Opgave 12 – Angreb på Autentificering & Password

Objective

Du lærer at identificere og udføre grundlæggende angreb mod autentificeringsmekanismer i webapplikationer. Øvelsen har fokus på dictionary attacks, brute force-metoder og password spraying – alt sammen med reel værdi for penetrationstest og sikkerhedstest af API'er og loginformularer.

Information

Formålet med disse øvelser er at give en grundlæggende introduktion til, hvordan man kan udføre test af autentificering i webapplikationer, der benytter brugernavn og adgangskoder.

Alle øvelser er beskrevet i Hacker Lab. Øvelserne starter med angreb mod **crAPI** og afsluttes med en øvelse i **Juice Shop**. Sørg for at læse afsnittet om prerequisites først.

> Øvelse 2 og 3 tager lidt tid at udføre. Start dem op og lad dem køre i baggrunden mens du arbejder videre med de andre opgaver. Alternativ kan du også udføre dem med F.eks. WFuzz

Instruktioner

1. Udfør øvelsen: Dictionary attack med Burp Suite
2. Udfør øvelsen: Dictionary attack med WFuzz
3. Udfør øvelsen: Exhaustive brute force attack med Burp Suite
4. Udfør øvelsen: Password spraying
5. Udfør øvelsen: Brute forcing OTP
6. Udfør øvelsen: Brute forcing i Juice Shop

Refleksion

- Hvilke værktøjer var mest effektive til de forskellige angrebstyper?
- Hvordan skelner man mellem en vellykket og en mislykket brute force i praksis?
- Hvordan kan applikationer mitigere disse typer angreb?

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