# Web Application Security

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

**digvijay.rathod@nfsu.ac.in**

# Common Vulnerability Scoring System Version 4.0

# Overview

- Common Vulnerability Scoring System (CVSS)
- A universal language to convey vulnerability severity and help determine urgency and priority of response
- Solves problem of multiple, incompatible scoring systems in use today
- Initially a NIAC project
  - Subgroup of the global Vulnerability Disclosure Framework WG
  - Now under the custodial care of FIRST-SIG
- Open
- Usable, understandable, and dissectible by anyone
- In v2 now (June 20th 2007)

# adopters

# Scope Constraints

CVSS is not:

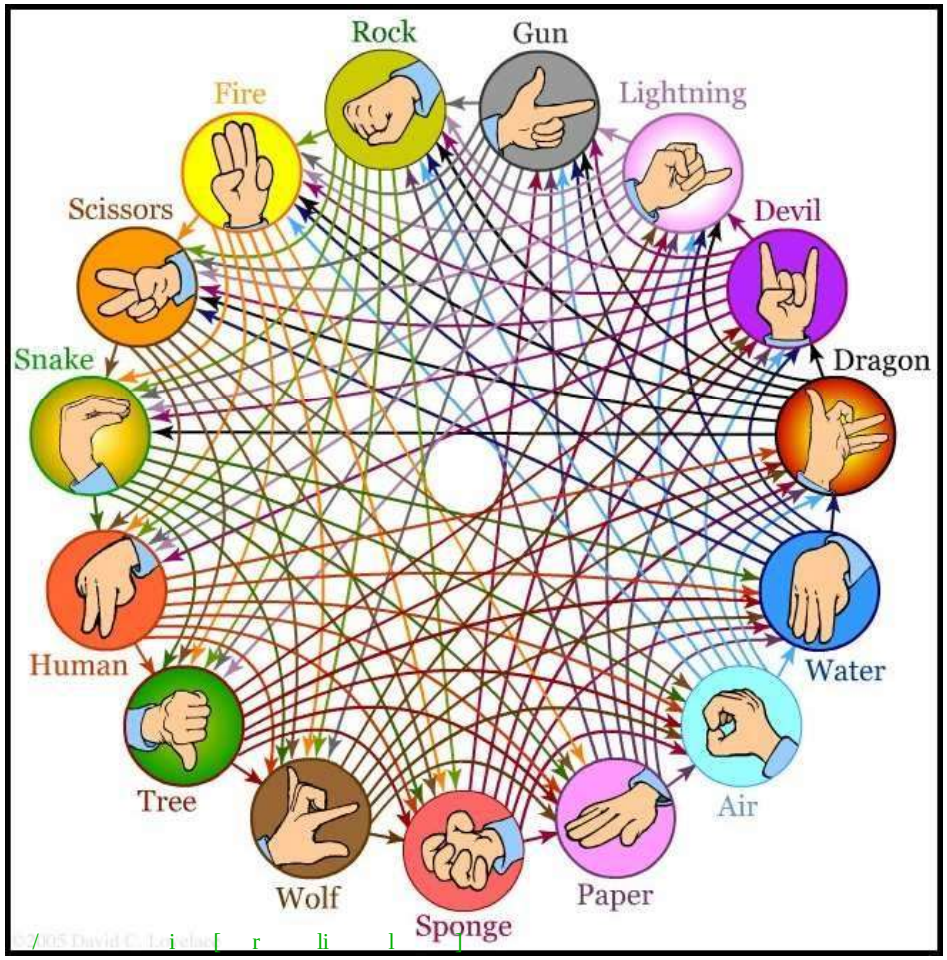
- Threat scoring system (The DHS color warning system)
- Vulnerability database (Symantec's bugtraq)
- Real-time attack scoring system (Symantec's Deepsight)
- Overall risk management program

# Why CVSS?

- Different Organizations
  - Vendors (response)
  - Coordinators (notification, coordination)
  - Reporters (research, discovery)
  - Users (mitigation)

  All have different roles, motivations, priorities, resources, etc
- We need a common way to communicate!
- Set an industry example on alert disclosure

# How do we score now?



# Vendor Scoring: Microsoft

| Rating | Definition |
|---|---|
| Critical | A vulnerability whose exploitation could allow the propagation of an Internet worm without user action. |
| Important | A vulnerability whose exploitation could result in compromise of the confidentiality, integrity, or availability of users data, or of the integrity or availability of processing resources. |
| Moderate | Exploitability is mitigated to a significant degree by factors such as default configuration, auditing, or difficulty of exploitation. |
| Low | A vulnerability whose exploitation is extremely difficult, or whose impact is minimal. |

# Coordinator Scoring: CERT/CC

The metric value is a number between 0 and 180 that assigns an approximate severity to the vulnerability. This number considers several factors, including:

- Q1 Is information about the vulnerability widely available or known?
- Q2 Is the vulnerability being exploited in the incidents reported?
- Q3 Is the Internet Infrastructure at risk because of this vulnerability?
- Q4 How many systems on the Internet are at risk from this vulnerability?
- Q5 What is the impact of exploiting the vulnerability?
- Q6 How easy is it to exploit the vulnerability?
- Q7 What are the preconditions required to exploit the vulnerability?

```
3 * (Q1 + Q2 + Q3) * (Q4 * Q5 * Q6 * Q7) / (20^4)
```

# Researcher Scoring: Secunia

| Rating | Definition |
|---|---|
| Extremely Critical | ypically used for remotely exploitable vulnerabilities, which can lead to system compromise. Successful exploitation does not normally require any interaction and exploits are in the wild. |
| Highly Critical | As Above, no known exploits |
| Moderately Critical | As Above, but DoS only or requiring user interaction |
| Less Critical | XSS, privilege escalation, sensitive data exposure |
| Not Critical | Very limited privilege escalation, locally exploitable DoS, non-sensitive data exposure |

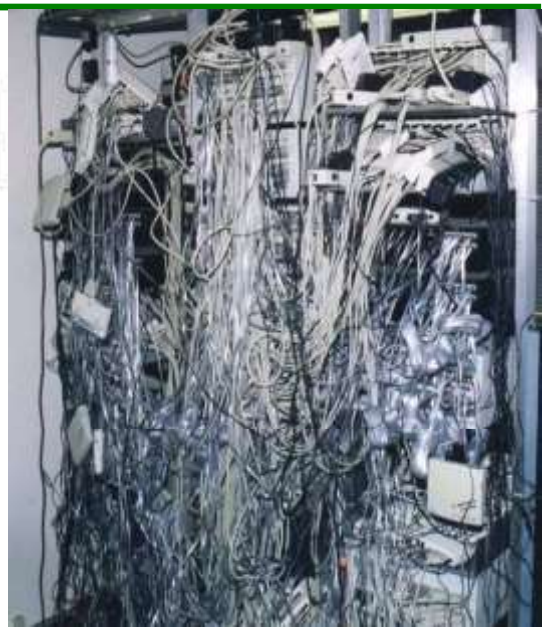
# And the User…?

- Microsoft says "Important"
- CERT says "47.31"
- Secunia says "Less Critical
- User says "Huh?"

# The Busy Security Operations Guy

**2000-2005**

| Year | 2000 | 2001 | 2002 | 2003 | 2004 | 1Q,2005 |
|---|---|---|---|---|---|---|
| Vulnerabilities | 1,090 | 2,437 | 4,129 | 3,784 | 3,780 | 1,220 |



- Read the descriptions
  - 4,129 vulnerabilities * 15 minutes = 129 days
- Affected by 10% of the vulnerabilities?
- Install patches on one system
  - 413 vulnerabilities * 1 hour = 52 days
- Reading reports and patching a single system costs 129 + 52 = 181 days
- Which vulnerability should I patch first? Remote root in DNS? Web server? Desktop systems? DoS affecting routing infrastructure?

# About CVSS

- ✓ The Common Vulnerability Scoring System (CVSS) provides a way to capture the principal characteristics of a vulnerability and produce a
  - ✓ numerical score reflecting its severity.
  - ✓ score ranging from 0 to 10
- ✓ The numerical score can then be translated into a qualitative representation **(such as low, medium, high, and critical)** to help organizations properly assess and prioritize their vulnerability management processes.
- ✓ **The CVSS Special Interest Group (SIG)** is proud to announce the official publication of CVSS v4.0

# About CVSS

- ✓ CVSS is owned and managed by FIRST.Org, Inc. (FIRST), a US-based non-profit organization, whose mission is to help computer security incident response teams across the world
- ✓ A self-paced on-line training course (https://learn.first.org/) is available for CVSS v4.0. It explains the standard without assuming any prior CVSS experience.(https://www.first.org/cvss/)
- ✓ The SIG is composed of representatives from a broad range of industry sectors, from banking and finance to technology and academia. Organizations and individuals interested in joining the SIG, or observing progress via the CVSS SIG mailing lists.

# About CVSS

- ✓ CVSS consists of four metric groups:
  - ✓ Base - The Base group represents the intrinsic qualities of a vulnerability that are constant over time and across user environments
  - ✓ Threat - reflects the characteristics of a vulnerability that change over time
  - ✓ Environmental, and - represents the characteristics of a vulnerability that are unique to a user's environment
  - ✓ Supplemental - do not modify the final score, and are used as additional insight into the characteristics of a vulnerability.

# About CVSS

- CVSS consists of four metric groups:
  - Base - The Base group represents the intrinsic qualities of a vulnerability that are constant over time and across user environments
  - Threat - reflects the characteristics of a vulnerability that change over time
  - Environmental, and - represents the characteristics of a vulnerability that are unique to a user's environment
  - Supplemental - do not modify the final score, and are used as additional insight into the characteristics of a vulnerability.

# About CWE

- ✓ Base metric values are combined with default values that assume the highest severity for Threat and Environmental metrics to produce a score ranging from 0 to 10.
- ✓ To further refine a resulting severity score, Threat and Environmental metrics can then be amended based on applicable threat intelligence and environmental considerations.
- ✓ Supplemental metrics do not modify the final score, and are used as additional insight into the characteristics of a vulnerability. **https://www.first.org/cvss/v4.0/examples**

# About CWE


Common Vulnerability Scoring System v4
Base
Metric Group
Exploitability Metrics
Attack Vector
Attack Complexity
Attack Requirements
Privileges Required
User Interaction
Impact Metrics
Vulnerable System Confidentiality
Vulnerable System Integrity
Vulnerable System Availability
Subsequent System Confidentiality
Subsequent System Integrity
Subsequent System Availability
Scope
Threat
Metric Group
Exploit Maturity
Remediation Level
Report Confidence
Environment
Metric Group
Modified Base Metrics
Attack Vector
Attack Complexity
Attack Requirements
Privileges Required
User Interaction
Vulnerable System Confidentiality
Vulnerable System Integrity
Vulnerable System Availability
Subsequent System Confidentiality
Subsequent System Integrity
Subsequent System Availability
Confidentiality Requirement
Integrity Requirement
Availability Requirement
Supplemental
Metric Group
Automatable
Recovery
Safety
Value Density
Vulnerability Response Effort
Provider Urgency
Key
Existing CVSSv3.1 Component with No Changes
Existing CVSSv3.1 Component with Changes
New CVSS V4 Component
No Longer a CVSS Component in V4

# About CWE

- ✓ Rest of the topic discussed on the basis of - https://www.first.org/cvss/calculator/4.0
- ✓ Example - https://www.first.org/cvss/v4.0/examples

# Mobile Phone Security

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

**digvijay.rathod@nfsu.ac.in**