

Test Case ID	Test Objective	Steps to Execute	Priority	Author	Date
TC01	Verify access control for unauthorized users	1. Log in as a regular user. 2. Attempt to access an admin-only page.	High	May	2025-01-16
TC02	Validate role-based permissions	1. Log in as admin. 2. Create a resource. 3. Log in as a viewer. 4. Attempt to edit the created resource.	High	May	2025-01-16
TC03	Prevent privilege escalation	1. Log in as a regular user. 2. Attempt to modify your role via API.	High	May	2025-01-16
TC04	Prevent direct object reference exploitation	1. Log in as User A. 2. Modify the URL parameter (e.g., /api/users/1) to access another user's data.	Medium	May	2025-01-16
TC05	Validate API endpoint protection	1. Use Postman or curl to send requests to various endpoints. 2. Observe the response for proper authentication and authorization headers.	High	May	2025-01-16
TC06	Test horizontal access control	1. Log in as User X. 2. Attempt to access User Y's data using User X's credentials.	Medium	May	2025-01-16
TC07	Test vertical access control	1. Log in as a user with viewer permissions. 2. Attempt to perform an action requiring admin permissions.	Medium	May	2025-01-16
TC08	Validate session management	1. Log in as a user. 2. Log out. 3. Attempt to access a protected page without re-authenticating.	High	May	2025-01-16
TC09	Ensure multi-factor authentication (MFA) enforcement	1. Log in as a user. 2. Attempt to perform a critical action without MFA.	High	May	2025-01-16
TC10	Verify audit logging	1. Attempt unauthorized actions (e.g., access admin page). 2. Review the system logs to ensure the actions are recorded.	Low	May	2025-01-16