Prefazione

Ho violato praticamente ogni cosa che era possibile violare, in un modo o nell'altro. Dal mio primo attacco (autorizzato, ovviamente) alla password root di un collega amministratore di sistema (nel lontano anno 1989), al controllo di una pompa da insulina, cui ho fatto espellere tutta la carica durante il mio keynote all'RSA 2012, il mio scopo è sempre stato quello di mostrare il mondo dal punto di vista del nostro grande avversario: come pensa e opera un hacker. Dopotutto, la conoscenza è l'ultimo baluardo di speranza che abbiamo per prevenire gli attacchi ai nostri computer.

Quando, nel 1999, ho scritto il mio primo libro, *Hacking Exposed: Network Secrets and Solutions*, sapevo quanto fosse importante per gli amministratori leggere contenuti riguardanti i loro avversari. Così ho scritto rapidamente uno dei primi libri sull'applicazione delle tecniche di hacking al mondo di Internet: *Web Hacking: Attacks and Defense*, pubblicato nel 2002. In quel libro, i miei coautori e io abbiamo utilizzato la stessa formula prescrittiva per educare i "difensori" e insegnare loro a prevenire gli attacchi alle loro proprietà web. Allora non sapevamo quanto sarebbero stati importanti gli sviluppatori di software per il successo o il fallimento degli attacchi. In poche parole, *il 100% degli attacchi riguarda il codice*.

Ogni singolo elemento di Internet funziona grazie al software. Dai router e dagli switch di rete ai server e agli endpoint fino alle tecnologie di controllo industriale, tutto ciò che utilizziamo per condividere, comunicare e diffondere informazioni conta sul codice. Quando viene rilevata una vulnerabilità, alla fine viene scovata nel codice sorgente. In questo libro, Malcolm fornisce esempi reali di attacchi riusciti e mostra come evitare di diventare la prossima vittima.

Sono due i grandi problemi del codice che causano falle nella sicurezza: la presenza di una falla e la mancanza di funzionalità di sicurezza nel codice atte a prevenire tale falla. Queste condizioni si combinano per causare il 100% degli attacchi; questo significa che solo gli sviluppatori possono prevenire gli attacchi, risolvendoli alla radice. Ogni altro livello è semplicemente una sorta di cortina fumogena: "Solo tu puoi prevenire gli attacchi!" è il grido di battaglia degli sviluppatori di tutto il mondo.

L'unico modo con il quale noi difensori possiamo battere i nostri avversari una volta per tutte consiste nel risolvere il problema alla radice: nel codice sorgente. Gli sviluppatori devono diventare guru della sicurezza, in grado di prevedere in che modo gli avversari potrebbero sfruttare il loro codice (o la mancanza di codice) per agire sui suoi punti

deboli. Per questo motivo, solo gli sviluppatori possono risolvere il problema della sicurezza dei computer.
Avevamo una grande necessità di poter contare su un libro come questo: semplice, intuitivo e facile da capire; scritto da sviluppatori per sviluppatori; parlando il linguaggio degli sviluppatori; offrendo consigli e assistenza in "bocconi" facilmente digeribili. Questo è esattamente ciò che ha fatto Malcolm. Non tratta solo il codice prodotto dagli sviluppatori, ma anche il codice open source. Inoltre, insegna ai programmatori a gestire le violazioni. I suoi sono passaggi pratici fondamentali per demistificare e destigmatizzare gli sviluppatori e il loro ruolo. Se intendete leggere un solo libro sulla sicurezza dei computer, ebbene questo è il libro giusto.
Web Security spiegata in modo facile consente a tutti gli sviluppatori, a tutti i livelli di preparazione, di comprendere le cause degli attacchi e di imparare a risolvere o mitigare i rischi in una base di codice. Malcolm fa chiarezza nelle acque torbide dell'hacking e dà agli sviluppatori la sicurezza necessaria per affrontare i problemi che affliggono il codice. Pertanto, *Web Security spiegata in modo facile* va considerato come un testo fondamentale sulle vulnerabilità nel codice. Ogni sviluppatore (e di conseguenza ogni essere umano) può trarre grandi benefici dalla lettura di ogni singola pagina di questo libro.

Stuart McClure, CEO di Qwiet AI,
autore e fondatore della serie di libri *Hacking Exposed*.