1. Introduction
2. HTML basics
3. Web app working
4. Diff between static and dynamic...
5. COOKIES, PORT, cache & SSH
6. Nmap scripting
7. Best Addons For Web Pentest
8. Dirbuster
9. Web server fingerprinting
10. Session Management
11. Encoding schemes
12. Open redirect Vulnerability
13. Same Origin Policy and Cross...
14. Burp Suite Notes
15. Burp suite vulnerabilities
16. W2021 owasp and testing.docx
17. Portswigger all labs links
18. SQL injection
19. CSRF
20. Cross site scripting XSS
21.Dom Based XSS
22.File upload Vulnerability
23. SSRF (Server Side Request Forgery
24. Cross site Port Attack
25. IDOR (Insecure Direct Object References)
26. XML External Entity
27. Insecure Deserialization.
28. Server Side Template Injection-
29. HTTP Request Smuggling.
30. OS Command Injection.
31. Clickjacking.
32. CORS
33. XXE
34. Directory traversal
35. Access control vulnerabilities
36. Broken Authentication
37. WebSockets
38. Web cache poisoning
39. Insecure deserialization-
40. Information disclosure
41. Business logic vulnerabilities
42. HTTP Host header attacks
43. OAuth authentication
44. JWT
45.common vulnerability
46.recent vulnerability
47.log4j vulnerability
48.osint,shodan.io

50.server side injection
51.heartbleed vulnerability
52.host header attack
53.misconfigurations
54.same origin resource sharing
55.Dos mitigation,DOS and DDOS and its prevention
56.buffer overflow
57.shellshock vulnerability
58.insufficient logging and monitoring
59.IDOR
59.layewise attack
60.important port
61.man in the middle attack
62.unvalidated redirect & forward
63.windows privilege escalation
64.Exploiting wordpress sites
65.phishing with ngrok
66.phishing with 2fa
67.Data tampering
68.Fuzzing technology
69.HTTP request smuggling (primary and common)
70.Prototype pollution