• What is Session Hijacking Explain with Techniques?

Session hijacking is a cyberattack in which bad actors gain unauthorized access to a user's active website or application session. These attacks exploit vulnerabilities in web session management by enabling the cyberattacker to impersonate a legitimate user.

• Find DoS/DDoS Attack Tools.

Flow-based Analysis. This technique looks closely at network traffic flows to identify any odd trends that might point to a DDoS attack. Flow-based analysis assists in identifying large-scale anomalies that are typical of DDoS attacks by monitoring the volume, frequency, and type of network traffic.

• Explain SYN Flooding Attack with example

In a TCP SYN Flood attack, the malicious entity sends a barrage of SYN requests to a target server but intentionally avoids sending the final ACK. This leaves the server waiting for a response that never comes, consuming resources for each of these half-open connections.

• List of Web App Hacking Methodology.

Hackers typically follow a systematic approach that includes information gathering, vulnerability analysis, exploiting weaknesses, and maintaining access to compromised systems.

• SQL Injection Methodology

SQL injection methodology involves crafting malicious SQL code to manipulate or retrieve data from a database through vulnerable web application inputs. Attackers exploit how applications construct SQL queries, often by injecting code into user input fields like login forms or search bars. This allows them to bypass security measures, access sensitive information, or even take control of the database server.

• Explain sql injection with any tool.

SQL injection is an attack used to manipulate the relational databases of a web application, such as MySQL, Oracle Database or Microsoft SQL Server. This should not be confused with NoSQL injections, which are attacks used to manipulate non-relational databases such as MongoDB or CouchDB