INSY7314 : Application Security by Talia

Lesson Notes

Lesson 1

Lab Notes and Module Textbook are on a GitHub repo, that will be shared by Talia.

Aims to understand common threats in cybersecurity.

Our task is to:

* Implement Security
* Attempt to break in
* Attempt to fix leaks.

POE Module

Concepts discussed in the Lesson:  
The importance of a Proxy Server.

A proxy server acts as an intermediary between a user's computer and the internet, forwarding requests and responses while potentially masking the user's IP address and enhancing security. Its importance lies in its ability to improve privacy, boost security, control web access, and potentially enhance performance.

Decreases the chance of a middleman intercepting what is being sent through the internet

The threats of untrusted data being stored on your computer:  
Can contain different types of malware, spyware and virus.

Our aim is to keep only clean data on your computer.

How does an anti-virus work?

Antivirus software works by scanning files and computer memory for known malware patterns (signatures) and also by monitoring for suspicious behavior that could indicate a new, unknown threat. It then quarantines or deletes infected files to prevent them from harming the system. Modern antivirus software also updates itself regularly to stay ahead of new malware variants.

What does HTTP stand for, and how does it drive Web Traffic?

HTTP stands for **Hypertext Transfer Protocol**. It is the foundation of data communication on the World Wide Web, enabling users to access and interact with web pages, download files, and use online applications. HTTP defines the rules for how web browsers and servers exchange messages, allowing for the transfer of information like text, images, audio, and video.

Lesson Task:  
Research the definitions provided on the slideshow, as well as how you would find and implement them.

* In basic terms:  
  Definition
* Purpose
* Security Risks
* Methods of Defence Against Security Risks.

Topics to research:  
Blacklist Input Validation VS Lack of Parameterized SQL.

My own research:

Blacklist input validation is a security method that involves identifying and rejecting known malicious or invalid input patterns.

It works by comparing user input against a predefined list of "bad" or unacceptable inputs, and any match results in the input being rejected. However, this approach is generally less effective than whitelisting because it's difficult to anticipate and block all possible malicious inputs.

A Parameterized Query, also known as a Prepared Statement, is a type of SQL statement that allows the database to execute the same or similar database queries more efficiently.

What can happen when there is a lack of Parametrized Queries?

SQL injection, also known as SQLI, is a common attack vector that uses malicious SQL code for backend database manipulation to access information that was not intended to be displayed. This information may include any number of items, including sensitive company data, user lists, or private customer details.

Class Discussion:  
What’s the difference between blacklist and whitelist validation?

Next Lesson: Practical work will start.

Mern:  
The MERN stack is a popular JavaScript-based web development framework that utilizes MongoDB, Express.js, React, and Node.js

This module will utilise VS Code.

Positive Defence Patterns:

* Query Parameterization
* Whitelisting (Strict Input Validation)
* Layered Controls (defence in depth)

Escaping: a technique used to prevent malicious code or commands from being executed when processing user input

Input Validation

Be sure to check out the Lab Guide, as it is a tutorial on what we will cover in the course of the semester.