CWE/Sans Top 25 Most Dangerous Programming Errors

Jan 2009

Top 25 Errors

- The Common Weakness Enumeration (CWE) is a formal list of software weakness types and is sponsored by the US Department of Homeland Security's National Cyber Security Division
- The SANS (SysAdmin, Audit, Network, Security) Institute was established in 1989 as a cooperative research and education organization
- Source: http://www.sans.org/top25errors/

Contributors

- Robert C. Seacord, CERT
- Pascal Meunier, CERIAS, Purdue University
- Matt Bishop, University of California, Davis
- Kenneth van Wyk, KRvW Associates
- Masato Terada, Information-Technology Promotion Agency (IPA), (Japan)
- Sean Barnum, Cigital, Inc.
- Mahesh Saptarshi and Cassio Goldschmidt, Symantec Corporation
- Adam Hahn, MITRE
- Jeff Williams, Aspect Security
- Carsten Eiram, Secunia
- Josh Drake, iDefense Labs at VeriSign, Inc.
- Chuck Willis, MANDIANT
- Michael Howard, Microsoft
- Bruce Lowenthal, Oracle Corporation
- Mark J. Cox, Red Hat Inc.
- Jacob West, Fortify Software
- Djenana Campara, Hatha Systems
- James Walden, Northern Kentucky University
- Frank Kim, ThinkSec
- Chris Eng and Chris Wysopal, Veracode, Inc.
- Ryan Barnett, Breach Security
- Antonio Fontes, New Access SA, (Switzerland)
- Mark Fioravanti II, Missing Link Security Inc.
- Ketan Vyas, Tata Consultancy Services (TCS)
- Lindsey Cheng, Ian Peters and Tom Burgess, Secured Sciences Group, LLC
- Hardik Parekh and Matthew Coles, RSA - Security Division of EMC Corporation Mouse
- Ivan Ristic Apple Product Security
- Software Assurance Forum for Excellence in Code (SAFECode)
- Core Security Technologies Inc.
- Depository Trust & Clearing Corporation (DTCC)

Kudos

- National Security Agency's Information Assurance Directorate
  - "The publication of a list of programming errors that enable cyber espionage and cyber crime is an important first step in managing the vulnerability of our networks and technology. There needs to be a move away from reacting to thousands of individual vulnerabilities, and to focus instead on a relatively small number of software flaws that allow vulnerabilities to occur, each with a general root cause. Such a list allows the targeting of improvements in software development practices, tools, and requirements to manage these problems earlier in the life cycle, where they can be solved on a large scale and cost-effectively.“
  - Tony Sager, National Security Agency's Information Assurance Directorate

Kudos

- Microsoft:
  - "The 2009 CWE/SANS Top 25 Programming Errors project is a great resource to help software developers identify which security vulnerabilities are the most important to understand, prevent and fix.“
  - Michael Howard, Principal Security Program Manager, Security Development Lifecycle Team, Microsoft Corp.
- Symantec:
  - "The 2009 CWE/SANS Top 25 Programming Errors reflects the kinds of issues we've seen in application software and helps provide us with actionable direction to continuously improve the security of our software."
  - - Wesley H. Higaki, Director, Software Assurance, Office of the CTO, Symantec Corporation

Insecure Interaction Among Components

- CWE-20: Improper Input Validation
  - It's the number one killer of healthy software, so you're just asking for trouble if you don't ensure that your input conforms to expectations…
- CWE-116: Improper Encoding or Escaping of Output
  - Computers have a strange habit of doing what you say, not what you mean. Insufficient output encoding is the often-ignored sibling to poor input validation, but it is at the root of most injection-based attacks, which are all the rage these days...
- CWE-89: Failure to Preserve SQL Query Structure (aka 'SQL Injection')
  - If attackers can influence the SQL that you use to communicate with your database, then they can...

Insecure Interaction Among Components

- CWE-79: Failure to Preserve Web Page Structure (aka 'Cross-site Scripting')
  - Cross-site scripting (XSS) is one of the most prevalent, obstinate, and dangerous vulnerabilities in web applications...If you're not careful, attackers can...
- CWE-78: Failure to Preserve OS Command Structure (aka 'OS Command Injection')
  - When you invoke another program on the operating system, but you allow untrusted inputs to be fed into the command string that you generate for executing the program, then you are inviting attackers...
- CWE-319: Cleartext Transmission of Sensitive Information
  - If your software sends sensitive information across a network, such as private data or authentication credentials, that information crosses many...

Insecure Interaction Among Components

- CWE-352: Cross-Site Request Forgery (CSRF)
  - With cross-site request forgery, the attacker gets the victim to activate a request that goes to your site. Thanks to scripting and the way the web works in general, the user might not even be aware that the request is being sent. But once the request gets to your server, it looks as if it came from the user, not the attacker.
- CWE-362: Race Condition
  - Attackers will consciously look to exploit race conditions to cause chaos or get your application to cough up something valuable...
- CWE-209: Error Message Information Leak
  - If you use chatty error messages, then they could disclose secrets to any attacker who dares to misuse your software. The secrets could cover a wide range of valuable data...

Risky Resource Management

- CWE-119: Failure to Constrain Operations within the Bounds of a Memory Buffer
  - Buffer overflows are Mother Nature's little reminder of that law of physics that says if you try to put more stuff into a container than it can hold, you're...
- CWE-642: External Control of Critical State Data
  - There are many ways to store user state data without the overhead of a database. Unfortunately, if you store that data in a place where an attacker can access it...
- CWE-73: External Control of File Name or Path
  - When you use an outsider's input while constructing a filename, you're taking a chance. If you're not careful, an attacker could...

Risky Resource Management

- CWE-426: Untrusted Search Path
  - If a resource search path (e.g. path to JAR file) is under attacker control, then the attacker can modify it to point to resources of the attacker's choosing. This causes the software to access the wrong resources at the wrong time...
- CWE-94: Failure to Control Generation of Code (aka 'Code Injection')
  - For ease of development, sometimes you can't beat using a couple lines of code to employ lots of functionality. It's even cooler when the code is executed dynamically…
- CWE-494: Download of Code Without Integrity Check
  - You don't need to be a guru to realize that if you download code and execute it, you're trusting that the source of that code isn't malicious. But attackers can perform all sorts of tricks...

Risky Resource Management

- CWE-404: Improper Resource Shutdown or Release
  - When your precious system resources (e.g. allocated memory) have reached their end-of-life, you need to dispose of them correctly…
- CWE-665: Improper Initialization
  - Just as you should start your day with a healthy breakfast, proper initialization helps to ensure your attacker doesn't initialize your data for you…
- CWE-682: Incorrect Calculation
  - When attackers have some control over the inputs that are used in numeric calculations, this weakness can lead to vulnerabilities. It could cause you to make incorrect security decisions. It might cause you to...

Porous Defenses

- CWE-285: Improper Access Control (Authorization)
  - If you don't ensure that your software's users are only doing what they're allowed to, then attackers will try to exploit your improper authorization and...
- CWE-327: Use of a Broken or Risky Cryptographic Algorithm
  - You may be tempted to develop your own encryption scheme in the hopes of making it difficult for attackers to crack. This kind of grow-your-own cryptography is a welcome sight to attackers...
- CWE-259: Hard-Coded Password
  - Hard-coding a secret account and password into your software's authentication module is...

Porous Defenses

- CWE-732: Insecure Permission Assignment for Critical Resource
  - If you have critical programs, data stores, or configuration files with permissions that make your resources accessible to the world - well, that's just what they'll become...
- CWE-330: Use of Insufficiently Random Values
  - If you use security features that require good randomness, but you don't provide it, then you'll have attackers laughing all the way to the bank...

Porous Defenses

- CWE-250: Execution with Unnecessary Privileges
  - Spider Man, the well-known comic superhero, lives by the motto "With great power comes great responsibility." Your software may need special privileges to perform certain operations, but wielding those privileges longer than necessary can be extremely risky...
- CWE-602: Client-Side Enforcement of Server-Side Security
  - Remember that underneath that fancy GUI, it's just code. Attackers can reverse engineer your client and write their own custom clients that leave out certain inconvenient features like all those pesky security controls...