Napadi na softverske sisteme i mehanizmi zaštite

Čedomir Dimić, Jana Milutinović, Miloš Samardžija

16. maj 2017

Sadržaj

Glava 1

Recenzent — ocena:3

1.1 O čemu rad govori?

Rad govori o napadima na softverske sisteme, i predlaže načine za njihovo sprečavanje. Navedeni su primeri najčešćih vrsta napada, kao i bezbednosni propusti u sistemima. Dobija se dobra slika o ranjivosti softvera i značaja dobrog dizanja.

1.2 Krupne primedbe i sugestije

Neke rečenice su preduge i zbunjujuće. Umesto nabrajanja bi možda bilo bolje odabrati manje primera, ali im posvetiti više pažnje.
Nisu navedene konkretne rečenice koje su recenzentu bile zbunjujuće. Potrudili smo se da tekst bude prilagođen neupućenom čitaocu.

1.3 Sitne primedbe

Odeljak 2.2 Antivirusni softver - "...postoje novi virusi koje antivirus nema registrovan u svojoj...". Trebalo bi da piše "...nema registrovane...". Odeljak 2.4 Virtuelna privatna mreža - "Takođe postoji autentikacija pošiljaoca da bi se onemogućilo neovlašćenim korisnicima pristup mreži". Redosled reči u ovoj rečenici nema smisla. Odeljak 5. Bezbednosni propusti pri implementaciji veb servera - Na par mesta u tekstu se našlo I umesto i. Takođe, trebalo bi upotrebljavati sinonime, umesto ponavljanja jedne reči u uzastopnim rečenicama.
Primedbe su prihvaćene i greške su ispravljene.

1.4 Provera sadržajnosti i forme seminarskog rada

1. Da li rad dobro odgovara na zadatu temu?
   Rad sasvim dobro pokriva napade koji se mogu izvršiti na neki softverski sistem. Posebno je dobro što postoje primeri za vrste napada koji su prikazani.

2. Da li je nešto važno propušteno?
   Uzimajući u obzir moje znanje o ovoj temi, nije.

3. Da li ima suštinskih grešaka i propusta?
   Nema.

4. Da li je naslov rada dobro izabran?
   Naslov rada dobro reflektuje sadržaj koji sledi u radu.

5. Da li sažetak sadrži prave podatke o radu?
   Sažetak ima sve bitne podatke o radu, kao i dobar uvod za temu koju rad obrađuje.

6. Da li je rad lak-težak za čitanje?
   Rad je malo teži za čitanje zbog nekih nepotrebno dugih rečenica i čudnih konstrukcija. Sa tehničke strane je jasan i čitljiv.
   Ovaj komentar je kontradiktoran.

7. Da li je za razumevanje teksta potrebno predznanje i u kolikoj meri?
   Potrebno je znati osnove veb tehnologija.

8. Da li je u radu navedena odgovarajuća literatura?
   Jeste.

9. Da li su u radu reference korektno navedene?
   Jesu.

10. Da li je struktura rada adekvatna?
    Ispoštovani su uslovi za izradu seminarskog rada, sem par sitnih propusta. Na primer, nije mi se učitala slika steka na strani 5 i stavka sa brojem 4 se nalazi na strani 11, umesto na strani 10 izmedju stavki 3 i 5.
    Ove greške su ispravljene.

11. Da li rad sadrži sve elemente propisane uslovom seminarskog rada (slike, tabele, broj strana...)?
    Da.

12. Da li su slike i tabele funkcionalne i adekvatne?
    Jesu, osim one slike steka, već navedene.
    Umesto slike steka, ubačena je tabela.

1.5 Ocenite sebe

Ocenio bih sebe kao srednje upućenog u ovu oblast. Nisam se previše bavio ovom temom u slobodno vreme, ali sam polagao kurs Informacioni sistemi, na kome je u nekoj meri bila obrađena ova oblast.

Glava 2

Recenzent — ocena:5

2.1 O čemu rad govori?

Rad prestavlja osnovne koncepte bezbednosti softvera kroz primere napada i savete kako se zaštiti od njih. Premda je ta sfera bezbednosti široka i konstanto se razvija, autori rada su uspeli da izdvoje najvažnije teme i da pruže svest o tome koliko se neki napadi mogu lako izvesti, a koliko opasnosti donose.

2.2 Krupne primedbe i sugestije

Krupna primedba je što su prevencije nekih napada površno objašnjeni (primeri: XSS, CSRF), bez ulaženja u detalje, koji su možda i najbitniji za tu tematiku (naš cilj je da sprečimo da se napad desi, bez adekvatnog objašnjenja je to teško).
Prevencija navedenih napada je detaljnije opisana.

2.3 Sitne primedbe

Sitna primedba je *Listing 2: Primer ranjivog upita.* Konkretno *Listing* nije relevantno navoditi uz ime primera.
Medju sitnijim primedbama je i ta što je veznik *i* veliko slovo u pojedinim delovima u tekstu između reči.
Primedbe su prihvaćene i ispravljene su greške.

2.4 Provera sadržajnosti i forme seminarskog rada

1. Da li rad dobro odgovara na zadatu temu?
   Rad dobro odgovara na pitanja o bezbednosti softvera i njegove zaštite.

2. Da li je nešto važno propušteno?
   Ništa suštinski nije propušteno, ono što je rečeno u uvodnim delovima i ono što se očekivalo od rada, zaista je detaljno i objašnjeno.

3. Da li ima suštinskih grešaka i propusta?
   Jedini propust su detalji prevencije napada, kao što je objašnjeno u sekciji **??**

4. Da li je naslov rada dobro izabran?
   Sam naslov bi mogao da bude adektvatniji, jer se rad dobrim delom posvetio i prevencijama napada.
   Koristili smo radni naslov koji je sada ispravljen tako da bolje odgovora sadržaju rada.

5. Da li sažetak sadrži prave podatke o radu?
   Konkretno, tema sažetka je slična uvodnom delu, što se može smatrati propustom (izuzetak je poslednja rečenica sažetka). U toj sekciji se očekivalo više o cilju rada i kroz koje teme rad prolazi.
   U potpunosti se slažemo sa ovom primedbom i izmenili smo sadržaj sažetka i uvoda tako da nema ponavljanja.

6. Da li je rad lak-težak za čitanje?
   Rad je lako čitljiv.

7. Da li je za razumevanje teksta potrebno predznanje i u kolikoj meri?
   Predznanje nije potrebno u velikoj meri, jer su se autori posvetili detaljnim objašnjenima većine rada.

8. Da li je u radu navedena odgovarajuća literatura?
   Literatura odgovara temama na koje se fokusira sam rad.

9. Da li su u radu reference korektno navedene?
   Sve činjenice su potkrepljene odgovarajućom literaturom.

10. Da li je struktura rada adekvatna?
    Za strutukturni deo rada postoji primedba za sekciju *5.2 Propusti i načini otklanjanja*, konkretno za nabrajanje koje je ispreturano (pojedini delovi samo izlistani bez objašnjenja).
    Tekst u poglavlju *5.2* je dorađen i sada su neke najvažnije stavke objašnjene a one za koje nije bilo mesta u ovom radu adekvatno napomenute.

11. Da li rad sadrži sve elemente propisane uslovom seminarskog rada (slike, tabele, broj strana...)?
    Radu fali sumiranje celokupnog istraživanja i načini unapređivanja (konkretno, fali sekcija *Zaključak*)
    Zaključak je dodat i tu je sumiran celokupan sadržaj.

12. Da li su slike i tabele funkcionalne i adekvatne?
    Slika 1: Stanje steka nakon izvršavanja strcpy nije funkcionalna, već je navedena putanja do nje, što čitaocima nije od preteranog značaja.
    Umesto slike 1, ubačena je tabela.

2.5 Ocenite sebe

Smatram sebe srednje upućenim u konkretnu oblast, jer sam izdvojio vreme za istraživanje teme koju su autori obradili.

Glava 3

Recenzent — ocena:5

3.1 O čemu rad govori?

U ovom radu su opisani napadi na softverske sisteme, kroz nedostatke u implementaciji samog softvera. Takođe su i predstavljene kraće celine govoreći o mehanizmima zaštite softvera, uobičajenim greškama u dizajnu i propustima pri implementaciji veb servera.

3.2 Krupne primedbe i sugestije

Uzimajući u obzir to da je tema i suština rada bila da se opišu napadi na softverske sisteme, dok sam čitala imala sam osećaj da tom poglavlju, pod naslovom Napadi, nije dat dovoljan značaj. Skratila bih neke delove, kako bi se moglo opširnije pisati o samim napadima. Još jedna stvar koja mi je zapala za oko je u poglavlju 3.1, Slika 1 čiju namenu nisam u potpunosti razumela, ili možda slika nije uspešno dodata. Nedostaje zaključak.
Potrudili smo se da uskladimo sadržaj i naslov rada. Prevencija nekih napada je opisana malo detaljnije. Umesto slike 1, ubačena je tabela. Zaključak je dodat.

3.3 Sitne primedbe

Postoji par štamparskih, sintaksnih i stilskih grešaka na koje sam naišla, koje ću navesti u nastavku:

1. Prva rečenica sažetka nije poravnata sa pasusom u kom se nalazi.
   Ispravljena je greška.

2. U glavi 2 pri navođenju osnovnih mehanizama zaštite na Internetu, smatram da su **zaštitni zid**, **antivirusni programi** i **šifrovanje** podataka trebali biti posebno naznačeni, na primer boldovani, kako bi se isticali od okolnog teksta i lakše uočili.
   Sugestije su prihvaćene.

3. U poglavlju 2.4 u 6. redu prvog pasusa piše obezbežuje umesto obezbeđuje.
   Greška je ispravljena.

4. U poglavlju 3.1 u primeru prekoračenja bafera, smatram da ako je primer toliki da može da stane na jednu stranu, da bude na jednoj strani, a ne da se prelama na dve, zbog čitljivosti.
   Greška je ispravljena.

5. Isto važi za poglavlje 3.2, primer ranjivog upita.
   Greška je ispravljena.

6. U poglavlju 3.5, kada se navodi podela XSS napada, smatram da je bolje navoditi tačkama, nego brojevima, sem u slučaju kada je redosled navođenja bitan.
   Sugestija je prihvaćena.

7. Isto važi i za glavu 4 pri navođenju propusta u dizajnu.
   Sugestija je prihvaćena.

8. U poglavlju 5.2, ako je već navođeno brojevima, redosled brojeva treba onda i poštovati, stavka pod rednim brojem 4. je van svog redosleda.
   Ispravljena je greška.

9. Na par mesta je napisano autentifikacija umesto autentikacija.
   Ispravljena je greška.

3.4 Provera sadržajnosti i forme seminarskog rada

1. Da li rad dobro odgovara na zadatu temu?
   Da, rad odgovara dobro na tu temu.

2. Da li je nešto važno propušteno?
   Svi zahtevi teme su obuhvaćeni, tako da ništa nije propušteno.

3. Da li ima suštinskih grešaka i propusta?
   Ono što sam ja primetila je da naslov nije u skladu sa sadržajem rada, kao i da nedostaje zaključak.
   Promenjen je naslov rada i dodat je zaključak.

4. Da li je naslov rada dobro izabran?
   Naslov nije u skladu sa sadržajem. Ne obuhvata sve teme obrađene u radu.
   Promenjen je naslov rada.

5. Da li sažetak sadrži prave podatke o radu?
   Da, u kratkim crtama je opisano o čemu rad govori.

6. Da li je rad lak-težak za čitanje?
   Rad je bio srednje-lak za čitanje, dakle formatiranje teksta nije savršeno, neke ključne stvari su trebale biti posebno istaknute (bold ili underline), kako bi se čitaocu olakšalo zapažanje tih ključnih stvari. Konstrukcija rečenica je bila dobra i lako razumljiva. Nije bilo predugačkih i zbunjujućih rečenica.

7. Da li je za razumevanje teksta potrebno predznanje i u kolikoj meri?
   Za razumevanje ovog teksta je potrebno neko osnovno znanje o programiranju, Vebu, bazama podataka.

8. Da li je u radu navedena odgovarajuća literatura?
   Da, navedena literatura je odgovarajuća.

9. Da li su u radu reference korektno navedene?
   Reference su korektno navedene.

10. Da li je struktura rada adekvatna?
    Struktura rada je adekvatna.

11. Da li rad sadrži sve elemente propisane uslovom seminarskog rada (slike, tabele, broj strana...)?
    Slika 1 izgleda da nije dobro učitana i prikazana, tabela nije bilo, a broj strana je adekvatan.
    Umesto slike 1, ubačena je tabela.

12. Da li su slike i tabele funkcionalne i adekvatne?
    Slika 1 izgleda da nije dobro učitana i prikazana, ostatak je u redu.
    Umesto slike 1, ubačena je tabela.

3.5 Ocenite sebe

Srednje sam upućena u navedenu oblast, s obzirom da sam i sama istraživala i učila o većini ovih stvari.

Glava 4

Recenzent — ocena:5

4.1 O čemu rad govori?

Upoznajemo se sa 3 osnovna aspekta bezbednosti, kao i sa mehanizmima zaštite koji omogućavaju da se navedeni aspekti ispoštuju. Pažnja je posvećena čestim tipovima napada na informacione sisteme, uz primere koji oslikavaju propuste i nastale probleme. Predočene su smernice za dizajn softvera koji olakšava izradu bezbednih aplikacija, kao i mogući propusti pri implementaciji veb servera.

4.2 Krupne primedbe i sugestije

U nastavku su primedbe i sugestije, kao i obrazloženja za njihovo navođenje u ovom odeljku.

- **Neophodno je preurediti sažetak** - Cilj sažetka je da ubedi čitaoca da je rad vredan njegovog vremena, da mu da uvid u ono što ga očekuje u nastavku, a ne da mu predstavi temu. Radova na svaku temu ima mnogo, bitno je naglasiti šta je to što ovaj rad donosi specifično.
  Preuređen je sažetak rada.

- **Nedostaje zaključak** - Bez adekvatnog zaključka, koji će spojiti sve ono što je rečeno u prethodnim sekcijama, gubi se smisao i poenta rada. Neophodno je čitaocu skrenuti pažnju na bitna zapažanja koja su posledice svega obrađenog u radu. Takođe, zaključak nam daje uvid u opravdanost obrađivanja ove teme i pokazuje stvarnu potrebu za njenim daljim izučavanjem.
  Zaključak je dodat.

- **Uvod bez informacija o samom radu** - Umesto i sadržinom rada, uvod se bavi samo sigurnošću softvera. U početku naučnog rada, bez ikakve najave, polazi se sa gomilom novih pojmova. Bolje bi bilo dodati ukratko šta će čitaoci sve naći u narednim sekcijama, pozvati se na literaturu koja šire obrađuje temu rada, itd.
  U sažetku su nabrojane teme kojima se ovaj rad bavi. Potrudili smo se

da sve nepoznate pojmove objasnimo, ali bilo je i onih koji nismo jer smo smatrali da su dovoljno jasni čitaocima kojima je ovaj rad namenjen.

- **Loše nabrajanje u sekciji 5.2** - U ovom nabrajanju se pojavljuju dva propusta:

  1. Neregularan redosled nabrajanja - nakon broja 3 slede brojevi 5 do 14, nakon čega se nabrajanje vraća na broj 4
     Greške su ispravljene.
  2. Menjanje stila - prve 4 stavke (po rednom broju, ne po redosledu pojavljivanja) su detaljnije objašnjene propratnim tekstom, dok one nakon toga nisu; Bilo bi mnogo smislenije da se stavke koje neće biti detaljnije obrađene navedu odvojeno od nabrajanja uz napomenu zašto su manje bitne od ostalih
     Tekst u poglavlju *5.2* je dorađen i sada su neke najvažnije stavke objašnjene a one za koje nije bilo mesta u ovom radu adekvatno napomenute.

4.3 Sitne primedbe

Kada je reč o sitnim, jezičkim greškama, neophodno je napomenuti propust pri uvođenju termina engleskog porekla *chat* korišćen je u tom obliku, bez ikakvog označavanja. Umesto toga, bilo bi mnogo prirodnije koristiti naš izraz *ćaskanje*, uz naglašavanje da se misli na gore navedeni termin.
Sugestija je prihvaćena.

Osim toga, u tekstu postoji više stamparskih grešaka, izostavljanje i dodavanje slova. Zbog njihove brojnosti neće biti ovde navedena svaka.
Ispravljene su štamparske greške.

4.4 Provera sadržajnosti i forme seminarskog rada

1. Da li rad dobro odgovara na zadatu temu?
   Rad uspešno odgovara na temu. Svaka sekcija predstavlja odgovor na jedno od pitanja postavljenih sa ciljem dobre analize teme.

2. Da li je nešto važno propušteno?
   Na sva suštinska pitanja koja se tiču teme je uspešno odgovoreno.

3. Da li ima suštinskih grešaka i propusta?
   Radu nedostaje zaključak. Celokupna priča nije zaokružena izvlačenjem ključnih tačaka koje bi naglasile čitaocu na šta posebno treba obratiti pažnju kada je reč o ovoj temi.
   Zaključak je dodat.

4. Da li je naslov rada dobro izabran?
   Stiče se utisak da su napadi na softverske sisteme samo sporedna stavka ovog rada i da se pažnja daleko više posvećuje dizajnu koji ih sprečava. Zbog toga ovaj naslov nije najadekvatnije rešenje.
   Naslov rada je promenjen tako da bolje odgovora samom sadržaju rada.

5. Da li sažetak sadrži prave podatke o radu?
   Sažetak više liči na uvod u kom se upoznajemo sa temom rada nego na stvaran sažetak sadržine. Umesto da u kratkim crtama privuče čitaoca da nastavi sa čitanjem rada, sažetak uvodi u temu (što je zadatak uvoda).
   Sažetak je izmenjen u skladu sa ovom primedbom.

6. Da li je rad lak-težak za čitanje?
   Rad je prilično lak za čitanje, bez nepotrebnog komplikovanja.

7. Da li je za razumevanje teksta potrebno predznanje i u kolikoj meri?
   Za razumevanje teksta je potrebno osnovno poznavanje iz oblasti računarskih nauka. Većina bitnih stavki potrebnih za razumevanje teme je u hodu objašnjena čitaocu. Stiče se utisak da bi i mnoga nestručna lica koja računare koriste u svakodnevnom radu mogla da razumeju veći deo rada.

8. Da li je u radu navedena odgovarajuća literatura?
   Literatura je uredno navedena. Svaka stavka pruža bolji uvid u segment priče na koji se odnosi.

9. Da li su u radu reference korektno navedene?
   U radu su reference korektno navedene, kako na slike, tako i pozivanja na literaturu.

10. Da li je struktura rada adekvatna?
    Struktura rada omogućava da se jasno vide odgovori na sva postavljena pitanja. Ostaje utisak da sažetak, uvod i zaključak nisu ispratili sam sadržaj svojim kvalitetom.
    Sažetak i uvod su izmenjeni, a zaključak je dodat.

11. Da li rad sadrži sve elemente propisane uslovom seminarskog rada (slike, tabele, broj strana...)?
    Radu nedostaje tabela. Ostali uslovi su ispunjeni.
    Tabela je dodata.

12. Da li su slike i tabele funkcionalne i adekvatne?
    Slika 1 nije uredno ubačena, te se u fajlu koji je meni prosleđen na recenziju umesto slike vidi putanja na kojoj bi ta slika trebala da se nalazi. Zamerka za drugu sliku je što nije preuređena tako da tekst na njoj bude na srpskom jeziku, u skladu sa ostatkom rada.
    Umesto slike 1, ubačena je tabela 1. Smatramo da je tekst koji se nalazi na drugoj slici dovoljno jasan i da se pomenuti termini češće koriste na engleskom jeziku.

4.5 Ocenite sebe

U temu rada sam srednje upućen. Sa pitanjima na koja rad pruža odgovore, upoznat sam toliko detaljno koliko je to obrađeno na fakultetskim kursevima. Nikada nisam bio u prilici da se detaljnije bavim bilo čime što bi imalo snažnije veze sa temom rada. U skladu sa tim, ova recenzija se više tiče forme pisanja rada nego njegovim sadržajem.

Glava 5

Dodatne izmene