



WHITE PAPER

Web Application Scanning

SECURING YOUR WEB SITE FROM MALICIOUS INTRUDERS



MITIGATING WEB APPLICATION SECURITY RISK

IT security and network administrators are responsible for protecting their networks and everything that runs on them, including Web applications. When there is a breach or an exploit, the responsible security team (or person) becomes the center of attention. This "attention" comes with a high price tag; in 2007 alone, security breaches cost United States companies over \$4 billion.

Widespread use of Web 2.0 applications such as social networking, instant messaging, web mail and RSS are bypassing existing vulnerability detection technologies and working their way into enterprise networks. For these reasons, Web applications need to be audited on a regular basis and closely monitored for changes and improper usage.

To avoid becoming the center of attention, security administrators need a mechanism to:

- Maintain availability of revenue generating and customer facing Web applications
- Ensure corporate and customer data such as credit card, social security numbers and account information is secure from exploits and attacks
- Adhere to compliance issues like Sarbanes-Oxley, HIPAA, and PCI

This paper explains and outlines what a security administrator needs to know about Web applications and how successful security teams protect their networks from malicious intruders.

BUSINESSES RELY ON WEB APPLICATIONS

Web applications enable businesses to provide services that had previously been difficult to deliver to customers, employees, and partners, offering extraordinary power and flexibility and integrating a wide variety of technologies. However, these applications can also test the security infrastructure to the breaking point. Companies are getting much better at preventing unauthorized access to data, but hackers are getting much more sophisticated, making securing the network an ongoing competition.

With millions of people using the Internet to bank, pay bills, shop, communicate and perform research, companies can no longer secure their networks by only locking down the perimeter from unauthorized users. These web applications, which have become good for business, are designed to be accessed externally and therefore bypass the firewall and other network-based controls.

The popularity of Web applications has made them a choice target for hackers who attempt to corrupt data, crash hosts, gain access to the corporate network and steal valuable information. Because web applications exist as a conduit between external users such as business partners, supply chain and employee remote access, and a company's internal databases, they can be one of the biggest risks for IT security. For web applications that take credit cards, the risk affects both the corporation and their clients.

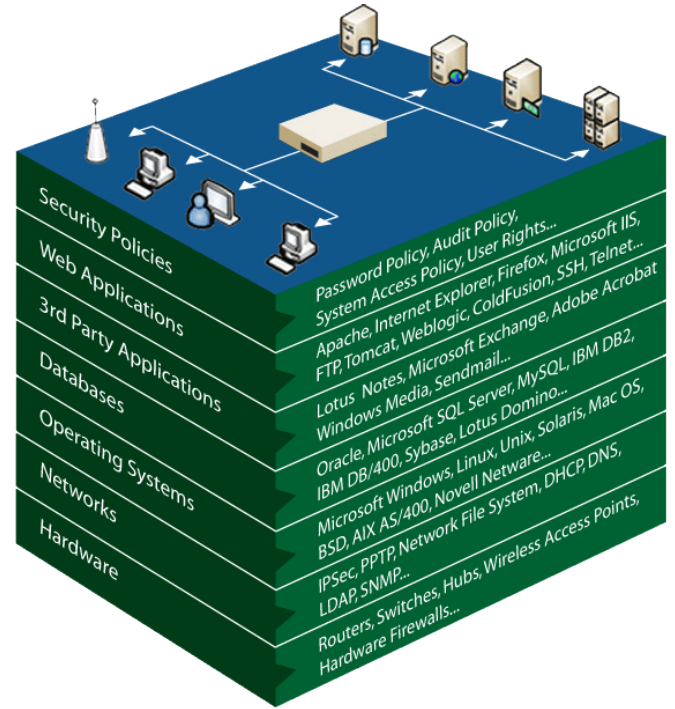
WEB 2.0 – SECOND GENERATION WEB APPLICATIONS

Web applications have grown in popularity due to their ease of use, update and maintenance without distributing and installing software on client computers. Web 2.0 concentrates on applications and services such as blogs, video sharing, social networking and podcasting that help make the Web more socially connected by enabling people to contribute as much as they can consume.

Enterprises are discovering that Web 2.0 applications have entered their infrastructures. Forrester Research defines Web 2.0 as, "a set of technologies and applications that enable efficient interaction among people, content, and data in support of collectively fostering new businesses, technology offerings, and social structures." By taking advantage of these technologies, businesses increase collaboration and access to information and people, enhance the end-user experience by embracing the latest Web technologies, and take advantage of legacy applications and data either through prepackaged applications or through composite Web applications.

WEB APPLICATION ARCHITECTURE

Web applications contain many moving parts. As you can see in the diagram to the right, web applications rely on multiple layers, each with a specific responsibility. In addition, Web applications are made up of three-layers: the Web browser, a content generation technology tool, and a database. Below these three layers are the network and operating system. Web applications can be tightly integrated or loosely coupled to create a cohesive user experience. If one layer malfunctions, the web application crashes and with it business revenue and customer satisfaction.



WEB APPLICATION EXPLOITS

According to the **SANS organization Top 20 report**, the threat landscape has changed over the last few years, where the types of vulnerabilities being exploited now have changed significantly over the years. Web application vulnerabilities account for almost half the total number of vulnerabilities discovered in 2007. These vulnerabilities are being exploited widely to convert trusted web sites into malicious servers serving client-side exploits and phishing scams. In addition, there has been significant growth in the number of client-side vulnerabilities, including vulnerabilities in browsers, in office software, in media players and in other desktop applications. Scanning the server without securing the client-side code leaves doors open for hackers to use to compromise your web application.

WEB APPLICATION VULNERABILITIES

According to the **Open Web Application Security Project (OWASP)**, the following chart lists the top ten Web application vulnerabilities and their definitions. For security administrators, the list provides the name as well as detailed information on the vulnerability. Security administrators should familiarize themselves with this list and the definitions to understand the ease of exploiting the vulnerability and the damage an exploit can inflict on their organization.

Cross Site Scripting (XSS)	XSS flaws occur whenever an application takes user supplied data and sends it to a Web browser without first validating or encoding that content. XSS allows attackers to execute script in the victim's browser which can hijack user sessions, deface Web sites, possibly introduce worms, etc.
Injection Flaws	Injection flaws, particularly SQL injection, are common in Web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.
Malicious File Execution	Code vulnerable to remote file inclusion (RFI) allows attackers to include hostile code and data, resulting in devastating attacks, such as total server compromise. Malicious file execution attacks affect PHP, XML and any framework which accepts filenames or files from users.
Insecure Direct Object Reference	A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, database record, or key,

	as a URL or form parameter. Attackers can manipulate those references to access other objects without authorization.
Cross Site Request Forgery (CSRF)	A CSRF attack forces a logged-on victim's browser to send a pre-authenticated request to a vulnerable Web application, which then forces the victim's browser to perform a hostile action to the benefit of the attacker. CSRF can be as powerful as the Web application that it attacks.
Information Leakage and Improper Error Handling	Applications can unintentionally leak information about their configuration, internal workings, or violate privacy through a variety of application problems. Attackers use this weakness to steal sensitive data, or conduct more serious attacks.
Broken Authentication & Session Management	Account credentials and session tokens are often not properly protected. Attackers compromise passwords, keys, or authentication tokens to assume other users' identities.
Insecure Cryptographic Storage	Web applications rarely use cryptographic functions properly to protect data and credentials. Attackers use weakly protected data to conduct identity theft and other crimes, such as credit card fraud.
Insecure Communications	Applications frequently fail to encrypt network traffic when it is necessary to protect sensitive communications.
Failure to Restrict URL Access	Frequently, an application only protects sensitive functionality by preventing the display of links or URLs to unauthorized users. Attackers can use this weakness to access and perform unauthorized operations by accessing those URLs directly.

WEB APPLICATION DEVELOPMENT AND WEB SCANNERS

Web Application Vulnerability Scanners are products designed to scan web applications for potential vulnerabilities. A web application scanner first crawls the entire application, analysing in-depth each file it finds, and displaying the entire application's structure. After this discovery stage, it performs an automatic audit for common security vulnerabilities by launching a series of web attacks. Web application scanners check for vulnerabilities on the web server, proxy server, web application server and even on other Web services. However, these products differ from general vulnerability assessment solutions in that they do not perform a broad range of checks on other software and hardware devices.

WEB APPLICATION DEVELOPMENT CHALLENGES

If developers could produce completely secure code 100% of the time, there would be no vulnerabilities in software. The real problems with web application development include:

- **Intense time-to-market pressure** – as developers rush to deliver an application, security considerations may not be top priority. Even if developers have a static code analysis product, they may not run it every time the application code is modified.
- **More casual view of testing in-house applications** - In-house applications are subjected to less scrutiny and QA than "shrink-wrap" software because the in-house software isn't sold as a product.



- **Lack of application testing on production servers** - To the extent that web applications are tested at all, they tend to be tested on a developer's workstation and/or staging server. Production testing by developers is a challenge because production application servers usually are managed by the IT team and not the development team.

WEB APPLICATION SCANNER CHALLENGES

In addition to the issues with application development and security, Web scanners may have some of the following security challenges:

- **Limited scanning** – Web scanners usually only scan the web application components and don't take into account the underlying network, operating systems and third party applications and data stores.
- **Infinite web sites** - To test web applications for vulnerabilities, finding all of its functional parts is a major challenge. Crawling deep links and misidentifying a dynamically created link can cause Web scanners to fall into an infinite scan.
- **Knowledge of Web 2.0 technology** – Many Web scanners are unable to scan AJAX, Flash, Flex and other Web 2.0 technologies appropriately, leaving many doors open to corporate data.
- **False positives and vulnerability duplicates** - It's very difficult to tell if several similar reported vulnerabilities are, in fact, the same issue. Vulnerable parameters may be shared across different scripts and URLs may contain dynamic content.

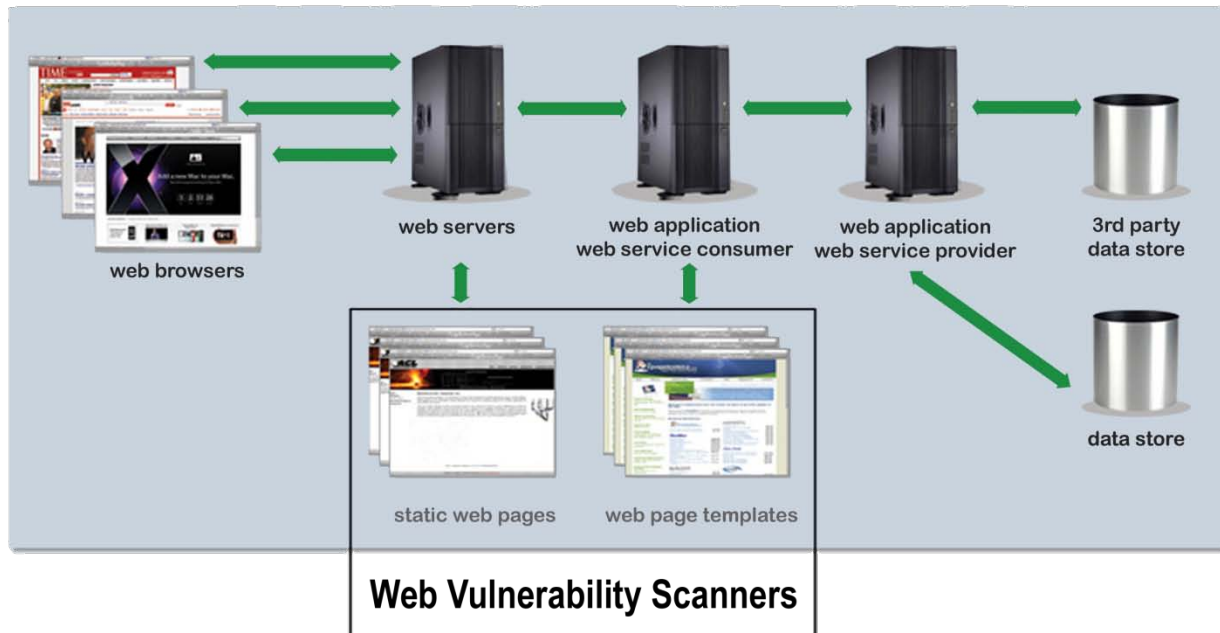
WEB APPLICATION SCANNING

THE NEED FOR COMPLETE VULNERABILITY SCANNING

Since Web applications are only as strong as their weakest link, scanning Web applications needs to go deeper to dig out weaknesses and vulnerabilities that exist on network devices, operating systems, databases. By using only a web scanner, security personnel increase the chance of attacks and exploits because they may miss exposures that open their entire network to attack. In addition, by limiting the vulnerability scan to just the Web application, companies cannot guarantee that sensitive customer and corporate data is secure.

The diagram below provides a simplified look at a web application's moving parts. In each area or layer, there could be vulnerabilities that must be located and remediated to reduce the risk of attack. For instance, when the underlying operating system on the web server is vulnerable, even inexperienced hackers can find and exploit that vulnerability to steal vital information or damage the application and render the entire system useless. This results in web application downtime and the loss of business revenue and customer satisfaction.

To effectively find and remediate vulnerabilities in Web applications, security administrators need more complete and reliable



scanning solutions than traditional web scanners offer. Vulnerability scanners are beginning to incorporate scanning technologies that dig deeper into the environment and provide a more complete and accurate picture of what security issues may be lurking inside of a web application.

Web application pass-through scanning

Most Web scanners can only report a single instance of inspection to security auditors. Web application pass-through scanning finds vulnerabilities and then uses information about the discovered vulnerability to scan deeper into the environment to uncover more exposures. In order to be useful, most web applications must have a connection to a database. If the web application contains a vulnerability (such as a SQL injection exposure), access to the underlying database is possible through the web application. Most often, if a hacker can access the database directly, he can use the database to access to the underlying operating system. Logically, if a hacker can penetrate database using the web application as a vector, the scanning technology you use to secure your applications should have the same capabilities.

Fast scanning for multiple Web applications

Most web scanners were built for web application programmers and web developers, enabling them to scan individual web applications during the build and test phases. However, they lack the functionality and speed to scan multiple Web applications at the same time.

Vulnerability scanners that support scanning Web applications implement Web spidering technology that scans Web sites and Web applications for vulnerabilities much like Google spidering searches for words and terms. Using this methodology, vulnerability assessment solutions spider the application to find and report on vulnerabilities. Using spidering technology in conjunction with pass-through web application scanning, vulnerability scanners can provide more accurate reporting of the exposures that are found in this complex environment.

Browser-based scanning

Web 2.0 applications take user interaction to a new level, opening up potential weaknesses that could affect the security of your entire networked environment. Companies need to scan the client-side components of the application to ensure your systems are



secured. Browser emulation or browser-based scanning is the only way to correctly scan Web 2.0 applications. Vulnerability scanners that implement browser-based scanning are able to analyze JavaScript, AJAX and Flash applications, providing a more in-depth and accurate report of the application.

Browser-based scanning is extremely important to Web development as well as the security team. The technology searches for vulnerabilities in Web applications the same way a hacker looks for openings. Web scanners lack browser-based scanning technology and search only the source code for vulnerabilities. Searching for vulnerabilities in the code is important, but having a vulnerability assessment solution that mimics the techniques a hacker would use to penetrate the application, provides more extensive scanning and therefore, secures your web applications more effectively.

CONCLUSION

Security experts agree that as more and more organizations develop web applications, vulnerabilities and exploits will increase dramatically. To mitigate the risk, businesses need to acquire vulnerability assessment solutions that help security administrators easily scan and secure all web application components and technologies, including networks, operating systems and third party applications. By implementing a complete vulnerability scanning solution that accurately scans for vulnerabilities in their entire IT environment, companies can avoid breaches and exploits and maintain business revenue and customer satisfaction.

ABOUT RAPID7

Rapid7 is a leader in vulnerability management and compliance, delivering a single unified solution across an organization's entire infrastructure. Rapid7 NeXpose is the only solution that includes support for web applications, databases, operating systems, and network devices in a single system. It separates real threats from the noise common to most vulnerability management systems, giving direct, actionable visibility into the real threats to mitigate risk and remain compliant. For more information on NeXpose products and services, visit www.rapid7.com.