



# Common Weakness Enumeration (CWE)

## 1.9 Status update

Conor Harris  
Software Systems Engineer, Senior  
MITRE Corporation



# Acknowledgements

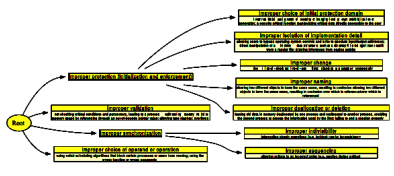
- Various MSM Contributors
  - Robert Martin, CWE Project Lead
  - Steve Christey, CWE Technical Lead
  - Sean Barnum, CAPEC Lead

# Common Weakness Enumeration (CWE)

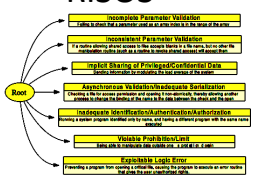
- **dictionary of weaknesses**
  - weaknesses that can lead to exploitable vulnerabilities (i.e. CVEs)
  - the things we don't want in our code, design, or architecture
  - web site with XML of content, sources of content, and process used
- **structured views**
  - currently provide hierarchical view into CWE dictionary content
  - will evolve to support alternate views
- **open community process**
  - to facilitate common terms/ concepts/facts and understanding
  - allows for vendors, developers, system owners and acquirers to understand tool capabilities/ coverage and priorities
  - utilize community expertise

Foundation for  
other **DHS, NSA,**  
**OSD, NIST,**  
**OWASP, SANS, and**  
**OMG SwA Efforts**

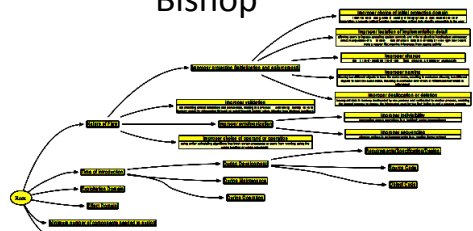
# Protection Analysis



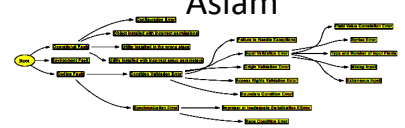
# RISOS



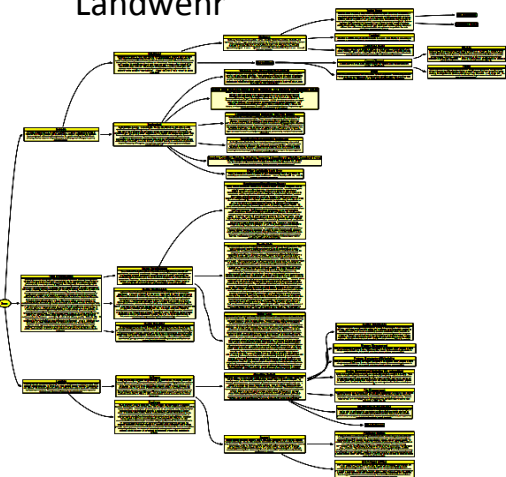
# Bishop



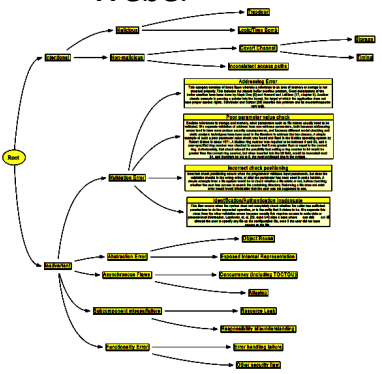
# Aslam



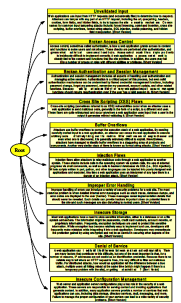
# Landwehr



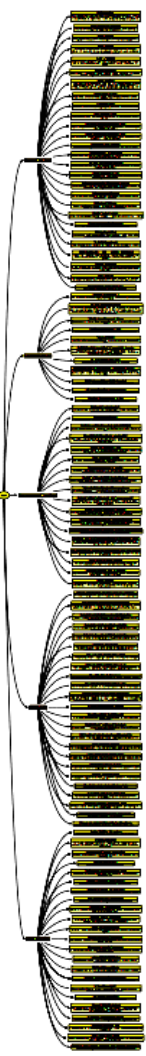
# Weber



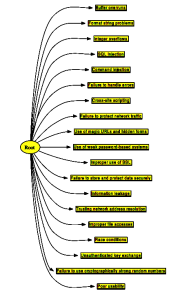
# OWASP



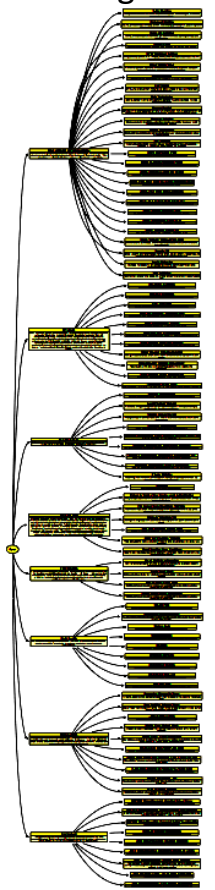
# CLASP



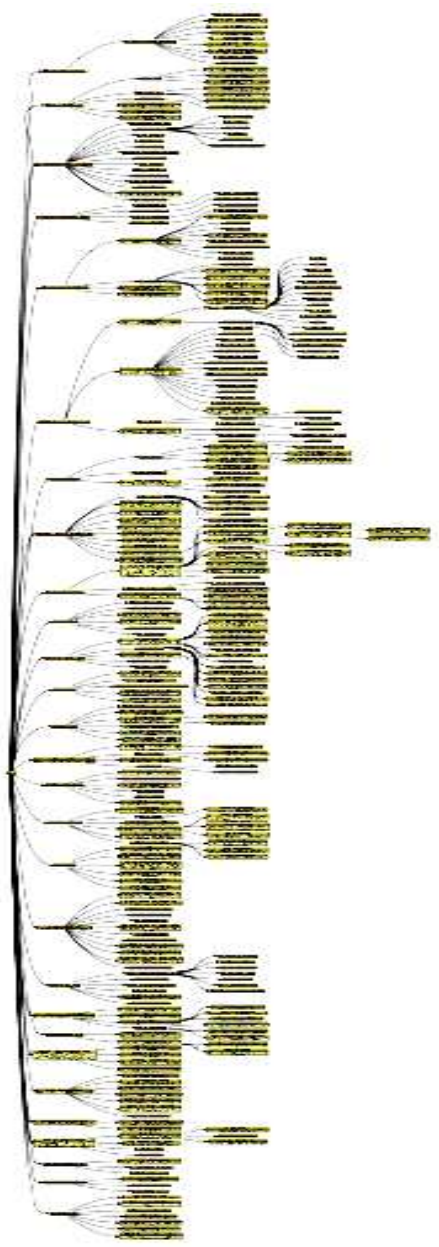
# Microsoft



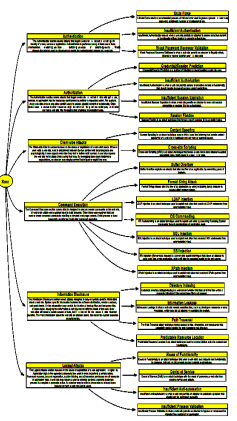
# 7 Kingdoms



# PLOVER



# WASC



# Tool B



# Tool A

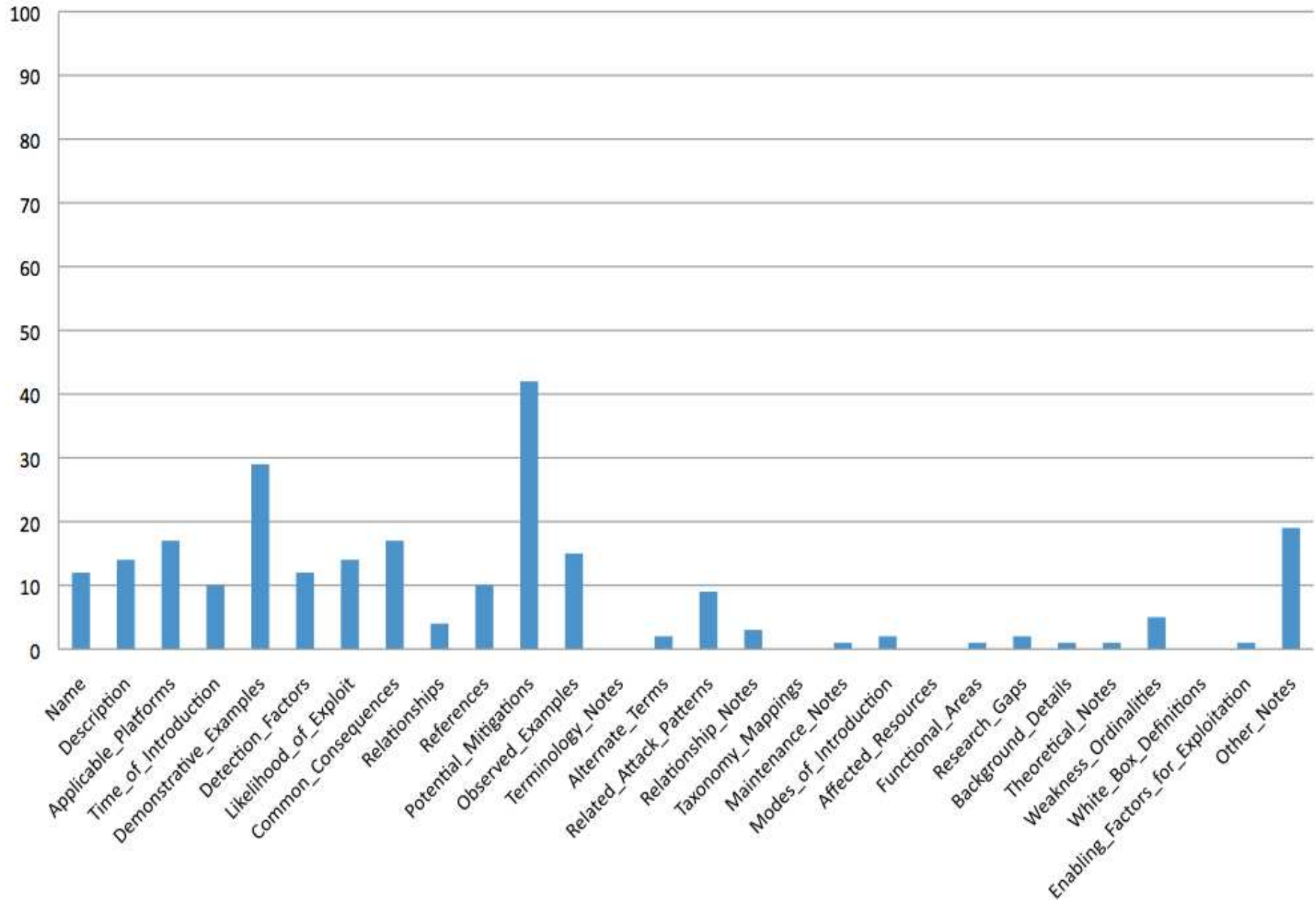


# 20010 CWE/SANS Top 25 Programming Errors

- **Sponsored by:**
  - National Cyber Security Division (DHS)
- **List was selected by a group of security experts from 34 organizations including:**
  - Academia: Purdue, Northern Kentucky University
  - Government: CERT, NSA, DHS
  - Software Vendors: Microsoft, Oracle, Red Hat, Apple, Juniper, McAfee, Symantec, Sun, RSA (of EMC)
  - Security Vendors: Veracode, Fortify, Cigital, Mandiant, Cigital, SRI, Secunia, Breach, SAIC, Aspect, WhiteHat
  - Security Groups: OWASP, WASC

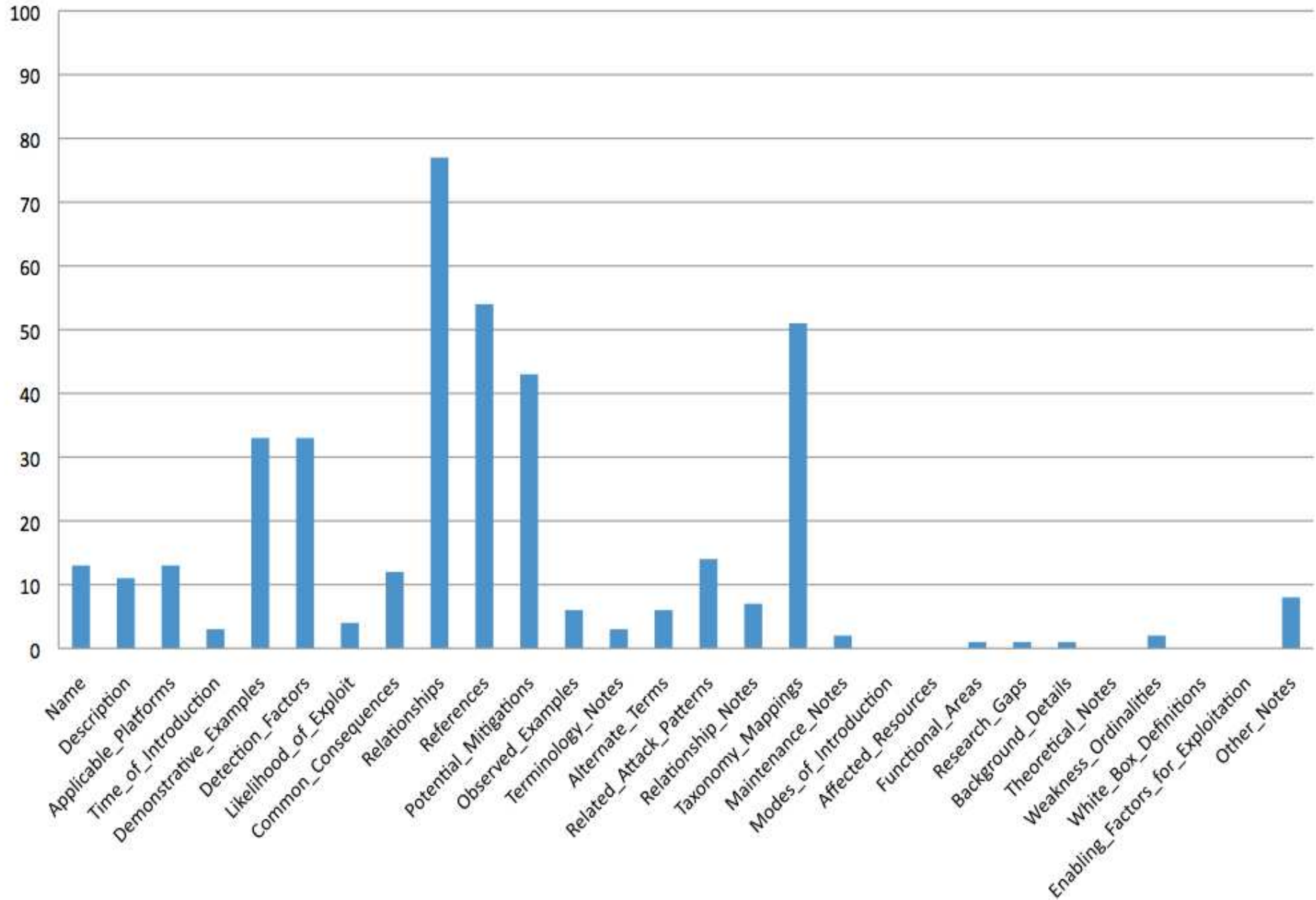
The screenshot shows the SANS website's page for the 2010 CWE/SANS Top 25 Most Dangerous Programming Errors. The page features a navigation bar with links like 'training', 'certification', and 'resources'. A main banner for 'SANS FIRE 2010' is visible. The content area lists the error categories: Insecure Interaction Between Components (8 errors), Risky Resource Management (10 errors), and Porous Defenses (7 errors). It also includes a list of error details such as ranking, links to full entries, remediation costs, and detection methods. A sidebar on the right contains a 'Yearly Archive' and a 'SANS AppSec Streetfighter Blog' announcement. The bottom right corner features a 'Real Threats, Real Skills, Real Success' banner for the SANS Cyber Guardian Program.

## Field Changes - 1.6 to 1.7

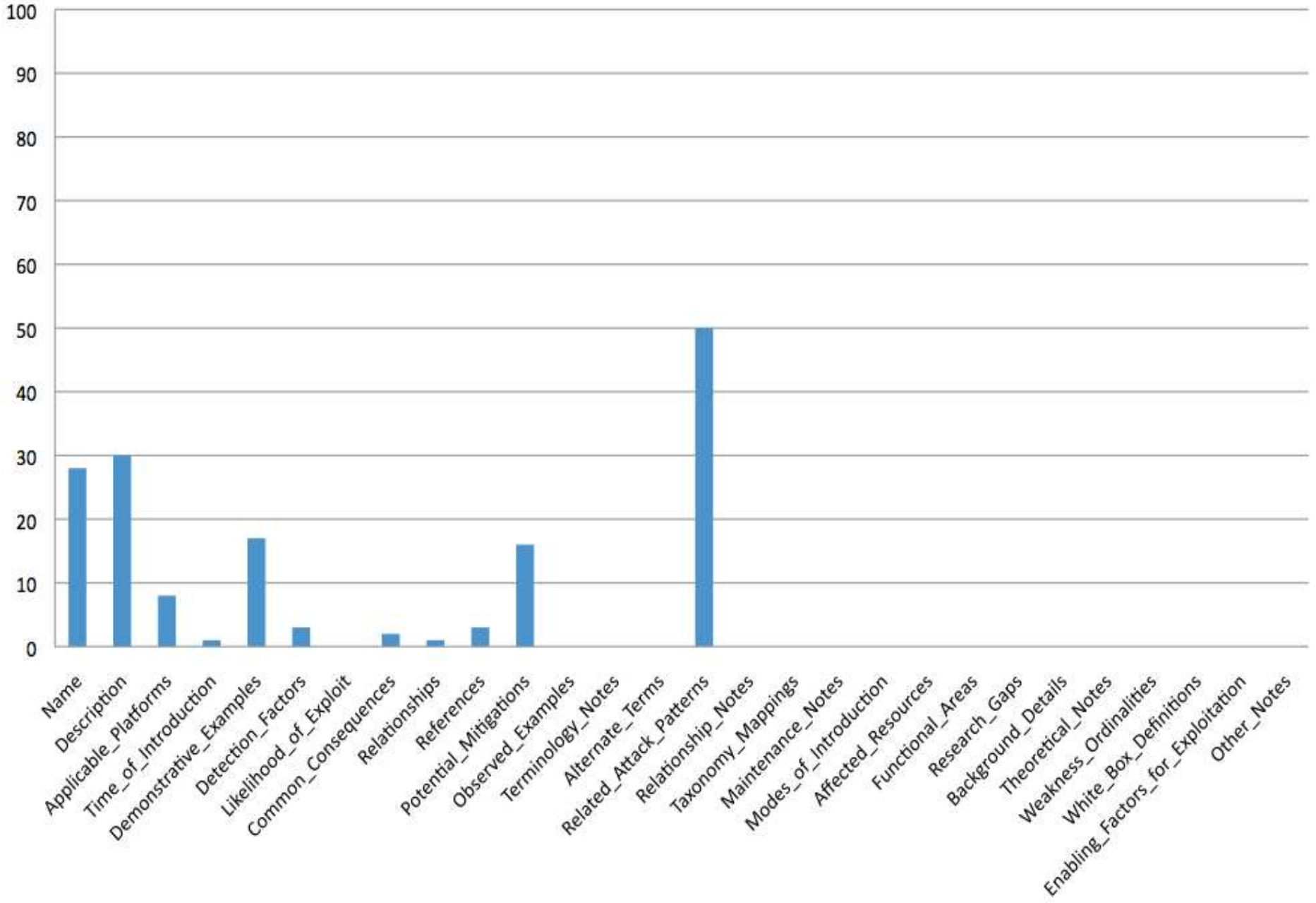




## Field Changes - 1.7 to 1.8

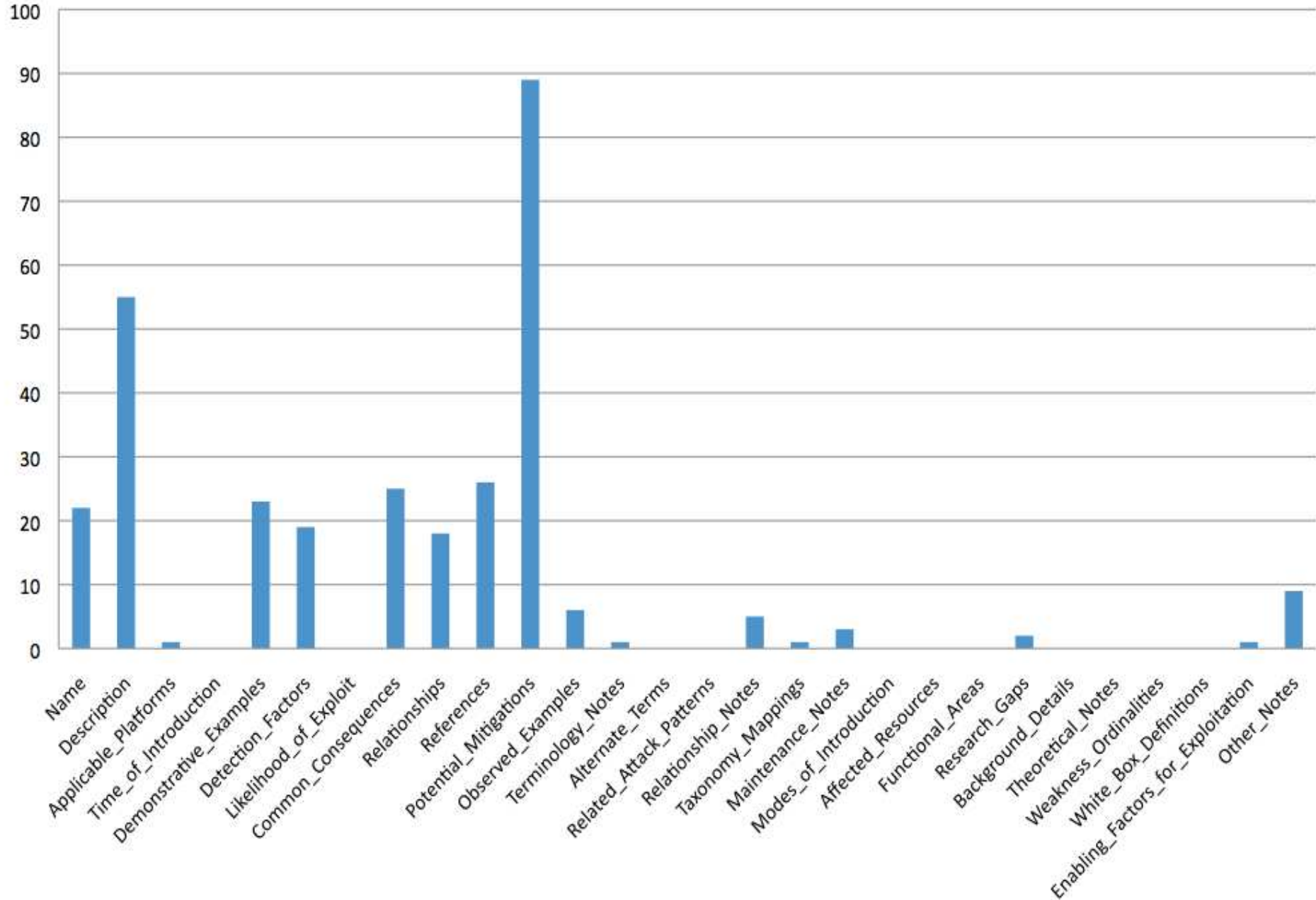


# Field Changes - 1.8 to 1.8.1





## Field Changes - 1.8.1 to 1.9



# Mitigation Library

- Normalize common mitigations across Top 25
  - E.g. general “Input Validation” mitigation can be applied across various injection issues (79, 89, 78, 129...) can be mitigated w/ validation
  - Analyze all Top 25 mits, merge overlap
  - Why is this good?
    - Higher quality
    - Easier to fill in (new entries and gaps)
    - Single point of maintenance

# Example: MIT-4.1

## GENERAL

Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid.

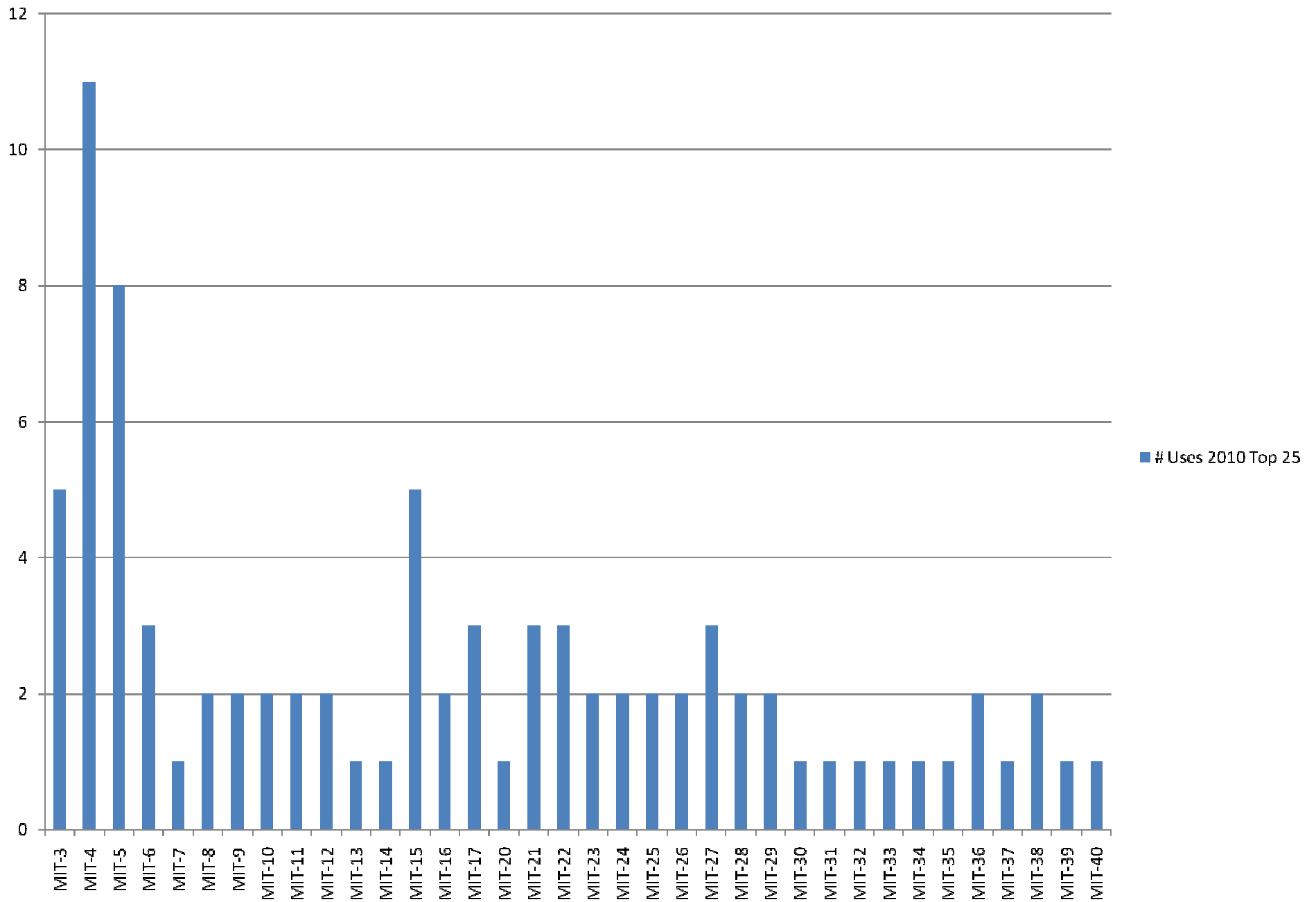
## SPECIFIC

Examples include the Safe C String Library (SafeStr) by Messier and Viega, and the Strsafe.h library from Microsoft. These libraries provide safer versions of overflow-prone string-handling functions. This is not a complete solution, since many buffer overflows are not related to strings.

# Heavy focus on Top 25

- Uses 36 of the 41 mitigations in the library
- 85 occurrences, for an average of 3.4 Top 25 entries per mitigation

## # Uses 2010 Top 25

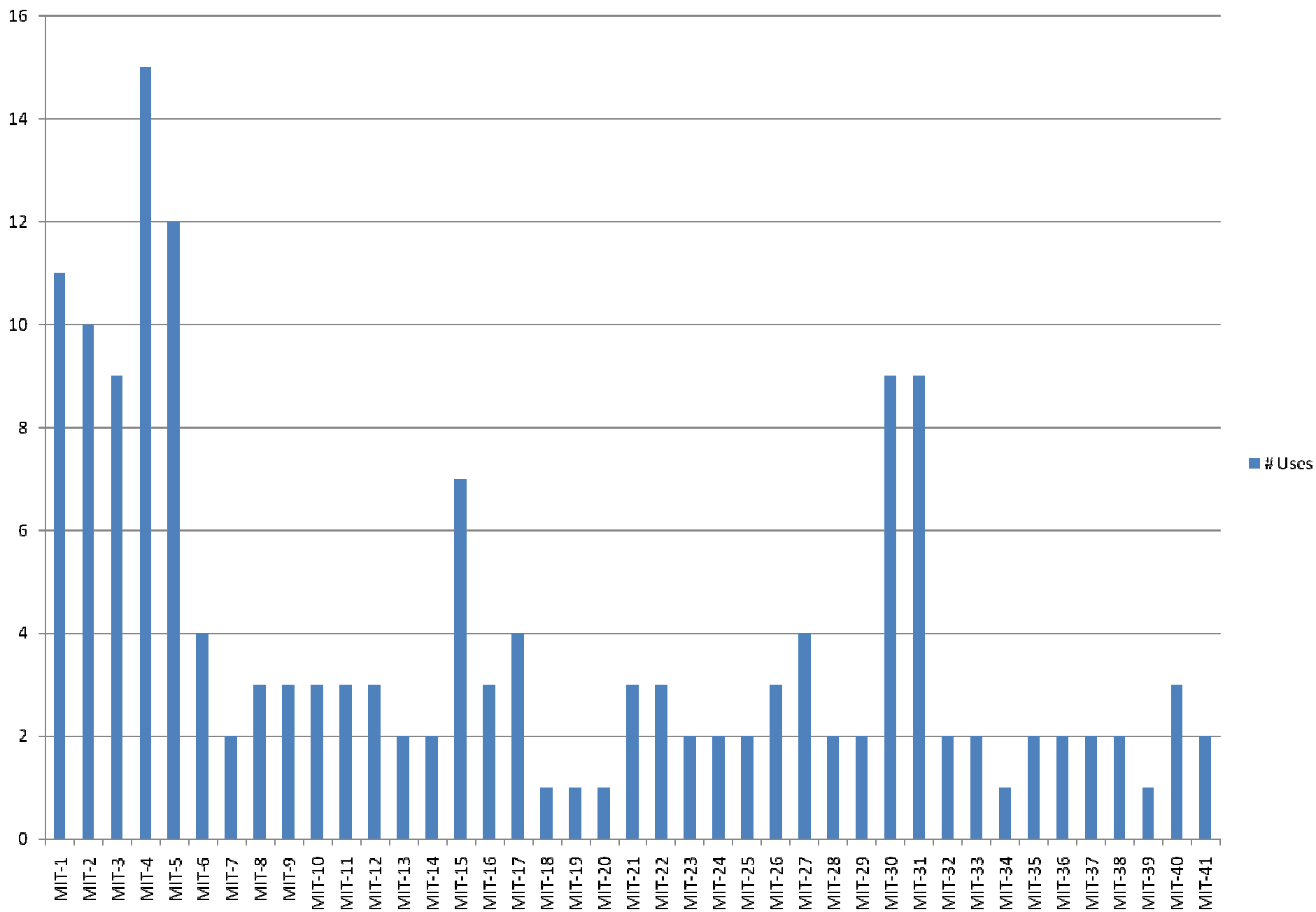


# Most frequently used across CWE merged

- 159 total library mitigations (41 unique)
- Less than 60% of usage is in Top 25
  - Spread easily
  - “Second” use case
    - XSS



# # Mitlib Uses All CWE



# Not Perfect...

- Copy + paste burden still exists
  - Backup checks in place
- What if only the impacted resource varies?
  - e.g.
    - use a reference map for safe URLs
    - use a reference map for safe file names
- Work in progress

# More Mitigation Work

- Top 25 Mitigation Strategies
  - Enumeration
    - e.g. Input Validation, Language Selection, Identify & Reduce Attack Surface
  - Machine detectable

# Top 25 Consequences

- Some standard content
- Technical Impacts
  - More specific than CIA
  - Allows for further automatic mapping
    - Feeds into pocket guide work
  - How to describe technical impact of information exposure?
    - Array indexing issue -> Read/Write mem
    - What about nabbing cookies via XSS?
    - Getting pathname via error message info exposure?

# Vocabulary Work

- <http://cwe.mitre.org/documents/glossary/index.html>
- Reduce usage of overloaded words

The screenshot shows a web browser window titled "CWE - CWE Glossary - Opera". The address bar displays "http://cwe.mitre.org/documents/glossary/index.html". The page content includes the CWE logo and the title "CWE Glossary". Below the title, it states "Document version: 0.4.3 Date: 2010-04-05". A disclaimer follows: "This is a draft document. It is intended to support maintenance of CWE, and to educate and solicit feedback from a specific technical audience. This document does not reflect any official position of the MITRE Corporation or its sponsors. Copyright © 2009, The MITRE Corporation. All rights reserved. Permission is granted to redistribute this document if this paragraph is not removed. This document is subject to change without notice." The author is listed as "CWE Team" and the URL is "http://cwe.mitre.org/documents/glossary/index.html". A "Table of Contents" section lists various terms such as Activation Point, Actor, Attacker, Authentication, Authorization, Base Weakness, Behavior, CRUD, Canonicalization, Canonicalize, Category, Chain, Check, Class weakness, Composite, Compound Element, Consequence, Control Sphere, Crossover Point, Enforce, Entry, Equivalence, Explicit Slice, Filter, Filtering, Graph, Handle, ICTA, Implicit Slice, Improper, Incorrect, Information Exposure, Insecure, Insufficient, Interaction Point, Internal, Leading, Loose Composite, Manipulation, Missing, Named Chain, Natural Hierarchy, Neutralization, Neutralize, Node, Permissions, Pillar, Primary Weakness, Property, Protection Mechanism, Reliance, and Reliance.

# CWE-809 OWASP Top 10 2010





# SANS Street Fighter Blog

The screenshot shows a web browser window with the title "Top 25 Series - Summary and Links - Opera". The address bar contains the URL "http://blogs.sans.org/appsecstreetfighter/2010/04/06/top-25-series-summary-links/". The page header features the "SANS SSI" logo and the text "The Application Security Street Fighter Blog". The main content area is titled "Top 25 Series - Summary and Links" and is posted by Frank Kim on April 6, 2010. It lists 20 programming errors with links to their respective articles. On the right side, there is a search bar and a "CATEGORIES" list with counts for various topics. An advertisement for "Build Security into Your Applications" is also visible.

Top 25 Series - Summary and Links

Posted by Frank Kim on April 6, 2010 - 3:41 pm  
Filed under Top25

As requested here are the links to all the posts on the Top 25 Most Dangerous Programming Errors. Please let us know if you have any suggestions or comments.

- 1 - [Cross-Site Scripting \(XSS\)](#)
- 2 - [SQL Injection](#)
- 3 - [Classic Buffer Overflow](#)
- 4 - [Cross-Site Request Forgery \(CSRF\)](#)
- 5 - [Improper Access Control \(Authorization\)](#)
- 6 - [Reliance on Untrusted Inputs in a Security Decision](#)
- 7 - [Path Traversal](#)
- 8 - [Unrestricted Upload of Dangerous File Type](#)
- 9 - [OS Command Injection](#)
- 10 - [Missing Encryption of Sensitive Data](#)
- 11 - [Hardcoded Credentials](#)
- 12 - [Buffer Access with Incorrect Length Value](#)
- 13 - [PHP File Inclusion](#)
- 14 - [Improper Validation of Array Index](#)
- 15 - [Improper Check for Unusual or Exceptional Conditions](#)
- 16 - [Information Exposure Through an Error Message](#)
- 17 - [Integer Overflow Or Wraparound](#)
- 18 - [Incorrect Calculation of Buffer Size](#)
- 19 - [Missing Authentication for Critical Function](#)
- 20 - [Download of Code Without Integrity Check](#)

**Build Security into Your Applications**  
Secure Coding Training and Certification for Java, .NET, and C/C++

Search for:

**CATEGORIES**

- Net (2)
- Authentication (3)
- Clickjacking (1)
- Database (2)
- defense (9)
- DoS (1)
- encryption (2)
- honeypot (2)
- ipv6 (1)
- Pentest (3)
- php (5)
- Sessions (4)
- Top25 (26)
- Uncategorized (26)

# Questions?

- Comments, criticism, questions welcome  
[cwe@mitre.org](mailto:cwe@mitre.org)

## Changes from 1.4 (May 2009) to 1.9 (June 2010)

