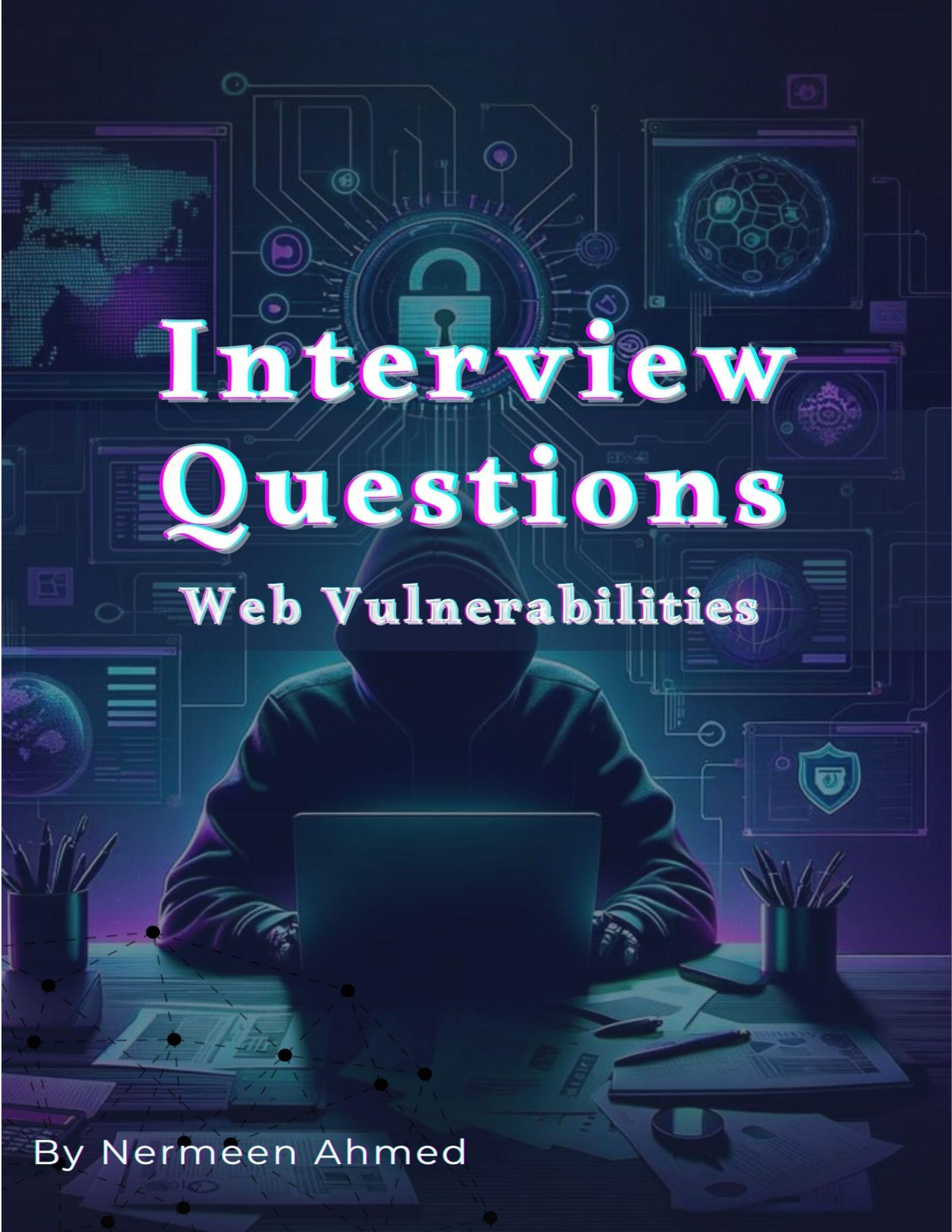

Interview Questions

Web Vulnerabilities

By Nermeen Ahmed

Red Team Awareness Report: Web Vulnerabilities

Author: Nermeen Ahmed Sonbol

____

Table of Contents

1. Introduction

As organizations continue to strengthen their defenses, Red Team professionals are expected not only to understand web vulnerabilities but also to communicate, report, and demonstrate their knowledge effectively in interviews.

This report is designed as a **practical awareness and preparation guide**, combining theoretical knowledge of web application security with structured interview-style questions and detailed guidance.

The aim is to help aspiring Red Teamers confidently explain concepts, demonstrate methodology, and showcase professional communication skills — all within an ethical and responsible framework

2 Red Team Interview Preparation: Questions & Detailed Guidance

A. Conceptual and Fundamental Questions

1. What is the core difference between a Red Team and a Blue Team?

- Guidance: Emphasize objectives. Red Team is offensive, simulating real-world adversaries to test defenses. Blue Team is defensive, focused on monitoring, detection, and incident response. Highlight that both are collaborative, working towards the same goal of improving security.

2. Can you explain the OWASP Top 10? Name a few.

- Guidance: Demonstrate broad knowledge. It's a consensus document listing the ten most critical web application security risks. Be prepared to name and briefly explain 5-7, such as Injection (A01), Broken Authentication (A02), Sensitive Data Exposure (A03), XXE (A05), Security Misconfigurations (A06), and XSS (A03:2021).

3. What is the purpose of penetration testing?

- Guidance: Focus on the business value. The purpose is to proactively identify and remediate security weaknesses before a malicious attacker can exploit them. It's about risk management and validating security controls.

4. How do you ensure you stay ethical during a test?

- Guidance: This is critical. Mention: Explicit Written Permission (get it in writing!), Defined Scope (what systems, what times, what techniques are allowed), Protection of Data (avoiding damage, handling any found data with extreme care), and Clear Communication with the client/Blue Team.

B. Tools and Practical Knowledge Questions

1. What tools do you use for reconnaissance?

- Guidance: Categorize your tools.
  - Passive Recon: whois, nslookup, dig, Shodan, Censys.
  - Active Scanning: Nmap (port scanning, service detection), Nikto (web server scanner), Gobuster/Dirb (directory busting).

2. Describe your approach to testing a web application.

- Guidance: Show a structured methodology.

1. Reconnaissance: Understand the application's structure, technologies.

2. Mapping (Enumeration): Spider the application, identify all endpoints, forms, parameters.

3. Vulnerability Analysis: Manually and with tools (like Burp Suite) test for the OWASP Top 10 (SQLi, XSS, CSRF, etc.).

4. Exploitation (Theoretical/Authorized): Attempt to safely demonstrate the impact of found vulnerabilities.

5. Reporting: Document findings, evidence, risk ratings, and clear remediation steps.

3. What measures do you take to protect sensitive data found during a test?

- Guidance: Stress confidentiality. Use encrypted drives for storing data, transmit findings securely, anonymize data in reports where possible, and securely delete all data after the engagement is complete and approved by the client.

C. Scenario-Based and Problem-Solving Questions

1. You discover a SQL injection vulnerability on a client's login page. What are your immediate next steps?

- Guidance: Show process, not eagerness to exploit.

1. Confirm: Ensure it's a true positive.

2. Document: Take detailed screenshots or notes of the request/response.

3. Assess Impact (Theoretically): Explain what could happen (e.g., "This could allow an attacker to bypass authentication"), but do not perform extensive exploitation unless it's within the agreed ROE.

4. Report: Include it in your report with clear steps to reproduce and mitigate.

2. During a scan, you find a server with ports 22 (SSH), 80 (HTTP), and 443 (HTTPS) open. How do you assess this?

- Guidance: Show prioritization. Check the web services (80/443) first as they are often the most exposed. Use a browser and tools like Burp Suite. For SSH (22), check if it's using weak passwords or vulnerable versions (within the scope of the test). Mention that finding open ports is just the first step; the service and its configuration determine the risk.

3. If you find multiple vulnerabilities, how do you prioritize them for reporting?

- Guidance: Use a risk-based approach. Prioritize based on Impact (what an attacker could achieve) and Exploitability (how easy it is to exploit). A critical RCE is higher priority than a low-impact informational disclosure. This shows you think like a security professional managing risk.

D. Soft Skills and Reporting Questions

1. How do you document your findings?

- Guidance: Describe a clear structure. A good finding includes: Title, Vulnerability Type, CVSS Score, Description, Proof of Concept (Steps to Reproduce), Impact, and Remediation Recommendations. Clarity and reproducibility are key.

2. How would you explain a technical vulnerability like XSS to a non-technical manager?

- Guidance: Use an analogy. "Imagine our website's comment section is a public whiteboard. An XSS vulnerability is like someone being able to write instructions on that whiteboard that automatically force anyone who reads it to hand over their keys (session cookies). We fix it by ensuring only plain text, not executable instructions, can be written."

3. Describe a time you had to work effectively with a Blue Team. What was the key to success?

- Guidance: Even if inexperienced, describe the ideal approach. Emphasize communication, transparency, and a shared goal. The key is to be a partner, not an adversary. Sharing timely, actionable intelligence from the Red Team helps the Blue Team improve their defenses.

3. Conclusion

Mastering technical skills is only one part of becoming an effective Red Team professional. The ability to clearly explain vulnerabilities, prioritize risks, and collaborate with Blue Teams is equally important — especially in interview settings.
By preparing with structured questions and real-world scenarios, professionals can demonstrate not just their knowledge of web vulnerabilities but also their problem-solving mindset and ethical approach.
This blend of technical and soft skills is what truly defines readiness for a Red Team role.

4. References / Resources

1. **OWASP Foundation:** https://owasp.org/ (Especially the OWASP Top 10, Testing Guide, and Cheat Sheets)

2. **PortSwigger Web Security Academy:** https://portswigger.net/web-security (Free, excellent learning resource)

3. **NIST Cybersecurity Framework & Guidelines**

4. **SANS Institute Reading Room** (Whitepapers on various security topics)

5. **Hack The Box / TryHackMe** (Platforms for practical, ethical skill development in controlled environments)