**HACKING PROJECT**

**By Brijesh Rakhsiya & Om Choksi**

1. **Types Of Webattacks**

Here is a list of various types of cyber attacks:

1. SQL Injection (SQLi): Attackers inject malicious SQL code into input fields to manipulate databases and gain unauthorized access to data.

2. Cross-Site Scripting (XSS): Attackers inject malicious scripts into web pages viewed by other users, which can steal information or perform actions on behalf of the victim.

3. Cross-Site Request Forgery (CSRF):Attackers trick users into unknowingly submitting malicious requests, often by embedding them in a link or image.

4. Denial of Service (DoS) and Distributed Denial of Service (DDoS): Attackers overwhelm a website or server with a flood of traffic, rendering it inaccessible to legitimate users.

5. Man-in-the-Middle (MitM): Attackers intercept communication between two parties, often to eavesdrop or manipulate the data being transmitted.

6. Phishing: Attackers use fake websites or emails to trick users into providing sensitive information, such as login credentials or financial details.

7. Brute Force Attacks: Attackers attempt to guess passwords or authentication tokens by trying different combinations until the correct one is found.

8. Clickjacking: Attackers trick users into clicking on a hidden or disguised malicious link, often by overlaying it on top of a legitimate web page.

9. File Inclusion: Attackers exploit vulnerabilities to include malicious files, such as scripts or executables, into a web page.

10. DNS Spoofing: Attackers manipulate DNS records to redirect users to malicious websites without their knowledge.

11. Drive-by-Download: Malware is downloaded onto a user's device without their consent, often by visiting a compromised website.

12. Session Hijacking: Attackers steal a user's session token to impersonate them and gain unauthorized access to their account.

13. Malware: Malicious software that infects a user's device to steal data, disrupt operations, or gain unauthorized access.

14. Ransomware: Malware that encrypts a user's files and demands a ransom for their release.

15. Zero-Day Exploit: Attackers exploit a vulnerability that is not known to the software developer, giving them a "zero-day" advantage.

16. Social Engineering: Attackers manipulate people into divulging confidential information, such as passwords or financial information.

17. Watering Hole Attack: Attackers infect websites that are likely to be visited by their target audience, exploiting the trust users have in those sites.

18. Eavesdropping: Attackers intercept and listen to communication between two parties, often to steal sensitive information.

19. Spoofing:\* Attackers impersonate a legitimate entity to deceive users, often used in phishing or man-in-the-middle attacks.

20. Insider Threat: Attacks or data breaches initiated by individuals within an organization, either maliciously or unintentionally.

**2)100 web vulnerabilities, categorized into various types:**

**Injection Vulnerabilities:**

1. SQL Injection (SQLi)

2. Cross-Site Scripting (XSS)

3. Cross-Site Request Forgery (CSRF)

4. Remote Code Execution (RCE)

5. Command Injection

6. XML Injection

7. LDAP Injection

8. XPath Injection

9. HTML Injection

10. Server-Side Includes (SSI) Injection

11. OS Command Injection

12. Blind SQL Injection

13. Server-Side Template Injection (SSTI)

**Broken Authentication and Session Management:**

14. Session Fixation

15. Brute Force Attack

16. Session Hijacking

17. Password Cracking

18. Weak Password Storage

19. Insecure Authentication

20. Cookie Theft

21. Credential Reuse

**Sensitive Data Exposure:**

22. Inadequate Encryption

23. Insecure Direct Object References (IDOR)

24. Data Leakage

25. Unencrypted Data Storage

26. Missing Security Headers

27. Insecure File Handling

**Security Misconfiguration:**

28. Default Passwords

29. Directory Listing

30. Unprotected API Endpoints

31. Open Ports and Services

32. Improper Access Controls

33. Information Disclosure

34. Unpatched Software

35. Misconfigured CORS

36. HTTP Security Headers Misconfiguration

**XML-Related Vulnerabilities:**

37. XML External Entity (XXE) Injection

38. XML Entity Expansion (XEE)

39. XML Bomb

**Broken Access Control:**

40. Inadequate Authorization

41. Privilege Escalation

42. Insecure Direct Object References

43. Forceful Browsing

44. Missing Function-Level Access Control

**Insecure Deserialization:**

45. Remote Code Execution via Deserialization

46. Data Tampering

47. Object Injection

**API Security Issues:**

48. Insecure API Endpoints

49. API Key Exposure

50. Lack of Rate Limiting

51. Inadequate Input Validation

**Insecure Communication:**

52. Man-in-the-Middle (MITM) Attack

53. Insufficient Transport Layer Security

54. Insecure SSL/TLS Configuration

55. Insecure Communication Protocols

**Client-Side Vulnerabilities:**

56. DOM-based XSS

57. Insecure Cross-Origin Communication

58. Browser Cache Poisoning

59. Clickjacking

60. HTML5 Security Issues

**Denial of Service (DoS):**

61. Distributed Denial of Service (DDoS)

62. Application Layer DoS

63. Resource Exhaustion

64. Slowloris Attack

65. XML Denial of Service

**Other Web Vulnerabilities:**

66. Server-Side Request Forgery (SSRF)

67. HTTP Parameter Pollution (HPP)

68. Insecure Redirects and Forwards

69. File Inclusion Vulnerabilities

70. Security Header Bypass

71. Clickjacking

72. Inadequate Session Timeout

73. Insufficient Logging and Monitoring

74. Business Logic Vulnerabilities

75. API Abuse

**Mobile Web Vulnerabilities:**

76. Insecure Data Storage on Mobile Devices

77. Insecure Data Transmission on Mobile Devices

78. Insecure Mobile API Endpoints

79. Mobile App Reverse Engineering

**IoT Web Vulnerabilities:**

80. Insecure IoT Device Management

81. Weak Authentication on IoT Devices

82. IoT Device Vulnerabilities

**Web of Things (WoT) Vulnerabilities:**

83. Unauthorized Access to Smart Homes

84. IoT Data Privacy Issues

**Authentication Bypass:**

85. Insecure "Remember Me" Functionality

86. CAPTCHA Bypass

**Server-Side Request Forgery (SSRF):**

87. Blind SSRF

88. Time-Based Blind SSRF

**Content Spoofing:**

89. MIME Sniffing

90. X-Content-Type-Options Bypass

91. Content Security Policy (CSP) Bypass

**Business Logic Flaws:**

92. Inconsistent Validation

93. Race Conditions

94. Order Processing Vulnerabilities

95. Price Manipulation

96. Account Enumeration

97. User-Based Flaws

**Zero-Day Vulnerabilities:**

98. Unknown Vulnerabilities

99. Unpatched Vulnerabilities

100. Day-Zero Exploits