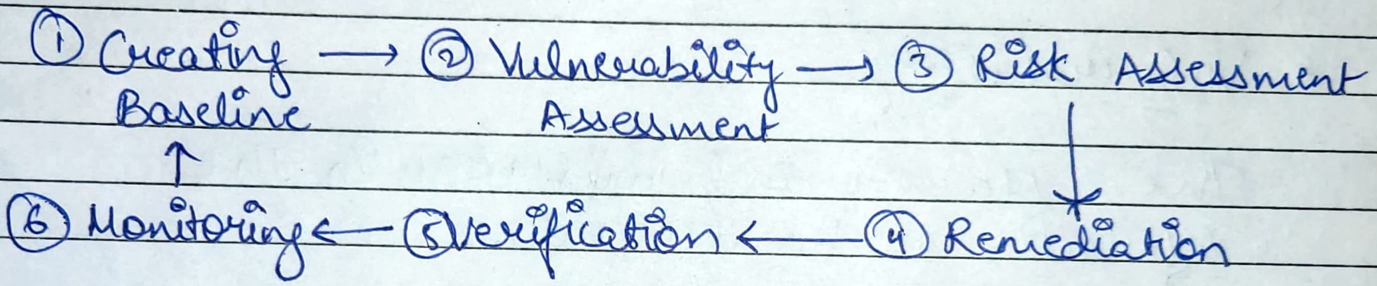
* Vulnerability Assessment

→ Process of Defining, identifying, classifing and prioritizing vulnerabilities in a computer system, application and network infrastructure

* Vulnerability Assessment life cycle.



① Before conducting VA, it's important to establish a baseline against which future assessment can be conducted

② Conducting a VA involves the use of tools and manual techniques to identify potential weaknesses.

③ Once weaknesses are identified, RA is done to determine likelihood and impact of an attack exploiting these vulnerabilities.

④ The next step is to remediate that involve patching the system, changing configuration etc.

⑤ After Remediation, the application should be retested to ensure mitigation.

⑥ At last, Monitoring is required to ensure the application remain secure over time.

* Unknown vulnerability.

Vuln. that aren't known by the developer

* Zero-day vulnerability

Vuln. that just came to know by the developer but isn't registered in CVE.

* Vulnerability

The flaws and mistakes in the software or hardware.

* Exposure

The Personally identifiable information which is kept available.

* False Positive

When a security issue is reported by a vuln scanner but doesnot actually exist as a vuln in the system.

* False positive → Acche ko bura
True Negative → Bure ko accha.

* In Antivirus, if signature isn't updated, true Negative can occur.

* Vulnerability Scanners

- → Nessus
- → OpenVAS
- → Qualys
- → Rapid7
- → Acunetix

* CVE

- → Common Vulnerability and exposure
- → Maintained By MITRE Corp. and FFRDC (Federally Funded Research & Dev. Center)
- → Sponsored by US Dept of Homeland Security and CISA (Cybersecurity Infrastructure Security Agency).
- → Database of publically disclosed info. security issues
- → CVE = [Year]-[Number]

  [Year] ↓ In which year it was reported

  [Number] ↓ Sequential Number assigned by CNA
- → CNA → CVE numbering authority.

* CWE

- → Common Weakness Enumeration
- → Maintained by MITRE Corp
- → A list of top 25 most dangerous CWE issues published annually by MITRE & SANS.
- → Serves as a common, vender-neutral taxonomy for security weaknesses.

→ Eg:- ① CWE 89 → SQL injection.
CWE 120 → Buffer Overflow

* Difference Between CVE & CWE

CVE	CWE
① Common Vuln. and Exposure	① Common weakness Enumeration.
② Identify & track specific vuln and exposures	② Describe broader category of S/w and h/w weakness.
③ Eg:- Heartbleed (CVE 2014-0160) Shellshock (CVE-2014-6271)	③ Eg:- Buffer Overflow (CWE-120) SQL injection (CWE-89)

* CVSS

→ Common vuln Scoring System.

→ Metric for rating vuln.

→ Open standard, originally created by a consortium of software vendors & non-profit security org^n.

→ CVSS is maintained by FIRST (Forum of Inc. Res. and Sec. Team)

→ Scoring depends on:

① Base equation: reflect inherent characteristics of the vuln.

② Temporal score: changes as attacker refine attacks & defender refine defenses

③ Environment score:

* NO scoring or ranking in STRIDE

* STRIDE [Threat classification system (TCS) by MS security engineers]

→ Spoofing :- Allows attacker to claim to be someone they're not, i.e., attacker assume another user's identity.

→ Tampering :- Let Attacker change data that should only be readable to them.

→ Repudiation :- Let user deny that they ever performed a given action.

→ Info. Disclosure :- Allow attacker to read data that they're not supposed to have access to.

→ DOS :- Attempts to knock out a targeted app so that user cannot access it.

→ Elevation of Privilege :- allow attacker to perform action they shouldn't normally be able to do.

* DREAD (TCS by MS security engineers)

→ Scores and Ranks the threat.

→ Damage Potential :- Can the software be damaged?

→ Reliability :- Can we put reponsibility who and how it was damaged?

→ Exploitability :- Is the application exploitable?

→ Affected User :- How many people are affected by the damage?

→ Disclosure :- How much information can be disclosed.

✱ Secure Source Code Review

→ Process of examining an application's source code.

→ Copying code from a place and using it in a website code had made website vulnerable to defacement.

→ Process of secure source code review :-

Planning
↓
Preparation
↓
Execution
↓
Issue identification → Issue Remediation
↑
Verification
↑
Documentation

→ Types of SSCR :-

① Automated → Fast but expensive.
SAST tools.

② Manual → Time-consuming but cheap.