SYNOPSYS®

Supported Vulnerabilities

SecureAssist is a lightweight static analysis tool that automatically detects vulnerabilities and provides just-in-time security guidance as you code. SecureAssist rules are provided out of the box, with the option to create your own custom rules.

.NET

Cryptography

- Weak encryption algorithm
- Weak hashing algorithm
- Weak cryptographic primitives

SQL injection

- ODBC / OLE DB
- Oracle / MySQL / SQLite
- Entity database

Other injection

- XPath injection
- Command injection
- LDAP injection
- Resource injection

XML

- XML DTD attack

ASP.NET code behind

- Impersonation handling
- Insecure data loaded in ASPX controls
- Trust boundary violations

Log injection and forging

- Log4net / Microsoft Enterprise logging APIs

Invalidated user input

- Path manipulation
- HTTP header manipulation
- URL redirection

Resource and thread handling

- Thread management
- Guessable temporary file names

MVC

- Disabled input validation
- Cross-site scripting
- Insecure script execution
- URL tampering
- Path manipulation
- Insecure view load

Password management

- Hard-coded password

MVC config

- Binding
- Attribute validation
- Information leakage
- Insecure configuration
- Transport level security
- Message security
- Behavior settings

ASPX config

- Disabled input validation
- Default error page missing
- Session management
- Insecure ASP.NET configuration
- Form authentication
- Cookie management
- Impersonation management

.NET (cont.)

ASPX

- Unencrypted view state
- Insecure ASP.NET configuration
- Disabled input validation and output encoding
- Information leakage

Code correctness

- Secure randomization
- Memory cleanup
- Resource handling

Others

- Cross-site scripting
- URL tampering
- Insecure scripts registered
- Disabled input validation and output encoding
- Denial-of-service attack

Java

Cross-site scripting

- Reflected XSS
- Persistent XSS
- Disabled input validation and output encoding

SQL injection

- Support for JDBC, Spring, Hibernate, and object persistence APIs

Named database query manipulation

- Support for Spring, Hibernate, and object persistence APIs

Other injection vulnerabilities

- LDAP injection
- Command injection
- XPath injection

Invalidated user input

- Path manipulation
- HTTP header manipulation
- URL redirection
- Email forging and injection

XML

- XML DTD attack
- XML injection

Password management

- Hard-coded password
- Minimum length

Log injection and forging

- Log4j and logger APIs

Code correctness

- Race condition
- Resource and thread handling
- Secure randomization
- Error handling

Spring Framework

- Session identifier in URL
- Information leakage
- Insecure configuration

Others

- Struts framework misconfiguration
- Trust boundary violations
- Denial-of-service attack
- Resource and thread handling
- Information leakage
- Session management
- Weak encryption algorithm

JavaScript

SQL injection

- NoSQL query injection

Information leakage

- Exposed directory listing
- X-Powered-By header enabled

Cross-site scripting

- Reflected XSS
- DOM-based XSS

Invalidated user input

- Open redirect
- Path manipulation

Injection vulnerabilities

- Regex injection
- Cookie injection
- Script code injection
- Header injection
- Command injection

JWT token security

- Ignored expiration time
- Unprotected token

Cookie security

- Insecure cookie

Others

- Weak cryptographic primitives and algorithms
- Hard-coded credentials
- Missing iframe sandbox
- Unchecked origin
- Unrestricted message target
- MongoDB mass assignment
- Session management
- Short HSTS max-age
- CSRF misconfiguration
- TLS not configured
- Broad whitelisting

PHP

SQL injection

- MS SQL
- ODBC
- Zend Framework

Other injection vulnerabilities

- XPath injection
- LDAP injection
- Command injection

Invalidated user input

- Path manipulation
- Remote code execution

Cross-site scripting

- Disabled input validation and output encoding
- Data sent directly to browser

Cryptography

- Weak hashing algorithm
- Weak encryption algorithm
- Invalidated user input
- Email forging
- URL redirection
- CURL requests

Code correctness

- Secure randomization
- Use of hidden fields
- Memory cleanup

Others

- Trust boundary violations
- Information leakage
- Log injection and forging
- PHP configuration manipulation
- Autocomplete turned on

This is a sampling of vulnerabilities identified by the default SecureAssist rulepack. Rules are updated regularly. Synopsys may add or remove rules from this list. For informational purposes only.

The Synopsys difference

Synopsys offers the most comprehensive solution for building integrity—security and quality—into your SDLC and supply chain. We've united leading testing technologies, automated analysis, and experts to create a robust portfolio of products and services. This portfolio enables companies to develop customized programs for detecting and remediating defects and vulnerabilities early in the development process, minimizing risk and maximizing productivity. Synopsys, a recognized leader in application security testing, is uniquely positioned to adapt and apply best practices to new technologies and trends such as IoT, DevOps, CI/CD, and the Cloud. We don't stop when the test is over. We offer onboarding and deployment assistance, targeted remediation guidance, and a variety of training solutions that empower you to optimize your investment. Whether you're just starting your journey or well on your way, our platform will help ensure the integrity of the applications that power your business.

For more information go to www.synopsys.com/software.

Synopsys, Inc.
185 Berry Street, Suite 6500
San Francisco, CA 94107 USA

U.S. Sales: 800.873.8193
International Sales: +1 415.321.5237
Email: sig-info@synopsys.com