sans.org

CWE/SANS TOP 25 Most Dangerous Software Errors

12-16 minutes

What Errors Are Included in the Top 25 Software Errors?

The Top 25 Software Errors are listed below in three categories:

- Software Error Category: Insecure Interaction Between Components (6 errors)
- Software Error Category: Risky Resource Management (8 errors)
- Software Error Category: Porous Defenses (11 errors)

Click on the CWE ID in any of the listings and you will be directed to the relevant spot in the MITRE CWE site where you will find the following:

- Ranking of each Top 25 entry,
- Links to the full CWE entry data,
- Data fields for weakness prevalence and consequences,
- Remediation cost,
- Ease of detection,
- Code examples,

- Detection Methods,
- Attack frequency and attacker awareness
- Related CWE entries, and
- Related patterns of attack for this weakness.

Each entry at the Top 25 Software Errors site also includes fairly extensive prevention and remediation steps that developers can take to mitigate or eliminate the weakness.

Archive

- View the Top 25 Software Errors for **2010** Here
- View the Top 25 Software Errors for **2009** Here

Insecure Interaction Between Components

These weaknesses are related to insecure ways in which data is sent and received between separate components, modules, programs, processes, threads, or systems.

CWE ID	Name
CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
CWE-434	Unrestricted Upload of File with Dangerous Type
CWE-352	Cross-Site Request Forgery (CSRF)

CWE ID	Name
CWE-601	URL Redirection to Untrusted Site ('Open Redirect')

Risky Resource Management

The weaknesses in this category are related to ways in which software does not properly manage the creation, usage, transfer, or destruction of important system resources.

CWE ID	Name
CWE-120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
CWE-494	Download of Code Without Integrity Check
CWE-829	Inclusion of Functionality from Untrusted Control Sphere
CWE-676	Use of Potentially Dangerous Function
CWE-131	Incorrect Calculation of Buffer Size
CWE-134	Uncontrolled Format String
CWE-190	Integer Overflow or Wraparound

Porous Defenses

The weaknesses in this category are related to defensive techniques that are often misused, abused, or just plain ignored.

CWE ID	Name
CWE-306	Missing Authentication for Critical Function
CWE-862	Missing Authorization

CWE ID	Name
CWE-798	Use of Hard-coded Credentials
CWE-311	Missing Encryption of Sensitive Data
CWE-807	Reliance on Untrusted Inputs in a Security Decision
CWE-250	Execution with Unnecessary Privileges
CWE-863	Incorrect Authorization
CWE-732	Incorrect Permission Assignment for Critical Resource
CWE-327	Use of a Broken or Risky Cryptographic Algorithm
CWE-307	Improper Restriction of Excessive Authentication Attempts
CWE-759	Use of a One-Way Hash without a Salt

Resources to Help Eliminate The Top 25 Software Errors

1. SANS Application Security Courses

   The SANS application security curriculum seeks to ingrain security into the minds of every developer in the world by providing world-class educational resources to design, develop, procure, deploy, and manage secure software. The application security faculty are real-world practitioners with decades of application security experience. The concepts covered in our courses will be applicable to your software security program the day you return to work:

- DEV522: Defending Web Applications Security Essentials
- DEV534: Secure DevOps: A Practical Introduction
- DEV540: Secure DevOps & Cloud Application Security

- DEV541: Secure Coding in Java / JEE
- DEV544: Secure Coding in .NET

  SANS maintains an Application Security CyberTalent Assessment that measures secure coding skills and allow programmers to determine gaps in their knowledge of secure coding and allows buyers to ensure outsourced programmers have sufficient programming skills. Organizations can learn more at https://www.sans.org/cybertalent/assessment-detail?msc=top25hp#appsec.

2. Developer Security Awareness Training

   The SANS Security Awareness Developer product provides pinpoint software security awareness training on demand, all from the comfort of your desk. Application security awareness training includes over 30+ modules averaging 7-10 minutes in length to maximize learner engagement and retention. The modules cover the full breadth and depth of topics for PCI Section 6.5 compliance and the items that are important for secure software development.

3. The TOP 25 Errors List will be updated regularly and will be posted at both the **SANS and MITRE sites**
   CWE Top 25 Software Errors Site

   MITRE maintains the CWE (Common Weakness Enumeration) web site, with the support of the US Department of Homeland Security's National Cyber Security Division, presenting detailed descriptions of the top 25 Software errors along with authoritative guidance for mitigating and avoiding them. That site also contains data on more than 700 additional Software errors,

design errors and architecture errors that can lead to exploitable vulnerabilities. CWE Web Site

4. **SAFECode** - The Software Assurance Forum for Excellence in Code (members include EMC, Juniper, Microsoft, Nokia, SAP and Symantec) has produced two excellent publications outlining industry best practices for software assurance and providing practical advice for implementing proven methods for secure software development.

   Fundamental Practices for Secure Software Development 2nd Edition
   http://www.safecode.org/publications/SAFECode_Dev_Practices0211.pdf

   Overview of Software Integrity Controls
   http://www.safecode.org/publications/SAFECode_Software_Integrity_Controls0610.pdf

   Framework for Software Supply Chain Integrity
   http://www.safecode.org/publications/SAFECode_Supply_Chain0709.pdf

   Fundamental Practices for Secure Software Development
   http://www.safecode.org/publications/SAFECode_Dev_Practices1108.pdf

   Software Assurance: An Overview of Current Industry Best Practices
   http://www.safecode.org/publications/SAFECode_BestPractices0208.pdf

5. Software Assurance Community Resources Site and DHS web sites

As part of DHS risk mitigation efforts to enable greater resilience of cyber assets, the Software Assurance Program seeks to reduce software vulnerabilities, minimize exploitation, and address ways to routinely acquire, develop and deploy reliable and trustworthy software products with predictable execution, and to improve diagnostic capabilities to analyze systems for exploitable weaknesses.

6. Nearly a dozen software companies offer automated tools that test programs for these errors.
7. New York State has produced draft procurement standards to allow companies to buy software with security baked in.

   If you wish to join the working group to help improve the procurement guidelines you can go to the New York State Cyber Security and Critical Infrastructure Coordination web site.

   Draft New York State procurement language will be posted at SANS Application Security Contract.

   For additional information on any of these:
   SANS: Mason Brown, mbrown@sans.org
   MITRE: Bob Martin, ramartin@mitre.org
   MITRE: Steve Christey, coley@mitre.org

   Contributors to the "CWE/SANS Top 25 Most Dangerous Software Errors":

- Mark J. Cox Red Hat Inc.
- Carsten Eiram Secunia (Denmark)
- Pascal Meunier CERIAS, Purdue University

- Razak Ellafi & Olivier Bonsignour CAST Software
- David Maxwell NetBSD
- Cassio Goldschmidt & Mahesh Saptarshi Symantec Corporation
- Chris Eng Veracode, Inc.
- Paul Anderson Grammatech Inc.
- Masato Terada Information-Technology Promotion Agency (IPA) (Japan)
- Bernie Wong IBM
- Dennis Seymour Ellumen, Inc.
- Kent Landfield McAfee
- Hart Rossman SAIC
- Jeremy Epstein SRI International
- Matt Bishop UC Davis
- Adam Hahn & Sean Barnum MITRE
- Jeremiah Grossman White Hat Security
- Kenneth van Wyk KRvW Associates
- Bruce Lowenthal Oracle Corporation
- Jacob West Fortify Software, an HP Company
- Frank Kim ThinkSec
- Christian Heinrich (Australia)
- Ketan Vyas Tata Consultancy Services (TCS)
- Joe Baum Motorola Solutions

- Matthew Coles, Aaron Katz & Nazira Omuralieva RSA, the Security Division of EMC
- National Security Agency (NSA) Information Assurance Division
- Department of Homeland Security (DHS) National Cyber Security Division

The following individuals and organizations aided in the development of the Top 25 through their input to the CWSS/CWRAF

CWSS / CWRAF

- Bruce Lowenthal Oracle
- Damir (Gaus) Rajnovic Cisco
- Stephen Chasko
- Chris Eng and Chris Wysopal Veracode
- Casper Jones
- Edward Luck and Martin Tan Dimension Data (Australia)
- James Jardine Jardine Software
- Jon Zucker Cenzic
- Jason Liu Northrop Grumman
- Ory Segal IBM
- Mahi Dontamsetti DTCC
- Hart Rossman SAIC
- OWASP

- EC-Council

How Important Are the Top 25 Software Errors?

We asked several of the participants why they thought this effort was important enough to merit a significant amount of their time and expertise. Here are a few of their answers. More are at the end of the announcement.

> "Just wanted to commend the depth of the CWE/SANS Top 25. The code examples are particularly excellent. I have asked all my developers to read one of these each day for the next 25 days. I'm taking my own advice as well, and even though I'm still reading some of the "easy" ones (like SQL injection), I still find that I am learning new things about old topics."
>
> -- Mark E. Haase, OpenFISMA Project Manager, Endeavor Systems, Inc.

> "Your document (2009 CWE/SANS Top 25 Most Dangerous Software Errors) is very useful. I would like to publish it on our intranet, for illustrating threats and vulnerabilities about coding."
>
> -- colonel Jean-Michel HOUBRE, from the french MOD.

> "We included the top25 reference in a request for bid last year. Project began in December and expect the project to be complete in October 2010. We are hopeful to have a much more secure and better application due to the reference and utilization of the SANS/MITRE Top 25."
>
> -- Richard Lemons, WV Department of Health and Human Resources

> "In the collaborated environment and ever increasing business requirements to integrate solutions, insecure applications are an easy target. The business today understands how much damage can be cause to business, revenue and customer confidence due to these issues. To ensure that our deliveries meet / surpass customer expectations on security, the CWE/SANS Top 25 Most Dangerous Software Errors is extensively leveraged in our software security assurance process."
>
> -- Ketan Vyas, Head Application Security Initiative, Tata Consultancy Services

> "I've read "2009 CWE/SANS Top 25 Most Dangerous Software Errors" article and found it very useful. I would like to translate it into Russian for our software testing community. Of course, link to original article will be stored."
>
> -- Alexander Kozyrev

> "The Top 25 provides much needed guidance for software developers focusing on eliminating software security defects in their products. If you're involved with software development at your organization and are looking to improve your product security posture, you need to read this."
>
> -- Robert Auger, Co Founder of The Web Application Security Consortium

> "The CWE/SANS Top 25 list provides a great starting point for developers who want to write more secure code. The majority of the flaw types of the most severe vulnerabilities that Red Hat fixed in 2009 are discussed in this document."
>
> -- Mark J. Cox, Director, Security Response, Red Hat.

> "The 2010 CWE/SANS Top 25 Software Errors provides valuable guidance to organizations engaged in the development or deployment of software. This list helps organizations focus on the most dangerous threats so that they can get the most out of their vulnerability reduction effort. The list can also be used as a framework to define short term and longer term programs for the elimination or mitigation of security vulnerabilities. Furthermore, it provides easy to comprehend description of the classes of vulnerabilities and high-level recommendations for mitigating or avoiding them altogether. This list is definitely a must-read for anyone who wishes to develop reasonably secure code."
>
> -- Bruce Lowenthal, Director Security Alert, Oracle Corp.

> "It's great to see the CWE/SANS Top 25 list continue to be maintained and mature. Relentlessly spreading the word about the most common security defects in programming is a vital need. The state of security in our software would without a doubt be much improved if everyone who touches software development reads and thoroughly understands this. Kudos."
>
> -- Kenneth R. van Wyk, KRvW Associates, LLC

Version 3.0 Updated June 27, 2011