



APPLICATION VULNERABILITY ASSESSMENT

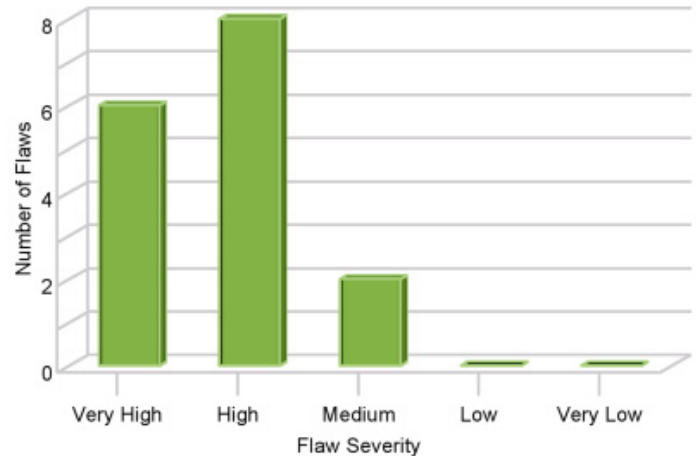
With better network level security technology hardening the network perimeter, malicious attackers are now focusing their efforts to strike at the least defended points the application. While hackers were once satisfied with defacing Web sites, unleashing denial of service attacks and trading illicit files through targeted networks, modern attackers are driven by profit, espionage, and potential cyber warfare. Federal government data and information systems have become targets.

Whether your organization develops, integrates or deploys software, you need to ensure that the applications are secure and free of major vulnerabilities. This on-demand software and application security assessment service identifies security risks in software code and applications and provides standards-based ratings to support actions and risk-based decisions.

FEATURES

Most software vendors, system integrators, and software development organizations lack an effective manner to evaluate the complete security quality of their applications. Government agencies that acquire these products and services need solutions to evaluate security risk and compliance with NIST and DOD security requirements. Traditional tools alone typically require access to source code which frequently isn't available. Manual penetration testing is time consuming, requires specialized resources and doesn't scale. The on-demand, automated security vulnerability testing:

- Determines if software meets minimum security risk acceptance prior to deployment;
- Independently verifies and validates the security of software;
- Detects software vulnerabilities such as cross-site scripting (XSS), SQL injection, and buffer overflows
- Detects back doors to protect you from malicious code injected into your application or inserted by outsourced application developers;
- Establish and monitor Security Metrics and SLAs with software providers;
- Available as either static analysis of binary code and/or dynamic testing of application based on system security impact level (FIPS PUB 199);
- Does not require access to source code;
- Shortens time to delivery and reduces costs associated with remediation after deployment;



- Increases and expands security testing capability without additional dedicated resources;
- Based on government and industry standards such as NIST Security Content Automation Program (SCAP) CWE CVSS, & SAMATE, and the Open Web Application Security Project (OWASP).
- Can be integrated with your existing security control assessment, vulnerability management and FISMA compliance efforts and solutions;
- Enables enterprises to conduct security audits by an independent trusted entity; and
- Pay as you go on a per application assessment basis establish an annual assessment program

SECURITY

The testing environment utilizes multiple layers of security consisting of:

Physical Security: Testing center infrastructure is a SAS 70 Type II certified datacenter which implements 24-hour physical security controls. Access to the testing center network and systems is protected by biometric scanners, man-traps, and card key readers. The entire facility is monitored by security cameras and full records of any physical access are maintained.

Perimeter Security: Testing center network perimeter is protected by multiple security systems to provide defense in depth. A combination of external and internal firewalls and intrusion detection systems, protect and monitor activity at the perimeter. All traffic between the Testing center and the customer is limited to Secure Socket Layer protocol. Security is monitored at each layer including network, operating system, application, and database layers. Configuration standards have been implemented for logging and monitoring security events.

Periodic network vulnerability assessments are also performed proactively using third party assessment tools, and identified vulnerabilities are remediated.

Personnel Security: Testing center employees must undergo background checks prior to employment. All personnel are issued access key cards which control and audit all access to systems and customer data.

Access Control: Testing center portal application uses role-based access control (RBAC) security model to govern access to your test results for the personnel you deem necessary. Access control follows least-privilege model to ensure that users only have access to the data necessary to perform their required job functions.

Customer Data: Customer data is destroyed when analysis is completed using secure deletion and overwriting of disk space.

SUPPORTED PLATFORMS

Static binary code analysis is supported for the following:

- C/C++ on Solaris, Windows and Linux
- C# on .NET / Windows
- Java J2SE, Java J2EE and JSP
- Applications must be packaged as executable and compiled with debug
- Scan can be performed without dependencies but will yield richer results if the dependencies are provided

Dynamic application testing is supported on the following platforms:

- Any web application built using Java, JavaScript, Perl, PHP or Python
- AJAX (Asynchronous JavaScript and XML), Web 2.0 technologies and Web services
- Technology must reside on the server and does not rely on dynamic client side (browser) computing.

CUSTOMER REQUIREMENTS

For static binary code analysis, the customer must provide or permit:

- IP address which is defined within its network. This address must be setup prior to start of task.
- Customer must complete a Data Source worksheet at the time of order which specifies includes the server IP addresses, communication port, instance name, and the password for the assessment user account.

For dynamic application testing, the customer must provide or permit:

- Complete test evaluation agreement which communicates responsibilities between the parties
- Provide publicly accessible URL or IP address. If the application is not publicly accessible, provide VPN access to the application.

- Testing or staging server / application. Testing on production systems is not recommended.
- Active devices such as IPS and WAF should be disabled in order to prevent the scan from being blocked.
- Contact information for system administrators and hosting providers monitoring these systems to avoid false alarms.
- Coordination and approval to run scan from hosting and network service providers.
- Valid user account with appropriate permissions if application requires authentication and any details on Single Sign-On if enabled.



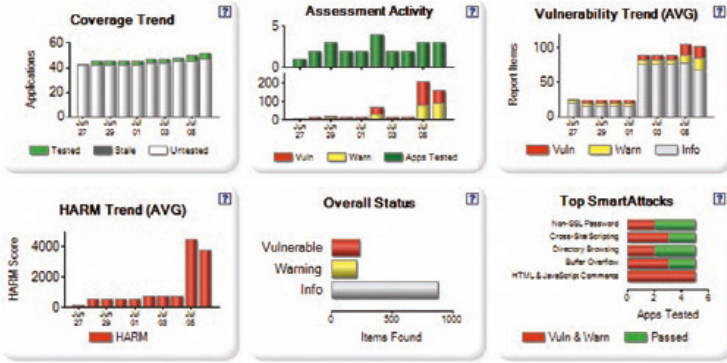
SERVICE AND DELIVERABLES

SecureIT has teamed with its partners, Veracode and Cenizc to offer award-winning technology and solutions in a fixed price approach. The solution provides your organization a complete security assessment without impacting the performance or stability of critical production systems.

Deliverables:

- Delivers actionable results within 72 hours.
- Software Assessment Report that provides program, product and security managers a security rating and detailed information as to the security vulnerabilities associated with the software or application.
- Identification of key policy, process, and technical findings
- Access to an online web-based portal that links vulnerability, remediation and software code to facilitate analysis and software remediation.
- Workflow to manage remediation and any follow up testing.

Security Summary: Jun 27, 2007 through Jul 06, 2007



Top 10 Applications by HARM: Jun 27, 2007 through Jul 06, 2007

<input type="checkbox"/>	Application	URL	Vuln	Warn	HARM Score	Status
<input type="checkbox"/>	Loan processing	http://crack.me.cenzic.com	109	96	22544	not queued report
<input type="checkbox"/>	Loan processing APAC	http://crack.me.cenzic.com	50	24	18954	not queued report
<input type="checkbox"/>	Loan staging - Fortify	http://loan.wf.com	34	45	1940	not queued report
<input type="checkbox"/>	Mail server	http://blackberry.cenzic.com:8080/	9	4	1268	queued report
<input type="checkbox"/>	Collaboration	http://blackberry.cenzic.com/	1	4	107	not queued report

CONTACT

SECURE|IT

Phone: 703.464.7010

Email: info@SecureIT.com

Web: www.SecureIT.com