

SALOTTO WEB

Come sviluppare Web app sicure

Mai come oggi la sicurezza delle applicazioni Web deve essere in cima alle preoccupazioni degli sviluppatori. La diffusione dei cosiddetti servizi 2.0, veri e propri software che vengono eseguiti direttamente nel browser, ha da un lato ampliato a dismisura il numero delle informazioni che siamo abituati a salvare e gestire online, dall'altro ha aperto le porte a metodi di programmazioni agili e veloci che devono fare i conti con diverse e più ampi problemi di sicurezza. Alle vecchie vulnerabilità, quelle che eravamo abituati a conoscere nella programmazione 1.0, se ne sono aggiunte di nuove e rimanere sempre aggiornati sui pericoli e sulle tecniche di programmazione sicura è un imperativo cui non deve sfuggire nessuno. Proprio per questo motivo abbiamo, in questo numero di Salotto Web, ospitato le esperte opinioni di tre consulenti informatici. A loro abbiamo chiesto di fare il punto della situazione e di dare qualche consiglio pratico a chi volesse, oggi, progettare un'applicazione sicura.

La prima domanda può sembrare banale, ma ci è stata utile a mettere a fuoco il problema che vogliamo trattare. Oggi le applicazioni Web, fa presente uno dei nostri ospiti, "accedono ai dati aziendali, gestiscono informazioni, elaborano modelli e logiche business, espongono servizi e presentano i risultati all'utente". La criticità di questi strumenti non solo incide notevolmente sulle informazioni che vengono gestite, ma potrebbero offrire un "rischio concreto di perdite economiche e d'immagine". Gli attacchi cui uno sviluppatore dovrebbe prestare attenzione sono decine. Il problema, dice un nostro ospite, va ribaltato: non si deve pensare agli attacchi, ma alle vulnerabilità. Ogni errore di programmazione può infatti offrire una breccia per diversi tipi di attacchi. E, allora, come fare a proteggere le nostre applicazioni? Lasciamo a voi la lettura degli utili consigli pratici.

Perché è importante la sicurezza in un'applicazione Web?



Luca Carettoni

Si occupa di sicurezza delle applicazioni. È relatore in tema di Information Security ai principali eventi Italiani ed internazionali (www.ikkisoft.com)

I vantaggi introdotti dalle applicazioni web sono ormai evidenti a tutti. Per loro stessa natura, le applicazioni online sono accessibili ad utenti generici tramite un canale tendenzialmente insicuro. È ormai chiaro che, all'aumentare dell'interesse legittimo nei confronti di queste tecnologie, stiamo di pari passo assistendo ad un progressivo aumento di abusi (attacchi informatici, frodi online, defacement). Per attività commerciali, così come per il singolo cittadino, subire un attacco informatico può significare un rischio concreto di perdite economiche e d'immagine. Se consideriamo poi le applicazioni di nuova generazione, sempre più flessibili ed integrate, garantire la confidenzialità dei dati e l'integrità delle informazioni non è un compito semplice.

Quali sono i principali attacchi cui uno sviluppatore dovrebbe prestare attenzione?

Ogni singolo componente utilizzato nello sviluppo di applicazioni web può diventare un potenziale target e, considerate le diverse tecnologie utilizzate, risulta difficile definire una principale forma di attacco. Volendo guardare la situazione negli ultimi anni, sono numerosi i casi di abuso tramite SQL Injection. La possibilità di inserire istruzioni SQL arbitrarie viene spesso sfruttata da aggressori remoti per modificare le informazioni contenute nei database e, in alcuni casi, prendere il controllo completo del database server. Sebbene questa modalità di attacco sia sfortunatamente popolare, è solamente una delle possibili vulnerabilità che affliggono le applicazioni online. Per avere un'idea di tutti i possibili vettori, suggerisco al lettore di consultare il sito web di OWASP (www.owasp.org) ed in particolare la OWASP Testing Guide.

Quali consigli pratici potresti dare per sviluppare applicazioni Web sicure?

Conoscere e comprendere le principali minacce online è il primo passo per proteggere le applicazioni web. In secondo luogo è necessario imparare le fondamentali linee guida per lo sviluppo sicuro, in maniera da sfruttare tutti i possibili accorgimenti tecnici al fine di evitare spiacevoli situazioni. In quest'ottica, Internet non rappresenta solo una minaccia ma può diventare lo strumento principale per aggiornarsi sui nuovi rischi e sulle nuove soluzioni di difesa. Come già accennato, il sito della comunità OWASP (Open Web Application Security Project) rappresenta un importante riferimento del settore. Diversi esperti contribuiscono su base volontaria alla realizzazione di documenti, tool ed eventi specifici per promuovere la sicurezza. Come suggerisce Mark Curphey, noto esperto di sicurezza, solo utilizzando il meglio della tecnologia, ottimi processi, grande conoscenza e persone competenti è possibile vincere la sfida della sicurezza nel mondo web.