Model pretnji - SEP

Tim 20 - Dimitrije Salić, Mihailo Stanarević i Marko Rašeta

Model pretnji za projekat iz predmeta sistemi elektronskog plaćanja urađen je po STRIDE modelu.

STRIDE je skraćenica za:

- *Spoofing* - lažno predstavljanje
- *Tampering* - nedozvoljena izmena nečega u bazi podataka
- *Repudiation* - poricanje istine ili validnosti nečega
- *Information disclosure* - odavanje informacija nekome ko inače ne bi imao pristup istim
- *Denial of Service* - onemogućavanje rada sistema tako što se sistemu šalje veliki broj zahteva u sekundi
- *Elevation of Privilege* - izvršavanje akcija koje nisu dozvoljene tom korisniku

Spoofing

Pretnja	**Mera predostrožnosti**
SQL Injection	Korišćenjem Hibernate-a SQL Injection napadi su onemogućeni zbog samog načina na koji je Hibernate implementiran (korisnikov unos se ne unosi direktno u upit).
Bruteforce napad	Sve lozinke sadrže barem 10 karaktera, od kojih je bar jedan veliko slovo, bar jedan je malo slovo, bar jednu cifru i specijalan karakter. Nakon pet neuspešnih pokušaja prijava na sistem sa istim korisničkim imenom, nalog tog korisnika se zaključava na 30 minuta. Samim tim, mogućnost uspešnog bruteforce napada je svedena na minimum.
Dobavljanje osetljivih informacija iz baze podataka	Napadač čak i ako dođe do osetljivih informacija, neće mu biti ni od kakve od vrednosti, obzirom da se lozinke šifriraju AES256 standardom za enkripciju.

XSS napadi	XSS napadi su automatski onemogućeni sa obzirom da sa novijim verzijama Angular-a se vrši automatska sanitizacija unesenog slobodnog teksta na klijentskoj strani. Na serverskoj strani su postavljeni odgovarajući header-i u response-u svakog zahteva (X-XSS-Protection:1;mode=block).

Tampering

Pretnja	**Mera predostrožnosti**
SQL Injection	Korišćenjem Hibernate-a SQL Injection napadi su onemogućeni zbog samog načina na koji je Hibernate implementiran (korisnikov unos se ne unosi direktno u upit).
Zaražavanje računara malware-om	Upoznati korisnike sa potencijalnim opasnostima usled zaražavanja malware-om. Bezbednost korisnika zavisi od zaštite njegovog računara od malware-a.
Keystroke logging napad	Bezbednost korisnika zavisi od zaštite njegovog računara od alata koji vrše ove napade.
Zloupotreba ranjivosti korišćenih tehnologija i biblioteka	Nakon generisanja izveštaja potencijalnih ranjivih biblioteka i tehnologija, potrebno je ažurirati biblioteke koje sadrže ranjivost bilo kog stepena na njihovu najstabilniju verziju.
Izmena log datoteka	Potrebno je implementirati ACL (*Access Control List*) nad svim datotekama od značaja

Repudiation

Pretnja	Mera predostrožnosti
Korisnik poriče izvršenu akciju koja može delovati kobno po sistem	Implementiran *logging system* kako bi se obezbedila neporecivost.

Information disclosure

Pretnja	Mera predostrožnosti
Napadač je u mogućnosti da vidi podatke od značaja tako što presretne zahtev	Implementiran HTTPS (HTTP *Secure*) nad celim sistemom.
Napadač krade sertifikate	Izbegavati nevalidne SS sertifikate.

Denial of Service

Pretnja	Mera predostrožnosti
Napadač koči saobraćaj na sistemu slanjem velikog broja zahteva u kratkom vremenskom periodu	Kako bi se izbeglo preopterećenje potrebno je pratiti saobraćaj na nivou mreže.

Elevation of Privilege

Pretnja	Mera predostrožnosti
Napadač vertikalnom elevacijom privilegija dobija pristup funkcionalnostima višeg nivoa	Obezbeđeno autentifikacijom i autorizacijom.

DREAD minus D

DREAD je skraćenica za:

- *Damage* - koliko je napad opasan po sistem
- *Reproducibility* - koliko je lako ponoviti napad
- *Exploitability* - koliko je truda potrebno uložiti za napad
- *Affected users* - koliko je korisnika zahvaćeno napadom
- *Discoverability* - koliko je lako otkriti napad

	Damage	**Reproducibility**	**Exploitability**	**Affected users**
SQL Injection	**10**	**10**	**2**	**10**
Bruteforce napad	**8**	**1**	**2**	**1**
Dobavljanje osetljivih informacija iz baze podataka	**5**	**9**	**9**	**10**
XSS napadi	**8**	**6**	**3**	**1**
Zaražavanje računara malware-om	**7**	**5**	**9**	**1**
Keystroke logging napad	**10**	**5**	**9**	**1**
Zloupotreba ranjivosti korišćenih tehnologija i biblioteka	**8**	**7**	**8**	**10**
Izmena log datoteka	**6**	**8**	**3**	**10**
Korisnik poriče izvršenu akciju koja može delovati kobno po sistem	**2**	**5**	**1**	**1**
Napadač je u mogućnosti da vidi podatke od značaja tako što presretne zahtev	**9**	**7**	**6**	**6**

Napadač krade sertifikate	**8**	**6**	**8**	**1**
Napadač koči saobraćaj na sistemu slanjem velikog broja zahteva u kratkom vremenskom periodu	**10**	**2**	**10**	**10**
Napadač vertikalnom elevacijom privilegija dobija pristup funkcionalnostima višeg nivoa	**8**	**1**	**10**	**10**