





# SSA Knowledgebase




Knowledgebase Search

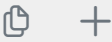
Software Security Test Cases

Rows per page: 30 

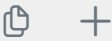
Search



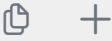
Authentication Testing



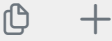
Authorization Testing



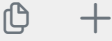
Testing Audit Trails



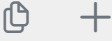
Testing Session Management



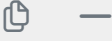
Data Security Testing



Testing for Client Side Attacks



Testing Data Validation



## Testing Data Validation

**\*\*1. Test for input validation\*\***

Objective: To test if application accepts input without validation.

Test case ID	Description	Expected results
DataValid.1.1	Validate if application accepts input without validation	Application always validates user input
DataValid.1.2	Check if input is validated immediately after user submits input	User input validate as soon as application receives user input

### \*\*2. Test for SQL injection\*\*

Objective: To test if SQL queries can be modified to perform unintended operation

Test case ID	Description	Expected results
DataValid.2.1	Validate if application accepts restricted characters as input and build database query	Application does not accept restricted characters as input. They are filtered at input validation stage
DataValid.2.2	Validate if application displays database error/exception message to end user	Application do not display database error/exception message. Incase of exception, end user is displayed generic error message
DataValid.2.3	Validate if application use concatenated strings to build Sql statements	Application uses parameterized queries
DataValid.2.4	Check if application uses parameterized queries	All queries used in application are parameterized queries
DataValid.2.5	Check if application validate inputs to stored procedures	Application validates input to stored procedures
DataValid.2.6	Validate that all SQL statements are executed with "Execute Only" permissions	All SQL statements are executed with "Execute Only" permissions
DataValid.2.7	Validate if application execute queries with least privilege account	Application uses least privilege database user for query execution

### \*\*3. Test for LDAP injection\*\*

Objective: To test if LDAP queries can be modified to perform unintended operation

Test case ID	Description	Expected results
DataValid.3.1	Validate if application accepts restricted characters as input and build LDAP query	Application does not accept restricted characters as input. They are filtered at input validation stage
DataValid.3.2	Validate if application displays LDAP error message to end user	Application do not display LDAP error message.
DataValid.3.3	Validate if application allow LDAP queries with attribute value '*'	* is part of restricted character set and not accepted as input

**Test case ID Description****Expected results**

Check if application allow end user to supply input that make LDAP query always true

Application validates each input from user and application do allow user to supply inputs that make LDAP query always true

**\*\*4. Test for XML injection\*\***

Objective: To test if XML processing failed to restrict malicious input

**Test case ID Description****Expected results**

Validate if XML constructs are validated through DTD before processing

DTDs are available for all XML constructs and XML data are validated before processing

Validate if restricted characters are accepted as input

Restricted characters are not allowed as input

Validate if XML tags are accepted as input

XML tags are not accepted as input

Check if captured XML is used to generate html, CDATA is stored as encoded characters

Application sends html data as encoded values

**\*\*5. Test for XPath injection\*\***

Objective: To test if XPath queries can be modified to perform unintended operation

**Test case ID Description****Expected results**

Validate if restricted characters are accepted as input

Restricted characters are not allowed as input

Check if all inputs forming XPath query are validated before forming query

Restricted characters are not allowed as input

Check if XQuery is used instead of XPath query

XQuery is used for XPath query

**\*\*6. Test for code execution\*\***

Objective: To test if application allow arbitrary code execution

**Test case ID Description****Expected results**

Validate if user supplied SSI statements are executed by application

SSI support is not enabled for application and application do not execute SSI statements

Validate if user supplied source code statement are executed by application

Application treat user supplier source code as data and do not execute them

Validate if application allow user to supply website address as input and display content from those websites

Application do not allow users to supply website address

**Test case ID Description****Expected results**

DataValid.6.4 Validate if application allow user to supply filename as input and perform file operation on given file

Application do not take file name as input from user

DataValid.6.5 Check if application has functionality that uses native or system calls. Input for such call are derived from user input

Application do not use native or system call

**\*\*7. Test for file processing\*\***

Objective: To test if application performs file operations correctly

**Test case ID Description****Expected results**

DataValid.7.1 Validate if application's file related calls are safe

File related calls are tested during functional testing and confirmed that they are safe

DataValid.7.2 Validate if file parsers function properly

Fuzz testing is done for file parser and files are processed correctly

DataValid.7.3 Validated file upload functionality is secure

Only approved file extensions are uploaded and access to stored file is restricted

**\*\*8. Testing email functionality\*\***

Objective: To test if email functionality in application function properly

**Test case ID Description****Expected results**

DataValid.8.1 Validate if application allow mail relaying

Application do not allow mail relaying

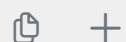
DataValid.8.2 Validate if application allow arbitrary mail command (SMTP/IMAP) as part of user supplied parameters

Application validates user inputs, state and commands properly and mail server is also hardened

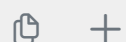
DataValid.8.3 Check if end user is displayed mail errors

End user is not displayed mail server error message but simple error is displayed

Buffer Overflow Testing



Configuration Testing



Denial of Service Testing

