PASSGATE LAB - STUDENT MANUAL

OVERVIEW

Welcome to PassGate! You are a security researcher tasked with testing a vulnerable employee portal. Your mission: find and exploit password security weaknesses to capture the flag.

STEP 1: LAB SETUP

1. Open Command Prompt
2. Navigate to the PassGate folder
3. Start the server: node server.js
4. Open http://localhost:3000 in your browser

STEP 2: INITIAL TESTING

1. Try logging in with random credentials
2. Open Developer Tools (F12)
3. Go to Network tab and check "Preserve log"
4. Submit the login form
5. Observe what happens

STEP 3: NETWORK ANALYSIS

1. In Network tab, find the POST /login request
2. Click on it and check the Response tab
3. Look carefully at the JSON response
4. What information is being exposed?

STEP 4: CREDENTIAL DISCOVERY

1. Identify the exposed base64 encoded values
2. Use CyberChef (https://gchq.github.io/CyberChef/) to decode them
3. Use "From Base64" operation in CyberChef
4. Discover the actual username and password

STEP 5: SECURITY ASSESSMENT

Document the security vulnerabilities you found:

- What makes the password weak?
- How were the credentials exposed?
- Why is base64 encoding insecure for passwords?

STEP 6: CAPTURE THE FLAG

1. Use the discovered credentials to login
2. Access the dashboard
3. Capture your flag!

LEARNING OBJECTIVES

- Understand password security weaknesses
- Learn about information leakage vulnerabilities
- Practice network traffic analysis
- Recognize why encoding ≠ security