Prefazione

Venti o anche solo dieci anni fa, gli hacker come me venivano arrestati per aver tentato di fare del bene. Oggi veniamo assunti da alcune delle aziende più importanti del mondo. Se state ancora valutando se siete in ritardo o meno per prendere il treno della caccia ai bug, sappiate che salirete a bordo in uno dei momenti più emozionanti della storia di questo settore. La comunità sta crescendo più velocemente che mai, poiché i governi stanno iniziando a chiedere che le aziende ospitino programmi di divulgazione delle vulnerabilità. Molte aziende *Fortune 500* stanno creando questo genere di politiche e le applicazioni rivolte alla sicurezza progettate da hacker crescono ogni giorno. Il valore di un esperto umano sarà sempre vitale nella difesa contro le nuove minacce, e il mondo *ci sta riconoscendo* come chi è davvero in grado di farlo.

La cosa bella del mondo della caccia ai bug è che, a differenza del tipico lavoro dalle nove alle cinque o di un lavoro di consulenza, vi consente di partecipare da dove volete, quando volete e sul sistema che preferite. Tutto ciò di cui avete bisogno è una connessione a Internet, decente, un buon caffè (o una bevanda a scelta), un po' di curiosità e la passione per "smontare" le cose. Non solo avrete la libertà di lavorare con i vostri tempi, ma le minacce si stanno evolvendo più velocemente della velocità dell'innovazione, cosa che vi offre ampie opportunità per imparare, sviluppare le vostre capacità e diventare esperti in un nuovo ramo.

Se siete interessati ad acquisire esperienza di hacking nel mondo reale, nel mercato della caccia ai bug potete farlo, in quanto offre un numero infinito di obiettivi di proprietà di grandi aziende come Facebook, Google o Apple. Non sto dicendo che sia facile trovare una vulnerabilità nei loro siti; tuttavia, i programmi di caccia ai bug offrono la piattaforma su cui andare a caccia, e la community di caccia ai bug spinge a saperne sempre di più sui nuovi tipi di vulnerabilità, ad accrescere le abilità e a continuare a provare anche quando le cose si fanno difficili. A differenza della maggior parte dei laboratori e dei Capture the Flags, i programmi di caccia ai bug non offrono soluzioni o una vulnerabilità garantita da sfruttare. Invece, vi chiederete sempre se determinate funzionalità sono davvero vulnerabili, o se potete forzare l'applicazione o le sue funzionalità per spingerla a fare cose che non dovrebbe. Questa incertezza può essere scoraggiante, ma rende molto più interessante la caccia.

In questo libro, Vickie esplora vari tipi di vulnerabilità per migliorare la vostra comprensione dell'hacking delle applicazioni web. Tratta le competenze che vi renderanno

"cacciatori" di successo, comprese analisi dettagliate su come scegliere il programma giusto, eseguire ricognizioni adeguate e scrivere report efficaci. Fornisce spiegazioni per condurre specifici attacchi come *Cross-Site Scripting*, *SQL Injection*, *Template Injection* e quasi tutte le altre tecniche di cui avete bisogno per riuscire nel vostro intento. Successivamente, vi porta oltre le basi delle applicazioni web e introduce argomenti come l'analisi del codice, l'hacking delle API, l'automazione del flusso di lavoro e il fuzzing. Per chiunque sia disposto a mettersi al lavoro, *Cacciatori di bug* offre tutte le basi necessarie.

Ben Sadeghipour
Hacker, creatore di contenuti e responsabile della formazione hacker presso HackerOne