Shaheed Sukhdev College of Business Studies

University of Delhi

Post Graduate Diploma in Cyber Security and Law

Sakshi Garg • Roll no-23726 • Semester-1

What is Cyber Security?

It is a practice of protecting systems,networks and programs from digital attacks, these cyber attacks 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 poor and good code.

What is Cyber Important?

In today's connected world, everyone benefits from advance cyber defence programs, everyone relies on critical infrastructure like power plants, hospitals,etc.

Types of Cyber Security Threats?

Phishing:

It is a practice of sending fraudlent emails that resembles emails from reputed sources. The aim is to steal data like credit card numbers, login information,etc.

Social Engineering:

It is a trick to reveal sensitive information

Malware:

It is a software designed to gain unorthorised access or to cause damage to the computer

What is OWASP TOP 10?

Open Web Application security project is an International non-profit organisation dedicated to web application security. One of the OWASP core principals 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-

1. Injection Attacks happens when untrusted data send to code

2. **Broken Authentication**- Weaknesses in authentication and session management can allow attackers to compromise user accounts, gain unauthorized access, or impersonate users.
3. **Sensitive data exposure**- Inadequate protection of sensitive data, such as passwords or financial information, can lead to data breaches. This risk involves insecure storage, transmission, or inadequate encryption of sensitive information.

4. **XXE Injection** - XXE vulnerabilities occur when an application processes XML input insecurely, allowing attackers to include malicious content and exploit the system.

5. **Broken Access Control** moves up from the fifth position; 94% of applications were tested for some form of broken access control. The 34 Common Weakness Enumerations (CWEs) mapped to Broken Access Control had more occurrences in applications than any other category.

6. **Security Misconfiguration** moves up from #6 in the previous edition; 90% of applications were tested for some form of misconfiguration. With more shifts into highly configurable software, it's not surprising to see this category move up. The former category for XML External Entities (XXE) is now part of this category.
7. **Cross-Site Scripting (XSS):** XSS vulnerabilities allow attackers to inject malicious scripts into web pages that are viewed by other users. This can result in the theft of user data or session hijacking.

8. **Insecure Deserialization:** Insecure deserialization can lead to remote code execution or other security issues. Attackers may manipulate serialized objects to execute malicious actions.

9. **Using Components with Known Vulnerabilities:** Integrating third-party components or libraries with known vulnerabilities can expose applications to exploitation. It's crucial to keep dependencies up-to-date.

10. **Insufficient Logging & Monitoring:** Inadequate logging and monitoring make it challenging to detect and respond to security incidents. Proper logging and monitoring are essential for identifying and mitigating attacks.