Introduzione

Soltanto quindici anni fa il Web era semplice e poco importante: uno strano meccanismo che consentiva a un gruppetto di studenti, e ad alcune persone asociali, che passavano il tempo nei seminterrati, di visitare le rispettive home page dedicate a scienze, animali o poesia. Oggi il Web è la piattaforma d'elezione per scrivere applicazioni interattive complesse (dai client di posta agli editor di immagini, fino ai giochi per computer) e un mezzo che raggiunge centinaia di milioni di utenti in tutto il mondo. È anche uno strumento essenziale nel commercio, tanto importante che secondo alcuni avrebbe causato una recessione quando scoppiò la bolla delle dot-com nel 2001.

Questa progressione dall'oscurità alla diffusione ubiquitaria è stata incredibilmente rapida, anche per gli standard a cui siamo ormai abituati nell'era dell'informazione, e la velocità di ascesa ha portato con sé un problema inatteso. I difetti di progettazione e le carenze di implementazione del World Wide Web sono indicatori di una tecnologia che non ha mai aspirato a raggiungere il suo stato attuale e che non ha mai avuto la possibilità di fare una pausa e riflettere sugli errori compiuti. I problemi che ne sono scaturiti si sono presto rivelati come minacce tra le più significative e diffuse per la sicurezza dei dati. Ci si è resi conto che gli standard di progettazione del protocollo che si potrebbero applicare a una pagina in testo nero su sfondo grigio piena di criceti danzanti non sono necessariamente gli stessi adatti per un negozio online che elabora milioni di transazioni di carte di credito ogni anno.

Dando uno sguardo all'ultimo decennio, risulta difficile non manifestare almeno un lieve disappunto: quasi tutte le applicazioni online degne di nota create finora hanno dovuto pagare un prezzo per le scorciatoie che si è scelto di prendere nelle fasi iniziali del Web. Il sito `xssed.com`, che segue un insieme ristretto di problemi di sicurezza legati al Web, ha messo insieme circa 50.000 record in circa tre anni di attività. Eppure i produttori di browser sono imperturbabili, e la stessa comunità della sicurezza non ha fornito molti spunti o consigli sul modo di affrontare una situazione così compromessa. Invece, molti esperti di sicurezza passano il loro tempo a costruire tassonomie di vulnerabilità bizantine e a grattarsi il capo pensando alle possibili cause di tutto quel caos.

Parte del problema sta nel fatto che gli esperti sono stati per lungo tempo insensibili a tutto il clamore fatto sulla sicurezza del Web, incapaci di comprendere di che cosa si trattasse. Sono stati veloci a etichettare i problemi di sicurezza del Web come manifestazioni banali del *confused deputy problem* o di qualche altra bella etichetta descritta in una rivista

di settore tre decenni prima. E perché dovrebbero preoccuparsi della sicurezza del Web, comunque? Qual è l'impatto di un commento osceno inserito in una noiosa home page dedicata agli animali, rispetto alla gravità di un difetto che porta a compromettere un sistema nel modo tradizionale?

> **NOTA**
>
> Il *confused deputy problem*, letteralmente "problema del deputato confuso", è un concetto generico utilizzato nel campo della sicurezza delle informazioni per riferirsi a un'ampia categoria di difetti di progettazione o di implementazione. Il termine descrive qualsiasi vettore che consenta a un aggressore di indurre un programma ad abusare di una "autorità" (privilegi di accesso) per manipolare una risorsa in maniera non corrispondente alle proprie intenzioni – ma che presumibilmente va a vantaggio dell'aggressore, comunque sia definito tale vantaggio. Il termine "confused deputy" è pronunciato spesso dagli studiosi di sicurezza in ambienti accademici, ma poiché praticamente tutti i problemi di sicurezza del mondo reale potrebbero rientrare in questa categoria, se considerati a un certo livello di astrazione, questo termine è quasi privo di significato.

Guardando i fatti in retrospettiva, sono abbastanza sicuro che la maggior parte di noi si sta mordendo la lingua. Non solo il Web è diventato molto più di quanto ci si aspettava in origine, ma non siamo stati in grado di prestare attenzione ad alcune caratteristiche fondamentali che vanno ben oltre il dominio del nostro controllo. Dopo tutto, anche le applicazioni web meglio progettate e ben controllate hanno molti più problemi, e più spesso, delle rispettive controparti che non utilizzano il Web.
Abbiamo combinato un bel caos, ed è giunta l'ora del ravvedimento. Con questo spirito, il libro cerca di fare un passo in avanti verso una situazione di normalità, ed è forse la prima pubblicazione a presentare un'analisi sistematica ed esauriente dello stato attuale delle cose nel campo della sicurezza delle applicazioni web. Nel fare questo, intende fare luce sull'unicità delle sfide che tutti noi – ingegneri della sicurezza, sviluppatori web e utenti – dobbiamo affrontare ogni giorno.
La struttura del libro è centrata sull'esame di alcuni dei più importanti elementi di base dei browser e di vari argomenti legati alla sicurezza derivati da questa trattazione. Ho scelto questo approccio ritenendolo più informativo e intuitivo rispetto a una semplice enumerazione degli argomenti realizzata utilizzando una tassonomia scelta in modo arbitrario (pratica adottata in molti altri libri che trattano di sicurezza dell'informazione). Spero, inoltre, che questo approccio renderà il testo di più agevole lettura.
Per i lettori in cerca di risposte rapide, ho deciso di inserire al termine di molti capitoli dei promemoria in cui sono elencati e brevemente descritti alcuni approcci per affrontare i più comuni problemi che si incontrano nella progettazione di applicazioni web. Inoltre, l'ultimo capitolo presenta una rapida panoramica delle vulnerabilità di implementazione ben note che si possono incontrare.

Ringraziamenti

Molte parti di questo libro nascono dalle ricerche svolte per il *Browser Security Handbook* di Google, un wiki tecnico che ho avviato nel 2008 e rilasciato al pubblico sotto licenza Creative Commons. Potete trovare il documento originale online presso `http://code.google.com/p/browsersec/`.

Sono fortunato a lavorare in un'azienda che mi ha consentito di perseguire questo progetto, e felice di lavorare con tanti colleghi di talento che mi hanno fornito eccellenti stimoli per rendere *Browser Security Handbook* ancora più utile e accurato. Ringrazio in particolare Filipe Almeida, Drew Hintz, Marius Schilder e Parisa Tabriz per il loro supporto.

Sono orgoglioso di stare sulle spalle di alcuni giganti. Questo libro deve molto alle ricerche sulla sicurezza dei browser svolte dai membri della comunità di sicurezza dell'informazione. Un ringraziamento speciale va a Adam Barth, Collin Jackson, Chris Evans, Jesse Ruderman, Billy Rios ed Eduardo Vela Nava per averci aiutato a progredire nella conoscenza di questo campo.

Grazie a tutti voi – e continuate così.