TREND MICRO™

A TrendLabs Cloud Security Primer

Web Application Vulnerabilities

HOW'S YOUR BUSINESS ON THE WEB?

Conducting Business on the Web

Enterprises develop web applications to leverage the convenience offered by Internet technologies and meet customer demand. Web applications can be as simple as applications that facilitate customer contact or as complex as those that facilitate online auctions, medical record keeping, banking, and such.

These applications process data and store results in a back-end database server where business-relevant data such as customer information sits. Web applications, depending on their specific purpose, regularly interact with customers, partners, and employees. Unfortunately, dependencies and interactions between in-house and third-party resources, objects, and inputs inevitably introduce security holes.

Enterprises continue to create and use web applications in order to provide user-friendly interfaces to users utilizing available technologies. The following factors, which involve the development and upkeep of web applications, contribute to security risks:

- **More complex transactions.** More and more mission-critical processes, not just externally oriented ones such as sales and marketing, are leveraging Internet connectivity.
- **Orphaned web applications.** Applications' development teams are sometimes no longer with the company and can no longer address security issues when these are found.
- **Legacy applications.** Older applications created before related security policies were instituted may suddenly be exposed once web interfaces are added to these.
- **Short time to market.** Rapid development and increased functionality requirements force developers to ship web applications without closely looking at possible security holes.
- **Custom-made web applications.** In-house-developed applications are difficult to standardize even within a company. Human error is always a possibility.
- **Coding without security in mind.** Security may have been overlooked in the software development life cycle.

At the same time, patch management problems such as those outlined in the TrendLabs Cloud Security Primer, "Maintaining Vulnerable Servers: What's Your Window of Exposure?," contribute to the difficulty of keeping even off-the-shelf web-related servers and databases updated with the latest patches.[1] Among these challenges are the need to test emergency patches prior to deployment, the choice to delay patch deployment if the patch proves unstable, or sometimes even the lack of security updates from the vendors themselves.

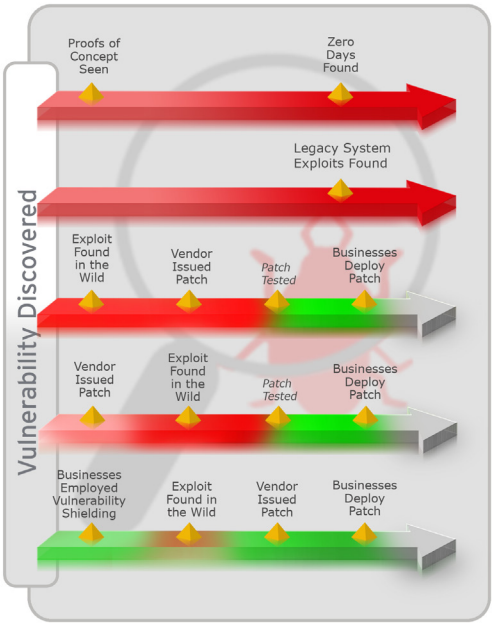
Furthermore, the administration of web, application, and database servers also adds security concerns. Running unnecessary services, using default configurations, enforcing weak passwords, and not reviewing permissions are easily remedied poor practices that many IT administrators still make the mistake of doing.

1 http://www.trendmicro.com/cloud-content/us/pdfs/business/white-papers/wp_vulnerability-shielding-primer.pdf

- According to Gartner, 75% of all external attacks occur at the application layer.[1]
- According to *CVEdetails.com*, 10 products associated with web application delivery and development are included in the "Top 50 Products with 'Distinct' Vulnerabilities" list.[2]
- According to Netcraft, the most common HTTP server is Apache (64%), followed by Microsoft IIS (14%).[3]

1 http://www.sigist.org.il/_Uploads/dbsAttachedFiles/GartnerNowIsTheTimeForSecurity.pdf
2 http://www.cvedetails.com/top-50-product-cvssscore-distribution.php
3 http://news.netcraft.com/archives/2012/06/06/june-2012-web-server-survey.html#more-6013

Window of Exposure Scenarios



The Weakest Link in Web 2.0 Security

The 2011 Trend Micro review of exploits and vulnerabilities predicted that the volume of vulnerability exploits will continue to increase throughout 2012.[2] Attacks that take advantage of server and application vulnerabilities allow attackers to penetrate a network and potentially access an organization's confidential data.

The Web is considered "stateless" in nature as web developers continuously create websites that are primarily designed to be fast and scalable and intended for various users. As such, security becomes a second priority. Conversely, web applications that are built on top of the stateless unsecured Web are more secured. Application developers focus more on user experience, making applications more user specific, thus maintaining a "stateful" nature.

How Vulnerable Are Your Servers?

Apart from web applications, vulnerabilities residing in web and database servers can be also exploited by attackers to get inside a network or to prevent an enterprise's customers from accessing its website. Here are some recent attack samples:

While Web 2.0 aids enterprises in conducting business, it also introduces a plethora of damaging risks.

- **Web server-related attacks**
  - Microsoft released an out-of-band update for a vulnerability in *ASP.NET* that, when exploited, can cause a denial of service (DoS) and potentially take down a server.[3] As such, this threat can disrupt business operations and potentially lead to financial loss.
  - Last year, in a mass compromise attack dubbed "Lizamoon," thousands of websites were compromised, affecting numerous companies in various industries. Malicious URLs were inserted to vulnerable websites through SQL injection, which led visitors to download FAKEAV and WORID malware.[4] Furthermore, last February 2012, the French confectionery website, *laduree.fr,* was also compromised to infect visitors' systems with ransomware.[5]
  - A vulnerability in *Apache HTTP Server (CVE-2011-3192),*[6] when exploited, can allow cybercriminals to launch a DoS attack against a vulnerable server with the mere act of sending an HTTP request.[7]
- **Web application server-related attack**
  - An e-commerce website was injected with a malicious code that affected nearly 300 view item pages showcasing gold-plated jewelry.[8] The said code led to a series of redirections that finally ended with the download of various malware. However, because the code had a missing tag, the infection chain, which could have caused a massive malware outbreak, failed to entirely execute.

Potential Attacks That Enterprises May Encounter

- Injection
- Cross-site scripting (XSS)
- Broken authentication and session management
- Insecure direct object references
- Cross-site request forgery (CSRF)
- Security misconfiguration
- Insecure cryptographic storage
- Failure to restrict URL access
- Insufficient transport layer protection
- Unvalidated redirects and forwards[1]

1 https://www.owasp.org/index.php/Top_10_2010-Main

2 http://blog.trendmicro.com/2011-in-review-exploits-and-vulnerabilities/
3 http://blog.trendmicro.com/microsoft-releases-out-of-band-update-before-year-ends/
4 http://blog.trendmicro.com/lizamoon-etc-sql-injection-attack-still-on-going/
5 http://blog.trendmicro.com/compromised-website-for-luxury-cakes-and-pastries-spreads-ransomware/
6 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3192
7 http://blog.trendmicro.com/solutions-now-available-for-apache-killer/
8 http://blog.trendmicro.com/missing-tag-foils-compromise/

- Database server-related attacks
  - A vulnerability in Oracle Database Server's *TNS listener*, which when successfully exploited, does not require a user name and/or password to gain network access was also discovered.[9] This allows an attacker to potentially access and steal corporate data.[10]
  - A security bug in previous versions of *MySQL* and *MariaDB* can allow an attacker to access a vulnerable database by submitting random passwords.[11]

These attacks do not only threaten to disrupt businesses or tamper with an enterprise's image but can also lead to unauthorized access to and/or use of an organization's critical data.

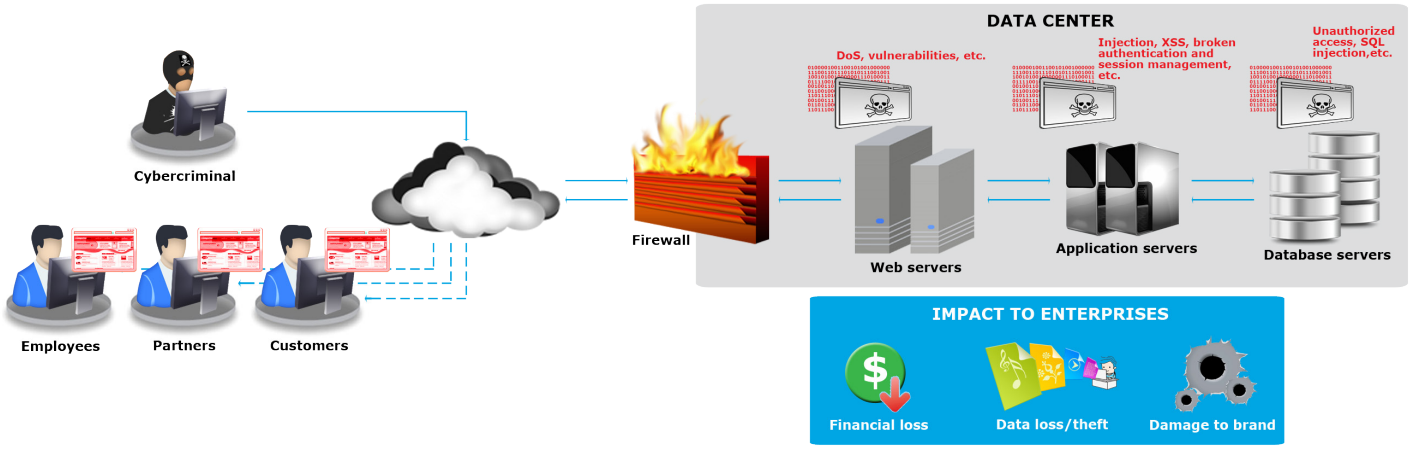


Figure 1: Security risk diagram for web applications and servers

Securing Web Applications

Baseline Web, Application, and Database Server Security Practices

Good web server security maintenance involves reviewing if you really need all the services that are set to run, enabling only relevant ports, using strong passwords, and limiting access to the server.

IT administrators should enforce security policies and audit all existing and future in-house-developed software for compliance, especially those that will have some form of user interaction or input required on the Web. Too many attacks succeed simply because the software developer did not set up user input validation before processing. Web applications should ideally be coded as securely as possible.

Updating security patches for web servers and applications should be an established practice considering the speed by which exploits are created. However, there will be scenarios wherein patching an "always-up" machine is extremely difficult and costly to a business. Sometimes, a vulnerability will be long exploited before a patch is ever released.

9 http://www.oracle.com/technetwork/topics/security/alert-cve-2012-1675-1608180.html
10 http://blog.trendmicro.com/microsoft-releases-an-update-covering-duqu-oracle-and-adobe-vulnerabilities-patched-too/
11 http://arstechnica.com/information-technology/2012/06/security-flaw-in-mysql-mariadb-allows-access-with-any-password-just-keep-submitting-it/

Vulnerability-Shielding Solutions

A range of solutions (e.g., web application scanners, database auditing and protection [DAP] tools, database activity monitoring [DAM] tools, file integrity monitoring software, etc.) are made available to protect web applications. Understandably, each solution has its own strengths and focus. However, in certain instances, where defense against exploits is needed even if patches are not yet available, the value of vulnerability shielding, aka "virtual patching," is distinguished. This is also especially useful in easing patch management difficulties. By examining the incoming or outgoing traffic to and from vulnerable applications, vulnerability-shielding solutions such as those embedded in *Trend Micro™ Deep Security* can correct traffic according to a vulnerability signature.[12]

Web Application Protection Technologies

The most common web application vulnerabilities lead to SQL injection and XSS attacks. Some web application protection technologies such as those present in *Deep Security* can defend public-facing web servers and applications against these attacks.

12 http://www.trendmicro.co.uk/media/ds/deep-security-datasheet-en.pdf

TREND MICRO™

Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global cloud security leader, creates a world safe for exchanging digital information with its Internet content security and threat management solutions for businesses and consumers. A pioneer in server security with over 20 years' experience, we deliver top-ranked client, server and cloud-based security that fits our customers' and partners' needs, stops new threats faster, and protects data in physical, virtualized and cloud environments. Powered by the industry-leading Trend Micro™ Smart Protection Network™ cloud computing security infrastructure, our products and services stop threats where they emerge—from the Internet. They are supported by 1,000+ threat intelligence experts around the globe.

TREND MICRO™

Securing Your Journey to the Cloud

TRENDLABS℠

TrendLabs is a multinational research, development, and support center with an extensive regional presence committed to 24 x 7 threat surveillance, attack prevention, and timely and seamless solutions delivery. With more than 1,000 threat experts and support engineers deployed round-the-clock in labs located around the globe, TrendLabs enables Trend Micro to continuously monitor the threat landscape across the globe; deliver real-time data to detect, to preempt, and to eliminate threats; research on and analyze technologies to combat new threats; respond in real time to targeted threats; and help customers worldwide minimize damage, reduce costs, and ensure business continuity.

TrendLabs
Global Technical Support & R&D Center of TREND MICRO