Web Application Security

Dr. Digvijaysinh Rathod
Professor
School of Cyber Security and Digital Forensics
National Forensic Sciences University

digvijay.rathod@nfsu.ac.in

CVE

(Common Vulnerabilities and Exposures)

CVE

- ✓ CVE (Common Vulnerabilities and Exposures) is a list of publicly known cybersecurity vulnerabilities and exposures that provides a standardized reference method for
  - ✓ identifying and
  - ✓ tracking vulnerabilities in software and hardware systems.

What is a CVE

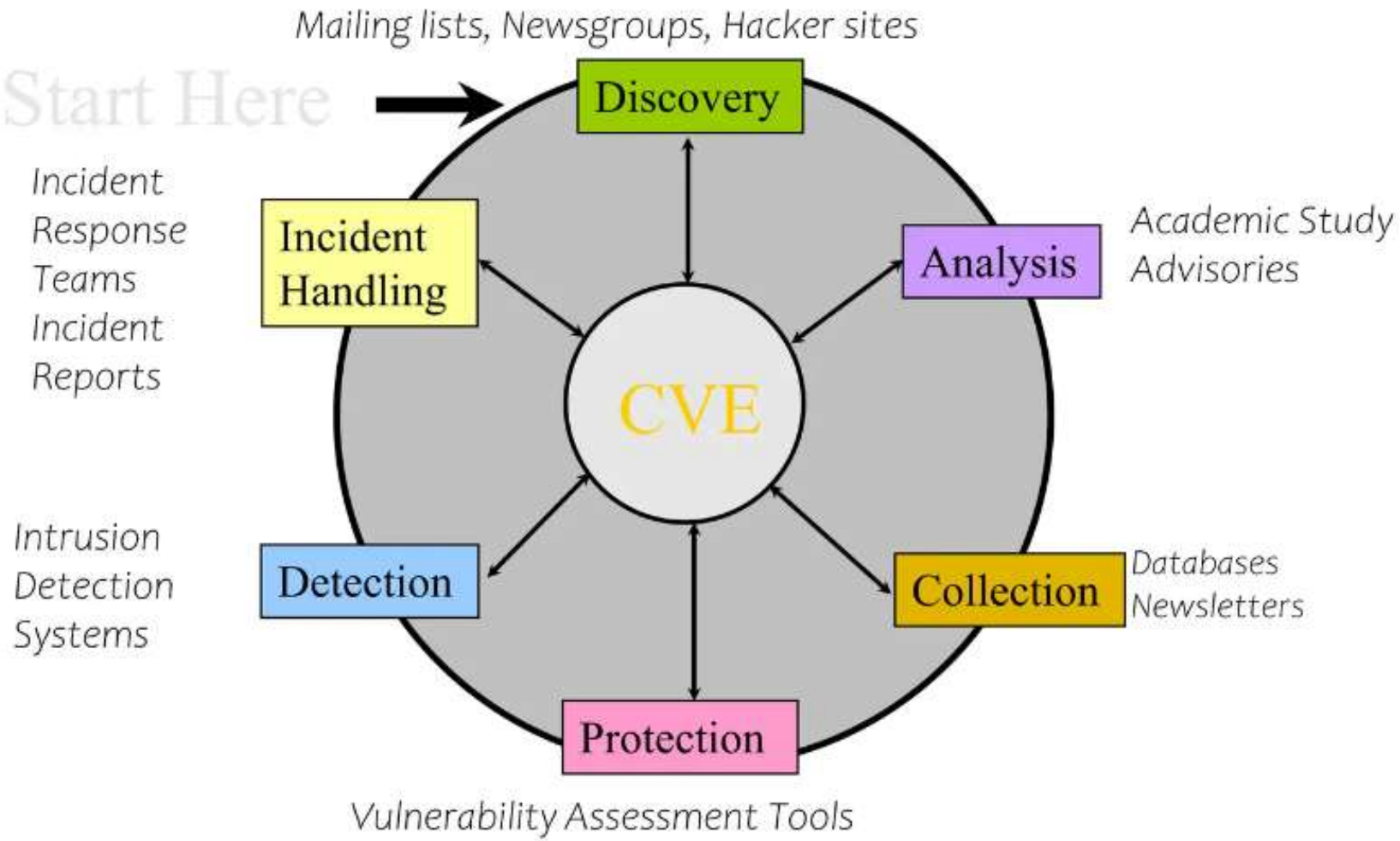
- **Common Vulnerabilities and Exposures** (CVE®) is a list of common identifiers for publicly known cyber security vulnerabilities.

- Use of "CVE Identifiers (CVE IDs)," which are assigned by CVE Numbering Authorities (CNAs) from around the world,
  - ensures confidence among parties when used to discuss or share information about a **unique software vulnerability**,
  - provides a **baseline for tool evaluation**, and
  - enables **data exchange for cyber security automation**.

CVE

- ✓ https://cve.mitre.org/
- ✓ https://www.cvedetails.com/

CVE


Mailing lists, Newsgroups, Hacker sites
Start Here
Discovery
Incident Response Teams Incident Reports
Incident Handling
Analysis
Academic Study Advisories
CVE
Intrusion Detection Systems
Detection
Collection
Databases Newsletters
Protection
Vulnerability Assessment Tools

CVE

- Difficult to correlate **data across multiple organizations** and tools
  - E.g. IDS and assessment tools
  - E.g. security tools and fix information
- **Incident information**
- Difficult to conduct a **detailed comparison** of tools or databases
- Vulnerabilities are counted differently
- Which is more comprehensive?

Common Vulnerabilities and Exposures (CVE): One Common Language

Name	Description
CVE-1999-0003	ToolTalk (rpc.ttdbserverd) buffer overflow
CVE-1999-0006	Buffer overflow in qpopper
CVE-1999-0067	Shell metacharacters in phf
CVE-1999-0344	Windows NT debug-level access bug (a.k.a. Sechole)

- Lists all publicly known security problems
- Assigns **unique identifier** to each problem
- Remains **independent** of multiple perspectives
- Is **publicly open** and shareable
- **Community-wide effort** via the CVE Editorial Board

Addressing Common Misconceptions of CVE

- Not a full-fledged vulnerability database
  - Simplicity avoids competition, limits debate
  - Intended for use by vulnerability database maintainers
- Not a taxonomy or classification scheme
- Focuses on vulnerabilities instead of attacks
  - Does not cover activities such as port mapping
- Not just “vulnerabilities” in the classical sense
  - Definitions of “vulnerability” vary greatly
  - “Exposure” covers a broader notion of “vulnerability”
- Competing vendors are working together to adopt CVE

CVE Editorial Board

- Members from 25 different organizations including researchers, tool vendors, response teams, and end users
- Mostly technical representatives
- Review and approve CVE entries
- Discuss issues related to CVE maintenance
- Monthly meetings (face-to-face or phone)
- Publicly viewable mailing list archives

Adding new entries

- Board member submits raw information to MITRE
- Submissions are grouped, refined, and proposed back to the Board as candidates
  - Form: CAN-YYYY-NNNN
  - Strong likelihood of becoming CVE-YYYY-NNNN
  - Delicate balance between timeliness and accuracy
- Board reviews and votes on candidates
  - Accept, modify, recast, reject, reviewing
- If approved, the candidate becomes a CVE entry
- Entry is included in a subsequent CVE version
  - Published on CVE web site
- Entries may later be modified or deprecated

CVE is:

- One name for one vulnerability or exposure
- One standardized description for each vulnerability or exposure
- A dictionary rather than a database
- How disparate databases and tools can "speak" the same language
- The way to interoperability and better security coverage
- A basis for evaluation among tools and databases
- Free for public download and use
- Industry-endorsed via the CVE Numbering Authorities, CVE Board, and CVE-Compatible Products

Why CVE

- CVE was launched in 1999, as a government US program
- different metrics to state the number of vulnerabilities or exposures they detected
- CVE is now the industry standard for vulnerability and exposure names.

CVE Identifier

- CVE Identifiers (also referred to by the community as "CVE IDs," "CVE entries," "CVE names," "CVE numbers," and "CVEs") are ***unique***, ***common identifiers*** for publicly known cyber security vulnerabilities.

- Each CVE Identifier includes the following:

  - **CVE identifier number** with four or more digits in the sequence number portion of the ID (i.e., "CVE-1999-0067", "CVE-2014-12345", "CVE-2016-7654321").
  - **Brief description** of the security vulnerability or exposure.
  - Any **pertinent references** (i.e., vulnerability reports and advisories).
  - CVE Identifiers are used by information security product/service vendors and researchers as **a standard method for identifying vulnerabilities** and for **cross-linking with other repositories** that also use CVE Identifiers.

State of CVE IDs

- **RESERVED ->** it has been reserved for use by a CVE Numbering Authority (CNA)
  1. the CVE is **populated** with details and **published on the CVE List**,
  2. it will become **available** in the **U.S. National Vulnerability Database (NVD)**
  3. As one of the final steps in the process, the **NVD Common Vulnerability Scoring System (CVSS) scores for the CVE ID** are assigned by the **NIST NVD team**.
- **DISPUTED** -> When one party disagrees with another party's assertion that a particular issue in software is a vulnerability
- **REJECT** -> Not accepted as CVE

- The **Common Vulnerability Scoring System (CVSS)** provides an open framework for communicating the characteristics and impacts of IT vulnerabilities.

CVSS v2.0 Ratings

Severity	Base Score Range
Low	0.0-3.9
Medium	4.0-6.9
High	7.0-10.0

CVSS v3.0 Ratings

Severity	Base Score Range
Low	0.0-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0

- ✓ Additional Notes

CVE

- ✓ Introduction to CVE
- ✓ CVE (Common Vulnerabilities and Exposures) is a list of publicly known cybersecurity vulnerabilities and exposures that provides a standardized reference method for identifying and tracking vulnerabilities in software and hardware systems. Here are some key points regarding

CVE

CVE:

- Identification: CVE assigns a unique identifier to each vulnerability or exposure, known as a CVE ID. This ID format consists of the prefix "CVE" followed by the year of assignment and a unique number (e.g., CVE-2022-1234).
- Standardization: CVE aims to standardize the names for vulnerabilities across various organizations and products, allowing easier information sharing and coordination in the cybersecurity community.
- Centralized Database: The CVE database is maintained by the MITRE Corporation, a not-for-profit organization. It serves as a centralized repository for information on vulnerabilities, including descriptions, impact assessments, and solutions.

CVE

- CVE:
- Publicly Accessible: The CVE List is publicly accessible, allowing security researchers, vendors, and organizations to search and reference vulnerabilities. This transparency facilitates collaboration and helps organizations prioritize security efforts.
- Importance in Security Practices: CVE identifiers are widely used in security practices such as vulnerability management, patch prioritization, and risk assessment. Security teams use CVE IDs to track and address vulnerabilities in their systems.
- Link to Security Advisories and Patches: CVE entries typically include references to security advisories, patches, or mitigation measures provided by vendors. This information helps users identify and implement solutions to mitigate the risks associated with the vulnerabilities.

CVE

- CVE:
- Lifecycle: Each CVE entry undergoes a lifecycle, starting from initial discovery or disclosure, through the coordination of information between vendors, researchers, and the CVE program, to eventual resolution or mitigation.
- Severity Assessment: CVE entries often include severity ratings, such as the Common Vulnerability Scoring System (CVSS) score, which helps users assess the potential impact of a vulnerability on their systems.
- Ongoing Updates: The CVE List is continuously updated as new vulnerabilities are discovered, disclosed, and addressed. Regular monitoring of the CVE database is essential for staying informed about emerging threats and vulnerabilities.
- Integration with Security Tools: Many security tools and platforms integrate with the CVE database to provide automated vulnerability scanning, detection, and remediation capabilities.

CVE

- CVE:
- Overall, CVE plays a crucial role in promoting cybersecurity awareness, collaboration, and risk management across the global IT ecosystem.

Application CVE in the vulnerability assessment

- CVE is widely used in vulnerability assessment processes to identify, prioritize, and manage security vulnerabilities effectively. Here's how CVE is applied in vulnerability assessment:

1. Identification of Vulnerabilities: Security researchers, vendors, and organizations use CVE IDs to uniquely identify and reference specific vulnerabilities. During vulnerability assessment, security teams leverage CVE identifiers to search for known vulnerabilities affecting their systems, applications, and infrastructure.
2. Vulnerability Scanning and Detection: Vulnerability assessment tools and scanners often utilize CVE identifiers to match detected vulnerabilities with entries in the CVE database. By correlating scan results with CVE IDs, security teams can quickly determine which vulnerabilities pose risks to their environment.

Application CVE in the vulnerability assessment

- Prioritization of Remediation Efforts: CVE entries typically include severity ratings, such as CVSS scores, which indicate the potential impact and exploitability of vulnerabilities. Security teams use this information to prioritize remediation efforts based on the criticality and risk associated with each vulnerability.
- Patch Management: CVE identifiers are linked to security advisories and patches provided by vendors. Security teams leverage CVE IDs to identify the specific patches or updates required to address known vulnerabilities in their systems. Patch management processes often involve mapping CVE IDs to applicable patches and tracking the status of patch deployment.
- Risk Assessment and Mitigation Planning: CVE data facilitates risk assessment by providing detailed information about vulnerabilities, including descriptions, affected systems, and available mitigations. Security teams use this information to assess the potential impact of vulnerabilities on their environment and develop mitigation strategies to reduce risk.

Application CVE in the vulnerability assessment

- Tracking Vulnerability Status: CVE entries undergo a lifecycle, from initial discovery or disclosure to resolution or mitigation. Security teams track the status of vulnerabilities by monitoring updates to CVE entries, including the release of patches, advisories, or mitigations provided by vendors. This helps ensure that vulnerabilities are addressed in a timely manner.
- Integration with Vulnerability Management Platforms: Vulnerability management platforms often integrate with the CVE database to streamline vulnerability assessment processes. These platforms leverage CVE data to automate vulnerability scanning, detection, prioritization, and remediation workflows, enabling efficient management of security risks.

Application CVE in the vulnerability assessment

8. Compliance and Reporting: CVE identifiers are commonly referenced in compliance frameworks and regulatory requirements. Security teams use CVE data to demonstrate compliance with security standards by identifying and addressing known vulnerabilities in their systems. CVE information also supports reporting and audit processes by providing evidence of vulnerability assessment activities and remediation efforts.

- Overall, the application of CVE in vulnerability assessment enables security teams to identify, prioritize, and manage security vulnerabilities effectively, thereby reducing the risk of security breaches and ensuring the overall security posture of their organizations.

Mobile Phone Security

Dr. Digvijaysinh Rathod
Associate Professor
School of Cyber Security and Digital Forensics
National Forensic Sciences University

digvijay.rathod@nfsu.ac.in