Course Project Proposal: E-Charge Stations

Objective

The main objective of this project is to design a secure and user-friendly e-commerce website. Through this platform, it will allow homeowners with electric vehicle (EV) charging stations to list their stations, set availability, and enable customers/users to book and pay for charging sessions.

A key focus of this project is security, since all e-commerce platforms handle sensitive user data, including login credentials and payment information. To mitigate security risks, the system will implement Multifactor Authentication (MFA) for enhanced user authentication and integrate a secure payment gateway to process transactions safely.

Through this project, we aim to identify common security challenges in e-commerce platforms and implement practical security solutions to safeguard user data, prevent fraud, and ensure secure payment processing.

E-Commerce Selection

The chosen platform is "eChargeStations," which is like Airbnb but for EV charging stations. Homeowners with charging stations can create accounts, list their stations, and set booking timings. Users looking to charge their electronic vehicles can book a time slot and pay for the service.

Project Scope

- Homeowners can create accounts, list charging stations, and set available timings.
- Users can browse available charging stations, book appointments, and pay for the service.
- The website will have a product catalog (the charging stations), a registration system, bookings, a checkout process, and information about the platform.
- Users, after paying, can then visit the homeowner’s location at the scheduled time to charge their vehicle.

Security Focus Security in this type of project is very critical for protecting user data and payment details. The website will use MFA for user authentication, ensuring only authorized users can access accounts and book charging stations. A secure payment gateway will be integrated to handle payments safely. Moreover, there will be extensive focus on input validation to prevent malicious attacks.

Security Challenges

- Protecting user data: User login information and personal data must be safeguarded and kept safely.

- Secure transactions: Payment details need to be protected to avoid fraud or theft.
- User authentication: Ensuring only legitimate users can access and use the service.
- SQL Injection Attacks: Attackers could try to inject malicious SQL queries into the database through user input fields.
- Sensitive user data such as personal details, payment information, and login credentials could be exposed in the event of a breach.
- Attackers may attempt to guess user credentials using brute force methods.

Security Solutions

- Implementing MFA: Implementing Multi-Factor Authentication (MFA) adds an extra layer of security during login by requiring more than just a password (e.g., a code sent to the user's phone authenticator app).
- Secure payment gateway: Integrate a trusted payment system, like Stripe, to ensure that all transactions are secure and verified.
- Implement input validation and sanitize user input to prevent malicious attacks, such as SQL injection attacks.
- SSL Certificate: Use of strong encryption (SSL/TLS) for data transmission to protect data in transit to prevent data breaches.
- Google reCAPTCHA: Implement CAPTCHA to prevent automated bots from attempting login.

Risk Assessment

Despite using MFA and a secure payment gateway, potential risks include:

- Weak passwords: Users may choose insecure passwords.
- Phishing: Attackers might try to trick users into revealing login details.
- Data breaches: Unauthorized access to user data if other parts of the system are compromised.

Project Timeline

- **Week 1-4:** Design and planning of website features, including user interface and security protocols.
- **Week 5-8:** Development of the registration system, station listing, and booking functionalities.
- **Week 9-12:** Integration of MFA, secure payment gateway, and additional security features.
- **Week 13:** Testing and debugging the website.
- **Week 14:** Documentation and final submission.