- **Web Service:** A web service is an application or software that is deployed over the Internet and uses standard messaging protocols such as SOAP, UDDI, WSDL, and REST to enable communication between applications developed for different platforms.
- **Web-based Timing Attack:** A web-based timing attack is a type of side-channel attack performed by attackers to retrieve sensitive information such as passwords from web applications by measuring the response time taken by the server.
- **Web Spidering/Crawling:** Web spiders/crawlers automatically discover the hidden content and functionality by parsing HTML forms and client-side JavaScript requests and responses.
- **WS-Address Spoofing:** In a WS-address spoofing attack, an attacker sends a SOAP message containing fake WS-address information to the server. The <ReplyTo> header consists of the address of the endpoint selected by the attacker rather than the address of the web service client.
- **Web API:** Web API is an application programming interface that provides online web services to client-side apps for retrieving and updating data from multiple online sources.
- **Webhooks:** Webhooks are user-defined HTTP callback or push APIs that are raised based on events triggered, such as receiving a comment on a post or pushing code to the registry.
- **Web Shell:** A web shell is a malicious piece of code or script that is developed using server-side languages such as PHP, ASP, PERL, RUBY, and Python and are then installed on a target server.
- **Web Application Fuzz Testing:** Web application fuzz testing (fuzzing) is a black-box testing method. It is a quality checking and assurance technique used to identify coding errors and security loopholes in web applications.
- **Whitelist Validation:** Whitelist validation is an effective technique in which only the list of entities that have been approved for secured access are accepted.
- **Wi-Fi:** Wireless network (Wi-Fi) refers to WLANs based on IEEE 802.11 standard, which allows the device to access the network from anywhere within an AP range.
- **Wired Equivalent Privacy (WEP):** WEP is a security protocol defined by the 802.11b standard; it was designed to provide a wireless LAN with a level of security and privacy comparable to that of a wired LAN.
- **Wi-Fi Protected Access (WPA):** WPA is a security protocol defined by 802.11i standards; it uses a Temporal Key Integrity Protocol (TKIP) that utilizes the RC4 stream cipher encryption with 128-bit keys and 64-bit MIC integrity check to provide stronger encryption and authentication.
- **WPA2:** WPA2 is an upgrade to WPA, and it includes mandatory support for counter mode with cipher block chaining message authentication code protocol (CCMP), an AES-based encryption mode with strong security.
- **WPA3:** WPA3 is an advanced implementation of WPA2 providing trailblazing protocols and uses the AES-GCMP 256 encryption algorithm.
- **Wireless Traffic Analysis:** Wireless traffic analysis enables attackers to identify vulnerabilities and susceptible victims in a target wireless network.
- **Wireless Intrusion Prevention Systems:** Wireless intrusion prevention systems (IPSs) protect networks against wireless threats and enable administrators to detect and prevent various network attacks.
- **Wrapping Attack:** A wrapping attack is performed during the translation of the SOAP message in the TLS layer where attackers duplicate the body of the message and sends it to the server as a legitimate user.
- **Web of Trust (WOT):** Web of trust (WoT) is a trust model of PGP, OpenPGP, and GnuPG systems.

X

- **Xmas Scan:** Xmas scan is a type of inverse TCP scanning technique with the FIN, URG, and PUSH flags set to send a TCP frame to a remote device.
- **XML External Entity Attack:** XML External Entity attack is a server-side request forgery (SSRF) attack that can occur when a misconfigured XML parser allows applications to parse XML input from an unreliable source.

Y

- **Yagi Antenna:** A Yagi antenna, also called Yagi–Uda antenna, is a unidirectional antenna commonly used in communications at a frequency band of 10 MHz to VHF and UHF.
- **YAK:** YAK is a public-key-based Authenticated Key Exchange (AKE) protocol.

Z

- **Zero-trust Principles:** Zero-trust principles constitute a set of standardized user pre-verification procedures that requires all users to be authenticated before providing access to any resource.
- **Zones and Conduits:** A network segregation technique used to isolate the networks and assets to impose and maintain strong access control mechanisms.
- **Zero Trust Network:** The Zero Trust model is a security implementation that assumes that every user trying to access the network is not a trusted entity by default and verifies every incoming connection before allowing access to the network.