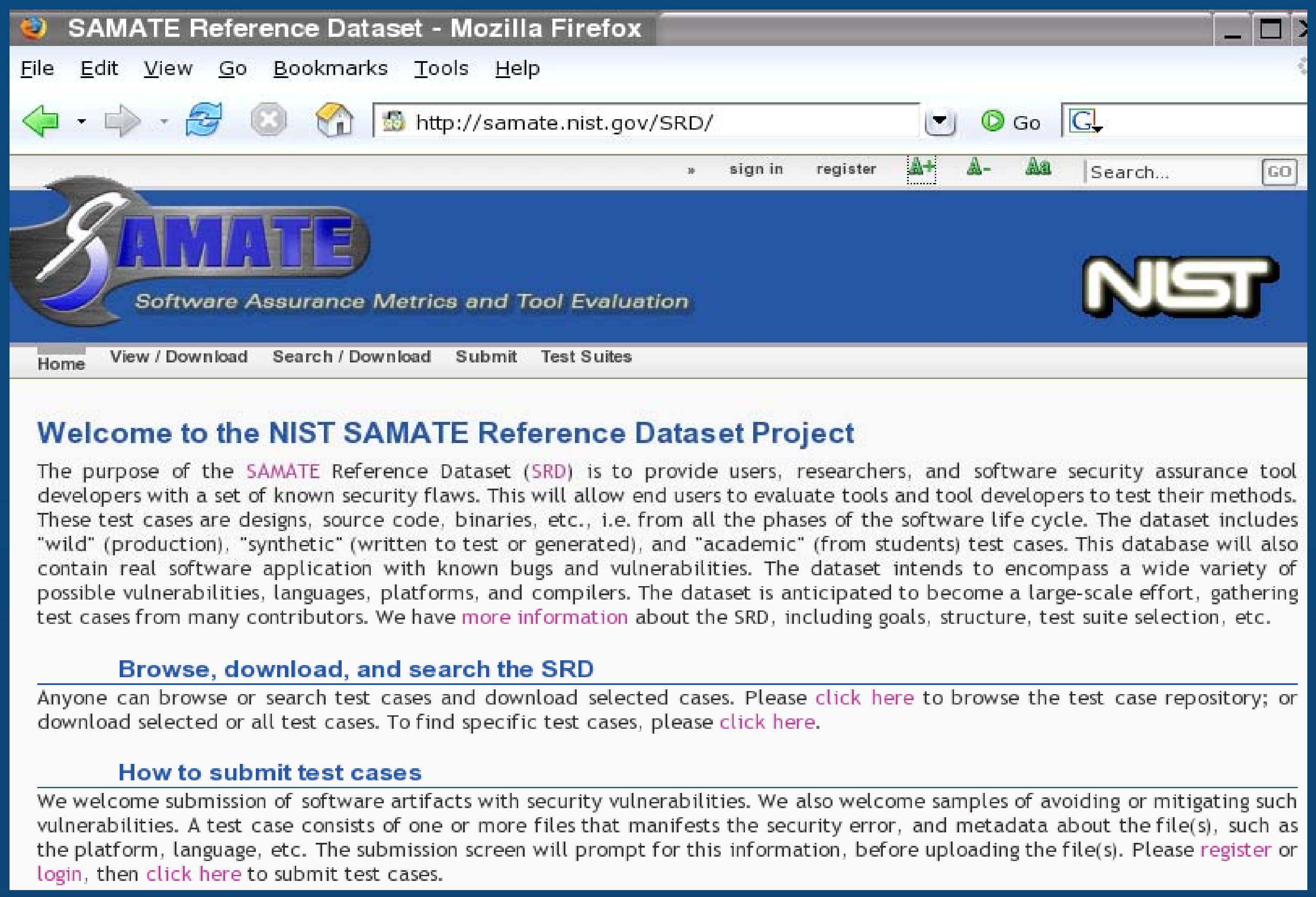
Preventing Website Hacking

Goal: Raise the level of software assurance (SA) in U.S.

Broad scope: The Software Assurance Metrics And Tool Evaluation (SAMATE) helps helps developers build better software, from OS to firewalls, SCADA to web services, source code security analyzers to correct-by-construction methods.

- ✓ Select classes of SA tools or methods, write specs, develop test procedures.
- ✓ Develop metrics for effectiveness of SA tools and methods.
- ✓ Identify gaps and develop R&D funding requirements and study proposals.
- ✓ Establish software reference dataset


SAMATE Reference Dataset - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://samate.nist.gov/SRD/
Go
» sign in register A+ A- Aa
Search...
GO
SAMATE
Software Assurance Metrics and Tool Evaluation
NIST
Home View / Download Search / Download Submit Test Suites

Welcome to the NIST SAMATE Reference Dataset Project

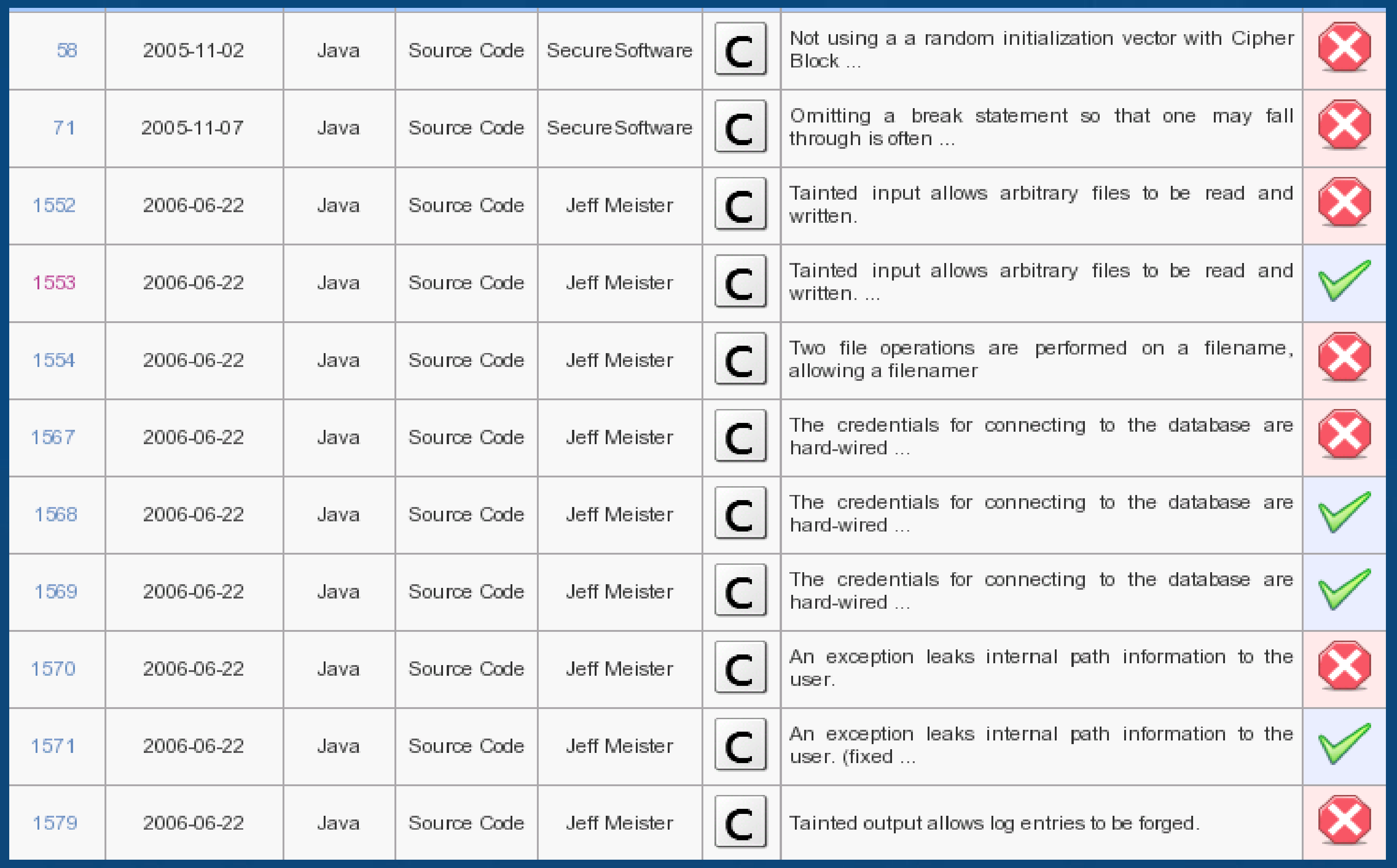
The purpose of the SAMATE Reference Dataset (SRD) is to provide users, researchers, and software security assurance tool developers with a set of known security flaws. This will allow end users to evaluate tools and tool developers to test their methods. These test cases are designs, source code, binaries, etc., i.e. from all the phases of the software life cycle. The dataset includes "wild" (production), "synthetic" (written to test or generated), and "academic" (from students) test cases. This database will also contain real software application with known bugs and vulnerabilities. The dataset intends to encompass a wide variety of possible vulnerabilities, languages, platforms, and compilers. The dataset is anticipated to become a large-scale effort, gathering test cases from many contributors. We have more information about the SRD, including goals, structure, test suite selection, etc.

Browse, download, and search the SRD

Anyone can browse or search test cases and download selected cases. Please click here to browse the test case repository; or download selected or all test cases. To find specific test cases, please click here.

How to submit test cases

We welcome submission of software artifacts with security vulnerabilities. We also welcome samples of avoiding or mitigating such vulnerabilities. A test case consists of one or more files that manifests the security error, and metadata about the file(s), such as the platform, language, etc. The submission screen will prompt for this information, before uploading the file(s). Please register or login, then click here to submit test cases.



58	2005-11-02	Java	Source Code	SecureSoftware	C	Not using a a random initialization vector with Cipher Block ...	✗
71	2005-11-07	Java	Source Code	SecureSoftware	C	Omitting a break statement so that one may fall through is often ...	✗
1552	2006-06-22	Java	Source Code	Jeff Meister	C	Tainted input allows arbitrary files to be read and written.	✗
1553	2006-06-22	Java	Source Code	Jeff Meister	C	Tainted input allows arbitrary files to be read and written. ...	✓
1554	2006-06-22	Java	Source Code	Jeff Meister	C	Two file operations are performed on a filename, allowing a filenamer	✗
1567	2006-06-22	Java	Source Code	Jeff Meister	C	The credentials for connecting to the database are hard-wired ...	✗
1568	2006-06-22	Java	Source Code	Jeff Meister	C	The credentials for connecting to the database are hard-wired ...	✓
1569	2006-06-22	Java	Source Code	Jeff Meister	C	The credentials for connecting to the database are hard-wired ...	✓
1570	2006-06-22	Java	Source Code	Jeff Meister	C	An exception leaks internal path information to the user.	✗
1571	2006-06-22	Java	Source Code	Jeff Meister	C	An exception leaks internal path information to the user. (fixed ...	✓
1579	2006-06-22	Java	Source Code	Jeff Meister	C	Tainted output allows log entries to be forged.	✗

Source Code Security Analysis Tool

Functional Specification Version 1.0

Currently:

Web application scanners

Source code security analyzers

Study: *Do tools help assurance?*

http://samate.nist.gov/SRD/

Partners: DHS National Cybersecurity Division, vendors, ITL Security Division, NSA

NIST
National Institute of Standards and Technology
U.S. Department of Commerce