HACKTHEBOX

BROKEN AUTHENTICATION
CHEAT SHEET

Categories of Authentication

- Knowledge: passwords, PINs, ...
- Ownership: ID cards, TOTP
- Inherence: Biometric authentication

Brute-Force Attacks

- User Enumeration
- Brute-Forcing Passwords
- Brute-Forcing Password Reset Tokens
- Brute-Forcing 2FA Codes
- Bypassing Brute-Force Protection
  - Rate Limit: `X-Forwarded-For` HTTP Header
  - CAPTCHAs: Look for CAPTCHA solution in HTML code

Password Attacks

- Default Credentials
  - CIRT.net
  - SecLists Default Credentials
  - SCADA
- Vulnerable Password Reset
  - Guessable Security Questions
  - Username Injection in Reset Request

Authentication Bypasses

- Accessing the protected page directly
- Manipulating HTTP Parameters to access protected pages

Session Attacks

- Brute-Forcing cookies with insufficient entropy

- Session Fixation
  - Attacker obtains valid session identifier
  - Attacker coerces victim to use this session identifier (social engineering)
  - Victim authenticates to the vulnerable web application
  - Attacker knows the victim's session identifier and can hijack their account
- Improper Session Timeout
  - Sessions should expire after an appropriate time interval
  - Session validity duration depends on the web application

HTB ACADEMY CHEATSHEET