**Assignment 2: E-commerce Project Implementation with Security Features and Functionality**

**GitHub Repository Link:** <https://github.com/pranjalbatra/secure_prog_ecommerce>

**YouTube Presentation Link:** <https://www.youtube.com/watch?v=dDyDanl1OTM>

Our e-commerce project has been developed to prioritize security at every level. The project is built using CodeIgniter(PHP MVC framework) and MySQL.

Below is an overview of the key security functionality implemented and threats mitigated to protect the application from various cyber-attacks like:

1. **Buffer Overflow Protection**

To prevent buffer overflow vulnerabilities, we have implemented user input validation in forms and boundary checking. Our application ensures that input data is properly sanitized and validated before being processed or stored, eliminating the risk of buffer overflow attacks.

1. **Command Injection Prevention (SQL and XSS)**

Through the use of and input validation and several inbuilt features of the framework, we ensure that user inputs are properly sanitized before interacting with the database. We implemented a custom security helper function `application/helpers/security\_helper.php` to escape strings, truncate if strings reach a certain length and remove any script or other tags. Additionally, CodeIgniter's Active Record methods automatically escapes queries to prevent SQL injection.

1. **Authentication Attack Prevention**

We have implemented the use of strong password setting rules in our project. This is essential for protection against brute-force attacks. We also hash our passwords (using md5) and add a salt to create secure hashes that cannot be decrypted easily. We have also implemented smart and efficient session handling.

1. **CSRF Protection (Cross-Site Request Forgery)**

Our application includes stringent CSRF protection mechanisms. Each request is accompanied by a unique token that is verified on the server side, mitigating the risk of unauthorized actions initiated by malicious entities.

Other Security Measures that can be implemented in the future:

* Multi-Factor Authentication (MFA) or Two-Factor Authentication (2FA) can be implemented to enhance user authentication.
* DDoS Protection: Our infrastructure can be fortified with DDoS protection mechanisms to thwart Distributed Denial of Service attacks, ensuring the availability and stability of the application even under high traffic conditions. Most cloud service providers now have this service.
* PCI DSS Compliance: Payment Card Industry Data Security Standard (PCI DSS) guidelines for securely storing and processing credit card information, ensuring customer payment data remains safe.
* SSL Certificates: Our application can enforce secure communication by utilizing SSL certificates, encrypting data transmitted between the user's browser and the server.

