CARNET

OWASP ZAP

CERT.hr-PUBDOC-2018-11-368

CERT.hr

Sadržaj

Ovaj dokument izradio je Laboratorij za sustave i signale Zavoda za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

1 Uvod

Već duže vrijeme raste broj web aplikacija te se značajan dio našeg privatnog i poslovnog života seli na web. Paralelno tome, raste i broj napada na web aplikacije te su posljedice takvih napada sve značajnije. Kako bi povećali razinu sigurnosti web aplikacija, jedan koristan postupak je ispitivanje njihove sigurnosti iz perspektive napadača.

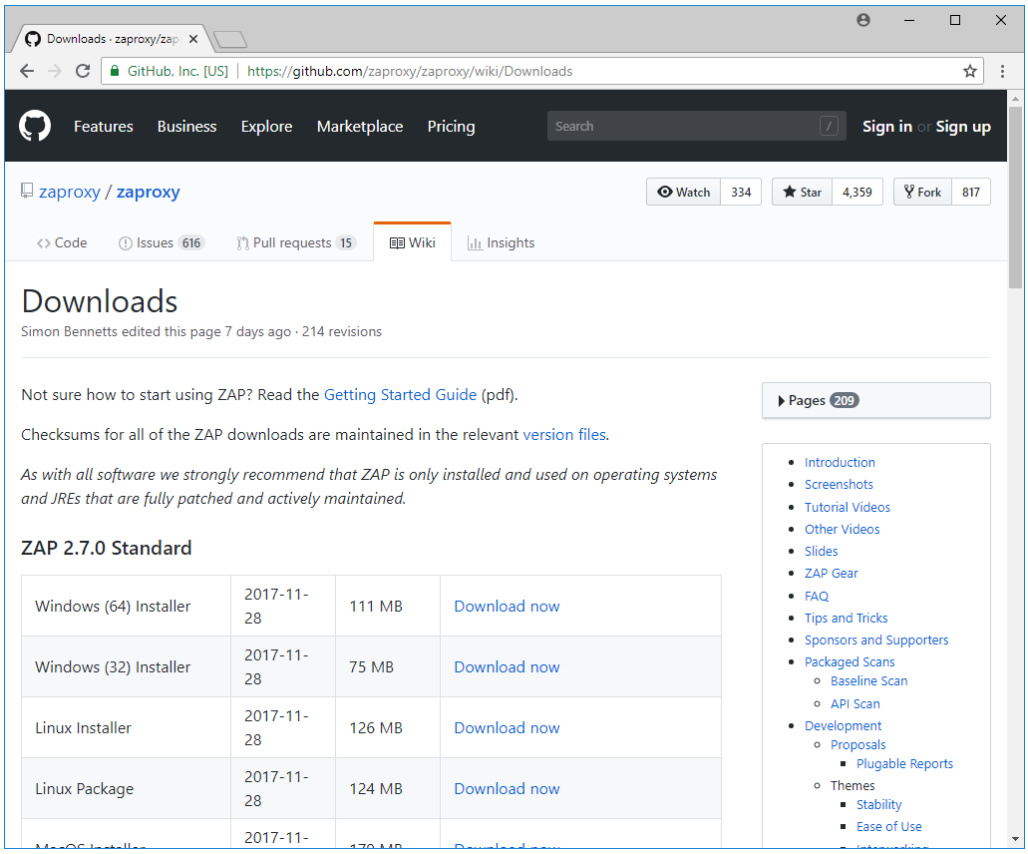
OWASP Zed Attack Proxy, kraće OWASP ZAP ili samo ZAP, jedan je od najčešće korištenih slobodnih (eng. *free and open source*) alata za ispitivanje sigurnosti web aplikacija. U tu svrhu ga koriste programeri aplikacija, ali i sigurnosni stručnjaci. OWASP ZAP je u suštini HTTP posrednik. U mreži, HTTP posrednik (eng. *HTTP proxy*) se nalazi između HTTP klijenta i poslužitelja, a njegova zadaća je da prenosi, analizira te po potrebi i mijenja HTTP promet koji prolazi kroz njega. U prethodnom dokumentu Nacionalnog CERT-a opisan je sličan alat, Telerik Fiddler – no njegova je glavna primjena ispravljanje grešaka (eng. *debugging*), dok je OWASP ZAP usmjeren na sigurnost.

Kao što i ime kaže, iza ovog alata stoji neprofitna organizacija OWASP (Open Web Application Security Project) koja uz pomoć velikog broja volontera razvija slobodno dostupnu dokumentaciju, alate i metodologije u području web sigurnosti. OWASP ZAP dostupan je na operacijskim sustavima Windows, Linux i macOS. Njegova trenutna inačica je 2.7 te će na toj inačici biti i prikazani primjeri u nastavku dokumenta.

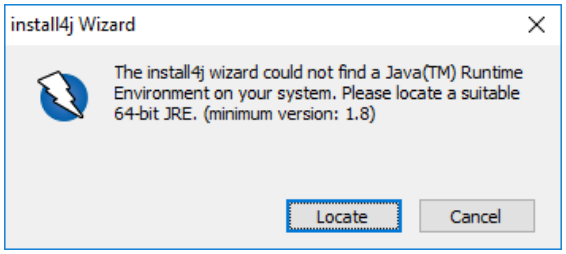
2 Instalacija alata OWASP ZAP

U ovom dokumentu bit će objašnjen instalacijski postupak na operacijskom sustavu Windows 10, no postupak je analogan i na ostalim inačicama sustava Windows. Za rad alata OWASP ZAP potrebno je instalirati okruženje za izvođenje programskog jezika Java (eng. *Java Runtime Environment*) koje je moguće preuzeti ovdje. Potrebno je preuzeti odgovarajuću inačicu – u ovom primjeru 64-bitna inačica za operacijski sustav Windows.

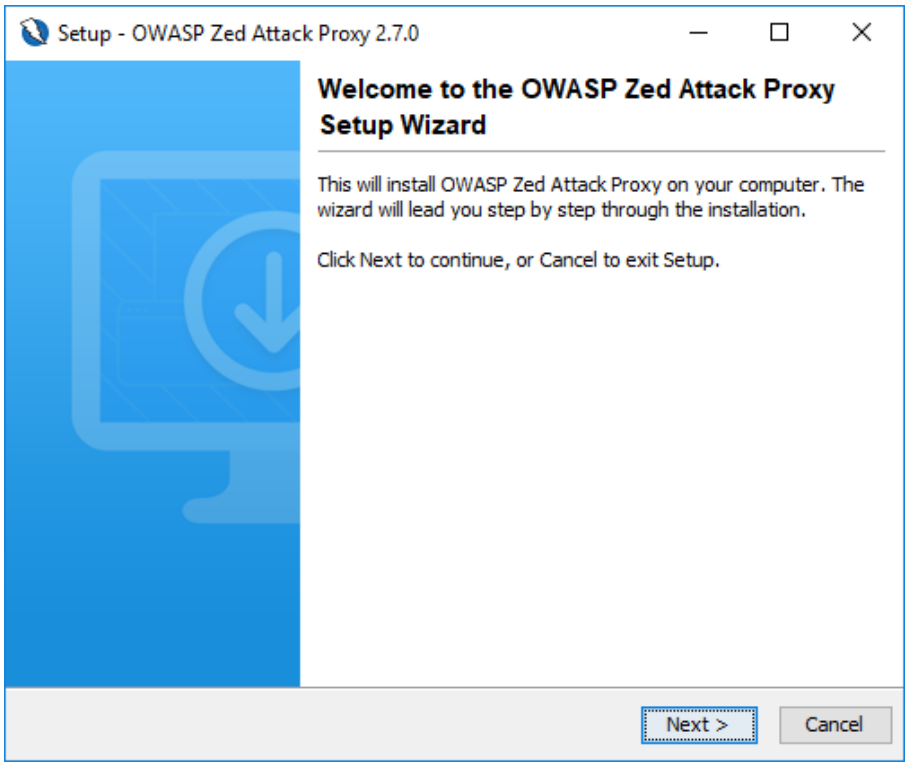
Najnoviju inačicu instalacijske datoteke alata ZAP moguće je preuzeti sa službene web stranice na ovoj poveznici. Pritiskom na poveznicu s natpisom ***Download now*** za odgovarajuću sustav, u ovom slučaju ***Windows (64) Installer***, počinje preuzimanje instalacijske datoteke.



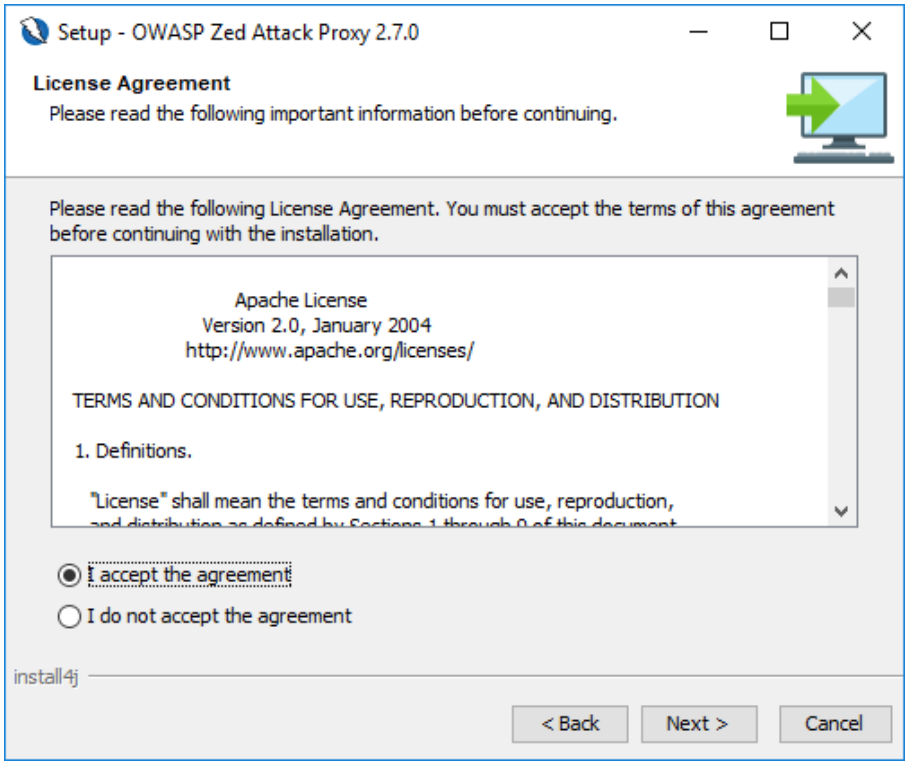
Nakon pokretanja preuzete datoteke, ako instalacijski program ne uspije pronaći okruženje za izvođenje programskog jezika Java, prikazat će se poruka s donje slike. U tom slučaju, potrebno je u izborniku datoteka odabrati lokaciju okruženja za izvođenje programskog jezika Java ili instalirati ga, ako to već nije napravljeno.



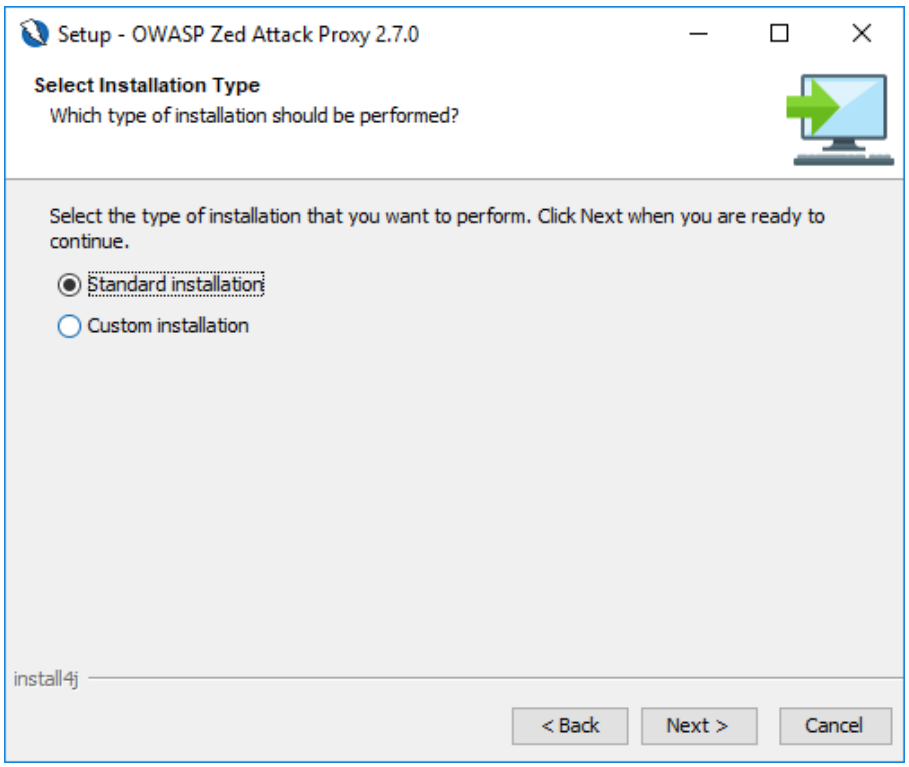
Nakon toga se otvara čarobnjak za instalaciju alata OWASP ZAP. Pritiskom na tipku ***Next*** prelazi se na sljedeći korak.



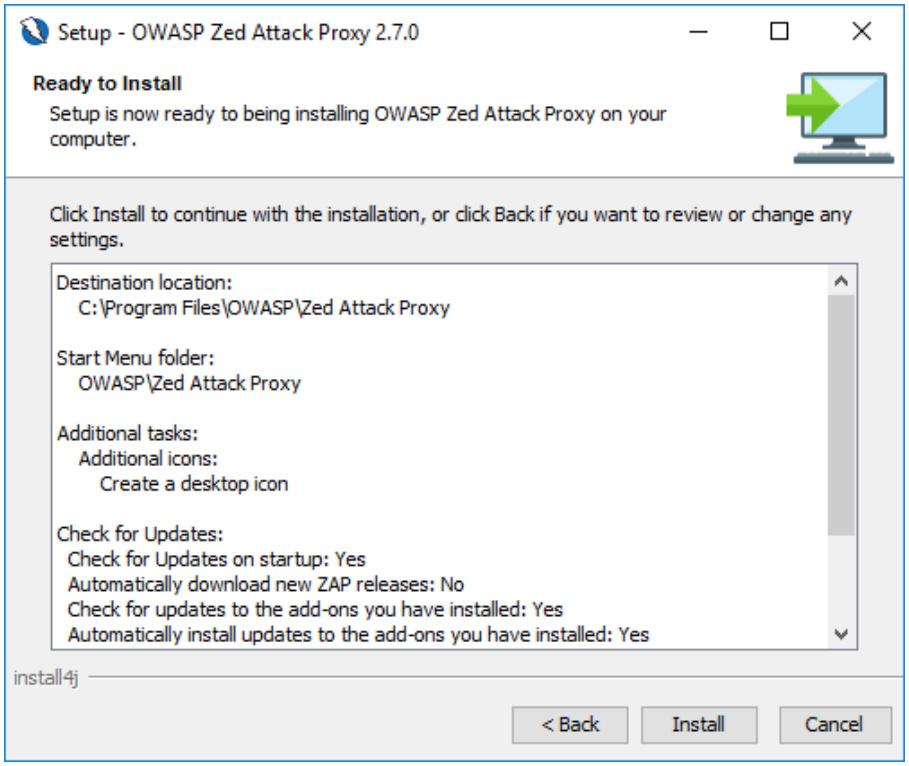
U ovom je koraku prikazana licenca koju koristi OWASP ZAP. Potrebno je odabrati ***I accept the agreement*** te pritisnuti ***Next*** za sljedeći korak instalacijskog postupka.



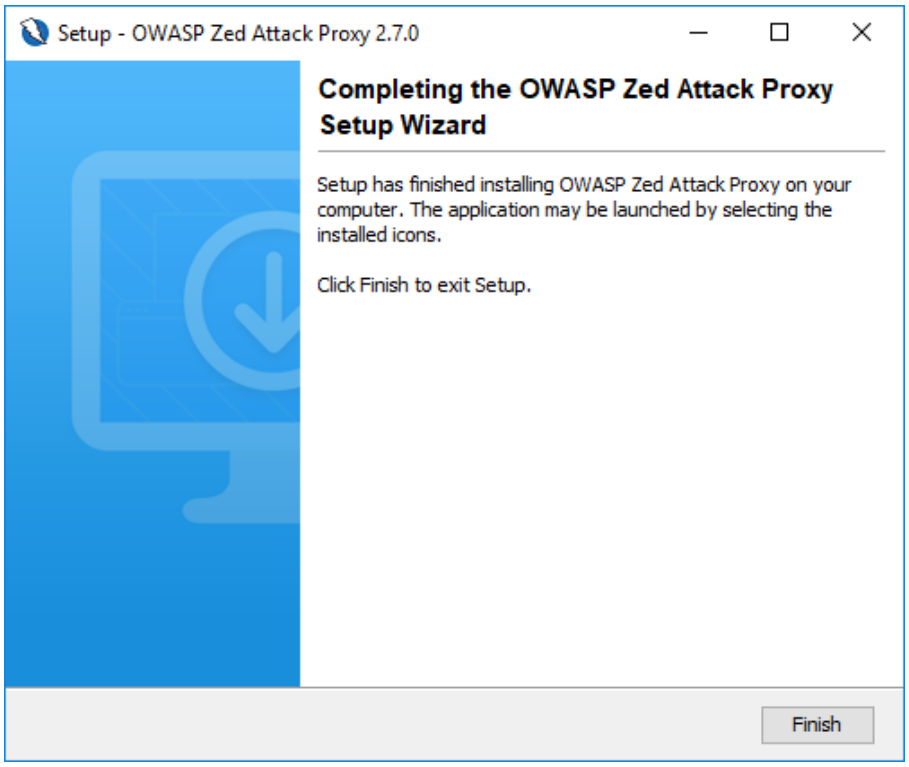
Zatim je moguće odabrati standardni ili prilagođeni instalacijski postupak. Standardne postavke su u ovom slučaju dovoljne pa je potrebno ostaviti odabranu opciju ***Standard installation*** te pritisnuti tipku ***Next*** za sljedeći korak.



U ovom koraku je moguće provjeriti postavke instalacije. Ukoliko je sve u redu, pritiskom na ***Install*** započinje postupak instalacije datoteka na računalo korisnika.

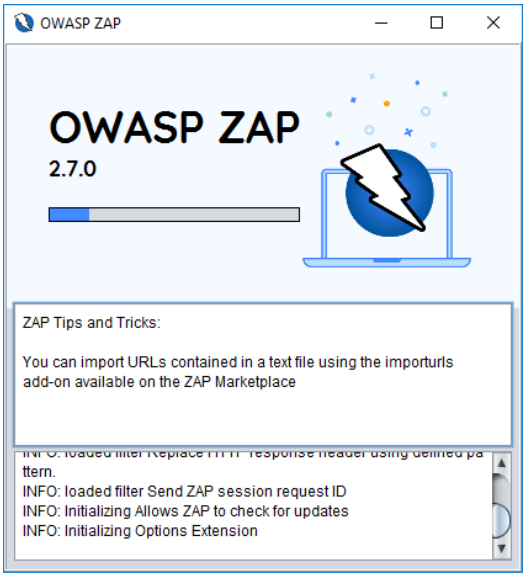


Nakon što instalacija završi, prikazuje se zadnji korak čarobnjaka. Klikom na ***Finish*** instalacijski čarobnjak se gasi te je sada moguće koristiti alat OWASP ZAP.

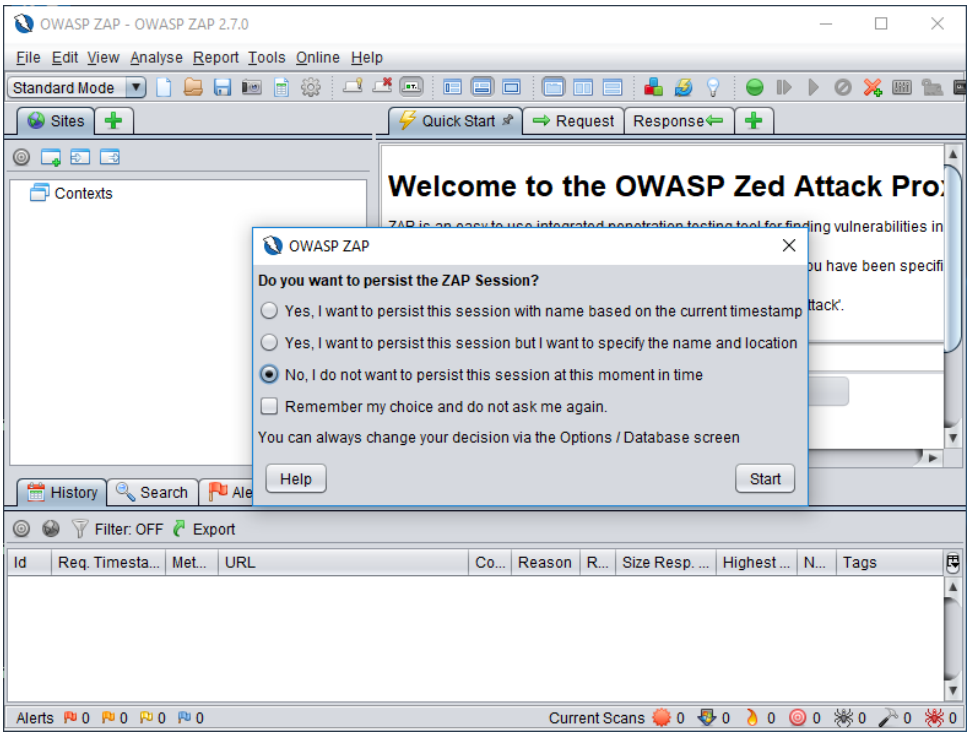


3 Korištenje alata OWASP ZAP

Prečicu na izvršnu datoteku alata OWASP ZAP moguće je naći na radnoj površini sustava ili pretraživanjem u glavnom izborniku. Pri pokretanju OWASP ZAP-a prvo se otvara prozor u kojem je prikazan napredak otvaranja alata. Zbog složenosti alata i velikog broja komponenti, ovaj postupak može potrajati i do minutu na sporijim računalima.



Nakon uspješnog otvaranja alata prikazuje se prozor u kojemu se može odabrati treba li ovu sjednicu korištenja alata pohraniti na računalo ili ne. U ovom slučaju to nije potrebno pa će biti odabrano *No, I do not want to persist this session at this moment in time* te će biti pritisnuta tipka ***Start***.

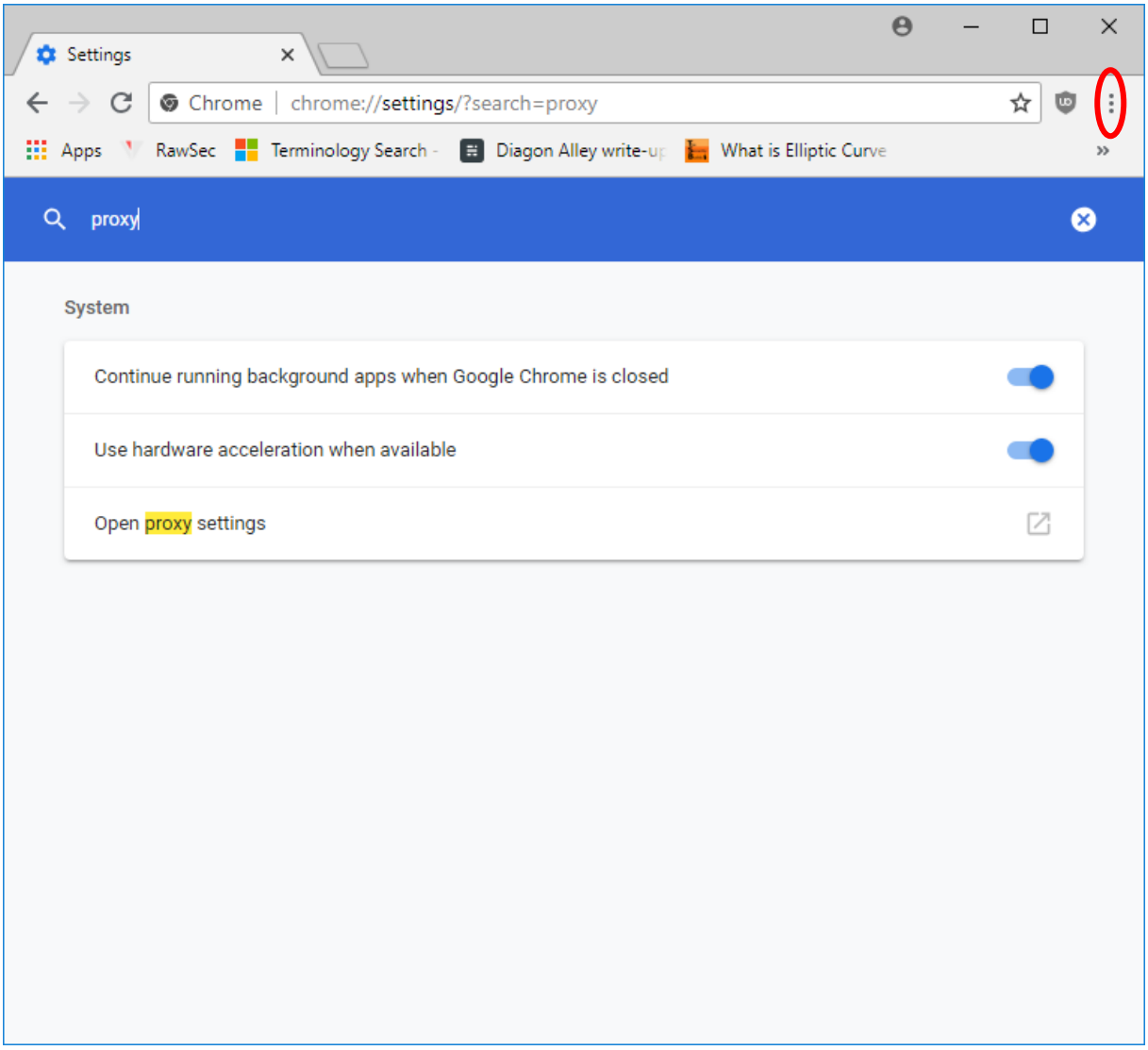


Sada se otvorio glavni prozor alata OWASP ZAP te je moguće koristiti njegove značajke, primjerice presretanje HTTP prometa ili ispitivanje sigurnosti web aplikacija.

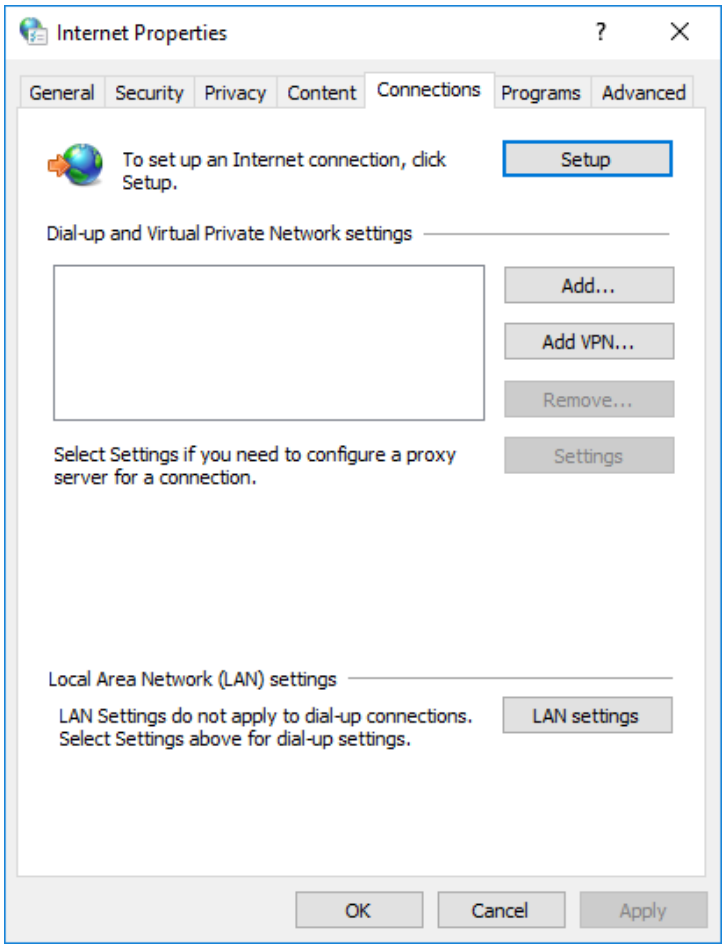
3.1 Konfiguracija HTTP posrednika (eng. *HTTP proxy*)

Kako bi HTTP promet bio usmjeren preko posrednika, tj. preko alata OWASP ZAP, potrebno je izmijeniti određene postavke u web pregledniku. Po pretpostavljenim (eng. *default*) vrijednostima, OWASP ZAP očekuje promet na priključku (eng. *port*) 8080. Tipično, u postavkama web preglednika moguće je ili ručno konfigurirati korištenje posrednika ili koristiti postavke posrednika operacijskog sustava. U ovom primjeru bit će opisano postavljanje posrednika u web pregledniku Google Chrome na operacijskom sustavu Windows 10.

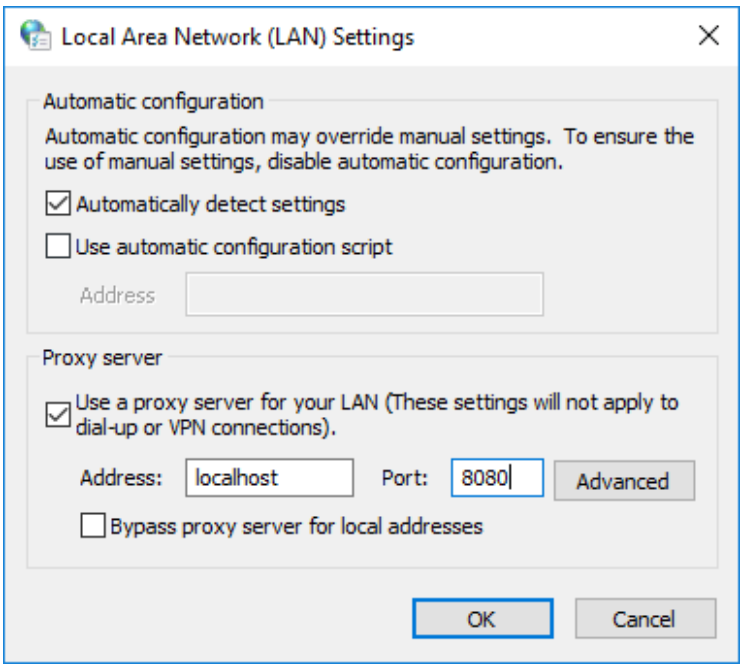
U glavnom izborniku preglednika Google Chrome (ikona s tri točkice u gornjem desnom kutu) prvo je potrebno odabrati ***Settings***. Tada je moguće pretražiti postavke pomoću riječi *proxy* te pritisnuti na ***Open proxy settings***.



Kako bi se konfiguriralo korištenje posrednika potrebno je pritisnuti ***Lan settings***.



Potrebno je označiti *Use proxy server for your LAN*, pod ***Address*** upisati **localhost** i pod ***port*** upisati **8080**.

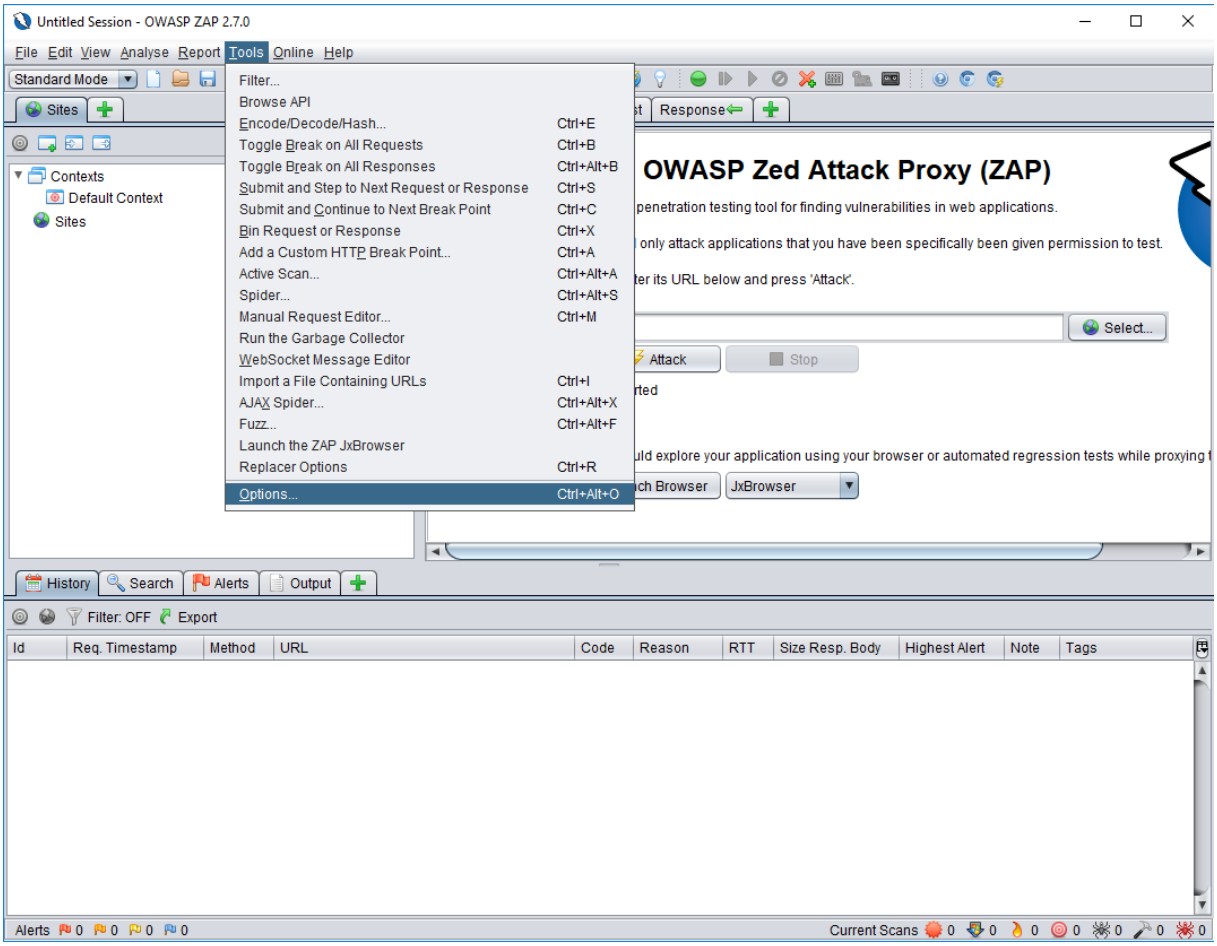


Ovakva konfiguracija dovoljna je za presretanje nezaštićenog HTTP prometa. No danas se sve više koristi HTTPS protokol koji šifrira i štiti mrežni promet između klijenta i poslužitelja. Kada se koristi HTTPS protokol, mrežni promet je zaštićen tako da ga u pravilu nitko ne može presresti – ni napadač, ali ni korisnik koji pokušava legitimno koristiti OWASP ZAP.

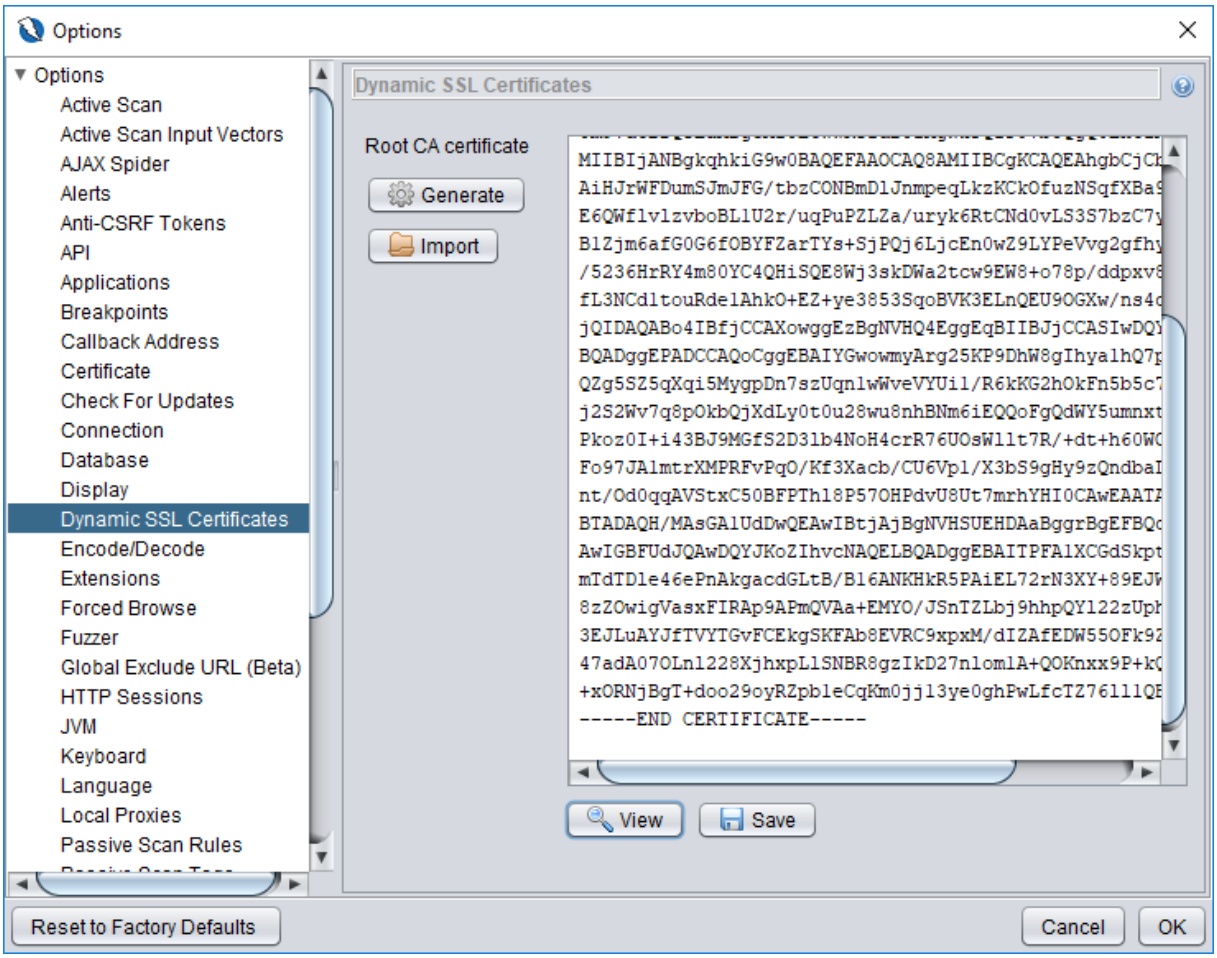
3.2 Konfiguracija za presretanje HTTPS prometa

Kako bi pomoću OWASP ZAP-a ipak mogli presretati mrežni promet zaštićen HTTPS protokolom, potrebno je napraviti dodatne korake za konfiguraciju web preglednika odnosno operacijskog sustava. Točnije, potrebno je uvesti TLS certifikat koji je generiran pomoću OWASP ZAP-a. Korištenjem tog certifikata OWASP ZAP može uspješno presretati HTTPS promet.

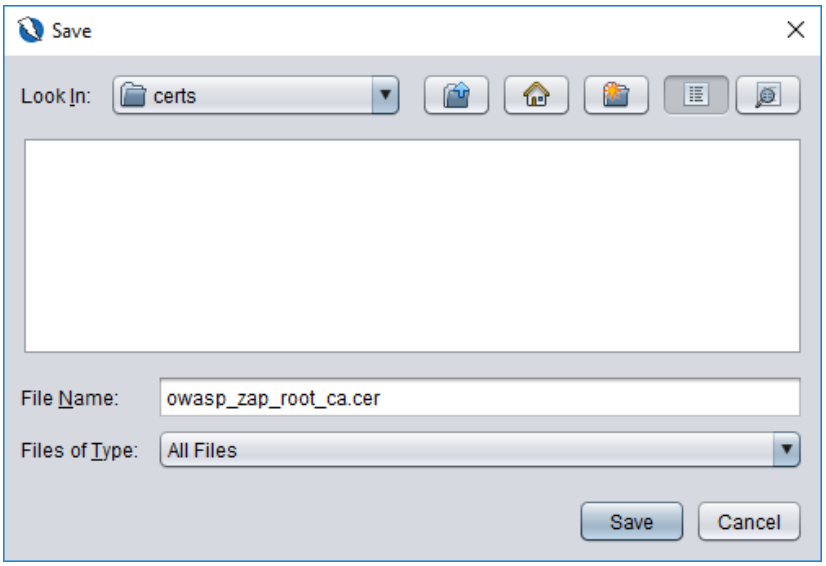
Za konfiguraciju presretanja HTTPS prometa, potrebno je prvo u glavnom izborniku alata OWASP ZAP odabrati ***Tools*** pa zatim ***Options***, kao što je prikazano na donjoj slici.



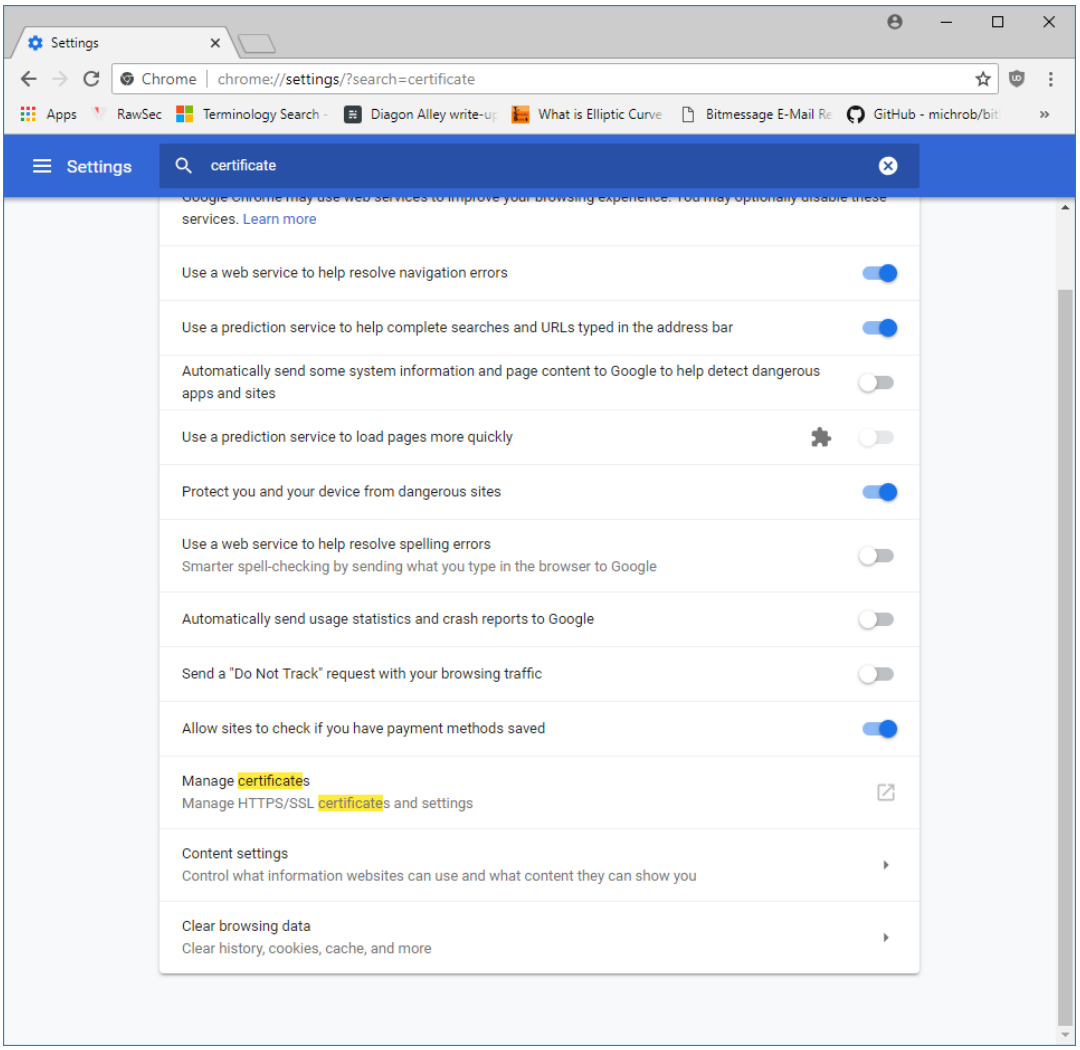
Zatim je u lijevom popisu prozora koji se upravo otvorio potrebno odabrati ***Dynamic SSL Certificates*** te pritisnuti tipku ***Generate*** kako bi se izradio certifikat.



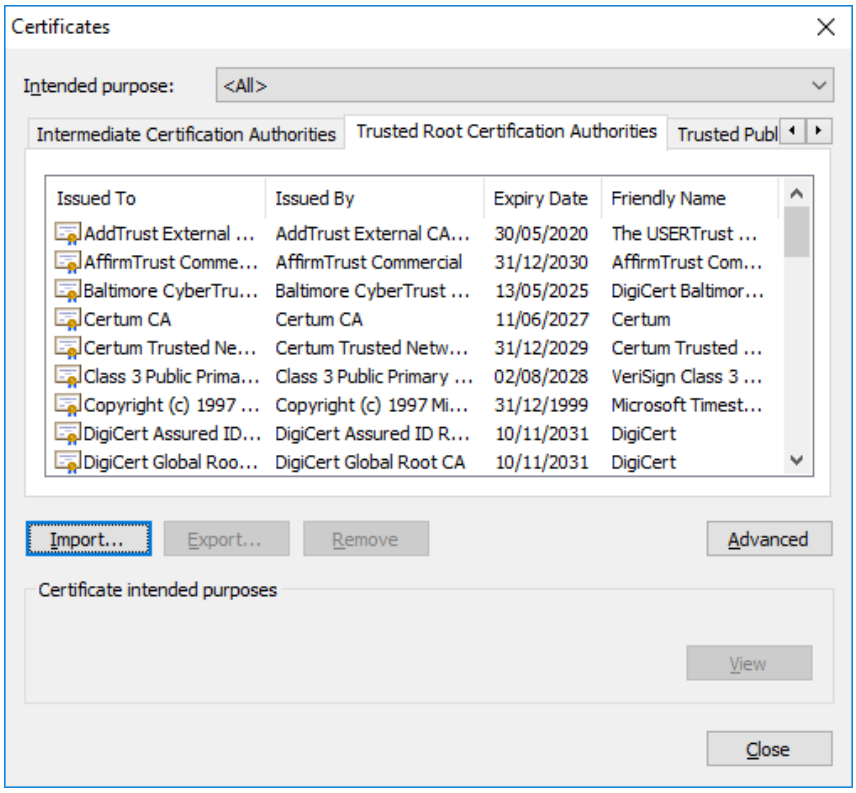
Zatim treba odabrati ***Save*** kako bi certifikat bio pohranjen u datoteku na računalu korisnika.



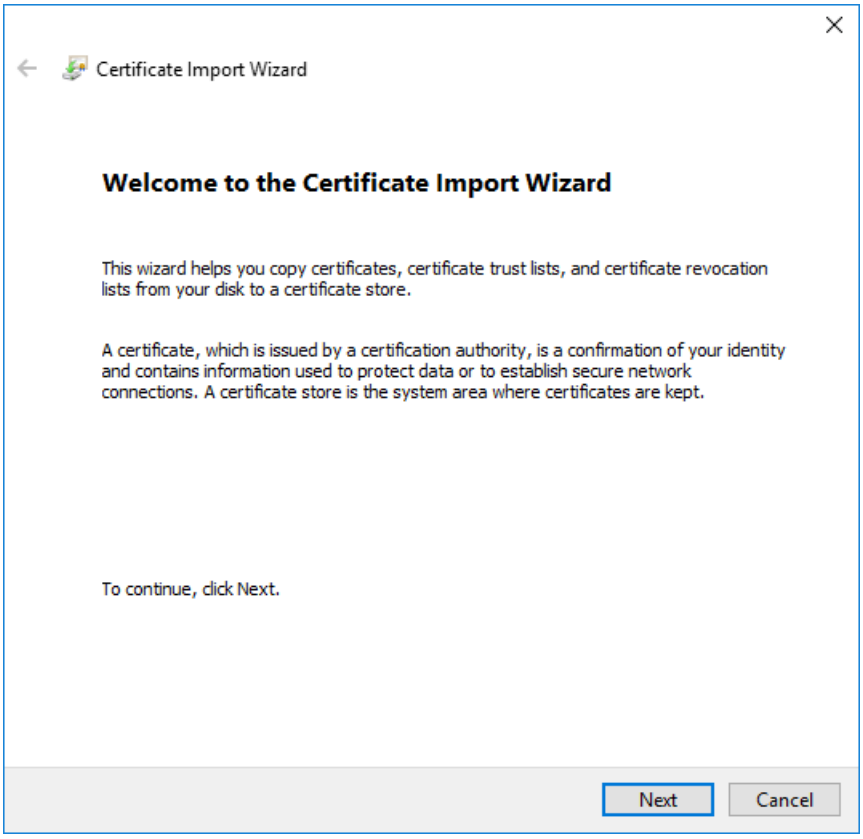
Nakon što je datoteka s certifikatom pohranjena na računalo, taj certifikat je potrebno uvesti u operacijski sustav tj. web preglednik. I u ovom primjeru korišten je web preglednik Google Chrome te operacijski sustav Windows 10. U postavkama preglednika Google Chrome moguće je pretražiti pojam *certificate* te zatim pritisnuti na ***Manage certificates*** kako bi se otvorila aplikacija za upravljanje certifikatima.



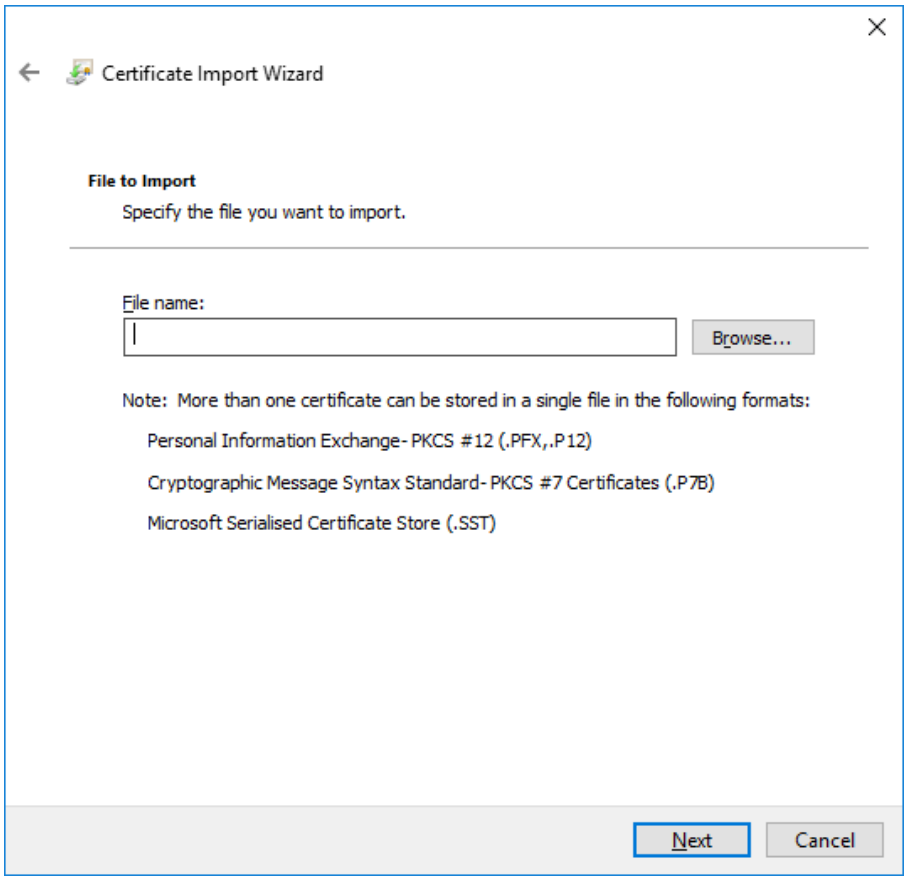
Otvaranjem kartice ***Trusted Root Certificate Authorities*** u otvorenom prozoru moguće je vidjeti postojeće certifikate te na računalo uvesti certifikat OWASP ZAP-a. Čarobnjak za pokretanje uvoza certifikata otvara se pritiskom na tipku ***Import***.



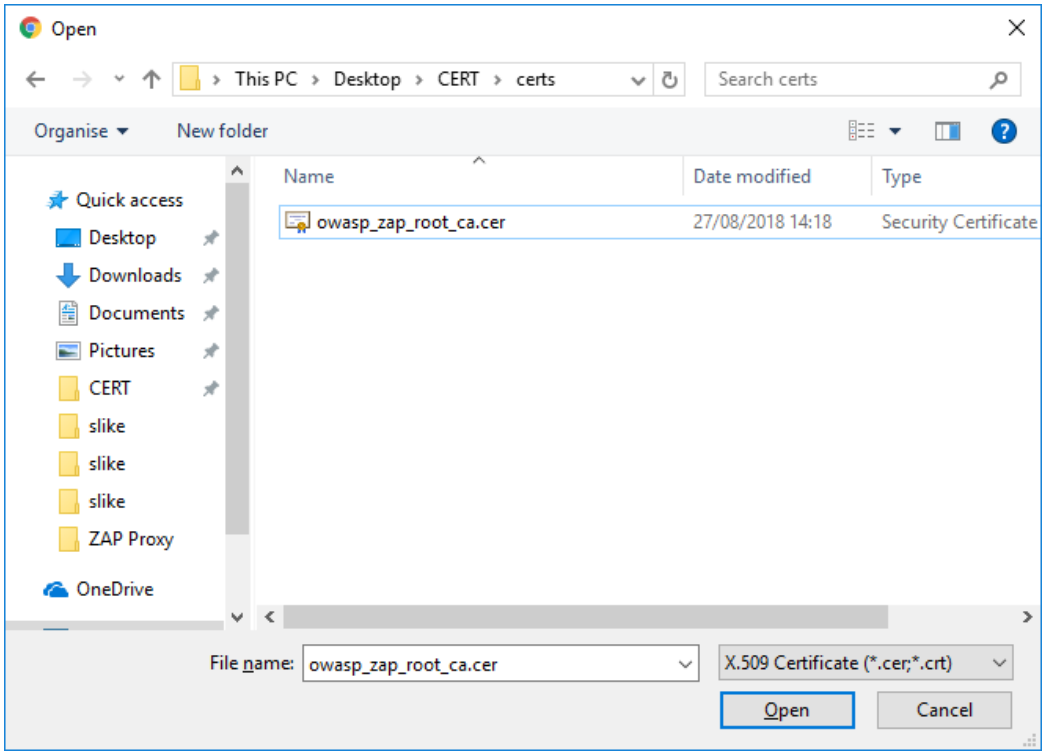
U čarobnjaku za uvoz certifikata potrebno je pritisnuti ***Next*** za sljedeći korak.



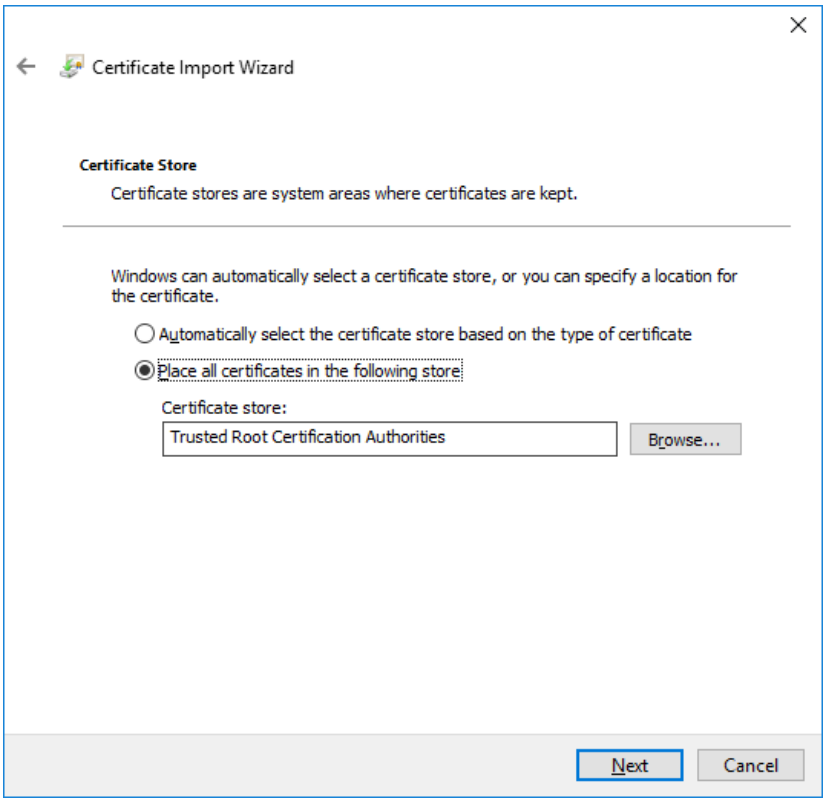
Sada je klikom na tipku ***Browse*** potrebno odabrati datoteku s certifikatom kojega je generirao OWASP ZAP.



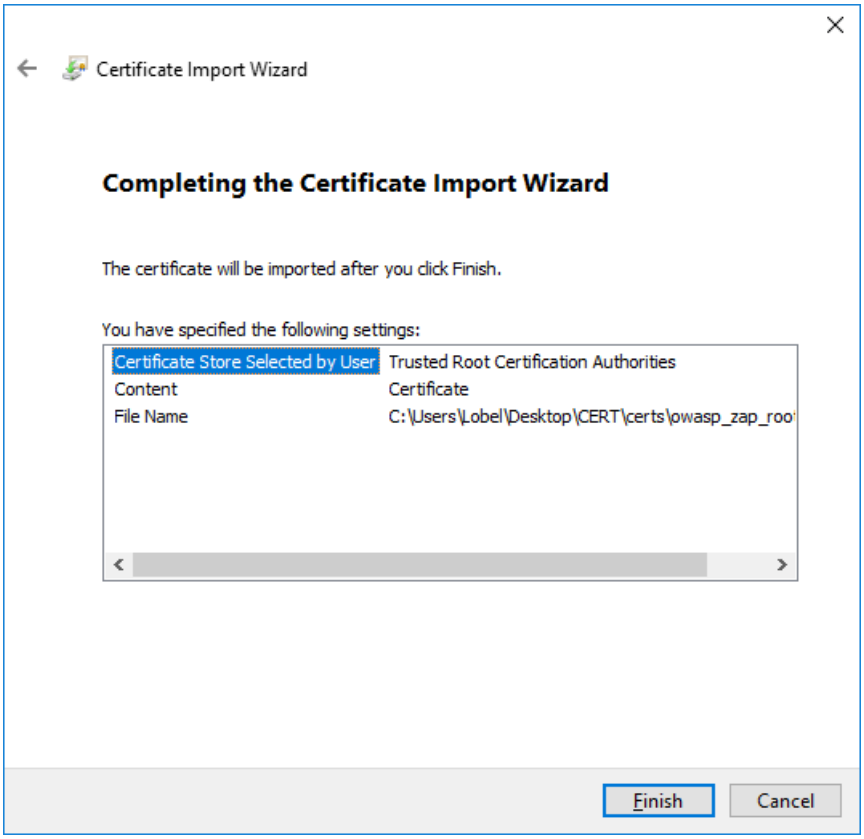
Nakon odabira datoteke potrebno je pritisnuti **Open** kako bi se zatvorio prozor za odabir datoteke te ***Next*** za sljedeći korak.



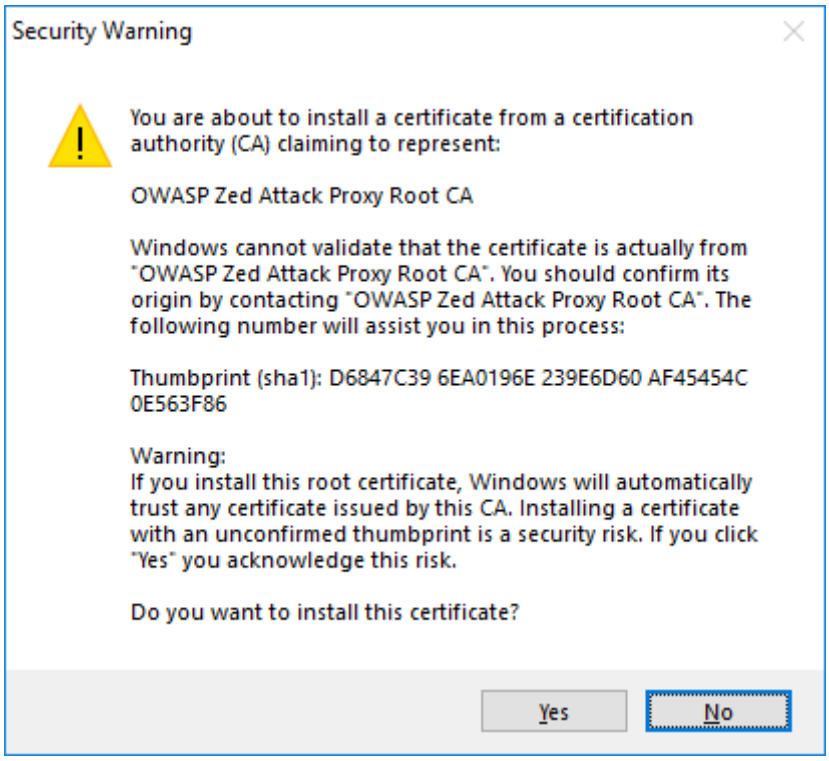
U ovom koraku nije potrebno ništa mijenjati, dovoljno je pritisnuti ***Next***.



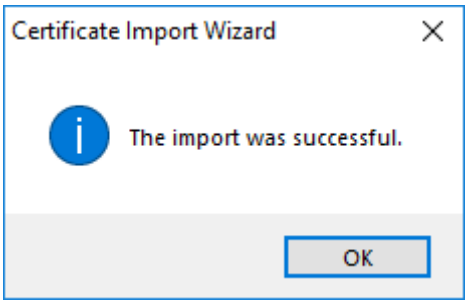
Sada se prikazuje zadnji korak čarobnjaka u kojemu su ispisane sve odabrane postavke te je pritiskom na tipku ***Finish*** potrebno završiti postupak uvoza certifikata.



Pojavljuje se prozor s upozorenjem da na računalo pokušavamo instalirati certifikat kojemu sustav Windows ne može potvrditi porijeklo. Kako je taj certifikat maloprije generiran alatom OWASP ZAP, možemo mu vjerovati te će se pritiskom na tipku ***Yes*** certifikat instalirati na računalo.



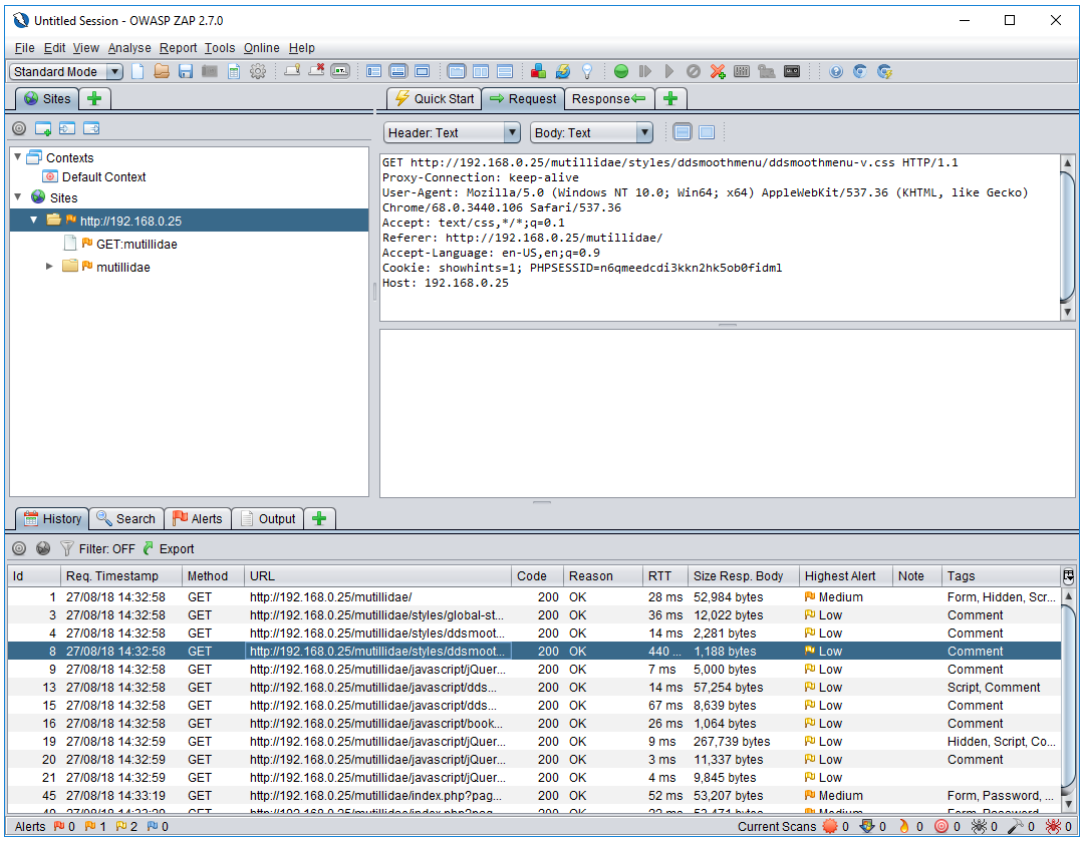
Sada je prikazana poruka u kojoj piše da je uvoz certifikata uspješan te je nakon ovoga moguće presretati HTTPS promet alatom OWASP ZAP.



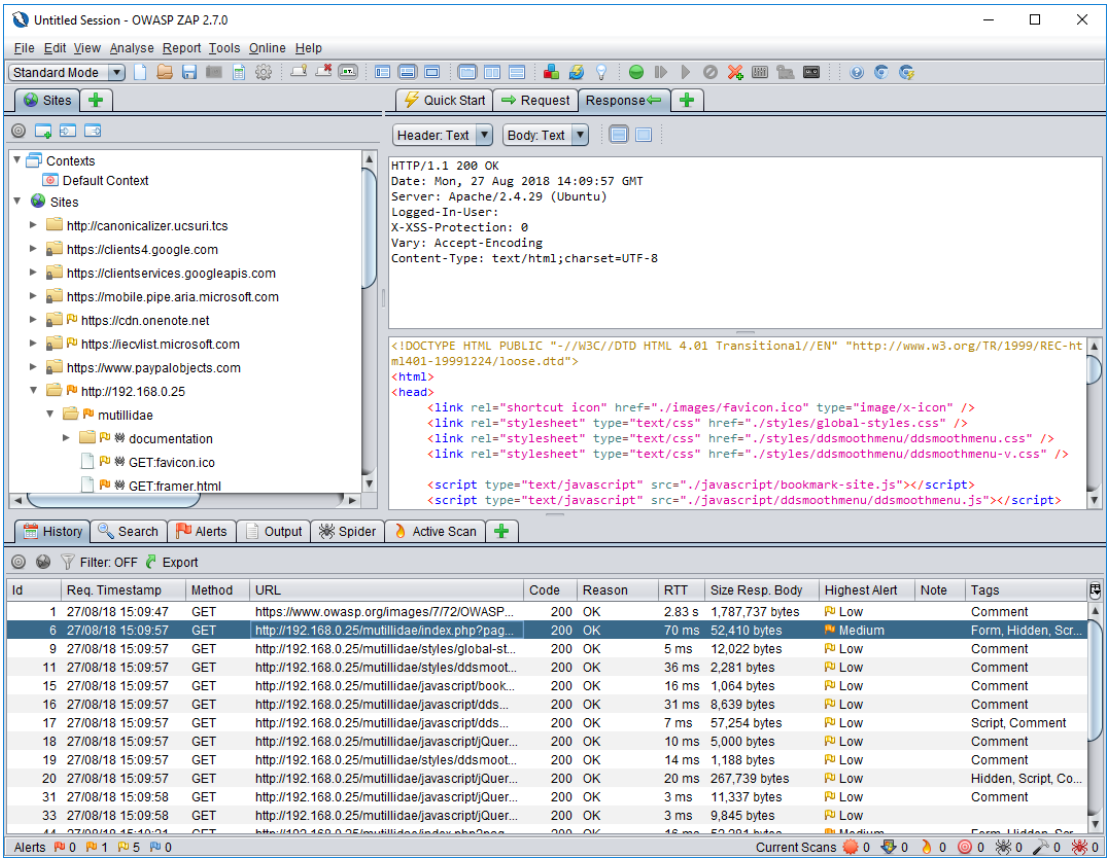
3.3 Korištenje OWASP ZAP HTTP posrednika

Nakon prethodne konfiguracije, otvaranjem web stranica u pregledniku, automatski se bilježe te prikazuju HTTP zahtjevi i odgovori u sučelju alata OWASP ZAP.

U donjem dijelu prozora u kartici ***History*** nalazi se popis svih HTTP zahtjeva. Dvoklikom na bilo koji zahtjev prikazuje se njegov sadržaj u kartici ***Request*** u gornjem desnom dijelu prozora, kao što je prikazano na sljedećoj slici.

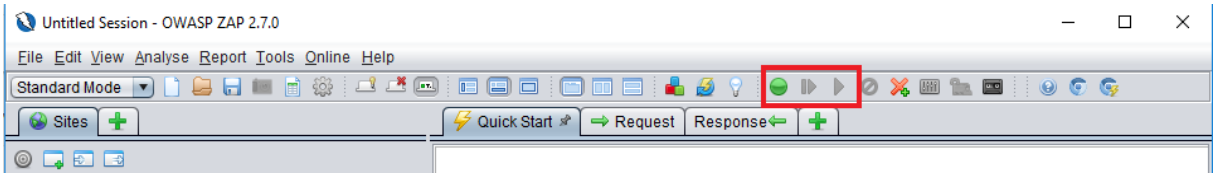


Osim zahtjeva, moguće je vidjeti i sadržaj HTTP odgovora klikom na karticu ***Response***. U gornjem dijelu kartice nalaze se zaglavlja, dok je u donjem dijelu tijelo HTTP odgovora.

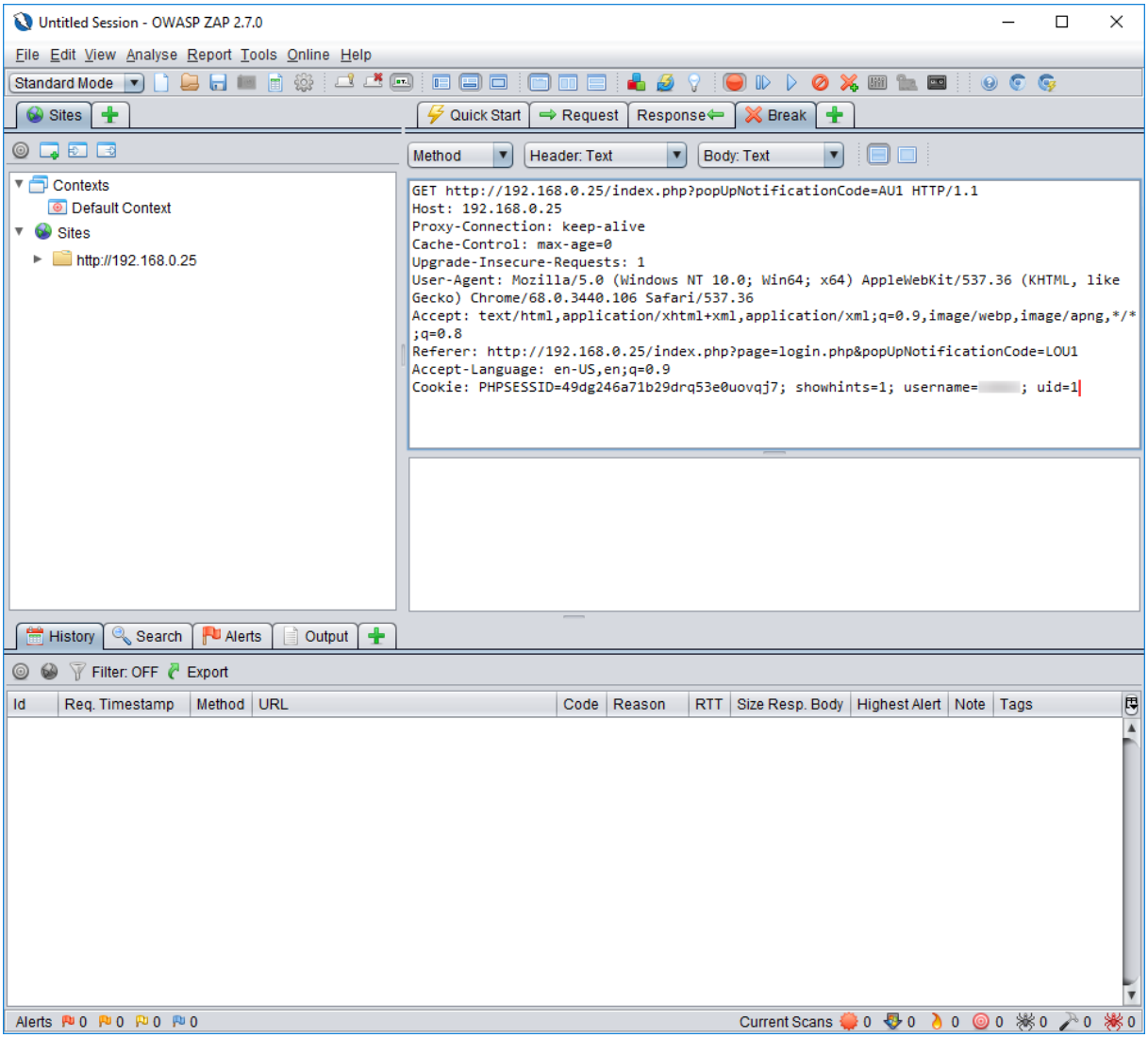


Mijenjanje HTTP zahtjeva jedna je od glavnih značajki OWASP ZAP-a. Mijenjanje zahtjeva izrazito je korisno za ispitivanje funkcionalnosti i sigurnosti web aplikacija. OWASP ZAP-om moguće je izmijeniti bilo koji dio HTTP zahtjeva, od primjerice HTTP kolačića (eng. *cookies*) do podataka poslanih u tijelu zahtjeva.

Osnovne tipke za rad s presretanjem i izmjenom HTTP zahtjeva nalaze se u alatnoj traci pri vrhu sučelja OWASP ZAP-a. Tri ikone koje će biti potrebne za ovu funkcionalnost označene su na donjoj slici.



Klikom na zeleni krug (prvu ikonu s lijeva), krug poprima crvenu boju. To označava da sada OWASP ZAP zaustavlja svaki HTTP zahtjev kako bi ga bilo moguće izmijeniti prije slanja poslužitelju. Primjerice, nakon pritiska na zeleni krug, otvaranje neke web stranice (u web pregledniku) će u sučelju OWASP ZAP-a prikazati zaustavljeni zahtjev u kartici ***Break***.



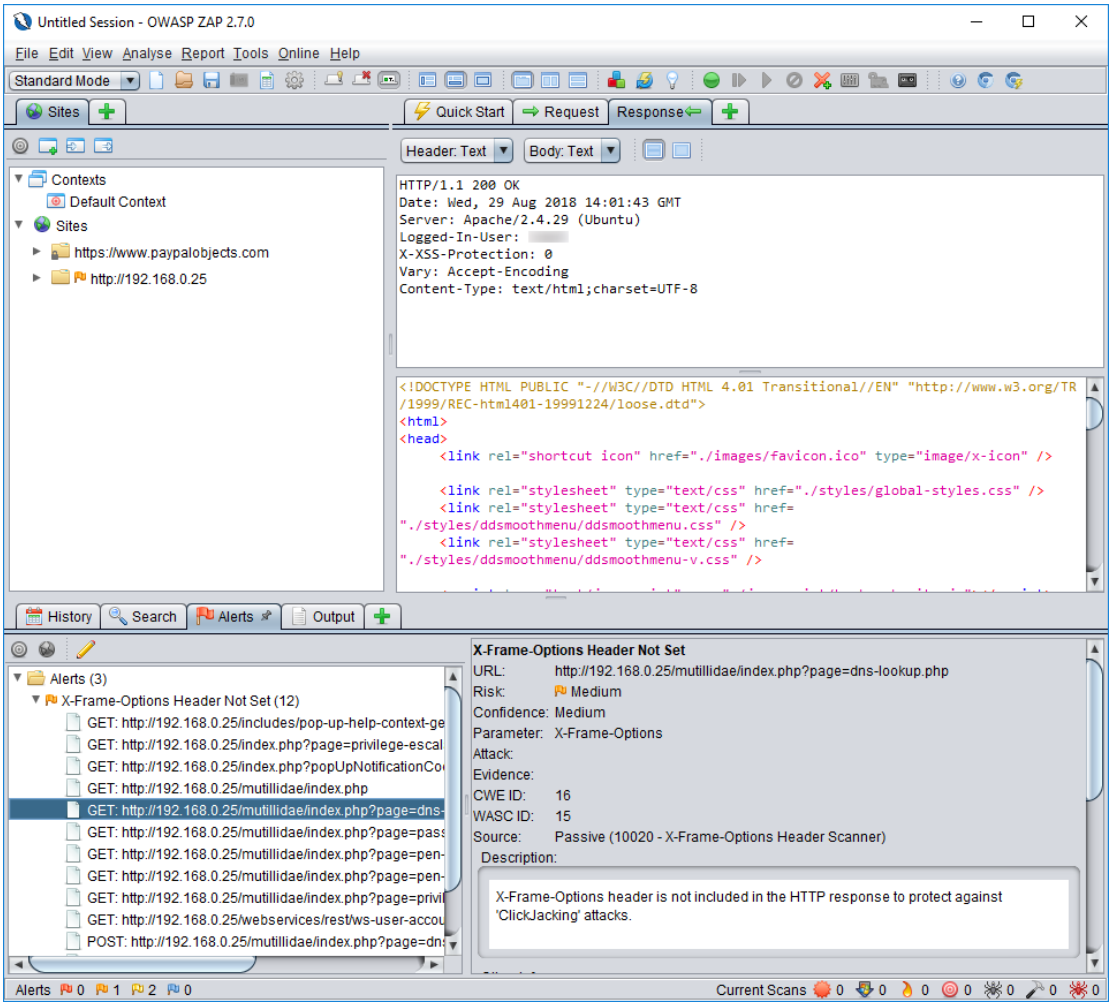
Bilo koji dio zahtjeva sada je moguće izmijeniti. Nakon izmjene, pritiskom na ikonu desno od kruga (srednju od tri prethodno označene ikone) zahtjev će biti poslan, te će se svaki sljedeći zahtjev također ovako zaustaviti. Pritiskom na krajnje desnu ikonu od tri prethodno označene, zahtjev će biti poslan, no OWASP ZAP sada neće više zaustavljati sljedeće zahtjeve.

3.4 Ispitivanje sigurnosti pomoću alata OWASP ZAP

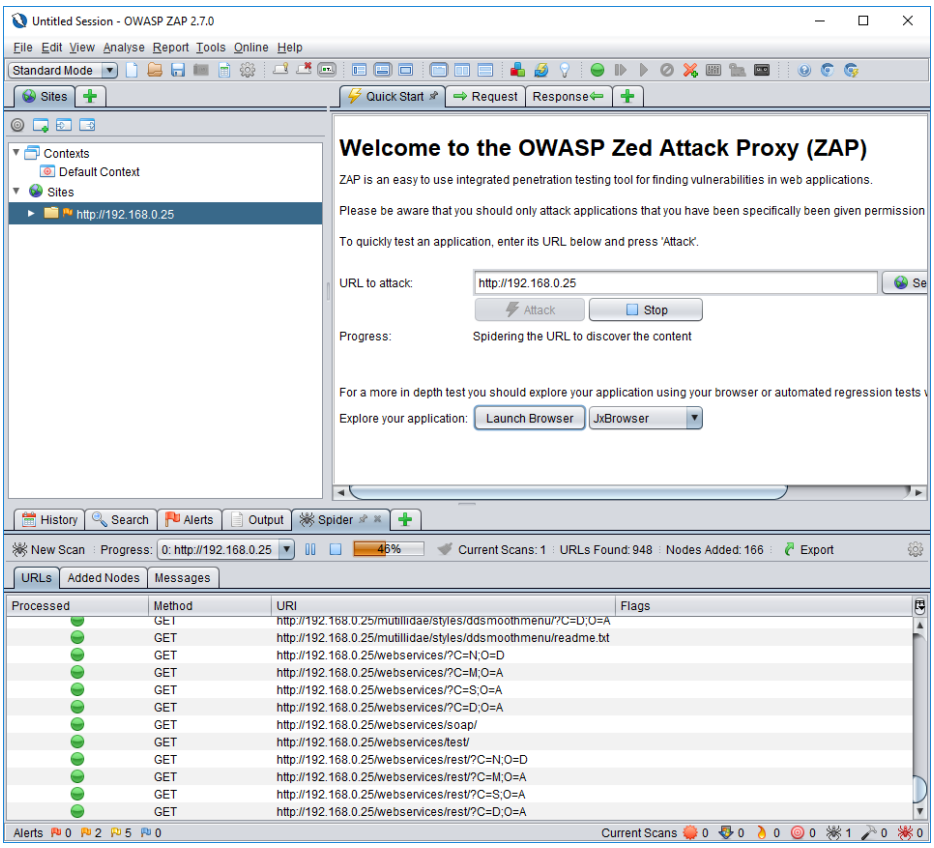
Prije objašnjenja postupka, bitno je naglasiti kako se **ispitivanje sigurnosti web aplikacije smije raditi isključivo uz dopuštenje vlasnika.**

Postoje dva načina ispitivanja sigurnosti web aplikacija u alatu OWASP ZAP: pasivno skeniranje i aktivno skeniranje.

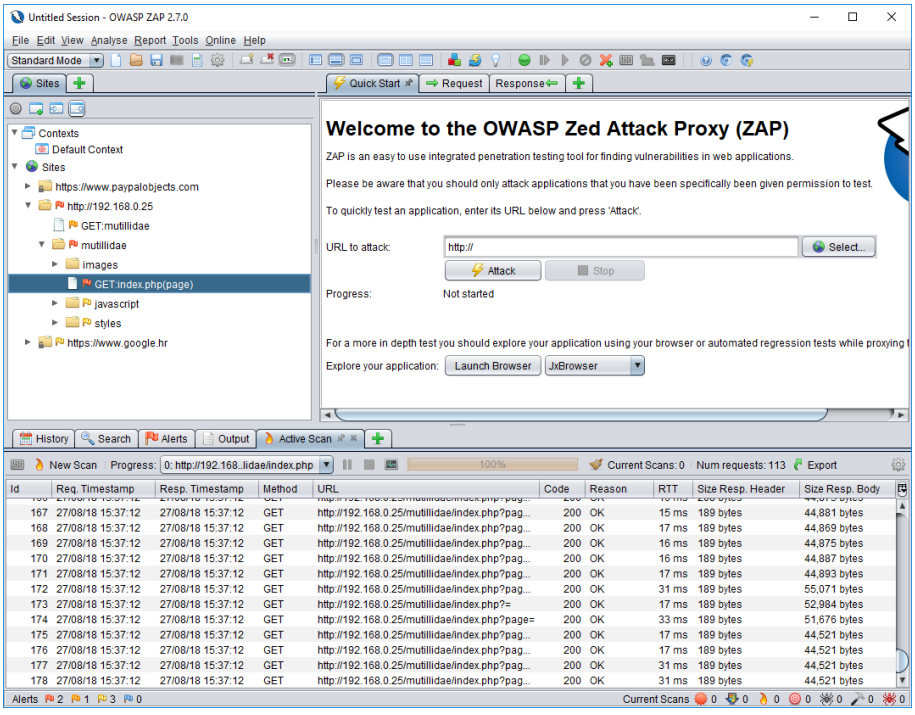
Pasivno skeniranje je automatski uključeno te ga je po potrebi moguće isključiti u postavkama. U pasivnom skeniranju, OWASP ZAP samo analizira promet koji putuje kroz njega. Primjerice, dok korisnik otvara i koristi neku web stranicu s OWASP ZAP-om kao posrednikom, OWASP ZAP će analizirati promet te na temelju njega bilježiti pronađene sigurnosne propuste. Rezultate skeniranja moguće je vidjeti u kartici ***Alerts*** u donjem dijelu glavnog prozora OWASP ZAP-a. Tamo je zabilježen popis mogućih sigurnosnih propusta kategoriziranih po vrsti. Pritiskom na pojedinu ranjivosti u toj kartici prikazuju se dodatne informacije kao što je prikazano na donjoj slici.



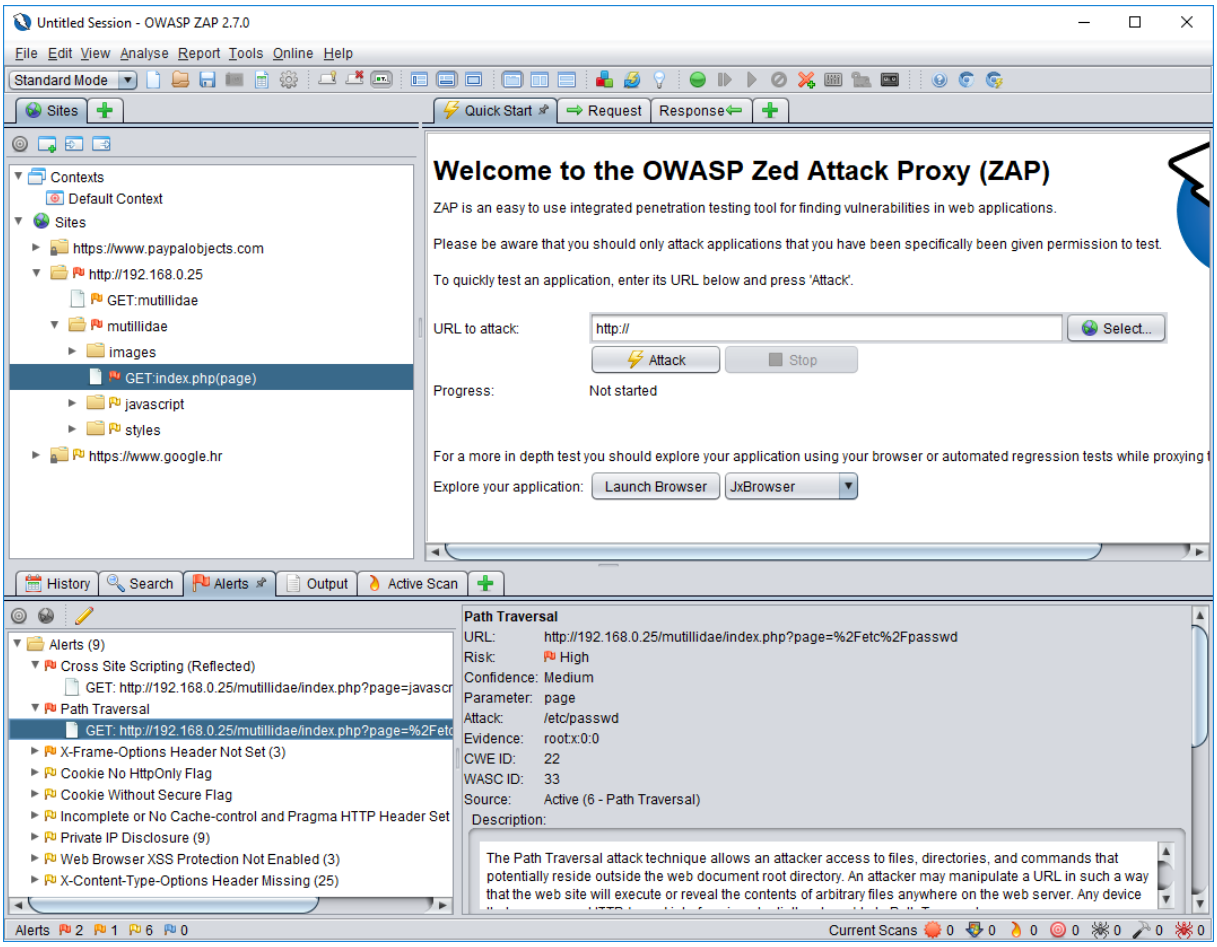
Za razliku od pasivnog skeniranja, aktivno skeniranje zapravo napada web aplikaciju na razne načine te tako pokušava otkriti ranjivosti. Najlakši način za pokretanje aktivnog skeniranja je upisivanje URL-a u polje na kartici ***Quick Start*** te pritisak na tipku ***Attack***.



OWASP ZAP prvo pokušava otkriti koji sve URL-ovi postoje na web aplikaciji, pa ih zatim po završetku toga aktivno skenira. U donjem dijelu prozora alata OWASP ZAP u kartici ***Active Scan*** vidljiv je napredak aktivnog skeniranja.



Također, OWASP ZAP sada sam pronalazi sigurnosne propuste te ih je, kao i kod pasivnog skeniranja, moguće pregledati u kartici ***Alerts***.



4 Zaključak

OWASP ZAP je moćan HTTP posrednik koji značajno olakšava ispitivanje sigurnosti web aplikacija. Osim funkcionalnosti HTTP posrednika, OWASP ZAP ima niz drugih funkcionalnosti usmjerenih na ispitivanje sigurnosti web aplikacija.

Iako OWASP ZAP koriste i sigurnosni stručnjaci, alat je prilagođen i korisnicima koji ne znaju puno o sigurnosti. Primjerice, OWASP ZAP koristan je autorima web aplikacija jer im na lagan način omogućuje osnovno ispitivanje sigurnosti razvijene aplikacije. OWASP ZAP sam po sebi ima mnoštvo funkcionalnosti, no uz njih, moguće ga je i proširiti dodacima (eng. *plugins*) te na taj način dodatno povećati korist alata.