Spring Security In-Depth Cheatsheet

1. Core Concepts

- Authentication: Verifies who the user is.
- Authorization: Verifies what user is allowed to do.
- Principal: The current logged-in user.
- GrantedAuthority: A role or permission (e.g., ROLE_USER).
- UserDetails: Holds user info.
- UserDetailsService: Loads user from DB or in-memory.
- AuthenticationProvider: Validates user credentials.
- AuthenticationManager: Delegates to providers.
- SecurityContextHolder: Stores user auth info per thread.

2. Java Config Example

```
@Configuration
@EnableWebSecurity
public class SecurityConfig {
    @Bean
    public SecurityFilterChain filterChain(HttpSecurity http) throws Exception {
        http
            .authorizeHttpRequests(auth -> auth
                .requestMatchers("/admin/**").hasRole("ADMIN")
                .anyRequest().authenticated()
            )
            .formLogin(Customizer.withDefaults())
            .logout(Customizer.withDefaults())
            .csrf(csrf -> csrf.disable());
        return http.build();
    }
}
```

3. Important Annotations

- @EnableWebSecurity
- @Configuration
- @Secured("ROLE_ADMIN")
- @PreAuthorize("hasRole('USER')")
- @PostAuthorize
- @WithMockUser (for tests)

4. Custom UserDetailsService

```
@Service
public class CustomUserDetailsService implements UserDetailsService {
    @Override
    public UserDetails loadUserByUsername(String username) {
        return new User(username, password, authorities);
    }
}
```

5. AuthenticationProvider Bean

```
@Bean
public AuthenticationProvider authProvider(UserDetailsService userDetailsService) {
    DaoAuthenticationProvider provider = new DaoAuthenticationProvider();
    provider.setPasswordEncoder(new BCryptPasswordEncoder());
    provider.setUserDetailsService(userDetailsService);
    return provider;
}
```

6. Testing Example

```
@Test
@WithMockUser(roles = "USER")
public void testProtectedEndpoint() {
    mockMvc.perform(get("/user/home"))
           .andExpect(status().isOk());
}
```

7. Common Methods in HttpSecurity

- authorizeHttpRequests()
- formLogin()
- logout()
- csrf().disable()
- httpBasic()
- sessionManagement()