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 sa 10 *Capture the flag* izazova za 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.

Prilikom uspešne prijave, napadač vidi spisak svih korisnika u sistemu i njihova korisnička imena, može da odabere neko postojeće korisničko ime, a na isti način kao i za administratora dobije informaciju o lozinci i pristupi sistemu kao običan korisnik.

Capture the flag #3 - *CWE-200 (Exposure of Sensitive Information to an Unauthorized Actor)* – Pronalazak 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 predstavlja potencijalni rizik.

Capture the flag #4 – *CWE-209* - Pronalazak informacije o postojećoj količini proizvoda

Korisnik je potrebno da pronađe informaciju o postojećoj količini proizvoda. Odlaskom na stranicu */product/id* i naručivanjem velike količine proizvoda (npr. unos broja 100 u polje amount), korisniku se ispisuje sledeća greška:

Error while adding to basket: There is not enough product with the name Black Forest for the order, current available quantity is 20 FOUND FLAG

Greška otkriva nepotrebne informacije korisniku koje mogu biti osetljivog karaktera.

Capture the flag #5 - *CWE-209 – Pronalazak promo koda*

Na stranici */basket* korisnik je u mogućnosti da unese promo kod za kupovinu proizvoda. Prilikom unosa nepostojećeg promo koda (promo50), korisniku se ispisuje greška:

Promocode promo50 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='promo50'; NO RESULTS FOUND

Na ovaj način, napadač dobija informaciju o nazivu tabele u kojoj se nalaze promo kodovi kao i koloni koja označava ime promo koda. Napadač je u mogućnosti da dobijene informacije iskoristi na stranici za pretragu proizvoda 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 promo kodova na sajtu između ostalog i promo kod *AWESOMEFLAG* koji predstavlja traženi *CTF #5*.

Capture the flag #6 – *CWE-209* - Pronalazak tajnog sastojka

Korisnik je potrebno da pronađe tajni sastojak poslastičarnice *Delicious corner*. Kada korisnik klikne na određen prozivod, sistem ga odvodi na stranicu */product/idproduct*. Ukoliko korisnik pokuša da unese *idproduct* koji ne postoji u bazi podataka, korisniku se ispisuje sledeća greška: *No product with id = 25*, dok se loguje sledeći ispis:

2023-12-23T01:12:23.859+01:00 ERROR 13196 --- [http-nio-8080-exec-7] c.r.c.c.DatabaseAuthenticationProvider : No data is available [2000-224]

2023-12-23T01:12:23.859+01:00 ERROR 13196 --- [http-nio-8080-exec-7] c.r.c.c.DatabaseAuthenticationProvider : QUERY: SELECT id,ingredients,name, description,producttype,price,image,secret FROM products WHERE id=25

Korisnik putem logova saznaje kako izgleda tabela *products* time može da izvrši *SQL injection:*

/' union select secret from products --

na stranici */searchByIngredients* i pristupi polju secret čime dobija sledeći ispis: A3, A9, C5, F1, G4, I6, L2, M10, N12, N7,N8,O11. Koristeći pretpostavku da je tajni sastojak šifrovan i da brojevi označavaju redni broj slova u poruci, preuređivanjem dobijenog ispisa korisnik dolazi do tajnog sastojka: *FLAG CINNAMON*.

Capture the flag #7 – *CWE-209* - Pronalazak tajne promocije

Korisnik je potrebno da pronađe tajnu promociju poslastičarnice *Delicious corner*. Kada korisnik klikne na određenu promociju, sistem ga odvodi na stranicu */promotion/idpromotion*. Ukoliko korisnik pokuša da unese *idpromotion* koji ne postoji u bazi podataka, korisniku se ispisuje sledeća greška:

No promotion with id = 10 cannot find an image /promotions/10.jpg

Existing files:

C:\Users\Dell\Desktop\Master\RBS\Seminarski

rad\cwe209\target\classes\static\promotions\1.jpg

C:\Users\Dell\Desktop\Master\RBS\Seminarski
rad\cwe209\target\classes\static\promotions\2.jpg

C:\Users\Dell\Desktop\Master\RBS\Seminarski
rad\cwe209\target\classes\static\promotions\3.jpg

C:\Users\Dell\Desktop\Master\RBS\Seminarski
rad\cwe209\target\classes\static\promotions\cinnamon bun.jpg

C:\Users\Dell\Desktop\Master\RBS\Seminarski
rad\cwe209\target\classes\static\promotions\cinnamon bun.txt

Ova greška navodi sve postojeće fajlove unutar foldera promotions i dodatno napadaču pruža informaciju o strukturi projekta što predstavlja potencijalni rizik za *Path Traversal* napad. Pristupom cinammon bun.txt fajlu napadač vidi sledeću poruku:

Free dounts on Monday 31st of December!

Flag found :)

Capture the flag #8 – *CWE-200* - Pronalazak bankovnih računa zaposlenih korisnika

Korisnik može pristupiti stranici *Employees* i videti spisak svih zaposlenih. Potrebno je da dođe do bankovnih računa zaposlenih korisnika. Odlaskom na inspect date stranice, može videti *hidden* polja u kojima se nalaze zapisi bankovnih računa. Ove informacije su osetljive, ne bi trebalo da budu pristupačne korisniku, predstavljaju *CWE-200* propust koji se odnosi na otkrivanje osetljivih informacija neautorizovanom korisniku.

Capture the flag #9 – *CWE-209* - Pristup svim poslatim pitanjima

Korisnik na stranici *Contact us* može poslati pitanje zaposlenima unosom *email-a* i samog pitanja. Ukoliko ne unese neko od polja prikazuje mu se sledeća greška:

NULL not allowed for column "EMAIL"; SQL statement: INSERT INTO questions (email, question) VALUES (?, ?) [23502-224]

Ovakva greška napadaču daje informaciju o nazivu tabele *questions* u kojoj su smeštena pitanja kao i o njenim kolonama *email* i *question*. Koristeći ove informacije, na stranici */ /searchByIngredients* može izvršiti *SQLInjection* kako bi pristupio svim poslatim pitanjima:

/' union select question from questions –

Čime se dobija sledeći ispis: Flag #9 Found.

Capture the flag #10 – *CWE-200* - Pronalazak tajne lokacije

Korisnik na stranici *Contact us* može videti postojeće lokacije poslastičarnice *Delicious corner*. Analiziranjem postojećih logova prilikom pristupa ovoj stranici uočava sledeći log:

2023-12-27T16:10:23.543+01:00 INFO 14408 --- [http-nio-8080-exec-4] c.r.c.repository.LocationRepository : Executing query: select id,name,phone,address,workinghours,src,open from locations where open=true

Ovaj log napadaču daje informacije o strukturi i nazivu tabele u kojoj se smeštaju lokacije poslastičarnice. Analiziranjem izvršenog *sql* upita može se doći do zaključka da postoje lokacije sa atributom *open=false*. Ovu informaciju, napadač može iskoristiti na stanici */searchByIngredients* i uz pomoć *SQL injection* napada doći do naziva tajne lokacije:

/' union select name from locations where open=false --

Izvršavanjem ovog upita dolazi do imena tajne lokacije *Secret delicious corner* i poslednjeg *CTF flag-a* u ovom sistemu.

Zaključak

Na osnovu implementacija *Capture the flag* izazova vezanih za propust *CWE-209* možemo zaključiti da informacije do kojih potencijalni napadači mogu doći putem ovog propusta, olakšavaju druge napade na sistem (npr. SQL injection, Path Traversal, Brute force). Veća osetljivost prikazane informacije dovodi do povećanog sigurnosnog rizika sistema.

Prilikom implementacije sistema, potrebno je kreirati poruke o grešci takve da sadrže samo minimalne detalje koji su potrebni korisnicima za razumevanje same greške. Poruke ne smeju sadržati detalje koji otkrivaju osetljive informacije o sistemu (npr. izgled tabela, metode, postojeći fajlovi i putanje). Potrebno je ukloniti postojeće debug poruke unutar sistema pre nego što sistem pređe u upotrebu. Ukoliko je neophodno da se greške detaljno opišu, detaljan opis treba smestiti u log fajlove, pri čemu je potrebno izbeći čuvanje osetljivih informacija, a same fajlove zaštititi od neautorizovanog pristupa. Potrebno je interno rukovati sistemskim izuzecima kako ne bi došlo do prikaza potencijalno osetljivih informacija korisnicima.