DIGITAL DEFENCE

Web Service Security

Respond
Service

OVERVIEW

Now, more than ever, websites and applications offered across the Internet are a critical part of an organization's business. They are more than a company's image on the Internet — employees, customers, and partners expect to be able to access data and conduct financial services across the Internet.

To meet this requirement, websites are becoming more complex—they have moved from a static collection of web pages to complex become complex database-driven displays that accept input from users and from third parties. Each complexity increases the risks to your organization.

What's protecting you from attackers using your website and its services?

Traditionally, firewalls, intrusion detection systems, and other network devices protect and secure networks. However, these safeguards cannot distinguish between legitimate and hostile traffic targeting a website.

DigitalDefence's proprietary website and web application methodology, based on OWASPstandards, will assure you and your client's that your web presence is not exposing your sensitive data.

BENEFITS OF REVIEW THE SECURITY OF YOUR WEB SERVICES

- Provides an overview of existing vulnerabilities; provides proof of how exploitation could lead to compromise of an organization's systems or controls, and loss or damage of data
- Tests and validates the effectiveness of security controls
- Reduces lost downtime and recovery costs associated with successful attacks
- Demonstrates due diligence, reducing exposure to civil or criminal liability in the event of a security breach

Improve corporate risk reduction with strategic security and privacy services.

Is the Web Service Security Service right for your company?

More than 65% of assessed websites have at least one instance of a HIGH or CRITICAL vulnerability

- Can your network and its data be compromised through your website?
- Are you required to assess website security to remain PCI compliant?

SERVICE DELIVERY

Digital Defence's web application assessment is based on internationally-endorsed standards (OWASP), and assesses the following:

- Policies, standards, and procedures that relate to the web services operating environment
- Analysis of the physical site containing the web server and supporting components
- Network and server infrastructure that directly supports the web site and associated applications, including the base operating system, all applications and middleware, and database
- Threat modeling, a structured process to identify and document security threats
- Analysis of data leakage to the Internet and other connected networks ("Google Hacking")
- Website and associated web-enabled applications to identify misconfigurations and vulnerabilities
- Functional review of any e-commerce or transactional applications
- Static source code review, if required
- Review of backup, storage, and recovery procedures to ensure survivability of the site should a compromise ever occur

Throughout testing, DigitalDefence will take a variety of approaches to assess security and privacy. For example, testing may be conducted from the Internet, with no internal testing; or, testing may be a mix of remote and on-site testing.

The final methodology used will be working out in advance with each client. Although both automated and manual tools will be used, all vulnerability findings are manually verified to reduce false results.

DigitalDefence also provides training in auditing website and web services, as well as developer-focused training.

Top 10 Website Vulnerabilities (OWASP.ORG)

- Injection flaws, particularly SQL injection
- Cross-site scripting, XSS
- Broken authentication and session management
- Insecure direct object reference
- Cross site request forgery, CSRF
- Security misconfiguration
- Insecure cryptographic storage
- Failure to restrict URL access
- Insufficient transport layer protection
- Unvalidated redirects and forwards
- Does your development team know how to identify, and mediate, these vulnerabilities?

About Digital Defence

Digital Defence provides complete protection against data security breaches. We provide the advisory services that align security with your business strategy and practices. Our protection services secure your data by assessing vulnerabilities and validating security controls using audits and penetration testing, or "ethical hacking". And should you suffer a security or privacy breach, we provide the 24x7 response services and expertise to minimize financial and reputational loss.

Digital Defence Inc.
Toll-Free 800-385-1632 | Tel 519-771-8808
info@digitaldefence.ca | www.digitaldefence.ca