



Web Application Assessment

Securing multi-tier dynamic web sites

Case Study

FishNet Security Corporate Headquarters
1710 Walnut Street / Kansas City, MO 64108
tel: (816) 421.6611 fax: (816) 421.6677
fishnetsecurity.com

Summary

When a global transportation company developed and improved their primary online point of sale (POS) web application suite, they had high expectations of functionality. The online users utilize the web application suite to manage full process flow; from transaction research to schedule completion. The application suite encompassed systems throughout the enterprise, including: databases, front-ends, directories, and legacy transaction systems. A large scale internal development effort was made to successfully provide the functionality needed to meet the organization's expectations. The client sought to bring security and confidence to the rollout of a major upgrade of the enterprise's web application suite.

Just a few weeks before production rollout, the Information Security department requested a third party assessment team to validate the web application suite against compromise. FishNet Security (FNS) was sought out as the provider for this vital assessment. Through a six week engagement, FNS discovered critical web application and web site security issues and collaborated in the mitigation of these issues, securing the web site and infrastructure from potential business threats and losses. The application security services provided by FNS enabled the client to move the application into production in a proactive, confident and secure manner while meeting aggressive rollout time lines.

Business Impact

Large public companies are measured for success by profitability, value, and market share. A company that suffers a web related security incident, quickly experiences a loss of customer retention, trust, profit, market share and value.

Business customers expect service providers to offer extensive online capabilities. The competitive nature of business demands that companies provide multifunctional web sites and applications for their customers to use and perform tasks ubiquitously. As with any business transaction, customer data is captured. With an on-line transaction this private and vital customer data is pipe lined through multi-functional dynamic web applications and sites. This customer data is usually personally identifiable information (PID) that should be protected from public, non-compliant and illegal access. When personally identifiable information is compromised, the responsible organization must rebuild customer confidence as well as potentially endure millions of dollars in liability.

The recent popularity of identity theft has made protecting PID information more important than ever. In California, (in accordance with statute SB 1386), any compromise that leads to the exposure of customer data must be publicly disclosed. Application threats that lead to compromise quickly impact a company's reputation and market performance while costing millions in lost revenue and expense.

The Environment

The dynamic, multi-tiered, database driven web application infrastructure assessed was complex and technologically advanced. As the complexity of the application infrastructure increases, so will the attack vectors. To properly assess the complex web application, a thorough understanding of the business purpose, technical environment, and the mind set of the attacker(s) had to be reached. Most companies lack the experience needed to properly test web applications. Even when internal staff armed with adequate skill sets are available, audit best practices recommend a qualified independent party perform the assessment to avoid conflict of interests.

The web based application suite used an extensive amount of dynamic Java based content. This content was comprised primarily of IBM technologies. Websphere was utilized as the web server front tier and the mid-tier Java application servers. DB2 on RedHat Enterprise servers provided the content and session data. IBM LDAP and legacy message queuing systems handled credential tracking and the links to all POS locations.

The Assessment

FishNet Security provided a variety of application security services as a part of this engagement including:

- Fault Injection/Black Box Testing
- Unauthenticated/Authenticated User Testing
- Application Architecture and Design Review
- Host Level Web Server Reviews
- Database Security Testing

The initial phase of the application assessment began with a “black box”, zero knowledge testing approach. In this portion of testing the transportation company’s web application proved to be vulnerable. Specifically, cross site scripting (XSS) attacks and weaknesses in cookie management were identified. These combined issues would subject the application to attacks that could result in customer login credential disclosure and possible identity theft. Therefore, an attacker with customer login credentials or an active customer session could obtain sensitive and privileged customer data.

The authenticated user testing phase started by requesting credentials from the company. The credentials are used to simulate attacks from the perspective of an authorized (or unauthorized with stolen credentials) user on the system. Most online applications that require a set of credentials display only public information and a login page to an unauthenticated visitor. Once credentials are presented by the user, a vast number of functions are permitted. Live credentials enabled FNS consultants the leverage to test all the business logic in the online application and search for vulnerabilities. The web application specific tests included: SQL injection, XSS, session tracking, and common methods of attack as dictated through web application community research.

FNS found that the combination of vulnerabilities exposed during unauthenticated testing and those from the authenticated phase could lead to complete compromise of the site. In depth analysis of the combined results, revealed new attack vectors and risks to the web application.

The database security testing phase takes the perspective of an attacker that has compromised a front-end machine with application level access to the back end components. Most web applications access the back end database with a static set of user credentials. The front-end and application code accesses a database system with defined credentials that have rights to the systems. A compromised front-end will give the attacker access to the back-end with these credentials. The web application being assessed used this exact configuration. The Websphere systems accessed the back-end DB2 databases with a set of defined credentials. FishNet Security obtained access to the back end systems with these credentials to determine the amount of access afforded to an attacker using the same account.

It quickly became clear that far too much access was given to the account. Shell access to the database servers was available. This lack of control allowed FNS to determine that the database installation needed to apply best practice. Permissions were still in place, which allowed the perusal of the database without any default authentication. With the use of free DB2 utilities, anyone could browse, and in some cases, manipulate the tables on the system.

Identifying these critical application and database related vulnerabilities proved to be invaluable to the client. Without this insight, the organization would not have understood the risk and exposure. If the client would have put the web application into production without proper testing and analysis, extensive costs and liabilities may have ensued. FishNet Security not only uncovered root cause issues, but worked in tandem with the organization's staff, developers, and application infrastructure team in developing mitigation techniques and strategies to prevent and manage the potential for future vulnerabilities. The FNS consultation team utilized mature and proven methodologies, providing immediate ROI to the client. Due to FNS' extensive real world experience and in-depth knowledge of the assessed technologies, the client was able to see a "true risk" to their business model. By meeting with business executives and relating the technical risks in a business context, FNS played a key role in establishing an appropriate risk rating and prioritizing the issues found during the engagement.

The Report

FishNet Security provided the client two main reports:

- Application and Database Technical Vulnerability Matrix
- Formal Comprehensive Report including: Executive Summary, Findings and Recommendations (F&R), and Assessment Testing Detail Summary

The transportation company's executive body appreciated the high level reporting of the issues directly impacting the business and the associated risks that were found. The F&R section that was provided to the client outlined each high-level risk observation, the recommended action items, client response, and an accountability/ownership model delegated to each risk item. The client's IT and Security management teams are now using the F&R section to assign and track tasks in order to mitigate discovered risk items. Technical staff are using the detailed vulnerability descriptions to find the exact methods for mitigation.

Conclusion

The enterprise web application security assessment conducted by FNS drastically reduced the exposure to sensitive customer information. FNS enabled the client to gain insight to weaknesses within the application that an unauthorized and authorized user/attacker could exploit.

At the completion of the assessment, all levels of the organization better understood the risks presented in exposing a web application to internet vulnerabilities and where they stood in regards to their current application posture. A new awareness of application threats and risk to the business execution was generated by the high-level findings. In addition, knowledge transfer of application vulnerabilities and mitigation strategies to the existing technical staff was equally accomplished.

The global transportation company successfully moved their new web application into production with confidence while securely enabling their online business practices.

The FishNet Security Advantage

FishNet Security is an information security solutions provider. Based on extensive experience, research, effort, and focus, FishNet Security has been providing complete solutions to enterprises, small and medium business, as well as state, federal and local governments for over nine years. Through a careful evaluation process, FishNet Security also partners with a wide-ranging, but selective group of security product providers. With this strategic focus on security, strong relationships with leading technology providers and a commitment to our customers, FishNet Security is uniquely qualified and dedicated to meeting the information security challenges of our customers.

For more information, please visit www.fishnetsecurity.com