SYNOPSYS®

Coverity Static Analysis Support for DISA-STIG Application Security Coding Standard

Ensure the safety, reliability, and security of Department of Defense information systems.

The Security Technical Implementation Guides (STIGs) are technical testing and hardening frameworks provided by the Department of Defense's (DoD's) Defense Information Systems Agency (DISA). To date DISA has issued 461 STIGs, and one of them focuses on application security. This STIG is derived from National Institute of Standards and Technology's (NIST) 800-53 and related documents and defines the guidelines to improve the security of DoD's information systems. Adhering to coding standards is a crucial step in establishing best coding practices. Standards adherence is particularly important in safety-critical, high-impact industries, such as automotive, medical, and networking. Software defects in products coming from these industries manifest themselves physically and tangibly—often with life- threatening consequences. The Application Security and Development STIG can be found here: https://public.cyber.mil/stigs/downloads/?_dl_facet_stigs=app-security%2Capp-security-dev Synopsys' Coverity Static Analysis identifies the vulnerabilities listed on DISA STIG guidelines for Application Security and Development, which are mapped to the Coverity checkers and help applications developers and application security managers find the violations of these rules in their applications. For more or a complete list of Finding IDs and descriptions listed on the following tables, see: https://vaulted.io/library/disa-stigs-srgs/Application_Security_Development_STIG Coverity Connect enables users to filter and visualize findings per the Coverity checker mapping to DISA STIG rules. Users can also request Synopsys Consulting services to build a script or write one on their own to generate a pdf report based on the DISA STIG filtered mapping available in Coverity Connect. DISA Application Security and Development STIG supported checkers

Finding ID	Description	Checker Names
APSC-DV000060	The application must clear temporary storage and cookies when the session is terminated	SENSITIVE_DATA_LEAK, UNENCRYPTED_SENSITIVE_DATA
APSC-DV-000170	The application must implement cryptographic mechanisms to protect the integrity of remote access sessions.	CONFIG.SPRING_SECURITY_WEAK_PASSWORD_HASH, INSECURE_SALT, RAILS_DEVISE_CONFIG, RISKY_CRYPTO, SA.RISKY_CRYPTO, WEAK_PASSWORD_HASH
APSC-DV-000500	The application must prevent non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/ countermeasures.	CONFIG.JAVAEE_MISSING_SERVLET_MAPPING, INSECURE_DIRECT_OBJECT_REFERENCE, CONFIG.MISSING_JSF2_SECURITY_CONSTRAINT, CONFIG.MYBATIS_MAPPER_SQLI, CONFIG.SPRING_SECURITY_DISABLE_AUTH_TAGS, CONFIG.STRUTS2_CONFIG_BROWSER_PLUGIN, JSP_SQL_INJECTION, RAILS_DEFAULT_ROUTES, RAILS_MISSING_FILTER_ACTION, SQLI, SQL_NOT_CONSTANT
APSC-DV-000530	The application must enforce the limit of three consecutive invalid logon attempts by a user during a 15 minute time period.	RAILS_DEVISE_CONFIG
APSC-DV-000580	The application must display the time and date of the users last successful logon.	INSUFFICIENT_LOGGING, UNLOGGED_SECURITY_EXCEPTION
APSC-DV-000650	The application must not write sensitive data into the application logs.	CONFIG.CORDOVA_EXCESSIVE_LOGGING, CONFIG.SEQUELIZE_ENABLED_LOGGING, CONFIG.SPRING_BOOT_SENSITIVE_LOGGING, EXPRESS_WINSTON_SENSITIVE_LOGGING, SENSITIVE_DATA_LEAK
APSC-DV-000670	The application must record a time stamp indicating when the event occurred.	INSUFFICIENT_LOGGING, UNLOGGED_SECURITY_EXCEPTION
APSC-DV-000700	The application must record the username or user ID of the user associated with the event.	INSUFFICIENT_LOGGING, UNLOGGED_SECURITY_EXCEPTION
APSC-DV-000940	The application must log application shutdown events.	INSUFFICIENT_LOGGING, UNLOGGED_SECURITY_EXCEPTION
APSC-DV-000950	The application must log destination IP addresses.	INSUFFICIENT_LOGGING, UNLOGGED_SECURITY_EXCEPTION
APSC-DV-000960	The application must log user actions involving access to data.	INSUFFICIENT_LOGGING, UNLOGGED_SECURITY_EXCEPTION
APSC-DV-000970	The application must log user actions involving changes to data.	INSUFFICIENT_LOGGING, UNLOGGED_SECURITY_EXCEPTION
APSC-DV-001280	The application must protect audit information from any type of unauthorized read access.	HARDCODED_CREDENTIALS, LOCALSTORAGE_WRITE, SENSITIVE_DATA_LEAK, UNENCRYPTED_SENSITIVE_DATA, UNRESTRICTED_ACCESS_TO_FILE
APSC-DV-001290	The application must protect audit information from unauthorized modification.	HARDCODED_CREDENTIALS, LOCALSTORAGE_WRITE, SENSITIVE_DATA_LEAK, UNENCRYPTED_SENSITIVE_DATA, UNRESTRICTED_ACCESS_TO_FILE
APSC-DV-001300	The application must protect audit information from unauthorized deletion.	HARDCODED_CREDENTIALS, LOCALSTORAGE_WRITE, SENSITIVE_DATA_LEAK, UNENCRYPTED_SENSITIVE_DATA, UNRESTRICTED_ACCESS_TO_FILE

Finding ID	Description	Checker Names
APSC-DV-001350	The application must use cryptographic mechanisms to protect the integrity of audit information.	AWS_SSL_DISABLED, CONFIG.ATS_INSECURE, CONFIG.SEQUELIZE_INSECURE_CONNECTION, CONFIG.SPRING_BOOT_SSL_DISABLED, CONFIG.SPRING_SECURITY_LOGIN_OVER_HTTP, DISABLED_ENCRYPTION, HARDCODED_CREDENTIALS, INSECURE_COMMUNICATION, INSECURE_COOKIE, INSECURE_MULTIPEER_CONNECTION, INSECURE_REMEMBER_ME_COOKIE, SENSITIVE_DATA_LEAK, STRICT_TRANSPORT_SECURITY, UNENCRYPTED_SENSITIVE_DATA, UNSAFE_SESSION_SETTING
APSC-DV-001360	Application audit tools must be cryptographically hashed.	INSECURE_SALT, RISKY_CRYPTO, WEAK_PASSWORD_HASH
APSC-DV-001370	The integrity of the audit tools must be validated by checking the files for changes in the cryptographic hash value.	INSECURE_SALT, RISKY_CRYPTO, WEAK_PASSWORD_HASH
APSC-DV-001650	The application must authenticate all network connected endpoint devices before establishing any connection.	AWS_VALIDATION_DISABLED, BAD_CERT_VERIFICATION, CONFIG.MYSQL_SSL_VERIFY_DISABLED, CONFIG.REQUEST_STRICTSSL_DISABLED, CONFIG.SPRING_BOOT_SSL_DISABLED, CORS_MISCONFIGURATION, CORS_MISCONFIGURATION_AUDIT, HPKP_MISCONFIGURATION, RISKY_CRYPTO, SA.RISKY_CRYPTO, WEAK_GUARD
APSC-DV-001660	Service-Oriented Applications handling non-releasable data must authenticate endpoint devices via mutual SSL/TLS.	AWS_SSL_DISABLED, AWS_VALIDATION_DISABLED, BAD_CERT_VERIFICATION, CONFIG.ATS_INSECURE, CONFIG.MYSQL_SSL_VERIFY_DISABLED, CONFIG.REQUEST_STRICTSSL_DISABLED, CONFIG.SEQUELIZE_INSECURE_CONNECTION, CONFIG.SPRING_BOOT_SSL_DISABLED, CONFIG.SPRING_SECURITY_LOGIN_OVER_HTTP, CORS_MISCONFIGURATION, CORS_MISCONFIGURATION_AUDIT, HPKP_MISCONFIGURATION, INSECURE_COMMUNICATION, INSECURE_MULTIPEER_CONNECTION, RISKY_CRYPTO, SA.RISKY_CRYPTO, SENSITIVE_DATA_LEAK, STRICT_TRANSPORT_SECURITY, UNENCRYPTED_SENSITIVE_DATA
APSC-DV-001680	The application must enforce a minimum 15-character password length.	RAILS_DEVISE_CONFIG
APSC-DV-001690	The application must enforce password complexity by requiring that at least one upper-case character be used.	RAILS_DEVISE_CONFIG
APSC-DV-001700	The application must enforce password complexity by requiring that at least one lower-case character be used.	RAILS_DEVISE_CONFIG
APSC-DV-001710	The application must enforce password complexity by requiring that at least one numeric character be used.	RAILS_DEVISE_CONFIG
APSC-DV-001720	The application must enforce password complexity by requiring that at least one special character be used.	RAILS_DEVISE_CONFIG

Finding ID	Description	Checker Names
APSC-DV-001740	The application must only store cryptographic representations of passwords.	CONFIG.CONNECTION_STRING_PASSWORD, CONFIG.HARDCODED_CREDENTIALS_AUDIT, CONFIG.HARDCODED_TOKEN, HARDCODED_CREDENTIALS, CONFIG.SPRING_SECURITY_WEAK_PASSWORD_HASH, INSECURE_SALT, RAILS_DEVISE_CONFIG, SENSITIVE_DATA_LEAK, UNENCRYPTED_SENSITIVE_DATA, WEAK_PASSWORD_HASH
APSC-DV-001750	The application must transmit only cryptographically-protected passwords.	AWS_SSL_DISABLED, CONFIG.ATS_INSECURE, CONFIG.SEQUELIZE_INSECURE_CONNECTION, INSECURE_COMMUNICATION, INSECURE_MULTIPEER_CONNECTION, SENSITIVE_DATA_LEAK, STRICT_TRANSPORT_SECURITY, UNENCRYPTED_SENSITIVE_DATA
APSC-DV-001770	The application must enforce a 60-day maximum password lifetime restriction.	RAILS_DEVISE_CONFIG
APSC-DV-001795	The application password must not be changeable by users other than the administrator or the user with which the password is associated.	CONFIG.CONNECTION_STRING_PASSWORD, CONFIG.HARDCODED_CREDENTIALS_AUDIT, CONFIG.HARDCODED_TOKEN, CONFIG.SPRING_SECURITY_HARDCODED_CREDENTIALS, CONFIG.SPRING_SECURITY_REMEMBER_ME_HARDCODED_KEY, HARDCODED_CREDENTIALS, UNSAFE_BASIC_AUTH, UNSAFE_SESSION_SETTING
APSC-DV-001810	The application, when utilizing PKI-based authentication, must validate certificates by constructing a certification path (which includes status information) to an accepted trust anchor.	AWS_VALIDATION_DISABLED, BAD_CERT_VERIFICATION, CONFIG.MYSQL_SSL_VERIFY_DISABLED, CONFIG.REQUEST_STRICTSSL_DISABLED, CONFIG.SPRING_BOOT_SSL_DISABLED, HPKP_MISCONFIGURATION
APSC-DV-001820	The application, when using PKI-based authentication, must enforce authorized access to the corresponding private key.	HARDCODED_CREDENTIALS, UNSAFE_SESSION_SETTING
APSC-DV-001830	The application must map the authenticated identity to the individual user or group account for PKI-based authentication.	BAD_CERT_VERIFICATION
APSC-DV-001840	The application, for PKI-based authentication, must implement a local cache of revocation data to support path discovery and validation in case of the inability to access revocation information via the network.	BAD_CERT_VERIFICATION
APSC-DV-001995	The application must not be vulnerable to race conditions.	ATOMICITY, BAD_CHECK_OF_WAIT_COND, BAD_LOCK_OBJECT, DC.DEADLOCK, GUARDED_BY_VIOLATION, LOCK, LOCK_EVASION, LOCK_INVERSION, MISSING_LOCK, NON_STATIC_GUARDING_STATIC, ORDER_REVERSAL, SERVLET_ATOMICITY, SINGLETON_RACE, SLEEP, TOCTOU, VOLATILE_ATOMICITY
APSC-DV-002000	The application must terminate all network connections associated with a communications session at the end of the session.	CONFIG.JSONWEBTOKEN_NON_EXPIRING_TOKEN, CONFIG.UNSAFE_SESSION_TIMEOUT, CORS_MISCONFIGURATION_AUDIT, HPKP_MISCONFIGURATION, INSUFFICIENT_PRESIGNED_URL_TIMEOUT, JSONWEBTOKEN_IGNORED_EXPIRATION_TIME, TEMPORARY_CREDENTIALS_DURATION
APSC-DV-002210	The application must set the HTTPOnly flag on session cookies.	CONFIG.JAVAEE_MISSING_HTTPONLY

Finding ID	Description	Checker Names
APSC-DV-002220	The application must set the secure flag on session cookies.	INSECURE_COOKIE, INSECURE_REMEMBER_ME_COOKIE, UNSAFE_SESSION_SETTING
APSC-DV-002230	The application must not expose session IDs.	CONFIG.SPRING_SECURITY_SESSION_FIXATION, SESSION_FIXATION
APSC-DV-002240	The application must destroy the session ID value and/or cookie on logoff or browser close.	CONFIG.JSONWEBTOKEN_NON_EXPIRING_TOKEN, CONFIG.UNSAFE_SESSION_TIMEOUT, CORS_MISCONFIGURATION_AUDIT, HPKP_MISCONFIGURATION, INSUFFICIENT_PRESIGNED_URL_TIMEOUT, JSONWEBTOKEN_IGNORED_EXPIRATION_TIME, SENSITIVE_DATA_LEAK, TEMPORARY_CREDENTIALS_DURATION, UNENCRYPTED_SENSITIVE_DATA
APSC-DV-002250	Applications must use system-generated session identifiers that protect against session fixation.	CONFIG.SPRING_SECURITY_SESSION_FIXATION, SESSION_FIXATION
APSC-DV-002260	Applications must validate session identifiers.	CONFIG.COOKIE_SIGNING_DISABLED
APSC-DV-002280	The application must not re-use or recycle session IDs.	CONFIG.JSONWEBTOKEN_NON_EXPIRING_TOKEN, CONFIG.UNSAFE_SESSION_TIMEOUT, CORS_MISCONFIGURATION_AUDIT, HPKP_MISCONFIGURATION, INSUFFICIENT_PRESIGNED_URL_TIMEOUT, JSONWEBTOKEN_IGNORED_EXPIRATION_TIME, TEMPORARY_CREDENTIALS_DURATION
APSC-DV-002300	The application must only allow the use of DoD-approved certificate authorities for verification of the establishment of protected sessions.	AWS_VALIDATION_DISABLED, BAD_CERT_VERIFICATION, CONFIG.MYSQL_SSL_VERIFY_DISABLED, CONFIG.REQUEST_STRICTSSL_DISABLED, CONFIG.SPRING_BOOT_SSL_DISABLED, HPKP_MISCONFIGURATION
APSC-DV-002370	The application must maintain a separate execution domain for each executing process.	ARRAY_VS_SINGLETON, BAD_ALLOC_ARITHMETIC, BUFFER_SIZE, COM.BAD_FREE, COM.BSTR.ALLOC, COM.BSTR.CONV, INCOMPATIBLE_CAST, INTEGER_OVERFLOW, INVALIDATE_ITERATOR, MISMATCHED_ITERATOR, MISSING_ASSIGN, MISSING_COPY, OVERRUN, REVERSE_NEGATIVE, SIZECHECK, STRING_OVERFLOW, STRING_SIZE, TAINTED_SCALAR, USE_AFTER_FREE, WRAPPER_ESCAPE
APSC-DV-002380	Applications must prevent unauthorized and unintended information transfer via shared system resources.	SENSITIVE_DATA_LEAK
APSC-DV-002390	XML-based applications must mitigate DoS attacks by using XML filters, parser options, or gateways.	XML_EXTERNAL_ENTITY, XML_INJECTION, XPATH_INJECTION
APSC-DV-002400 (cont.)	The application must restrict the ability to launch Denial of Service (DoS) attacks against itself or other information systems.	BUSBOY_MISCONFIGURATION, COM.ADDROF_LEAK, COM.BAD_FREE, COM.BSTR.ALLOC, CONFIG.CORDOVA_EXCESSIVE_LOGGING, CONFIG.DEAD_AUTHORIZATION_RULE, CONFIG.DWR_DEBUG_MODE, CONFIG.JAVAEE_MISSING_SERVLET_MAPPING, CONFIG.MISSING_JSF2_SECURITY_CONSTRAINT, CONFIG.MYBATIS_MAPPER_SQLI, CONFIG.SOCKETIO_MAXHTTPBUFFERSIZE_SET_TOO_LARGE, CONFIG.SOCKETIO_ORIGINS_ACCEPT_ALL, CONFIG.SPRING_SECURITY_DISABLE_AUTH_TAGS, CONFIG.STRUTS2_CONFIG_BROWSER_PLUGIN, (cont. on next page)

Finding ID	Description	Checker Names
APSC-DV-002400 (cont.)	The application must restrict the ability to launch Denial of Service (DoS) attacks against itself or other information systems.	CONFIG.STRUTS2_DYNAMIC_METHOD_INVOCATION, CONFIG.STRUTS2_ENABLED_DEV_MODE, CTOR_DTOR_LEAK, EXPRESS_SESSION_UNSAFE_MEMORYSTORE, , FILE_UPLOAD_MISCONFIGURATION, FORMAT_STRING_INJECTION, IMPLICIT_INTENT, HARDCODED_CREDENTIALS, INSECURE_DIRECT_OBJECT_REFERENCE, JSP_SQL_INJECTION, LOCALSTORAGE_WRITE, LOCK, MISSING_ASSIGN, MISSING_COPY, MISSING_PERMISSION_FOR_BROADCAST, MULTER_MISCONFIGURATION, NEGATIVE_RETURNS, NO_EFFECT, PW.NON_CONST_PRINTF_FORMAT_STRING, RAILS_DEFAULT_ROUTES, RAILS_DEVISE_CONFIG, RAILS_MISSING_FILTER_ACTION, RESOURCE_LEAK, RUBY_VULNERABLE_LIBRARY, SENSITIVE_DATA_LEAK, SQLI, SQL_NOT_CONSTANT, STACK_USE, TAINTED_SCALAR, UNENCRYPTED_SENSITIVE_DATA, UNLIMITED_CONCURRENT_SESSIONS, UNRESTRICTED_ACCESS_TO_FILE, USE_AFTER_FREE, VIRTUAL_DTOR, WRAPPER_ESCAPE, XML_EXTERNAL_ENTITY
APSC-DV-002440	The application must protect the confidentiality and integrity of transmitted information.	AWS_SSL_DISABLED, BAD_CERT_VERIFICATION, CONFIG.ATS_INSECURE, CONFIG.REQUEST_STRICTSSL_DISABLED, CONFIG.SEQUELIZE_INSECURE_CONNECTION, CONFIG.SPRING_BOOT_SSL_DISABLED, CONFIG.SPRING_SECURITY_LOGIN_OVER_HTTP, CORS_MISCONFIGURATION, CORS_MISCONFIGURATION_AUDIT, DISABLED_ENCRYPTION, HARDCODED_CREDENTIALS, INSECURE_COMMUNICATION, INSECURE_COOKIE, INSECURE_MULTIPEER_CONNECTION, INSECURE_REMEMBER_ME_COOKIE, RISKY_CRYPTO, SA.RISKY_CRYPTO, SENSITIVE_DATA_LEAK, STRICT_TRANSPORT_SECURITY, UNENCRYPTED_SENSITIVE_DATA, UNSAFE_SESSION_SETTING
APSC-DV-002460	The application must maintain the confidentiality and integrity of information during preparation for transmission.	AWS_SSL_DISABLED, CONFIG.CONNECTION_STRING_PASSWORD, CONFIG.SPRING_BOOT_SSL_DISABLED, CONFIG.SPRING_SECURITY_EXPOSED_SESSIONID, CONFIG.SPRING_SECURITY_LOGIN_OVER_HTTP, CONFIG.SPRING_SECURITY_WEAK_PASSWORD_HASH, CONFIG.SPRING_SECURITY_UNSAFE_AUTHENTICATION_FILTER, CORS_MISCONFIGURATION, CORS_MISCONFIGURATION_AUDIT, DC.WEAK_CRYPTO, DISABLED_ENCRYPTION, HARDCODED_CREDENTIALS, HPKP_MISCONFIGURATION, INSECURE_ACL, INSECURE_COMMUNICATION, INSECURE_RANDOM, INSECURE_REFERRER_POLICY, INSECURE_SALT, PREDICTABLE_RANDOM_SEED, RAILS_DEVISE_CONFIG, REVERSE_TABNABBING, RISKY_CRYPTO, SA.RISKY_CRYPTO, SENSITIVE_DATA_LEAK, UNENCRYPTED_SENSITIVE_DATA, UNSAFE_BUFFER_METHOD, WEAK_GUARD, WEAK_PASSWORD_HASH, VERBOSE_ERROR_REPORTING, WEAK_URL_SANITIZATION

Finding ID	Description	Checker Names
APSC-DV-002470	The application must maintain the confidentiality and integrity of information during reception.	AWS_SSL_DISABLED, BAD_CERT_VERIFICATION, CONFIG.ATS_INSECURE, CONFIG.REQUEST_STRICTSSL_DISABLED, CONFIG.SEQUELIZE_INSECURE_CONNECTION, CORS_MISCONFIGURATION, CORS_MISCONFIGURATION_AUDIT, INSECURE_COMMUNICATION, INSECURE_MULTIPEER_CONNECTION, RISKY_CRYPTO, SA.RISKY_CRYPTO, SENSITIVE_DATA_LEAK, STRICT_TRANSPORT_SECURITY, UNENCRYPTED_SENSITIVE_DATA
APSC-DV-002480	The application must not disclose unnecessary information to users.	ANDROID_CAPABILITY_LEAK, ANDROID_DEBUG_MODE, ASPNET_MVC_VERSION_HEADER, CONFIG.ANDROID_BACKUPS_ALLOWED, CONFIG.ASPNET_VERSION_HEADER, CONFIG.ASP_VIEWSTATE_MAC, CONFIG.CONNECTION_STRING_PASSWORD, CONFIG.DEAD_AUTHORIZATION_RULE, CONFIG.DWR_DEBUG_MODE, CONFIG.DYNAMIC_DATA_HTML_COMMENT, CONFIG.ENABLED_DEBUG_MODE, CONFIG.ENABLED_TRACE_MODE, CONFIG.JAVAEE_MISSING_SERVLET_MAPPING, CONFIG.MISSING_CUSTOM_ERROR_PAGE, CONFIG.MISSING_GLOBAL_EXCEPTION_HANDLER, CONFIG.MISSING_JSF2_SECURITY_CONSTRAINT, CONFIG.MYBATIS_MAPPER_SQLI, CONFIG.SEQUELIZE_ENABLED_LOGGING, CONFIG.SPRING_BOOT_SENSITIVE_LOGGING, CONFIG.SPRING_SECURITY_DEBUG_MODE, CONFIG.SPRING_SECURITY_DISABLE_AUTH_TAGS, CONFIG.STRUTS2_CONFIG_BROWSER_PLUGIN, CONFIG.STRUTS2_DYNAMIC_METHOD_INVOCATION, CONFIG.STRUTS2_ENABLED_DEV_MODE, EXPOSED_PREFERENCES, EXPRESS_WINSTON_SENSITIVE_LOGGING, EXPRESS_X_POWERED_BY_ENABLED, IMPLICIT_INTENT, INSECURE_DIRECT_OBJECT_REFERENCE, JSP_SQL_INJECTION, MISSING_PERMISSION_FOR_BROADCAST, MISSING_PERMISSION_ON_EXPORTED_COMPONENT, MOBILE_ID_MISUSE, OPEN_REDIRECT, RAILS_DEFAULT_ROUTES, RAILS_MISSING_FILTER_ACTION, REVERSE_TABNABBING, SENSITIVE_DATA_LEAK, SQLI, SQL_NOT_CONSTANT, UNRESTRICTED_ACCESS_TO_FILE, UNENCRYPTED_SENSITIVE_DATA, URL_MANIPULATION
APSC-DV-002485	The application must not store sensitive information in hidden fields.	SENSITIVE_DATA_LEAK
APSC-DV-002490	The application must protect from Cross-Site Scripting (XSS) vulnerabilities.	ANGULAR_SCE_DISABLED, CONFIG.SPRING_SECURITY_DEPRECATED_XSS_HEADER, DOM_XSS, REACT_DANGEROUS_INNERHTML, VUE_TEMPLATE_UNSAFE_VHTML_DIRECTIVE, XSS
APSC-DV-002500	The application must protect from Cross-Site Request Forgery (CSRF) vulnerabilities.	CONFIG.CSURF_IGNORE_METHODS, CONFIG.HANA_XS_PREVENT_XSRF_DISABLED, CONFIG.SPRING_SECURITY_CSRF_PROTECTION_DISABLED, CONFIG.SYMFONY_CSRF_PROTECTION_DISABLED, CSRF
APSC-DV-002510	The application must protect from command injection.	OS_CMD_INJECTION, TAINTED_ENVIRONMENT_WITH_EXECUTION

Finding ID	Description	Checker Names
APSC-DV-002520	The application must protect from canonical representation vulnerabilities.	BUSBOY_MISCONFIGURATION, FILE_UPLOAD_MISCONFIGURATION, JSP_DYNAMIC_INCLUDE, MULTER_MISCONFIGURATION, PATH_MANIPULATION, RUBY_VULNERABLE_LIBRARY
APSC-DV-002530	The application must validate all input.	ANGULAR_EXPRESSION_INJECTION, CONFIG.UNSAFE_SESSION_TIMEOUT, COOKIE_SERIALIZER_CONFIG, CORS_MISCONFIGURATION_AUDIT, DISTRUSTED_DATA_DESERIALIZATION, FORMAT_STRING_INJECTION, HPKP_MISCONFIGURATION, INSUFFICIENT_PRESIGNED_URL_TIMEOUT, JAVA_CODE_INJECTION, JCR_INJECTION, JSP_DYNAMIC_INCLUDE, LDAP_INJECTION, LDAP_NOT_CONSTANT, NEGATIVE_RETURNS, NOSQL_QUERY_INJECTION, OGNL_INJECTION, PATH_MANIPULATION, PW.NON_CONST_PRINTF_FORMAT_STRING, REGEX_INJECTION, REVERSE_NEGATIVE, RUBY_VULNERABLE_LIBRARY, SCRIPT_CODE_INJECTION, TAINTED_SCALAR, TEMPLATE_INJECTION, TEMPORARY_CREDENTIALS_DURATION, UNCHECKED_ORIGIN, UNKNOWN_LANGUAGE_INJECTION, UNRESTRICTED_DISPATCH, UNRESTRICTED_MESSAGE_TARGET, UNSAFE_DESERIALIZATION, UNSAFE_JNI, UNSAFE_NAMED_QUERY, UNSAFE_REFLECTION, XPATH_INJECTION
APSC-DV-002540	The application must not be vulnerable to SQL Injection.	CONFIG.MYBATIS_MAPPER_SQLI, DYNAMIC_OBJECT_ATTRIBUTES, JSP_SQL_INJECTION, NOSQL_QUERY_INJECTION, RUBY_VULNERABLE_LIBRARY, SQLI, SQL_NOT_CONSTANT
APSC-DV-002550	The application must not be vulnerable to XML-oriented attacks.	XML_EXTERNAL_ENTITY, XML_INJECTION, XPATH_INJECTION
APSC-DV-002560	The application must not be subject to input handling vulnerabilities.	NEGATIVE_RETURNS, REVERSE_NEGATIVE, TAINTED_SCALAR
APSC-DV-002570	The application must generate error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries.	CONFIG.CORDOVA_EXCESSIVE_LOGGING, CONFIG.SEQUELIZE_ENABLED_LOGGING, CONFIG.SPRING_BOOT_SENSITIVE_LOGGING, EXPRESS_WINSTON_SENSITIVE_LOGGING, INSUFFICIENT_LOGGING, SENSITIVE_DATA_LEAK, UNLOGGED_SECURITY_EXCEPTION
APSC-DV-002590	The application must not be vulnerable to overflow attacks.	ALLOC_FREE_MISMATCH, ARRAY_VS_SINGLETON, BAD_ALLOC_ARITHMETIC, BAD_ALLOC_STRLEN, BAD_CERT_VERIFICATION, BAD_FREE, BUFFER_SIZE, BUFFER_SIZE_WARNING, CALL_SUPER, CHAR_IO, COM.ADDROF_LEAK, COM.BAD_FREE, COM.BSTR.ALLOC, COM.BSTR.CONV, CTOR_DTOR_LEAK, DELETE_ARRAY, DELETE_VOID, EVALUATION_ORDER, INCOMPATIBLE_CAST, INTEGER_OVERFLOW, INVALIDATE_ITERATOR, MISMATCHED_ITERATOR, MISRA_CAST, MISSING_COPY, MISSING_ASSIGN, NO_EFFECT, NEGATIVE_RETURNS, OVERRUN, PW.BAD_CAST, PW.COVERSION_TO_POINTER_LOSES_BITS, RAILS_DEVISE_CONFIG, READLINK, RESOURCE_LEAK, REVERSE_NEGATIVE, SENSITIVE_DATA_LEAK, SIGN_EXTENSION, SIZECHECK, SQLI, STACK_USE, STRING_NULL, STRING_OVERFLOW, STRING_SIZE, TAINTED_SCALAR, USE_AFTER_FREE, VIRTUAL_DTOR, WRAPPER_ESCAPE

Finding ID	Description	Checker Names
APSC-DV-003100	The application must use encryption to implement key exchange and authenticate endpoints prior to establishing a communication channel for key exchange.	BAD_CERT_VERIFICATION, CONFIG.CSURF_IGNORE_METHODS, CONFIG.HANA_XS_PREVENT_XSRF_DISABLED, CONFIG.REQUEST_STRICTSSL_DISABLED, CONFIG.SPRING_SECURITY_CSRF_PROTECTION_DISABLED, CONFIG.SYMFONY_CSRF_PROTECTION_DISABLED, CONFIG.UNSAFE_SESSION_TIMEOUT, CORS_MISCONFIGURATION, CORS_MISCONFIGURATION_AUDIT, CSRF, CSRF_MISCONFIGURATION_HAPI_CRUMB, HPKP_MISCONFIGURATION, INSUFFICIENT_PRESIGNED_URL_TIMEOUT, JSONWEBTOKEN_UNTRUSTED_DECODE, MULTER_MISCONFIGURATION, RISKY_CRYPTO, SA.RISKY_CRYPTO, TEMPORARY_CREDENTIALS_DURATION, UNCHECKED_ORIGIN, WEAK_GUARD
APSC-DV-003110	The application must not contain embedded authentication data.	CONFIG.CONNECTION_STRING_PASSWORD, CONFIG.HARDCODED_CREDENTIALS_AUDIT, CONFIG.HARDCODED_TOKEN, CONFIG.SPRING_SECURITY_HARDCODED_CREDENTIALS, CONFIG.SPRING_SECURITY_REMEMBER_ME_HARDCODED_KEY, HARDCODED_CREDENTIALS, UNSAFE_BASIC_AUTH, UNSAFE_SESSION_SETTING
APSC-DV-003215	The application development team must follow a set of coding standards.	ALLOC_FREE_MISMATCH, ASSERT_SIDE_EFFECT, ASSIGN_NOT_RETURNING_STAR_THIS, AWS_VALIDATION_DISABLED, BAD_CERT_VERIFICATION, BAD_COMPARE, BAD_EQ, BAD_EQ_TYPES, BAD_OVERRIDE, BAD_SHIFT, BAD_SIZEOF, BUFFER_SIZE, CALL_SUPER, CHAR_IO, CHROOT, COM.ADDROF_LEAK, COM.BAD_FREE, COM.BSTR.BAD_COMPARE, COM.BSTR.NE_NON_BSTR, CONFIG.COOKIES_MISSING_HTTPONLY, CONFIG.COOKIE_SIGNING_DISABLED, CONFIG.DEAD_AUTHORIZATION_RULE, CONFIG.DUPLICATE_SERVLET_DEFINITION, CONFIG.HTTP_VERB_TAMPERING, CONFIG.SPRING_BOOT_SSL_DISABLED, CONFIG.SPRING_SECURITY_SESSION_FIXATION, CONFIG.STRUTS2_DYNAMIC_METHOD_INVOCATION, CONFIG.UNSAFE_SESSION_TIMEOUT, CONSTANT_EXPRESSION_RESULT, COOKIE_INJECTION, COPY_PASTE_ERROR, COPY_WITHOUT_ASSIGN, CORS_MISCONFIGURATION, CORS_MISCONFIGURATION_AUDIT, DC.DANGEROUS, DC.DEADLOCK, DC.STREAM_BUFFER, DC.STRING_BUFFER, DEADCODE, EL_INJECTION, ENUM_AS_BOOLEAN, EVALUATION_ORDER, EXPLICIT_THIS_EXPECTED, HFA, HIBERNATE_BAD_HASHCODE, HPKP_MISCONFIGURATION, IDENTICAL_BRANCHES, IDENTIFIER_TYPO, INCOMPATIBLE_CAST, INSECURE_HTTP_FIREWALL, INVALIDATE_ITERATOR, MISMATCHED_ITERATOR, MISRA_CAST, MISSING_ASSIGN, MISSING_AUTHZ, MISSING_BREAK, MISSING_COMMA, MISSING_COPY, MISSING_MOVE_ASSIGNMENT, MISSING_RESTORE, MISSING_RETURN, MISSING_THROW, MIXED_ENUMS, NEGATIVE_RETURNS, NESTING_INDENT_MISMATCH, NO_EFFECT, OPEN_ARGS, ORM_LOAD_NULL_CHECK, ORM_LOST_UPDATE, ORM_UNNECESSARY_GET, OVERFLOW_BEFORE_WIDEN, PARSE_ERROR, PASS_BY_VALUE, PROPERTY_MIXUP, PW.ASSIGN_WHERE_COMPARE_MEANT, PW.BAD_CAST, PW.BAD_PRINTF_FORMAT_STRING, PW.BRANCH_PAST_INITIALIZATION, PW.CONVERSION_TO_POINTER_LOSES_BITS, PW.DIVIDE_BY_ZERO, PW.EXPR_HAS_NO_EFFECT, PW.INCLUDE_RECURSION, (cont. on next page)

Finding ID	Description	Checker Names
APSC-DV-003215 (cont.)	The application development team must follow a set of coding standards.	PW.INTEGER_OVERFLOW, PW.INTEGER_TOO_LARGE, PW.NON_CONST_PRINTF_FORMAT_STRING, PW.RETURN_PTR_TO_LOCAL_TEMP, PW.SHIFT_COUNT_TOO_LARGE, PW.TOO_FEW_PRINTF_ARGS, PW.TOO_MANY_PRINTF_ARGS, PW.UNSIGNED_COMPARE_WITH_NEGATIVE, READLINK, REGEX_CONFUSION, RETURN_LOCAL, SECURE_TEMP, SELF_ASSIGN, SIGN_EXTENSION, SIZEOF_MISMATCH, SLEEP, STRAY_SEMICOLON, STREAM_FORMAT_STATE, SWAPPED_ARGUMENTS, TAINT_ASSERT, UNINIT, UNINIT_CTOR, UNINTENDED_GLOBAL, UNINTENDED_INTEGER_DIVISION, UNREACHABLE, UNUSED_VALUE, USELESS_CALL, USER_POINTER, USE_AFTER_FREE, VARARGS, VIRTUAL_DTOR, WRAPPER_ESCAPE, WRONG_METHOD This directive is also partially covered by checkers for the SEI CERT and MISRA standards. Contact Synopsys to obtain a full list of SEI CERT and MISRA checkers that address the issues related to Finding ID APSC-DV-003215. Synopsys customers can also find this list in the Checker Reference technical guide.
APSC-DV-003235	The application must not be subject to error handling vulnerabilities.	BAD_COMPARE, CHECKED_RETURN, ORM_LOAD_NULL_CHECK, NEGATIVE_RETURNS, REVERSE_NEGATIVE, UNCAUGHT_EXCEPT
APSC-DV-003300	The designer must ensure uncategorized or emerging mobile code is not used in applications.	FB.FI_PUBLIC_SHOULD_BE_PROTECTED
APSC-DV-003320	Protections against DoS attacks must be implemented.	BAD_FREE, COM.BSTR.CONV, DC.DEADLOCK, DIVIDE_BY_ZERO, FORWARD_NULL, INFINITE_LOOP, LOCK_INVERSION, NULL_RETURNS, ORDER_REVERSAL, PW.DIVIDE_BY_ZERO, REVERSE_INULL, TAINTED_SCALAR

The Synopsys difference

Synopsys helps development teams build secure, high-quality software, minimizing risks while maximizing speed and productivity. Synopsys, a recognized leader in application security, provides static analysis, software composition analysis, and dynamic analysis solutions that enable teams to quickly find and fix vulnerabilities and defects in proprietary code, open source components, and application behavior.

For more information about the Synopsys Software Integrity Group, visit us online at 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