WH40K Dreadnought-Rated Cybersecurity Curriculum

Audience: Final-year students with advanced technical background  
Duration: 12 weeks

## Week 1: API Programming & Security I

Build insecure APIs using Flask/Express. Use Postman to test routes. Intro to CORS.

## Week 2: API Programming & Security II

Secure APIs with JWT and OAuth2. Explore token expiration and session handling.

## Week 3: Advanced Web Exploitation

Explore XXE, CSRF, SSTI, and logic flaws. Use Burp Suite and OWASP Juice Shop.

## Week 4: Cloud Security (AWS)

Learn IAM roles and S3 bucket hardening. Hands-on misconfig CTF.

## Week 5: Secure Code Review

Use Semgrep and GitHub SAST tools. Find and fix insecure code.

## Week 6: Container & K8s Security

Secure Docker containers and basic Kubernetes RBAC. Use kube-hunter.

## Week 7: SIEM & Threat Hunting I

Use Splunk/Wazuh to detect brute force attacks. MITRE ATT&CK mapping.

## Week 8: SIEM & Threat Hunting II

Build dashboards and detections for DNS tunneling and exfil.

## Week 9: Offensive Scripting

Automate recon and lateral movement in Python/Bash.

## Week 10: API Pentesting & Recon

Use Kiterunner, Amass, ffuf. Bypass rate limits and tokens.

## Week 11: Purple Team Simulation

Simulate a breach with Red and Blue teams in pairs.

## Week 12: Capstone Project

Build and attack peer APIs. Submit a full report.