Web Security

Securing online chat based application

Keywords : SQL injection, Password encryption, Testing, Cryptography, Authorization.

Tanmay Kumar   : 19BCE2146
Mudit Jain   : 20BCE0362
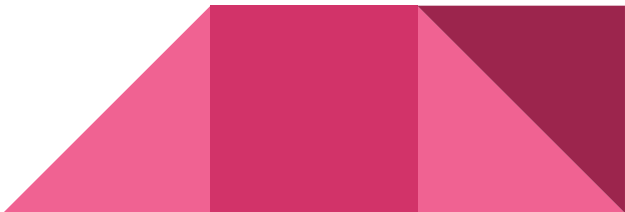Anusha Ajay Bamzai : 20BCE2833

Problem Statement

To Create and secure a fully functional website for online chat based communication from all the basic threats and vulnerabilities.

Abstract

Stealing the Data is a big concern in these chat based applications.

This application is going to be specially for developers and they don't want their data to be leaked, So in order to overcome this problem, We must consider some good security measures.

Survey Table

Link to the Survey Table : <u>Click Here</u>

1. Empirical Analysis of Web Attacks
2. CSRF protection in JavaScript frameworks and the security of JavaScript applications
3. FIDO2 puts biometrics at heart of web security
4. Electrolint and security of electron applications
5. Secure Hash Algorithms and the Corresponding FPGA Optimization Techniques.

Security measures under consideration

At the 1st Completion, we are going to consider only the basic level security constraints.

- We will try to add session Management.
- Prevention from SQL injection.
- Password protection.
- Standard level of data encryption.

Implementation Details :

- **SQL Injection :** For that we will try to add constraints towards the user input with the help of prepared statements and Regular expressions so that the user can't be able inject any SQL program.
- **Password Encryption :** We will try to use techniques like Blowfish algorithm or SHA so that we can secure the password via encrypting it.
- **Data Encryption :** we will use AES algorithm for protecting the data against the Meet in The Middle attacks.
- **Authentication :** JAX-RS 22 - REST API Authentication Mechanism
- We may also try to make a decentralized Server, so that if the attacker gets the access over a particular server node, It won't be much harmful.