**SSCBS**

**MAYANK CHOPRA**

**ROLLNO -23719**

**What is cyber security**

**This is the practice of protecting systems, networks and program form digital attack, this cyber-attack are usually aimed at accessing, changing or destroying sensitive information. Implementing effective cyber security measures like secure methods for website development, developers should know the proper and good code.**

**WHEN is CYBER SECURITY IMPORTANT->**

**In todays connected world, everyone benefits from advanced cyber defence programs. Everyone relies on critical infrastructure like powerplants, hospitals.**

**TYPES OF CYBER SECURITY THREATS –**

**PHISIPING - it is a practice of sending fraudulent emails that resembles from reputed resource.**

**The aim is to steal data like credit card numbers, login information etc.**

**SOCIAL ENGINERRING – it is trick to reveal sensitive information.**

**MALWARE – it is a software designed to gain unauthorize access or to cost damage to the computer**

**WHAT IS OWASP TOP 10 – OPEN web SECURITY PROJECT. is a international non-profit organization dedicated to web application security, one of the OWASP principles is that all of their materials be freely available and easily accessible on their website making it possible for anyone to improve their own web application security.**

**The top 10 OWASP security are –**

**Injection attacks happens when untrusted data send to code.**

**Broken authentication –**

 The essence of Broken Authentication is where you (Web Application) allow your users to get into your website by creating a new account and handling it for specific reasons.

**Sensitive data exposure –**

**Sensitive data** is**anything** that should not be accessible to**unauthorized** access, known as sensitive data.

**XXE-** XML**external entity injection** (also known as XXE) is a web security vulnerability that allows an attacker to interfere with an application's processing of XML data. I

**Broken Access Control –**

Access control enforces policy such that users cannot act outside of their intended permissions. Failures typically lead to unauthorized information disclosure, modification, or destruction of all data or performing a business function outside the user's limits.

**Security Misconfiguration**

**Cross Site Scripting**

**Insecure Deserialization**

**Using components with known vulnerabilities**