Web Apps Security (Part 1)

Security Principles, Authentication

Refer to the Security Chapter from the Textbook to answers the following questions

Note: You can find a PDF version of Ch16: Security under (Exercises > 08 SEC > Fundamentals of Web Dev - 3rd - Chapter 16 Security.pdf)

1. What are the three components of the CIA security triad? What does each one of them mean? And how important it is to web security?
2. What are the categories of security policies and how important are them to protect a system?
3. What is the difference between a threat and a vulnerability?
4. What is the difference between authentication and authorization? Give an example for each.
5. What are the type of authentication factors? What is the downside of each type?
6. Why is two-factor authentication more secure than single factor?
7. How does the secure by design principle get applied in the software development life cycle?
8. What are the three types of actor that could compromise a system? Explain in details.
9. What is security theater? Is it effective?
10. Explain the difference between HTTP Basic authentication, Form-Based authentication, HTTP token authentication and third party authentication (OAuth).

Answers:

1. The three components of the CIA security triad are:

    a. Confidentiality: Ensuring that information is not accessed by unauthorized individuals.
    b. Integrity: Ensuring that information is not altered by unauthorized individuals, and that it remains accurate and trustworthy.
    c. Availability: Ensuring that information and systems are available to authorized users when needed. This triad is fundamental to web security as

it provides a basic framework for assessing and implementing security measures.

2. Categories of security policies include:

    a. Preventive Policies: Aim to prevent security incidents.
    b. Detective Policies: Aim to detect security incidents.
    c. Corrective Policies: Aim to correct systems and processes after a security incident. These policies are crucial to protecting a system as they establish guidelines and procedures for maintaining security.

3. Difference between a threat and a vulnerability:

    a. A threat is a potential cause of an unwanted incident, which may result in harm to a system or organization.
    b. A vulnerability is a weakness which can be exploited by a threat to gain unauthorized access to a resource.

4. Difference between authentication and authorization:

    a. Authentication is the process of verifying the identity of a user or system. Example: Logging in with a username and password.
    b. Authorization is the process of verifying what specific applications, files, and data a user has access to. Example: After logging in, the user can only access the files they have permissions for.

5. Types of authentication factors and their downsides:

    a. Knowledge factors (something you know): e.g., password. Downside: Can be forgotten or guessed.
    b. Possession factors (something you have): e.g., security token. Downside: Can be lost or stolen.
    c. Inherence factors (something you are): e.g., fingerprint. Downside: Can be invasive and raise privacy concerns.

6. Why two-factor authentication is more secure:

    a. It provides an additional layer of security by requiring two different authentication factors, making it much harder for an unauthorized person to gain access.

7. Secure by design in the software development life cycle:
    a. Involves integrating security measures from the earliest stages of design and development, rather than as an afterthought, ensuring security is an integral part of the entire process.

8. Three types of actors that could compromise a system:

    a. Hackers: Individuals who seek unauthorized access to computer systems for personal gain, to cause disruption, or to challenge security measures.
    b. Insiders: Employees or contractors who misuse their access to an organization's systems.
    c. Organized Crime Groups: Groups that target systems for financial gain or to access sensitive information.

9. What is security theater?
    a. Security theater refers to security measures that make people feel more secure without actually providing tangible security benefits. It is often not effective in providing real protection and can waste resources.

10. Difference between various authentication methods:

    a. HTTP Basic Authentication: A method for an HTTP user agent to provide a user name and password when making a request. It is not secure unless used over HTTPS as credentials are only base64 encoded.

b. Form-Based Authentication: Involves the user submitting a form with their credentials. It is more flexible and can be more secure if implemented correctly and used over HTTPS.
c. HTTP Token Authentication: Utilizes a token that the server generates and the client sends with each request. It is secure and stateless, often used in modern web APIs.
d. Third-Party Authentication (OAuth): Allows users to authenticate using well-known third-party services like Google or Facebook. This delegates the authentication process to the third party, which can be more secure and convenient for the user.

🔥 Hands-On

Exercise 1: Implementing Basic Authentication

Follow the steps in this tutorial to implement basic authentication to your website. Push the code to Github.

References

- https://www.geeksforgeeks.org/basic-authentication-in-node-js-using-httpheader/
- https://www.pearson.com/en-us/subject-catalog/p/fundamentals-of-webdevelopment/P200000003214/9780136792857 -