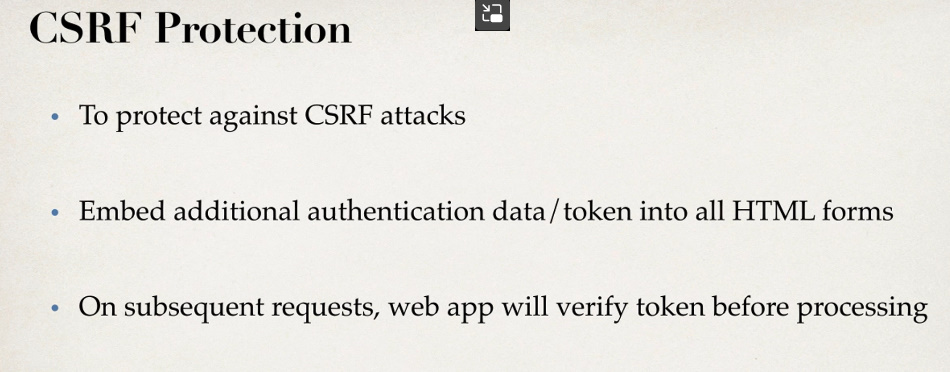
* Trebuie neaparat sa folosim <form:form> cand trimitem vreun request la Spring Security.
* Spring Security ne protejeaza impotriva la Cross Site Request Forgery(CSRF)
* Se traduce ca “falsificare cererilor pe mai multe siteuri”

**CSRF**

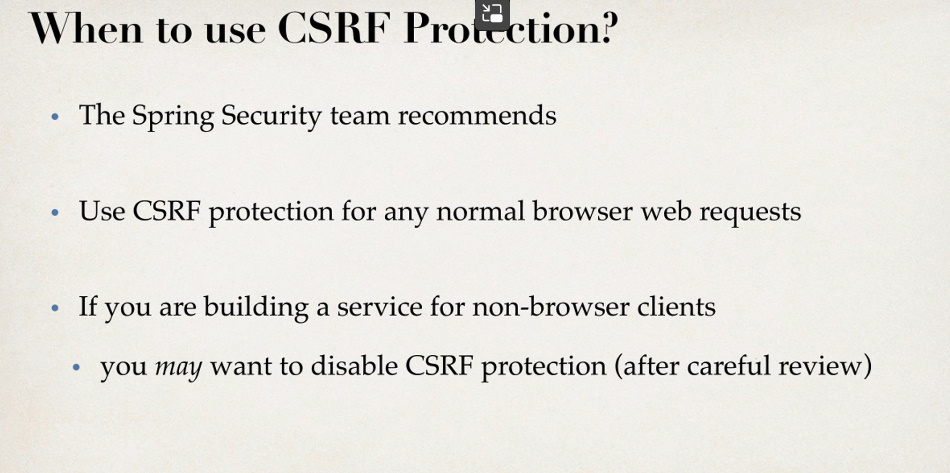
* CSRF – security atac unde un site rau te pacaleste ca sa executi o actiune pe o webapplication pe care esti logat la moment.
* Exemple:
* esti logat intr-o bankink app si esti mintit sa trimiti bani la o alta persoana
* esti logat intr-o e-commerce app si esti mintit sa cumperi iteme nedorite
* 
* Deci, e suficient ca o persoana rea sa iti trimita un link care este un request pentru a face un transfer bancar, de ex, si cand vei da click pe el, vei da acel request catre aplicatia unde esti logat si requestul se va face.De ex, persoana rea poate trimite un mesaj unde spune ca userul trebuie sa schimbe urgent parola, si sa dea cica un buton pentru a face asta:
* <a href="http://netbank.com/transfer.do?acct=AttackerA&amount=$100">Read more!</a>

Dar, cand userul da click pe el, se va trimite un request catre webapp, ca cel de sus, care e folosit pentru a face transferuri bancare, si userul nici nu va sti

**Spring Security Protection**

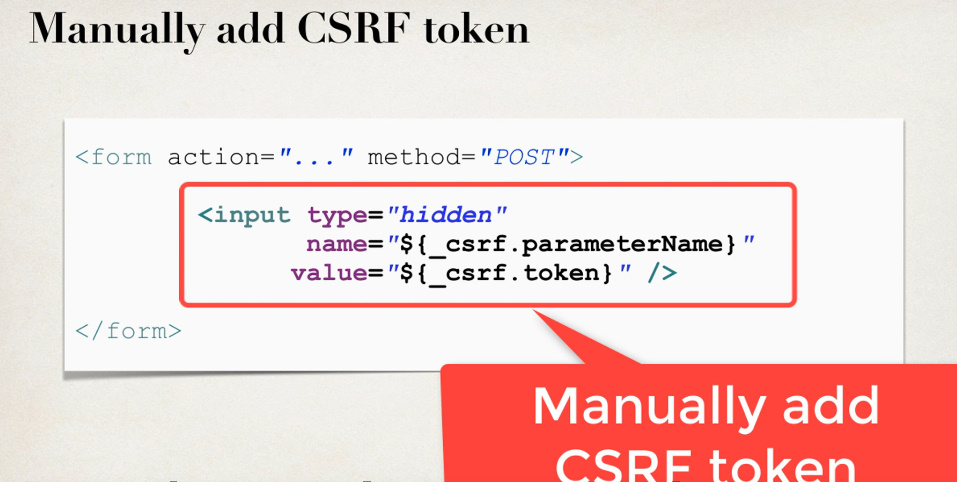


Deci, Spring Security verifica orice request ce vine, ca sa se asigure ca vine anume de la forma creata de noi in JSP. El adauga niste date in forma, cu un input type=”hidden”, pentru fiecare sesiune, si verifica daca request venit contine acele date.

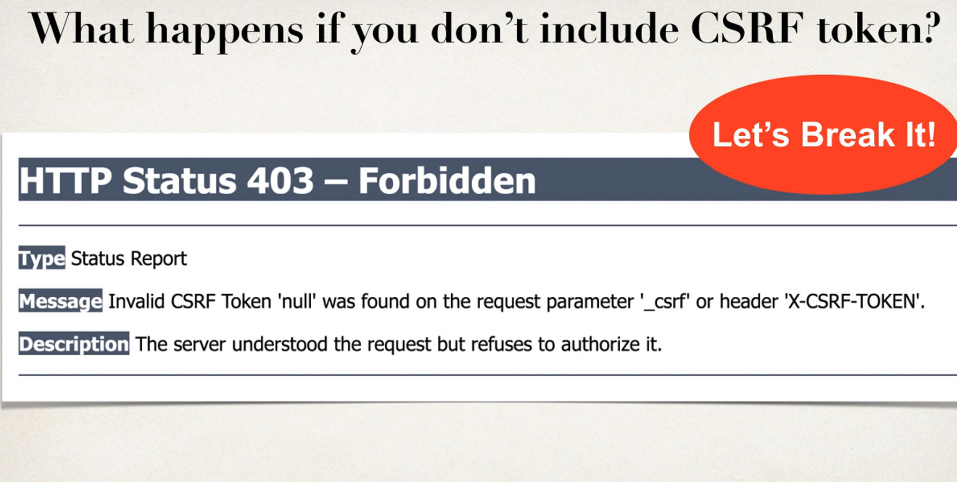




* Plus, POST trimitele datele mai securizat
* <form:form> automat adauga CSRF token
* Daca nu folosim <form:form>, trebuie manual sa punem CSRF token



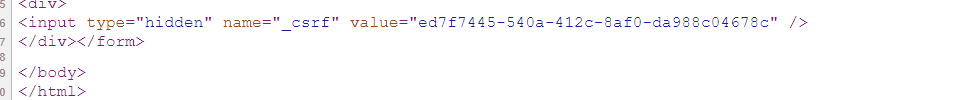
Deci,manual, in forma trebuie sa cream un input de tip hidden, ca sa nu fie vazut de user, ce contine niste date, pe care Spring Security le va verifica ca sa fie sigur ca request vine anume de la forma creata de noi si corespunde cu datele trimise de el pentru forma noastra **create pentru aceasta** Session.



Spring Security nici nu ne va da voie sa facem un reuqest fara CSRF token

**Practic**

* Daca folosim <form:form> si la pagina de logare inspectam sursa sa vedem codul HTML, vom observa in forma un camp nou:



El e adaugat automat de <form:form>

Deci, Spring stie ce valoare trebuie sa aiba acest camp,caci el le trimite pentru fiecare Sesseion, ca sa accepte requestul