

UNIVERZITET U BEOGRADU
ELEKTROTEHNIČKI FAKULTET



SONARQUBE IZVEŠTAJ

Projekat iz predmeta Razvoj bezbednog softvera

Profesor:

Žarko Stanisavljević, prof. dr

Student:

Filip Kojić 2023/3297

Beograd, Februar 2024.

SADRŽAJ

SADRŽAJ..... 2

1. PREGLED STAVKI U SONARQUBE ANALIZI PROJEKTA..... 3

1. PREGLED STAVKI U SONARQUBE ANALIZI PROJEKTA

| Slika | Problem | Oznaka | Obrazloženje |
|---------|---|----------------------|---|
| Slika 1 | CSRF zaštita onemogućena | True positive | Detektovano je da je CSRF zaštita isključena u aplikaciji, što predstavlja sigurnosni rizik. Efikasno rešenje je da se aktivira ugrađena CSRF zaštita ili da se implementira sistem tokena. U ovom sistemu, pri svakom pokretanju korisničke sesije generiše se jedinstveni CSRF token pomoću CSPRNG-a, koji se čuva u sesiji i šalje korisniku. Svaki korisnički zahtev mora uključivati ovaj token, a server ga verifikuje sa tokenom iz sesije da bi osigurao legitimnost zahteva. |
| Slika 2 | SQL Injection – Komentarisanje poklona | True positive | Konkatenacija stringa za kreiranje SQL upita. |
| Slika 3 | SQL Injection – Dohvatanje svih komentara za poklon | True positive | Konkatenacija stringa za kreiranje SQL upita. |
| Slika 4 | SQL Injection – Pretraga poklona | True positive | Konkatenacija stringa za kreiranje SQL upita. |
| Slika 5 | SQL Injection – Dohvatanje poklona po id | False positive | Vrši se konkatenacija celog broja(int), što ne omogućava SQL Injection napad. |

| | | | |
|----------|--|----------------------|---|
| Slika 6 | SQL Injection – Dohvatanje poklona po id i njegovih tagova | False positive | Vrši se konkatencija celog broja(int), što ne omogućava SQL Injection napad. |
| Slika 7 | SQL Injection – Brisanje poklona sa zadatim id | False positive | Vrši se konkatencija celog broja(int), što ne omogućava SQL Injection napad. |
| Slika 8 | SQL Injection – Brisanje rejtinga za poklon | False positive | Vrši se konkatencija celog broja(int), što ne omogućava SQL Injection napad. |
| Slika 9 | SQL Injection – Brisanje komentara za poklon | False positive | Vrši se konkatencija celog broja(int), što ne omogućava SQL Injection napad. |
| Slika 10 | SQL Injection – Brisanje tagova za poklon | False positive | Vrši se konkatencija celog broja(int), što ne omogućava SQL Injection napad. |
| Slika 11 | SQL Injection – Dohvatanje heširanog korisnika po korisničkom imenu | True Positive | Konkatencija stringa za kreiranje SQL upita. |

| | | | |
|----------|--|----------------------|---|
| Slika 12 | SQL Injection – Dohvatanje liste permisija na osnovu zadatog roleId | False positive | Vrši se konkatencija celog broja(int), što ne omogućava SQL Injection napad. |
| Slika 13 | SQL Injection – Pretraga osoba po zadatom parametru | True Positive | Konkatencija stringa za kreiranje SQL upita. |
| Slika 14 | SQL Injection – Dohvatanje osobe po id | True Positive | Konkatencija stringa za kreiranje SQL upita. |
| Slika 15 | SQL Injection – Brisanje osobe sa zadatim id | False positive | Vrši se konkatencija celog broja(int), što ne omogućava SQL Injection napad. |
| Slika 16 | SQL Injection – Ažuriranje osobe | True Positive | Konkatencija stringa za kreiranje SQL upita. |
| Slika 17 | SQL Injection – Kreiranje novog ili ažuriranje postojećeg rejtinga poklona | False Positive | Vrši se konkatencija celog broja(int), što ne omogućava SQL Injection napad. |

| | | | |
|----------|--|----------------------|--|
| Slika 18 | SQL Injection – Dohvatanje svih rejtinga za poklon sa zadatim id | True Positive | Konkatenacija stringa za kreiranje SQL upita. |
| Slika 19 | SQL Injection – Dohvatanje liste rola za korisnika sa zadatim roleId. | False Positive | Vrši se konkatenacija celog broja(int), što ne omogućava SQL Injection napad. |
| Slika 20 | SQL Injection – Dohvatanje korisnika po prosleđenom korisničkom imenu. | True Positive | Konkatenacija stringa za kreiranje SQL upita. |
| Slika 21 | SQL Injection – Validiranje kredencijala (korisničko ime i lozinka) | True Positive | Konkatenacija stringa za kreiranje SQL upita. |
| Slika 22 | SQL Injection – Brisanje korisnika iz tabele users na osnovu zadatog userId. | False Positive | Vrši se konkatenacija celog broja(int), što ne omogućava SQL Injection napad. |

| | | | |
|-------------|---------------------|----------------------|--|
| Slika 23-43 | e.printStackTrace() | True Positive | <p>Identifikovano je da upotreba e.printStackTrace() u kodu predstavlja sigurnosni rizik, označen kao 'True Positive'. Ovaj metod može nehotice otkriti osetljive informacije o unutrašnjoj strukturi sistema, uključujući nazive tabela i polja u bazi podataka, strukturu SQL upita, kao i detalje o korišćenim tehnologijama i njihovim verzijama. Ovo može dati potencijalnim napadačima uvid u moguće slabosti sistema. Preporučuje se umesto toga koristiti odgovarajući sistem za logovanje, poput LOG klase, koji omogućava kontrolisano i sigurno zapisivanje grešaka bez izlaganja osetljivih informacija.</p> |
|-------------|---------------------|----------------------|--|