Premessa

Molte lune fa (beh, non è passato *molto* tempo, ma il mondo della tecnologia si muove così velocemente…), mi è stato affidato il compito di realizzare e poi curare un sistema in grado di gestire le informazioni delle carte di credito. Tali sistemi devono soddisfare gli *standard di sicurezza* PCI DSS (*Payment Card Industry Data Security Standards*), che richiedono un estenuante audit annuale per garantire il rispetto dei requisiti di sicurezza. Uno di questi requisiti consiste nel formare ogni anno il team di sviluppo sulle principali vulnerabilità del software, che potrebbero influenzare il sistema e su come proteggersi. "Giusto", ho pensato: "Dovrebbe essere semplice: Internet offre moltissime informazioni liberamente accessibili sulla sicurezza delle applicazioni web".

Ma in realtà c'è fin troppo materiale fra cui scegliere. Internet è ricco di *tantissime* informazioni sulla sicurezza delle applicazioni web: dettagliate, disorganizzate, a volte obsolete o duplicate e spesso rivolte ai professionisti della sicurezza piuttosto che ai programmatori. Volevo qualcosa di compatto e pertinente. Quali sono le cose più essenziali da sapere se potessi occupare solo un giorno del tempo di uno sviluppatore? E come potrei strutturare al meglio tali informazioni? Certamente non volevo sequestrare tutti i membri del team di sviluppo in una sala conferenze per otto ore e proporre loro presentazioni PowerPoint su informazioni che già in gran parte conoscono. Quella frustrazione mi ha portato a creare Hacksplaining.com e, infine, a scrivere questo libro.

La sicurezza delle applicazioni web è un argomento curioso, in quanto ogni programmatore (anche appena uscito da un corso o con una laurea fresca fresca in mano) ne avrà una discreta conoscenza, ma tendiamo a ritenere (giustamente) che dovremmo saperne un po' di più. Ma fare ricerche sul Web può sembrare come entrare in una biblioteca disorganizzata e raccogliere testi a caso, sperando di ottenere qualche buon indizio. Inoltre, a nessuno piace andare dal capo e ammettere di avere lacune nelle proprie conoscenze, quindi tendiamo a essere un po' insicuri riguardo a ciò che potremmo non sapere.

Con questo libro ho cercato di seguire alcune regole.

- In queste pagine trovate tutto ciò che dovete sapere sulla sicurezza delle applicazioni web.
- Tutto quello che leggerete è utile.
- Ho cercato di non lasciare troppe domande senza risposta al lettore curioso. I suggerimenti sulla sicurezza che trovate in Internet tendono a essere scritti così: "Basta usare i token anti-snarfing per proteggersi dalla vulnerabilità snarf-warbling, altrimenti

un hacker snarferà le vostre trasmissioni". Quando leggo questo tipo di consigli, comincio subito a chiedermi: "Sì, ma come posso fare a snarfare le trasmissioni di qualcuno? Si può trovare lavoro come snarf-warbler?". E così mi coglie l'improvviso desiderio di sapere tutto sullo snarf warbling.

Per affrontare questa situazione, laddove la lunghezza lo consente, ho provato a mostrare gli strumenti utilizzati dagli hacker, perché:

1. conoscere questi strumenti dà un senso più reale della minaccia che rappresentano e
2. è divertente conoscerne alcuni segreti.

Gli hacker tendono a essere un po' dei prestigiatori, dotati di poteri incredibili, ma una volta che sai come funziona un trucco, scoprite che attuarlo è terribilmente banale ma la preparazione necessaria per realizzarlo è sorprendentemente impressionante. Sbirciare dietro le quinte dovrebbe dare al lettore una motivazione per approfondire quello che altrimenti potrebbe essere un argomento piuttosto arido; nel farlo acquisirà alcune informazioni utili per valutare i rischi.

Il risultato è (spero) il libro che avrei voluto leggere quando ho iniziato a lavorare come sviluppatore e che avrei approfondito come sviluppatore esperto per scacciare il sospetto di essermi perso qualche dettaglio (e probabilmente approfondirò anch'io l'argomento: essendo un programmatore di mezza età, per me questo libro è stata l'occasione per rinfrescare le mie conoscenze). Questo è certamente il libro che metterò sulla scrivania di ogni nuovo membro del mio team di sviluppo, dicendogli: "Leggi questo libro appena puoi. Se scopri che sai già tutto, questo è un ottimo segno".

Noi programmatori tendiamo a imparare dai nostri errori; dopotutto, non puoi davvero definirti uno sviluppatore esperto se non hai impedito, almeno una volta, l'uscita in produzione. Ma gli errori che riguardano la sicurezza *non sono decisamente* quel tipo di cose che vuoi imparare dall'esperienza. Se questo libro vi aiuterà a prevenire *un singolo* errore relativo alla sicurezza prima che raggiunga la fase di produzione, direi che avete fatto bene a leggerlo.