White Paper

Security

Solutions Business Manager 11.5 Web Application Security Assessment

MICRO FOCUS

Table of Contents

page

Micro Focus applies a multi-layered approach for security within SBM, incorporating best practices for preventing security breaches, as well as ensuring data integrity and confidentiality.

Micro Focus Takes Security Seriously

Internet applications are always vulnerable to attacks by various malicious users, abusive bots, and crawlers that can exploit weaknesses in the data security model to gain unauthorized access to important data. Micro Focus® Solutions Business Manager (SBM) is scanned for Web application security as part of the certification process upon each release, and it is thoroughly tested to validate the security of the enterprise data that is stored in the database.

Micro Focus understands that any vulnerability that is detected during these tests can be exploited to gain access to sensitive enterprise data and ultimately lead to financial loss. Our development and quality assurance organizations endeavor to expose and resolve these types of potential vulnerabilities during each testing cycle. Micro Focus takes security seriously. We strive to aggressively enhance SBM to safeguard against any new vulnerabilities that are discovered.

Who Should Read This Paper?

This paper is intended for system administrators or others who are interested in understanding existing security safeguards within SBM and reviewing the latest security Web application scan results.

Solutions Business Manager Security Safeguards

Micro Focus applies a multi-layered approach for security within SBM, incorporating best practices for preventing security breaches, as well as ensuring data integrity and confidentiality.

Server and Database Configuration

SBM Configurator provides an easy mechanism to deploy the various SBM database and application components across multiple servers. This serves to minimize the "attack surface." For example, data updated by users can be stored on one server, data used to build and describe process apps and other design artifacts stored on another, and then configuration and administrative data stored on yet another machine. Administrators can then appropriately restrict access to those servers, making it much harder for an adversary to exploit the system simply by hacking into any one server or physical machine.

Data in Transit Encryption

Data is most vulnerable to unauthorized access as it travels across the Internet or within networks. Therefore, SBM Configurator provides the mechanism to configure applicable servers to use secure HTTP (HTTPS) and Secure Socket Layer (SSL) to encrypt, authenticate, and ensure data integrity. This can be for interactions with end users, inter-component communication, communication with third-party systems, and infrastructure such as LDAP servers and relational databases.

Data at Rest Encryption

The data residing on storage systems and media presents serious security concerns with regards to corporate data protection and privacy of data. SBM has two facets to data at rest—data stored in a relational database and data stored on the file system.

For data in the relational database, there are two factors to securing it. The first factor is restricting access to the data via permissions for the databases used by SBM. This is governed either by the DBMS user accounts or the Windows domain accounts that have been granted access to the databases. The second factor is that the data in the databases can be encrypted by the DBMS for an added layer of security.

Data stored on the file system, such as configuration and connection information, must also be secured. SBM encrypts credentials used to connect to its various databases using a triple-DES encryption algorithm with 184-bit keys. Also, information used to connect to identity providers for the purpose of Single Sign-On (SSO) can be considered sensitive, so SBM provides the option to encrypt this information. SSO uses 256-bit keys with either Blowfish, AES, or 3DES.

Authentication and Session Management

No matter what access method (Web browser, mobile apps, or desktop applications), all user access goes through an authentication process. SBM Configurator provides several options for identity providers, such as internal user database, Windows domain, LDAP, or other third-party providers. Session management in SBM can be configured to use HTTP cookies, NTLM, or security tokens via SSO. SBM also allows for more complex scenarios when using SSO, including validation against multiple identity providers and two-factor authentication via smart cards.

In addition, SBM provides controls for managing the idle timeout of session token lifetimes for security tokens.

Authorization (Access Control)

SBM Application Administrator provides administrators with the ability to set user permissions at role, group, and individual levels, giving administrators the ability to follow the principal of least privilege—allowing users to have the least possible authority necessary to do their job.

Additionally, SBM provides for two-way SSL connections to restrict access to non-end user interfaces.

Web Application Security

SBM provides integrated proprietary and third-party firewalling and sanitizing capabilities for various types of attacks:

- XML/HTML content attacks (cross-site scripting attacks [XSS], JavaScript injections, SQL injection, and well-formedness)
- Cryptographic attacks (denial of service and replay attacks)

- SBM has two facets to data at rest—data stored in a relational database and data stored on the file system.
- No matter what the access method, all user access goes through an authentication process.
- SBM provides integrated proprietary and thirdparty firewalling and sanitizing capabilities for various types of attacks.

- The Burp Web Vulnerability Scanner is highly regarded in the industry and uses feedback-driven scan logic rather than a static list of possible vulnerabilities.
- Micro Focus evaluated the results of the scans, looking for requests with potential vulnerabilities.

- SOAP attacks (SOAP operation filtering and rogue SOAP attachments)
- Communication attacks (HTTP header and query string analysis)
- Authentication attacks (cross-site request forgery attacks [CSRF])

SBM provides customization of this sanitization via SBM Application Administrator.

SBM can use IIS to proxy all server requests, which enables tighter monitoring capabilities. This forces all SBM traffic through IIS on port 443 and disables all Tomcat HTTP connectors. For details, refer to the *SBM Installation and Configuration Guide* or SBM Configurator help.

In addition to content sanitization and monitoring, SBM provides a Web application firewall. This can be used for monitoring purposes or can be set to actively block requests based on defined security rules. These security rules are customizable and allow administrators to tailor security configuration to suit their particular content needs or heightened security requirements. In the event a security vulnerability is found, this also allows for virtual patching of the systems in the field.

Web Application Security Test Results for SBM

Testing was performed using Burp Suite Professional v.1.7.33. The Burp Web Vulnerability Scanner, a tool within this suite, was specifically used to actively scan requests from a client. This tool is highly regarded in the industry and uses feedback-driven scan logic rather than a static list of possible vulnerabilities.

Test Setup

Burp Suite was run on a dedicated machine that acts as a proxy server monitoring requests made through the Web browser. For the purpose of these tests, Burp Suite monitored requests on a remote, self-contained installation of SBM with SBM Internal authentication and SSO session management. Burp Suite recorded requests made through the browser, noting passively detected vulnerabilities at the same time. Burp Suite was then used to actively scan all recorded requests with parameters, sending numerous (hundreds or thousands) of requests formatted after each scanned request but with parameter alterations that attempt to expose vulnerabilities.

SBM was configured to use HTTPS for requests and SSO was enabled. To handle customization variability, a custom Web application firewall ruleset was also put in place.

Scanning tested for the following types of attacks:

- SQL Injection
- OS command injection
- Server-side code and template injection

- Reflected and stored cross site scripting
- File path traversal/manipulation
- External/out-of-band interaction
- HTTP header injection
- XML/SOAP injection
- LDAP injection
- Cross-site request forgery
- Open redirection
- Header manipulation
- Server-level issues

Micro Focus evaluated the results of these scans, looking for requests with potential vulnerabilities.

Use Cases

Scanning was done against what can be considered typical usage of SBM. This includes:

- Logging into SBM
- Viewing item data
- Viewing reports
- Viewing backlogs
- Viewing activities
- Viewing Kanban
- Viewing external feeds for Kanban

Special attention was focused on operations that store or modify data in the system, including:

- Submitting an item
- Transitioning an item
- Creating and modifying a report
- Creating backlogs
- Creating activities
- Work Center search
- User Workspace search
- Updating user profile information
- Creating Kanban
- Creating users in SBM Application Administrator
- Requesting for query at runtime

- Scanning was done against what can be considered typical usage of SBM.
- Special attention was focused on operations that store or modify data in the system.

The results of the security scans were evaluated. No serious vulnerabilities were found.

- Reporting for query at runtime
- Attaching a file/URL to a field
- Viewing a file/URL in a field
- Adding and viewing quick links and favorites
- Adding and viewing folders

Findings

The results of the security scans were evaluated. No serious vulnerabilities were found. Results that were flagged as potential low severity issues that should be evaluated were inspected manually and determined not to be a problem as detailed below.

Security Issue	Area(s) Tested	Result
Cacheable HTTPS response	■ Submit, view, transition item ■ User profile modification ■ Work Center ■ Kanban execution ■ Backlog ■ Request for query at runtime ■ Application Administrator	Passed
Content types incorrectly stated	■ Work Center	Passed
Content type is not specified	■ Submit, view, transition item ■ User profile modification ■ Work Center ■ Kanban creation ■ Kanban execution ■ Backlog	Passed
Cross-domain Referer leakage	■ User Workspace	Passed
Cross Site Request Forgery (CSRF)	■ User profile modification ■ Attach a file/URL to a field	Passed
CSRF	■ User Workspace	Passed. No data is changed.
CSRF	■ Submit, view, transition item	Passed. Session ID prevents CSRF attack.
DOM-based XSS	■ Work Center ■ User Workspace	Passed
DOM data manipulation (DOM-based)	■ Submit, view, transition item ■ User Workspace	Passed
Feed field values in JSON call	■ Report creation and execution ■ Kanban creation	Passed. Response does not get interpreted as HTML.
File path manipulation	■ User profile modification	Passed
Form action hijacking	■ Work Center	Passed
HTTP Parameter Pollution (HPP)	■ Report creation and execution	Passed. No data is changed.
HTTP response header injection	■ Work Center ■ User Workspace	Passed
LDAP injection	■ Work Center	Passed
Link manipulation	■ Work Center ■ User Workspace	Passed
Multiple content types specified	■ Work Center ■ User Workspace	Passed

Continued on next page

Security Issue	Area(s) Tested	Result
Open redirection	■ Work Center ■ User Workspace	Passed
Parameter injection (URL)	■ Submit, view, transition item	Passed. Response does not get interpreted as HTML.
Parameter injection (body)	■ Submit, view, transition item	Passed. Response does not get interpreted as HTML.
Path-relative style sheet import	■ Submit, view, transition item ■ Report creation and execution ■ User profile modification ■ Work Center	Passed. Returns 404 error on modified paths.
Suspicious input transformation	■ Report creation and execution	Passed
User agent-dependent response	■ Submit, view, transition item	Passed
X-Forwarded-For dependent response	■ Submit, view, transition item ■ Report for query at runtime	Passed
XSS stored	■ User profile modification ■ View a file/URL in a field	Passed
XSS stored/reflected	■ Work Center ■ User Workspace ■ Application Administrator ■ Adding and viewing folders	Passed

OWASP Top Ten Results

ID	Area Tested	Result	Additional Information
A1	Injection	No issues found	SBM actively monitors for different injection attacks and follows design patterns used to prevent them.
A2	Broken Authentication and Session Management	No issues found	SBM uses industry best practices for session management, authentication, and password management.
A3	Cross Site Scripting (XSS)	No issues found	SBM actively monitors for XSS attacks and provides fine-grained configuration for allowed content.
A4	Broken Access Control	No issues found	All access of objects inside of SBM go through a centralized access control to verify the user's permission. All data requests are validated at the client and server levels to ensure proper permissions to data.
A5	Security Misconfiguration	No issues found	SBM provides a configuration application to ease the configuration of security settings and provides guidance on how to secure the configuration properly.
A6	Sensitive Data Exposure	No issues found	Sensitive data stored by SBM is stored securely at rest and, if configured to do so, in transit to the server.
A7	Insufficient Attack Protection	No issues found	SBM prevents attacks across the entire spectrum. If an attack is attempted, SBM logs the attempt, which enables an administrator to review the logs and identify the attack. Brute force attacks, such as attempting to guess a user's password, can be prevented by SBM's authentication setting that disables a user account after a certain number of failed login attempts. Patches that prevent future security vulnerabilities are also developed for SBM as they are discovered.
A8	Cross Site Request Forgery (CSRF)	No issues found	SBM has active monitoring and mitigation for CSRF attacks.
A9	Using Components with Known Vulnerabilities	No issues found	As part of the release process, third-party components are checked against vulnerability lists and updated accordingly.
A10	Underprotected APIs	No issues found	SBM provides secure APIs that require strong authentication. Private session and login data is not exposed in these APIs, and SBM provides access only to the authenticated user's data and not any other data on the system. API parameters are scrubbed and hardened against attacks.