FREE eBook

LEARNING security

Free unaffiliated eBook created from
Stack Overflow contributors.

#security

Table of Contents

About

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.

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

Chapter 1: Getting started with security

Remarks

This section provides an overview of what security is, and why a developer might want to use it.

It should also mention any large subjects within security, and link out to the related topics. Since the Documentation for security is new, you may need to create initial versions of those related topics.

Examples

Introduction

Security is a very general, broad field, and touches every aspect of development, deployment, support, among other areas. Per the (ISC)2, there are 10 domains, and include Physical security, in addition to the "Software" aspects. The intent of information security is to protect the confidentiality, integrity and availability of information. Various security professionals also have added other aspects to these attributes, but in general, these appear to be the most popular. Another aspect of security is that the measure to protect some piece of information should not cost more than the value of the information being protected.

At the beginning

During design, the architect should look at what parts of the system need restricted access, and which parts can be less protected. For example, everyone can have read access to the public web page of the company, but only authorized individuals can edit the content.

To help with the decisions to be taken and to detect weaknesses in the design a threat model should be created as documented for example here at OWASP. Such a threat model is invaluable when designing a secure application as it sheds a light on different perspectives of the system under development, like the assets in question, trust levels, entry points and data flows. So you can easily spot weaknesses and possible attack scenarios for your application.

A threat model is something also used by serious pentesters and hackers in the first phase of a test or attack: collecting information and putting it all together to detect possible weaknesses.

High Level Introduction to Information Security

It is a basic human instinct to assess risk and to accept or take some kind of action on that risk. This is the essence of security, which is the body of knowledge that provides a framework around this instinct.

Security defines three key concepts in a triangular paradigm - Confidentiality, Integrity, and Availability (The CIA paradigm).

While it is common for society to believe that security is simply about protecting confidentiality, as a developer there is nothing done that does not fall somewhere under the banner of security. For example, code is written to add features to software (availability), to keep credentials safe (confidentiality), or to ensure that the simplest of functions produces a consistent and correct output (integrity).

The three concepts are quite often at odds by their nature. Imagine making a company's information available via an extranet. This availability opens up attack vectors that could compromise the confidentiality of the data. Similarly, a company with onerous confidentiality demands will hamper the company's desire to make data available to customers and partners. Or perhaps they wanted the data to be made available so fast the development of the site was rushed and led to data leaks between users - a lack of data integrity.

Following on from this, whoever or whatever is having software developed has different CIA values. Imagine that a retail website may value availability over integrity or confidentiality, while a bank will likely value confidentiality over availability and integrity. This is not to say that all are not valued in each case, but that each scenario carries different weightings of these values depending on the underlying risks.

In the real world, the CIA triad is often added to with up to 3 further factors, making up the Parkerian hexad: Possession or Control, Authenticity and Utility, and for transactional models, Non-Repudiation. So as you can see there is no simple model that fits all scenarios.

As a developer, "good security" is about knowing the right balance for what is being protected and how to protect it, and this is vastly different based on the type of data involved and the problems the software is solving.

Read Getting started with security online: https://riptutorial.com/security/topic/4900/getting-started-with-security

Credits

S. No	Chapters	Contributors
1	Getting started with security	Community, Frank, jotap, Rory Alsop, SRao