Penetraciono testiranje

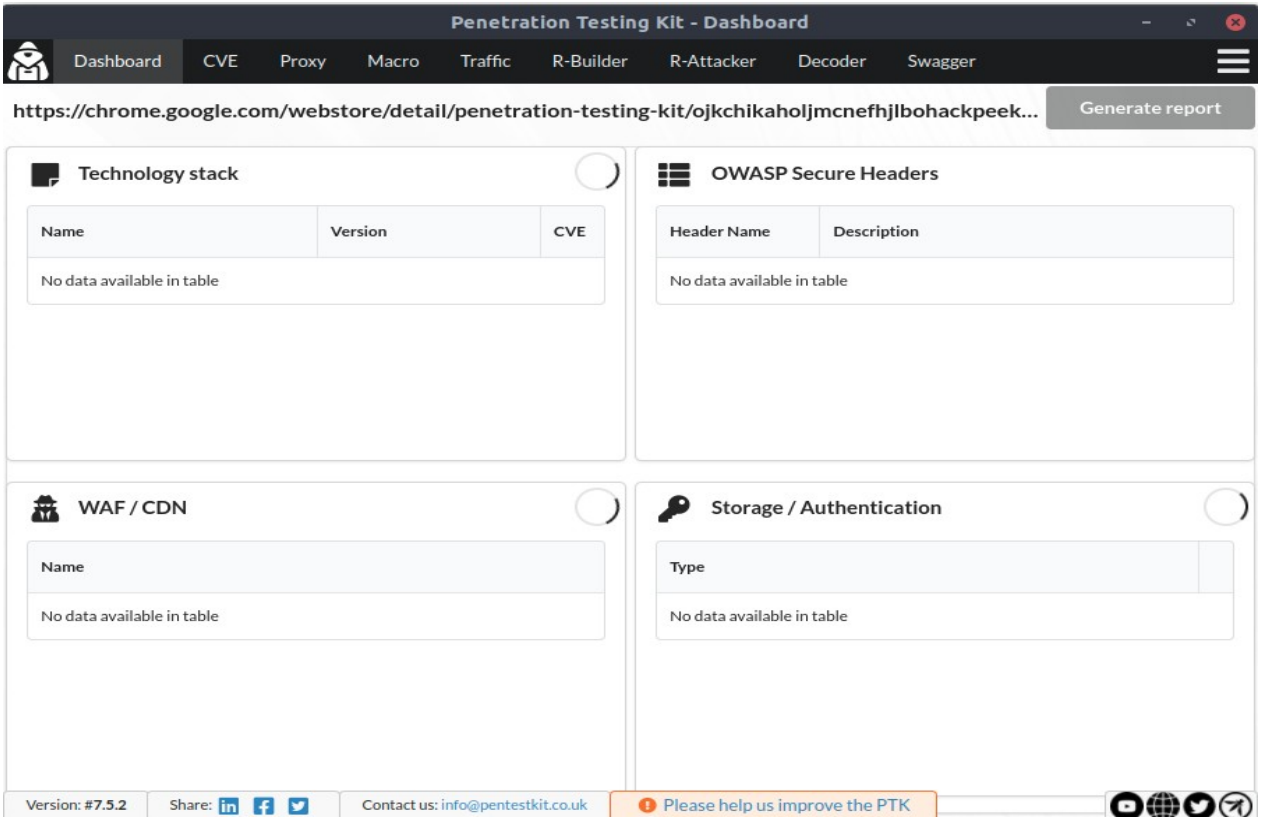
SEP

Tim 21

Authors:
Stevan Rašković E2-54/2021
Jelena Budiša E2-47/2021
Stefan Jokić E2-57/2021

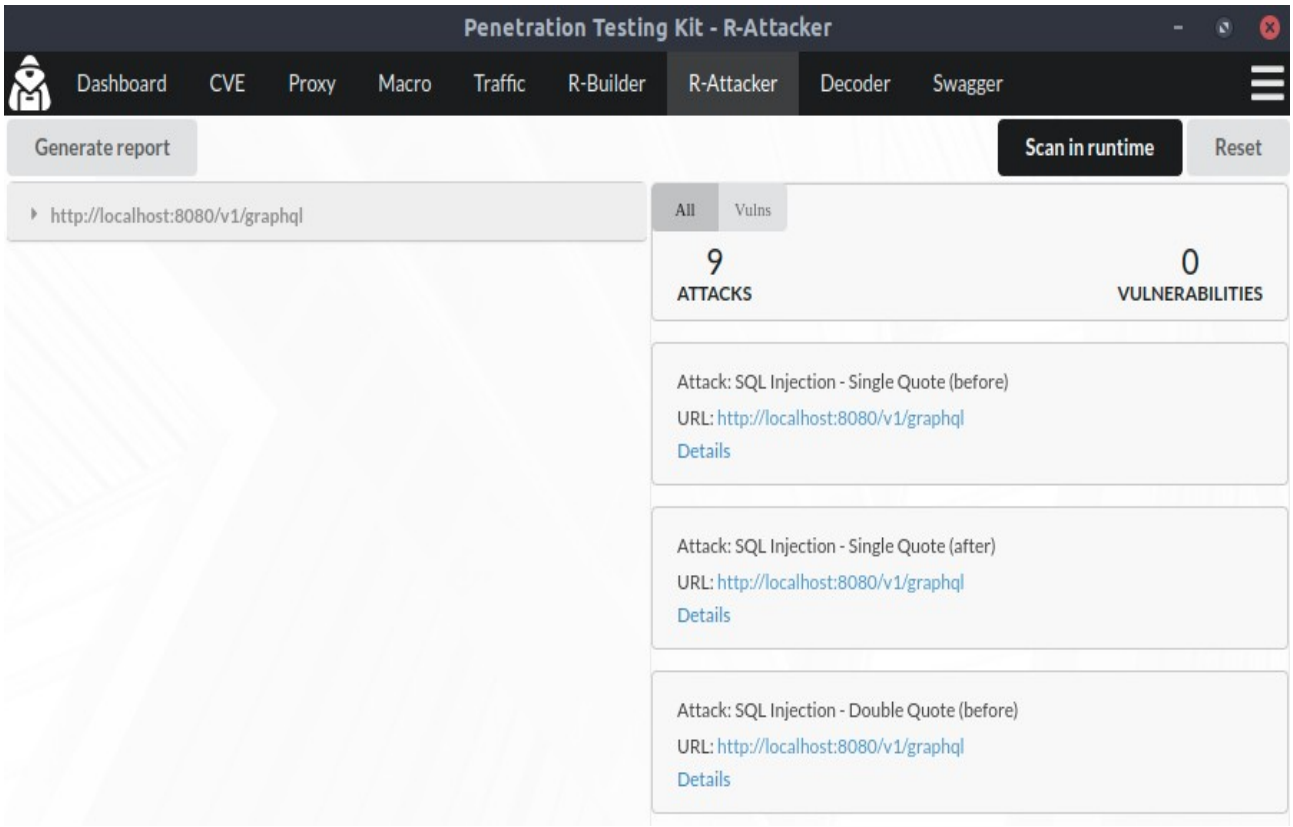
Penetration Testing Kit (PTK)

Penetration Testing Kit je ekstenzija u browseru zasnovana na *Wappalyzer NPM* modulu, koja proširuje mogućnosti *browser*-a i omogućava korisniku da izvrši penetraciono testiranje svoje *web* aplikacije. Takođe daje i uvid u karakterestike aplikacije i evidetentira saobraćaj podataka. Primer *PTK dashboard*-a se može videti na slici 1.



Slika 1. PTK Dashboard

Dva glavna *feature*-a ove ekstenzije su *R-Builder* i *R-Attacker*. Pomoću *R-Builder*-a je moguće ponovno slati zahteve, dok *R-Attacker* služi za izvršavanje napada na *web* aplikaciju i to napada poput, *XSS, SQL injection, OS Command injection*. Unutar *Proxy* funkcionalnosti se nalaze već okinuti zahtevi, koji se šalju *R-Attacker*-ru, kako bi ih on skenirao i napravio zahteve za napad (primer slika 2).

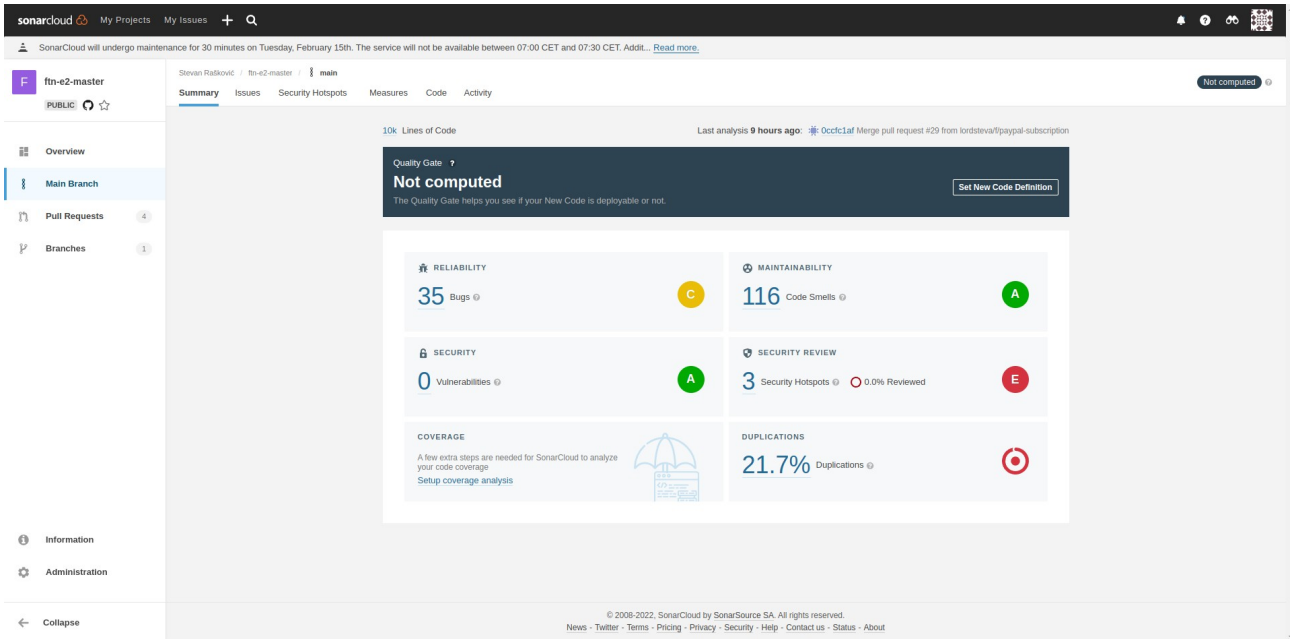


Slika 2. Napadi R-Attacker-a za određeni zahtev

Napadi koji su se koristili za penetraciono testiranje naše aplikacije su sledeći:

- *SQL Injection Single Quote before*
- *SQL Injection Single Quote after*
- *SQL Injection Double Quote before*
- *SQL Injection Double Quote after*
- *XSS - Unfiltered <script> tag*
- *XSS - Script tag after noscript tag*
- *XSS - Svg tag with animation event*
- *XSS - Img onerror*
- *OS Command Injection - Unix File (cat passwd)*
- *JWT None Algorithm*

U ovom folderu se takođe nalaze primeri napada, kao i odgovori naše aplikacije u *HTML* formatu. Takođe primetljivo je da ovaj alat nije uspeo da otkrije slabosti naše aplikacije. Ovu činjenicu potvrđuje i *Sonar Cloud* (slika 3), koji je korišćen za kvalitet koda.



Slika 3. Izveštaj Sonar Cloud-a za naš repozitorijum