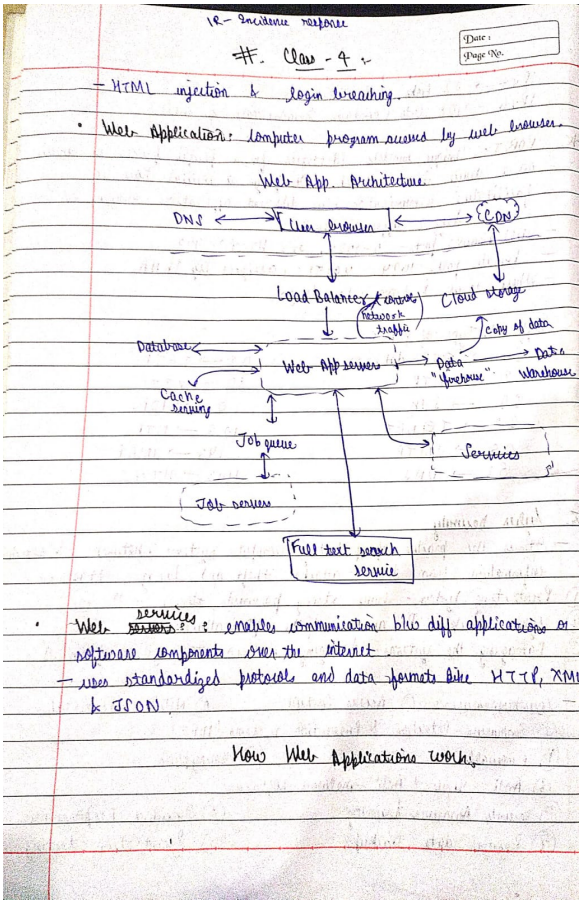
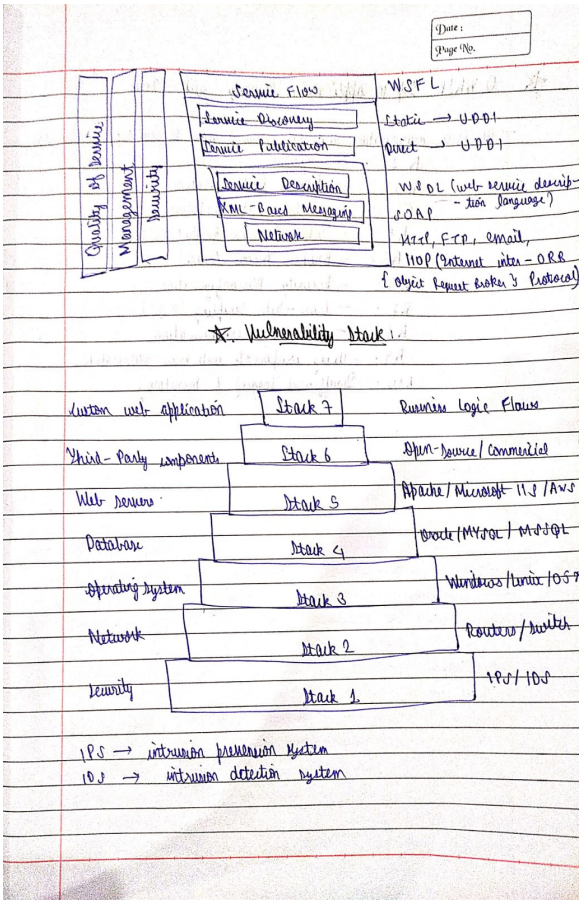
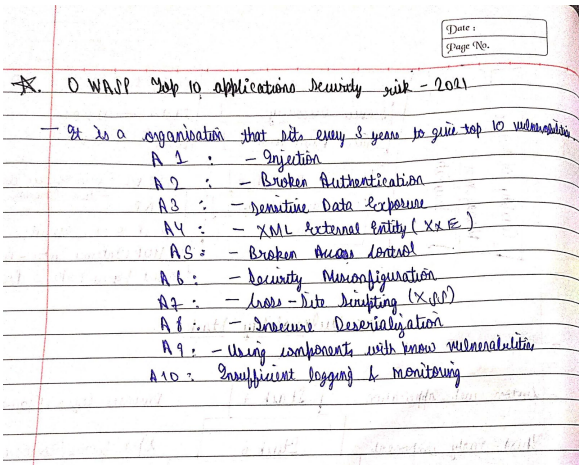
Class 4 - 25/08/2023

In this class we studied about how the web applications works, it’s architecture, the vulnerability stack and the top 10 OWASP application vulnerabilities. We also got to see the practical session of the HTML injection and the broken authentication.

Here are the ss from the short notes that i made from the lecture:







Task: Top 10 OWASP vulnerability with one cwe and it’s business impact

OWASP Vulnerability	CWE	Description	Business Impact
A01:2021-Broken Access Control	CWE-863: Incorrect Authorization	This vulnerability occurs when there is a lack of proper authorization or authentication mechanisms in place. This can allow attackers to gain unauthorized access to systems or data.	This vulnerability can have a significant impact on businesses, as it can lead to data breaches, financial losses, and reputational damage.

OWASP Vulnerability	CWE	Description	Business Impact
A02:2021-Cryptographic Failures	CWE-327: Use of Insufficiently Strong Cryptographic Algorithm	This vulnerability occurs when cryptographic algorithms or implementations are not properly implemented or configured. This can allow attackers to decrypt sensitive data or bypass security controls.	This vulnerability can have a significant impact on businesses, as it can lead to data breaches, financial losses, and compliance violations.
A03:2021-Injection	CWE-79: Improper Input Validation	This vulnerability occurs when un-validated or malicious input is passed to an application. This can allow attackers to execute arbitrary code or gain unauthorized access to systems or data.	This vulnerability can have a significant impact on businesses, as it can lead to data breaches, financial losses, and system outages.
A04:2021-Insecure Design	CWE-295: Improper Implementation of Authentication	This vulnerability occurs when security is not considered during the design of an application or system. This can lead to a variety of security flaws, such as weak authentication, insecure data storage, and inadequate access control.	This vulnerability can have a significant impact on businesses, as it can lead to data breaches, financial losses, and compliance violations.

OWASP Vulnerability	CWE	Description	Business Impact
A05:2021-Security Misconfiguration	CWE-209: Security Misconfiguration	This vulnerability occurs when security settings are not properly configured or managed. This can leave systems and data vulnerable to attack.	This vulnerability can have a significant impact on businesses, as it can lead to data breaches, financial losses, and compliance violations.
A06:2021-Vulnerable and Outdated Components	CWE-693: Use of Vulnerable Component	This vulnerability occurs when outdated or vulnerable software components are used in an application or system. These components can contain known security flaws that can be exploited by attackers.	This vulnerability can have a significant impact on businesses, as it can lead to data breaches, financial losses, and system outages.
A07:2021-Identification and Authentication Failures	CWE-362: Use of Weak or Improperly Randomized Passwords	This vulnerability occurs when there are flaws in the way that users are identified and authenticated. This can allow attackers to impersonate legitimate users and gain unauthorized access to systems or data.	This vulnerability can have a significant impact on businesses, as it can lead to data breaches, financial losses, and system outages.

OWASP Vulnerability	CWE	Description	Business Impact
A08:2021-Software and Data Integrity Failures	CWE-614: Improper Handling of Sensitive Data	This vulnerability occurs when there are flaws in the way that software or data is protected from unauthorized modification. This can allow attackers to tamper with software or data, which can have a negative impact on the integrity of the system or data.	This vulnerability can have a significant impact on businesses, as it can lead to financial losses, compliance violations, and loss of customer trust.
A09:2021-Security Logging and Monitoring Failures	CWE-793: Failure to Implement Security Logging	This vulnerability occurs when there are flaws in the way that security logs are collected, stored, or analyzed. This can make it difficult to detect and respond to security incidents.	This vulnerability can have a significant impact on businesses, as it can make it difficult to identify and respond to security incidents, which can lead to data breaches, financial losses, and system outages.
A10:2021-Server-Side Request Forgery	CWE-911: Improper Input Validation for Security-Critical Input	This vulnerability occurs when an attacker can trick a server into executing unintended actions by submitting malicious requests.	This vulnerability can have a significant impact on businesses, as it can be used to steal data, make unauthorized changes to systems, or launch denial-of-service attacks.