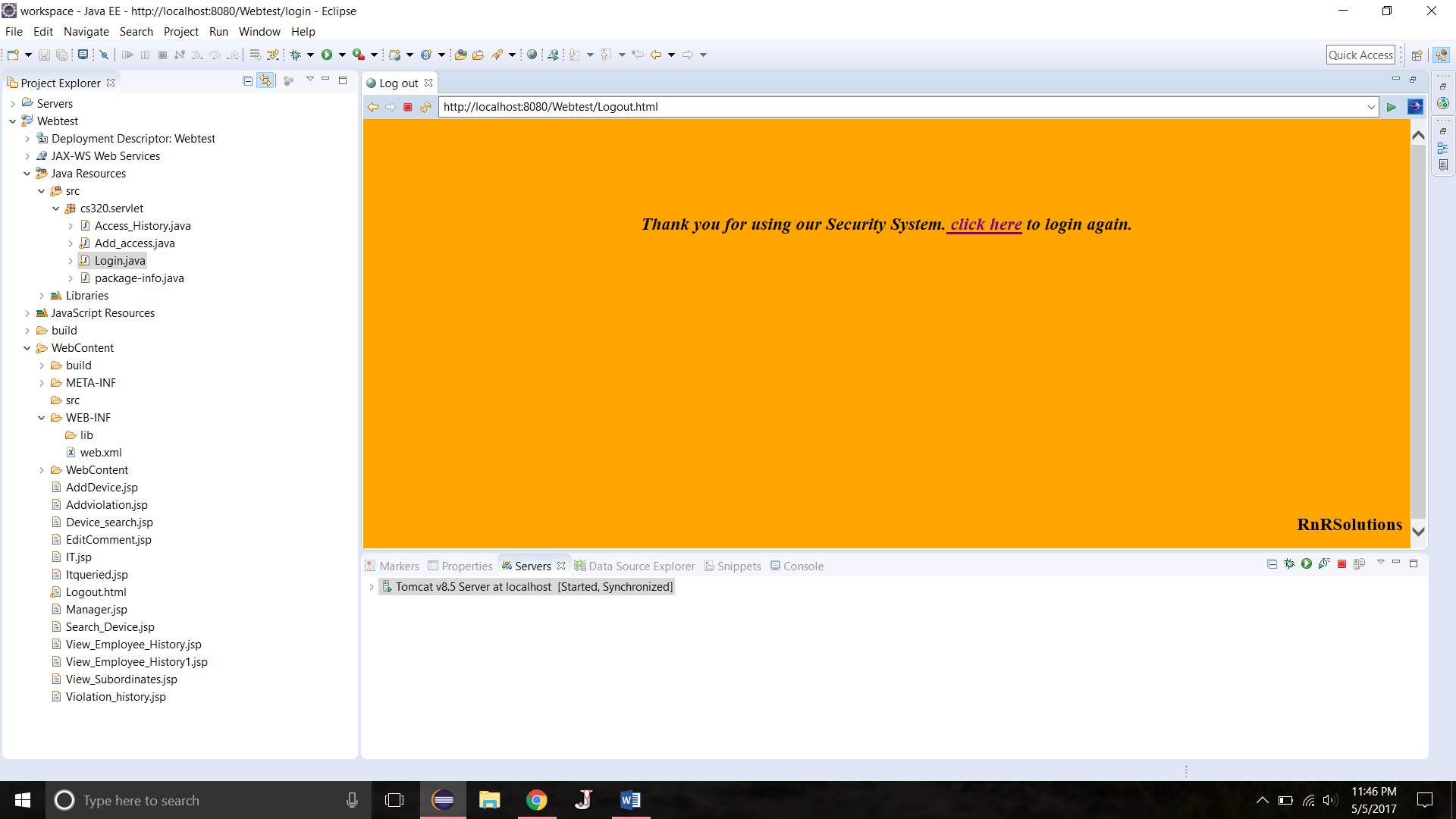
**UI screen shots**

**Login**

This screen is used to authenticate the user. Depending on the type of user his pages will be followed.



**Logout**

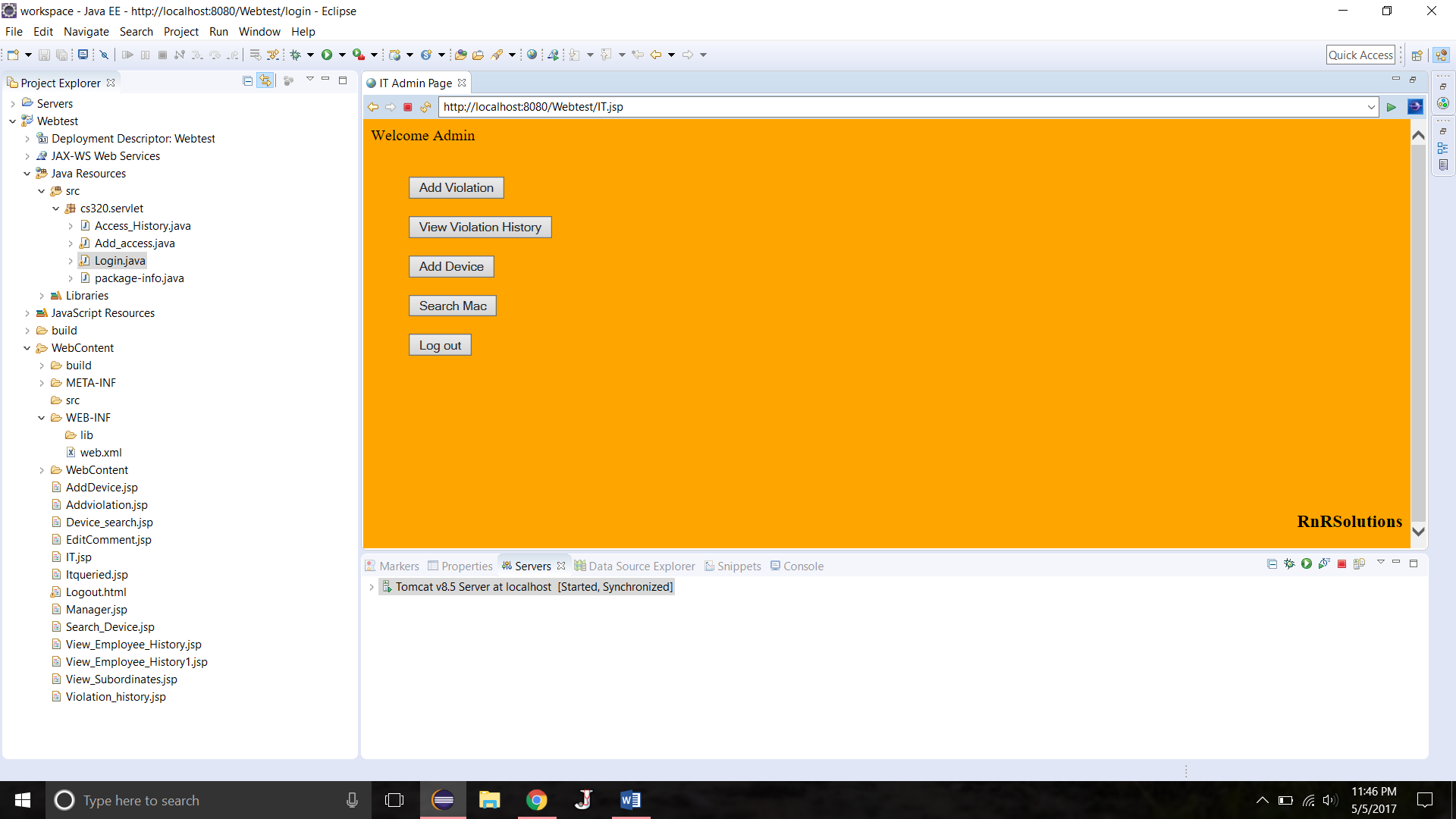


This is a logout page with a feature to login again.

**Navigation Page**

Depending on the type of user his navigation page is decided

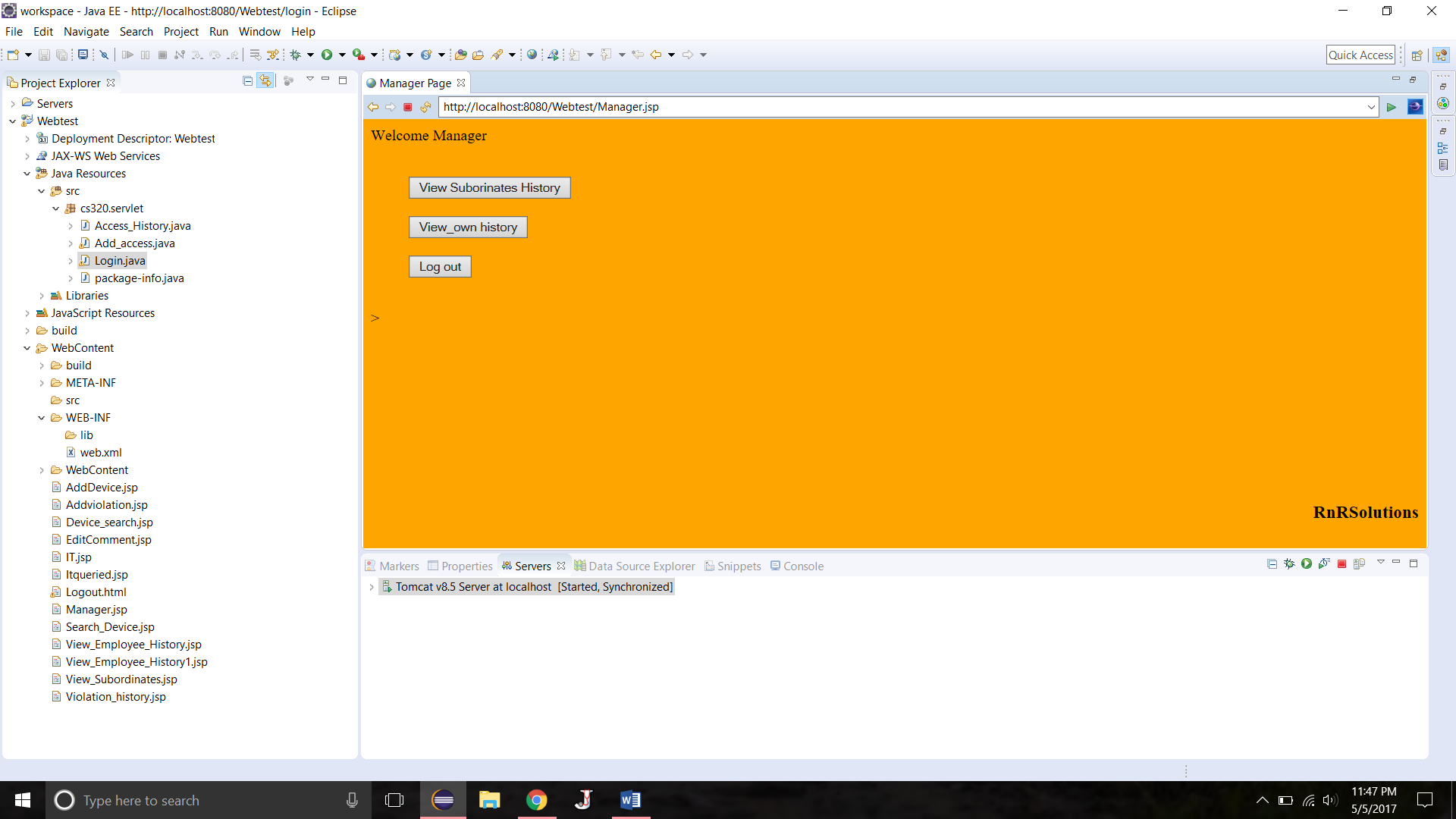
**IT admin**



* This user is a master user he will have all access over the application he can add a user, delete a user, send alert to his employees, search mac address of an employee etc..

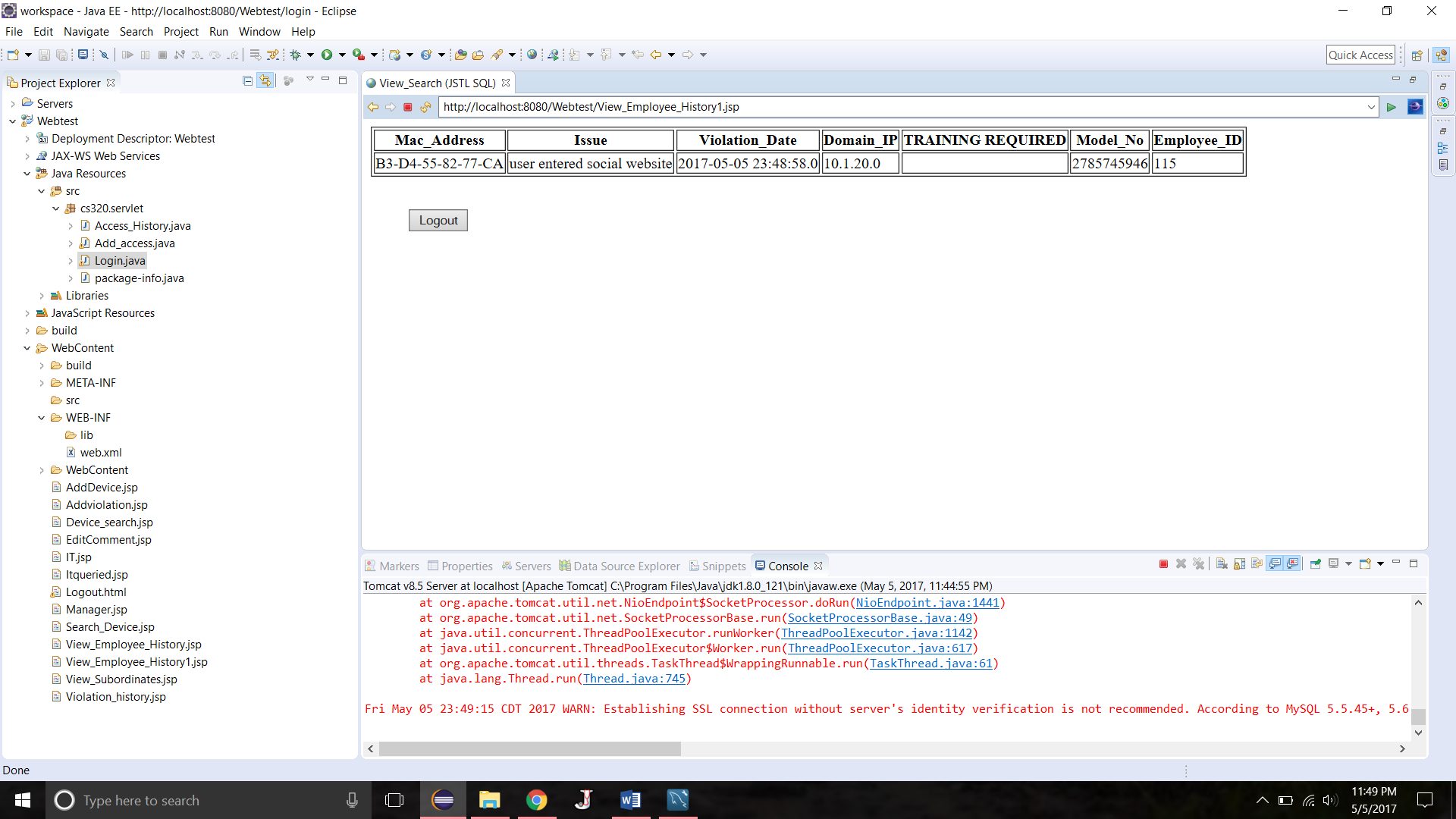
**Manager**

Manager will have access to view violation history of his own and his subordinates.



**Employee**

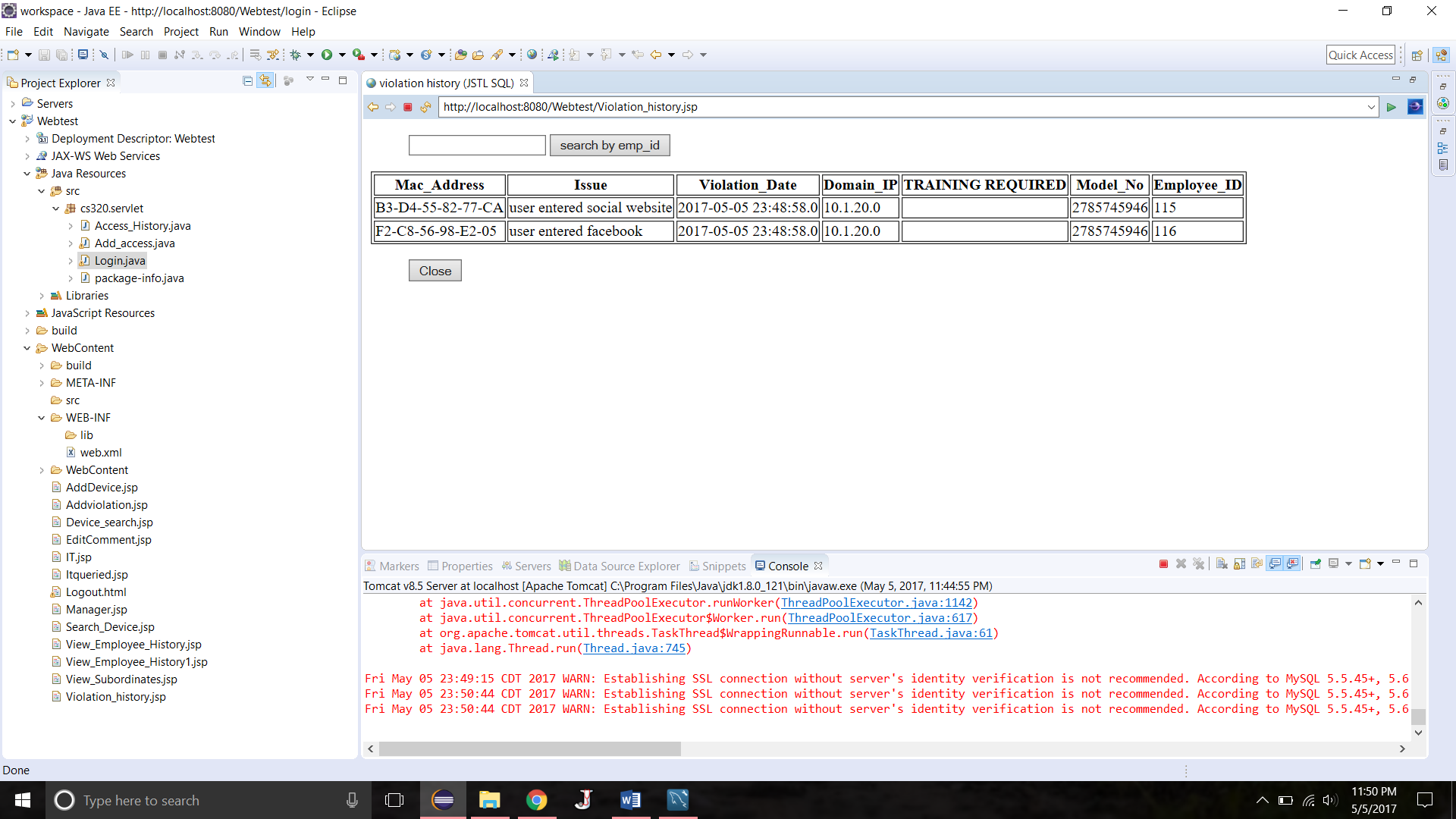
Employee can view his own violation history.



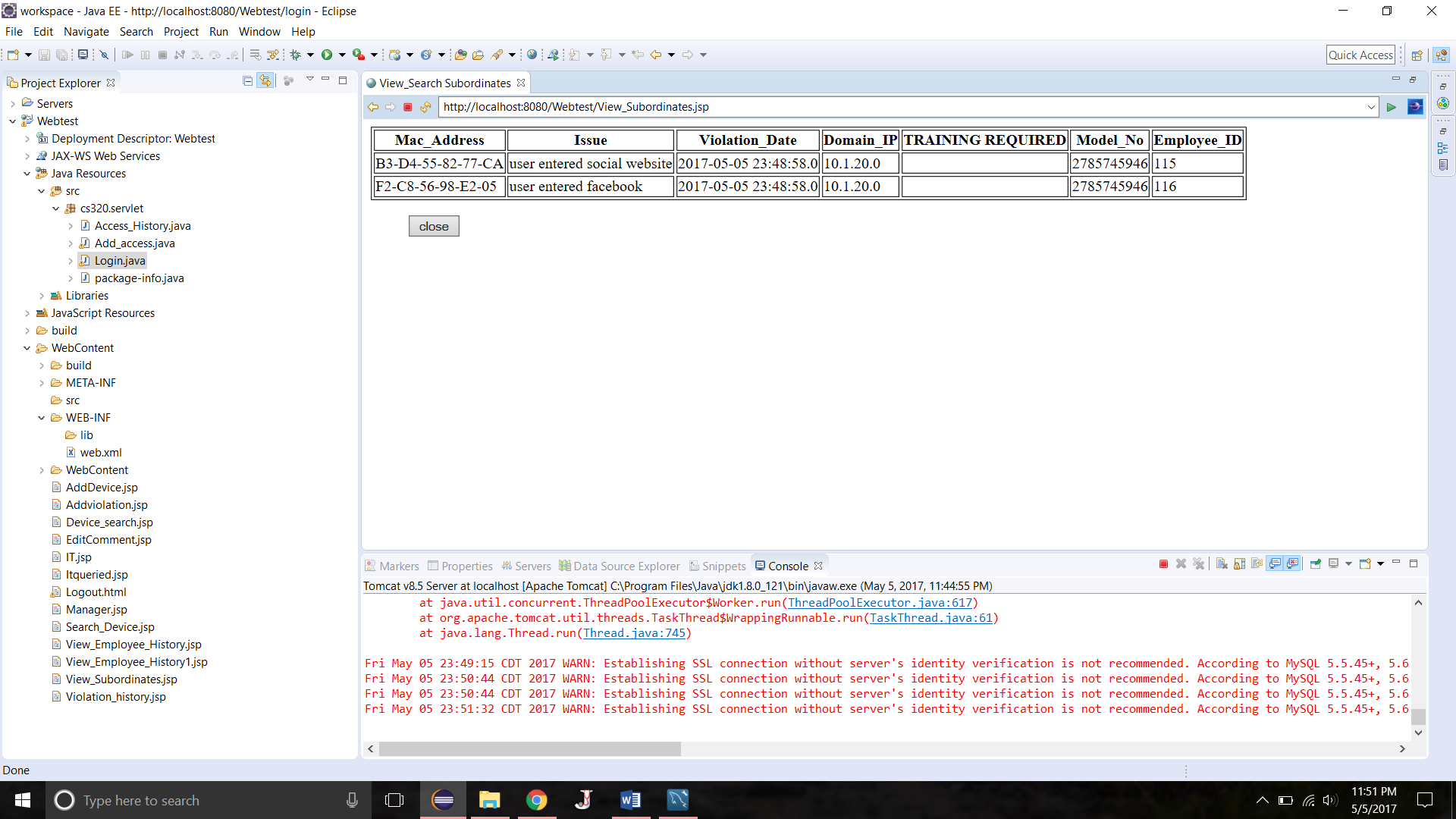
**Other Pages:**

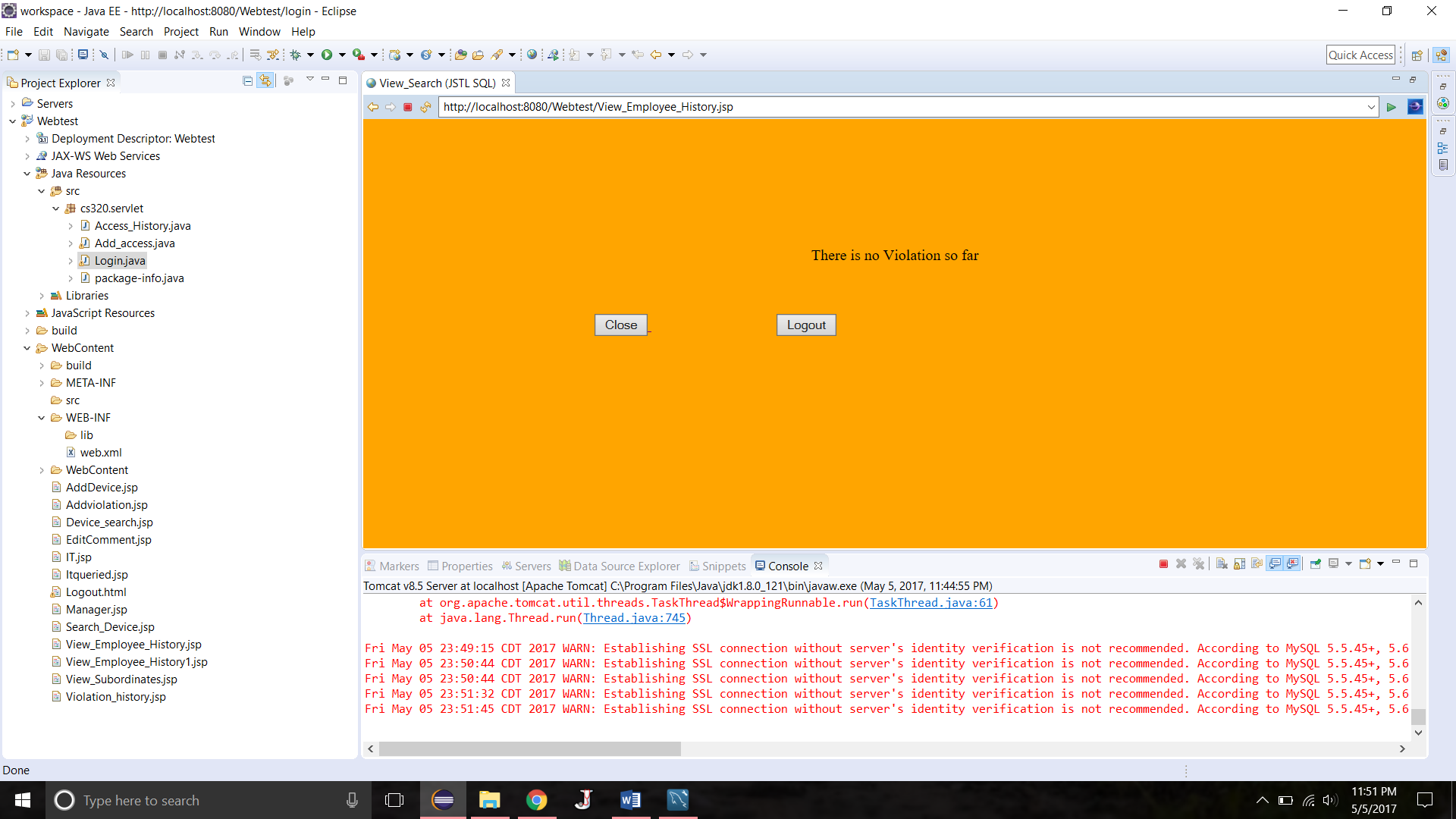
**View Violation history:**

This page is common but content differs from designation. For instance IT admin can view all the employees violation history



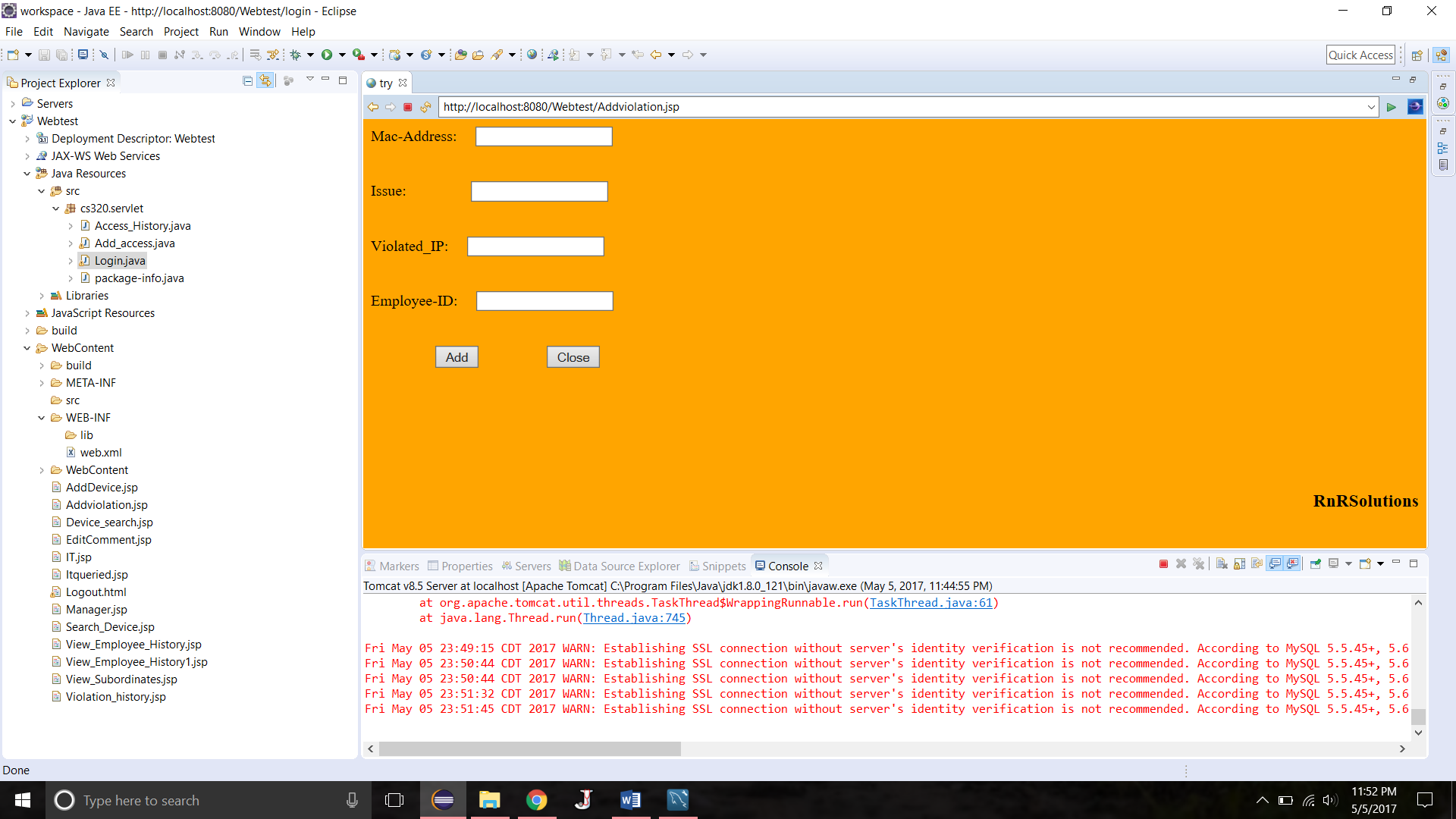
**Manager can view his subordinates and his own**





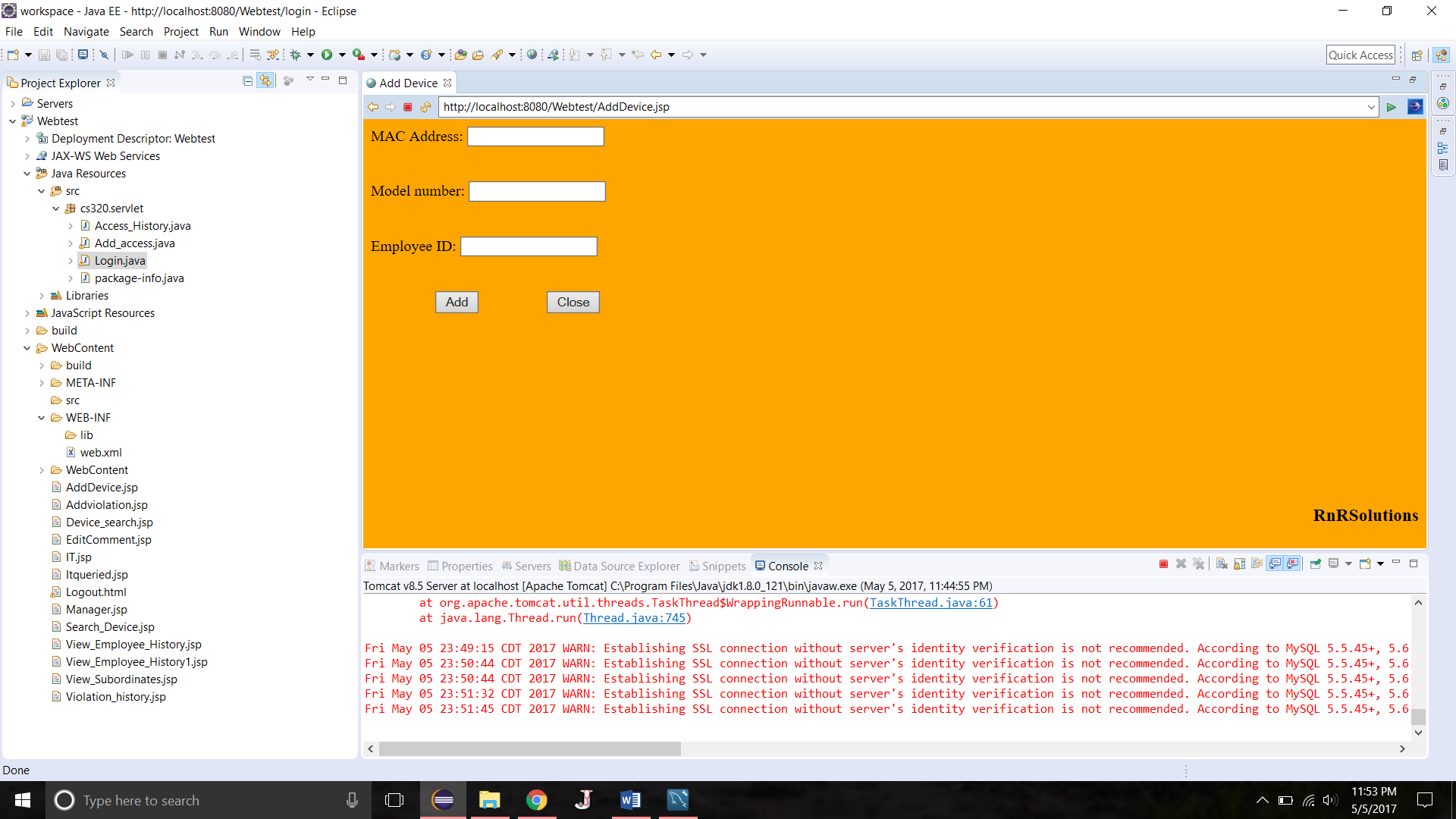
**Add Violation History**

This is only for admin to add an violation history entry.



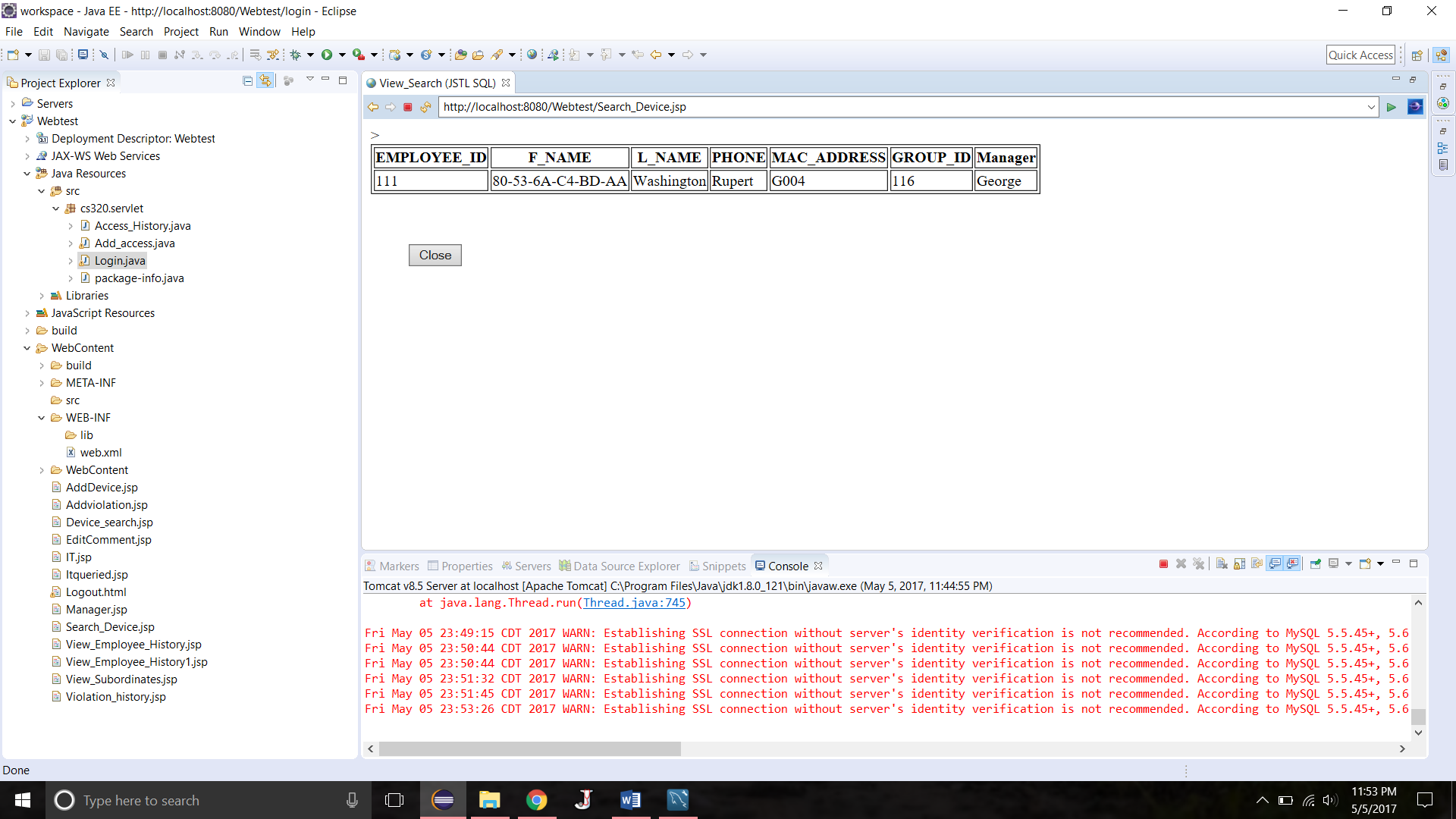
**Add Device**

**This page is to add a device**



**Search Mac:**

This page is to search Mac address of an employee



**Training Required**

The feature is if an employees record is updated thrice or more than that his training attribute will be updated to **‘yes’.**

