Web Application Security

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

digvijay.rathod@nfsu.ac.in

Common Weakness Enumeration (CWE™)

Version 4.15

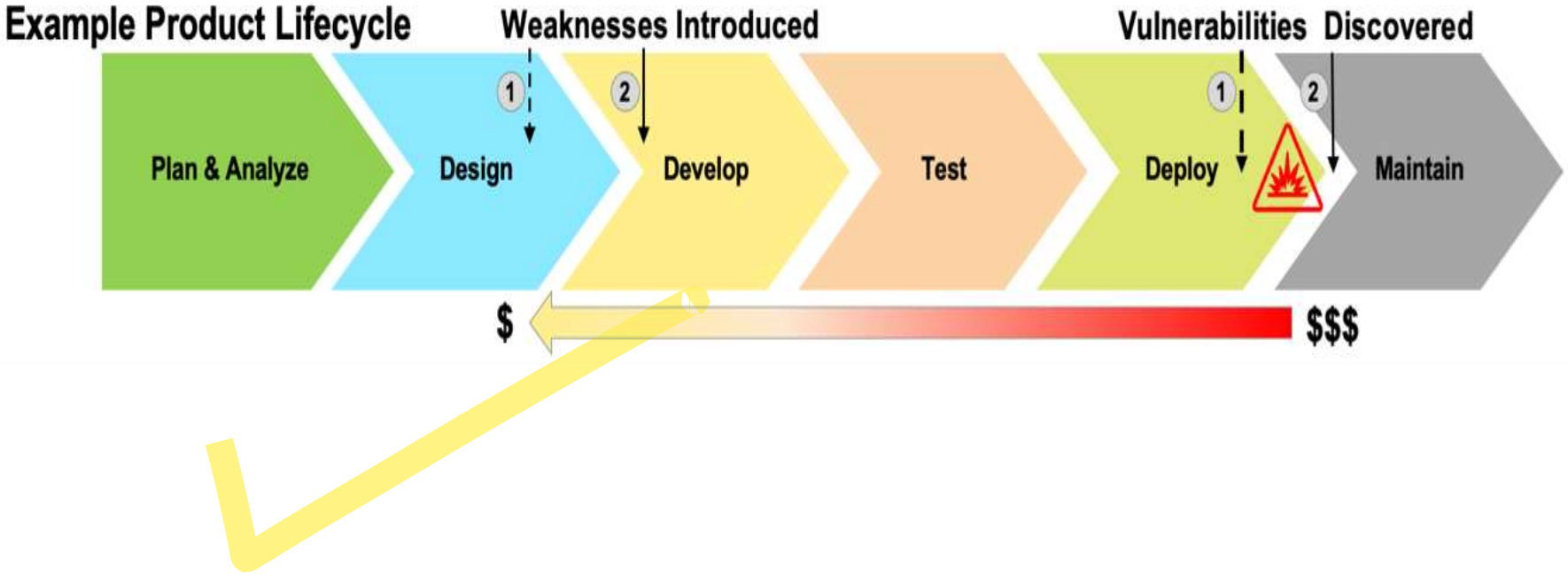
About CWE

- ✓ Common Weakness Enumeration (CWE™) is a community-developed list of
- ✓ common software and hardware weaknesses.
- ✓ A “weakness” is a condition in a software, firmware, hardware, or service component that, under certain circumstances, could contribute to the introduction of vulnerabilities.
- ✓ The CWE List and associated classification taxonomy identify and describe weaknesses in terms of CWEs.

About CWE

- ✓ Knowing the weaknesses that result in vulnerabilities means
  - ✓ software developers,
  - ✓ hardware designers, and
  - ✓ security architects
- ✓ can eliminate them before deployment, when it is much easier and cheaper to do so.

About CWE


Example Product Lifecycle
Weaknesses Introduced
Vulnerabilities Discovered
1
2
1
2
Plan & Analyze
Design
Develop
Test
Deploy
Maintain
$
$$$

Using the CWE List

- ✓ The CWE List is fully searchable and may be
  - ✓ viewed or
  - ✓ downloaded in its entirety.
- ✓ There is also a the CWE REST API to make CWE content available to community applications and websites in a more convenient way.

Using the CWE List

- ✓ The **Software Development (CWE-699)** view organizes items by concepts that are frequently used or encountered during software development.
- ✓ The **Hardware Design view** organizes weaknesses around concepts that are frequently used or encountered in hardware design, and
- ✓ **Research Concepts (CWE-1000)** facilitates weakness type research by organizing items by behaviors.

Using the CWE List

- ✓ Other views provide insight for a certain domain or use cases, such as weaknesses introduced during design or implementation;
- ✓ weaknesses with indirect security impacts; those in software written in C, C++, Java, and PHP; in mobile applications; and many more.
- ✓ Another useful feature is the external mappings of CWE content to related resources including the annual **CWE Top 25; OWASP Top Ten**; Seven Pernicious Kingdoms; Software Fault Pattern Clusters; and SEI CERT Coding Standards for C, Java, and Perl.

Useful CWE Links

- ✓ About CWE - https://cwe.mitre.org/about/index.html
- ✓ **Details about CWE with example -** https://cwe.mitre.org/about/new_to_cwe.html
- ✓ CWE List Version 4.15 - https://cwe.mitre.org/data/index.html
- ✓ View by software development - https://cwe.mitre.org/data/definitions/699.html
- ✓ View by Hardware Design - https://cwe.mitre.org/data/definitions/1194.html
- ✓ View by Research Concepts - https://cwe.mitre.org/data/definitions/1000.html

Useful CWE Links

- ✓ External Mappings : These views are used to represent mappings to external groupings such as a Top-N list, as well as to express subsets of entries that are related by some external factor. - https://cwe.mitre.org/data/index.html
- ✓ CWE Top 25 Most Dangerous Software Weaknesses - https://cwe.mitre.org/top25/
- ✓ 2021 CWE Most Important Hardware Weaknesses - https://cwe.mitre.org/scoring/lists/2021_CWE_MIHW.html

Most Important CWE Links

- ✓ CWE List Version 4.15 – Downloads

  https://cwe.mitre.org/data/downloads.html

- ✓ Navigate CWE
- ✓ External Mappings

For example

- ✓ https://cwe.mitre.org/about/new_to_cwe.html

Mobile Phone Security

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

digvijay.rathod@nfsu.ac.in