Federated Networks Protected WebGoat Application Vulnerability Assessment

Introduction

BT performed a vulnerability assessment of the FN Connect Secure **Web Application Gateway** (protecting the Webgoat Web application). The overall purpose of this assessment was to identify web application level security issues including the Open Web Application Security Project (OWASP) 'TOP 10 FOR 2010" risks associated with the use of web application, more specifically as related to FN Connect Secure Web Application Gateway's ability to mitigate known threats inherent in an OWASP software security training website, Webgoat, which is a deliberately insecure J2EE web application designed to teach web application security lessons.

BT has extensive experience helping clients secure their application and network infrastructures and evaluate the effectiveness of protections to the loss of intellectual property. Our Security Consultants have helped many of the world's largest institutions protect their Web-based service delivery systems and we have assisted clients that offer electronic commerce solutions. BT's Global Ethical Hacking Center of Excellence (EHCOE) is one of the largest security practices in the world, The team consists of a security community of 1800+ full time client facing consultants / architects / designers, including R&D/V. These industry leading resources that have produced over 20,000 engagements, 100 registered patents, 190 security papers, 108 registered patents. BT is recognized in the industry as "highest capability maturity" by the NSA and "Of the top Three" from Gartner. BT' engagements do not simply perform "scans" of a client's network. We perform highly detailed tests with our proven process and methodologies based from over 20,000 engagements. As not all vulnerabilities fall under the category of a specific published vulnerability, we also employ a proprietary library of manual tests and custom developed tools that are used to check for hard-to-find vulnerabilities, as well as many well-known commercial and public domain tools.

The assessment was conducted by consultants from the BT Ethical Hacking Center of Excellence (EHCOE), an industry leader in protecting business critical information assets.

Description of Testing

At the request of Federated Networks, BT has performed an application vulnerability assessment against: Federated Networks application identified in the Federated Networks Protected WebGoat Application Vulnerability Final Report.pdf

The objective of the FN Protected WebGoat Application assessment was to determine the overall security of the application by analyzing all possible transactions, user input variables, and application components that reside on client systems and test the FN connect software for the proper protection against any applicable application-level attacks

During this testing, BT ran the Webgoat application for those OWASP 'TOP 10 FOR 2010" covered by the Webgoat and FN lessons outlined in Schedule A. In addition, BT ran certain other tests, of its design, based on its customized process for conducting Ethical Hacking assessments of applications to determine the extent to which an attacker can view, alter, or delete information without proper authorization.

Other Federated Networks and third-party vendor systems, such as the underlying network infrastructure, were beyond the scope of this project. This testing also did not attempt any active network-based DoS attacks.

Various commercial, publicly available, and BT developed proprietary tools were used during testing. Publicly available tools used by BT have undergone a detailed review and evaluation. Review methods include—but are not limited to—validation of functionality, source code review, and sniffer log analysis.

Upon completion of the testing, BT presented all identified vulnerabilities/risks to Federated Networks in a detailed final report. Each vulnerability or risk identified was categorized as *high*, *medium,* or *low*, as follows:

- **High Risk:** These findings identify conditions that could directly result in the compromise or unauthorized access of a network, system, application, or information.
- **Medium Risk:** These findings identify conditions that do not immediately or directly result in the compromise or unauthorized access of a network, system, application, or information, but do provide a capability or information that could, in combination with other capabilities or information, result in the

compromise or unauthorized access of a network, system, application, or information.

- **Low Risk:** These findings identify conditions that do not immediately or directly result in the compromise of a network, system, application, or information, but do provide information that could be used in combination with other information to gain insight into how to compromise or gain unauthorized access to a network, system, application, or information. Low risk findings may also demonstrate an incomplete approach to or application of security measures within the environment.
- **Notes:** In addition to Findings, our reports also may contain Notes. Notes can include testing notes, discussions of security best practices, and other supplemental information that may not necessarily be related to the security posture of the systems tested.

Testing Results – Summary Opinion

The vulnerability assessment and testing was performed as outlined above against the FN Protected WebGoat Application, and Connect Secure Application**.** As a result of the testing and verification process completed on November 3, 2010, BT can confirm that there are ***no open High-Risk, no open Medium-Risk, and no open Low-Risk*** vulnerabilities identified at this time. **Further, the FN Connect Secure Web Application Gateway was able to stop all OWASP 'TOP 10 FOR 2010" covered by the WebGoat and FN lessons outlined in Schedule A**. In addition, BT ran certain other tests, of its design, to determine the extent to which an attacker may be able to view, alter, or delete information without proper authorization, each of which was unsuccessful in its attempt to exploit vulnerabilities.

Cautionary Note

The application assessments that BT performed was based on past experiences, currently available information, and known threats as of the date of testing. Given the constantly evolving nature of information security threats and vulnerabilities, there can be no assurance that any assessment will identify all possible vulnerabilities, or propose exhaustive and operationally viable recommendations to mitigate those exposures.

The statements relevant to the security of the Federated Networks applications in this letter reflect the conditions found at the completion of testing.

In accepting our report on the Federated Network's Secure Connect Protected WebGoat Application Federated Networks has acknowledged the validity of the above cautionary

statement. BT also strongly recommends that any network, information system, or online application be subject to periodic reassessment and policy review, in addition to complementary training of the key support personnel on such policies and procedures for the above infrastructure in order to maintain a strong security profile in the face of potential threats.

Appendix A

No.	OWASP Top 10 (2010)	Webgoat/ Fn Section	Webgoat/Fn Lesson	Mitigation Result
1 WG	**Injection Flaws**	Inject Flaws	Blind SQL Injection	✓
			Numeric SQL Injection	✓
			String SQL Injection	✓
			LAB: SQL Injection Stage1: String SQL Injection	✓
			LAB: SQL Injection Stage1: Numeric SQL Injection	✓
			Database Backdoors	✓
2 WG	Cross Site Scripting	Cross Site Scripting	Phishing with XSS	✓
			LAB: Cross Site Scripting: Stage 1: Stored XSS	✓
			LAB: Cross Site Scripting: Stage 3: Stored XSS Revisited	✓
			LAB: Cross Site Scripting: Stage 5: Reflected XSS	✓
			Stored XSS Attacks	✓
			Reflected XSS attacks	✓
			Cross Site Tracing (XST) Attacks	✓
3 WG	Broken Authentication & Session Management	Session Management Flaws	Hijack a Session	✓
			Spoof an Authentication Cookie	✓
			Session fixation	✓
4 FN	Insecure Direct Object Reference (direct url access)		FN Insecure Direct Object Reference (direct url access)	✓

5 WG	Cross-Site Request Forgery (Url/Parameter Manipulation)	Cross Site Scripting	Cross Site Request Forgery	✓
6 WG	Security Mis-Configuration	No Direct Lesson	Webgoat configuration of Tom Cat causes even a simple port scan creates a DOS outcome.	✓
7 FN	Insecure Cryptographic Storage		FN ~ Insecure Cryptographic Storage	✓
8 FN	Failure to Restrict URL Access (direct url access)		FN ~ Failure to Restrict URL Access (direct url access)	✓
9 FN	Insufficient Transportation Layer Protection (SSL)		FN ~ Insufficient Transportation Layer Protection (SSL)	✓
10 FN	Unvalidated Redirects and Forward (Url redirect)		FN ~ Unvalidated Redirects and Forward (Url redirect)	✓
No.	**Other Web Goat Lessons Tested**	**Webgoat/ Fn Section**	**Webgoat/Fn Lesson**	**Result**
11 WG	Access Control Flaws	Access Control Flaws	Bypass a Path Based Access Control Scheme LAB: Role Based Access Control - Stage 1: Bypass Business Layer Access Control	✓
			Remote Admin Access	✓
12 WG	Web Service Attacks	Web Services	WSDL Scanning	✓
			Web Service SAX Injection	✓
			Web Service SQL Injection	✓
13 WG	Ajax Security	Ajax	BT LAB: DOM-Based cross-site scripting	✓