





SSA Knowledgebase




Knowledgebase Search



Software Security Test Cases

Rows per page: 30 



Search



Authentication Testing

Authorization Testing

Authorization Testing

****1. Testing restricted file access****

Objective: To test if application allows access to restricted files directly.

Test case ID	Description	Expected results
Autho.1.1	Validate if application allow direct access files into restricted directory	Files are not accessible
Autho.1.2	Validate if server configuration files are accessible to non administrative users	Server configuration or property file is not accessible to non administrative users
Autho.1.3	Validate if application allow direct access to files outside webroot	Application do not allow access to files outside webroot
Autho.1.4	Validate if application allow user to create file on web server through PUT request	Application do not allow PUT method usage

****2. Testing for path traversal****

Objective: To test if application allows access restricted files through path traversal.

Test case ID	Description	Expected results
Autho.2.1	Validate if application accept URL with "../" string (and its url encoded, double encoded values)	Files are not accessible by providing ../ as input
Autho.2.2	Validate if application accept URL with url encoded or double encoded or UTF-8 encoded values of dot (.) , slash (/) or backslash (\)	Application do not accept URL encoded values that can form "../" construct
Autho.2.3	Validate if application accept filename as input from user	Application do not accept filename from user
Autho.2.4	Validate if application uses hidden directories with public access	Application do not use hidden directories with public access
Autho.2.5	Validate if application displays directory listing	Application do not display directory listing

3. Testing horizontal privilege escalation

Objective: To test if application allows access restricted functionality to user who don't have privileges

Test case ID	Description	Expected results
Autho.3.1	Validate if user can access functions and perform operations for which user do not have privileges	Users are not allowed to access functions or operations for which they do not have privilege
Autho.3.2	Validate if it one user can access functions and resources for other user who has same privileges	User can not access resource / functionality for other users
Autho.3.3	Validate if user is able to perform action or access resource which is explicitly denied for user	User can not perform action which is explicitly denied
Autho.3.4	Validate if user is able to access resources after logout	User can not access resource after logout

4. Testing vertical privilege escalation

Objective: To test if application allows access functionality allowed only for higher privilege users

Test case ID	Description	Expected results
Autho.4.1	Validate if user can access functions and perform operations for which user do not have privileges	Users are not allowed to access functions or operations for which they do not have privilege

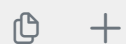
Test case ID	Description	Expected results
Autho.4.2	Validate if it one user can access functions and resources for other user who has low privileges	User can not access resource / functionality for other users
Autho.4.3	Validate if user could perform actions assigned for high privilege users	User can not access resource / functionality which require higher privilege
Autho.4.4	Validate if application user can access administrative functionality	Normal user can not access administrative functionality
Autho.4.5	Check if users are able to execute functions or operations with non application level privileges (OS user, application server admin, database user)	Users can not perform application operations or execute functions with non application privileges
Autho.4.6	Validate if user could bypass approval hierarchy	Users can not bypass approval hierarchy

5. Testing for Special Cases

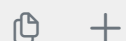
Objective: To test if application allows access of information in emergencies

Test case ID	Description	Expected results
Autho.5.1	Validate if user can access basic and necessary information (like Health Information) in emergency situation	Emergency Access Procedure is established and information is accessible faster and on time.

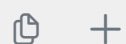
Testing Audit Trails



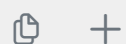
Testing Session Management



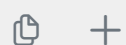
Data Security Testing



Testing for Client Side Attacks



Testing Data Validation



Buffer Overflow Testing

