# Iskorišćeni metodi za zaštitu od poznatih propusta

## 10.Unvalidated redirect and forwards

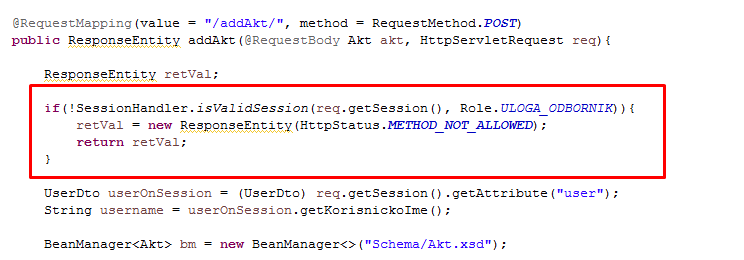
Nigde u aplikaciji se ne koristi mehanizam redirekta, klijentski deo je „single page“.

## Using components with known vulnerabilities

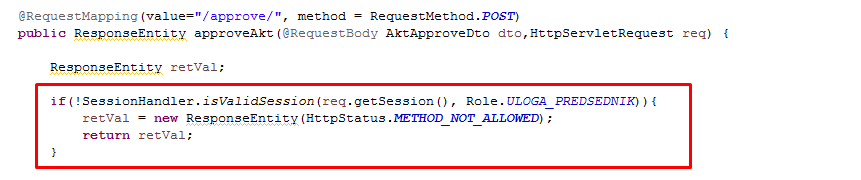
-Prilikom izrade projekta korišćene su pouzdane i proverene komponente koje su preuzete sa oficijalnih sajtova, sa dobrim preporukama korisnika. U periodu korišćenja aplikacije biće praćeno ažuriranje verzija komponenti, i po potrebi izvšeno ažuriranje u aplikaciji.

## Missing function level access control

-Prilikom predlaganja aktova/amandmana ili usvajanja aktova/amandamna, proverava se na serverskoj strani ko je ulogovan, i u slučaju da traženi zahtev nije u skladu sa ulogom korisnika, zahtev se odbije.



-------------------------------------------------------------------------------------------------------------

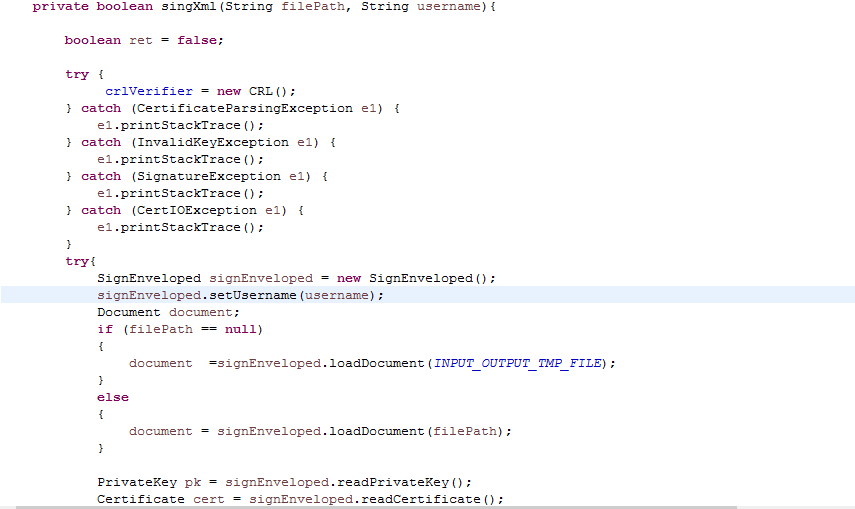
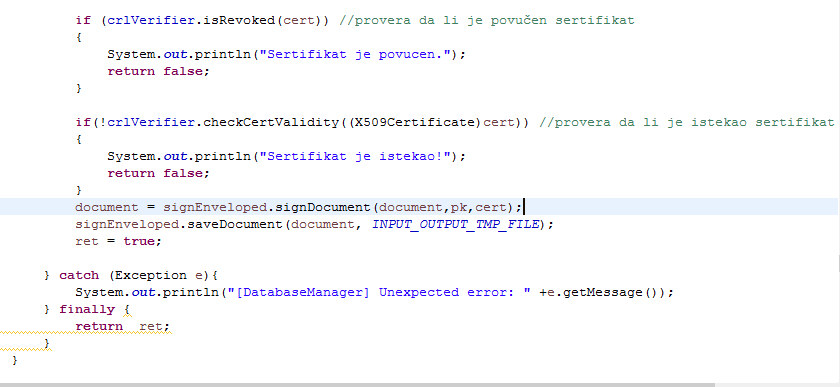


## Sensitive data exposure

Problem se odnosi na nedostatak ispravne zaštite osetljivih podataka. (Prve dve podtačke detaljinije obradjene u okviru **tačke2**(*Broken authentification and session management*))

* Enkripcija datoteka, podataka u bazi, heširanje lozinki,…(pogledaj ***tačku2***)
* Ručno digitalno potpisivanje i kriptovanje poruka

-Digitalno potpisivanje dokumenata odradjeno je u aplikaciji prilikom upisa dokumenata u bazu i prilikom razmenjivanja poruka izmedju 2 subjekta. Tom prilikom je potrebno potpisati poruku(dokument) validnim sertifikatom(npr da nije istekao, nije povučen..). To je realzovano na sledeći način:

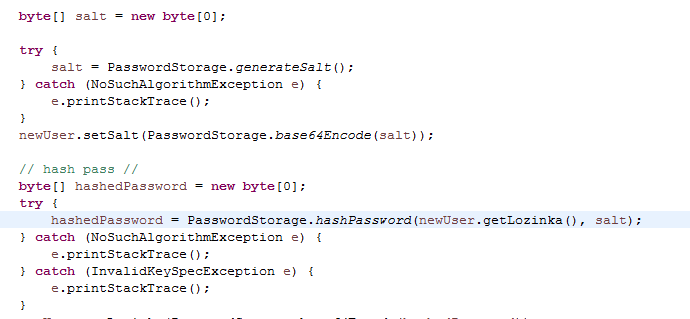
## Broken authentication and session management

Dešava se kada aplikacije u bilo kojoj fazi loše osiguravaju sesije i kredencijale.

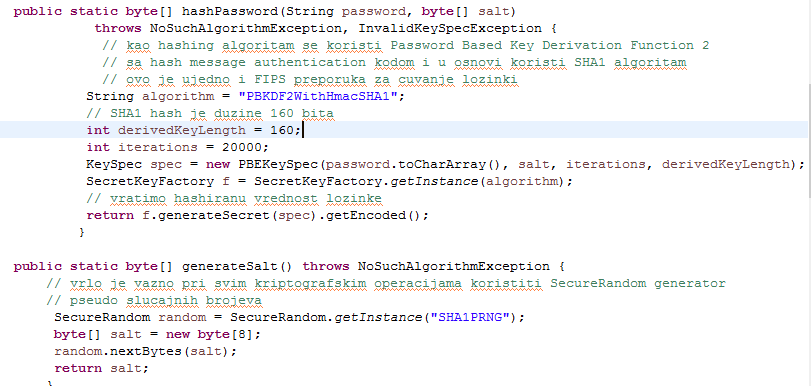
* Za upravljanje sesijom koriste se pouzdana i testirana rešenja.
* Da li se lozinke čuvaju na siguran način?

-Lozinke se u bazi podataka čuvaju kao „posoljeni“ hash(hash & salt) i time je onemogućeno da napadač vidi lozinke u slučaju dobijanja pristupa bazi.

-U kodu je to realizovano na sledeći način:



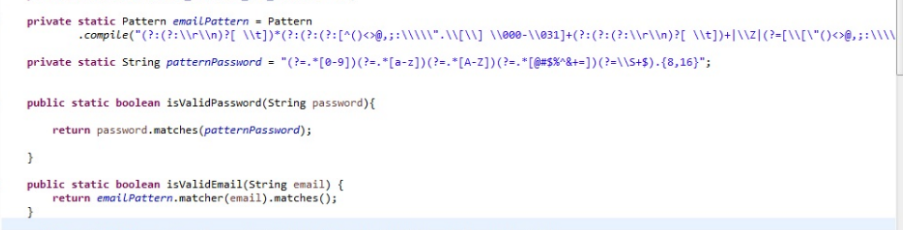
--------------------------------------------------------------------------------------------------------------



* Kakva je politika za formiranje lozinki?

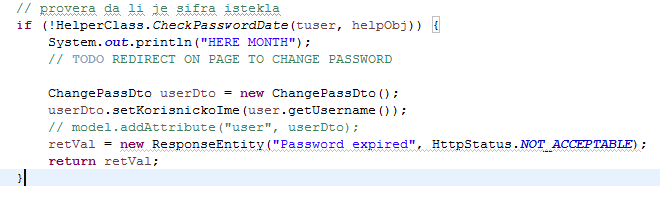
-Kada se formira lozinka ona mora biti u odredjenom formatu. Lozinka mora sadržati minimalno 8 karaktera a maksimalno 16, od toga mora biti:

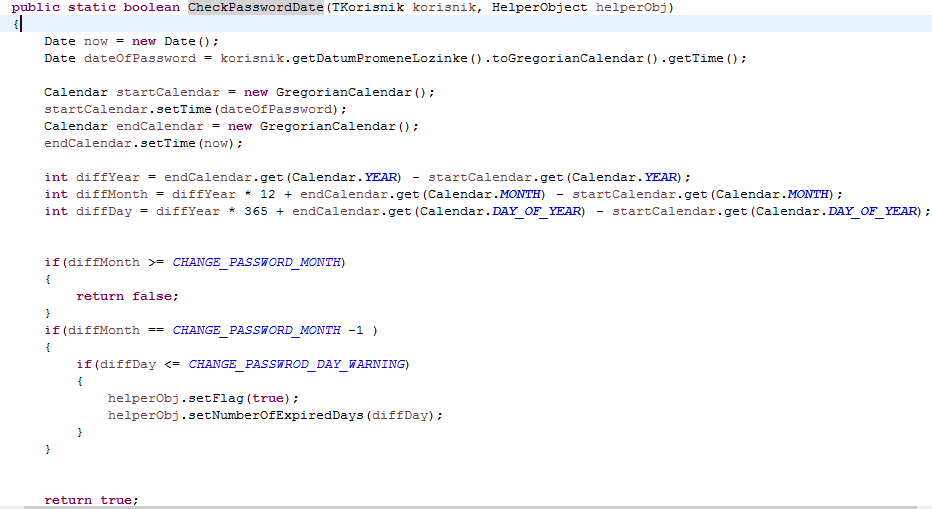
* + bar jedno veliko slovo(A-Z)
  + bar jedno malo slovo(a-z)
  + bar jedna cifra(0-9)
  + bar jedan specijalni karakter



* Koliko često korisnik mora da menja lozinku?

-Korisnik na svakih 6 meseci mora da promeni lozinku.





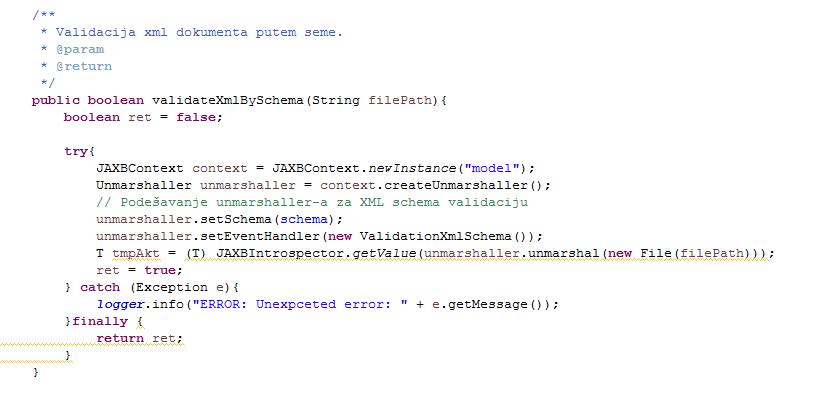
* Da li je komunikacija između klijenta i servera kriptovana?

-Komunikacija izmedju servera i klijenta odvija se preko HTTPS –a

## Injection- XML entity injection

Napad na slabo konfigurisan XML parser . Dovodi do DoS-a (XEE - XML entity expansion), otkrivanje podataka iz sistema (XXE - XML eXternal entity). Bazirano na konceptu spoljnog ENTITY-a u XML-u.

Ovaj napad je rešen preko validacije putem XML šeme prilikom slanja novog akta od strane korisnika(odbornika).



----------------------------------------------------------------------------------------------------------------------------

