



INFORMATION SECURITY ASSESSMENT

Prepared for

EnterpriseWizard



Prepared by

Security Management Partners

391 Totten Pond Road
Suite 101
Waltham, MA 02451

- Report -

Date Issued: May, 2009

Confidentiality Statement

The following report contains confidential information. Do not distribute, email, fax, or transfer via any electronic mechanism unless it has been approved by your organization's security policy. All copies and backups of this document should be maintained on protected storage at all times. Do not share any of the information contained within this report with anyone else unless you confirm they are authorized to view the information.

Table of Contents

I. PREFACE	4
II. EXECUTIVE SUMMARY	5
Risk Factor Definitions	6
Discovered Vulnerabilities	6
III. APPROACH	7
IV. TESTING RESULTS AND FINDINGS	8
Web Server Findings	8
V. APPLICATION TESTING	9
EnterpriseWizard KnowledgeBase	9

I. PREFACE

The use of information technologies to enable business processes naturally creates a level of technical risk. Management of such risk is accomplished by identification of critical and sensitive processes and systems, assessment of the risk associated with each, remediation of identified risk, and periodic re-evaluation of the environment.

The risk assessment findings described in this document are the result of in-depth system evaluations and interviews with key personnel conducted by Security Management Partners during April and May, 2009.

Risk assessment represents Security Management Partners professional opinions of the threats, vulnerabilities, loss impact, and likelihood of occurrence for the respective technology process and system areas described in this document.

Security Management Partners provides information security consulting to assist organizations in meeting and exceeding industry best practices. For the past 10 years SMP has performed engagements for hundreds of private, public and government firms. SMP services range from operational and network assessments that provide independent auditing of processes and systems to incident response and digital forensics. Through consulting services, SMP provides knowledgeable solutions that address the needs of the organization while maintaining a strong adherence to security best practices.

All Security Management Partners consultants contributing to this assessment maintain industry certifications such as CISSP and CISA and have a minimum of 6 years experience in the information security field. SMP consultants testing methodology follows industry standards from organizations such as US-CERT, NIST as well as other industry accepted Information security organizations like the Open Web Application Security Project (OWASP).

Observations recorded in this document represent observations that were valid in the assessment period, and should be periodically re-evaluated to reflect changing business and technical conditions.

Questions regarding this document should be directed to:

*Peter Bamber, CISA, CISSP
VP Consulting
T: 781-890-7671 ext. 219
pbamber@smpone.com*

II. EXECUTIVE SUMMARY

EnterpriseWizard has engaged Security Management Partners to assess the security of its external network and web based application. Testing consisted of external scanning and vulnerability testing for the standard web and secure web ports and manual penetration testing against the application. SMP performed tests from the perspective of multiple users as well as unauthenticated access.

Security is an ongoing process. As EnterpriseWizard's network undergoes periodic changes such as the addition of new services or upgraded infrastructure, security must be repeatedly tested. Even the absence of change can affect the security of EnterpriseWizard's network. Hackers are continuously discovering new vulnerabilities in applications and protocols. Without the application of patches or upgrades to software, it is possible that a vulnerability addressed in one of the patches has available exploit code, which could endanger the security of the system and eventually the entire network. Furthermore, "open doors" on the network can enable hackers to breach EnterpriseWizard's perimeter and access valuable intellectual capital. Continuous and repeated assessments are the best defense to ensure sustained protection and a secure network.

SMP followed a multilevel approach to gather information in order to provide a comprehensive, business focused, network security assessment to determine the ease or difficulty of gaining access to EnterpriseWizard's critical data. The assessment included testing using automated scanning tools and manual probing by our security specialists. Because we do not believe that off-the-shelf network auditing products provide a complete analysis, our assessment methods include the use of Hacker techniques. SMP's testing methodology gives a complete and realistic assessment of EnterpriseWizard's current security posture against the most likely attacks.

Observations recorded in this document represent observations that were valid in the testing time period and should be periodically re-evaluated to reflect changing business and technological conditions. SMP's risk ratings indicate our assessment of the risks relative to other financial organizations, and to industry best practices. These ratings do not imply any judgment or opinion of the appropriateness of the risk to EnterpriseWizard. It is the responsibility of EnterpriseWizard to determine what level of risk it is willing to accept.

Risk Factor Definitions

In the report, each identified vulnerability is assigned a level of severity or “risk factor” ranging from high to informational. An explanation of these designations is as follows:

High Risk – Immediate Threat. All security threats that can compromise the integrity of your data are classified as high risk. These types of threats should probably be addressed first and are typically easy to exploit.

Medium Risk – Minimal Threat. Security threats that can open your system(s) to unauthorized access or expose your data, be used to take your system(s) off-line, or can be used for denial of service (DoS) attacks are considered medium risk. These may be more complex to exploit, but they are important to address.

Low Risk – Potential Threat. This classification of threats is used for problems that typically cannot be used independently to gain unauthorized access to your data or compromise your system(s). However, these threats are commonly combined with other information to exploit your network and should also be addressed.

Informational/Best Practice – Security related information, such as best practices, service banners and port information. Usually no action is necessary to prevent a vulnerability; however, best practices suggest strong preventative measures that develop a proactive approach to security often resulting in a strong defense in depth, which can mitigate other potential vulnerabilities.

Discovered Vulnerabilities

Web Server

The following external IP address was scanned and penetration tested from April 3rd to May 21st 2009:

- 72.20.102.61

There were no **HIGH**, **MEDIUM** or **LOW** risk vulnerabilities found on the web server.

KnowledgeBase Application

There were no **HIGH**, **MEDIUM** or **LOW** risk vulnerabilities found within the KnowledgeBase application.

III. APPROACH

Security as an Ongoing Process

For complete security, organizations need to invest in a robust, operational security architecture, which must be properly installed, monitored, and maintained. This often requires knowledge transfer to keep staff competency at a high level. Other organizations successfully outsource these maintenance functions. Assessments should be conducted on a periodic basis to assess information security defenses under “live” conditions. A Security Policy is essential because it binds all of these maintenance procedures together and provides the procedures to follow and standards upon which to base results. The process is cyclical and begins with a solid methodology. SMP developed a four-point methodology, the “Security Evolution Lifecycle” to assist clients in maintaining optimal security of their network infrastructure.

The components of this methodology are:

1. **Evaluate** – SMP assesses the current security posture while remaining sensitive to a client’s business needs and practices. It is important to perform both a theoretical and practical analysis, in order to develop a comprehensive assessment, which includes all possible risk factors. An SMP Security Assessment takes a comprehensive security snapshot of any threats, risks, and vulnerabilities and then goes one step further to inform the client on how to best solve the potential risks to their network.
2. **Strategize** – SMP uses the results of the “Evaluate” phase to develop a detailed report explaining the potential impact of each identified risk and providing specific recommendations for remediation. This takes into account everything from a company’s business practices, data transfer needs, customer information exchanges and includes confidentiality, integrity, and availability requirements.
3. **Secure** – With SMP’s roadmap in hand, steps can be taken to secure the organization. The program must be dynamic to address the ever-changing landscape of information security. SMP clients leverage our team of security experts who remain current on all security issues.
4. **Monitor** – Change management is an important part of network security which is why SMP conducts repeated assessments to evaluate the impact of these changes. Whether seen as benign or complex, recurring services make certain there are no “open doors” on the network to invite hackers. Repeatedly testing the level of security is the best way to ensure that your security program is protecting your information assets.



Security Threats to EnterpriseWizard’s Data

There are three primary aspects to network security:

- ◆ **Integrity**—Data on company servers must be safe from tampering. If tampering occurs, it may be feasible for EnterpriseWizard to have systems in place to detect and warn about this before any critical exposure. SMP will review the needs and report its findings.
- ◆ **Availability**—Availability of the system is simply keeping services up and available to users. Sometimes it is easier for a hacker to simply take down a service being provided using traffic flooding or other means. This can often be simpler and quicker than breaking into a system.
- ◆ **Confidentiality**—Access must be restricted such that outsiders cannot view private data on EnterpriseWizard’s servers. There must be a balance between accessibility of information and security of confidential data.

IV. TESTING RESULTS AND FINDINGS

The findings of the report contain summaries of the different pieces of the technical assessment performed for EnterpriseWizard. Security Management Partners makes recommendations within the findings section of the report that present steps which are important to preserve or enhance general security measures. If there are more detailed recommendations they can be found in other areas of the report with further explanation.

Web Server

Host	Port	Vulnerability	Severity	Recommended Fix
72.20.102.61	NA	Utilizing DNS the host is identified as: sa11.enterprisewizard.com.	INFO	Information Only.
72.20.102.61	22 TCP	The address offers an SSH service for remote management. This service allows encrypted remote access to the address. The banner displays: SSH version : SSH-2.0-OpenSSH_5.1	INFO	Information Only.
72.20.102.61	443 TCP	The address offers an HTTPS service for secure web pages. The banner of the service displays: Server: Apache-Coyote/1.1 X-Powered-By: Servlet 2.4; JBoss-4.2.2.GA (build: SVNTag=JBoss_4_2_2_GA	INFO	Information Only.
72.20.102.61	443 TCP	The secure web service accepts connections with only the TLSv1 and SSLv3 protocols.	INFO	Information Only.

Web Server Findings

Security Management Partners conducted an external port and vulnerability scan of the standard web ports and remote command line management ports for the address provided in the Executive Summary. Any ports that returned as open during the port scan were then tested for vulnerabilities. Two (2) ports were identified, including a service for Secure Shell (SSH) and a service for HTTPS secure web pages on port 443 TCP. No vulnerabilities were identified in these services that would allow unauthorized access to content or the internal network.

The Secure Shell (SSH) protocol allows for remote command line management of operating systems. This service is preferred to telnet because of the inclusion of stronger security measures to ensure that the user is connected to the intended host and that the communication between user and host is securely encrypted.

The HTTPS service is identified as an Apache Coyote web service that utilizes JBoss for additional functionality. No issues were identified in the versions of the server software utilized to host the secure web service. During the testing SMP attempted to identify the presence of directories through enumeration techniques. Directory searching techniques

returned a '403 Forbidden' page. Although there is no information leak through the default error page, it is possible to design custom error pages that redirect users to desired areas or displays a static message rather than the default error page.

Testing of the encryption capabilities of the secure web service of port 443 TCP identified that the available Secure Sockets Layer (SSL) protocols and encryption ciphers make it hard for an attacker to intercept communication and negotiate a weak encryption that would lessen the security of the communication. By default web browsers negotiate from the strongest encryption possibilities to the weakest. For EnterpriseWizard, the weakest settings do not allow the use of the older SSL version 2 protocol, which has security weaknesses in the protocol and is considered obsolete. SMP noted that all ciphers used for the encryption of communication represent strong encryption

SMP also identified that the SSL certificate utilized by EnterpriseWizard has newly been replaced to ensure the strongest hashing is utilized to prevent the possibility of collisions with other certificates. With collisions it is possible that a malicious user could generate a spoofed certificate to direct users away from the legitimate site; however, EnterpriseWizard has actively updated their certificate to prevent this attack.

V. APPLICATION TESTING

Security Management Partners performs manual probing of applications to determine the effectiveness of controls. If a user can circumvent the controls in place and access or modify information, the controls in place may not be accomplishing their purpose. SMP utilizes testing methodologies that are intended to test the limits of applications and identify areas that the application can be forced to act in a manner that is not intended.

As part of the assessment, Security Management Partners was tasked with testing the website for the KnowledgeBase application through the portal, <https://sa11.enterprisewizard.com/gui2/>. All findings are discussed below.

At the time of testing the KnowledgeBase application, it was found to be secure in the following areas:

- **Secure Sockets Layer (SSL) Secure Sessions**
- **Cross Site Scripting (XSS) attacks**
- **Dynamic Interface & Permissions**

EnterpriseWizard KnowledgeBase

Security Management Partners performed testing of the provided demo KnowledgeBase server using unauthenticated assess as well as account information supplied by EnterpriseWizard. All attempts to bypass the authentication functionality were unsuccessful. Utilizing credentials reveals that the site is heavily protected through the use of cookies and session requirements. With access as a valid user, SMP was able to explore the interface of the application; however, all testing performed indicated that EnterpriseWizard has strong security measures in place to ensure appropriate use of the application.

SMP performed testing in the areas of session hijacking, privilege escalation and Cross Site Scripting (XSS). All of the attempted inappropriate field input by SMP was properly handled by the server. All attempts to access content that is

not intended for a user based upon their group and roles assigned were not permitted. All attempts to create multiple user sessions were unsuccessful and user logons from multiple sources resulted in expiration of user sessions.

SMP identified that session and cookies are controlled such that users cannot have multiple simultaneous logon sessions and as new sessions are started the previous sessions are expired immediately. The use of cookies represents a strong protection to the user session to ensure the validity of the session and prevent capturing or sharing of the session ID and utilizing it from a different location.

A drawback from using cookies is that user behavior and browser configurations, beyond the control of EnterpriseWizard, could cause interference with the user's experience in visiting the web application. Users that have browser settings that deny cookies will not be able to visit the page. Additionally, EnterpriseWizard cannot control user access to other Internet sites that could be harmful and gain access to or manipulate the cookie file on the user's machine through Cross Site Scripting (XSS) attacks. By setting expiration timers for cookies and renegotiating cookie content, it is possible to minimize the length of time that a cookie is stored at the client host.

During the testing, SMP attempted to perform Cross Site Scripting (XSS) attacks that would direct valid user sessions away from the site and also attempted to test the permissions encapsulating the demo site from other sites and the permissions restricting users to only content to which they are intended to have access.

With the large amount of user generated content within the application, it is possible for accidental or malicious input of improper data into the system. Whenever possible it is recommended to restrict user input to dropdown lists or checkboxes that supply accepted data input. For the areas that allow user generated content, such as comment boxes on many pages throughout the site, SMP attempted to create JavaScript code that would be executed by a browser when viewed outside of the edit screen. All attempts to have code executed were unsuccessful and the page displayed the input provided by SMP in a literal fashion. This represents that the server is properly not evaluating any of the content supplied by users.

Additionally, SMP identified the use of search and filtering functions within the application. Within these functions it is often possible to alter the information returned by attempting to provide additional SQL syntax to the search function. This methodology is known as SQL injection and can often return information from unauthorized areas of the backend database if successful. SMP's attempts to perform the SQL injection attacks against these functions were unsuccessful.

Also, because of the dynamic nature of the site, users of different privilege levels view the site differently. Navigation pages are restricted from showing content that is not intended to users based upon group and roles defined within the application by administrative users. SMP attempted to bypass these restrictions by requesting pages manually rather than following links in the navigation menu. SMP utilized the knowledge of pages from a higher privilege account and the request history from that account to generate requests for the unprivileged user. Additionally, SMP attempted to manipulate requests by altering the variables communicated with the page requests to values that were provided for the privileged user when connected as the unprivileged user. Each of these requests did not return successful page access and the majority of requests resulted in expiration of the user session. Upon changing select variables, SMP was presented with a customized error page that allows submission of an error report.

During the assessment SMP gained no information was obtained that would assist in extending beyond the intended environment of the demo system provided for SMP. Also within the application, SMP was unable to impact the environment to alter the permissions of users from unprivileged accounts. Attempts to access information by a user that does not have permission to access the information were unsuccessful and resulted in expiration of the user's current session.

SMP did identify that import functionality within the application does not validate the user supplied input before accepting and creating content. SMP was able to upload an executable file to the server and generate items within the

application based upon the textual interpretation of the code provided to the server. More than 5,000 items were created by the file uploaded and SMP identified that a user could upload a file and navigate away from the page while the server continued to process the file. This suggests that a user could attempt a denial of service attack against the server by repeatedly and consecutively uploading large files. In order to ensure valid input is provided to the application, enforce stronger checks on data inserted so that only human readable characters are imported.

SMP noted that the application has logging of user activity, which is recommended for tracking inappropriate alteration of items within the application. The application logging does not identify all page requests and attempted access that is available at the web server log level; however, it is a strong step towards ensuring data integrity within the application. With proper backup of user data, it is possible to undo malicious changes to the environment and recover from data loss.

SMP also noted that when editing a user's information, that it is possible to mark users as active and inactive. This field can be used to create rules that would automatically remove user access once they are marked as inactive, but does not remove user access. Informational language has been added to clarify the purpose of the field for administrators.

EnterpriseWizard KnowledgeBase Recommendations

- **(Rating INFO / BEST PRACTICE)** Provide checks on the user data files before importing to ensure that valid content is created as a result of a successful import.
- **(Rating INFO / BEST PRACTICE)** Assist application owners with understanding the full functionality available through the KnowledgeBase to ensure proper use and monitoring of the environment.