



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).

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-http-header/>
- <https://www.pearson.com/en-us/subject-catalog/p/fundamentals-of-web-development/P200000003214/9780136792857>
-