Software Security Assurance

Software Security Assurance

SSA Knowledgebase

Knowledgebase Search

Software Security Test Cases

Rows per page: 30

Search

- Authentication Testing
- Authorization Testing
- Testing Audit Trails
- Testing Session Management
- Data Security Testing
- Testing for Client Side Attacks
- Testing Data Validation
- Buffer Overflow Testing
- Configuration Testing

Configuration Testing

1. Test for SSL/TLS

Objective: To test if application uses weak cryptographic options.

Test case ID	Description	Expected results
Config.1.1	Validate if application hosted without SSL	Application is hosted with SSL
Config.1.2	Validate if recent version of protocol and strong cipher suite is used for certificate	Application deploys latest version of protocol and strong cipher suite
Config.1.3	Validate if certificate issuer, date and website names are proper and clients are not issuing warning against them	Certificates are issued by trusted certification authority, period is valid and website name matches with issued certificate
Config.1.4	Check if server's private key is stored securely	Server's private key is stored securely

2. Test for web and application server

Objective: To test if web/application servers are configured securely.

Test case ID	Description	Expected results
Config.2.1	Validate if latest secure version of product are installed	Latest secure version of products are installed
Config.2.2	Check if directory traversal are enabled	Directory traversal is disabled
Config.2.3	Validate if application deployed on default configuration	Each configuration parameter understood thoroughly and after that it is enabled / disabled or removed
Config.2.4	Validate if default, old, sample or demo files present on server	Server is hardened and all default configuration, old files, samples, demo and accounts are removed from server
Config.2.5	Validate if server run with least privilege	Server is running with least privilege account
Config.2.6	Validate if there are backdoor account, test account or default accounts present on server	Only administrative and user accounts present on server. Default and test accounts are removed from server
Config.2.7	Validate if sensitive configuration data are encrypted	All sensitive configuration data (i.e. credentials) are encrypted
Config.2.8	Validate if configuration backup is stored securely	Backup of configuration is stored securely

Test case ID	Description	Expected results
Config.2.9	Validate if file extensions are handled properly	There is default response for all unknown file extensions
Config.2.10	Validate if change management process exist for configuration change and used effectively	Change management process is followed for smallest configuration change
Config.2.11	Validate if logs are properly generated, securely stored and review periodically	All defined events are captured into logs and they are written on write once media, media access is restricted to authorized users and review periodically.
Config.2.12	Administrative activity logs are generated separately (if support available in product)	Logs for administrative activity are generated separately and all administrative activity follow change management process
Config.2.13	Validate if developer has access to application hosted on production system	Developers are not given access to application hosted on production system. Only designated administrators have access to production system
Config.2.14	Validate if IP based restriction applied for remote management	IP based restriction is applied for remote management
Config.2.15	Validate if strict restriction applied on protocol methods	Web and application server allows defined methods only

3. Test for database server

Objective: To test if database servers are configured securely

Test case ID	Description	Expected results
Config.3.1	Validate if latest secure version of product are installed	Latest secure version of products are installed
Config.3.2	Validate if server run with least privilege	Server is running with least privilege account
Config.3.3	Validate if database account and system accounts are different	System and database accounts are different
Config.3.4	Validate if sensitive data stored into database is encrypted	Sensitive data stored into database is encrypted and even DBA couldn't convert it in clear text
Config.3.5	Validate if application connects to database using DBA privilege user	Application has least privilege account. For read functionality there is separate user and for modify/delete functionality there is separate user

Test case ID	Description	Expected results
Config.3.6	Validate if communication with database happen through secure channel	Communication with database happen through secure channel
Config.3.7	Validate if auditing & logging is enabled for sensitive change / transactions	Database auditing and logging functionality is enabled and also all sensitive change / transactions

4. Test for application configuration

Objective: To test if application is configured securely

Test case ID	Description	Expected results
Config.4.1	Validate if application configuration are restricted and access reconciliation happen on periodic basis	Application configuration are accessible to authorized users only and reconciliation for account and privileges happens on periodic basis
Config.4.2	Validate if changes to configuration follow change management process	Change to application configuration follow change management process
Config.4.3	Validate if sensitive configuration data is encrypted	Configuration data is encrypted

5. Test for infrastructure configuration

Objective: To test if infrastructure is configured securely

Test case ID	Description	Expected results
Config.5.1	Validate if latest secure version of product are installed	Latest secure version of product are installed
Config.5.2	Validate if components are hardened as per application requirement	Hardening is done as per requirement
Config.5.3	Validate if IP based restriction applied for remote management	IP based restriction is applied for remote management
Config.5.4	Validate if default accounts are changed and unwanted features, services and components are disabled	Default accounts are renamed, periodic credentials are changed, unnecessary features, services and components are disabled
Config.5.5	Validate if secure protocols are used for administrative activity	Secure protocols (i.e. HTTPS, SSH, SCP) are used for administrative activity
Config.5.6	Validate if infrastructure penetration testing report has any finding	There are no findings into infrastructure penetration testing report