SQL injection (SQLi) i Cross-site scripting (XSS)

Opis:

A screenshot of a computer

Description automatically generated

A screenshot of a web page

Description automatically generated

Na stranici na kojoj se pregleda pojedinačni poklon (Slika 1.3) nalazi se forma za ostavljanje komentara. Proveriti da li preko ove forme može da se izvrši neka vrsta XSS ili SQLi napada. Cilj napada je da se iskoristi kombinacija XSS i/ili SQLi napada za ubacivanje novog korisnika u bazu podataka i obezbedi mogućnost krađe kolačića sesije korisnika preko stranice persons.html (Slika 1.4). Voditi računa, novog korisnika je potrebno ubaciti u tabelu person, a ne u tabelu user u bazi. Stranica persons.html (Slika 1.4) je ranjiva na XSS napad, pa je konačni zadatak da ubačeni korisnik, kao neki od svojih atributa ima zlonamernu JavaScript skriptu koja će na konzolni izlaz da ispiše vrednost kolačića sesije korisnika. Ranjivost se aktivira prilikom pretrage korisnika na stranici persons.html (Slika 1.4). Obavezno je dokumentovati ovaj napad i poslati ga sa projektnim zadatkom.

Neophodno je zaštititi se od prethodno opisanog napada tako da ne može da se izvrši napad preko forme za ostavljanje komentara. Odnosno, neophodno izvršiti zaštitu od SQLi napada i od XSS napada. Takođe, na stranici persons.html (Slika 1.4) neophodno je popraviti ranjivosti koje omogućuju XSS napad. Popravka ranjivosti ne sme da naruši ili promeni funkcionalnost aplikacije.

Rešenje:

Kao što vidimo iz opisa problema forma za ostavljanje komentara je ranjiva na SQLi napad. To takođe vidimo iz SonarQube izveštaja. Kod za upis komentara u bazu izgleda ovako:

A screen shot of a computer

Description automatically generated

Jasno je da pošto je komentar tipa String da tu možemo umetnuti naš SQL upit koji želimo da izvršimo. Kako takođe znamo da je stranica za pretragu korisnika ranjiva na XSS, mi možemo za neki od atributa korisnika (recimo email jer se čak ni tu ne vrši validacija) postaviti JavaScript kod koji ispisuje kolačić (console.log(document.cookie)) – u nekom pravom slučaju ne bi ispisali kolačić u konzoli nego bi pozvali naš remote server gde bi smo sačuvali taj kolačić za dalje napade.

SQLi izazivamo sledećim komentarom:

SQLiLovesXSSLovesJESSIONID'); insert into persons values (666, 'NotoriousAcko', 'hackerZ', '<img src="x" onerror="console.log(document.cookie)"/>'); --

A screenshot of a computer

Description automatically generated

To će postaviti komentar SQLiLovesXSSLovesJESSIONID i kreirati zlonamernog korisnika NotoriousAcko. Ovaj tip XSS napada je uskladišteni (perzistentni) jer se čuva u bazi servera i svaki korisnik je izložen njemu.

A white rectangular object with a black border

Description automatically generatedA screenshot of a computer

Description automatically generated

Kako pretraga korisnika ima ranjivost na XSS napad jer se korisnik renderuje koristeći innerHtml iako su sva polja tekstualna pretragom korisnika će stranica pokušati da učita sliku x koja ne postoji i trigerovati onerror funkciju koja će ispisati korisnikov kolačić.

A screen shot of a computer program

Description automatically generated

A screenshot of a computer

Description automatically generated

Odbrana od ovog napada je poprilično standardna, za SQLi je potrebno koristiti PreparedStatement umesto query teksta koji se generiše konkatenacijom stringova i sami parametri se ubacuju u tekst, već treba taj query kompajlirati na SQL serveru i onda odvojeno slati podatke i time će komentar upravo biti onaj koji smo uneli.

A screen shot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

XSS ranjivost popravljamo tako što innerHtml menjamo sa textContent kod tekstualnih polja i onda tekstualna polja interpertiramo kao to što jesu (tekst), a ne HTML, tako da čak i u slučaju da imamo skriptu perzistovanu u bazi, pretraga korisnika neće biti ranjiva.

A screen shot of a computer program

Description automatically generated

Takođe je potrebno ispraviti renderovanje komentara gde u slučaju da je komentar validan HTML kod zbog korišćenja th:utext on bi se izvršio, tako da utext treba zameniti sa text.

A computer screen shot of a computer code

Description automatically generated

A screenshot of a computer

Description automatically generated

Aleksandar Ivanović, 2023/3468