Zbornik radova Fakulteta tehničkih nauka, Novi Sad

UDK: 004.9
DOI: https://doi.org/10.24867/06BE24Samardzic

ANALIZA BEZBEDNOSNIH RIZIKA I MERA ZAŠTITE VEB APLIKACIJA

SECURITY RISK ANALYSIS AND WEB APPLICATION SECURITY MEASURES

Bojana Samardžić, *Fakultet tehničkih nauka, Novi Sad*

Oblast – ELEKTROTEHNIKA I RAČUNARSTVO

Kratak sadržaj – *U radu je opisan problem bezbednosti veb orijentisanih informacionih sistema. Radi demonstracije načina na koje je moguće ugraditi sigurnosne mehanizme u softversko rešenje, razvijena je aplikacija za kupovinu i prodaju dostupnih artikala iz ponude. Realizovano rešenje oslanja se na radni okvir Spring i MySQL relacionu bazu podataka.*

Ključne reči: *aplikacija, baza podataka, bezbednost, maliciozni napadač, MySQL, napad, OWASP, pouzdanost, ranjivost, sigurnost, Spring*

Abstract – *The paper describes the security problem of web-oriented information systems. To demonstrate how security mechanisms can be incorporated into a software solution, an application has been developed to buy and sell available items from the offer. The implemented solution relies on the Spring framework and the MySQL relational database.*

Keywords: *application, database, security, malicious attacker, MySQL, attack, OWASP, reliability, vulnerability, safeness, Spring*

1. UVOD

U domenu informacionih tehnologija najveću vrednost imaju informacije. Vremenom se razvila grana koja je otišla u smeru krađe podataka, podmetanja virusa, prisluškivanja komunikacije između klijentske i serverske strane, ubrizgavanja malicionih skripti koje se izvršavaju na pretraživaču žrtve, kreiranja sadržaja koji može zbuniti interpreter baze podataka i izvršiti neželjenu transakciju, krađe korisničkih kredencijala, izmene prava pristupa, krađe kriptografskih ključeva i sl.

Veb aplikacije su se inkorporirale u veći deo mreže savremenog društva. U značajnoj meri su uticale na promenu dosadašnjih zahteva i očekivanja korisnika. Kako ova vrsta aplikacija radi u realnom vremenu, čim se desi neka izmena, ona postaje vidljiva i utiče na dalji rad sistema.

Cilj rada je upoznavanje osnovnih bezbednosnih koncepata i implementacija istih na primeru aplikacije za kupovinu i prodaju dostupnih artikala iz ponude.

NAPOMENA:
Ovaj rad proistekao je iz master rada čiji mentor je bio dr Aleksandar Kupusinac, vanr. prof.

2. BEZBEDNOST U INFORMACIONIM SISTEMIMA

Bezbednost informacionih sistema se primarno fokusira na zaštitu računara, mreža i njihovih korisnika. Digitalne pretnje dolaze u svim oblicima i veličinama: krađa privatnih podataka nakon upada u bazu podataka, instalacija zlonamernih softvera na mašini, namerno izazivanje prekida u radu servisa i druge [1].

2.1. Terminologija pretnji

Informaciona sigurnost odnosi se na sprečavanje ili makar smanjenje verovatnoće neovlašćenog pristupa, upotrebe, otkrivanja, ometanja, brisanja/uništavanja, korupcije, modifikacije i devalvacije informacija, a podrazumeva i smanjenje štetnih posledica incidenata. Upravljanje informacionom sigurnošću je proces detaljnog analiziranja i definisanja bezbednosnih kontrola u cilju zaštite informacionih sredstava.

2.1.1. Pretnja i rizik

Sa stanovišta računarske sigurnosti pod pojmom pretnja podrazumeva se potencijalna opasnost koja može iskoristiti ranjivost kako bi narušila bezbednost i samim tim prouzrokovala štetu. Rizik se objašnjava kao gubitak poverljivosti, integriteta i/ili dostupnosti informacija.

2.1.2. Ranjivost

Ranjivost se definiše kao osobina koju poseduje sistem u celosti ili neka njegova komponenta, a koja ostavlja prostor za zloupotrebu.

2.1.3. Resurs

Resursi su objekti od značaja – ako oni nisu raspoloživi ili ako su kompromitovani, sistem neće moći da funkcioniše ispravno.

2.1.4. Subjekat

Termin subjekat (u literaturi se sreće i pojam agent) označava entitet koji ima trenutno aktivnu ulogu u sistemu i može da obavlja akcije koje su mu stavljene na raspolaganje, tj. za koje ima ovlašćenja.

2.1.5. Napad

Realizacija pretnje. Napad je akcija koja se sprovodi sa ciljem da iskoristi detektovane ranjivosti sistema ne bi li se napadač domogao informacija koje može zloupotrebiti. Realizuje se vektorom napada (putanja ili način na koji se ostvaruje cilj).

2.1.6. Napadač

Čovek ili grupa ljudi koji nameravaju da ugroze resurse odabranog preduzeća.

2.1.7. Protivmere

Cilj definisanja bezbednosnih kontrola jeste svođenje eksploatacije ranjivosti sistema na minimum. Protivmere koje se uglavnom sprovode nad veb aplikacijama su heširanje lozinki, kriptovanje podataka u skladištu, upotreba sertifikata izdatih od strane poverljivih sertifikacionih tela, vođenje evidencije o aktivnostima koje se dešavaju u sistemu i druge.

2.2. Trijada informacione sigurnosti – CIA

U središtu sigurnosti informacija nalazi se *CIA* trijada: poverljivost, integritet i dostupnost. Rizici, pretnje i ranjivosti sa kojima se suočavaju softverski sistemi mere se na osnovu njihove potencijalne sposobnosti da kompromituju jedan ili više elemenata trijade.

2.2.1. Poverljivost

Koncept poverljivosti odnosi se na zaštitu podataka od subjekata koji nemaju ovlašćenje da im pristupaju, čime se osigurava to da se potreban nivo tajnosti primenjuje na svim mestima na kojima se vrši spajanje i obrada informacija.

2.2.2. Integritet

Pod pojmom integritet podrazumeva se obezbeđivanje tačnosti i pouzdanosti informacija i sistema, kao i sprečavanje neovlašćenih izmena.

2.2.3. Dostupnost

Termin dostupnost znači da informacije može pregledati i modifikovati svaki entitet koji za to ima dozvolu u odgovarajućem vremenskom roku.

2.3. Osnovni sigurnosni mehanizmi

Baza na kojoj je razvijena politika informacione sigurnosti sačinjena je od tri komponente: mehanizma identifikacije, autentifikacije i autorizacije. Podjednako važan bezbednosni mehanizam je i neporecivost.

2.3.1. Identifikacija

Identifikacija je čin predstavljanja sistemu, tj. tvrdnja ko je neko ili šta.

2.3.2. Autentifikacija

Autentifikacija je postupak utvrđivanja verodostojnosti tvrdnje da je subjekat to za šta se predstavlja.

2.3.3. Autorizacija

Autorizacija se objašnjava kao postupak utvrđivanja i proveravanja koja se ovlašćenja trebaju vezati za kog korisnika. Obavezno joj prethodi uspešna autentifikacija.

2.3.4. Neporecivost

Neporecivost znači da subjekat ne može da porekne da je preduzeo korake koji su doveli do izvršenja jedne ili niza akcija.

3. OWASP TOP 10 NAJKRITIČNIJIH SIGURNOSNIH RIZIKA VEB APLIKACIJA

3.1. OWASP zajednica

Politika *OWASP* zajednice (eng. *Open Web Application Security Project – OWASP*) usmerena je na identifikaciju pretnji i detekciju ranjivosti koje uslovljavaju njihovu pojavu, na uspostavu bezbednosnih praksi koje su se pokazale kao najdelotvornije, a nudi i upozorenja, ideje, savete, alate i procedure za izgradnju kvalitetnog rešenja.

3.1.1. Sigurnost veb aplikacija

OWASP organizacija kreirala je listu 10 najučestalijih napada na veb aplikacije, koja se periodično ažurira kako bi mogla odgovoriti konstantnoj pojavi novih pretnji [2].

3.1.1.1. Injection

Ideja napada je da eksploatiše interpreter komandi, odnosno parser. Onaj ko sprovodi napad dobija pristup tokovima podataka za koje nema pravo, a ostavlja se mogućnost i da napadač stvori potpuno novi tok podataka koji nije predviđen dizajnom. Najefikasniji način odbrane jeste validacija svih ulaznih podataka.

3.1.1.2. Broken Authentication

Meta ovog napada je autentifikaciona logika. Može se realizovati ukoliko se informacijama vezanim za sesiju upravlja na neadekvatan način usled čega je ugrožena korisnička identifikacija. Sprečavanje ove klase napada vrši se implementacijom multifaktorske autentifikacije.

3.1.1.3. Sensitive Data Exposure

Nastaje kao posledica toga što informacije namenjene isključivo ovlašćenim osobama bivaju slučajno otkrivene neautorizovanim korisnicima u nekriptovanom, slabo zaštićenom ili nezaštićenom okruženju. Dobra praksa za izbegavanje napada iz ove grupe jeste identifikacija osetljivih podataka, nakon čega sledi realizacija adekvatnih bezbednosnih mehanizama zaštite.

3.1.1.4. XML External Entites

Servisno orijentisani sistemi osetljivi su na klasu napada koji eksploatišu postupak parsiranja *XML* šeme. Napad je omogućen ukoliko je obrada *XML* ulaza koji sadrži referencu na neki eksterni entitet poverena loše konfigurisanom *XML* parseru. Rešenje ovog problema bila bi validacija po *XML* šemi.

3.1.1.5. Broken Access Control

Grupa napada koja iskorišćava izostanak kontrole pristupa na nivou funkcija i nebezbednih direktnih referenci na objekte. Za uspešno prevazilaženje ove vrste ranjivosti neophodno je vršiti rigorozne kontrole svih permisija koje se dodeljuju subjektima.

3.1.1.6. Security Misconfiguration

Meta napada je čitav sistem. Manipuliše nepravilnom implementacijom kontrolnih mehanizama koji bi aplikaciju trebali da održe bezbednom. Kao posledicu može imati to da se napadač potpuno infiltrira u sistem a da se za to neko vreme ne zna. Najdelotvornija mera odbrane jeste gašenje svega onog što nije neophodno.

3.1.1.7. Cross-Site Scripting

Napad koji eksploatiše i klijentsku i serversku stranu, što može dovesti do krađe kolačića i kompromitivanja osetljivih podataka. Za uspešnu realizaciju potrebno je da maliciozni napadač prvo preuzme kontrolu nad veb čitačem napadnutog subjekta, nakon čega može prinuditi veb čitač žrtve da izvrši bilo kakav podmetnuti *JavaScript*

kod zaobilazeći polisu zajedničkog porekla. Validacija podataka jedan je od načina odbrane od ove klase napada.

3.1.1.8. Insecure Deserialization

Distribucija malicioznih sadržaja vrši se pomoću serijalizovanih objekata. Uspešan napad može uzrokovati kompromitovanje ili brisanje podataka sačuvanih na disku, stvaranje potrebnih uslova za realizaciju *injection* grupe napada i eskalaciju privilegija. Sprečavanje ove klase napada zahteva onemogućavanje deserijalizacije podataka koji su potekli od neproverenih izvora.

3.1.1.9. Using Components with Known Vulnerabilities

Ako se radi sa već gotovim komponentama, bibliotekama i radnim okvirima, mora se obratiti pažnja na ranjivosti koje one unose u sistem. Prevencija napada moguća je ukoliko se vodi precizna evidencija o korišćenim komponentama i ako se one redovno održavaju.

3.1.1.10. Insufficient Logging & Monitoring

Nedovoljno često i detaljno nadgledanje u kombinaciji sa neefikasnom integracijom sa odgovarajućim odgovorima na incident ostavljaju dovoljno prostora napadačima da izvrše napad. Najvažnija bezbednosna kontrola koja se sprovodi sa ciljem smanjenja rizika od ove grupe napada je svakodnevno praćenje saobraćaja koji se razmenjuje i analiziranje dnevnika aktivnosti u aplikaciji.

4. RADNI OKVIR SPRING

Spring je radni okvir otvorenog koda koji pruža sveobuhvatnu infrastukturnu podršku za razvoj *Java* aplikacija. *SpringBoot* je proširenje *Springa*. Dozvoljava da se više koraka spoji u jedan, zahvaljujući čemu se postupak podešavanja konfiguracije pojednostavljuje.

4.1. Arhitektura veb aplikacije za kupovinu i prodaju artikala iz ponude zasnovane na Spring radnom okviru

Aplikacija namenjena kupovini i prodaji artikala iz ponude organizovana je tako da se može uočiti jasna razlika između modela, prezentacionog sloja, upravljačkog sloja, servisnog sloja i repozitorijuma. Pripadajuće klase svakog od slojeva smeštene su u zasebnim paketima.

5. BAZA PODATAKA

5.1. Relaciona baza podataka

Relaciona baza podataka oslanja se na relacioni model koji je specifičan po tome što podatke organizuje u skup relacija između kojih se uspostavljaju odgovarajuće veze i ograničenja.

5.1.1. MySQL relaciona baza podataka – osnovni koncepti i integracija sa aplikacijom za kupovinu i prodaju artikala iz ponude

Da bi veb aplikacija namenjena kupovini i prodaji artikala iz ponude mogla da koristi podatke sačuvane u *MySQL* relacionoj bazi podataka, neophodno je podesiti konfiguracione parametre u okviru *application.properties* fajla i u *pom.xml* fajl dodati odgovarajuće zavisnosti.
Kreiranje tabela i međurelacionih ograničenja u bazi vrši se na osnovu *Spring* anotacija – sve klase moraju biti propisno anotirane kako bi se znalo kom sloju pripadaju i na koji način će se uspostaviti veze između njih.

6. BOOKSTORE APLIKACIJA

Bookstore je veb aplikacija primarno namenjena kupovini i prodaji artikala iz ponude. Ideja je da implementirano softversko rešenje omogući rad sa sistemom koji je otporan na neke od poznatih učestalih sigurnosnih napada.

6.1. Veza između korisničkih uloga i raspoloživih funkcionalnosti

U aplikaciji se pravi razlika između korisnika. Oni se klasifikuju na registrovane i neregistrovane posetioce. Registrovani korisnici se potom dele na administratore i na obične registovane posetioce sajta.

Tabela 1 sadrži pregled informacija o tome koja korisnička uloga može obavljati koje od funkcionalnosti aplikacije.

Tabela 1 *Pregled informacija o tome koja korisnička uloga može obavljati koje od funkcionalnosti aplikacije*

Funkcionalnost / korisnička uloga	*Neregistrovani korisnik*	*Običan registrovan posetilac sajta*	*Administrator*
slanje poruka	+	+	+
registracija	+	+	+
prijava	-	+	+
promena lozinke	-	+	+
ažuriranje korisničkog naloga	-	+	+
deaktivacija korisničkog naloga	-	+	+
pretraga dostupnih artikala	+	+	+
prikazivanje detaljnih informacija o odabranom artiklu	+	+	+
kupovina artikala	-	+	-
upravljanje nalozima običnih registrovanih posetilaca sajta	-	-	+
dodavanje novih artikala u ponudu	-	-	+
izmena postojećih artikala	-	-	+
brisanje artikala iz ponude	-	-	+

6.2. Sigurnosni mehanizmi implementirani u veb aplikaciji za kupovinu i prodaju artikala iz ponude

Implementirana veb aplikacija razvijena je u skladu sa politikom razvoja bezbednog softverskog proizvoda.
Rešenje je osmišljeno tako da ga je u bilo kom trenutku moguće nadograditi dodatnim sigurnosnim kontrolama, ukoliko se za tim javi potreba.

6.2.1. Sigurna komunikacija preko mreže

Za uspostavu bezbedne komunikacije između klijentske i serverske strane korišćen je *HTTPS* protokol. Na taj način sprečeno je neovlašćeno prisluškivanje saobraćaja na mreži, kao i *man in the middle* napad.

6.2.2. Logovanje aktivnosti

Softversko rešenje realizovano je tako da podržava logovanje svih dešavanja u aplikaciji. Na osnovu istorije aktivnosti moguće je zaključiti kada su nad sistemom počete da se preduzimaju sumnjive radnje, a takođe se garantuje i neporecivost zato što se tačno zna ko je i u kom trenutku izvršio koju operaciju.

6.2.3. Kriptovanje i heširanje korisničkih kredencijala

Podaci u skladištu naročito su ranjive prirode ukoliko se skladište u formi običnog teksta. Detektovani najosetljiviji podaci kojima sistem rukuje su korisnički kredencijali. Oni se u bazi podataka čuvaju u šifrovanom, odnosno heširanom obliku. Za heširanje lozinke korišćena je ugrađena klasa *BcryptPasswordEncoder*. Kriptovanje korisničkog imena vrši se *AES* algoritmom.

6.2.4. Validacija korisničkih unosa

Razvijena veb aplikacija ima proveru korisničkih unosa i na strani klijenta i na strani servera. Validacija podataka vrši se kombinovanom upotrebom liste dozvoljenih vrednosti i liste zabranjenih unosa jer se u praksi ovaj pristup pokazao najefikasnijim.

6.2.5. JSON Web Token

JSON Web Token je mehanizam koji se koristi da omogući da strane koje učestvuju u komunikaciji mogu samostalno i na siguran način razmenjivati podatke u *JSON* formatu. U pitanju je otvoreni standard koji garantuje da su informacije verifikovane i da im se može verovati zahvaljujući tome što su digitalno potpisane.
U aplikaciji za kupovinu i prodaju dostupnih artikala mehanizam *JWT*-a primenjen je u postupku autorizacije, čime je sprečen napad na neporecivost.

6.2.6. Cross-Site Request Forgery

U implementiranoj aplikaciji postoji zaštita od *CSRF* napada, što znači da nije moguće sprovesti napad koji bi naterao autentifikovanog korisnika da inicira operaciju koju ne želi. Zaštita od ove klase napada zahteva anotiranje konfiguracionih klasa na odgovarajući način.

6.2.7. Permisije i sopstvene anotacije

Razvijeni sistem poštuje strogu kontrolu pristupa resursima. Da bi se postigao efekat da svaku od ponuđenih funkcionalnosti aplikacije može da izvrši tačno određena uloga, uvedene su sopstvene permisije i anotacije.

7. ZAKLJUČAK

U radu su detaljno opisani osnovni koncepti informacione sigurnosti, izloženi su najčešći napadi na veb aplikacije i objašnjeno je zbog kojih je sve razloga potrebno raditi na razvoju bezbednih softverskih sistema.

Investiranje u proces razvoja pouzdanih i sigurnih softverskih rešenja dovodi do unapređenja procesa poslovanja zato što se njihova snaga ogleda upravo u mogućnosti da korisnicima daju garanciju da mogu obavljati visoko rizične operacije poput novčanih transakcija i ostavljanja ličnih podataka na uvid administratorskom osoblju bez brige o tome da li će oni u bilo kom trenutku i na bilo koji način biti kompromitovani i/ili čak zloupotrebljeni.
Ukoliko se poslušaju praktični saveti koji podstiču izgradnju bezbednog softvera, ako se za proces implementacije angažuju programeri koji vode računa o tome da je neophodno eliminisati što je moguće veći broj potencijalnih ranjivosti, kvalitet dobijenog rešenja bio bi na izuzetno visokom nivou.
Zahvaljujući tome, značajno bi se smanjila verovatnoća realizacije efikasnih napada i povećalo bi se poverenje koje korisnici imaju u sistem.

8. LITERATURA

[1] https://www.computersciencedegreehub.com/faq/what-is-information-systems-security (pristupljeno u avgustu 2019.)

[2] https://www.owasp.org/images/7/72/OWASP_Top_10-2017_(en).pdf.pdf (pristupljeno u avgustu 2019.)

Kratka biografija:

Bojana Samardžić rođena je 20.07.1995. u Novom Sadu. Završila je osnovnu školu „Jovan Dučić“ u Petrovaradinu. Nakon završene osnovne škole upisuje srednju školu, gimnaziju „Svetozar Marković“ u Novom Sadu. 2014. godine upisuje „Fakultet tehničkih nauka“ u Novom Sadu, smer *Računarstvo i automatika*. Školske 2016/17. godine opredeljuje se za usmerenje *Primenjene računarske nauke i informatika*. Školske 2017/18. godine upisuje modul *Internet i elektronsko poslovanje*. Zvanje *diplomirani inženjer elektrotehnike i računarstva* dobija 29.08.2018. Školske 2018/19. godine upisuje master akademske studije, smer *Primenjene računarske nauke i informatika – Elektronsko poslovanje*. Zvanje *saradnik u nastavi* na Departmanu za računarstvo i automatiku na Fakultetu tehničkih nauka u Novom Sadu dobija 09.11.2018.

kontakt: bojana.samardzic@uns.ac.rs