SONICWALL

# EXECUTIVE BRIEF: WHY YOU NEED WEB APPLICATION SECURITY

## Understanding the Inherent Risks of Business Websites


## Abstract

Web applications are more indispensable to business than ever before. However, they carry significant risks. This brief explores potential web-based exploits and attacks that IT must address, including:

- Code injection/remote code-inclusion
- Cross-site scripting (XSS) vulnerabilities
- Web session hijacking
- Insufficient authentication and authorization


## Introduction

In today's application-centric world, web applications are a key enabler for most organizations competing in a globally contested digital-business environment. This includes branding, publicity, competitiveness and customer acquisition, to just name a few.

Businesses, institutions and government are constantly under pressure to innovate and develop useful web applications to fulfill users' endless appetite for instantaneous access to information, services and support.

### The explosive growth of web applications in business

Internet users now account for over half[1] of the world population. Ninety-three percent[1] of all internet users now go online, and perhaps stay online longer using their mobile devices as opposed to their computers. Moreover, with the addition of the Internet-of-Things (IoT), we have now added tens of billions[2] of devices already connected, communicating and exchanging data through web and mobile applications today – from TVs, digital wearables, cars, gaming consoles and vending units, to all sorts of smart appliances.

As a result, organizations strive to provide the highest possible service experience and engagement through different types of

interactive web applications and user-friendly mobile applications. This makes web applications more indispensable now than ever before. Businesses must keep them all online and safe.

### Inherent security concerns

However, anytime a web application software is deployed alongside the data it needs to access, it becomes a security risk. This is because it is a potential entry point for attackers who wants to steal such data or gain further access to more sensitive parts of the network. Every web application deployed exposes organizations to a very large spectrum of potential web-based exploits and attacks.

One recent report[3] states that nearly 50 percent of web applications are always vulnerable throughout the year. These harmful flaws include information leakage (37%), cross-site scripting (33%), content spoofing (27%), insufficient transport layer protection (21%) and cross-site request forgery (15%). In terms of critical business impact, SQL injection ranks as the highest-severity vulnerability, followed by cross-site scripting (XSS), cross-site request forgery (XSFR) and insufficient authorization.

These findings indicate that web applications continue to experience serious source code quality issues and security concerns. Web development teams seems to have not yet fully incorporate necessary security practice into developing their code. According to Gartner[4], "Developers will keep developing insecure code, and there's nothing they can do about it. It's a losing battle with hackers."

Poor web development process, along with insufficient security patching, are putting compliance data at risk. As a result, companies are failing to comply with regulatory security controls, such as PCI, HIPPA and GDRP. Software vulnerabilities are regularly reported and being exploited in applications such as Content Management Systems (CMS), forums and portals used by organization of all sizes and industries.

Exacerbating this problem is the use of many protocols in web applications, such as HTTP(S), JSON, XML and SOAP, and the unrestricted and openness nature of the user-interface (UI). In addition, organizations put their web applications at risk while waiting for internal and/or third-party software developers to patch these systems.

### Attack scenarios

As an example, let's examine a typical web form which was designed using a popular web development language, such as JavaScript or PHP.

This form accepts various parameters for the web applications to process the information being collected. If the application lacks security safeguards, such as parsing and validation of the input data, attackers can potentially exploit the application, and compromise the service by posting arbitrary content to the form.

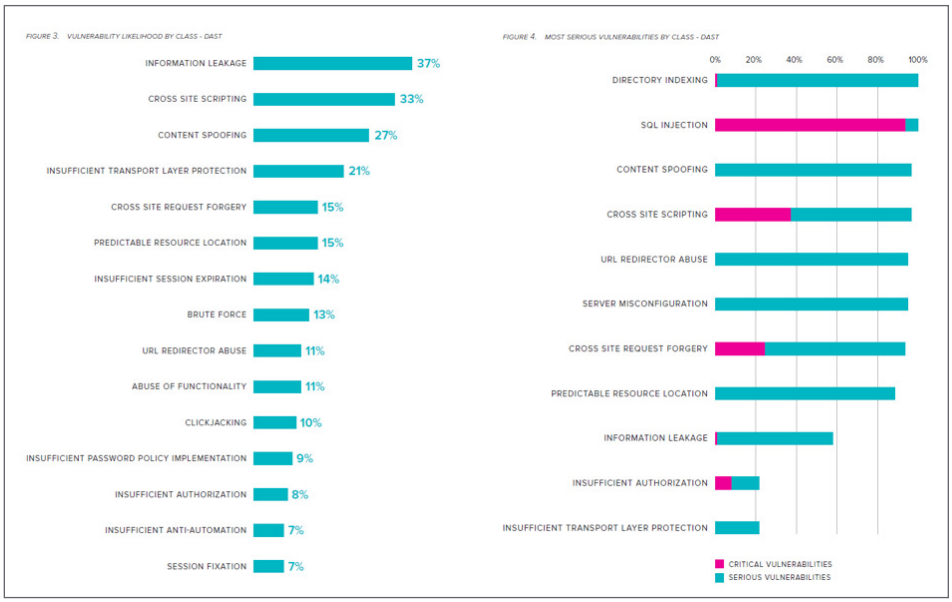
In this scenario, it is possible that one or more common PHP application vulnerabilities would allow attackers to include their own code in the targeted web application. This is typically known as a local or remote code inclusion type of attack.

Typical web servers today host multiple web applications on a single host, and are accessible via a single port (port 80 for HTTP and 443 for HTTPS). This creates a large attack surface for organizations to defend.

## Conclusion

Businesses can neither depend nor rely on their web development team to present flawless web applications. With the number of attempted web attacks that can range from hundreds of thousands to even millions over the course a year, IT administrators must take security matters into their own hands.

**Learn more.** Read our solution brief, "Best Practices for Web Application Firewall" or visit www.sonicwall.com/web-application-firewall.




[1] https://thenextweb.com/contributors/2017/04/11/current-global-state-internet/
[2] https://cdn.ihs.com/www/pdf/IoT-ebook.pdf
[3] https://info.whitehatsec.com/rs/675-YBI- 674/images/WHS%202017%20Application%20Security%20Report%20FINAL.pdf
[4] https://sdtimes.com/automation/stop-fighting-yesterdays-software-security-wars/

### About Us

SonicWall has been fighting the cyber-criminal industry for over 25 years, defending small, medium size businesses and enterprises worldwide. Our combination of products and partners has enabled a real-time cyber defense solution tuned to the specific needs of the more than 500,000 businesses in over 150 countries, so you can do more business with less fear.

If you have any questions regarding your potential use of this material, contact:

SonicWall Inc.
1033 McCarthy Boulevard
Milpitas, CA 95035

Refer to our website for additional information.
**www.sonicwall.com**