Top 10 Web Application Security Risks

OWASP

Tim 13: Aleksa Goljović R2 29/21, Jelena Cupać R2 30/21, Milan Marinković R2 31/21

- ## Injection

  Izvršena je validacija podataka, kako na frontend-u, tako i na backend-u. Za validaciju podataka na frontend-u korišćeni su Vue rules, dok je na backend-u validacija implementirana upotrebom javax anotacija u okviru DTO objekata koji se preuzimaju u kontrolerima kao RequestBody.
  Što se tiče SQL Injection-a, Hibernate interno koristi prepared statements. Prepared statements obezbeđuju to da napadač ne može da promeni namenu upita,čak i ako pokušava u upit da ugradi maliciozni SQL.
  Budući da se ne koristi NoSQL baza podataka, NoSQL napadi nisu mogući.

- ## Broken Authentication

  Prilikom prijave na sistem korisnik će biti blokiran u slučaju da sa iste IP adrese tri puta unese pogrešnu lozinku. Blokiranje je privremeno i traje 24 sata. Takođe, ukoliko korisnik dugo vremena nije bio aktivan (period duži od 90 dana) njegov nalog automatski biva trajno blokiran. Pri svakom definisanju lozinke, proverava se da li lozinka postoji na NIST-ovoj listi nebezbednih lozinki. Ukoliko postoji korisnik će biti obavešten i od njega će biti zatraženo da unese novu lozinku. Za lozinku je definisana politika, mora da sadrži barem 8 karaktera, od toga mora da postoji broj, specijalni karakter, malo i veliko slovo. Lozinka je u bazi heširana. Takođe, prilikom registracije na sistem korisniku će biti poslat verifikacioni link na email adresu. Trajanje JWT tokena je podešeno na 30 minuta.

- ## Sensitive data exposure

  U osetljive podatke u sistemu spada lozinka, te je ona u bazi heširana korišćenjem Bcrypt algoritma. Podaci za plaćanje, kao što su PAN, security code, merchant id, merchant password i sl. takođe predstavljaju osetljive podatke koje je neophodno zaštititi. Ovi podaci su enkriptovani, pri čemu je za kriptovanje korišćen je simetrični algoritam, AES/ECB/PKCS5Padding. Podaci koji se prenose preko mreže su samo oni koji su neophodni i zaštićeni su HTTPS-om.

- ## XML External Entities

  U projektu se ne radi sa podacima u XML formatu.

- ## Broken Access Control

  Primenjen je RBAC kako bi se kontrolisao pristup svim endpoint-ima u sistemu. Definisane su tri role –prodavac, kupac opreme i kupac kursa i konferencije. Svakoj od ovih rola dodeljene su adekvatne permisije. Svaki endpoint u projektu je zaštićen, odnosno, podešene su potrebne permisije koje korisnik mora da ima da bi pristupio endpoint-u. Vue rute su takođe zaštićene.

- ## Security Misconfiguration

  Ne koriste se nalozi koji imaju default-no korisničko ime i lozinku. Ne postoje nepotrebni feature-i i web stranice. Poruke o greškama ne otkrivaju senzitivne podatke, niti daju previše informacija.

- ## Cross Site Scripting (XSS)

  Angular je korišćen za razvoj klijentskog dela aplikacija. Angular poseduje ugrađenu zaštitu od XSS napada. Na koji način? Da bi sprečio XSS napade, Vue sve vrednosti tretira kao untrusted. Vrši se inspekcija untrusted vrednosti, koja će vrednost pretvoriti u sigurnu i ubaciti je u DOM stablo.
  Za serverski deo aplikacije korišćen je Spring Boot, koji, takođe, štiti od XSS napada. X-XSS Protection header signalizira browseru da blokira sve što liči na XSS. Spring Security automatski dodaje pomenuti header u response. Ovo smo podesili u okviru Spring Security konfiguracione klase. Na ovaj način browser ne renderuje ukoliko detektuje XSS. Nažalost, neki browseri ne koriste ovaj header, te se koriste Content-Security-Policy (CSP) filteri.

- ## Insecure Deserialization

  Na backend-u sav saobraćaj koji bi trebao da stigne je validiran (u vidu anotacija za atribute DTO-a ili u okviru metode), na frontend-u validirane su sve forme. Svaki potpisan saobraćaj podrazumeva validiranje samog potpisa.

  Takođe, upotreba formata za razmenu podataka, kao što je JSON, smanjuje mogućnost za ovu vrstu napada, jer se podaci prenose u tekstualnom obliku, a potom deserijalizuju upotrebom proverenih deserijalizatora.

- ## Using Components With Known Vulnerabilities

  Korišćen je OWASP dependency checker, kako bismo bili svesni ranjivosti svih biblioteka koje se koriste u sistemu, zatim smo pokušali i da ih otklonimo.

- ## Insufficient Logging & Monitoring

  Saobracaj vezan za svaku komponentu sistema se loguje. Svaka komponenta sistema ima svoje skladište logova. Za logovanje je korišćena log4j biblioteka, tako da se za svaku log datoteku kreira backup na mesečnom nivou.