**Name**: Amar Dagaura

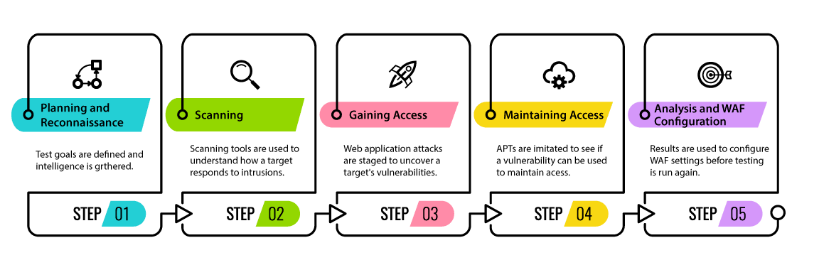
**Student ID:** 210129

**Module**: Pen-Testing (B.Sc.(hons) Ethical Hacking and cybersecurity)

**What is Pen testing?**

Penetration Testing is a legal, structured procedure to evaluate the security posture of an organization. This practice simulates an attack against the security infrastructure of the enterprise, such as its network, applications, and users, to identify the exploitable vulnerabilities. It determines the efficacy of the company’s security policies, controls, and strategies. To strengthen the system, penetration testers proactively analyse for design flaws, technical weaknesses, and other vulnerabilities.

**Penetration Testing: Approach, Methodology, Types of Tests**

****

* Recon

The recon phase consists in searching for open-source information on the target of the security audit. All information potentially useful for an attacker is collected, for example: IP addresses, domain and sub-domain names, types and versions of technologies used, technical information shared on forums or social networks, data leaks

* Mapping

The mapping phase allows listing all functionalities of the audit target. This step enables pen testers to have a better visibility on the most critical and exposed elements. This step is particularly essential when the objective of the security audit is to conduct tests on all the functionalities of a target.

* Discovery

The discovery phase is an attack phase: pen testers look for vulnerabilities through manual searches complemented by automated tools. The objective is to discover as many vulnerabilities as possible on the target.

* Exploitation

The exploitation phase consists in testing possible exploitations of the flaws identified in the previous phase. This step allows using certain flaws as “pivots”, to discover new vulnerabilities.

**Types of Tests**

|  |  |  |
| --- | --- | --- |
| Black Box Penetration Testing | White Box Penetration Testing | Gray Box Penetration Testing |
| A penetration tester has no previous knowledge of the system to be tested. It is like blind testing as the pen testers find their own way into the system. | A penetration tester has complete knowledge of the system to be tested. The known information includes details about IP addresses, network infrastructure schematics, or the protocols in use. | A penetration tester has limited knowledge of the system to be used. |

**Penetration Testing Execution Standard**

Penetration Testing Execution Standard (PTES) defines penetration testing as 7 phases. Particularly, PTES Technical Guidelines give hands-on suggestions on testing procedures, and recommendation for security testing tools.

* Pre-engagement Interactions
* Intelligence Gathering
* Threat Modeling
* Vulnerability Analysis
* Exploitation
* Post Exploitation
* Reporting

**Tools for Penetration testing**

—apt search dirsearch

-Nmap

- sandbox

- nosql- mysql /phpmyadmin

- apache

- nessus

- Golang> naabu, httpx

- pip3 install requests

- pip3 install bs4

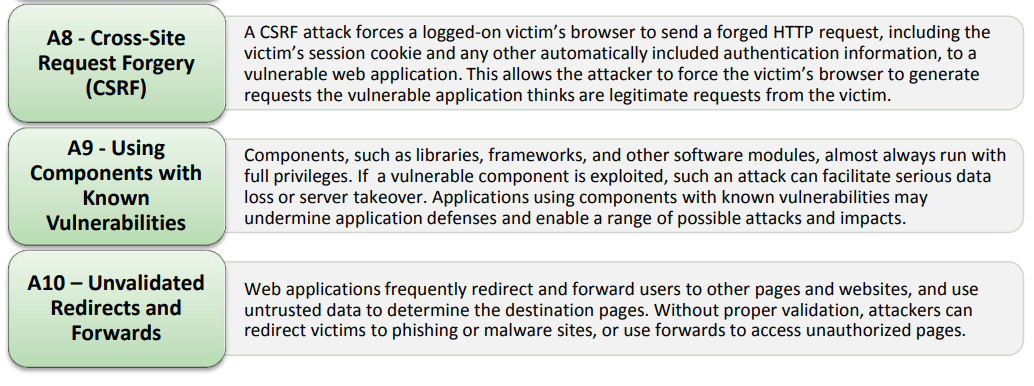
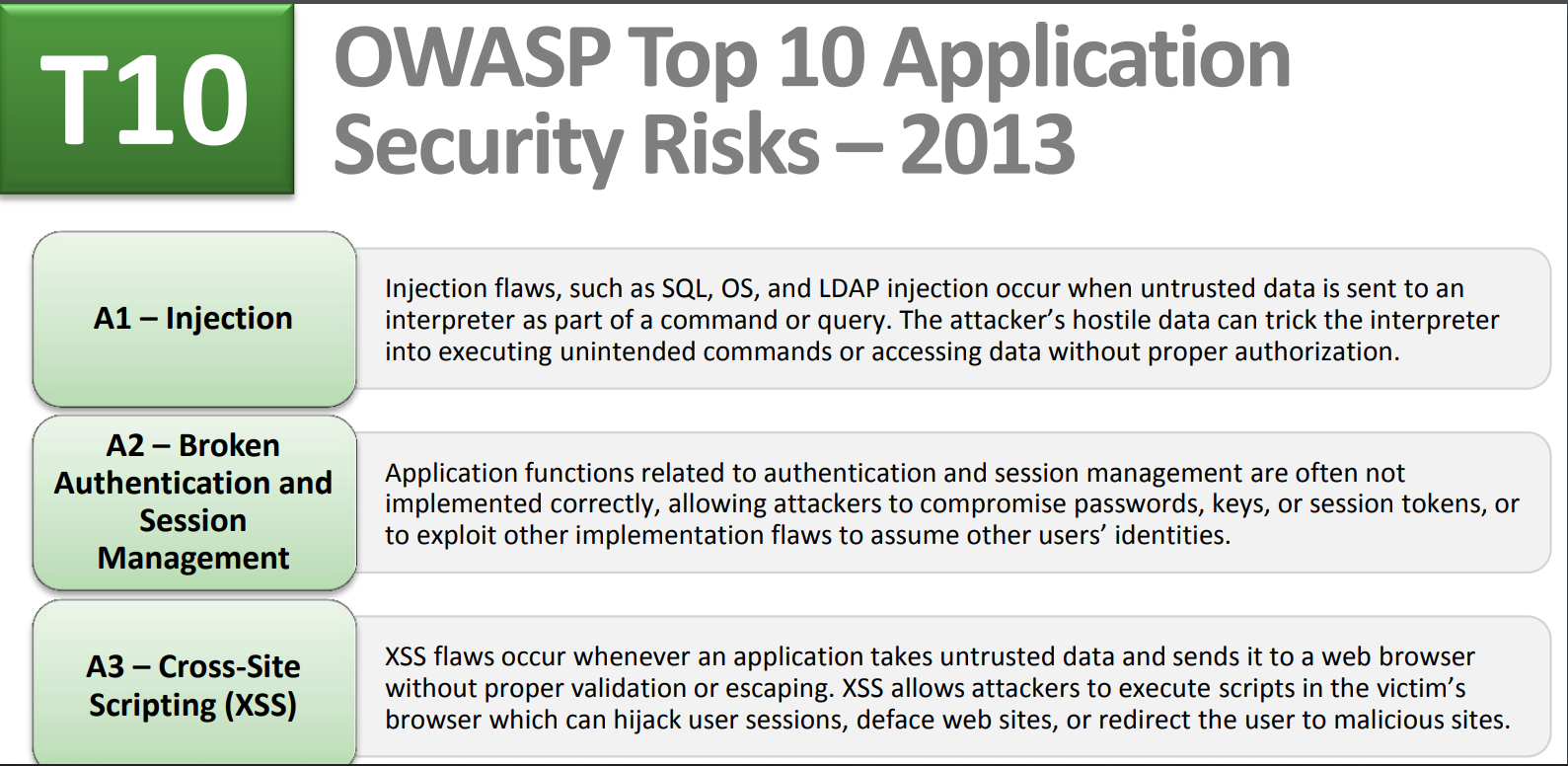
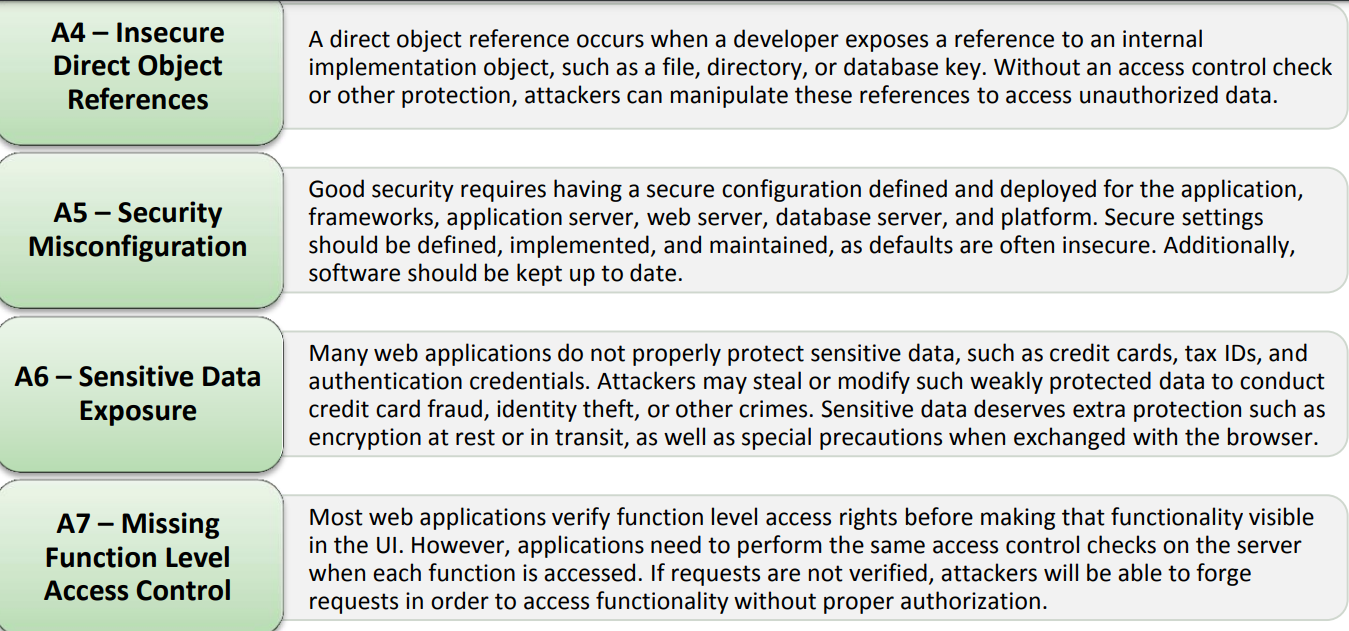
- dirsearch

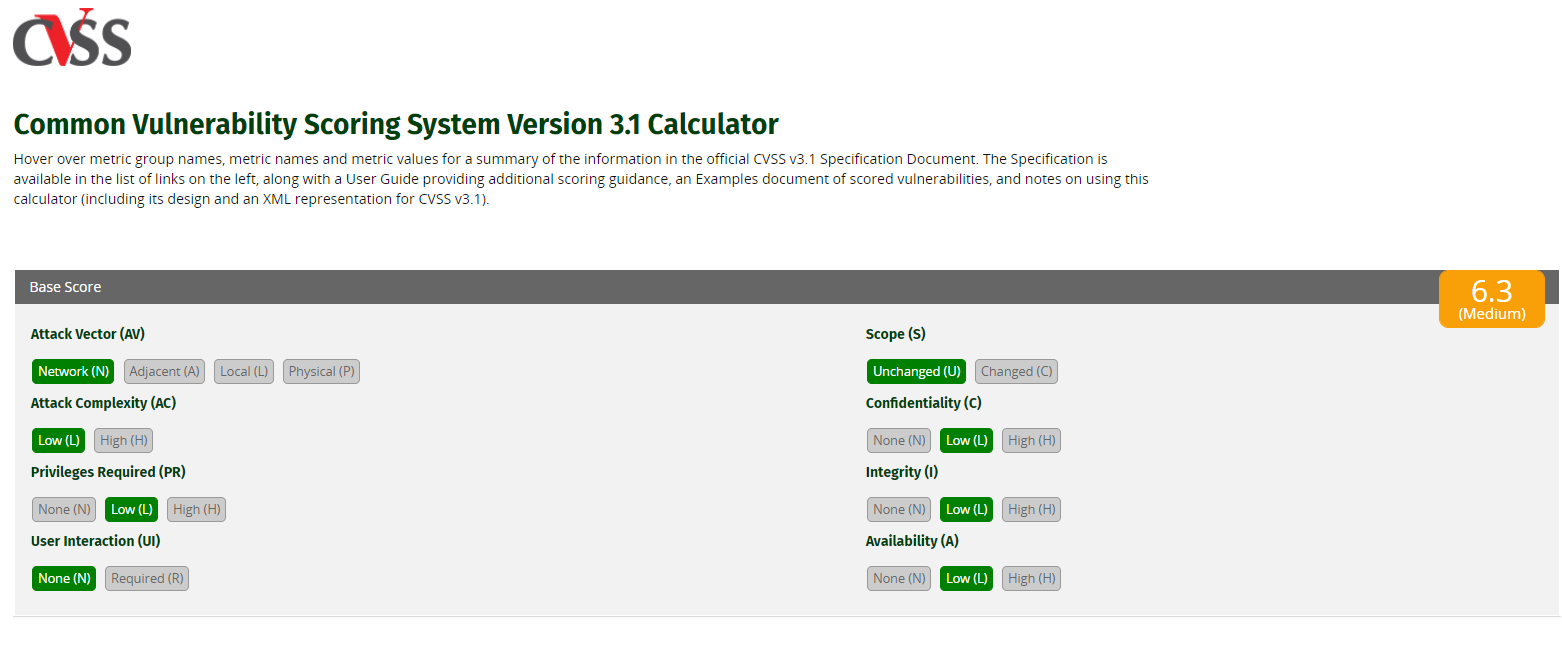
- legion

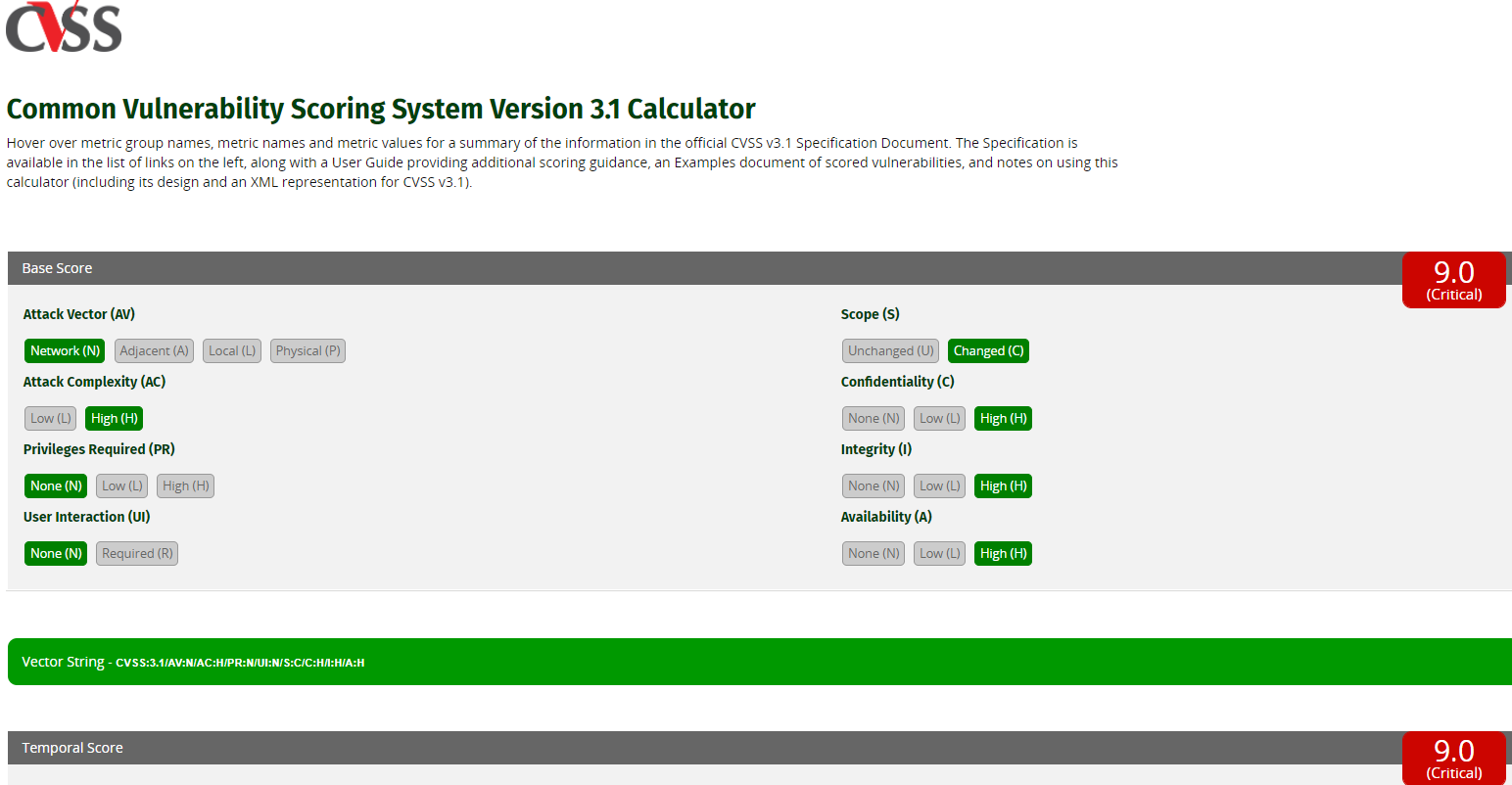
- nikto

- wpscan

- DVWA

**OWASP**

****CVSS 3.2 “**Common Vulnerability Scoring System Version 3.1 Calculator”**

****

**Regex for ip address/range**

string txt = "10.13.11.12-100";

string re1 = "((?:(?:25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\\.){3}(?:25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?))(?![\\d])";

string re2 = ".\*?"; // Non-greedy match on filler

string re3 = @"\b([0-9]{1,2}|1[0-9]{2}|2[0-4][0-9]|25[0-5])\b";//"([0-255])";

Regex r = new Regex(re1 + re2 + re3, RegexOptions.IgnoreCase | RegexOptions.Singleline);

Regex r2 = new Regex(re1, RegexOptions.IgnoreCase |RegexOptions.Singleline);

Match m = r.Match(txt);

Match m3 = r2.Match(txt);

if (m.Success || m3.Success)

{...}