**Burp Suite**

Burp Suite je popularan softwerski alat koji se koristi za testiranje sigurnosti web aplikacija. Razvio ga je *PortSwigger Web Security* i koristi ga veliki broj sigurnosnih stručnjaka i istraživača. Alat se sastoji od nekoliko modula koji se koriste za testiranje različitih aspekata web aplikacije. Navedeni moduli uključuju:

* ***Proxy -*** on presreće *HTTP/HTTPS* promet između klijenta i poslužitelja i omogućuje izmjenu zahtjeva i odgovora onome koji testira api-eve.

* ***Scanner -*** ovaj modul automatski testira web aplikacije u potrazi za ranjivostima kao što su SQL injections, cross site scripting(XSS) i slično.

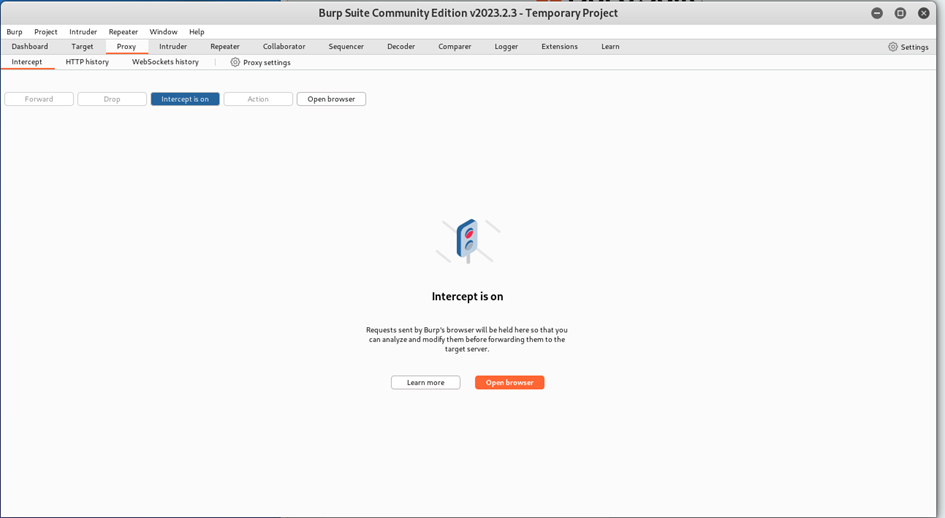
* ***Intruder*** - koristi se za automatizaciju procesa slanja velikog broja zahtjeva meti, pri čemu svaki zahtjev koristi drugu vrijednost za određeni parametar. Često se koristi pri provjeri kod testiranja unosa aplikacije.
* ***Repeater-*** omogućuje testeru izmjenu i slanje pojedinačnih zahtjeva, što ga čini korisnim za testiranje određenih ranjivosti i funkcionalnosti.

* ***Sequencer-*** analizira nasumične sesije tokena ili drugih podataka koje generira aplikacija i može se koristititi za prepoznavanje slabosti u generiranju nasumičnosti aplikacije.

* ***Decoder-*** omogućuje testeru dekodiranje kodiranih podataka, kao što su base64 ili URL kodirani podatci.

Koristiti ćemo alat za testiranje api-eva na našoj Openshift okolini.

Izgled sučelja:



**Slika 1.** *Burp Suite sučelje*