Assignment 3 Report

Zain Mehdi – 5630186

Task 1

Task 1

5630186 Zain Mehdi

COMP804: Web Security
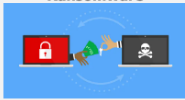
Assignment 1, due at the end of Week 5

Task 2

Task 2

Activity	Date
First day to enrol for re-enrolling (continuing students)	20 Nov 2023
First day to enrol for new students (commencing students)	04 Dec 2023
Orientation Further information click here	19 Feb - 22 Feb 2024
Lectures Commence (weeks 1-7)	26 Feb - 12 Apr 2024
Last day to enrol / add subjects yourself	08 Mar 2024
Last day to enrol / add subjects with Head of Students approval	15 Mar 2024

Task 3

Task 3

Name	Web Attacks
Malware	Malware is a term for various pieces of software that are intentionally designed to damage a computer, server, client or computer network. Malware often operates covertly, exploiting vulnerabilities in a system's security to gain unauthorized access or manipulate data. It can be distributed through various means, including email attachments, infected websites, removable storage devices, and malicious downloads. McAfee
XSS Attacks	Cross-Site Scripting (XSS) attacks, where malicious scripts are injected into trusted websites through vulnerable web applications. Attackers exploit these vulnerabilities to send harmful code to unsuspecting users' browsers, allowing them to access sensitive information like cookies and session tokens. XSS attacks pose significant risks by deceiving browsers into executing scripts from seemingly trusted sources, ultimately compromising the security of web users. owasp.org
Man in the Middle (MITM) attacks	A man-in-the-middle (MITM) attack occurs when a perpetrator intercepts communication between a user and an application to eavesdrop or impersonate one party. The aim is to steal personal information like login credentials and credit card details, often targeting users of financial apps, e-commerce sites, and other platforms requiring authentication. This stolen information can be used for identity theft, unauthorized transactions, or as part of advanced persistent threat (APT) infiltration tactics. www.imperva.com
SQL Injection	A SQL injection attack involves inserting SQL queries into client input data, enabling unauthorized access to or manipulation of a database. Successful exploitation can lead to the extraction of sensitive data, alteration of database contents, execution of administrative tasks, and even issuing commands to the operating system. These attacks exploit vulnerabilities in data input mechanisms, allowing attackers to control SQL commands executed by the application. owasp.org
Ransomware	Ransomware is a common and dangerous type of malware. It works by locking up or encrypting your files so you can no longer access them. A ransom, usually in the form of cryptocurrency, is demanded to restore access to the files. Cybercriminals might also demand a ransom to prevent data and intellectual property from being leaked or sold online. Cyber.gov.au

Task 4
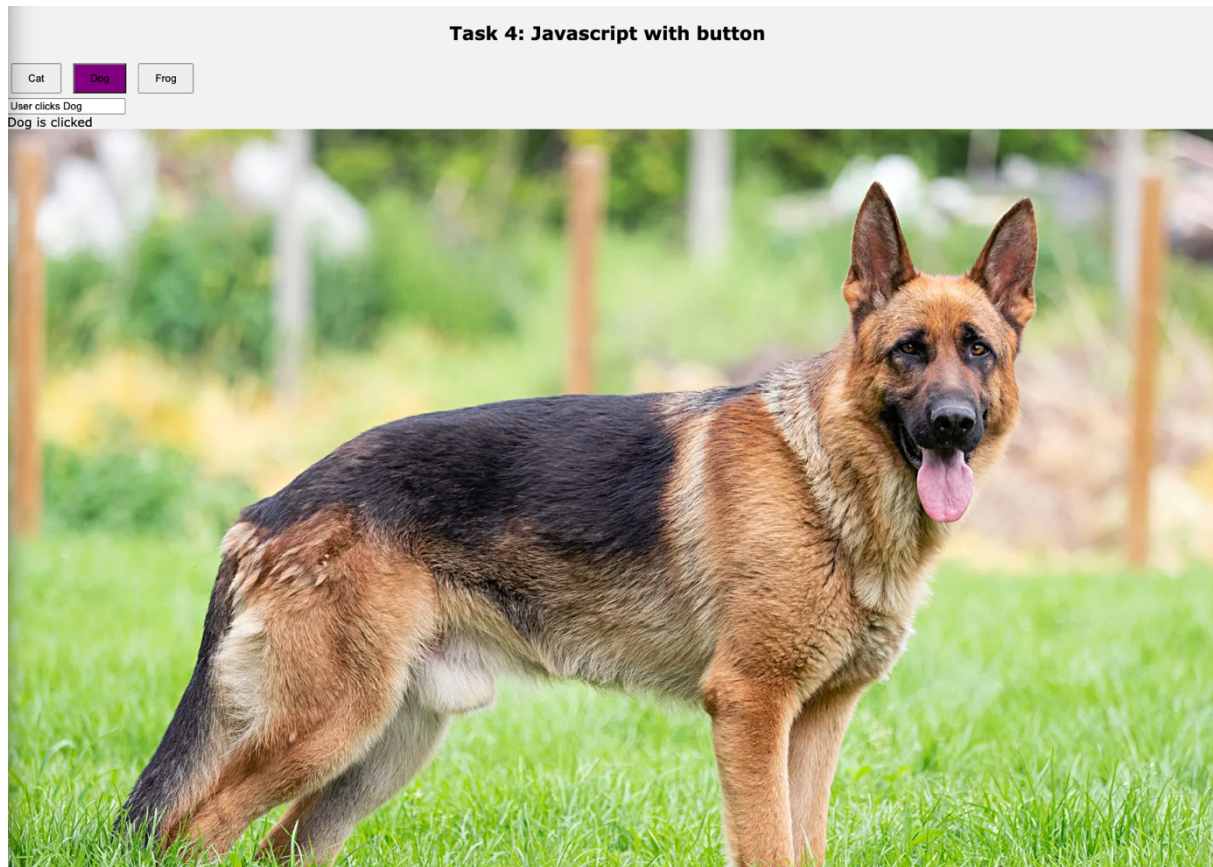
Task 5

To add the files of this assessment task to the repository the following commands were used in order.

Step 1 – git add .

Step 2 – git commit "or" git commit –m "Initial commit of HTML Assignment 3"
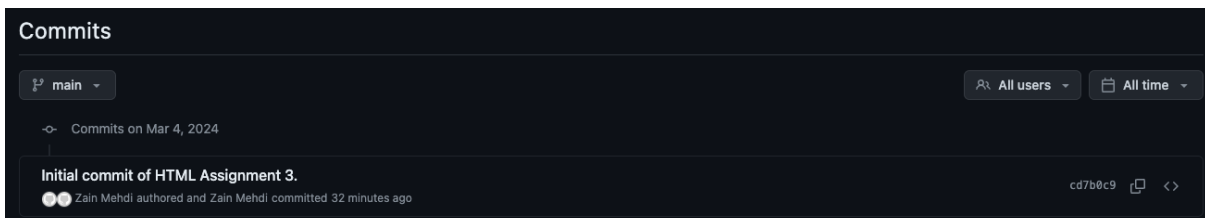
Step 4 – git push (pushes the files that have been staged to the repository)

Link to repository: https://github.com/zainsmehdi/Assignment-3