

Tested by Security Innovation Program



Server Application Criteria



Security Innovation, Inc
187 Ballardvale Street, Suite A170
Wilmington, MA 01887

1.978.694.1008

www.securityinnovation.com

Boston

Amsterdam

Seattle

Table of Contents

1.0 Executive Summary	3
2.0 Tested by Security Innovation – Server Application Criteria - Introduction	3
3.0 Tested by Security Innovation – Server Application Criteria – Authentication	4
4.0 Tested by Security Innovation – Server Application Criteria – Authorization.....	4
5.0 Tested by Security Innovation – Server Application Criteria – Cryptography.....	4
6.0 Tested by Security Innovation – Server Application Criteria – Data Access	4
7.0 Tested by Security Innovation – Server Application Criteria – Error Handling.....	5
8.0 Tested by Security Innovation – Server Application Criteria – Logging	5
9.0 Tested by Security Innovation – Server Application Criteria – Input and Data Validation ...	5
10.0 Tested by Security Innovation – Server Application Criteria – Sensitive Data	5
11.0 Tested by Security Innovation – Server Application Criteria – Session Management	6

1.0 Executive Summary

About Security Innovation

Security Innovation is the leading independent provider of risk analysis, risk mitigation and education services to mid-size and Fortune 500 companies. Global technology vendors and enterprise IT organizations such as IBM, Sony, Microsoft, ING, Symantec, Visa, SAP and GE rely on our expertise to understand the security risks in their software systems and facilitate the software and process change necessary to mitigate them.

The company has developed unparalleled expertise in the most dominant and demanding computing platforms & development environments. This practical experience gained through deep assessment of the world's most robust software applications combined with research on pressing security issues continues to position the company at the apex of the application security market.

About the "Tested by Security Innovation" Program

The "Tested by Security Innovation" Program helps software development companies establish a security baseline for their products and provide their customers with the confidence they need to deploy them. All applications are subject to a battery of tests that assess the integrity of critical security features and focus on key areas such as proper authentication, strong input/output validation, clear separation of roles, restricted data access, etc. Products awarded the "Tested by Security Innovation" logo withstood these rigorous tests conducted by the company's expert security engineers and meet the Program's security requirements for design, process and test coverage.

2.0 Tested by Security Innovation – Server Application Criteria - Introduction

The Tested by Security Innovation Server Application Criteria document describes test criteria that server applications have to meet in order to be issued the Tested by Security Innovation seal.

Unless noted otherwise, the candidate Server application must only meet the requirements that appear in this document.

Scope of Assessment

Our assessment focuses on the immediate application under test and its environment. Items out of scope for this assessment include, but are not limited to, the following:

- ▣ Backend systems
- ▣ Physical security of the <<Customer name>> site, servers, firewall configuration etc.
- ▣ Effectiveness of failover or redundant systems, power protection, etc.
- ▣ Protection from insider threats from employees or others with physical or electronic access
- ▣ Review of internal IT security policy
- ▣ Social engineering, industrial espionage, etc.
- ▣ Review of documentation or requirements for compliance with laws, standards or certification programs

3.0 Tested by Security Innovation – Server Application Criteria – Authentication

SUMMARY: Verify that the authentication mechanism is not subject to attacks aimed at bypassing it.

- A1. User cannot elevate privileges with malformed input
- A2. Passwords are stored in encrypted or hashed form.
- A3. User identity is verified before resetting/changing a password
- A4. Predefined passwords are unique and require reset
- A5. Only administrators can add, modify or delete user ID's
- A6. Lockouts are enforced with a limited duration
- A7. Strong passwords are enforced
- A8. Password renewal is enforced
- A9. Error pages do not give away usernames
- A10. SSL/TLS is used when transmitting credentials

4.0 Tested by Security Innovation – Server Application Criteria – Authorization

SUMMARY: Verify that the authorization mechanism is not subject to attacks aimed at bypassing it.

- U1. Server-side authorization checks are performed for each server resource that is accessed
- U2. Security decisions are not based on client-side validation

5.0 Tested by Security Innovation – Server Application Criteria – Cryptography

SUMMARY: Verify that cryptography is well implemented.

- C1. Industry standard cryptographic methods are used
- C2. Sufficient key length is used
- C3. Cryptographic keys are stored securely

6.0 Tested by Security Innovation – Server Application Criteria – Data Access

SUMMARY: Verify that strong data access controls are in place.

- D1. Database accounts conform to principle of least privilege
- D2. The application protects data from malicious modification
- D3. The application protects data from being disclosed to unauthorized users
- D4. Connection strings are stored securely
- D5. Database access credentials are stored securely
- D6. Only trusted hosts can access the database

7.0 Tested by Security Innovation – Server Application Criteria – Error Handling

SUMMARY: Verify error messages do not reveal confidential information

- E1. Error messages don't contain internal application details

8.0 Tested by Security Innovation – Server Application Criteria – Logging

SUMMARY: Verify that logging is performed and is not subject to attacks aimed at altering the logging functionality.

- L1. The application restrict users from interacting directly with the logging framework
- L2. The application must be protected against attacks aimed at deceiving the logging framework into attributing actions to other users.
- L3. The application must be protected against attacks aimed at modifying the behavior of the logging functionality via abnormal input.
- L4. Logging stores enough appropriate data to detect and deconstruct an attack against the system.
- L5. The application logs enough appropriate data to detect and deconstruct an attack against the system
- L6. Logs do not contain sensitive data
- L7. The logging framework is appropriately protected to prevent logs from being stolen or modified

9.0 Tested by Security Innovation – Server Application Criteria – Input and Data Validation

SUMMARY: Verify Input/Output is validated properly and securely

- I1. All user input is validated for type, length, format and range
- I2. All input is properly encoded before being echoed back to the user
- I3. User supplied filename and path input is filtered
- I4. Client side validation is not relied upon

10.0 Tested by Security Innovation – Server Application Criteria – Sensitive Data

SUMMARY: Verify sensitive data is stored and encrypted properly.

- S1. Sensitive data is encrypted before being stored on the local machine
- S2. Sensitive data is encrypted before being sent on the network
- S3. Sensitive data is encrypted in the database
- S4. Log files do not contain sensitive information

11.0 Tested by Security Innovation – Server Application Criteria – Session Management

SUMMARY: Verify tokens are formatted and sent securely.

- M1. Authentication tokens are transmitted over a secure connection
- M2. Authentication tokens are not predictable