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*. 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***

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*.

Prilikom login-a, kao admin za username se unose

ucestala korisnicka imena za admine dok se neki ne poklopi sa postojecim.

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

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 se 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 infromaciju o ispravnoj lozinci.

je pronaci lozinku, u debug-u console.log ispisuje kada sifra nije jednaka