Assignment 1

Secure Programming

B00159127 Lan Ngai, B00160080 Celine Bourbon, B00166142 Nathan Lynch

Contents

[Authentication Bypass 2](#_Toc213442643)

[SQL Injection 3](#_Toc213442644)

[IDOR 4](#_Toc213442645)

[XSS 4](#_Toc213442646)

[Credential Leaking 5](#_Toc213442647)

[Password Visibility 5](#_Toc213442648)

[Shoulder Surfing 5](#_Toc213442649)

# Authentication Bypass

‘/admin\_panel’ shown in requests when clicking on the sitemap option on the website. That’s how that page was made known to me.

A screenshot of a computer

AI-generated content may be incorrect.

Adding ‘/admin\_panel’ we get access to that page.

A screenshot of a computer

AI-generated content may be incorrect.

# SQL Injection

In the login page by putting the following (‘OR 1=1 --) in both the username and password fields logs you in due to that being a statement which is always true.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

# IDOR

After that I noticed that the Url changed to <http://127.0.0.1:5000/profile/1> so I changed the number and the profile changed to that of another user.

A screenshot of a computer

AI-generated content may be incorrect.

# XSS

A screenshot of a computer

AI-generated content may be incorrect.

# Credential Leaking

# Password Visibility

# Shoulder Surfing