Attacking Login Forms With Burp Suite

Demo: Attacking Login Forms With Burp Suite

Attacking Login Forms With OTP Security

OTP Security

- OTP (One-Time Password) security is a two-factor authentication (2FA) method used to enhance the security of user accounts and systems.
- OTPs are temporary, single-use codes that are typically generated and sent to the user's registered device (such as a mobile phone) to verify their identity during login or transaction processes.
- The primary advantage of OTPs is that they are time-sensitive and expire quickly, making them difficult for attackers to reuse.

OTP Security Methods

- Time-Based OTPs (TOTP): TOTP is a widely used OTP method that generates codes based on a shared secret key and the current time. These codes are typically valid for a short duration, often 30 seconds.

- SMS-Based OTPs: OTPs can be sent to users via SMS messages. When users log in, they receive an OTP on their mobile phone, which they must enter to verify their identity.

- Rate Limiting and Lockout: Implement rate limiting and account lockout mechanisms to prevent brute force attacks on OTPs. Lockout accounts after a certain number of failed OTP attempts.

OTP Rate Limiting

- OTP rate limiting is a security mechanism used to prevent brute force attacks or abuse of one-time password (OTP) systems, such as those used in two-factor authentication (2FA).
- Rate limiting restricts the number of OTP verification attempts that can be made within a specified time period.
- By enforcing rate limits, organizations can reduce the risk of attackers guessing or trying out multiple OTPs in quick succession.

Demo: Attacking Login Forms With OTP Security