



EBook Gratuito

APPENDIMENTO

security

Free unaffiliated eBook created from
Stack Overflow contributors.

#security

Sommario

Di.....	1
Capitolo 1: Iniziare con la sicurezza	2
Osservazioni.....	2
Examples.....	2
introduzione.....	2
All'inizio.....	2
Introduzione di alto livello alla sicurezza delle informazioni.....	2
Titoli di coda	4

You can share this PDF with anyone you feel could benefit from it, downloaded the latest version from: [security](#)

It is an unofficial and free security ebook created for educational purposes. All the content is extracted from [Stack Overflow Documentation](#), which is written by many hardworking individuals at Stack Overflow. It is neither affiliated with Stack Overflow nor official security.

The content is released under Creative Commons BY-SA, and the list of contributors to each chapter are provided in the credits section at the end of this book. Images may be copyright of their respective owners unless otherwise specified. All trademarks and registered trademarks are the property of their respective company owners.

Use the content presented in this book at your own risk; it is not guaranteed to be correct nor accurate, please send your feedback and corrections to info@zzzprojects.com

Capitolo 1: Iniziare con la sicurezza

Osservazioni

Questa sezione fornisce una panoramica di cosa è la sicurezza e perché uno sviluppatore potrebbe volerlo utilizzare.

Dovrebbe anche menzionare qualsiasi argomento di grandi dimensioni all'interno della sicurezza e collegarsi agli argomenti correlati. Poiché la Documentazione per la sicurezza è nuova, potrebbe essere necessario creare versioni iniziali di tali argomenti correlati.

Examples

introduzione

La sicurezza è un campo molto generale e ampio e tocca tutti gli aspetti dello sviluppo, dell'implementazione, del supporto, tra le altre aree. Per (ISC) 2, ci sono 10 domini e include la sicurezza fisica, oltre agli aspetti "Software". L'intento della sicurezza delle informazioni è quello di proteggere la riservatezza, l'integrità e la disponibilità delle informazioni. Vari professionisti della sicurezza hanno anche aggiunto altri aspetti a questi attributi, ma in generale, questi sembrano essere i più popolari. Un altro aspetto della sicurezza è che la misura per proteggere alcune informazioni non dovrebbe costare più del valore delle informazioni protette.

All'inizio

Durante la progettazione, l'architetto dovrebbe esaminare quali parti del sistema necessitano di accesso limitato e quali parti possono essere meno protette. Ad esempio, chiunque può avere accesso in lettura alla pagina Web pubblica dell'azienda, ma solo le persone autorizzate possono modificare il contenuto.

Per aiutare con le decisioni da prendere e per individuare i punti deboli nella progettazione, è necessario creare un modello di minaccia come documentato ad esempio [in OWASP](#). Tale modello di minaccia è inestimabile quando si progetta un'applicazione sicura in quanto fa luce su diverse prospettive del sistema in fase di sviluppo, come le attività in questione, i livelli di fiducia, i punti di ingresso e i flussi di dati. In questo modo puoi facilmente individuare punti deboli e possibili scenari di attacco per la tua applicazione.

Un modello di minaccia è qualcosa che viene utilizzato anche da pentesters e hacker seri nella prima fase di un test o di un attacco: raccogliere informazioni e mettere tutto insieme per individuare possibili punti deboli.

Introduzione di alto livello alla sicurezza delle informazioni

È un istinto umano fondamentale per valutare il rischio e accettare o intraprendere qualche tipo di azione su tale rischio. Questa è l'essenza della sicurezza, che è il corpo della conoscenza che

fornisce una struttura attorno a questo istinto.

La sicurezza definisce tre concetti chiave in un paradigma triangolare: riservatezza, integrità e disponibilità (il paradigma della CIA).

Mentre è comune per la società credere che la sicurezza sia semplicemente quella di proteggere la riservatezza, come sviluppatore non c'è nulla che non rientri da qualche parte sotto la bandiera della sicurezza. Ad esempio, il codice viene scritto per aggiungere funzionalità al software (disponibilità), per mantenere le credenziali sicure (riservatezza) o per garantire che la più semplice delle funzioni produca un output coerente e corretto (integrità).

I tre concetti sono abbastanza spesso in contrasto con la loro natura. Immagina di rendere disponibili le informazioni di un'azienda tramite una extranet. Questa disponibilità apre i vettori di attacco che potrebbero compromettere la riservatezza dei dati. Allo stesso modo, un'azienda con esigenze di riservatezza onerose ostacolerà il desiderio dell'azienda di mettere i dati a disposizione di clienti e partner. O forse volevano che i dati venissero resi disponibili così velocemente lo sviluppo del sito è stato accelerato e portato a perdite di dati tra gli utenti - una mancanza di integrità dei dati.

A seguito di ciò, chiunque o qualunque cosa stia sviluppando software ha diversi valori CIA. Immagina che un sito Web di vendita al dettaglio possa valutare la disponibilità per integrità o riservatezza, mentre una banca probabilmente valuterà la riservatezza rispetto alla disponibilità e all'integrità. Ciò non vuol dire che non siano tutti valutati in ciascun caso, ma che ogni scenario abbia una diversa ponderazione di questi valori a seconda dei rischi sottostanti.

Nel mondo reale, la triade della CIA viene spesso aggiunta con fino a 3 ulteriori fattori, che costituiscono l'esadecimale di Parker: possesso o controllo, autenticità e utilità, e per i modelli transazionali, non ripudio. Quindi, come puoi vedere, non esiste un modello semplice che si adatti a tutti gli scenari.

Come sviluppatore, "buona sicurezza" riguarda il sapere il giusto equilibrio per ciò che viene protetto e come proteggerlo, e questo è molto diverso in base al tipo di dati coinvolti e ai problemi che il software sta risolvendo.

Leggi Iniziare con la sicurezza online: <https://riptutorial.com/it/security/topic/4900/iniziare-con-la-sicurezza>

Titoli di coda

S. No	Capitoli	Contributors
1	Iniziare con la sicurezza	Community , Frank , jotap , Rory Alsop , SRao