Assignment

Case study —

1) Importance of incident response planning (IRP) in mitigating incidents and trust

Ans)

(i) Incident Categorization : Determine the severity and nature of the breach; based on impact, type of data compromized and potential consequences.

(ii) Detection : Rapid detection is crucial to minimize damage

(iii) Legal / Regulatory Considerations

(iv) Mitigating Incidents

(v) Maintaining State holder's Trust

(vi) Compliance Requirements

2) The exploitation of vulnerabilities such as SQL injection and cross-site scripting (XSS)

① SQL injection (SQLi)

- It involves probing web applications for vulnerabilities that allow malicious SQL code to be injected into a dbs query.
- Use of automated tools like SQL map or manual techniques to identify input fields susceptible.
- Once a vulnerable input field is identified, ethical hackers attempt to manipulate the input SQL commands or leak sensitive data from db.

(II)

- Cross - Site Scripting (XSS) - Focus on identify web applications susceptible to malicious script injection.
- Search for input fields, such as search bars or comment sections, where user - supplied data is reflected back to other users without proper sanitization.
- Using tools like Burp suite
- The injected scripts may be designed to steal session cookies, redirect users to malicious websites.
- To perform unauthorized actions or compromise user accounts.

3) Privilege escalation - is a hacking technique where an attacker exploits vulnerabilies or misconfigurations in a system to gain higher levels of access or privileges than originally intended.

(I) Implications —

- Increased Access
- Persistence
- Data Theft
- System Compromise

(II) Preventive Measures —

- Regular Patching
- Least Privilege Principle
- Authentication
- Access Controls
- Monitoring and Logging
- Security Awareness Training