Spring Security

Emir Öztürk

Spring Security

- Authentication
- Authorization
- Exploits

Spring Security

- Authentication
  - Kimlik
  - Erişim isteyenin doğruluğu
- Kullanıcı adı ve şifre
  - Servlet
  - WebFlux
- Oauth 2.0
- SAML 2.0, JAAS, X509 …

Spring Security

- Şifrelerin saklanması
  - Plain text
  - Çift yönlü
  - Tek yönlü
- SHA-256
- Rainbow tables
- Salt
  - Random
  - Plaintext

Spring Security

- Authorization
  - Onaylanmış kullanıcıların izni
- Tüm düğümlerin herkese açılmaması
- Yetki farkı
- Her kişinin eriştiği veri
- User token

Spring Security

- Exploit
  - CSRF
  - Security HTTP Response Headers
  - HTTP / HTTPS requests

Spring Security

- CSRF
  - Cross site request forgery
  - Kullanıcı yetkisinin eldesi
  - Cookie
  - Kullanıcıdan habersiz gönderilen istekler
- Token kontrolü

Spring Security

- Http Headers
  - Cache Control
  - Content type
    - Content Sniffing
  - Http Strict Transport Security
    - MITM
  - Http Public Key Pinning
    - MITM
  - https://docs.spring.io/spring-security/reference/features/exploits/headers.html

Spring Security

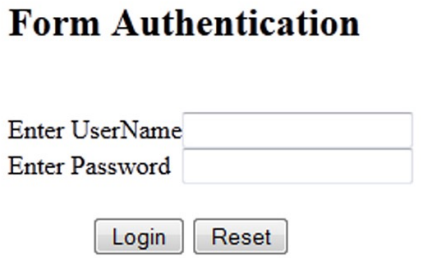
- Http Requests
  - Redirect to HTTPS
  - Strict Transport Security

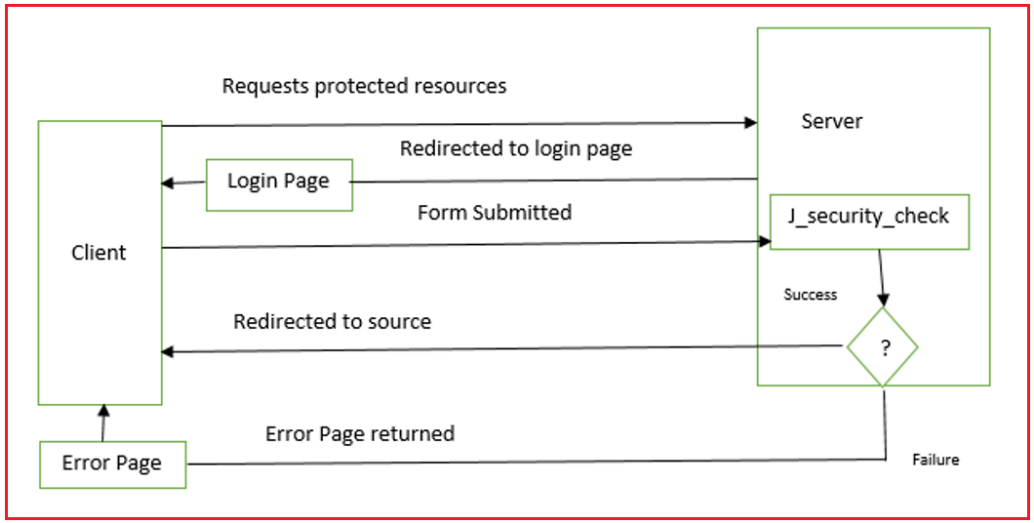
Spring Security

- Kullanıcı adı – şifreye erişim
  - Form
  - Basic Auth
  - Digest
  - Oauth 2.0

Spring Security

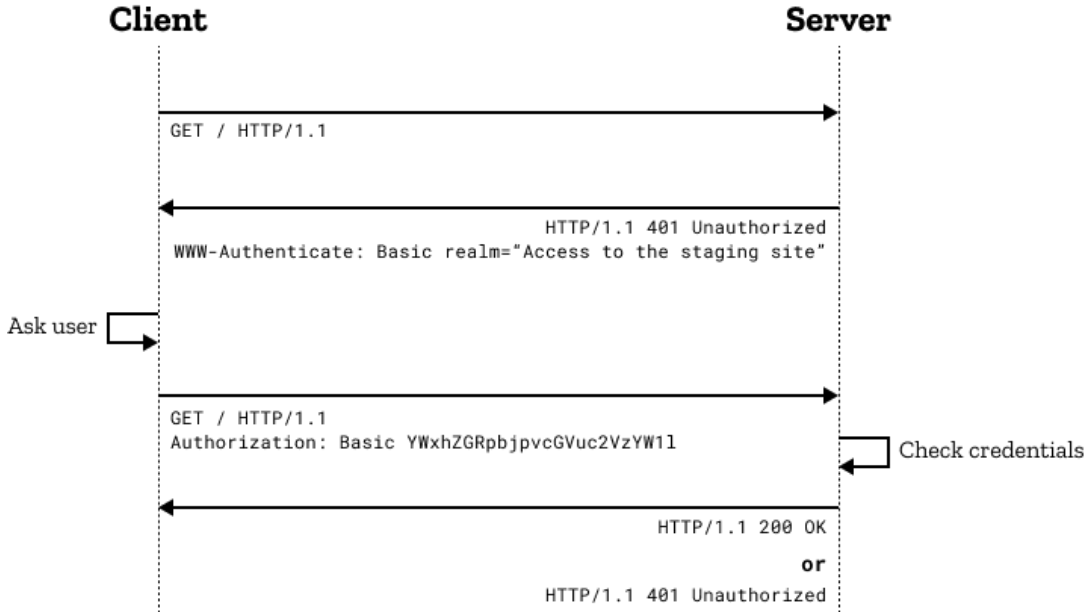
- Form
  - Kullanıcı adı şifre girişi
  - Cookie
  - Session





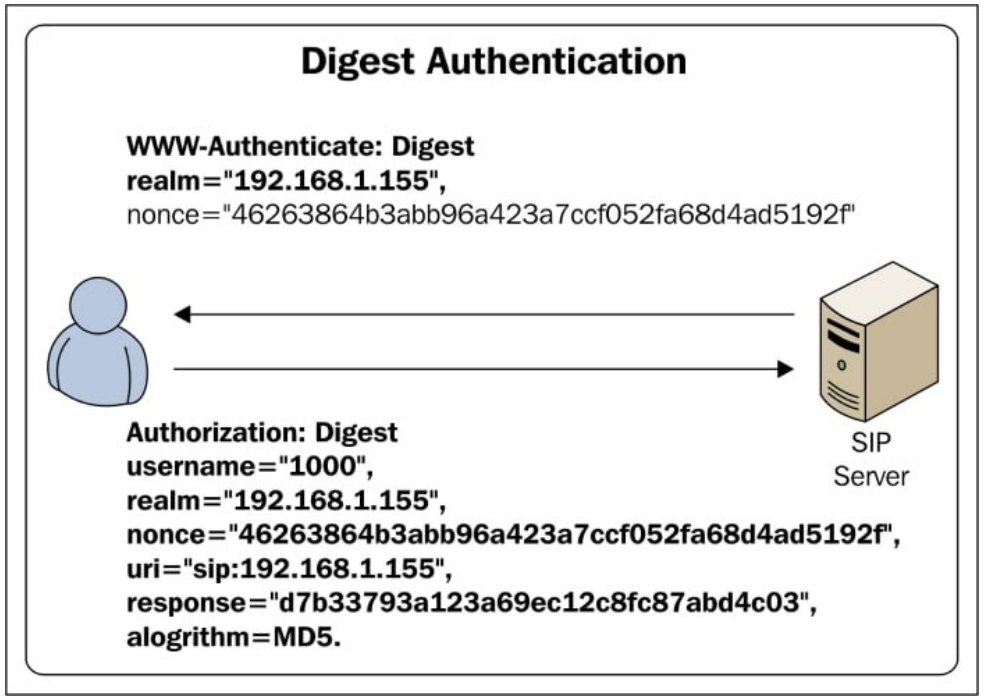
Spring Security

- Basic
  - Header ile gönderim
  - Kullanıcı adı şifre
  - Hash olabilir
  - Login düğümü



Spring Security

- Digest
  - Digest MD5 – Geri döndürülemez
  - Basic Auth Base64 – Geri döndürülebilir
  - Replay atakları için nonce



Spring Security

- OAuth 2.0
  - Open Authorization
  - Access Token
    - JWT
  - Diğer sitelerin kullanıcı kaydı