HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Analiza Paros programskog paketa

CCERT-PUBDOC-2003-09-39

CARNet CERT u suradnji s LS&S

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi.

Rezultat toga rada ovaj je dokument koji je nastao suradnjom CARNet CERT-a i LS&S-a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

CARNet CERT, www.cert.hr - nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, www.lss.hr - laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. Uvod

Paros (http://www.proofsecure.com/index.shtml) programski paket besplatan je alat namijenjen ispitivanju sigurnosti Web aplikacija. Rad programa bazira se na ugrađenoj *proxy* funkcionalnosti koja omogućuje presretanje HTTP i HTTPS sjednica te njihovu analizu u svrhu otkrivanja potencijalnih sigurnosnih nedostataka i ranjivosti.
Program, osim što omogućuje presretanje i modifikaciju HTTP/HTTPS sjednica, također posjeduje i brojne druge funkcionalnosti, koje ga čine vrlo atraktivnim alatom za sve one koji se bave razvojem i ispitivanjem sigurnosti aplikacija baziranih na Web servisu. Kao primjer se može navesti mogućnost detekcije *Cross Site Scripting* (XSS) i *SQL Injection* ranjivosti, mogućnost promjene vrijednosti HTTP formi, otkrivanje strukture Web sadržaja na poslužitelju, kodiranje podataka i sl.
Također treba napomenuti da je Paros programski paket u potpunosti napisan u Java programskom jeziku, što ga čini neovisnim o platformi na kojoj se pokreće.
U nastavku dokumenta opisani su postupci instalacije i konfiguracije programa, kao i njegove osnovne funkcionalnosti te mogućnosti primjene.

2. Instalacija i konfiguracija programa

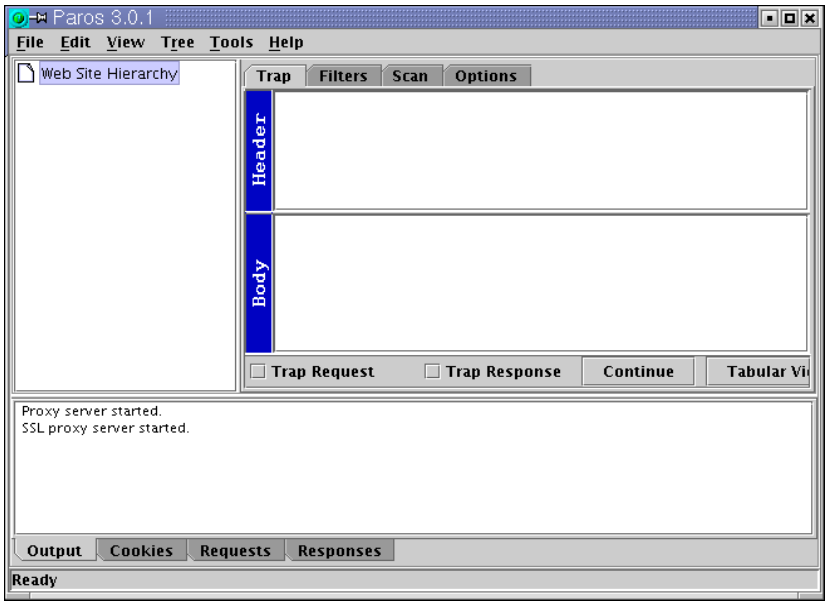
Budući da je Paros programski paket napisan u Java programskom jeziku, osnovni preduvjet za njegovu instalaciju je prisutnost Java Run Time Enviroment (JRE) 1.4 okruženja na računalu na kojem se program želi pokretati. Spomenuto okruženje, koje će omogućiti izvršavanje Java aplikacija, moguće je dobaviti na URL adresi: http://java.sun.com/j2se, a postupak instalacije vrlo je jednostavan i automatiziran.
Nakon što je ispunjen navedeni preduvjet, moguće je pristupiti instalaciji samog Paros programskog paketa. Program dolazi u zip arhivi (`paros-3.0.1-unix.zip`) i moguće ga je dobaviti sa sljedeće URL adrese: http://www.proofsecure.com/download.shtml.
Dobavljenu arhivu moguće je otpakirati naredbom:

```
# unzip paros-3.0.1-unix.zip
```

koja će rezultirati raspakiravanjem sadržaja arhive u poddirektorij pod nazivom paros. Nakon pozicioniranja u novonastali direktorij, program je moguće jednostavno pokrenuti naredbom:

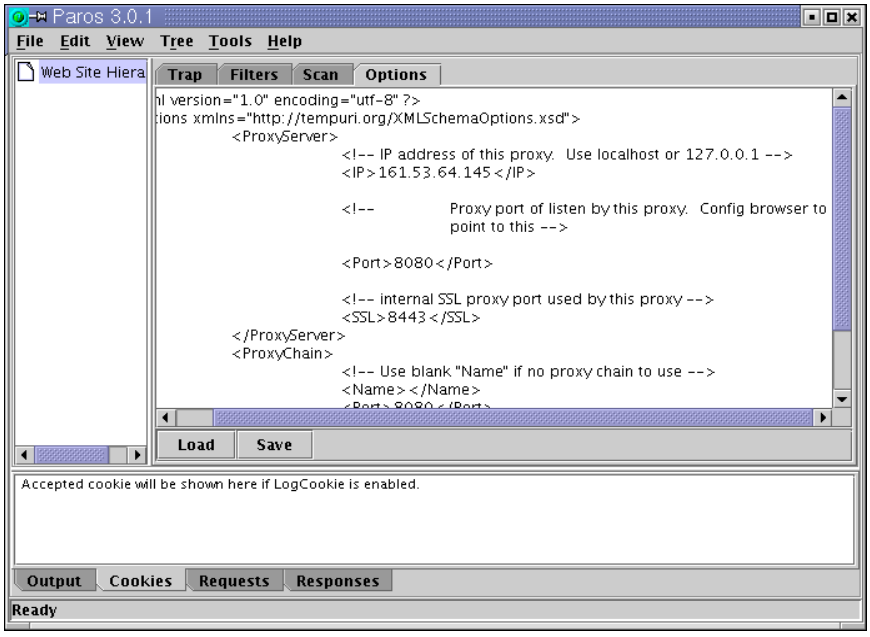
```
# java –jar paros.jar
```

Na sljedećoj slici (Slika 1) prikazan je glavni prozor Paros programskog paketa. Sučelje programa podijeljeno je na tri dijela. U lijevom prozoru glavnog sučelja prikazana je hijerarhija Web resursa koji su posjećeni putem Paros *proxy* poslužitelja; unutar desnog prozora moguće je podesiti različite parametre kojima je moguće utjecati na način rada programa, dok su u donjem prozoru prikazani svi podaci koji se razmjenjuju između klijenta i poslužitelja (*cookie* datoteke, HTTP/HTTPS upiti i odgovori i sl.).
Na temelju provedenih testova sučelje se može ocijeniti prilično preglednim i funkcionalnim. Navigacija kroz program vrlo je jednostavna i intuitivna, što olakšava njegovo korištenje.



Slika 1: Glavni prozor Paros programa

Proxy poslužitelj ugrađen u Paros programski paket koristi dva porta, 8080 i 8443, a njihove vrijednosti moguće je modificirati prema potrebi. Port 8080 koristi se za presretanje i prosljeđivanje HTTP/HTTPS konekcija, dok se port 8443 koristi interno za upravljanje SSL konekcijama. Ukoliko inicijalno odabrani portovi iz određenih razloga korisniku ne odgovaraju (npr. filtriranje mrežnog prometa na vatrozidu ili trenutna zauzetost nekog od navedenih portova), postavke Paros *proxy* poslužitelja moguće je promijeniti unutar sučelja *Options* (Slika 2). Nakon promjena na konfiguracijskoj datoteci programa, istu je potrebno pohraniti pritiskom na karticu Save u donjem dijelu prozora.



Slika 2: Podešavanje parametara Paros proxy poslužitelja

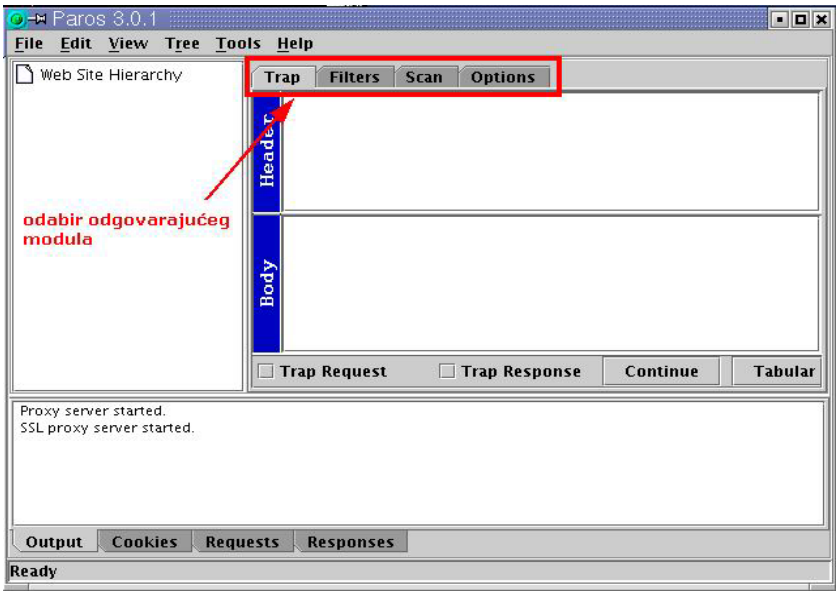
3. Primjena programa

Paros programski paket podijeljen je u nekoliko osnovnih modula, koji se međusobno razlikuju prema svojoj namjeni i mogućnostima. Radi se o sljedećim modulima:

- Scanner,

- Trap,
- Filter,
- Spider.

Postavke pojedinog modula moguće je uređivati unutar glavnog prozora Paros programa, pritiskom na polje koje odgovara njegovom imenu (*Slika 3*). Iznimka je modul *Spider* koji se omogućava unutar padajućeg izbornika. U nastavku poglavlja biti će ukratko opisani navedeni moduli, zajedno s njihovim mogućnostima i načinom primjene.



Slika 3: Odabir odgovarajućeg modula

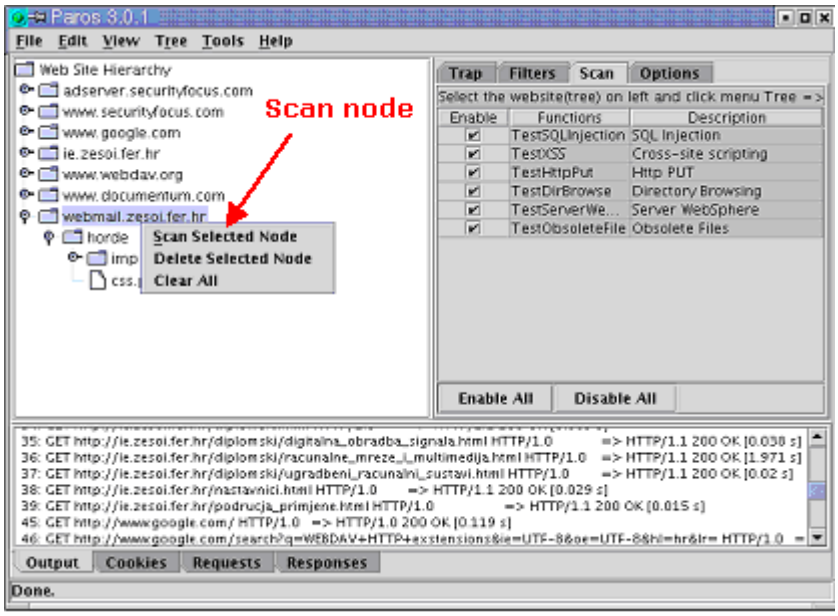
3.1. Scanner modul

Scanner modul namijenjen je pregledavanju sadržaja Web poslužitelja, u svrhu otkrivanja potencijalnih sigurnosnih nedostataka, odnosno ranjivosti. Ono što je posebno zanimljivo kod *Scanner* modula je sam način na koji se odabiru Web resursi koji će biti podvrgnuti ispitivanju. Ispitivanje dijelova Web poslužitelja ne provodi se na temelju dane URL adrese, nego na temelju resursa zabilježenih unutar *Web Site Hieararchy* sučelja s lijeve strane glavnog prozora. To znači da se ispituju samo oni Web sadržaji koje je korisnik prethodno posjetio i koji su, kao posljedica toga, zabilježeni unutar spomenutog prozora.

Ovakav pristup pregledavanja sadržaja osmišljen je kako bi se na taj način omogućilo ispitivanje kompletnih struktura Web *siteova*, a ne samo onih stranica koje su inicijalno dostupne. Naime, dosadašnja iskustva pokazala su da velik broj Web *site*-ova posjeduje stranice kojima je moguće pristupiti samo uz prethodnu autorizaciju ili neki drugi uvjet. Automatizirano ispitivanje takovih *siteova,* bez dodatnih zahvata provoditelja testiranja, obično rezultira površnim i nepotpunim rezultatima, koji administratoru ostavljaju lažan dojam sigurnosti.

Osnovna ideja opisane metode je ta da se korisnik kod takovih Web *siteova* (portali, forumi, *webmail* programi, i sl.) prethodno prijavi u sustav, na temelju čega će se automatski kreirati struktura posjećenih Web stranica koje se kasnije mogu podvrgnuti detaljnijoj analizi. Elemente koji će biti ispitani korisnik može sam odabrati prema potrebi.

Odabirom opcije *Tree->Scan All* moguće je pokrenuti pregledavanje kompletne Web hijerarhije zabilježene unutar *Web Site Hiearchy* prozora, dok je pregledavanje pojedinih čvorova moguće odabrati desnim pritiskom miša na željeni čvor te odabirom opcije **Scan Selected Node.**



Slika 4: Scanner modul

Provjere koje Paros program trenutno provodi uključuju:

- Dozvoljeno izvršavanje HTTP PUT naredbe;
- Mogućnost pregledavanja sadržaja direktorija;
- Pretraživanje zastarjelih datoteka;
- Provjera *Cross Site Scripting* (engl. XSS) ranjivosti;
- Mogućnost umetanja SQL upita (engl. *SQL Injection Vulnerabilities*);
- Pretraživanje inicijalnih datoteka na poslužitelju, koje nisu bitne za rad aplikacije;

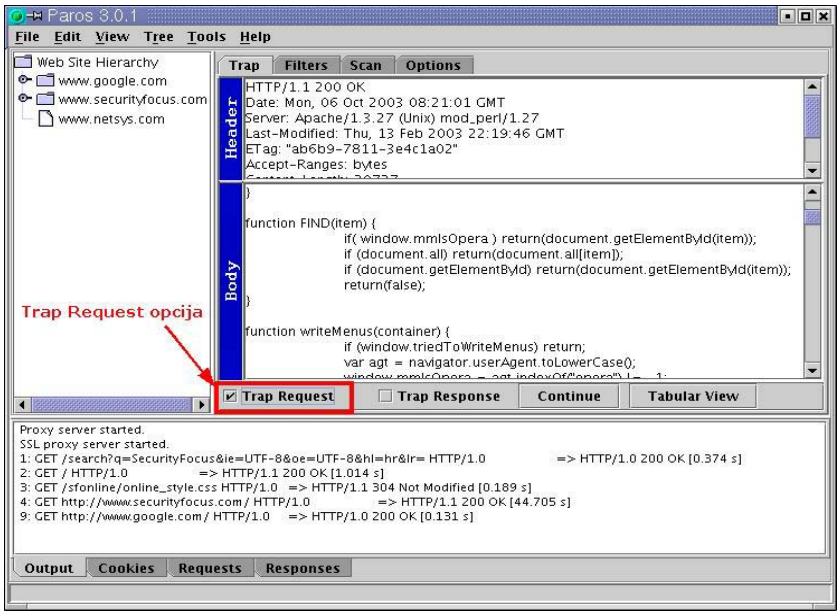
Svaku od ovih provjera moguće je po potrebi omogućiti, odnosno onemogućiti unutar sučelja **Scan** glavnog prozora aplikacije (uključivanjem/isključivanjem odgovarajućih *checkbox* polja).
Treba napomenuti da Paros program u trenutnoj inačici ne podržava pregledavanje URL adresa koje se generiraju putem JavaScript programskog koda.

3.2. Trap modul

Trap modul ugrađen u Paros programski paket omogućuje presretanje HTTP i HTTPS prometa, kao i modifikaciju pojedinih paketa koji se razmjenjuju između klijenta i poslužitelja. Modul se sastoji od dva dijela, od kojih jedan omogućuje presretanje upita klijenata, a drugi presretanje odgovora koje vraća poslužitelj. U nastavku slijedi kratki opis spomenutih funkcionalnosti, zajedno s primjerom njihovog korištenja.

3.2.1. Trap Request

Trap Request modul omogućuje presretanje HTTP/HTTPS zahtjeva i moguće ga je omogućiti uključivanjem **Trap Request** *checkbox* polja (*Slika 5*), unutar sekcije **Trap**.



Slika 5: Trap Request funkcionalnost

Kako bi se omogućilo presretanje zahtjeva, unutar Web preglednika klijenta potrebno je podesiti *proxy* poslužitelj koji će odgovarati IP adresi i mrežnom portu Paros programa. Nakon toga svi zahtjevi klijenta biti će proslijeđeni na IP adresu Paros *proxy* poslužitelja, gdje je moguća njihova analiza i modifikacija, nakon čega će biti proslijeđeni ciljnom Web poslužitelju.

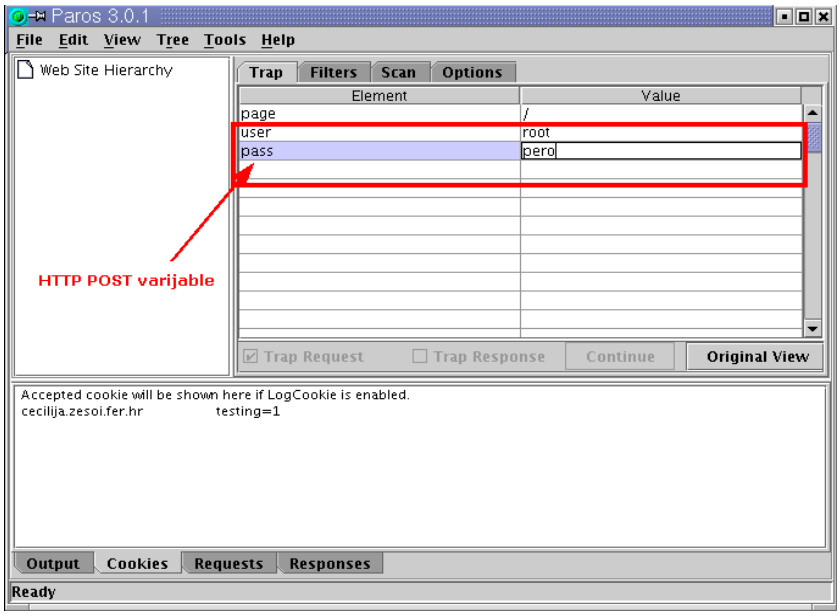
"Uhvaćene" zahtjeve program prikazuje unutar prozora **Header**, unutar kojega je ujedno moguće obaviti željene promjene. Nakon što su obavljene preinake na upitu, moguće ga je proslijediti poslužitelju pritiskom na karticu **Continue**.

Upiti klijenta, zajedno s odgovorima poslužitelja, također se prikazuju u donjem prozoru aplikacije, kako bi se na taj omogućilo kontinuirano i pregledno praćenje ranijih događaja i konekcija.

Mogućnost presretanja i modifikacije HTTP, odnosno HTTPS upita, pokazala se vrlo praktičnom i korisnom prilikom testiranja Web aplikacija. Testiranja su pokazala da je ovim putem moguće generirati različite "neuobičajene" formate HTTP/HTTPS upita, te promatrati odzive poslužitelja ne bi li se na taj način uočile potencijalne nepravilnosti.

Opcija **Tabular View**, koja se nalazi s desne strane kartice **Continue**, omogućuje jednostavnije i preglednije modificiranje parametara koji se Web poslužitelju prosljeđuju putem HTTP POST metode. Spomenuta opcija može se koristiti samo ukoliko je omogućena *Trap Request* opcija i ukoliko se unutar prozora **Body** nalazi odgovarajući HTML sadržaj. Pritiskom na karticu **Tabular View**, Web forme unutar stranice biti će prikazane u tabelarnom obliku, što omogućuje njihovo preglednije uređivanje i prosljeđivanje poslužitelju.

U nastavku (*Slika 6*), dan je primjer u kojem je Paros programski paket iskorišten za presretanje HTTPS sjednice između klijenta i poslužitelja te za modifikaciju varijabli proslijeđenih POST metodom (u ovom slučaju to su `user` i `pass` polja za autentikaciju putem Web sučelja).



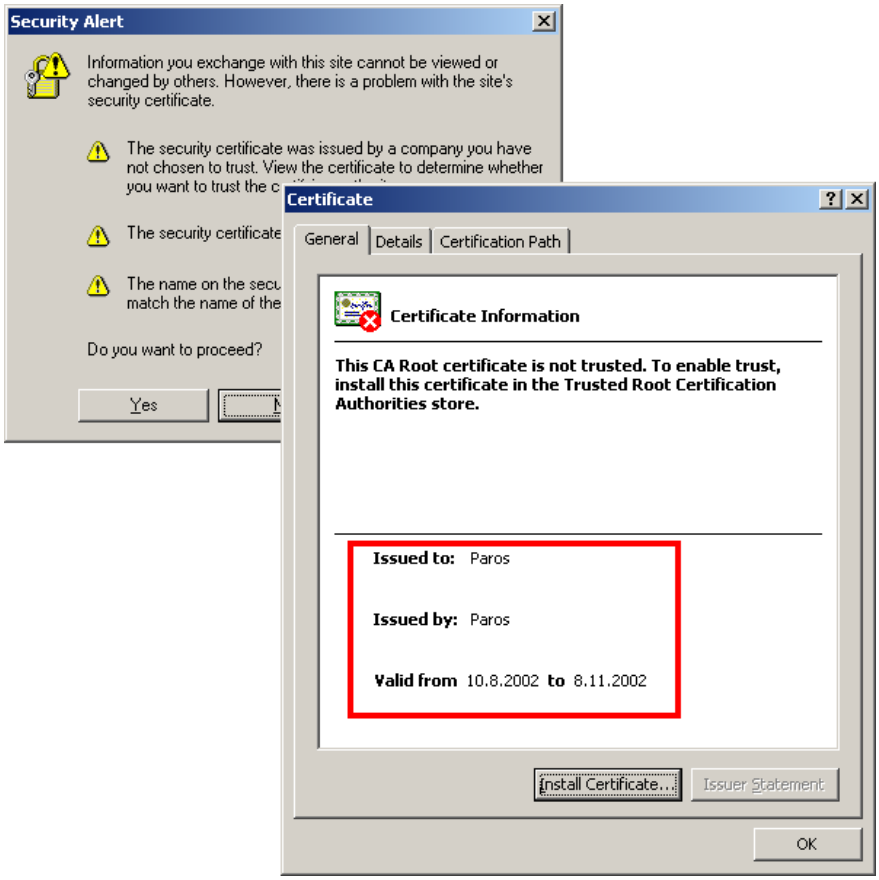
Slika 6: Modifikacija HTTP POST varijabli

HTML kod stranice koja je prikazana na gornjoj slici izgleda ovako:

```
<form action=/login.cgi method=post>
<input type=hidden name=page value='/'>
<table border width=40%>
<tr bgcolor=#9999ff> <td><b>Login to Webapps</b></td> </tr>
<tr bgcolor=#cccccc> <td align=center><table cellpadding=3>
<tr> <td>You must enter a username and password td> </tr>
<tr> <td><b>Username</b></td>
<td><input name=user size=20 value=''></td> </tr>
<tr> <td><b>Password</b></td>
<td><input name=pass size=20 type=password></td> </tr>
<tr>    <td    colspan=2    align=center><input    type=submit
value='Login'>
<input type=reset value='Clear'><br>
<input type=checkbox name=save value=1> Remember permanently?
</td> </tr>
</table></td></tr></table><p><hr>
</form>
```

Forme `user` i `pass` (označene žuto), pomoću kojih se korisnik prijavljuje u sustav, unutar Paros aplikacije izdvojene su i prikazane u obliku tablice (*Slika 6*). Ovakvo rješenje, osim što je vrlo pregledno, korisniku omogućuje jednostavno modificiranje vrijednosti POST varijabli.

Za presretanje HTTPS sjednica Paros program koristi svoj vlastiti certifikat, kojeg korisnik mora prihvatiti prilikom iniciranja konekcije. Ukoliko korisnik ne prihvati ponuđeni certifikat, konekcija se prekida. Na sljedećoj slici (*Slika 7*) prikazan je certifikat koji se korisniku nudi prilikom iniciranja HTTPS konekcije putem Paros *proxy* poslužitelja.



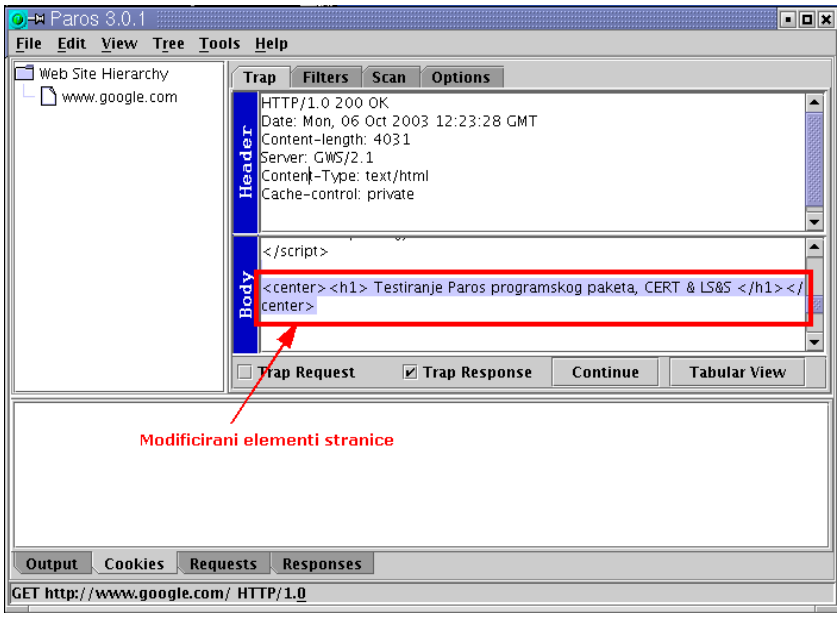
Slika 7: Paros certifikat

3.2.2. Trap Response

Trap Response opcija vrlo je slična ranije opisanoj *Trap Request* funkcionalnosti, s jedinom razlikom da se u ovom slučaju radi o presretanju odgovora poslužitelja. Opciju je moguće uključiti **Trap Response** *checkbox* poljem.

Na sličan način kao i u prethodnom poglavlju, moguće je uređivati zaglavlja HTTP/HTTPS odgovora, kao i sam sadržaj Web stranice. Nakon upita Web klijenta (koji se poslužitelju prosljeđuje putem Paros *proxy* poslužitelja), zatražena Web stranica, zajedno sa pripadajućim HTTP/HTTPS zaglavljem, biti će prikazana unutar **Header** i **Body** prozora Paros programa, gdje je moguće načiniti željene modifikacije. Primjer korištenja opisane funkcionalnosti dan je u nastavku. U prvom koraku klijent inicira HTTP upit upućen na adresu http://www.google.com. Konekcija se poslužitelju prosljeđuje putem Paros *proxy* poslužitelja (jer je to tako podešeno unutar samog Web preglednika), nakon čega poslužitelj zatraženu stranicu vraća na adresu s koje je došao upit (IP adresa Paros *Proxy* poslužitelja).

Paros program unutar prozora **Header** i **Body** sučelja prikazuje zatraženu stranicu gdje ju je moguće modificirati prema želji (*Slika 8*).

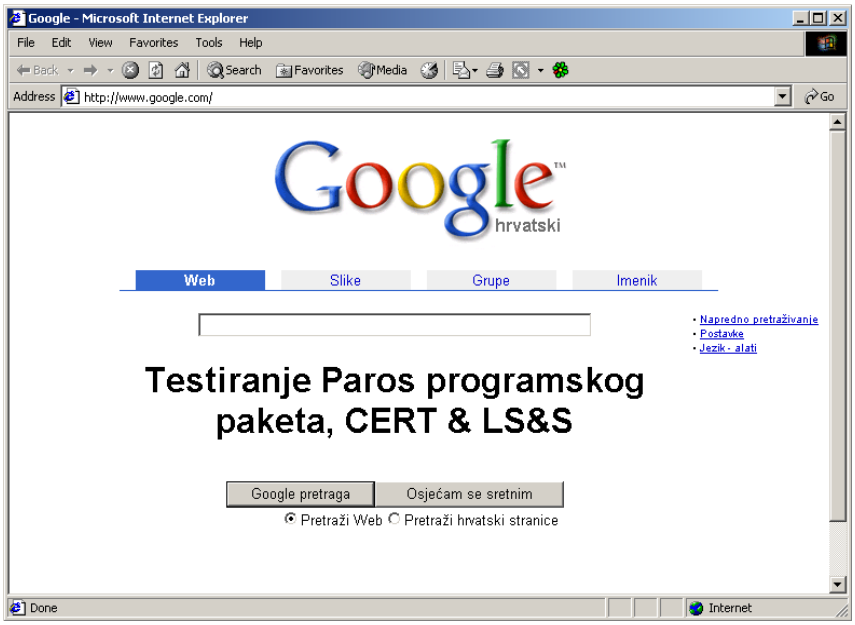


Slika 8: Modificiranje odgovora poslužitelja

U svrhu testiranja *Trap Response* funkcionalnosti, unutar Web stranice dodan je HTML kod:

```
<H1> Testiranje Paros programskog paketa </H1>
```

koji je klijentu proslijeđen pritiskom na karticu **Continue**. U posljednjem koraku modificirana stranica proslijeđena je klijentu koji je inicirao konekciju, gdje se prikazuje unutar Web preglednika (*Slika 9*).



Slika 9: Prikaz modificirane stranice unutar Web preglednika

Treba napomenuti da prilikom korištenja *Trap Response* funkcionalnosti **Tabular View** opcija nema smisla.

3.3. Filter modul

Filter modul Paros programskog paketa omogućuje filtriranje pojedinih elemenata HTTP/HTTPS upita, odnosno odgovora. Ideja ovog modula je da se korisniku olakša praćenje i analiza HTTP/HTTPS prometa, bez potrebe za eksplicitnim presretanjem svakog pojedinog upita. Prema dokumentaciji Paros programa, korištenje ugrađenih filtara omogućuje:

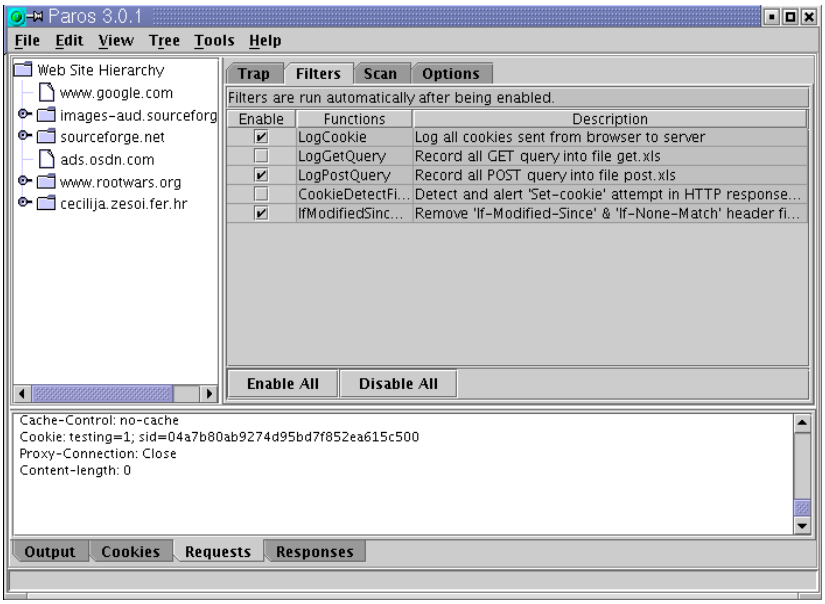
- Detekciju unaprijed definiranih elemenata HTTP upita i odgovora uz obavješćivanje korisnika;
- Bilježenje i praćenje točno određenih elemenata koji su interesantni korisniku (npr. *cookie* datoteke).

Za korištenje filtar funkcionalnosti potrebno je odabrati sekciju **Filters** u gornjem dijelu glavnog prozora. Trenutni HTTP/HTTPS filtri koje podržava Paros programski paket opisani su u sljedećoj tablici (*Tablica 1*).

Naziv filtra	Opis filtra
`LogCookie`	- ovim filtrom omogućuje se bilježenje svih ranije prihvaćenih *cookie* datoteka koje Web preglednik prosljeđuje poslužitelju. Detektirane *cookie* vrijednosti također se prikazuju i unutar donjeg prozora pod nazivom **Cookies**.
`LogGetQuery`	- omogućuje se bilježenje svih zahtjeva klijenta upućenih GET metodom. Detektirani zahtjevi zapisuju se u datoteku pod nazivom `get.xls` unutar radnog direktorija `paros` programa.
`LogPostQuery`	- omogućuje se bilježenje svih zahtjeva klijenta upućenih POST metodom. Detektirani zahtjevi zapisuju se u datoteku pod nazivom `post.xls` unutar radnog direktorija `paros` programa.
`CookieDetectFilter`	- uz uključen ovaj filtar, svaki puta kada se detektira `Set-cookie` HTTP zaglavlje, korisnik će biti obaviješten, kako bi se na taj način omogućila i njegova modifikacija;
`IfModifiedSinceFilter`	- ovim filtrom se omogućuje uklanjanje `If-Modified-Since` i `If-None-Match` zaglavlja iz HTTP/HTTPS upita. Ovaj filtar koristi se u slučajevima kada se od Web poslužitelja umjesto odgovora "`HTTP 304 not modified`" želi dobiti odgovor "`HTTP 200 OK`".

Tablica 1: Trenutno podržani filtri unutar Paros programskog paketa

Pojedini filtri omogućavaju se, odnosno onemogućavaju uključivanjem/isključivanjem odgovarajućeg *checkbox* polja, unutar ranije spomenute sekcije **Filters** (*Slika 10*).



Slika 10: Sučelje unutar kojeg je moguće uključiti i isključiti pojedine filtre

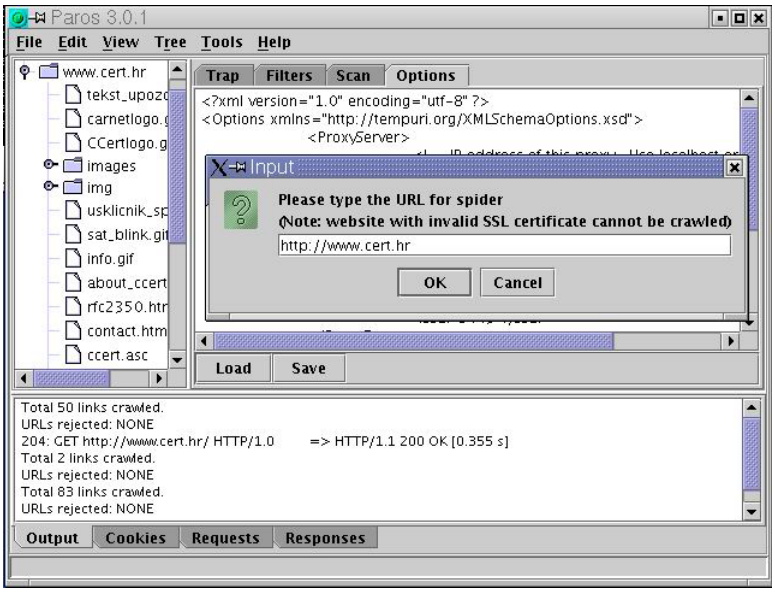
Budući da se odabrani filtri u realnom vremenu primjenjuju na sav HTTP i HTTPS promet koji se razmjenjuje između klijenta i poslužitelja, istovremeno omogućavanje više njih može znatno degradirati performanse Paros *proxy* poslužitelja. Iz tog razloga preporučuje se korištenje samo onih filtara koji se smatraju neophodnima za pojedinu primjenu.

3.4. Spider modul

Spider modul omogućuje pretraživanje zadanih URL adresa s ciljem pronalaženja što većeg broja veza (engl. *links*) na druge dokumente, odnosno stranice. Korištenje *Spider* modula korisniku omogućuje jednostavan i automatiziran dolazak do strukture Web sadržaja na zadanom poslužitelju. Modul je trenutno u beta razvojnoj fazi, i u budućnosti se mogu očekivati njegova poboljšanja.

Spider modul moguće je uključiti pritiskom na polje *Spider*, unutar padajućeg izbornika *Tools* (*Tools->Spider*). Pritiskom na spomenuto polje otvara se sučelje unutar kojega je potrebno navesti URL adresu Web *site-a* čija se struktura želi utvrditi.

Nakon toga se pokreće sam modul, koji analizira sadržaj zadanog Web okruženja, pri čemu se njegova struktura prikazuje unutar *Web Site Hierarchy* sučelja s lijeve strane. U nastavku je dan primjer pokretanja Spider modula na Web stranicama CERT-a (http://www.cert.hr), *Slika 11*.

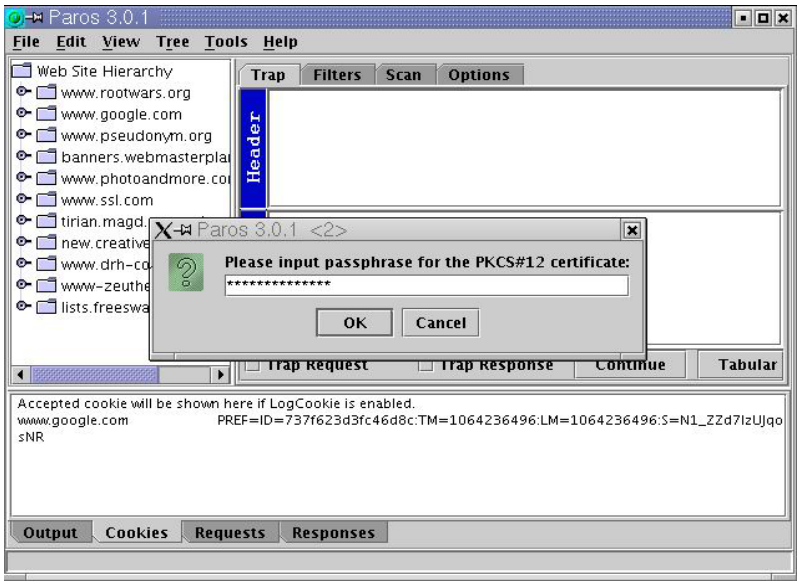


Slika 11: Spider modul

3.5. Ostale mogućnosti

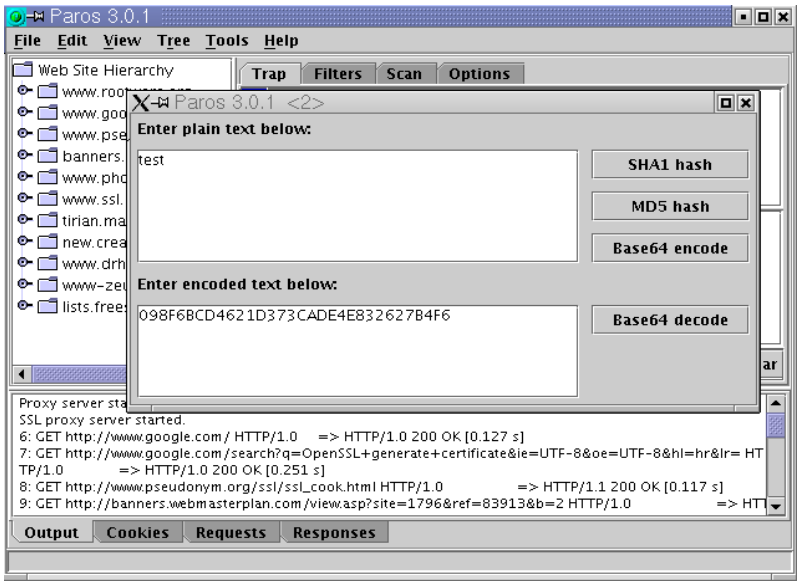
Od ostalih mogućnosti Paros programskog paketa treba napomenuti sljedeće:

- podrška za klijentske certifikate – mogućnost učitavanja klijentskih certifikata neophodna je za presretanje sjednica prema Web poslužiteljima koji zahtijevaju certifikat na strani klijenta. Ovim putem omogućuje se presretanje konekcija i analiza prometa između takovih Web aplikacija i klijenata, što programu daje dodatnu snagu. Certifikat je moguće učitati korištenjem *Tools -> Enable Client Certificate* opcije, pri čemu certifikat mora biti u PKCS#12 formatu (*Slika 12*).



Slika 12: Učitavanje certifikata u Paros aplikaciju

– mogućnost kodiranja podataka MD5, SHA1 i Base64 algoritmima (*Tools -> Hash/Encoding*). Spomenuto sučelje za konverziju podataka prikazano je na sljedećoj slici (*Slika 13*).



Slika 13: Sučelje za kodiranje podataka

– bilježenje svih HTTP/HTTPS upita i odgovora, zajedno s vremenom odziva poslužitelja (engl. *response time*). Ovi podaci prikazuju se u donjem dijelu prozora (sučelje **Output**).

4. Zaključak

U ovome dokumentu opisan je Paros programski paket namijenjen ispitivanju sigurnosti Web aplikacija. Osim što je namijenjen sigurnosnim stručnjacima koji se bave ispitivanjem sigurnosti Web aplikacija, program je namijenjen i Web programerima koji se bave njihovim razvojem.

Princip rada programa bazira se na ugrađenoj *proxy* funkcionalnosti, koja korisniku omogućuje presretanje i analizu HTTP/HTTPS sjednica te modifikaciju njihovih parametara. U sklopu testiranja ispitane su osnovne funkcionalnosti programa te mogućnost njihove primjene. Testiranja su pokazala da se radi o vrlo jednostavnom i dobro zamišljenom programskom paketu, od kojeg se u budućnosti mogu očekivati dodatna poboljšanja.