Univerzitet u Beogradu

Elektrotehnički fakultet

Razvoj bezbednog softvera

CWE-209

Generation of Error Message Containing Sensitive Information

Seminarski rad

Studenti:  
Jelena Pančevski 2023/3231

Đorđe Milinović 2023/3368

Beograd, školska 2023/2024

**Zadatak**

Cilj seminarskog rada jeste izrada sistema u okviru kog je kreirano 10 *Capture the flag* izazovaza propust *CWE-209* tj*. Generation of Error Message Containing Sensitive Information* i njemu povezanim propustima. Propust *CWE-209* se odnosi na to da kreirani sistem generiše poruku o grešci koja uključuje osetljive informacije o svom okruženju, korisnicima ili povezanim podacima. Osetljive informacije mogu biti vredne informacije same po sebi (kao što je lozinka), ili mogu biti korisne za pokretanje drugih, ozbiljnijih napada. Poruka o grešci može biti kreirana na različite načine:

* samostalno generisana: izvorni kod eksplicitno konstruiše poruku o grešci i isporučuje je.
* eksterno generisana: spoljašnje okruženje, kao što je interpreter jezika, upravlja greškom i konstruiše sopstvenu poruku, čiji sadržaj nije pod direktnom kontrolom programera.

U nastavku biće dat opis svih implementiranih izazova.

**Capture the flag #1 - *CWE-209 – Pronalazak korisničkog imena admin korisnika***

Korisnik je potrebno da se loginuje kao admin. Koristeći implementirane propuste potrebno je da dođe do informacije o korisničkom imenu korisnika tipa admin kao i lozinci. Ukoliko korisnik pokuša da se loginuje sa nekorektnim kredencijalima, postoje dve situacije:

* Ukoliko korisnik unese nepostojeći *username*, sistem korisniku ispisuje grešku: *The entered username doesn't exist*
* Ukoliko korisnik unese postojeći *username*, sistem korisniku ispisuje grešku: *Wrong password for username*

Ovaj propust omogućava napadaču da sakupi informacije o postojećim korisničkim imenima unutar sistema. Napadač je u mogućnosti da brute force metodom, unošenjem često korišćenih korisničkih imena za administratore sistema, pronađe korisničko ime administratora - *admin*.

**Capture the flag #2 – *CWE-1295 (Debug Messages Revealing Unnecessary Information) – Pronalazak lozinke admin korisnika***

Sledeće što je potrebno učiniti jeste pronaći lozinku administratora sa korisničkim imenom *admin.* U sistemu se nalazi propust *CWE-1295* koji predstavlja prikazivanje nepotrebnih informacija u debug porukama, u ovom slučaju, ukoliko lozinka nije tačna ispisuje tačnu lozinku. Ovakve poruke korisne su tokom implementacije, ali kada je sistem u upotrebi predstavljaju rizik, a u konkretnom slučaju napadač na osnovu pogrešno unete lozinke dobija informaciju o ispravnoj lozinci.

**Capture the flag #3 - *CWE-200 (Exposure of Sensitive Information to an Unauthorized Actor) – Pronlazak stranice sa logovima***

Nakon uspešnog login-a na sistem, korisnik se odvodi na stranicu */home*. Analiziranjem *HTTP Response Header-a* korisnik pronalazi *FLAG\_LOGS : /logs* koji korisniku prikazuje informaciju o postojećem *endpoint-u* koji prikazuje sve do tada izvršene logove. CWE-200 predstavlja propust kojim se poverljivi podaci prikazuju neautorizovanom korisniku. U ovom slučaju, korisnik saznaje da postoji stranica sa svim logovima na serverskoj strani, što može dovesti do curenja bitnih informacija i potencijalni rizik.

**Capture the flag #4 - *CWE-209 – Pronalazak promokoda***

Na stranici */basket* korisnik je u mogućnosti da unese promokod za kupovinu proizvoda. Prilikom unosa nepostojećeg promokoda, korisniku se ispisuje greška:

*Promocode doesn’t exist.*

Pregledom stranice sa svim izvršenim logovima, napadač uočava sledeći log:

2023-12-22T22:45:51.876+01:00 ERROR 11892 --- [http-nio-8080-exec-1] c.r.c.repository.PromocodeRepository : No data is available [2000-224] BAD QUERY: SELECT \* FROM promocodes WHERE name='badpromo'; NO RESULTS FOUND

Na ovaj način, napadač dobija informaciju o nazivu tabele u kojoj se nalaze promokodovi kao i koloni koja označava ime promokoda. Napadač je u mogućnsti da dobijene informacije iskoristi na stranici za pretragu prozivoda na osnovu sastojka *(/searchByIngridients*), na kojoj se nalazi polje preko kog je moguće izvršiti *SQL injection* unosom:

*badingredient' union select name from promocodes--*

Ovim napadač dobija izlistana imena svih postojećih promokodova na sajtu između ostalog i promokod AWESOMEFLAG koji predstavlja traženi CTF #4.

**Capture the flag #5 -**