Web Apps Security (Part 2)

Cryptography, HTTPS, Best Practices, Common Threat Vectors

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 type of cryptography addresses the problem of agreeing to a secret symmetric key?
2. What is a cryptographic one-way hash?
3. What does it mean to salt your passwords?
4. What is a Certificate Authority, and why do they matter?
5. What is a DoS attack, and how does it differ from a DDoS attack?
6. What can you do to prevent SQL injection vulnerabilities?
7. How do you defend against cross-site scripting (XSS) attacks?
8. What features does a digital signature provide?
9. What is a self-signed certificate?
10. Why are slow hashing functions like bcrypt recommended for password storage?
    What is a downgrade attack and how can you protect a site against it?

🔥 Hands-On

Exercise 1: Encrypting and decrypting a message manually

Follow this tutorial to learn how to encrypt and decrypt data using node.js. Use it to encrypt your name and submit your encrypted name to Blackboard.

Exercise 2: Bruit-force

Go to the (Web-Dev GitHub Page > Demos > 08 SEC > brute-fource.js) and explore different passwords and see how hard/easy are they to be cracked!

References

- https://www.tutorialspoint.com/encrypt-and-decrypt-data-in-nodejs
-