Application Security

Marcin Zelent

May 2018

Contents

1 Introduction

One of the mandatory activities in Computer Science course at Erhvervsakademi Sjælland is an individual specialization project. In this project, student has to choose a subject, which was not presented during the lectures, research it and describe it in the synopsis.

I have chosen application security as the topic that I want to learn more about. Application security is an umbrella term for all of the measures that need to taken in order to make a secure application. That means finding, fixing and preventing security vulnerabilities.

I decided to work on this subject, because in previous semesters we have learned how to make programs, services and web applications, but we did not learn how to make them safe from exploitation. It is important, since a potential attacker could use it to gain access to the system without authorization, retrieve some sensitive data, abuse or even break the system. This could lead to some serious consequences.

2 Problem definition

During my research I am going to delve deeper into the subject of application security, its meaning, principles, importance in the modern software development, as well as practical implementation. The main question which I would like to answer is:

How to make a secure application?

In order to give an answer to it, I will first need to find solutions to the following problems:

- What is application security?
- What are the most common application security flaws and attack techniques?
- How software developers can prevent them?

3 Method

The method which I am going to use in my research consists of a few activities:

- Getting general information about application security using all of the sources available on the internet, this could include reading articles, watching videos, talks, lectures and and online courses
- Reading books related to the subject of application security
- Finding detailed descriptions and tutorials about specific attack techniques
- Trying to reproduce the attacks by creating vulnerable applications and exploiting them

4 Plan

To optimize my work and to make sure I will deliver the finishied synopsis before the deadline, I have prepared a plan which I will try to follow:

Week 18	Week 19 & 20	Week 21
Writing introduction	Doing an actual research	Writing conclusion
Defining the problem	Describing the work	Reflecting on the work
Choosing the method	Preparing examples	Putting finishing touches
Planning		

Table 1: Week plan

The first week is a project initialization phase, in which I will describe what I am going to do in the next weeks, how and why.

In the second and third week I will focus on learning, finding information and describing the results of it. I am also going to work on the practical part of this project, which is learning how to use different attack techniques and creating examples for the presentation of them.

In the last week I will look back at my work, write summary of it, as well as reflections on the research process. I will also proof read my synopsis and correct any mistakes that I find.

5 Work

5.1 What is application security?

Application security describes activities that need to be taken into consideration by a developer who creates an application which will be available to a broader group of users. Having a large userbase means that there is a risk that, among the regular users, there might be some individuals with malicious intents.

These people, usually called attackers, could try to access sensitive data stored in the database connected to the application or use functions that normally are only available for the users with special privileges. Such data could include for example a list of users, some important documents or money in a bank account. Administrator actions, like adding/removing users or changing application's settings could be an example of functionality wanted by the attackers.

In order to achieve their goals, the attackers try to find vulnerablities, unintended flaws or weaknesses in the application, and exploit them. Although the application security improved over the years, some of the most common vulnerabilities remain unchanged and include: broken authentication, broken access controls, SQL injection, cross-site scripting (XSS), information leakage and cross-site request forgery (CSRF).

When talking about application security, it usually means web application security. The reason for this is the fact that web apps are nowadays the most common form of application. Every day billions of people are searching for information using Google, browsing Facebook and watching videos on YouTube. All of these are web applications. What makes them different from regular websites is that they do not just display static content, but allow users to interact with them. Users can for example sign up, log in, write comments, upload videos. A lot of sensitive data is flowing between the user and the system. This, and being publicly available, makes them frequent targets of the attackers.

Other common targets are mobile and desktop applications, with the emphasis on the first one. Just like web apps they are usually part of a bigger system and process private data. Moreover, their security is often neglected by the developers in favor of having more features. That could make them security holes, easy gateways leading to the precious resources.

5.2 Why application security is important?

There should be no doubt about the importance of application security. There are many reasons for that.

First and most important is the risk of unwanted disclosure of sensitive data to the attackers, if the application becomes compromised. This could include names, addresses, login credentials, credit card information, bank account details, private photos and many more information about the users of the system. By breaking into the unprotected system, attackers could also gain access to company's internal data: important documents, list of employees, private keys and passwords. All this information could be useful for them in various ways. For example, it could be used to buy things or perform financial operations without the knowledge of the account owner. The data could be sold on the black market or published on the internet. It could be used to harass or black-

mail the unfortunate users. Attackers could also impersonate them and cause even more problems. It could be especially dangerous when pretending to be a corporate worker as their actions could harm the entire business.

6 Conclusion

7 Reflection

References

[1] Dafydd Stuttard, Marcus Pinto. *The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws, 2nd Edition.* John Wiley & Sons Inc, ISBN: 978-1118026472, 2011.

[2] Caroline Wong. *Learning the OWASP Top 10.* `https://lynda.com/IT-Infrastructure-tutorials/Learning-OWASP-Top-10/642483-2.html`

[3] Michael Coates. *Application Security - Understanding, Exploiting and Defending against Top Web Vulnerabilities.* `https://youtu.be/sY7pUJU8a7U`

[4] Sarah Vonnegut. *Mobile Application Security: 15 Best Practices for App Developers* `https://checkmarx.com/2015/08/19/mobile-application`