





SSA Knowledgebase




Knowledgebase Search

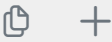
Software Security Test Cases

Rows per page: 30 

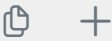
Search



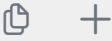
Authentication Testing



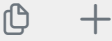
Authorization Testing



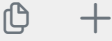
Testing Audit Trails



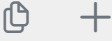
Testing Session Management



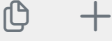
Data Security Testing



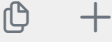
Testing for Client Side Attacks



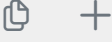
Testing Data Validation



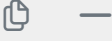
Buffer Overflow Testing



Configuration Testing



Denial of Service Testing



Denial of Service Testing

1. Test for account lockout

Objective: To test if application prevent legitimate user through lockout

Test case ID	Description	Expected results
DoS.1.1	Validate if application locks user account after specified number of unsuccessful login attempts	Application locks user account after specified number of unsuccessful login attempts
DoS.1.2	Validate if there is provision to unlock user account after validating user's identity	Application has provision through which user can unlock their account automatically
DoS.1.3	Validate if administrative accounts get locked	Administrative account can't be locked however IP based access restriction is applied to avoid administrative account lockout
DoS.1.4	Validate if application display different response for unsuccessful login attempt through various entry points	Application displays same response irrespective of entry point and user input
DoS.1.5	Validate if anti brute forcing mechanism is applied into application	Application uses CAPTCHA to avoid automated attacks

2. Test for computational and storage resource exhaust

Objective: To test if computational and storage resource can be exhausted by supplying malicious inputs.

Test case ID	Description	Expected results
DoS.2.1	Validate if application accept large size data as input	Inputs are checked by validate library and if length is more then specified one, error response is delivered
DoS.2.2	Validate if certain queries take more time if input contain Sql wildcard characters	Application validates input for restricted characters so Sql wildcard characters are not reached upto database query
DoS.2.3	Validate if supplied input or its derivative is used to create counter for loop or array bound or object creation or allocation size.	Application validates all inputs before use. It do not use supplied inputs for such purposes. If they are used, application has upper bound check for each usage

Test case ID	Description	Expected results
DoS.2.4	Validate if application handle huge data as input and if data is written on log file	Application handles huge data however to put data in file, there is an upper bound on size of data written into log. After specified size, application sends an alert to administrator and discards data
DoS.2.5	Validate if application releases system objects like file, memory, thread, database, registry, named pipe, socket after use	Application leaves no open connection after use.
DoS.2.6	Validate if application stores large amount of data into session	Application don't have requirement to store large amount of data into session. Data is validated for length along with other checks as soon as received.

3. Test for race condition

Objective: To test if race condition is generated through malicious inputs

Test case ID	Description	Expected results
DoS.3.1	Validate if application writes into shared area	Application do not write into shared area
DoS.3.2	Validate if write operation is performed on shared resource by multiple threads without locking it	Each thread in application locks a shared resource before use and releases it on completion of operation
DoS.3.3	Validate if temporary object (i.e. file) names are randomly generated	Application generates temporary objects with random names
DoS.3.4	Validate if global objects or variables are used into application	Application do not use global objects or variables
DoS.3.5	Validate if application work properly with multi processor system	Concurrency tests are performed on multi processor system and application works properly
DoS.3.6	Validate if multiple locks are released in opposite order (last lock shall be released first).	Locks are released in opposite order
DoS.3.7	Validate if signals are delivered to other threads before completion of operation	Signals are delivered only after completion of operation.
DoS.3.8	Validate if transactional integrity is maintained into system	Transactional integrity is maintained into system