**COMP3911 Coursework 2**

**Pair Submission**

Razvan-Antonio Berbece (sc19rab), Konstantinos Kakarelis (sc19kk)

# **1 Analysis of Flaws**

1. **SQL Injection** - the POST form data is not sanitised on any of the client and server (application is vulnerable to information disclosure and elevation of privilege threats)
2. **HTTP used over HTTPS** - sensitive POST form data (usernames, passwords, patient surnames) can be eavesdropped and interpreted
3. **Passwords are stored in plain text** - the user passwords are stored in plain text in the SQL database, which means that they can easily be retrieved and interpreted
4. **Information leak in HTTP response headers** - the server's response headers hold information about the version of the server framework which can then be researched by attackers to find more Jetty exploits
5. **Password auth is implemented poorly** – authentication brute force attacks are possible because there is no tracking of failed login attempts or account lockouts
6. **Users can have the same username** – the database schema does not enforce unique username entries
7. **SQL Server can be accessed without credentials** –the sqlite3 database can be accessed both from code and in the terminal without any credentials, which means that bad actors with access to a machine running the web app can mutate or read the database
   1. SQL Injection

The form fields on the “login.html” page have no validation on the client-side and are sent as is to the server. We proved this by looking at the actual payload of the HTTP POST request sent to the server. Additionally, there is no restriction on the form field details that a user can input in the user interface (anything can be input in the fields).

The server does not do ANY input validation either, which means that the form field values are used in the SQL statements as is. We proved this by investigating the codebase, and (for example), the username and password strings provided by the client are formatted into the final SQL command without any other validation or checking.

This means that the service app is vulnerable to:

1. **Information disclosure** (reading confidential patient data without needing the required access credentials)
2. **Elevation of Privilege** (being use the system without being a registered user)

**To Reproduce:**

**- With no username & no password (Critical)**

**1. Input the “' or '1'='1” string into the username field**

**2. Input the “' or '1'='1” string into the password field**

**3. Submit POST form**

The application will display “No records found.” in both cases, which means that the server ran the query with an empty surname string for an unauthorized user (no password or username provided).

**We also found a way to query ALL existing patient records in the database without a valid credentials pair (Critical):**

1. Input the “' or '1'='1” string into the username field

2. Input the “' or '1'='1” string into the password field

3. Input the “' or surname=surname; --” – *to get all entries for which the surname field exists*

4. Submit POST form

* 1. HTTP used over HTTPS

We discovered this vulnerability by checking that the protocol used in the URL of the web app (<http://localhost:8080/>) is indeed HTTP, and by confirming that the Jetty server setup code has no HTTPS configuration implemented or used for the server instantiation.

This vulnerability can be exploited by an attacker if they have access to a machine which runs the patient records application. They could then eavesdrop (through a ‘***tcpdump’*** command) on the outbound and inbound connections to and from the compromised machine and narrow it down through filtering it by protocol (i.e., HTTP) and / or the port number (i.e., 8080).

This means that the service is vulnerable to:

1. Information disclosure (of patient data from the response traffic, of account details from request traffic)

Graphical user interface

Description automatically generatedThe picture below depicts what an attacker running the ‘***tcpdump’*** command on a compromised machine which runs the application could see in the case of an **outgoing request**.

Note that the POST form data sent (username, password, surname) is visible and not encrypted.

# **Fixes Implemented**

* 1. Fix for SQL Injection

In order to fix the vulnerable SQL statement string formatting which allows SQL injection attacks, we used Java PreparedStatements.

The prepared statement query strings use a question mark to note where variables should be formatted in (e.g.: “select \* from user where username=? and password=?”). **Because of this question mark placeholder feature, attackers won’t be able to force close the starting apostrophe (‘) in a classic SQL Java formatted query string (e.g. ”select \* from user where username=’%s’ and password=’%s’”) via a malicious user input and add more query clauses to force the queries to be evaluated to true or return authorized data**. The prepared queries post-fix will look like this: “select \* from user where username=' or '1'='1 and password=' or '1'='1”, which will fail and clearly not evaluate to true, preventing the injection attack.

We applied the PreparedStatement fix (replacing the string interpolation construct ‘%s’ with a question mark) to both AUTH\_QUERY and SEARCH\_QUERY as both queries use parameters received unsanitized from the client.

In the searchResults() and authenticated() methods, to pre-compile and prepare the statements, a PreparedStatement object is created and initialized using the .prepareStatement() method of an SQL connection. The placeholders are then switched to actual values using the .setString() method that a PreparedStatement object has access to using the parameter index and the variable value to inject in the pre-compiled statement.

* 1. Fix for HTTP used over HTTPS