Common Weakness Enumeration

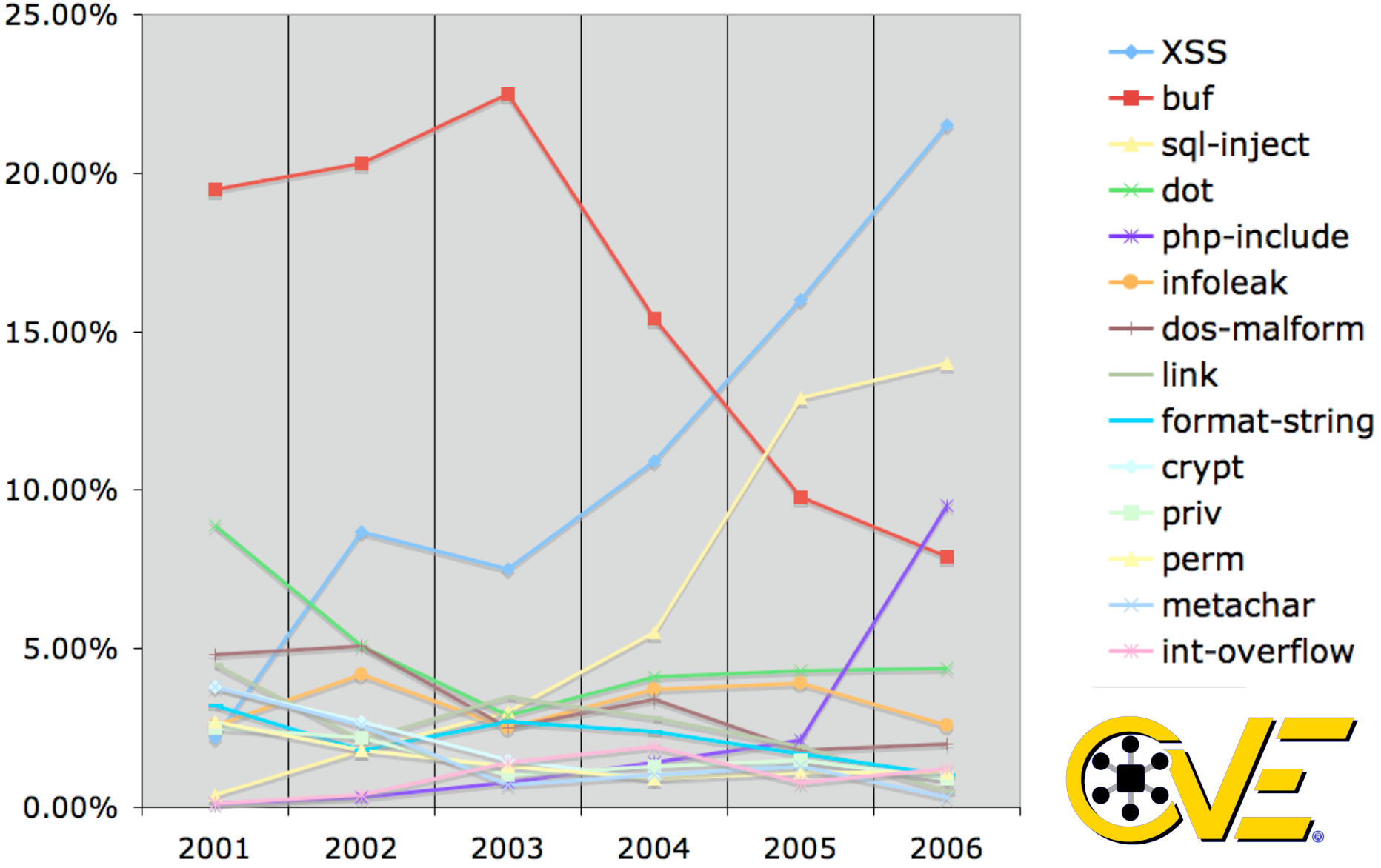
9 May 2007

Robert A. Martin

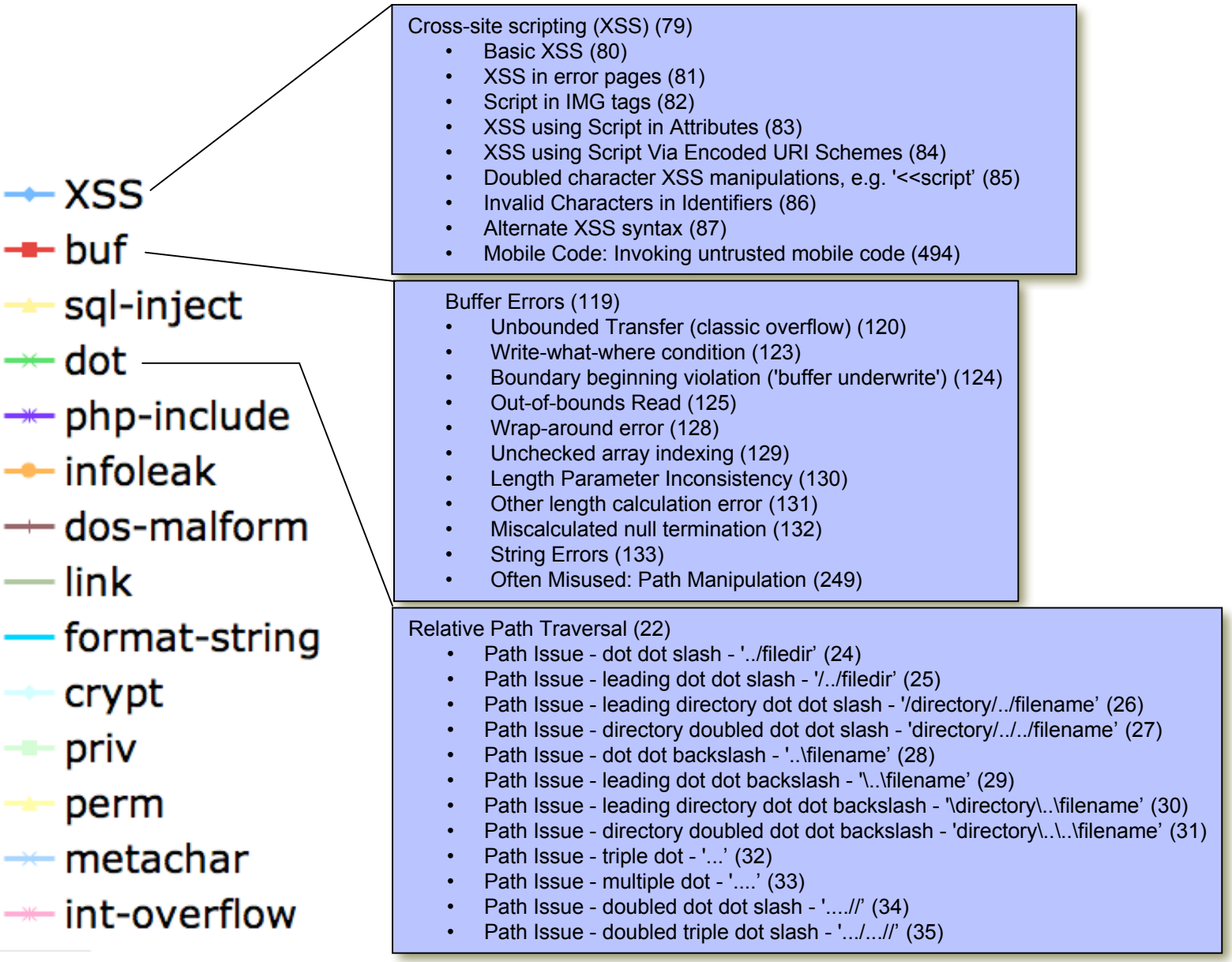
Making Security Measurable™

MITRE

Vulnerability Type Trends: A Look at the CVE List (2001 - 2006)

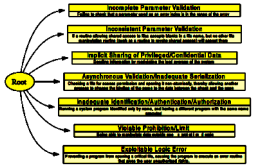


Removing and Preventing the Vulnerabilities Requires More Specific Definitions…CWEs

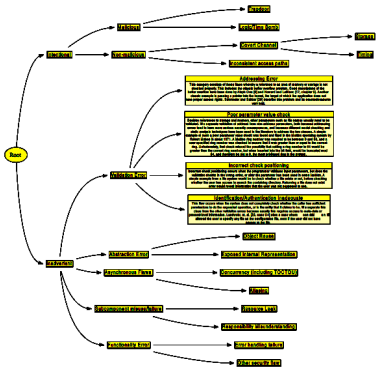


Protection Analysis

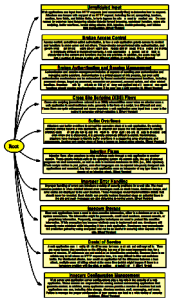
RISOS



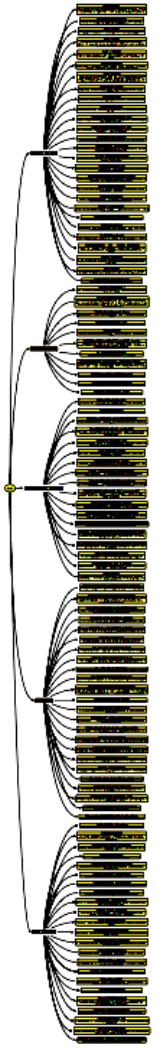
Weber



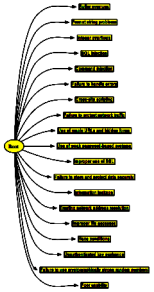
OWASP



CLASP

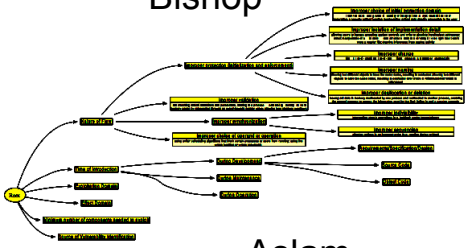


Microsoft



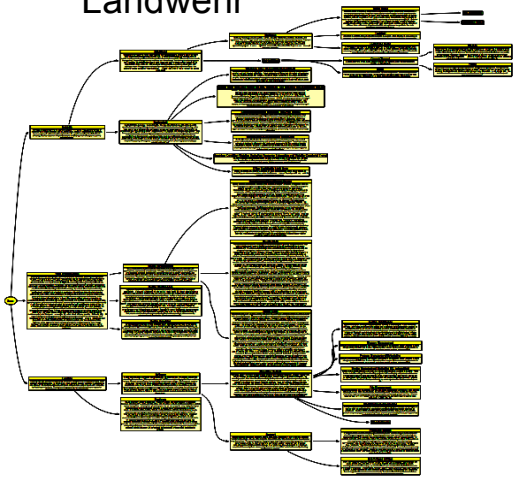
PLOVER

Bishop

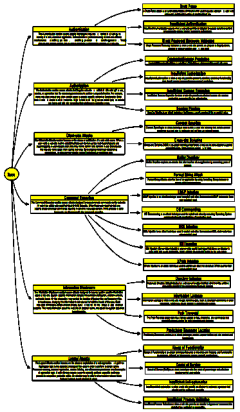


Aslam

Landwehr

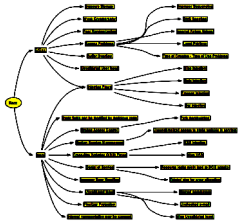


WASC

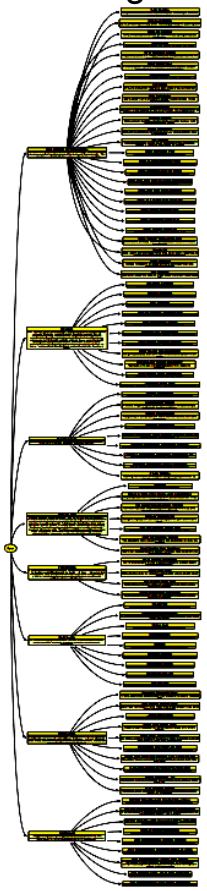


Tool B

Tool A



7 Kingdoms



Current Community Contributing to the Common Weakness Enumeration

- AppSIC
- Booz Allen Hamilton Inc.
- Cenzic
- CERIAS/Purdue University
- CERT/CC
- Cigital
- CodescanLabs
- Core Security
- Coverity
- Fortify
- Gramma Tech
- IBM Interoperability Clearing House
- JHU/APL
- JMU
- Kestrel Technology
- KDM Analytics
- Klocwork
- McAfee/Foundstone
- Microsoft
- MIT Lincoln Labs
- MITRE
- North Carolina State University
- NIST
- NSA
- Oracle
- Ounce Labs
- OWASP
- Palamida
- Parasoft
- PolySpace Technologies
- proServices Corporation
- SANS Institute
- SecurityInnovation
- Secure Software
- Security University
- Semantic Designs
- SofCheck
- SPI Dynamics
- SureLogic, Inc.
- UNISYS
- VERACODE
- Watchfire
- WASC
- Whitehat Security, Inc.
- Tim Newsham

Making Security Measurable™

To join send e-mail to cwe@mitre.org

Using A Unilateral NDA with MITRE to Bring in Info

Purpose:

- Sharing the proprietary/company confidential information contained in the underlying Knowledge Repository of the Knowledge Owner's Capability for the sole purpose of establishing a public Common Weakness Enumeration (CWE) dictionary that can be used by vendors, customers, and researchers to describe software, design, and architecture related weaknesses that have security ramifications.
- The individual contributions from numerous organizations, based on their proprietary/company-confidential information, will be combined into a consolidated collection of weakness descriptions and definitions with the resultant collection being shared publicly.
- The consolidated collection of knowledge about weaknesses in software, design, and architecture will make no reference to the source of the information used to describe, define, and explain the individual weaknesses.

CWE-79 Cross-site scripting (XSS)

[cwe.mitre.org/data/definition/79.html]

Individual CWE Dictionary Definition (Draft 6)

Search by ID

Cross-site scripting (XSS)

CWE ID	79
Description	Cross-site scripting weakness occurs when dynamically generated web pages display input, such as login information, that is not properly validated, allowing an attacker to embed malicious scripts into the generated page and then execute the script on the machine of any user that views the site. If successful, Cross-site scripting vulnerabilities can be exploited to manipulate or steal cookies, create requests that can be mistaken for those of a valid user, compromise confidential information, or execute malicious code on the end user systems for a variety of nefarious purposes.
Alternate Terms	"CSS" was once used as the acronym for this problem, but this can cause confusion with the "Cascading Style Sheets," so its use has declined significantly, and its use is discouraged by the author.
Likelihood of Exploit	High to Very High
Weakness Ordinality	Resultant (Weakness is typically related to the presence of some other Weaknesses)
Causal Nature	Explicit (This is an explicit weakness resulting from behavior of the developer)
Common Consequences	Confidentiality: The most common attack p… information stored in user cookies. Access control: In some circumstances it m… when cross-site scripting is combined with …
Potential Mitigations	Carefully check each input parameter again… specific characters and format allowed. All i… supposed to specify, but all data in the requ… so forth. A common mistake that leads to c… expected to be redisplayed by the site. We … application server or the application that th… currently reflected may be used by a future… is recommended. This involves "HTML Entity Encoding" all no… the user and is now being written to the re… With Struts, you should write all data from … Additionally, to help mitigate XSS attacks a… HttpOnly. In browsers that support the Htt… prevents the user's session cookie from bei… to a XSS attack.
Demonstrative Examples	The following JSP code segment reads an er… user. **JSP Example:** <% String eid = request.getParameter("eid"

Section Contents
- CWE List
  - Full Dictionary View
  - Classification Tree
  - Leaf Nodes
  - Other Views
- Other Items of Interest
  - Sources

References	M. Howard and D. LeBlanc. "Writing Secure Code". 2nd Edition. Microsoft. 2003.
Node Relationships	ChildOf - Injection (74) ResultsIn - Mobile Code: Invoking untrusted mobile code (494) ParentOf - Basic XSS (80) ParentOf - XSS in error pages (81) ParentOf - Script in IMG tags (82) ParentOf - XSS using Script in Attributes (83) ParentOf - XSS using Script Via Encoded URI Schemes (84) ParentOf - Doubled character XSS manipulations, e.g. '<<script' (85) ParentOf - Invalid Characters in Identifiers (86) ParentOf - Alternate XSS syntax (87)
Source Taxonomies	PLOVER - Cross-site scripting (XSS) 7 Pernicious Kingdoms - Cross-site Scripting CLASP - Cross-site scripting
Applicable Platforms	C C++ Java .NET SOAP

BACK TO TOP

Making Security Measurable™

Building Consensus About A Common Enumeration

Previously Published Vulnerability Taxonomy Work

CVE-based PLOVER Work

GMU, Stanford, IBM, SEI, VERACODE, NSA/CTC, UC Berkeley, Purdue, JMU, Coverity, SPI Dynamics, Core Security, Kestrel Technology, Parasoft, MIT LL, Watchfire, Unisys, Security Institute, Oracle, Cenzic, KDM Analytics, UMD, NCSU

Cigital's Gary McGraw's Work and Taxonomy

OWASP's Checklist and Taxonomy

Secure Software's John Viega's CLASP and Taxonomy

Fortify's Brian Chess's Work and Taxonomy

Microsoft's Mike Howard's Work and Taxonomy

Gramma Tech's Checklist and Taxonomy

Ounce Lab's Taxonomy

Klocwork's Checklist and Taxonomy

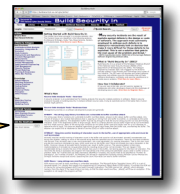
CVE and NVD using CWEs

Dictionary

Common Weakness Enumeration (CWE)

- call & count the same
  - enable metrics

DHS's BSI Web site



DHS's SwA CBK

SEI CERT Secure Coding Standards Effort

SANS National Secure Programming Skills Assessment

Center for Assured SW

OMG OBJECT MANAGEMENT GROUP SwA SIG

OWASP & WASC

CWE Compatibility

List of CWEs that a Tool finds

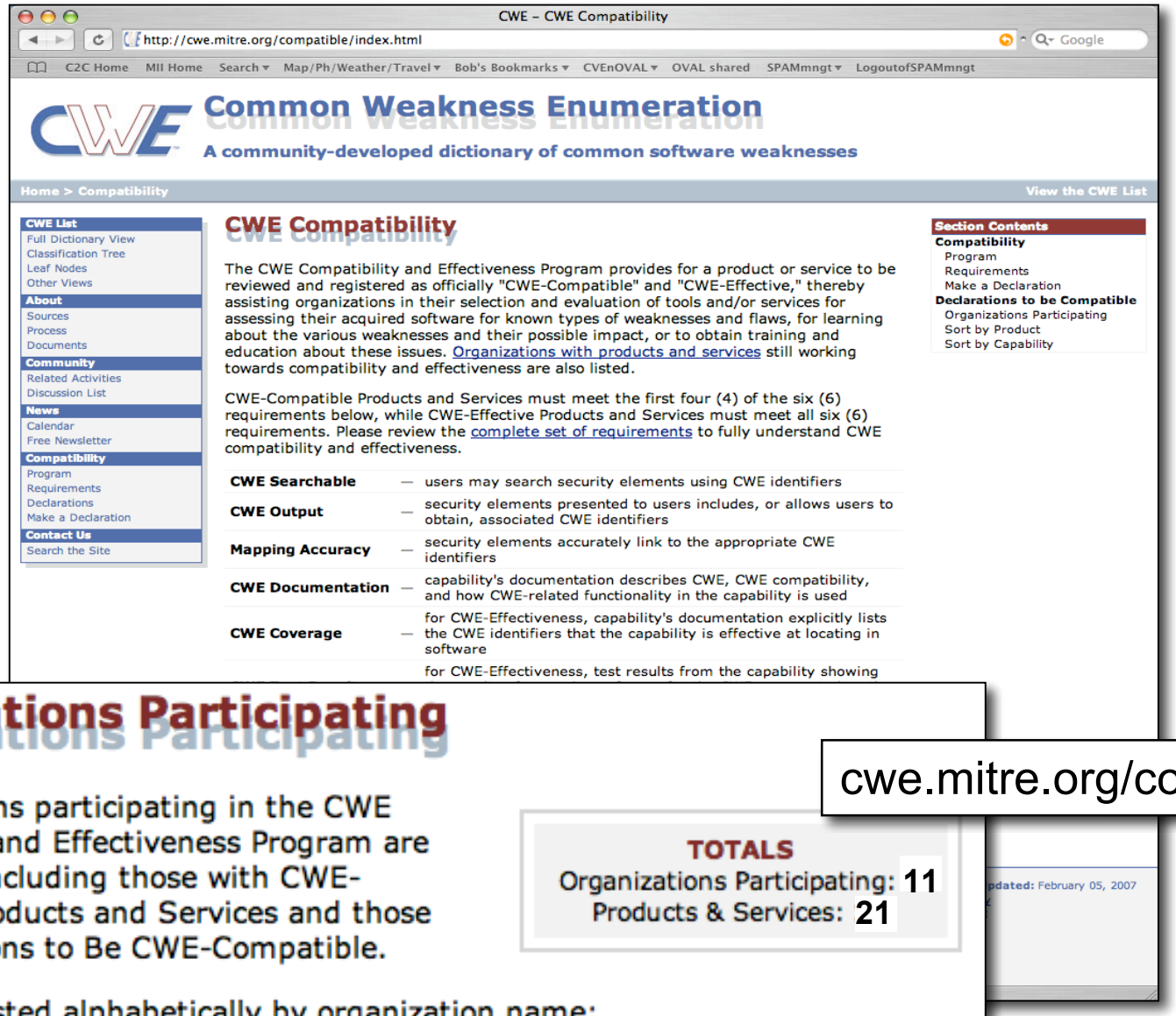
DHS/NIST SAMATE Tool Assessment

Reference Dataset

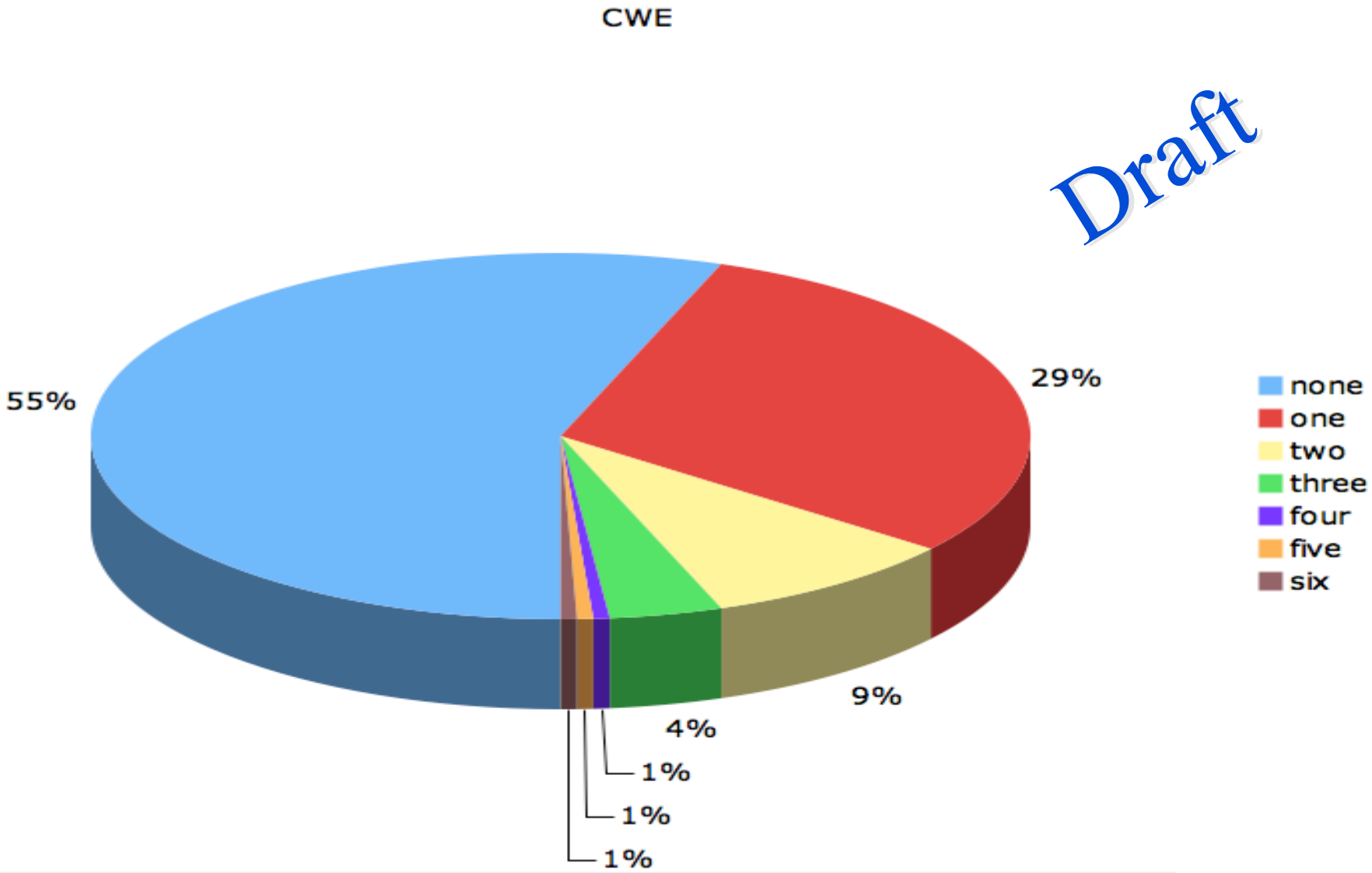
Reference Dataset

CWE Compatibility & Effectiveness Program

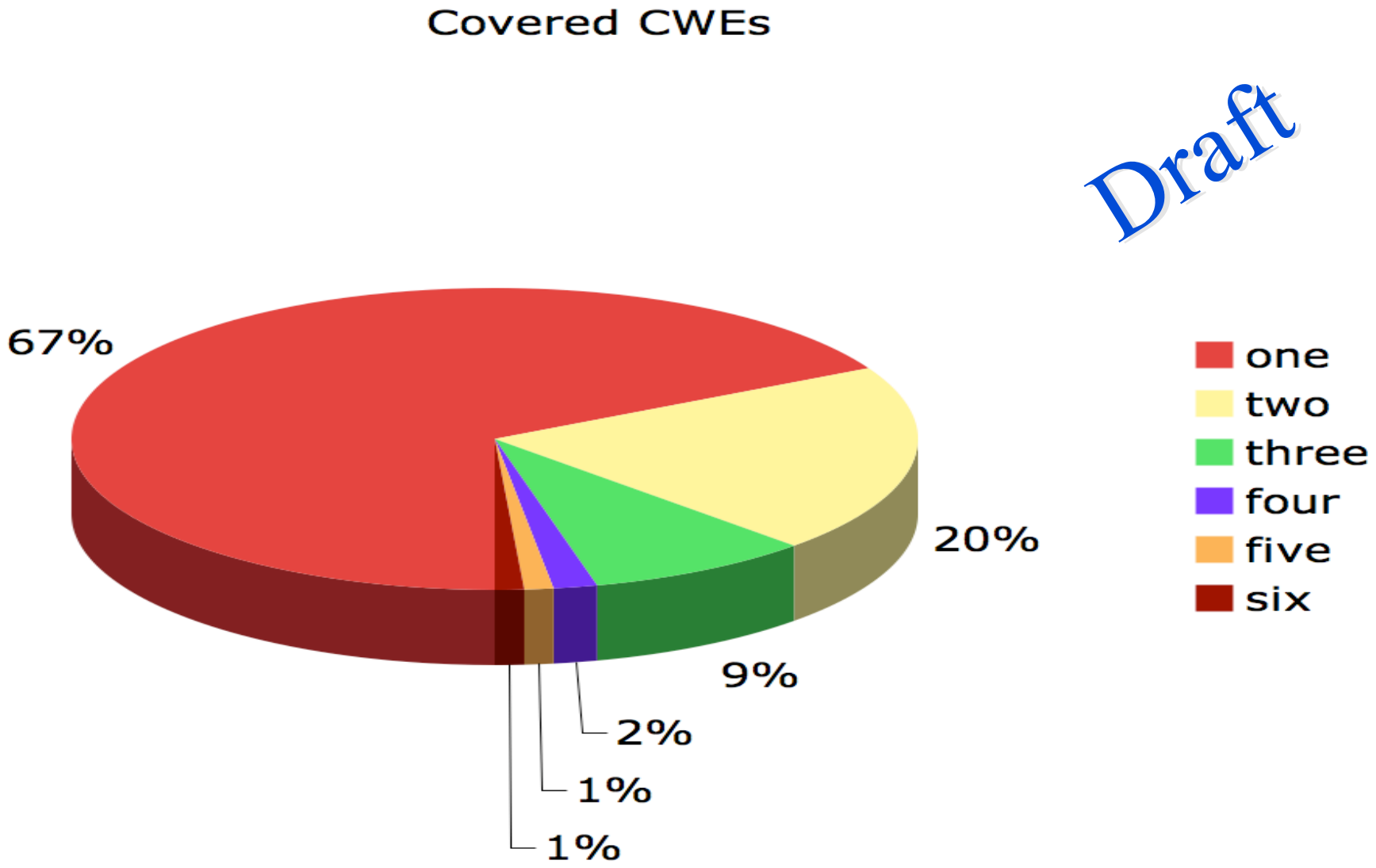
(launched Feb 2007)



Coverage of CWE



Covered CWEs - By Number of Tools



What are the Building Blocks of a "Security Architecture"

- Standard ways for enumerating "things we care about"
- Languages for encoding high fidelity information about how to find the "things we care about"
- Repositories of content in languages for use in communities or individual organizations
- Adoption/branding and vetting programs to encourage adoption by tools and services

Making Security Measurable™

The Building Blocks Are:

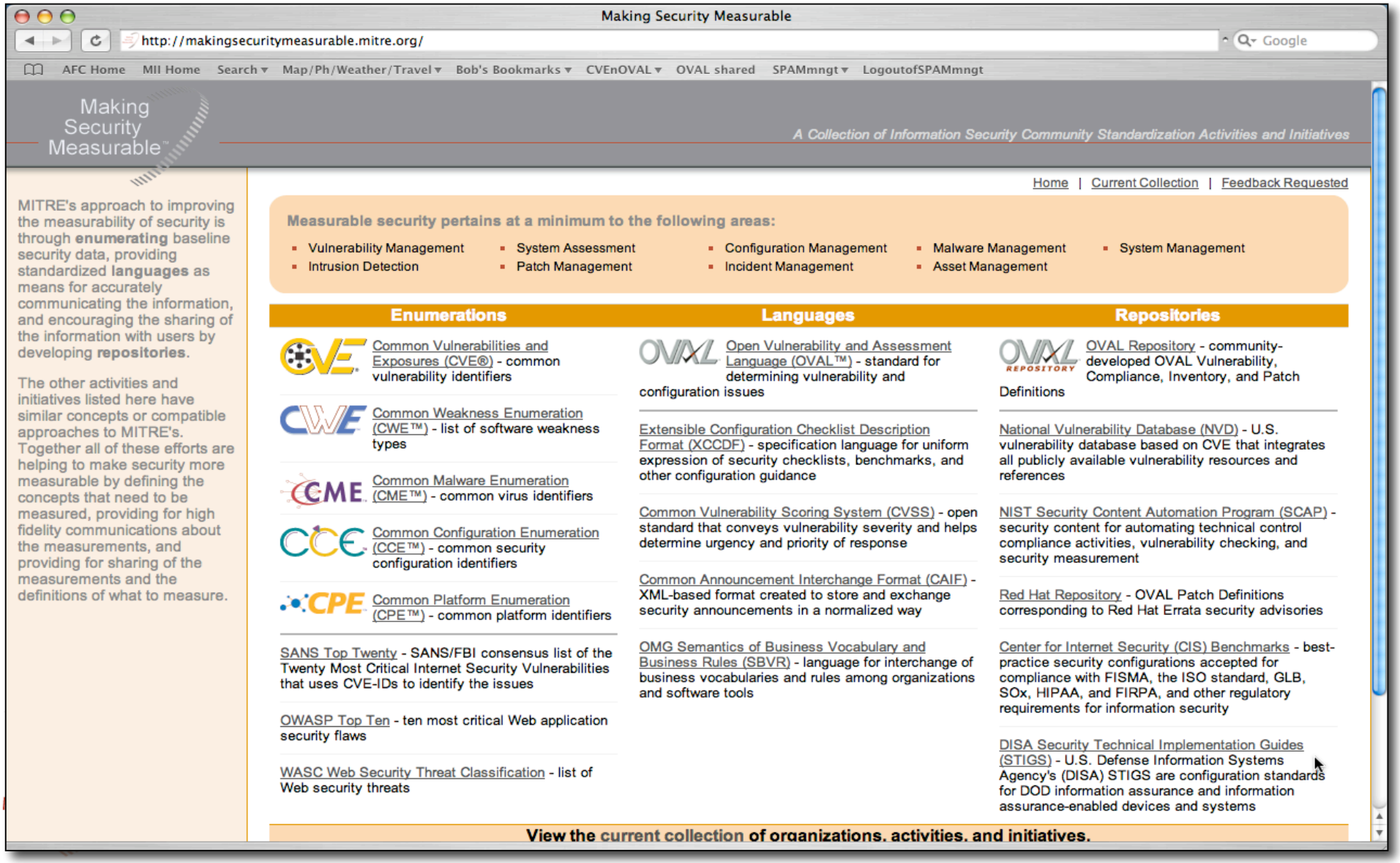
- Enumerations
  - Catalog the fundamental entities in IA, Cyber Security, and Software Assurance
    - Vulnerabilities (CVE), misconfigurations (CCE), software packages (CPE), malware (CME), attack patterns (CAPEC), weaknesses in code/design/architecture (CWE)
- Languages/Formats
  - Support the creation of machine-readable state assertions, assessment results, and messages
    - Configuration/vulnerability/patch/asset patterns (XCCDF & OVAL), software security patterns (SBVR), event patterns (CEE), malware patterns (MAEC), risk of a vulnerability (CVSS), information messages (CAIF & *DEF)
- Knowledge Repositories
  - Packages of assertions supporting a specific application
    - Vulnerability advisories & alerts, (US-CERT Advisories/IAVAs), configuration assessment (NIST Checklists, CIS Benchmarks, NSA Configuration Guides, DISA STIGS), asset inventory (NIST/DHS NVD), code assessment & certification (NIST SAMATE, DoD DIACAP & eMASS)

Tools

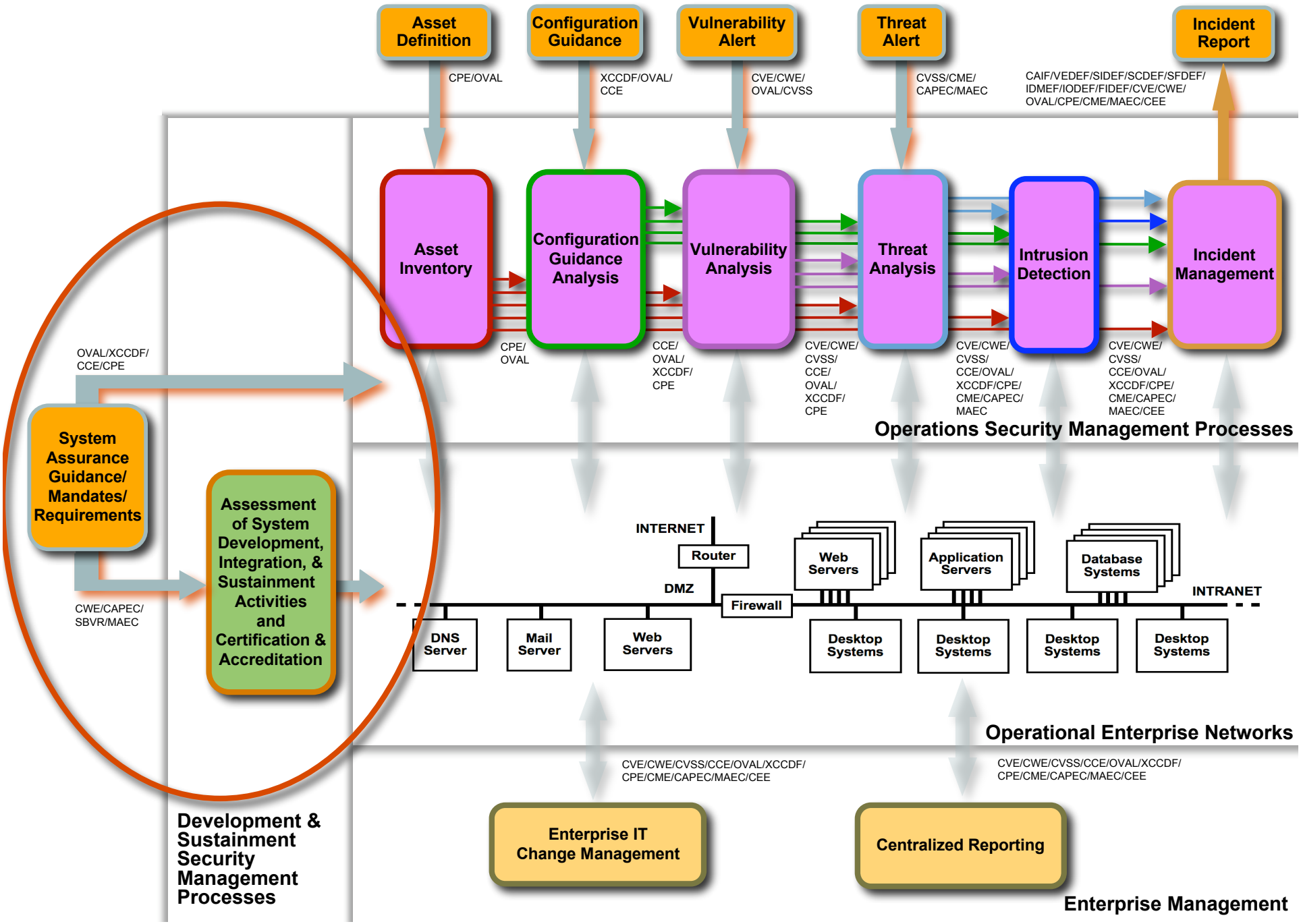
- Interpret IA, Cyber Security, and SwA content in context of enterprise network
- Methods for assessing compliance to languages, formats, and enumerations

Making Security Measurable™

For More Information
[makingsecuritymeasurable.mitre.org]



Knowledge Repositories



OVAL/XCCDF/
CCE/CPE

System Assurance Guidance/ Mandates/ Requirements

CWE/CAPEC/
SBVR

Certification & Assessment of System Development, Integration, & Sustainment Activities