A close up of a logo

AI-generated content may be incorrect.

**INDIVIDUAL ASSIGNMENT**

**LEVEL 5**

**COMP50004**

**SERVER-SIDE PROGRAMMING**

**COM2421/SENG2421**

**Hand Out Date: Week 02**

**Hand In Date: Week 13**

**INSTRUCTION TO CANDIDATES**

1. **Students are advised to underpin their answers with the use of references (cited using the Harvard Referencing Style).**
2. **Late submission will be awarded zero (0) unless extenuating circumstances (EC) are upheld.**
3. **Cases of plagiarism will be penalized.**
4. **The assignment should be submitted as a softcopy:**
   1. **The softcopy of the written assignment and source code must be uploaded to given link in the LMS.**

**LARAVEL SECURITY DOCUMENTATION**

**Table of Contents**

[Summary 3](#_Toc210401334)

[1. Vulnerabilities and their Mitigations 4](#_Toc210401335)

[1.1. SQL Injection 4](#_Toc210401336)

[1.2. Cross-Site Request Forgery (CSRF) 4](#_Toc210401337)

[1.3. Broken Authentication 5](#_Toc210401338)

[1.4. Cross‑Site Scripting (XSS) 5](#_Toc210401339)

[2. Authentication Management (Laravel Jetstream) 6](#_Toc210401340)

[3. Server-side Validation 7](#_Toc210401341)

[Github Link: 7](#_Toc210401342)

[Hosted Link: 7](#_Toc210401343)

# Summary

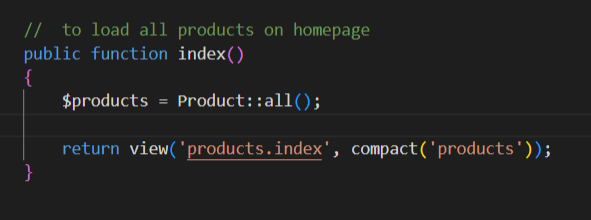
In this report I conducted an analysis and security assessment of my e-commerce website, Arcanum, which is built on Laravel, to secure the site against common web vulnerabilities. To prevent these risks, I secured these areas of the application using Laravel’s built-in security features, such as, parameterized queries, CSRF tokens, Blade’s input escaping, secure cookie attributes, and strong server-side validation. After these vulnerabilities have been secured, Arcanum remains a safe, reliable, and trustworthy digital space for collectors and shoppers.

# Vulnerabilities and their Mitigations

## SQL Injection

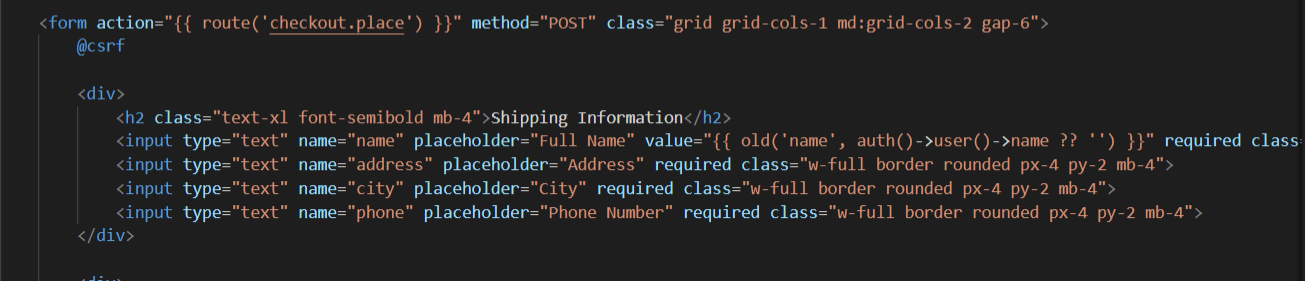
**What it does:** SQL injection happens when user input is concatenated into SQL text, allowing an attacker to change the query logic and exfiltrate or manipulate data..

**How I fixed it**: I replaced raw, interpolated SQL with parameter binding or Eloquent queries so user input is treated as data (not SQL). This prevents an attacker from injecting SQL tokens into the query.

****

## Cross-Site Request Forgery (CSRF)

CSRF (Cross-Site Request Forgery) is when a trusted user's browser is manipulated to unknowingly submit a state-changing (form, AJAX) request to your website. In Arcanum, a checkout form, adding items to a cart, or updating user profile information is an ideal scenario: if CSRF protection is not in place, an attacker could force a victim to place orders or update shipping addresses, all based on the victim's session.

**Example:  
**

## Broken Authentication

**What it does:** Storing or handling passwords in plain text (or skipping validation) exposes users to credential theft and account takeovers if the database is compromised.

**How I fixed it:** I added server-side validation for registration, and I hash passwords before saving using Laravel’s Hash::make().

A computer screen shot of a program

AI-generated content may be incorrect.

## Cross‑Site Scripting (XSS)

Cross-Site Scripting (XSS) happens when an application includes untrusted input in a web page, without proper validation or escaping, which allows an attacker to execute redundent Javascript in victims’ browsers. In Arcanu, product names, descriptions, or user-generated inputs are possible entry points. Stored XSS is particularly dangerous because the malicious code is persisted in the database, being executed whenever any user views the affected page, potentially exposing user data or manipulating the UI.

**Example:**

A screen shot of a computer code

AI-generated content may be incorrect.

# Authentication Management (Laravel Jetstream)

A screen shot of a computer code

AI-generated content may be incorrect.



# Server-side Validation

A screen shot of a computer program

AI-generated content may be incorrect.

A computer screen shot of text

AI-generated content may be incorrect.

# Github Link:

<https://github.com/nathaniel1219/Arcanum_Web>

# Hosted Link:

<https://arcanumweb-production.up.railway.app/login>