# Basic Authentication

Questo NON e’ il default per spring security.  
Per abilitarlo bisogna creare una classe @Configuration e @EnableWebSecurity che estende il WebSecurityConfigurerAdapter e fa override del configure sull’http (dove si puo’ scegliere quali url coprire etc).  
In questo modo si abilita la basic authentication, che NON usa sessione.  
Prevede che per ogni singola richiesta il cliente deve inviare username:password (messi sotto encoding base64).  
Tipicamente un pattern che si puo’ usare se si vuole customizzare la pagina di login (senza modificare e usare quella di spring) è abilitare la sessione sulla basic auth (così che si puo’ inviare una sola volta username:password per autenticarsi su tutte le richieste) ed esporre l’autenticazione su un solo url specifico (single point basic authentication with session).   
NB: per la basic auth username:password (in base 64) devono viaggiare come header parameter nella richiesta (user:username, password:password)

# Form Based Authentication

Questo è il default per spring boot (quando si installano le dipendenze di spring security e non si configura nulla).  
Di default il form based copre tutti gli indirizzi, ed è con sessione.  
Quando l’utente non ha il cookie di sessione che indica che è loggato, se prova ad accedere ad una risorsa, viene fatto redirect sul form di login. Se logga correttamente viene salvato in sessione il cookie e quindi avrà accesso a tutte le risorse.  
NB: per la form based auth username e pw viaggiano nel body della richiesta POST (del form).  
NB2: di default il form based auth di spring boot utilizza un csrf-token per evitare i csrf-attack.