

Version <X.Y>

<Date>

Prepared for:

<Organization>

Prepared by:

<Author(s)>

Contract: <Contract ID>

<Other Front Matter>

<Organization-specific legal boilerplate, if applicable>

For Internal <Organization> Use. This document was prepared for authorized distribution only. It has not been approved for public release.



This document is derived from  
*MITRE Adaptive Capabilities Testing (ACT)™*.  
act.mitre.org | act@mitre.org

<Organization>

MITRE Adaptive Capabilities Testing (ACT)™

<System Name> (<System Acronym>)

Web Application Assessment  
Guide and Checklist

Record of Changes

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Responsible Author | Description of Change |
| 1.0 | May 30, 2025 | Mike Gazdus | Initial release of MITRE ACT templates and work aids. |

Use of This Guide and Checklist

This is *not* a **comprehensive** checklist. Rather, it is intended to help the assessor gather their thoughts on the many areas of a web application that need to be tested to assure a comprehensive vulnerability assessment of the application. In addition to using the items identified in this guide, a baseline document of security controls must be used to ensure that the system’s identified security controls are in-place and working as intended. These tests should be mapped to the security baseline to ensure a comprehensive test.

**Note to the Author Using this Template:**

This is a *template* for producing a MITRE ACT template tailored to your specific organization. Everything in this template can and should be customized by you to meet your organization’s specific needs and objectives.

Various objects and sections of text throughout the template are highlighted – these are **items that are very likely to require customization**, but you are free and encouraged to **edit the entire document and process** to suit your organization’s needs. By documenting your actual ACT process (including how it deviates from the baseline herein) in this template you are ensuring that your ACT assessments are consistent, repeatable, and can be accurately compared to assessments from other organizations’ implementations of ACT.

Table of Contents

[1. Logistics 1](#_Toc199444066)

[2. Pre-Test Checklist 1](#_Toc199444067)

[3. Session Control Tests 1](#_Toc199444068)

[4. Identification & Authentication 3](#_Toc199444069)

[5. Authorization & Access Control 6](#_Toc199444070)

[6. SQL Injection 8](#_Toc199444071)

[7. Cross-Site Scripting (XSS) 8](#_Toc199444072)

[8. Database 8](#_Toc199444073)

[9. Infrastructure 9](#_Toc199444074)

[10. Input Validation 9](#_Toc199444075)

[11. Audit 9](#_Toc199444076)

[12. Error Handling 10](#_Toc199444077)

# 

# Assessment Logistics

|  |  |
| --- | --- |
| Official System Name | Official System Name |
| System Acronym | ABCD |
| Assessor Name | John Doe |
| Assessment Date(s) | Jan 1 – 3, 2025 |

# Pre-Test Checklist

|  |  |
| --- | --- |
| Assessment Check | Assessment Result |
| 1. Does the application test environment emulate the Production environment in functionality? |  |
| 1. Have application developer interviews been scheduled? |  |
| 1. Have test accounts been created? |  |
| 1. Have test accounts been used for system logon? |  |
| 1. Has a live application demonstration been performed? |  |
| 1. Is the application fully functional? |  |

# Session Control Tests

|  |  |
| --- | --- |
| Assessment Check | Assessment Result |
| 1. Session protected with TLS? |  |
| 1. Logon page loaded with TLS rather than pass-off? |  |
| 1. Can session be modified by changing URL from HTTPS to HTTP? |  |
| 1. If App is using HTTPS, confirm that port 80 is not open on the server. Use automated tool to capture logon credentials if port 80 is open. |  |
| 1. Which session ID exchange mechanism is used to maintain session state? Cookies? Hidden form fields? URL parameters? Can a second exchange mechanism be used? |  |
| 1. Identify which tokens may be used for session management after authentication. Remove identified tokens successively to determine the session token. |  |
| 1. Session fixation: Is session token changed after authentication? |  |
| 1. Are a fresh set of tokens issued with each logon/logoff? |  |
| 1. Does the session ID use the default name/value pair that gives insight to the technology used? Does the session ID have a length of at least 128 bits? Is the token random? |  |
| 1. Modify portions of session token to determine whether the entire token is required. |  |
| 1. Logon with different usernames to see variations in the token and any patterns. Do similar usernames show similar tokens? |  |
| 1. Do tokens use a concealed sequence, time dependency, or weak random number generation? |  |
| 1. Use automated tool to check for randomness of token. |  |
| 1. Can an invented token be supplied successfully that meets the current format? |  |
| 1. Can an old session token be reused? |  |
| 1. Can session token be decoded? |  |
| 1. Is session token transmitted in URL query string? |  |
| 1. Are concurrent sessions permitted? Is there a valid business reason for concurrent sessions if they are permitted? |  |
| 1. Liberal cookie scope? Confirm the HTTP Response Set-Cookie header attributes are configured: domain=app.hostname.org; path=/app/; httponly; secure; |  |
| 1. Does the application session timeout? Acceptable timeout length? |  |
| 1. Session invalidated after logout (Does browser “Back ß” button give access to previously viewed content after logout)? |  |
| 1. Is session expiration implemented on the server side? |  |
| 1. Is session destroyed through framework API? |  |

# Identification & Authentication

|  |  |
| --- | --- |
| Assessment Check | Assessment Result |
| 1. Is a Warning Banner present for the application? |  |
| 1. Logon: Password sufficient length enforced? |  |
| 1. Change Password Screen: Password sufficient length enforced? |  |
| 1. Forgot Password Screen: Password sufficient length enforced? |  |
| 1. Logon: Password complexity enforced? |  |
| 1. Change Password Screen: Password complexity enforced? |  |
| 1. Forgot Password Screen: Password complexity enforced? |  |
| 1. Password & username similarity? |  |
| 1. Change passwords. Password history enforced? |  |
| 1. Change Password screen accessible without authentication? |  |
| 1. Change Password screen contain a username field—hidden or visible? |  |
| 1. Change Password screen ask for existing password? |  |
| 1. Account lockout after unsuccessful logon attempts? |  |
| 1. Acceptable lockout threshold enforced by system? |  |
| 1. Are there Hidden form fields with I&A information? |  |
| 1. Brute force: Permits unrestricted guessing attempts on Logon, Change Password and Forgot Password screens? Logon processing occurring if account is suspended? |  |
| 1. Can account names be harvested through the logon screen? Change password screen? |  |
| 1. Does the application indicate whether accounts/passwords are valid through informational messages? Check for different application responses to determine valid usernames/passwords. Try an incorrect username and then a correct username for differences. |  |
| 1. Is the POST method used to transmit credentials / session token / sensitive information? |  |
| 1. Can a POST request be changed to a GET to transmit credentials? |  |
| 1. Passing of credentials in the clear? |  |
| 1. Does App notify users of last logon day/time and any unsuccessful attempts since last logon (usually in High systems)? |  |
| 1. Are any test accounts present in the Production application? |  |
| 1. Are any group accounts in use? |  |
| 1. Major system action (e.g. password change, account suspension) notification sent to user’s registered email? |  |
| 1. Easily guessed “secret” questions on Forgot Password Screen? |  |
| 1. Is “secret” question enumeration possible on logon screen with fresh logons? |  |
| 1. Are “secret” questions only presented after initial authentication? |  |
| 1. Is the same “secret” question presented to the user until answered correctly? |  |
| 1. Is “secret” question enumeration possible by modifying hidden form fields? |  |
| 1. Forgotten password displayed by application after challenge met? |  |
| 1. Account recovery drop user into authenticated session after challenge met or is recovery URL sent to user’s registered email address? |  |
| 1. “Remember Me” functionality exploitable for another user? Does it use a persistent cookie, username or other identifier that can be enabled? |  |
| 1. Is self-registration permitted? |  |
| 1. Are unique usernames enforced? |  |
| 1. System-generated usernames? Predictable usernames? Predictable passwords? |  |
| 1. New accounts sent out-of-band? Time-limited? Require password change on logon? |  |
| 1. Account activation/recovery URL predictable? Reusable? Time-limited? |  |
| 1. Fail-open authentication logic? Does modification of IA credentials give illegitimate access? |  |
| 1. Defects in multistage logon? Can any particular stage be bypassed? Does App leak info on which stage has been bypassed? |  |
| 1. CAPTCHA solution in hidden form field or image tag? |  |
| 1. Re-authentication required for sensitive functions (password updates, sensitive transactions, shipping a purchase to a new address)? |  |
| 1. Self-signed certificates used? Strong ciphers used? |  |
| 1. Does the App use two-factor authentication for logon (usually sensitive Apps)? What second factor is used (e.g. RSA hardware token, PIV card, etc)? What e-Authentication level does the App use (Level 1, 2, 3, 4)? Is this e-Auth level sufficient considering the sensitivity of the data it processes? |  |
| 1. Can the App distinguish between a human and Bot for initial registration of new accounts? What controls are in-place to prevent automated registration through a Bot? Investigate. |  |
| 1. Is IP geo-location functionality present to detect IPs from unusual locations (e.g. overseas)? |  |
| 1. Is an IP/identity velocity filter used? Investigate. |  |
| 1. For Apps that require sensitive info for registration (i.e. Name, DOB, SSN, address), what controls or processes are in-place to prevent a bad actor from registering with a victim’s stolen PII data? Investigate. |  |
| 1. How does the App perform Identity Proofing? Investigate. |  |
| 1. If Identity Proofing fails, is there a backup mechanism to proof App users. Describe. |  |
| 1. Does the App enforce reliable initial registration for new accounts through some combination of a layered identity proofing security approach (e.g. knowledge-based authentication (KBA) questions AND out-of-band authentication AND financial account verification (bank account, credit card info))? Describe. |  |
| 1. Note: Apps should make limited use of KBA. Use of PII from a user’s credit file is no longer a best practice. If KBA questions are used for initial registration, do questions incorporate both the user’s credit and biographical data? Is KBA the only control for authentication or is a layered security approach used? Are KBA questions presented to the user through a 3rd party (e.g. Experian, Equifax, Lexis Nexus)? Is there a time limit for answering the questions? Does question difficulty increase if some questions are answered incorrectly? |  |
| 1. Does the organization use internally generated KBA questions for follow-up authentication (e.g. “What was last transaction date?”, “What was last transaction amount?”, etc.) |  |
| 1. Best Practice: Is out-of-band (OOB) authentication used as part of the layered authentication approach? (e.g. PIN sent via snail mail to user’s registered address of record, message sent to user’s previously registered e-mail address, phone call to user, credit card verification)? Is the OOB authentication step required to be complete before a password to the App can be obtained? Does follow-up authentication require username/password AND OOB authentication prior to App access? |  |
| 1. How does this App’s Identity Proofing process compare against other agency/industry best practices? Investigate. |  |
| 1. What anti-fraud countermeasures does the App implement to detect & mitigate/eliminate fraud? Investigate. |  |
| 1. Is fraud intelligence information provided by an external organization? |  |
| 1. Is a Risk Analytics engine used to perform fraud risk scoring? If risk scoring is used, are transactions blocked if a risk score exceeds the threshold? Can the risk analytics engine capability be modified in accordance with the current threat landscape? |  |
| 1. Is some type of anomaly detection analytics used to identity atypical user behavior (e.g. odd frequency, time of day, attempted activity)? Is device profiling used to identify devices used in previous fraud attempts? Are analytics near real-time? |  |
| 1. Does the App notify account holders of attempted/successful transactions? How does the App notify users? |  |

# Authorization & Access Control

|  |  |
| --- | --- |
| Assessment Check | Assessment Result |
| 1. Does URL contain any information that can be used or exploited by another user? |  |
| 1. Can a static web server resource be accessed through the URL? |  |
| 1. Can the URL be manipulated to escalate privileges? Can administrator content be accesssed as a general user. |  |
| 1. Can browsing be forced? Try unauthorized URLs discovered during Spidering. |  |
| 1. Is Admin role functionality displayed in URL? Easy-to-guess? |  |
| 1. Does HTML or JavaScript indicate admin functionality? |  |
| 1. (Vertical Privilege Escalation) Can privileged functions be performed as a non-privileged user? |  |
| 1. (Horizontal Privilege Escalation) Can privileged functions be performed as a non-privileged user at the same role/level? |  |
| 1. Are users restricted to least privilege? |  |
| 1. Can functionality in a multistage function be bypassed? Try each stage individually. |  |
| 1. Does ‘admin=true’ in the URL query string or POST method give additional access? |  |
| 1. Per-transaction authentication implemented for security critical applications? |  |
| 1. Is there fine-grained user access to database tables using a table of privileges? |  |
| 1. Are database queries executed with only the necessary privileges? |  |
| 1. Is a centralized component used for application access control? |  |
| 1. Have access control roles and the resources users have access to been documented? |  |
| 1. Is default web server debug functionality available (e.g. /phpinfo.php in URL)? Spider to discover different directories and resources. |  |
| 1. Is default web server functionality available? |  |
| 1. Is a default web server directory listing available? |  |
| 1. Are unnecessary HTTP methods available on the web server (OPTIONS, TRACE, PUT, DELETE)? |  |
| 1. Can the web server be used as a proxy? |  |
| 1. Does browser use autocomplete=”on” in form tag or input field? |  |
| 1. Try deleting parameters and their values to determine whether any logic flaws exist. |  |
| 1. Is there a file upload capability that permits unauthorized file type uploads? |  |
| 1. Does the application permit an unauthorized file upload when the file extension is changed to an authorized file type? |  |
| 1. Is the content of the file checked to determine whether the uploaded file is an authorized file type? |  |
| 1. Are uploaded files virus scanned? |  |
| 1. Is Path Traversal possible? |  |
| 1. Is command injection possible? |  |
| 1. Are redirects and forwards validated? |  |
| 1. Is Cross Site Request Forgery (CSRF) possible? |  |
| 1. Is Clickjacking possible? |  |

# SQL Injection

|  |  |
| --- | --- |
| Assessment Check | Assessment Result |
| 1. Is SQL injection possible? |  |
| 1. Use commands for the specific database software to try to elicit unauthorized database output. |  |
| 1. Does the App use a NoSQL database (e.g. MongoDB, CouchDB, Cassandra, Hbase)? |  |
| 1. Is NoSQL Injection possible? |  |

# Cross-Site Scripting (XSS)

|  |  |
| --- | --- |
| Assessment Check | Assessment Result |
| 1. Reflected XSS possible? |  |
| 1. Stored XSS possible? |  |
| 1. DOM XSS possible? |  |
| 1. Is use of JavaScript possible in the URL? |  |
| 1. Is injection possible into JavaScript event handler? |  |
| 1. Can XSS be used to capture a user token? |  |
| 1. Is input validation performed? |  |
| 1. Is output sanitization performed? |  |
| 1. Try best practices for exploiting XSS. |  |
| 1. Is Server-Side JavaScript Injection (SSJI) possible? |  |

# Database

|  |  |
| --- | --- |
| Assessment Check | Assessment Result |
| 1. How does the application interact with the database? |  |
| 1. Are dynamic SQL queries in use? Are stored procedures parameterized? Are prepared statements used? |  |
| 1. Request sample SQL statement. |  |
| 1. Does the App use a different database account for reading and updating data? |  |
| 1. Are logon credentials stored in the database in unencrypted form? |  |
| 1. Is Production data in the Test/Staging/Validation environment? |  |

# Infrastructure

|  |  |
| --- | --- |
| Assessment Check | Assessment Result |
| 1. Where is the application hosted? Internally? Service Provider? |  |
| 1. Are application tiers (presentation, application, and data layers) securely segregated from each other? |  |
| 1. Is the application deployed in accordance with the CMS Technical Reference Architecture? |  |
| 1. Can the exploitation of one tier adversely impact another tier? |  |
| 1. Is web server software up-to-date? |  |
| 1. Are unnecessary ports open? |  |

# Input Validation

|  |  |
| --- | --- |
| Assessment Check | Assessment Result |
| 1. Does the application accept incorrect data length, type, range, format in form field? |  |
| 1. Client checks duplicated on server side? |  |

# Audit

|  |  |
| --- | --- |
| Assessment Check | Assessment Result |
| 1. Is every event logged where sensitive data is accessed or a sensitive action is performed? |  |
| 1. Does App record login, logout, password change, password reset, invalid password, account suspension, account recovery, session termination/expiration, maximum user sessions in log files? |  |
| 1. Do logs contain username and IP address for transactions? |  |
| 1. Is a logging, monitoring, and alerting capability in place? |  |
| 1. How long are logs maintained? Are logs maintained for a sufficient period of time to correlate past events with new activity? |  |
| 1. Are logs migrated to a centralized audit capability where they can be analyzed and correlated? How often? |  |
| 1. How often are log files reviewed by staff? |  |

# Error Handling

|  |  |
| --- | --- |
| Assessment Check | Assessment Result |
| 1. Does the application produce verbose (e.g. application software name, version, etc.) messages when an error occurs? |  |