Dreadnought Lab – Week 02: JWT Exploitation & Auth Analysis

# 🎯 Objectives

Explore how JWTs can be decoded, modified, and abused in poorly implemented authentication systems.

# 📋 Lab Tasks

* ☐ Capture a JWT using Burp or curl.
* ☐ Decode the JWT on jwt.io and identify weaknesses (e.g., alg=none).
* ☐ Modify the token and replay it against the API to attempt privilege escalation.

# 💡 Challenge Task

☐ Use a forged JWT to access an admin endpoint or break role-based access.

# 🧠 Reflection

What design flaws made this JWT attack possible, and how should it have been secured?