Assignment 3.

1. What are the key lessons you learned about web application security, and how do they relate to the CIA Triad?

   --Input validation and sanitization: Need to validate and sanitize user inputs to prevent injection attacks such as SQL injection and Cross site scripting. Unchecked inputs can allow attackers to manipulate queries and execute malicious code.
   The above can protect Integrity by ensuring data and application logic remain unaltered and unauthorized input. Can maintain Confidentiality by preventing unauthorized access.

   --Authorization and authentication : Need of implementing strong authentication mechanisms such as multi-factor auth and enforce strict authorization policies such that only the required user are able to access the required data . Restrict access to sensitive contents where maintaining Confidentiality. Integrity by preventing unauthorized modifications.

   --Encryption of data: Learnt about use of SSL/TLS protocol to encrypt and decrypt data so that data remain confidential and integrity is maintained throughout the data exchange process.

   --Rate limiting: This ensures that resources that are present on the web is available all the time to the intended users. DDOS can be mitigated. Availability can be maintained from this.

2. How do vulnerabilities and exploits affect web applications, and how can you defend against these attacks?

   -Vulnerabilities are nothing but weakness in one system. These can be exploited so that attackers can gain access to the system. This can be understanded by using a live example of SQL injection. Here SQL injection is type of attack where, attackers can run the SQL commands from the input form to get unauthorized access of data. Here the vulnerability is not doing input validation, which can be exploited. These lead to manipulation of databases, so that it may hamper the system working. It can be mitigated by the input validation and sanitization and using stored procedures. There are other attacks that can be done on vulnerabilities that may hamper the work of web application. We need to look over all these attacks and try to mitigate those as early as possible based on CSVV

3. What role do different layers (client, server, database, etc.) play in web security, and what specific threats exist at each layer?

   --Each layer is associated with different security issues
   Client: It handles the user interaction, input validation. Threats associated with are Cross site scripting, cross site request forgery. We need to mitigate these threat by input sanitization and introducing CSRF tokens. One more thing is adapting content security policy with restrict sources of executable scripts.

Server: The place where the clients request is got processed, enforces business logic and interact with database. Some of the threats involved here are Injection attacks(one of the common is SQL INJECTION), broken authentication, misconfiguration of server, and weak policies. These can mitigated by incorporating stored procedures in SQL, server side input validation, giving least privilege to the users and incorporating the firewalls.

Database layer: The client information , server configurations are stored in database. Most of the data stored here is sensitive data. The threats involved here are , excessive permission, data leaks, database failure, storing data in public cloud. The mitigation steps are , role-based access control so that only the legitimate user with high privilege only can access the data along with adapting RAID technology to avoid the data loss.

Network: It creates the bridge between all other entities such as client server and database. Threats such as Man in the middle, DDOS, and open ports where , discovery of those ports can lead to the REC. These can mitigated by using TLS/SSL protocol in network for communication which encrypt the data. Along with adding rules to firewall to avoid unnecessary connection with unknow users.

4. Discuss how web application security can fail in terms of configuration, policy, or assumptions. Provide an example you've learned about.
   -- By taking the example of Playstation attack 2011 ,

   - Configuration Failures
     • Out-of-date software: Failing to apply security patches or keep infrastructure up to date can leave known vulnerabilities exploitable.
     • Misconfigured servers: Incorrectly set permissions, unprotected endpoints, or overly broad network access controls can give adversaries a foothold.
     • Exposed administrative tools: Tools intended only for internal use may unintentionally be left accessible over the public internet
   - Policy Failures
     • Lax data storage and encryption policies: Storing sensitive user data without robust encryption or hashing (e.g., storing passwords as plain text) opens the door to massive breaches once attackers gain access.
     • Insufficient logging/monitoring: Without proper logging, detecting intrusions or unauthorized data access becomes more difficult, prolonging the time attackers spend inside the system.
     • Lack of incident response plans: Organizations with weak or no formal incident response experience delays in containing an active breach, escalating its impact.
   - Incorrect Assumptions
     • Overreliance on perimeter defenses: Assuming that "firewalls" alone or other network barriers will keep attackers out, without preparing for what happens if internal controls are bypassed.

• Trust in third parties or legacy integrations: If components or third-party services are not audited and hardened, attackers can find overlooked vulnerabilities through those connections.

• Underestimating attackers' capabilities: Organizations might assume they are too small or not significant enough to be targeted, failing to keep defenses current and robust.

5. How do you think about risk and impact when evaluating web application security?
   - ■ Defining Risk in Context

     • Threat Modeling: Identify possible attack vectors and threat actors, then evaluate which systems and data they are most likely to target. Assess what protections exist to mitigate or prevent these attacks.

     • Vulnerability Assessments and Pen Tests: Regular scanning for known vulnerabilities and periodic penetration tests help you find weak points. Aligning discovered vulnerabilities with business context and potential attacks gives you a clearer picture of the risk landscape.
   - ■ Understanding Impact

     • Data Sensitivity: The impact of a breach or attack that compromises personal information, financial records, or proprietary data is higher than that of a system exposing only nonsensitive logs. Data classification (e.g., confidential, restricted, public) can help you determine impact.

     • Confidentiality, Integrity, Availability: Consider these three pillars (often referred to as the CIA triad). A breach of confidentiality (e.g., stolen personal data), integrity (tampering with code or data), or availability (denial of service) can each have unique and significant impacts on the business and its users.

     • Reputational Damage: Beyond direct loss (e.g., stolen funds or intellectual property), organizations risk losing customer trust and brand value. Once consumer faith is shaken, it can be difficult and expensive to rebuild.

     • Regulatory Consequences: Depending on the region and industry, a data breach that exposes personal or financial data can lead to fines or legal action (e.g., GDPR, CCPA, PCI DSS). The severity of consequences often depends on the volume and type of data compromised.
6. What prevention strategies have you found most effective.?
   - ■ Fixing misconfigured config files
   - ■ Adding rating limiter to the websites
   - ■ Following OWSAP principles of development
   - ■ Try to reducing attack vectors