# Opgave 13 – Angreb på Autentificering & Tokens

## Objective

Du lærer at identificere og misbruge svagheder i token-baseret autentificering. Øvelsen fokuserer på JWT (JSON Web Tokens), herunder manipulation af payload, udnyttelse af manglende signaturvalidering.

## Information

Formålet med disse øvelser er at give en grundlæggende introduktion til, hvordan man kan udføre test af autentificering i webapplikationer, som anvender tokens efter succesfuld login.

Alle øvelser er beskrevet i Labbet. Øvelserne starter med angreb mod **crAPI** og afsluttes med en token-manipulationsøvelse i **Juice Shop**. Sørg for at læse afsnittet om prerequisites først.

> Sværhedsgraden i token-øvelserne er lidt højere end normalt. Det er helt forventeligt, at du skal prøve mere end én gang – det er en del af læringen

## Instruktioner

1. Udfør øvelsen: Introduction to JWT Tokens
2. Udfør øvelsen: Manipulating the JWT payload
3. Udfør øvelsen: Basic Attack Against Authentication Tokens in Juice Shop

## Reflect & Discuss

- Hvad gør JWT-tokens sårbare, hvis signaturen ikke valideres korrekt?
- Hvad er sikkerhedsimplikationerne ved at gemme følsom information i token payloads?
- Hvordan kan udviklere beskytte sig mod misbrug af password recovery og OTP-mekanismer?
- Hvordan kan rate limiting og MFA være effektive forsvar mod angreb på tokens?

**Etisk refleksion**: Hvordan kan du dokumentere og kommunikere fundne sårbarheder i token-håndtering uden at afsløre brugeres følsomme data?

Last update: 2025-10-26 13:39:46