Carnegie Mellon University
Software Engineering Institute

# SCALe

## Evaluating Source Code for Adherence to Secure Coding Standards

**EXPERIENCE SHOWS THAT MOST SOFTWARE CONTAINS CODING FLAWS THAT LEAD TO VULNERABILITIES.** Static analysis tools produce a large number of alerts with high false-positive rates that an engineer must painstakingly examine to find legitimate flaws. Researchers in the SEI's CERT Division have developed SCALe—Source Code Analysis Laboratory—to help analysts be more efficient and effective at auditing source code for security flaws.

### What is SCALe?

Static analyzers can be used to look for source code flaws that might be exploitable. Each analyzer has unique strengths; no analyzer finds everything. Using multiple tools finds the most security flaws, but each analyzer also provides its own interface for managing its alerts, complicating attempts to use multiple analyzers on the same codebase. Static analyzers often have high false-positive rates and provide many alerts that are not related to security flaws.

SCALe consists of tools and processes developed by CERT researchers to address these problems. SCALe has been used to analyze software for the DoD, energy delivery systems, medical devices, and more.

### SCALe Auditing Framework

The SCALe auditing framework aggregates output from commercial, open source, and experimental analysis tools. These SCALe tools map warnings about possible code flaws (i.e., alerts) from code analysis tools to taxonomies of code flaws (e.g., CERT Secure Coding Rules and Common Weakness Enumeration [CWE]).

The tools provide a graphical interface that an analyst uses to filter and prioritize alerts as well as examine code associated with an alert. The analyst can also mark alert determinations (e.g., true or false) and store data for the audited code project. Some static analysis tool output formats are already integrated with the SCALe tools; the SCALe user manual explains the simple API that enables users to integrate new tools.

We provide the SCALe auditing framework tools to many DoD organizations and some non-DoD organizations for their use in evaluating their source code for adherence to secure coding standards. We provide services to help organizations adopt the SCALe auditing framework to improve their secure development lifecycle practices.

### SCALe Research Prototype

We create SCALe research prototypes by adding new, experimental functionality to the SCALe auditing framework and processes. For example, a research project may use different rules for determining which alerts to audit or which alert determination lexicon to use. These prototypes may be distributed to collaborators during a project; we often integrate innovative technologies and processes from the prototypes into SCALe. Recent research involving such prototypes focuses on adding machine learning to SCALe tools and processes.

### SCALe Conformance Testing

SCALe conformance testing provides organizations with an evaluation of their source code for its adherence to secure coding standards. We use the SCALe auditing framework and commercial, open source, and experimental analysis tools to provide this service. For each CERT secure coding standard, the source code for the software is certified at a level of conformance against the standard.

### The SCALe Conformance Process

Conformance testing motivates organizations to invest in developing conforming systems by testing code against CERT secure coding standards, verifying that code conforms with those standards, using the CERT seal, and maintaining a certificate registry of conforming systems. When you request SCALe conformance testing, the following process is initiated:

1. You submit your source code for analysis.
2. CERT staff examines the code using analyzer tools.
3. CERT staff validates and summarizes the results.
4. You receive a detailed report of findings to guide your repair of the source code.
5. You address the identified violations and resubmit the repaired code.
6. CERT staff reassesses the code to ensure that you mitigated all violations properly.
7. Your certification for that version of the product is published in a registry of certified systems.

## The CERT SCALe Seal

If CERT SCALe conformance testing determines that your software conforms to a secure coding standard, you may use the CERT SCALe seal.

The seal must be specifically tied to the software passing conformance testing and not applied to untested products or the organization. Use of the CERT SCALe seal is contingent upon (1) the organization entering into a service agreement with Carnegie Mellon University and (2) the software being designated by the CERT Division as conforming.

With some exceptions, modifications made to software after it is designated as conforming voids the conformance designation.

### CERT SCALe Certificates

CERT SCALe certificates contain the name and version of the software system that passed the conformance test and the results of the test. This process is similar to that followed by The Open Group.

Initially, all assessments are performed by researchers in the CERT Division of the Software Engineering Institute. In the future, third parties may be accredited to perform certifications.

## Related Research

Our research in machine learning, specifically alert classification and prioritization, is intended to help organizations secure their code more efficiently by using statistical methods to triage and prioritize static analysis alerts.

### Watch SCALe Videos

Our videos demonstrate the use of the SCALe auditing framework. Find them by searching for “SEI SCALe Videos” from your browser.

## About the CERT Division

The CERT® Division of Carnegie Mellon University’s Software Engineering Institute studies and solves problems with widespread cybersecurity implications, researches security vulnerabilities in software products, contributes to long-term changes in networked systems, and develops cutting-edge information and training to help improve cybersecurity.

## Contact Us

CARNEGIE MELLON UNIVERSITY
SOFTWARE ENGINEERING INSTITUTE
4500 FIFTH AVENUE; PITTSBURGH, PA 15213-2612

sei.cmu.edu
412.268.5800 | 888.201.4479
info@sei.cmu.edu