Introduzione

Ricordo ancora la prima volta che ho individuato una vulnerabilità ad alto impatto. Avevo già individuato alcuni bug a basso impatto nell'applicazione che stavo sottoponendo a test, tra cui un CSRF, un IDOR e alcune fughe di informazioni. Alla fine, sono riuscita a usarli insieme per un'acquisizione completa di ogni account del sito web: avrei potuto accedere come chiunque, leggere i dati di chiunque e modificarli come volevo. Per un istante, mi sono sentita come se avessi dei superpoteri.

Ho segnalato il problema all'azienda, che ha prontamente risolto la vulnerabilità. Gli hacker sono probabilmente la cosa più vicina ai supereroi che ho incontrato nel mondo reale. Superano i limiti del software con le loro abilità, per fare in modo che le applicazioni facciano molto di più di quanto era inizialmente previsto; è questo ciò che amo dell'hacking delle applicazioni web: bisogna pensare in modo creativo, mettersi alla prova e fare più di quello che sembra possibile.

Inoltre, come i supereroi, gli hacker etici aiutano a mantenere al sicuro la società. Nei soli Stati Uniti, ogni anno si verificano migliaia di violazioni dei dati. Scoprendo le vulnerabilità e i modi in cui si verificano, potete utilizzare le vostre conoscenze a fin di bene per prevenire gli attacchi, proteggere le applicazioni e gli utenti e rendere Internet un luogo più sicuro.

Non molto tempo fa, l'hacking e la sperimentazione con le applicazioni web erano attività illegali. Oggi, grazie ai programmi di caccia ai bug, potete eseguire hacking legalmente; le aziende istituiscono programmi di caccia ai bug per premiare i ricercatori in grado di trovare le vulnerabilità delle loro applicazioni. *Cacciatori di bug* vi insegna a eseguire l'hacking di applicazioni web e a farlo legalmente, partecipando a questi programmi. Imparerete a navigare nei programmi di caccia ai bug, a eseguire ricognizioni su un target e a identificare e sfruttare le vulnerabilità.

A chi è rivolto questo libro

Questo libro aiuterà chiunque a imparare da zero l'hacking del Web e la caccia ai bug. Potete essere studenti che cercano di entrare nel campo della sicurezza web, sviluppatori web che desiderano capire il vero significato della sicurezza di un sito web o hacker esperti che vogliono imparare ad attaccare le applicazioni web. Se siete curiosi di conoscere l'hacking web e la sicurezza web, questo libro è per voi.

Non è necessario alcun background tecnico per leggere e padroneggiare il materiale contenuto in questo libro. Tuttavia, è bene conoscere almeno le basi della programmazione. Sebbene questo libro sia rivolto anche ai principianti, gli hacker esperti potrebbero trovarlo un utile riferimento. In particolare, tratto alcune tecniche avanzate e presento molti suggerimenti e trucchi utili che ho imparato lungo il cammino.

Che cosa troverete in questo libro

Cacciatori di bug tratta tutto ciò di cui avete bisogno per iniziare a eseguire l'hacking di applicazioni web e a partecipare a programmi di caccia ai bug. Questo libro è suddiviso in quattro parti.

- *Parte I – Il settore della caccia ai bug.* La prima parte del libro si concentra sul settore della caccia ai bug. Il Capitolo 1 tratta i vari tipi di programmi per la caccia ai bug e aiuta a sceglierne uno adatto ai vostri interessi e al vostro livello di esperienza. Il Capitolo 2 vi insegna le abilità non tecniche di cui avete bisogno per avere successo nel settore della caccia ai bug: scrivere un buon report, costruire relazioni professionali e affrontare i conflitti e le frustrazioni.
- *Parte II – Le basi*. La seconda parte del libro vi prepara all'hacking del Web e vi introduce alle tecnologie e agli strumenti di base di cui avrete bisogno per andare a caccia di bug.

  Il Capitolo 3 spiega le basi delle tecnologie Internet, introduce i meccanismi di sicurezza che incontrerete, come la gestione delle sessioni, l'autenticazione basata su token e la politica *same-origin*.

  Il Capitolo 4 spiega come impostare l'ambiente di hacking, come configurare Burp Suite e come utilizzare efficacemente i suoi moduli per intercettare il traffico e cercare i bug.

  Il Capitolo 5 descrive in dettaglio le strategie di ricognizione che potete adottare per raccogliere informazioni su un target. Include anche un'introduzione allo scripting bash e mostra come creare da zero uno strumento di ricognizione automatizzato.
- *Parte III – Vulnerabilità web.* Qui inizieremo a svolgere attività di hacking. Questa parte, il fulcro del libro, approfondisce i dettagli di specifiche vulnerabilità. Ogni capitolo è dedicato a una vulnerabilità e spiega che cosa causa tale vulnerabilità, come prevenirla e come individuarla, sfruttarla e ampliarla per ottenere il massimo impatto.

  I Capitoli da 6 a 18 discutono le vulnerabilità più comuni che potrete incontrare nelle applicazioni della vita reale: *Cross-Site Scripting* (XSS), Open Redirects, *Clickjacking*, *Cross-Site Request Forgery* (CSRF), *Insecure Direct Object References* (IDOR), *SQL Injection*, *Race Condition*, *Server-Side Request Forgery* (SSRF), Insecure Deserialization, *XML External Entity Vulnerabilities* (XXE), *Template Injection*, errori nella logica dell'applicazione e nel controllo degli accessi ed *Remote Code Execution* (RCE).

  Il Capitolo 19 si tuffa in una delle difese fondamentali di Internet, oggi: la politica *same-origin*. Imparerete a riconoscere gli errori commessi dagli sviluppatori durante la creazione di applicazioni che aggirano la politica *same-origin* e scoprirete come gli hacker possono sfruttare questi errori.

Il Capitolo 20 illustra i modi più comuni in cui le applicazioni implementano le funzionalità Single Sign-On, i potenziali punti deboli di ciascun metodo e come è possibile sfruttarli.

Infine, il Capitolo 21 discute diversi modi per estrarre informazioni sensibili da un'applicazione web.

- *Parte IV – Tecniche avanzate.* La parte finale del libro contiene tecniche rivolte all'hacker esperto. Questa parte vi aiuterà ad affinare le vostre capacità, una volta che avrete compreso le nozioni di base trattate nella Parte III.

  Il Capitolo 22 vi insegna a identificare le vulnerabilità nel codice sorgente. Avrete anche la possibilità di esercitarvi a valutare alcuni frammenti di codice.

  Il Capitolo 23 vi insegna a configurare il vostro ambiente di hacking mobile e a trovare le vulnerabilità nelle applicazioni Android.

  Il Capitolo 24 discute le API, le interfacce di programmazione delle applicazioni, una parte essenziale di molte applicazioni, oggi. Tratto i vari tipi di API e mosto come cercare le loro vulnerabilità.

  Il Capitolo 25 conclude il libro mostrandovi come cercare automaticamente le vulnerabilità utilizzando un metodo chiamato *fuzzing*. Vi eserciterete nel fuzzing di un'applicazione web con un fuzzer open source.

Buon Hacking!

Cacciatori di bug non è semplicemente un libro sulla caccia ai bug. È un manuale per aspiranti hacker, penetration tester e persone semplicemente curiose di sapere come funziona la sicurezza su Internet. Nei capitoli che leggerete scoprirete come gli hacker sfruttano i più comuni errori di programmazione per raggiungere i loro obiettivi e come potete aiutare le aziende segnalando in modo etico queste vulnerabilità tramite i loro programmi di caccia ai bug. Ricordatevi di esercitare sempre questo potere in modo responsabile. Le informazioni contenute in questo libro devono essere utilizzate esclusivamente per scopi legali. Attaccate solo sistemi per i quali avete ottenuto il permesso di agire e fate sempre estrema attenzione a quello che fate.
Buon hacking!

L'autrice

Vickie Li è una sviluppatrice e ricercatrice nel campo della sicurezza, abile nel trovare e sfruttare le vulnerabilità delle applicazioni web. Ha segnalato vulnerabilità ad aziende come Facebook, Yelp e Starbucks, e cura numerosi programmi di formazione online e blog tecnici. Potete trovarla su `https://vickieli.dev`, un blog di notizie sulla sicurezza, tecniche e scoperte recenti di caccia ai bug.

Il revisore tecnico

Aaron Guzman è coautore di *IoT Penetration Testing Cookbook* e responsabile della sicurezza dei prodotti in Cisco Meraki. Trascorre le sue giornate migliorando la sicurezza dei prodotti IoT e realizzando progetti che proteggano gli utenti dalle violazioni. Co-presidente dell'IoT Working Group di Cloud Security Alliance e revisore tecnico per diversi libri sulla sicurezza, cura anche molte iniziative open source, migliorando la consapevolezza sull'hacking nel campo IoT e sulle strategie difensive proattive nell'ambito dei progetti IoT ed Embedded Application Security di OWASP. Ha una grande esperienza come conferenziere, avendo tenuto conferenze, attività di formazione e workshop, a livello globale. Potete seguire Aaron su Twitter: *@scriptingxss.*