The Security Technical Implementation Guides (STIGs) are security configuration guidelines and hardening frameworks provided by the Department of Defense’s (DoD’s) Defense Information Systems Agency (DISA). To date DISA has issued more than 450 STIGs, and one of them focuses on application security. This Application Security and Development (ASD) STIG is derived from National Institute of Standards and Technology’s (NIST) 800-53 and related documents and defines the guidelines for use throughout the application development life cycle. This STIG provides guidance needed to promote the development, integration, and updating of secure applications. Following the guidelines and adhering to coding standards are crucial steps 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 non-compliance to the guidelines listed in DISA STIG 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 STIG 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 IDs and categories. 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.
<table>
<thead>
<tr>
<th>STIG ID</th>
<th>Description</th>
<th>Checker Names</th>
</tr>
</thead>
<tbody>
<tr>
<td>APSC-DV000060</td>
<td>The application must clear temporary storage and cookies when the session is terminated.</td>
<td>SENSITIVE_DATA_LEAK, UNENCRYPTED_SENSITIVE_DATA</td>
</tr>
<tr>
<td>APSC-DV-000170</td>
<td>The application must implement cryptographic mechanisms to protect the integrity of remote access sessions.</td>
<td>CONFIG.SPRING_SECURITY_WEAK_PASSWORD_HASH, INSECURE_SALT, RAILS_DEVISE_CONFIG, RISKY_CRYPTO, SA.RISKY_CRYPTO, WEAK_PASSWORD_HASH</td>
</tr>
<tr>
<td>APSC-DV-000500</td>
<td>The application must prevent non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.</td>
<td>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</td>
</tr>
<tr>
<td>APSC-DV-000530</td>
<td>The application must enforce the limit of three consecutive invalid logon attempts by a user during a 15 minute time period.</td>
<td>RAILS_DEVISE_CONFIG</td>
</tr>
<tr>
<td>APSC-DV-000580</td>
<td>The application must display the time and date of the users last successful logon.</td>
<td>INSUFFICIENT_LOGGING, UNLOGGED_SECURITY_EXCEPTION</td>
</tr>
<tr>
<td>APSC-DV-000650</td>
<td>The application must not write sensitive data into the application logs.</td>
<td>CONFIG.CORDOVA_EXCESSIVE_LOGGING, CONFIG.SECUENLIZE_ENABLED_LOGGING, CONFIG.SPRING_BOOT_SENSITIVE_LOGGING, EXPRESS_WINSTON_SENSITIVE_LOGGING, SENSITIVE_DATA_LEAK</td>
</tr>
<tr>
<td>APSC-DV-000670</td>
<td>The application must record a time stamp indicating when the event occurred.</td>
<td>INSUFFICIENT_LOGGING, UNLOGGED_SECURITY_EXCEPTION</td>
</tr>
<tr>
<td>APSC-DV-000700</td>
<td>The application must record the username or user ID of the user associated with the event.</td>
<td>INSUFFICIENT_LOGGING, UNLOGGED_SECURITY_EXCEPTION</td>
</tr>
<tr>
<td>APSC-DV-000940</td>
<td>The application must log application shutdown events.</td>
<td>INSUFFICIENT_LOGGING, UNLOGGED_SECURITY_EXCEPTION</td>
</tr>
<tr>
<td>APSC-DV-000950</td>
<td>The application must log destination IP addresses.</td>
<td>INSUFFICIENT_LOGGING, UNLOGGED_SECURITY_EXCEPTION</td>
</tr>
<tr>
<td>APSC-DV-000960</td>
<td>The application must log user actions involving access to data.</td>
<td>INSUFFICIENT_LOGGING, UNLOGGED_SECURITY_EXCEPTION</td>
</tr>
<tr>
<td>APSC-DV-000970</td>
<td>The application must log user actions involving changes to data.</td>
<td>INSUFFICIENT_LOGGING, UNLOGGED_SECURITY_EXCEPTION</td>
</tr>
<tr>
<td>APSC-DV-001280</td>
<td>The application must protect audit information from any type of unauthorized read access.</td>
<td>HARDCODED_CREDENTIALS, LOCALSTORAGE_WRITE, SENSITIVE_DATA_LEAK, UNENCRYPTED_SENSITIVE_DATA, UNRESTRICTED_ACCESS_TO_FILE</td>
</tr>
<tr>
<td>APSC-DV-001290</td>
<td>The application must protect audit information from unauthorized modification.</td>
<td>HARDCODED_CREDENTIALS, LOCALSTORAGE_WRITE, SENSITIVE_DATA_LEAK, UNENCRYPTED_SENSITIVE_DATA, UNRESTRICTED_ACCESS_TO_FILE</td>
</tr>
<tr>
<td>APSC-DV-001300</td>
<td>The application must protect audit information from unauthorized deletion.</td>
<td>HARDCODED_CREDENTIALS, LOCALSTORAGE_WRITE, SENSITIVE_DATA_LEAK, UNENCRYPTED_SENSITIVE_DATA, UNRESTRICTED_ACCESS_TO_FILE</td>
</tr>
<tr>
<td>STIG ID</td>
<td>Description</td>
<td>Checker Names</td>
</tr>
<tr>
<td>-------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>APSC-DV-001350</td>
<td>The application must use cryptographic mechanisms to protect the integrity of audit information.</td>
<td>AWS_SSL_DISABLED, CONFIG.ATS_INSECURE, CONFIG.SPRING_BOOT_SSL_DISABLED, CONFIG.SPRING_SECURITY_LOGIN_OVER_HTTP, DISABLED_ENCRYPTION, HAPI_SESSION_MONGO_MISSING_TLS, 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</td>
</tr>
<tr>
<td>APSC-DV-001360</td>
<td>Application audit tools must be cryptographically hashed.</td>
<td>INSECURE_SALT, RISKY_CRYPTO, WEAK_PASSWORD_HASH</td>
</tr>
<tr>
<td>APSC-DV-001370</td>
<td>The integrity of the audit tools must be validated by checking the files for changes in the cryptographic hash value.</td>
<td>INSECURE_SALT, RISKY_CRYPTO, WEAK_PASSWORD_HASH</td>
</tr>
<tr>
<td>APSC-DV-001650</td>
<td>The application must authenticate all network connected endpoint devices before establishing any connection.</td>
<td>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</td>
</tr>
<tr>
<td>APSC-DV-001660</td>
<td>Service-Oriented Applications handling non-releasable data must authenticate endpoint devices via mutual SSL/TLS.</td>
<td>AWS_SSL_DISABLED, AWS_VALIDATION_DISABLED, BAD_CERT_VERIFICATION, CONFIG.MYSQL_SSL_VERIFY_DISABLED, CONFIG.REQUEST.StrictSSL_DISABLED, CONFIG.SPRING_BOOT_SSL_DISABLED, CONFIG.SPRING_SECURITY_LOGIN_OVER_HTTP, CORS_MISCONFIGURATION, CORS_MISCONFIGURATION_AUDIT, DISABLED_ENCRYPTION, HAPI_SESSION_MONGO_MISSING_TLS, HPKP_MISCONFIGURATION, INSECURE_COMMUNICATION, INSECURE_MULTIPEER_CONNECTION, RISKY_CRYPTO, SA.RISKY_CRYPTO, SENSITIVE_DATA_LEAK, STRICT_TRANSPORT_SECURITY, UNENCRYPTED_SENSITIVE_DATA</td>
</tr>
<tr>
<td>APSC-DV-001680</td>
<td>The application must enforce a minimum 15-character password length.</td>
<td>MISSING_PASSWORD_VALIDATOR, RAILS_DEVISE_CONFIG</td>
</tr>
<tr>
<td>APSC-DV-001690</td>
<td>The application must enforce password complexity by requiring that at least one uppercase character be used.</td>
<td>MISSING_PASSWORD_VALIDATOR, RAILS_DEVISE_CONFIG</td>
</tr>
<tr>
<td>APSC-DV-001700</td>
<td>The application must enforce password complexity by requiring that at least one lowercase character be used.</td>
<td>MISSING_PASSWORD_VALIDATOR, RAILS_DEVISE_CONFIG</td>
</tr>
<tr>
<td>APSC-DV-001710</td>
<td>The application must enforce password complexity by requiring that at least one numeric character be used.</td>
<td>MISSING_PASSWORD_VALIDATOR, RAILS_DEVISE_CONFIG</td>
</tr>
<tr>
<td>APSC-DV-001720</td>
<td>The application must enforce password complexity by requiring that at least one special character be used.</td>
<td>MISSING_PASSWORD_VALIDATOR, RAILS_DEVISE_CONFIG</td>
</tr>
<tr>
<td>STIG ID</td>
<td>Description</td>
<td>Checker Names</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>APSC-DV-001740</td>
<td>The application must only store cryptographic representations of passwords.</td>
<td>CONFIG.CONNECTION_STRING_PASSWORD, CONFIG.HARDCODED_CREDENTIALS_AUDIT,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CONFIG.HARDCODED_CREDENTIALS, CONFIG.HARDCODED_TOKEN,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CONFIG.SPRING_SECURITY_WEAK_PASSWORD_HASH, INSECURE_SALT,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RAILS_DEVISE_CONFIG, SENSITIVE_DATA_LEAK, UNENCRYPTED_SENSITIVE_DATA,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WEAK_PASSWORD_HASH</td>
</tr>
<tr>
<td>APSC-DV-001750</td>
<td>The application must transmit only cryptographically-protected passwords.</td>
<td>AWS_SSL_DISABLED, CONFIG.ATS_INSECURE, CONFIG.SEQUELIZE_INSECURE_CONNECTION,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>INSECURE_COMMUNICATION, INSECURE_MULTIPEER_CONNECTION, SENSITIVE_DATA_LEAK,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>STRICT_TRANSPORT_SECURITY, UNENCRYPTED_SENSITIVE_DATA</td>
</tr>
<tr>
<td>APSC-DV-001770</td>
<td>The application must enforce a 60-day maximum password lifetime restriction.</td>
<td>RAILS_DEVISE_CONFIG</td>
</tr>
<tr>
<td>APSC-DV-001795</td>
<td>The application password must not be changeable by users other than the administrator or the user with which the password is associated.</td>
<td>CONFIG.CONNECTION_STRING_PASSWORD, CONFIG.HARDCODED_CREDENTIALS_AUDIT,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CONFIG.HARDCODED_TOKEN, CONFIG.SPRING_SECURITY_HARDCODED_CREDENTIALS,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CONFIG.SPRING_SECURITY_REMEMBER_ME_HARDCODED_KEY, HARDCODED_CREDENTIALS,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>UNSAFE_BASIC_AUTH, UNSAFE_SESSION_SETTING</td>
</tr>
<tr>
<td>APSC-DV-001810</td>
<td>The application, when utilizing PKI-based authentication, must validate certificates by constructing a certification path (which includes status information) to an accepted trust anchor.</td>
<td>AWS_VALIDATION_DISABLED, BAD_CERT_VERIFICATION,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CONFIG.MYSQL_SSL_VERIFY_DISABLED, CONFIG.REQUEST_STRICTSSL_DISABLED,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CONFIG.SPRING_BOOT_SSL_DISABLED, HPKP_MISCONFIGURATION</td>
</tr>
<tr>
<td>APSC-DV-001820</td>
<td>The application, when using PKI-based authentication, must enforce authorized access to the corresponding private key.</td>
<td>HARDCODED_CREDENTIALS, UNSAFE_SESSION_SETTING</td>
</tr>
<tr>
<td>APSC-DV-001830</td>
<td>The application must map the authenticated identity to the individual user or group account for PKI-based authentication.</td>
<td>BAD_CERT_VERIFICATION</td>
</tr>
<tr>
<td>APSC-DV-001840</td>
<td>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.</td>
<td>BAD_CERT_VERIFICATION</td>
</tr>
<tr>
<td>APSC-DV-001995</td>
<td>The application must not be vulnerable to race conditions.</td>
<td>ATOMICITY, BAD_CHECK_OF_WAIT_COND, BAD_LOCK_OBJECT, DC.DEADLOCK, GUARDED_BY_VIOLATION, LOCK,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>LOCK_EVASION, LOCK_INVERSION, MISSING_LOCK, NON_STATIC_GUARDING_STATIC, ORDER_REVERSAL, SERVLET_ATOMICITY, SINGLETON_RACE, SLEEP, TOCTOU, VOLATILE_ATOMICITY</td>
</tr>
<tr>
<td>APSC-DV-002000</td>
<td>The application must terminate all network connections associated with a communications session at the end of the session.</td>
<td>CONFIG.JSONWEBTOKEN_NON_EXPIRING_TOKEN, CONFIG.UNSAFE_SESSION_TIMEOUT, CORS_MISCONFIGURATION_AUDIT, HPKP_MISCONFIGURATION, INSUFFICIENT_PRESIGNED_URL_TIME, JSONWEBTOKEN_IGNORED_EXPIRATION_TIME, TEMPORARY_CREDENTIALS_DURATION</td>
</tr>
<tr>
<td>APSC-DV-002210</td>
<td>The application must set the HTTPOnly flag on session cookies.</td>
<td>CONFIG.JAVAEE_MISSING_HTTPONLY</td>
</tr>
<tr>
<td>STIG ID</td>
<td>Description</td>
<td>Checker Names</td>
</tr>
<tr>
<td>------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------</td>
</tr>
<tr>
<td>APSC-DV-002220</td>
<td>The application must set the secure flag on session cookies.</td>
<td>INSECURE_COOKIE, INSECURE_REMEMBER_ME_COOKIE, UNSAFE_SESSION_SETTING</td>
</tr>
<tr>
<td>APSC-DV-002230</td>
<td>The application must not expose session IDs.</td>
<td>CONFIG.SPRING_SECURITY_SESSION_FIXATION, SESSION_FIXATION</td>
</tr>
<tr>
<td>APSC-DV-002240</td>
<td>The application must destroy the session ID value and/or cookie on logoff or browser close.</td>
<td>CONFIG.JSONWEBTOKEN_NON_EXPIRING_TOKEN, CONFIG. UNSAFE_SESSION_TIMEOUT, CORS_MISCONFIGURATION_AUDIT, HPKP_MISCONFIGURATION, INSUFFICIENT_PREIGNED_URL_TIMEOUT, JSONWEBTOKEN_IGNORED_EXPIRATION_TIME, SENSITIVE_DATA_LEAK, TEMPORARY_CREDENTIALS_DURATION, UNENCRYPTED_SENSITIVE_DATA</td>
</tr>
<tr>
<td>APSC-DV-002250</td>
<td>Applications must use system-generated session identifiers that protect against session fixation.</td>
<td>CONFIG.SPRING_SECURITY_SESSION_FIXATION, SESSION_FIXATION</td>
</tr>
<tr>
<td>APSC-DV-002260</td>
<td>Applications must validate session identifiers.</td>
<td>CONFIG.COOKIE_SIGNING_DISABLED</td>
</tr>
<tr>
<td>APSC-DV-002280</td>
<td>The application must not re-use or recycle session IDs.</td>
<td>CONFIG.JSONWEBTOKEN_NON_EXPIRING_TOKEN, CONFIG. UNSAFE_SESSION_TIMEOUT, CORS_MISCONFIGURATION_AUDIT, HPKP_MISCONFIGURATION, INSUFFICIENT_PREIGNED_URL_TIMEOUT, JSONWEBTOKEN_IGNORED_EXPIRATION_TIME, TEMPORARY_CREDENTIALS_DURATION</td>
</tr>
<tr>
<td>APSC-DV-002300</td>
<td>The application must only allow the use of DoD-approved certificate authorities for verification of the establishment of protected sessions.</td>
<td>AWS_VALIDATION_DISABLED, BAD_CERT_VERIFICATION, CONFIG.MYSQL_SSL_VERIFY_DISABLED, CONFIG.REQUEST_STRICTSSL_DISABLED, CONFIG.SPRING_BOOT_SSL_DISABLED, HPKP_MISCONFIGURATION</td>
</tr>
<tr>
<td>APSC-DV-002370</td>
<td>The application must maintain a separate execution domain for each executing process.</td>
<td>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</td>
</tr>
<tr>
<td>APSC-DV-002380</td>
<td>Applications must prevent unauthorized and unintended information transfer via shared system resources.</td>
<td>SENSITIVE_DATA_LEAK</td>
</tr>
<tr>
<td>APSC-DV-002390</td>
<td>XML-based applications must mitigate DoS attacks by using XML filters, parser options, or gateways.</td>
<td>WEAK_XML_SCHEMA, XML_EXTERNAL_ENTITY, XML_INJECTION, XPATH_INJECTION</td>
</tr>
<tr>
<td>APSC-DV-002400</td>
<td>The application must restrict the ability to launch Denial of Service (DoS) attacks against itself or other information systems. (cont.)</td>
<td>BUSBOY_MISCONFIGURATION, COM.ADDROF_LEAK, COM.BAD_FREE, COM.BSTR_ALLOCC, CONFIG.CORDOVA.EXCESSIVE_LOGGING, CONFIG.DEAD_AUTHORIZATION_RULE, CONFIG.DWR_DEBUG_MODE, CONFIG.JAVEE_MISSING_SERVLET_MAPPING, CONFIG.MISSING_JSF2_SECURITY_CONSRAINT, CONFIG.MYBATIS_MAPPER_SQLI, CONFIG.SOCKEITIO_MAXHTTPBUFFERSIZE_SET_TOO_LARGE, CONFIG.SOCKEITIO_ORIGINS_ACCEPT_ALL, CONFIG.SPRING_SECURITY_DISABLE_AUTH_TAGS, CONFIG.STRUTS2_CONFIG_BROWSER_PLUGIN, (cont. on next page)</td>
</tr>
<tr>
<td>STIG ID</td>
<td>Description</td>
<td>Checker Names</td>
</tr>
<tr>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>APSC-DV-002400 (cont.)</td>
<td>The application must restrict the ability to launch Denial of Service (DoS) attacks against itself or other information systems.</td>
<td>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, TAINED_SCALAR, UNENCRYPTED_SENSITIVE_DATA, UNLIMITED_CONCURRENT_SESSIONS, UNRESTRICTED_ACCESS_TO_FILE, USE_AFTER_FREE, VIRTUAL_DTOR, WEAK_XML_SCHEMA, WRAPPER_ESCAPE, XML_EXTERNAL_ENTITY</td>
</tr>
<tr>
<td>APSC-DV-002440</td>
<td>The application must protect the confidentiality and integrity of transmitted information.</td>
<td>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, HAPI_SESSION_MONGO_MISSING_TLS, 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</td>
</tr>
<tr>
<td>APSC-DV-002460</td>
<td>The application must maintain the confidentiality and integrity of information during preparation for transmission.</td>
<td>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, CONFIG.WEAK_SECURITY_CONSTRAINT, CORS_MISCONFIGURATION, CORS_MISCONFIGURATION_AUDIT, DC.WEAK_CRYPTO, DISABLED_ENCRYPTION, HARDCODED_CREDENTIALS, HPKP_MISCONFIGURATION, INSECURE_ACI, 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</td>
</tr>
<tr>
<td>STIG ID</td>
<td>Description</td>
<td>Checker Names</td>
</tr>
<tr>
<td>------------</td>
<td>------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>APSC-DV-002470</td>
<td>The application must maintain the confidentiality and integrity of information during reception.</td>
<td>AWS_SSL_DISABLED, BAD_CERT_VERIFICATION, CONFIG.ATS_INSECURE, CONFIG.REQUEST STRICTSSL_DISABLED, CONFIG.SEQUELIZE_INSECURE_CONNECTION, COR.S_MISCONFIGURATION, COR.S_MISCONFIGURATION_AUDIT, INSECURE_COMMUNICATION, INSECURE_MULTIPEER_CONNECTION, RISKY_CRYPTO, SA.RISKY_CRYPTO, SENSITIVE_DATA_LEAK, STRICT_TRANSPORT_SECURITY, UNENCRYPTED_SENSITIVE_DATA</td>
</tr>
<tr>
<td>APSC-DV-002480</td>
<td>The application must not disclose unnecessary information to users.</td>
<td>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_DIRECTORY_LISTING, EXPRESS_WINSTON_SENSITIVE_LOGGING, EXPRESS_XPOWERED_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</td>
</tr>
<tr>
<td>APSC-DV-002485</td>
<td>The application must not store sensitive information in hidden fields.</td>
<td>SENSITIVE_DATA_LEAK</td>
</tr>
<tr>
<td>APSC-DV-002490</td>
<td>The application must protect from Cross-Site Scripting (XSS) vulnerabilities.</td>
<td>ANGULAR_SCE_DISABLED, CONFIG.SPRING_SECURITY_DEPRECATED_XSS_HEADER, DOM_XSS, React._DANGEROUS.InnerHTML, VUE_TEMPLATEUnsafe_vHTML директивы, XSS</td>
</tr>
<tr>
<td>APSC-DV-002500</td>
<td>The application must protect from Cross-Site Request Forgery (CSRF) vulnerabilities.</td>
<td>CONFIG.CSRF_IGNORE_METHODS, CONFIG.DJANGO_CSRF_PROTECTION_DISABLED, CONFIG.HANA_XS_PREVENT_XSRF_DISABLED, CONFIG.SPRING_SECURITY_CSRF_PROTECTION_DISABLED, CONFIG.SYMfony_CSRF_PROTECTION_DISABLED, CSRF</td>
</tr>
<tr>
<td>STIG ID</td>
<td>Description</td>
<td>Checker Names</td>
</tr>
<tr>
<td>--------------</td>
<td>------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>APSC-DV-002510</td>
<td>The application must protect from command injection.</td>
<td>OS_CMD_INJECTION, TAIANTED_ENVIRONMENT_WITH_EXECUTION</td>
</tr>
<tr>
<td>APSC-DV-002520</td>
<td>The application must protect from canonical representation vulnerabilities.</td>
<td>BUSBOY_MISCONFIGURATION, FILE_UPLOAD_MISCONFIGURATION, JSP_DYNAMIC_INCLUDE, MULTER_MISCONFIGURATION, PATH_MANIPULATION, RUBY_VULNERABLE_LIBRARY</td>
</tr>
<tr>
<td>APSC-DV-002530</td>
<td>The application must validate all input.</td>
<td>ANGULAR_EXPRESSION_INJECTION, CONFIG.UNSAFE_SESSION_TIMEOUT, COOKIE_SERIALIZER_CONFIG, CORS_MISCONFIGURATION_AUDIT, DISTRUSTED_DATA_DESERIALIZATION, FORMAT_STRING_INJECTION, HOST_HEADER_VALIDATION_DISABLED, 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</td>
</tr>
<tr>
<td>APSC-DV-002540</td>
<td>The application must not be vulnerable to SQL Injection.</td>
<td>CONFIG.MYBATIS_MAPPER_SQLI, DYNAMIC_OBJECT_ATTRIBUTES, JSP_SQL_INJECTION, NOSQL_QUERY_INJECTION, RUBY_VULNERABLE_LIBRARY, SQLI, SQL_NOT_CONSTANT</td>
</tr>
<tr>
<td>APSC-DV-002550</td>
<td>The application must not be vulnerable to XML-oriented attacks.</td>
<td>WEAK_XML_SCHEMA, XML_EXTERNAL_ENTITY, XML_INJECTION, XPARPATH_INJECTION</td>
</tr>
<tr>
<td>APSC-DV-002560</td>
<td>The application must not be subject to input handling vulnerabilities.</td>
<td>NEGATIVE_RETURNS, REVERSE_NEGATIVE, TAIANTED_SCALAR</td>
</tr>
<tr>
<td>APSC-DV-002570</td>
<td>The application must generate error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries.</td>
<td>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</td>
</tr>
<tr>
<td>APSC-DV-002590</td>
<td>The application must not be vulnerable to overflow attacks.</td>
<td>ALLOC_FREE_MISMATCH, ARRAY_VS_SINGLETON, BAD_ALLOCS_ARITHMETIC, BAD_ALLOCS_STRLEN, BAD_CERT_VERIFICATION, BAD_FREE, BUFFER_SIZE, BUFFER_SIZE_WARNING, CALL_SUPER, CHAR_IO, COM_ADDROF_LEAK, COM.BAD_FREE, COM.BSTRALLOC, 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, (cont. on next page)</td>
</tr>
<tr>
<td>STIG ID</td>
<td>Description</td>
<td>Checker Names</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>APSC-DV-002590 (cont.)</td>
<td>The application must not be vulnerable to overflow attacks.</td>
<td>REVERSE_NEGATIVE, SENSITIVE_DATA_LEAK, SIGN_EXTRACTION, SIZECHECK, SQI, STACK_USE, STRING_NULL, STRING_OVERFLOW, STRING_SIZE, TAINED_SCALAR, USE_AFTER_FREE, VIRTUAL_DTOR, WRAPPER_ESCAPE, WRITE_CONST_FIELD, Y2K38_SAFETY</td>
</tr>
<tr>
<td>APSC-DV-003100</td>
<td>The application must use encryption to implement key exchange and authenticate endpoints prior to establishing a communication channel for key exchange.</td>
<td>BAD_CERT_VERIFICATION, CONFIG.CSRF_IGNORE_METHODS, CONFIG.DJANGO_CSRF_PROTECTION_DISABLED, CONFIG.HANA_XS_PREVENT_XSF-disabled, CONFIG.REQUEST STRICTSSL_DISABLED, CONFIG.SPRING_SECURITY_CSRF_PROTECTION_DISABLED, CONFIG.SYMFSN_CSRF_PROTECTION_DISABLED, CONFIG.UNSAFE_SESSION_TIMEOUT, CORS_MISCONFIGURATION, CORS_MISCONFIGURATION_AUDIT, CSRF_CSRF_MISCONFIGURATION_HAPI_CRUMB, HOST_HEADER_VALIDATION_DISABLED, HPKP_MISCONFIGURATION, INSUFFICIENT_PRESIGNED_URL_TIMEOUT, JSONWEBTOKEN_UNTRUSTED_DECODE, MULTER_MISCONFIGURATION, RISKY_CRYPTO, SA_RISKY_CRYPTO, TEMPORARY_CREDENTIALS_DURATION, UNCHECKED_ORIGIN, WEAK_GUARD</td>
</tr>
<tr>
<td>APSC-DV-003110</td>
<td>The application must not contain embedded authentication data.</td>
<td>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</td>
</tr>
<tr>
<td>APSC-DV-003215</td>
<td>The application development team must follow a set of coding standards.</td>
<td>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, EXPPLICIT THIS_EXPECTED, HFA, HIBERNATE_BAD_HASHCODE, HPKP_MISCONFIGURATION, IDENTICAL_BRANCHES, IDENTIFIER_TYPO, INCOMPATIBLE_CAST, INSECURE_HTTP_FIREWALL, INVALIDATE_ITERATOR, MISCONFIGURATION, MISMATCHED_ITERATOR, MISSTRA_CAST, MISSING_ASSIGN, MISSING_AUTHZ, MISSING_BREAK, MISSING_COMM, MISSING_COPY, MISSING_MOVE_ASSIGNMENT, MISSING_RESTORE, MISSING_RETURN, MISSING_THROW, MIXED_ENUMS, NEGATIVE_RETURNS, NESTING_INDENT_MISMATCH, (cont. on next page)</td>
</tr>
</tbody>
</table>
### STIG ID | Description | Checker Names
--- | --- | ---
APSC-DV-003215 (cont.) | The application development team must follow a set of coding standards. | 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, 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, SELF_ASSIGN, SECURE_TEMP, SIZEOF_MISMATCH, SLEEP, STREAM_FORMAT_STATE, SWAPPED_ARGUMENTS, TAINT_ASSERT, UNINIT, UNINITCTOR, UNINTENDED_GLOBAL, UNINTENDED_INTEGER_DIVISION, UNREACHABLE, UNUSED_VALUE, USELESS_CALL, USER_POINTER, USE_AFTER_FREE, VARARGS, VIRTUAL_DTOR, WRAPPER_ESCAPE, WRONG_METHOD

This ASD STIG ID is also partially covered by checkers for the SEI CERT C/C++, SEI CERT Java, MISRA, and AUTOSAR standards. Contact Synopsys to obtain a full list of checkers that address the issues related to STIG 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.FILE_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_INNULL, TAINTED_SCALAR

This datasheet applies to Coverity 2020.12 and later releases.

---

### 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](http://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

©2020 Synopsys, Inc. All rights reserved. Synopsys is a trademark of Synopsys, Inc. in the United States and other countries. A list of Synopsys trademarks is available at [www.synopsys.com/copyright.html](http://www.synopsys.com/copyright.html). All other names mentioned herein are trademarks or registered trademarks of their respective owners. December 2020