VAPT SCENARIO BASED QUESTIONS & ANSWERS

BY IZZMIER IZZUDDIN

1. **You are performing a penetration test for a financial institution and notice unauthorized access attempts on their database. How would you proceed?**

I would first validate the unauthorized access attempts to ensure they are not false positives. Next, I would document the details, including the IP addresses, times, and any patterns observed. I would notify the client immediately about the potential security breach. After that, I would investigate the extent of the breach, how the attacker might have gained access, and what data could be at risk. I would also provide recommendations for immediate containment and mitigation, such as blocking suspicious IPs, reviewing and updating access controls, and applying necessary patches.

2. **During a vulnerability assessment for a healthcare provider, you discover a critical vulnerability in their patient records system. What steps would you take to address this?**

Upon discovering the critical vulnerability, my first step would be to validate and confirm its existence and severity. I would then document the findings with detailed information about the vulnerability, including the potential impact and exploitation methods. I would inform the client immediately, providing them with a clear understanding of the risk. Next, I would work with their IT and security teams to prioritize and implement the necessary patches or security measures. Additionally, I would recommend a review of their security policies and procedures to prevent future vulnerabilities and ensure compliance with healthcare regulations.

3. **You are given a tight deadline to perform a penetration test on a retail company's e-commerce platform. How would you ensure the assessment is thorough within the limited time frame?**

Given the limited time frame, I would start by conducting a risk-based assessment to prioritize the most critical assets and components of the e-commerce platform. I would focus on high-risk areas such as payment processing, customer data handling, and authentication mechanisms. Using automated scanning tools, I would quickly identify common vulnerabilities and then perform manual testing on the high-risk areas to uncover more complex issues. Throughout the process, I would maintain clear communication with the client to keep them informed of the progress and any critical findings that need immediate attention. Finally, I would provide a detailed report with prioritized recommendations for remediation.

4. **During a vulnerability assessment, your automated scanning tool reports multiple vulnerabilities. How would you handle potential false positives?**

To handle potential false positives, I would first cross-check the automated scan results with manual testing methods to verify the vulnerabilities. This involves using different tools and techniques to replicate the reported issues. I would also review the scan configuration and adjust the sensitivity settings if necessary. For each identified vulnerability, I would gather additional evidence such as logs, screenshots, and network traffic analysis to confirm its validity. By combining automated and manual approaches, I can ensure accurate results and provide the client with a reliable assessment report.

5. **You are conducting a phishing simulation for a government agency. How would you design the simulation and measure its effectiveness?**

To design an effective phishing simulation, I would start by understanding the agency's structure, typical email communication patterns, and common threats they face. I would create realistic phishing emails that mimic legitimate communication the employees might receive. These emails could include links to fake login pages or attachments that prompt users to provide sensitive information.

I would then deploy the simulation in phases, targeting different departments and tracking the response rates. Metrics such as the number of employees who clicked the link, provided credentials, or reported the phishing email would be collected.

Post-simulation, I would analyse the data to identify trends and areas of weakness. I would provide a detailed report to the agency, highlighting the findings and recommending targeted training and awareness programs to improve their resilience against phishing attacks. The effectiveness of the simulation would be measured by the reduction in susceptibility rates over time and the increased reporting of phishing attempts by employees.

6. **You have discovered an SQL injection vulnerability in the financial institution's web application. What are your immediate steps?**

Upon discovering an SQL injection vulnerability, my immediate steps would include:

- Validating the vulnerability to confirm its existence and the risk level.
- Documenting the details of the vulnerability, including how it can be exploited and the potential impact.
- Notifying the client immediately about the discovery and its potential implications.
- Recommending immediate mitigation steps, such as applying web application firewall (WAF) rules to block the malicious queries and updating the application's code to use parameterized queries or prepared statements to prevent SQL injection.

7. **What would be your approach to assessing the risk and potential impact of this SQL injection vulnerability on the financial institution?**

To assess the risk and potential impact of the SQL injection vulnerability:

- Determine the level of access an attacker could gain through the vulnerability (e.g., reading data, modifying data, or gaining administrative control).
- Evaluate the sensitivity of the data that could be exposed or altered.

- Analyse the potential business and reputational impact on the financial institution if the vulnerability were to be exploited.
- Assess the complexity of exploiting the vulnerability and the likelihood of it being discovered by attackers.

8. **How would you help the financial institution mitigate and remediate the discovered SQL injection vulnerability?**

To mitigate and remediate the SQL injection vulnerability:

- Work with the development team to implement secure coding practices, such as using parameterized queries or prepared statements.
- Apply necessary patches or updates to the affected web application.
- Conduct thorough testing to ensure the vulnerability is fully resolved.
- Recommend regular security training for developers to prevent similar issues in the future.
- Suggest implementing additional security measures, such as a web application firewall (WAF) and regular security assessments.

9. **Can you describe the process you follow for conducting a vulnerability assessment on a web application?**

The process for conducting a vulnerability assessment on a web application includes:

- Planning and scoping the assessment to understand the application's architecture, technologies used, and critical components.
- Conducting reconnaissance to gather information about the application and its environment.
- Using automated scanning tools to identify common vulnerabilities.
- Performing manual testing to validate findings from automated scans and to discover more complex vulnerabilities.
- Documenting the findings with detailed descriptions, evidence, and potential impact.
- Providing recommendations for remediation and working with the client to address the vulnerabilities.
- Conducting a follow-up assessment to verify that the issues have been resolved.

10. **How do you keep yourself updated with the latest security vulnerabilities and exploits?**

To stay updated with the latest security vulnerabilities and exploits:

- Regularly read security blogs, forums, and websites such as OWASP, SANS, and the National Vulnerability Database (NVD).
- Follow security researchers and experts on social media platforms like Twitter and LinkedIn.
- Participate in security conferences, webinars, and workshops.
- Subscribe to vulnerability and threat intelligence feeds.

- Engage with the security community through online forums and discussion groups.
- Continuously practice and experiment with new tools and techniques in lab environments.

11. **You've identified a critical vulnerability in a client's network during a penetration test. How would you communicate this to the client?**

To communicate a critical vulnerability to the client:

- Prepare a clear and concise report detailing the vulnerability, including its description, impact, and potential exploitation methods.
- Schedule a meeting with the client's key stakeholders to discuss the findings.
- Present the vulnerability in a way that is understandable to both technical and non-technical audiences.
- Explain the immediate risks and potential consequences of not addressing the vulnerability.
- Provide recommendations for immediate mitigation and long-term remediation.
- Offer to assist with the remediation process and conduct a follow-up assessment to ensure the issue is resolved.

12. **Describe a time when you had to handle a difficult client. How did you manage the situation?**

To handle a difficult client:

- Maintain professionalism and stay calm, even if the client is upset or uncooperative.
- Listen actively to understand the client's concerns and perspective.
- Communicate clearly and provide regular updates on the progress of the project.
- Set realistic expectations and deliver on promises.
- Find common ground and offer solutions that address the client's concerns.
- Document all communications and agreements to avoid misunderstandings.
- Escalate the issue to higher management if necessary, while continuing to work towards a resolution.

13. **Imagine you are performing a penetration test on a client's network, and during the testing, you accidentally cause a disruption to a critical service. How would you handle this situation?**

If a disruption to a critical service occurs during a penetration test:

- Immediately stop the testing and assess the situation.
- Inform the client about the disruption as soon as possible.
- Work with the client's IT team to identify the cause and restore the affected service.
- Document the incident, including the steps taken and lessons learned.

- Review and update the testing procedures to prevent similar incidents in the future.
- Offer to assist with any additional remediation or compensatory measures.

14. **You are conducting a penetration test for a client, and you discover a zero-day vulnerability in their web application that has the potential to be exploited by attackers. How would you proceed with this information?**

Upon discovering a zero-day vulnerability:

- Validate and document the vulnerability with detailed evidence and potential impact.
- Immediately inform the client about the critical nature of the vulnerability and the potential risks.
- Recommend immediate actions to mitigate the risk, such as applying temporary workarounds or disabling affected components.
- Collaborate with the client to report the zero-day vulnerability to the appropriate vendors or security organizations for a patch or fix.
- Provide ongoing support and monitoring until a permanent solution is implemented.

15. **During a penetration test, you use Nessus to scan a client's network and identify several critical vulnerabilities. What steps would you take to prioritize and address these findings?**

To prioritize and address critical vulnerabilities identified by Nessus:

- Validate the vulnerabilities to confirm their existence and severity.
- Prioritize the vulnerabilities based on factors such as potential impact, ease of exploitation, and the criticality of affected systems.
- Document each vulnerability with detailed descriptions, evidence, and potential consequences.
- Develop a remediation plan in collaboration with the client's IT and security teams, prioritizing the most critical issues.
- Provide recommendations for immediate mitigation, such as applying patches, reconfiguring settings, or implementing compensating controls.
- Conduct a follow-up assessment to ensure that the vulnerabilities have been effectively addressed.

16. **You are tasked with performing a web application security test using Burp Suite**. **You discover a SQL injection vulnerability. How would you verify this finding and what recommendations would you provide to the client?**

    To verify a SQL injection vulnerability found using Burp Suite, I would perform manual testing to confirm it and recommend using parameterized queries and input validation to the client.

17. **While using Metasploit, you successfully exploit a vulnerability on a client's server, gaining access to sensitive data. What are your next steps to ensure the client understands the severity and takes appropriate action?**

    After exploiting a vulnerability and gaining access to sensitive data with Metasploit, I would document the findings, explain the severity to the client, and provide recommendations for securing the system.

18. **In a mobile application security assessment using OWASP ZAP, you find that the application is vulnerable to an insecure data storage issue. How would you demonstrate the impact of this vulnerability to the client?**

    To demonstrate the impact of an insecure data storage issue in a mobile app, I would show how sensitive data can be accessed and advise the client on secure storage practices.

19. **After conducting a configuration review of a client's firewall using KALI Linux tools, you discover several misconfigurations. What process would you follow to communicate these issues and assist the client in remediation?**

    Upon discovering firewall misconfigurations, I would communicate the issues clearly, prioritize them based on risk, and assist the client in applying necessary configuration changes.

20. **Using Netsparker, you identify cross-site scripting (XSS) vulnerabilities in a client's web application. How would you approach testing for and confirming these vulnerabilities, and what steps would you recommend for remediation?**

    For cross-site scripting (XSS) vulnerabilities found using Netsparker, I would validate them through manual testing, explain the risk to the client, and recommend proper input sanitization and output encoding.

21. **During a source code review using automated tools and manual inspection, you identify hardcoded credentials in a client's application. What would be your process for reporting and addressing this issue with the development team?**

    When identifying hardcoded credentials in a client’s application, I would report the issue to the development team, suggest removing the credentials from the code, and implementing secure credential management.

22. **You are conducting a thick-client application penetration test and use Wireshark to capture traffic, revealing unencrypted sensitive information. How would you present these findings to the client and recommend improvements?**

    Upon capturing unencrypted sensitive information with Wireshark, I would present the findings to the client and recommend encrypting data transmissions to enhance security.

23. **While reviewing database configurations using DB auditing tools, you discover that several critical databases are missing security patches. How would you prioritize these findings and work with the client to ensure timely patching?**

    For missing security patches in critical databases, I would prioritize based on the risk level, inform the client of the urgency, and work with them to ensure timely patching.

24. **Using Threat Intelligence platforms, you identify that a client's network is being targeted by a newly discovered exploit. How would you incorporate this information into your penetration testing activities and advise the client on mitigating the risk?**

    Incorporating threat intelligence about a new exploit targeting a client's network, I would update the penetration testing strategy and provide actionable recommendations to mitigate the risk.

25. **You are using Nessus to scan a client's network and identify several high-risk vulnerabilities. What would be your approach to validate and prioritize these findings?**

    To validate and prioritize high-risk vulnerabilities found using Nessus, I would confirm them with manual testing, assess their impact, and develop a remediation plan with the client.

26. **During a web application test with Burp Suite, you find a potential SQL injection vulnerability. How would you confirm this vulnerability and demonstrate its impact to the client?**

    To confirm a potential SQL injection vulnerability found during a Burp Suite scan, I would manually test it, demonstrate its impact to the client, and recommend secure coding practices to prevent it.

27. **While conducting a penetration test using Metasploit, you gain unauthorized access to a client's server. What are your next steps to document this finding and communicate the risk to the client?**

    After gaining unauthorized access to a client's server using Metasploit, I would document the incident, inform the client immediately, and discuss the necessary steps to secure their server.

28. **Using OWASP ZAP, you discover a critical cross-site scripting (XSS) vulnerability in a client's web application. How would you validate this vulnerability and advise the client on fixing it?**

    To validate a critical XSS vulnerability discovered using OWASP ZAP, I would perform manual testing, explain the potential risks to the client, and advise on remediation measures such as input sanitization.

29. **You are performing a configuration review of a client's firewall with** KALI Linux **tools and find several security misconfigurations. How would you prioritize these issues and recommend remediation steps?**

    For security misconfigurations found during a firewall review with KALI Linux tools, I would prioritize based on severity and work with the client to apply the recommended security settings.

30. **While assessing a mobile application with MobSF (Mobile Security Framework), you find that sensitive data is stored insecurely. How would you demonstrate the risk and advise the client on secure storage practices?**

    Demonstrating insecure data storage in a mobile application, I would show how sensitive data can be accessed, highlighting the risk, and advise the client on secure data storage practices.

31. **During a source code review with SonarQube, you identify hardcoded credentials in a client's application code. What process would you follow to report this finding and help the development team address it?**

    Upon identifying hardcoded credentials with SonarQube, I would report the issue to the client, suggest removing credentials from the code, and implementing secure credential management solutions.

32. **Using Wireshark during a thick-client application test, you capture unencrypted sensitive information being transmitted. How would you present these findings to the client and recommend mitigation strategies?**

    After capturing unencrypted sensitive information during a thick-client application test with Wireshark, I would present the findings and recommend encrypting data in transit to the client.

33. **After reviewing a client's database configuration with DB auditing tools, you find that critical security patches are missing. How would you address this issue with the client to ensure timely patching?**

    Addressing missing security patches in database configurations, I would prioritize based on risk, communicate the urgency to the client, and assist with timely patching.

34. **You receive threat intelligence indicating that a client's network is being targeted by a newly discovered exploit. How would you incorporate this information into your VAPT activities and provide actionable recommendations to the client?**

    When receiving threat intelligence about a new exploit targeting a client’s network, I would integrate this information into VAPT activities and provide actionable recommendations to mitigate the threat.

35. **You have identified a critical SQL injection vulnerability in the client's web application using Burp Suite. Can you describe the steps you would take to validate this finding, assess its impact, and communicate your results to the client?**

    To validate a critical SQL injection vulnerability identified using Burp Suite, I would manually test it, assess its impact, and clearly communicate the findings and remediation steps to the client.