Propusti u bezbednosti softvera i prevencija njihove zloupotrebe

Aleksandra, David, Sreten

Recenzija: Miloš Samardžija

21. april 2017

1 O čemu rad govori?

Rad pruža osnovne informacije iz oblasti bezbednosti softvera. Na razumljiv način je opisana razlika između pojmova koji se često mešaju - identifikacija, autentikacija i autorizacija. Opisani su sigurnosni rizici Veb aplikacija uopšte, kao i neki od najčešćih napada, uz navedene primere. Date su osnovne preporuke za održavanje Veb servera, u cilju očuvanja bezbednosti samog servera, kao i aplikacija koje se nalaze na njemu.

2 Krupne primedbe i sugestije

1. Potrebno je preformulisati problem kod umetanja SQL upita. Nije dovoljno reći da sistem ne zna kako da rukuje sa podacima. Navesti šta je stvarni problem (nedovoljna validacija korisničkog unosa, itd.). Objasniti uopšteno koji delovi aplikacije su najranjiviji (deo za Log In se možda najčešće koristi kao početna tačka za upad, ali svakako nije jedina, ranjiv je svaki deo u kojem postoji izvršavanje upita u kojem učestvuje korisnički unos, poput pretrage na sajtu, itd.).

2. Primer 2.1: Jedna od najpovoljnijih situacija je ukoliko program nasilno prekine sa radom. Napadač ovaj propust može iskoristiti za mnogo opasnije stvari, kao što su zaobilaženje raznih bezbedonosnih mehanizama, izmenu podataka, i za izvršavanje proizvoljnog zlonamernog koda.

3 Sitne primedbe

Delovi koji sadrže grešku su podebljani.

1. Sažetak, prva rečenica (ispraviti naznačenu reč): *Ovaj rad pruža osnovne informacije o bezbednosti softvera, posledicama koje nastaju usled njenog zanemarivanja i načinima* ***prevenecije*** *njenih zloupotreba.*

2. Bezbednost softvera, drugi pasus (predložena izmena dela prve rečenice): *Dok softver koji se razvija skoro uvek ima greške u implementaciji...*

3. Bezbednost veb aplikacija, prvi pasus: Nakon dela gde piše “pružanja različitih informacija“ staviti zarez.

4. Umesto termina “zlonamerni programer“, koristiti termin “zlonamerni korisnik“. Napadač ne mora biti programer, čak šta više, ne mora biti ni stručan (pogledati termin script kiddie).

5. Umesto termina “injektovani“, poželjnije je koristiti termin “umetnuti“.

6. Sačuvani XSS, prvi pasus: “Stored XSS“ navesti kao “sačuvani XSS“, i u zagradi staviti od koje engleske reči termin potiče.

7. Uklanjanje nepotrebnih servisa, druga rečenica: *Na taj način se povećava broj slabih tačaka servera, te* ***je ga je*** *teže održavati.*

8. Udaljeni pristup, druga rečenica: Pre “te je“ staviti zarez.

4 Provera sadržajnosti i forme seminarskog rada

1. Da li rad dobro odgovara na zadatu temu?
   Rad dobro odgovara na zadatu temu. Obuhvata sva pitanja predviđena ovom temom.

2. Da li je nešto važno propušteno?
   Nakon detaljne analize, smatram da rad nema važnijih propusta.

3. Da li ima suštinskih grešaka i propusta?
   Rad sadrži sitne greške nastale prilikom kucanja, i određene delove je potrebno prepraviti/dopuniti.

4. Da li je naslov rada dobro izabran?
   Naslov rada je u skladu sa samim sadržajem.

5. Da li sažetak sadrži prave podatke o radu?
   Sažetak u kratkim crtama obuhvata sadržaj rada, i sadrži prave podatke.

6. Da li je rad lak-težak za čitanje?
   Rad je lak za čitanje i sadrži ilustrativne primere.

7. Da li je za razumevanje teksta potrebno predznanje i u kolikoj meri?
   Potrebno je poznavanje HTML-a, SQL-a i HTTP protokola na osnovnom nivou.

8. Da li je u radu navedena odgovarajuća literatura?
   U radu je navedena odgovarajuća literatura i citirana je u okviru rada.

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

10. Da li je struktura rada adekvatna?
    Struktura rada je adekvatna. Sadrži naziv teme, autore, apstrakt, uvod, razradu i zaključak.

11. Da li rad sadrži sve elemente propisane uslovom seminarskog rada (slike, tabele, broj strana...)?
    Rad sadrži slike/tabele, ograničenja za literaturu i broj strana su zadovoljena.

12. Da li su slike i tabele funkcionalne i adekvatne?
    Slike i tabele su funkcionalne, i referisane su u tekstu.

5 Ocenite sebe

Veoma sam upućen u oblast koju recenziram. Obrađivao sam sličnu temu. Takođe, sa navedenim temama, konceptima i pojmovima sam bio u kontaktu i ranije.

6 Poverljivi komentari