# EXECUTIVE BRIEF: LA NECESSITÀ DI SICUREZZA DELLE APPLICAZIONI WEB

**Capire i rischi intrinseci dei siti Web aziendali**


## Abstract

Le applicazioni Web sono più indispensabili che mai per le aziende, ma comportano anche dei rischi significativi. Questo brief esplora i potenziali exploit e gli attacchi basati sul Web che l'IT si trova a dover affrontare, tra cui:

- Iniezione di codice/inclusione di codice remoto
- Vulnerabilità cross-site scripting (XSS)
- Hijacking della sessione Web
- Autenticazione e autorizzazione insufficienti


## Introduzione

Nel mondo odierno, incentrato sulle applicazioni, le applicazioni Web sono un elemento chiave per la maggior parte delle organizzazioni che si trovano a competere in un ambiente di business digitale a livello globale. Ciò include il branding, la pubblicità, la competitività e l'acquisizione dei clienti, per nominare solo alcuni aspetti. Le imprese, le istituzioni e i governi sono costantemente sotto pressione per innovare e sviluppare applicazioni Web utili a soddisfare l'appetito insaziabile degli utenti alla ricerca di un accesso istantaneo a informazioni, servizi e assistenza.

### La crescita esplosiva delle applicazioni Web nel mondo degli affari

Gli utenti di Internet rappresentano ormai oltre la metà[1] della popolazione mondiale. Oggi il 93%[1] di tutti gli utenti di Internet è online e probabilmente rimane online più a lungo utilizzando i propri dispositivi mobili anziché i computer. Inoltre, con l'avvento dell'Internet of Things (IoT), si sono aggiunte decine di miliardi[2] di dispositivi già connessi, che comunicano e scambiano dati tramite applicazioni Web e mobili: TV, dispositivi indossabili digitali, automobili, console di gioco, distributori automatici e ogni tipo di dispositivi intelligenti.

Di conseguenza, gli sforzi delle organizzazioni sono rivolti ad offrire il meglio in termini di esperienza e coinvolgimento del servizio con diversi tipi di applicazioni Web interattive e applicazioni mobili user-friendly. Le applicazioni Web diventano

quindi più indispensabili che mai e le aziende devono occuparsi di mantenerle tutte online e sicure.

### Problemi di sicurezza intrinseca

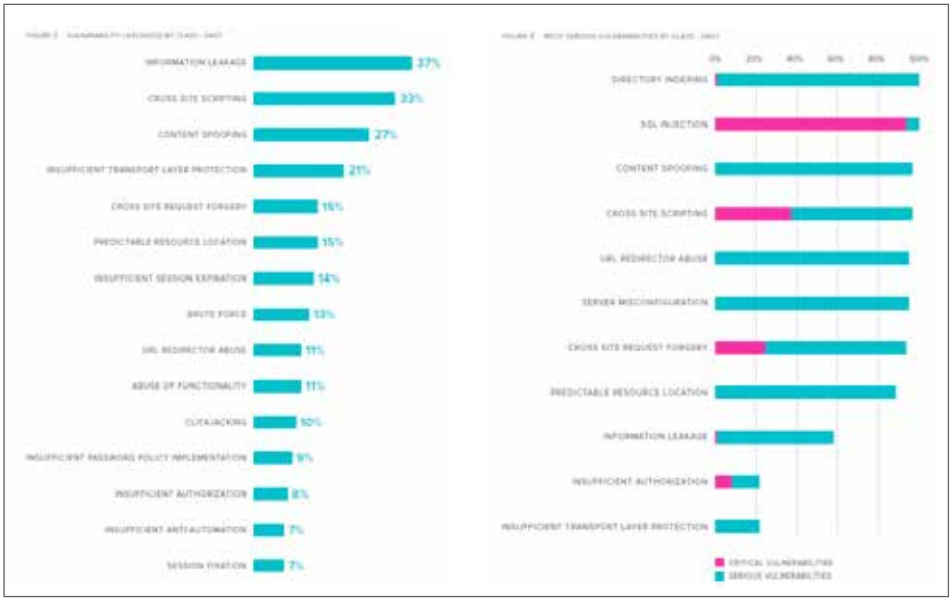
Tuttavia, ogni volta che il software di un'applicazione Web viene distribuito insieme ai dati a cui deve accedere, esso diventa un rischio per la sicurezza. Questo accade perché si tratta di un potenziale punto di ingresso per coloro che intendono sferrare un attacco per rubare tali dati oppure ottenere l'accesso a parti più sensibili della rete. Ogni applicazione Web implementata espone le organizzazioni a un ventaglio molto ampio di potenziali exploit e attacchi basati sul Web.

Un recente rapporto[3] afferma che quasi il 50% delle applicazioni Web è sempre vulnerabile durante tutto l'anno. Questi difetti dannosi includono perdita di informazioni (37%), *cross-site scripting* (33%), spoofing dei contenuti (27%), protezione insufficiente del livello di trasporto (21%) e *cross-site request forgery* (15%). In termini di criticità dell'impatto sull'azienda, la *SQL injection* si classifica come la vulnerabilità più grave, seguita dal *cross-site scripting* (XSS), dal *cross-site request forgery* (XSFR) e dall'autorizzazione insufficiente.

Questi risultati indicano che le applicazioni Web continuano a riscontrare gravi problemi di qualità del codice sorgente e problematiche di sicurezza. A quanto pare, i team di sviluppo Web non hanno ancora integrato completamente le pratiche di sicurezza necessarie nello sviluppo del loro codice. Secondo Gartner[4], «Gli sviluppatori continueranno a sviluppare codice non sicuro, e non c'è nulla che possano fare al riguardo. È una battaglia persa contro gli hacker».

La scarsa qualità dei processi di sviluppo Web, unita a patch di sicurezza inadeguate, mette a rischio i dati di compliance. Di conseguenza, le aziende non riescono a rispettare i controlli di sicurezza imposti dalle normative, come PCI, HIPPA e GDRP. Le vulnerabilità del software vengono regolarmente segnalate e sfruttate in applicazioni come Content Management System (CMS), forum e portali utilizzati da organizzazioni di ogni dimensione e da tutti i settori.

Ad aggravamento ulteriormente questo problema vi è l'uso di molti protocolli nelle applicazioni Web, come HTTP(S), JSON, XML e SOAP, e la natura illimitata e aperta dell'interfaccia utente (UI). Inoltre, le organizzazioni mettono a rischio le proprie applicazioni Web nell'attesa che gli sviluppatori di software interni e/o di terze parti correggano questi sistemi.




### Scenari di attacco

Come esempio è possibile esaminare un tipico modulo Web progettato utilizzando un popolare linguaggio di sviluppo Web, come JavaScript o PHP.

Questo modulo accetta vari parametri per le applicazioni Web al fine di elaborare le informazioni raccolte. Se l'applicazione non dispone di misure di sicurezza, come il parsing e la convalida dei dati immessi, gli utenti malintenzionati possono potenzialmente sfruttare l'applicazione e compromettere il servizio pubblicando contenuti arbitrari nel modulo.

In questo scenario, è possibile che una o più vulnerabilità delle comuni applicazioni PHP consentano agli autori degli attacchi di includere il proprio codice nell'applicazione Web di destinazione. In genere, questa situazione è nota come un tipo di attacco di inclusione di codice locale o remoto.

Oggi i tipici server Web ospitano più applicazioni Web su un singolo host e sono accessibili tramite un'unica porta (porta 80 per HTTP e 443 per HTTPS), andando a creare una vasta superficie di attacco che le organizzazioni devono difendere.

## Conclusione

Le aziende non possono né dipendere dal proprio team di sviluppo né fare affidamento su di esso per presentare applicazioni Web impeccabili. Con i tentativi di attacchi Web che possono variare da centinaia di migliaia fino addirittura a milioni nel corso di un anno, gli amministratori IT devono farsi carico personalmente delle questioni legate alla sicurezza.

**Per saperne di più.** Leggete il nostro Brief sulle soluzioni: «Le migliori pratiche per Web Application Firewall» oppure visitate il sito 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/

**Informazioni su SonicWall**

Da oltre 25 anni SonicWall combatte il crimine informatico, proteggendo piccole, medie e grandi imprese in ogni parte del mondo. La nostra combinazione di prodotti e partner ha permesso di realizzare una soluzione di difesa informatica in tempo reale ottimizzata per le specifiche esigenze di oltre 500.000 aziende internazionali in più di 150 paesi, per consentire loro di fare più affari con maggior sicurezza.

Per qualsiasi domanda sul potenziale utilizzo di questo materiale, contattare:

SonicWall Inc.
1033 McCarthy Boulevard
Milpitas, CA 95035

Per maggiori informazioni consultare il nostro sito web.
www.sonicwall.com