TREND MICRO™

A TRENDLABS SECURITY ADVISORY ON THE RECENT ATTACK AGAINST WEB APPLICATION VULNERABILITIES

Conducting Business on the Web

On October 2, 2014, JP Morgan filed a report to the United States Securities and Exchange Commission to disclose that the data of approximately 76 million households and 7 million small businesses was compromised.[1] Stolen data were said to include names, addresses, phone numbers, and email addresses. The data breach was reportedly accomplished through attacks against web applications used by the bank -- attackers leveraged on vulnerabilities found in the web applications in order to gain access to the bank's internal network.

- According to CVEdetails.com, several products associated with web application delivery and development are included in the "Top 50 Products with 'Distinct' Vulnerabilities" list.[1]
- According to Netcraft, the most common web servers are Microsoft, Apache and nginx.[2]

The attack highlights the role of web applications as an infection point, as well as the great need to ensure that these web applications are secure from vulnerabilities. This enterprise primer aims to help enterprises understand this need, and to guide them in terms of security strategies they can adapt to make sure that their business stays safe from attacks.

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.

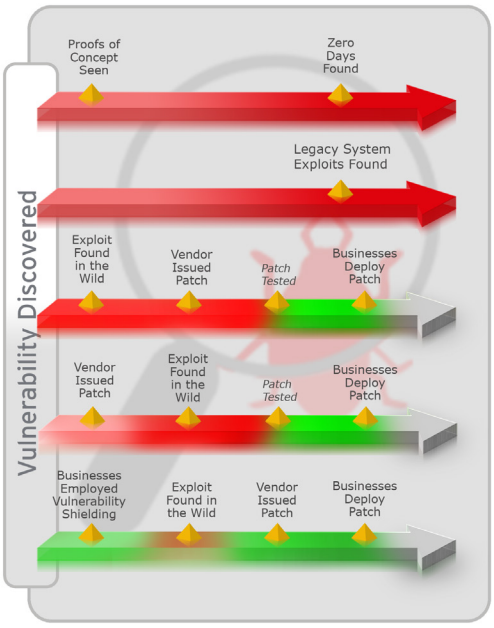
These applications process data and store results in a back-end database server where business-relevant data such as customer information sits. Web applications, depending on their specific purpose, regularly interact with customers, partners, and employees. Unfortunately, dependencies and interactions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

1 http://www.cvedetails.com/top-50-vendors.php
2 http://news.netcraft.com/archives/2014/09/24/september-2014-web-server-survey.html

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:

- **Increasingly 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.

Window of Exposure Scenarios



1 http://investor.shareholder.com/JPMorganChase/secfiling.cfm?filingID=1193125-14-362173

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.[2] 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.

The Weakest Link in Web 2.0 Security

Reports of server-side data breaches and zero-days found for widely used web applications continue have become quite common in recent years.[3] Attacks that take advantage of server and application vulnerabilities allow attackers to penetrate a network and potentially access an organization's confidential data.

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

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:

- **Web server-related attacks**
  - A vulnerability was found in Plesk -- a popular hosting control panel -- which could allow an attacker to fully control a vulnerable webserver. This vulnerability is easily exploitable with the exploit code available and successful exploitation can lead to complete compromise of the system with web service privileges.[4]

Potential Attacks That Enterprises May Encounter

- Injection
- Broken authentication and session management
- Cross-site scripting (XSS)
- Insecure Direct Object References
- Security Misconfiguration
- Sensitive Data Exposure
- Missing Function Level Access Control
- Cross-site request forgery (CSRF)
- Using Component with Known Vulnerabilities
- Unvalidated Redirects and Forwards[1]

1 https://www.owasp.org/index.php/Top_10_2013-Top_10

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

3 http://about-threats.trendmicro.com/us/security-roundup/2014/2Q/turning-the-tables-on-cyber-attacks/

4 http://blog.trendmicro.com/trendlabs-security-intelligence/plesk-zero-day-exploit-results-in-compromised-webserver/

- In August 2014, users from Japan were hit by an attack involving an exploit kit that relied on a compromised website add-on. This particular add-on is used by site owners who want to add social media sharing buttons on their sites. However, this script was being used for malicious purposes. On certain sites, instead of the original add-on script, users were redirected to the script of the FlashPack exploit kit. [5]
- Recently, Shellshock,[6] a vulnerability found in the Bash command shell, that is the default on Linux, alarmed the security community because of the possible attack scenarios that were revealed. Attackers can use Shellshock to change the content of web server and website code, deface the website or steal user data from databases, among others. And with over half of the 1 Billion servers on the Internet using Apache, the problem is significant[7]

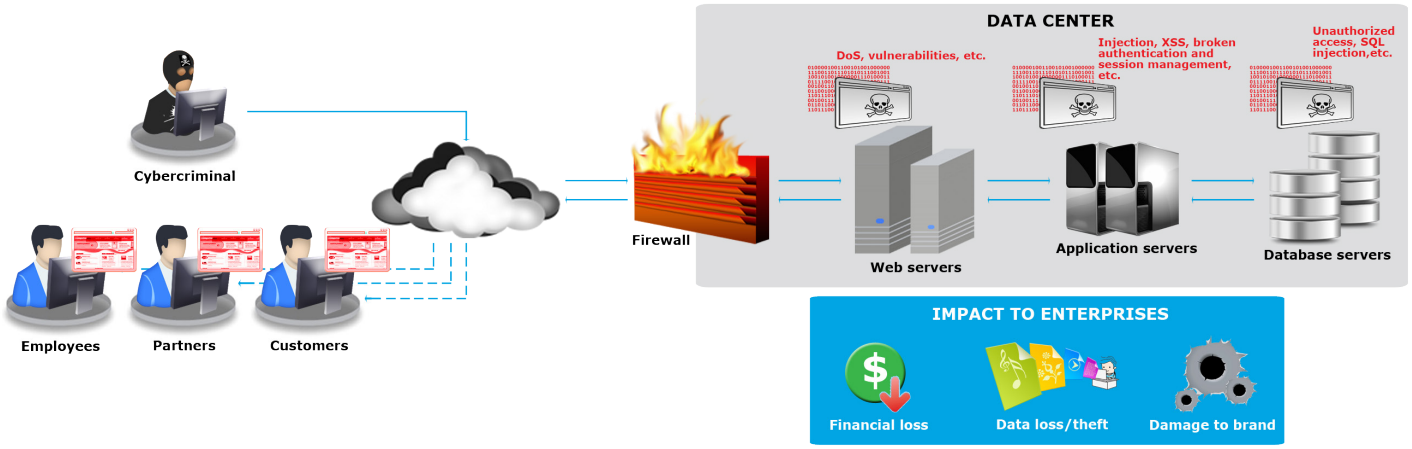


Figure 1: Security risk diagram for web applications and servers

- **Web application server-related attack**
  - An old attack once found an e-commerce website 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.[8]
  - According to the Verizon 2014 Data Breach Investigation Report, 35% of breaches they tracked in 2013 are due to web application attacks, described as exploiting a weakness in an application or using stolen credentials.[9]

5 http://blog.trendmicro.com/trendlabs-security-intelligence/website-add-on-targets-japanese-users-leads-to-exploit-kit/
6 http://blog.trendmicro.com/trendlabs-security-intelligence/shell-attack-on-your-server-bash-bug-cve-2014-7169-and-cve-2014-6271/
7 http://www.internetlivestats.com/total-number-of-websites/
8 http://blog.trendmicro.com/missing-tag-foils-compromise/
9 http://www.verizonenterprise.com/DBIR/2014/

- API leaks have become common occurrences in some noteworthy incidents in the past. Researchers, in one instance, released two exploits for a photo messaging application site,[10] one which allowed hackers to match user names with phone numbers, and another which allows hackers to create fake accounts. Other web applications have suffered the same fate as well.[11] [12]

- 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.[13] This allows an attacker to potentially access and steal corporate data.[14]
  - A security bug in previous versions of *MySQL* and *MariaDB* can allow an attacker to access a vulnerable database by submitting random passwords.[15]
  - An online auction site disclosed that they had suffered a breach that compromised a database containing "encrypted passwords and other non-financial data". While they said there was no evidence of unauthorized activity or access to financial information, they recommended all of their users to change their passwords.[16]

These attacks 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.

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. Or, like the recent Shellshock vulnerability, the issue may be so widespread that it will simply take a lot of time to both figure out where the vulnerable servers are and then get the patches in place.

10 http://www.technewsworld.com/story/79705.html
11 http://blog.internot.info/2014/06/paypals-2-factor-authentication2fa-good.html
12 http://arstechnica.com/security/2014/09/apple-knew-of-icloud-api-weakness-months-before-celeb-photo-leak-broke/
13 http://www.oracle.com/technetwork/topics/security/alert-cve-2012-1675-1608180.html
14 http://blog.trendmicro.com/microsoft-releases-an-update-covering-duqu-oracle-and-adobe-vulnerabilities-patched-too/
15 http://arstechnica.com/information-technology/2012/06/security-flaw-in-mysql-mariadb-allows-access-with-any-password-just-keep-submitting-it/
16 http://blog.trendmicro.com/trendlabs-security-intelligence/ebay-latest-victim-of-massive-data-breach/

Sometimes, a vulnerability will be long exploited before a patch is ever released. This is why there is a need for vulnerability and application shielding.

Server Vulnerability Shielding

It is not always going to be possible to patch immediately for known vulnerabilities. Patches often take time for the application developer to deliver, and then the patches need to be applied. Organizations have an opportunity to put protection in place in advance of deploying patches, leveraging technologies like Intrusion Prevention (IPS) that can be deployed both at the perimeter as well as at the server or host. Taking a host-based approach has numerous advantages, including protecting from external attacks, as well as those that may originate inside the enterprise as a result of a breach that has occurred at an earlier date. Host-based protection also enables the application of environment-specific protection in a timely way, ensuring that unnecessary generic enforcement at the perimeter doesn't somehow interfere with ongoing business. In addition to helping with specific known vulnerabilities, a host-based IPS can help address zero-day attacks through protection from common malicious patterns, anomalies and uncommon behavior, as well as disabling functionality that is not commonly used. It is important to choose a security partner that has both experience in detecting and addressing vulnerabilities, as well as one that can react quickly and allow organizations to put shielding in place quickly. For example, Trend Micro released updated IPS rules for Deep Security, a market-leading data center and cloud security platform, in under 24 hours for the recent Shellshock vulnerability and is actively protecting customers from global attacks today.

Web Application Protection

Knowing what vulnerabilities are present across a web infrastructure is a critical step in the overall security of web applications. It is recommended that both the platform components (ex: web server, OS) as well as application components are regularly scanned for both known and potential vulnerabilities. Taking this multi-layered approach enables a more complete view of potential issues as well as a clearer path to putting protection in place, whether that is through a patch, code changes, or leveraging an IPS and/or Web Application Firewall (WAF). As a best practice for web application scanning, look for offerings, such as Deep Security for Web Apps, that use a generic "attack" approach to probe the web application and test for threats like OS command injection (like the Shellshock vulnerability). This allows organizations to get a clear picture quickly of what the current state is, and then enable remediating steps to be taken.

It is clear that web applications will continue to play an increasing role in the way that businesses operate, with the cloud accelerating their use at an exponential rate. As discussed in this paper, attacks on vulnerabilities like Shellshock, Heartbleed, and others clearly demonstrate that proactive steps need to be taken in protecting those applications, particularly beyond traditional perimeter security and basic patching. Trend Micro has market-leading solutions optimized for virtualized and cloud environments that are helping thousands of organizations today to protect their web application infrastructure. Find out more about how Trend Micro can help your organization at **www.trendmicro.com/datacenter.**

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