HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Analiza TrustSight Security Scanner alata

CCERT-PUBDOC-2004-01-59

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 4

2. SIGURNOSNO SKENIRANJE WEB APLIKACIJA 4

3. INSTALACIJA I KORIŠTENJE ALATA 5

4. DODATNE MOGUĆNOSTI ALATA 7

4.1. TERMINAL ZA RUČNO ISPITIVANJE 7
4.2. DEFINIRANJE VLASTITIH TESTOVA 7
4.3. KORIŠTENJE *PROXY* POSLUŽITELJA 9
4.4. IZBJEGAVANJE IDS SUSTAVA 9

5. ZAKLJUČAK 10

1. Uvod

TrustSight Security Scanner, tvrtke Syhunt (http://www.syhunt.com), trenutno je jedan od moćnijih programa za ispitivanje sigurnosti Web poslužitelja koji se mogu pronaći na tržištu. Mogućnosti ovog alata uključuju:

- Više od 25,000 provjera za najpopularnije Web poslužitelje
- Provjera 20 najvažnijih ranjivosti prema klasifikaciji SANS-a i FBI-a
- Mogućnost provjere ranjivosti dinamičkih Web sadržaja (PHP, ASP, Cold Fusion i CGI)
- Mogućnost skeniranja mrežne opreme (usmjerivači i vatrozidi) sa ugrađenim Web sučeljem
- Detekcija aplikacijskih vatrozida
- Detekcija Honeypot sustava
- Testiranje IDS filtara
- Podrška za HTTP I HTTPS protokole
- Podrška za korištenje Proxy poslužitelja
- Kompatibilnost s CVE (engl. *Common Vulnerability Exposure*) listom ranjivosti
- Rezultati skeniranja prezentirani su u jednostavnom i jasnom izvještaju u HTML formatu
- Posjeduje filtere za prepoznavanje i uklanjanje lažnih ranjivosti iz izvještaja
- U mogućnosti je izvoditi napade prepisivanjem spremnika

U ovom dokumentu ukratko će biti opisan način rada i podešavanje TrustSight skenera, kao i korištenje nekih naprednijih opcija.

2. Sigurnosno skeniranje Web aplikacija

Zbog sadržaja koje nude, kao što su npr. brojevi kreditnih kartica i bankovnih računa te mnoge druge osobne informacije, Web aplikacije česta su meta malicioznih korisnika. Navedeni rizik povećava se zbog vrlo čestih nadogradnji Web poslužitelja i popratnih aplikacija radi uvođenja novih (često sigurnosno neprovjerenih) funkcionalnosti u dinamičke Web sadržaje.

Sigurnosne propuste unutar Web aplikacija moguće je podijeliti na tehničku i logičku grupu propusta. Pod tehničkim propustima podrazumijevaju se ranjivosti sadržane u programskom kodu Web poslužitelja i samih Web aplikacija, kao i pogreške načinjene prilikom njihove konfiguracije. Ova grupacija ranjivosti omogućuje izvođenje sljedećih vrsta napada:

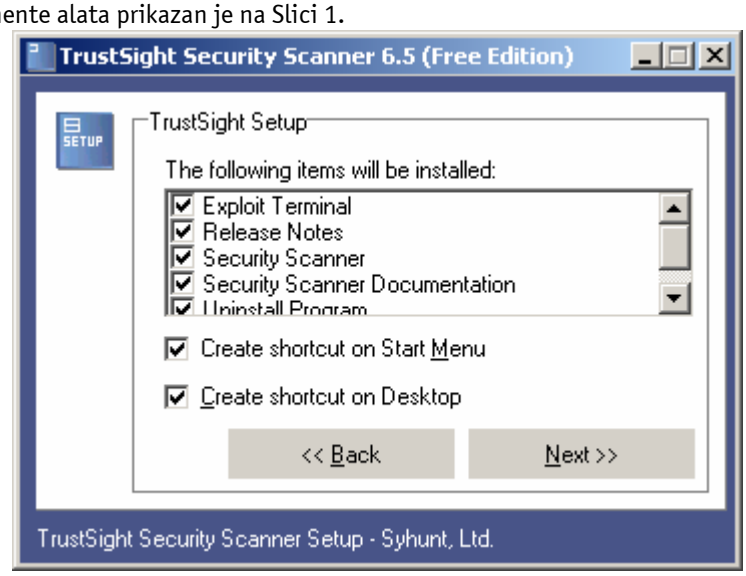
- *Cross Site Scripting*
- *SQL Injection*
- *Directory Traversal*
- *Command Injection*
- *Frame Spoofing*
- *Buffer Overflows*
- *Directory Indexing*
- *Backup Files/Directories*
- *Configuration File Disclosure*

Logički propusti, s druge strane, nastaju uslijed loše programiranih Web aplikacija i neovlaštenom korisniku omogućuju radnje kao što su izmjena prikazanog Web sadržaja, promjena razine ovlasti korisničkih računa, kreiranje lažnih korisničkih računa ili lažno predstavljanje korisnika te izvođenje neovlaštenih transakcija.

Za iskorištavanje logičkih propusta potrebna je ljudska inteligencija te stoga ovu vrstu propusta nije moguće uočiti automatiziranim postupkom skeniranja. Ipak, u većini slučajeva, razina sigurnosti postignuta uklanjanjem tehničkih propusta sasvim je prihvatljiva. Korištenjem rješenja kao što je TrustSight Security Scanner ili bilo koji drugi alat iste namjene, postupak ispitivanja sigurnosti Web aplikacija znatno se pojednostavljuje i pojeftinjuje. Pri tome je poželjno da rezultate skeniranja pregleda stručnjak za računalnu sigurnost, jer njihova pogrešna interpretacija može rezultirati nepotrebnom panikom ili suprotno, samo djelomičnim uklanjanjem propusta.

3. Instalacija i korištenje alata

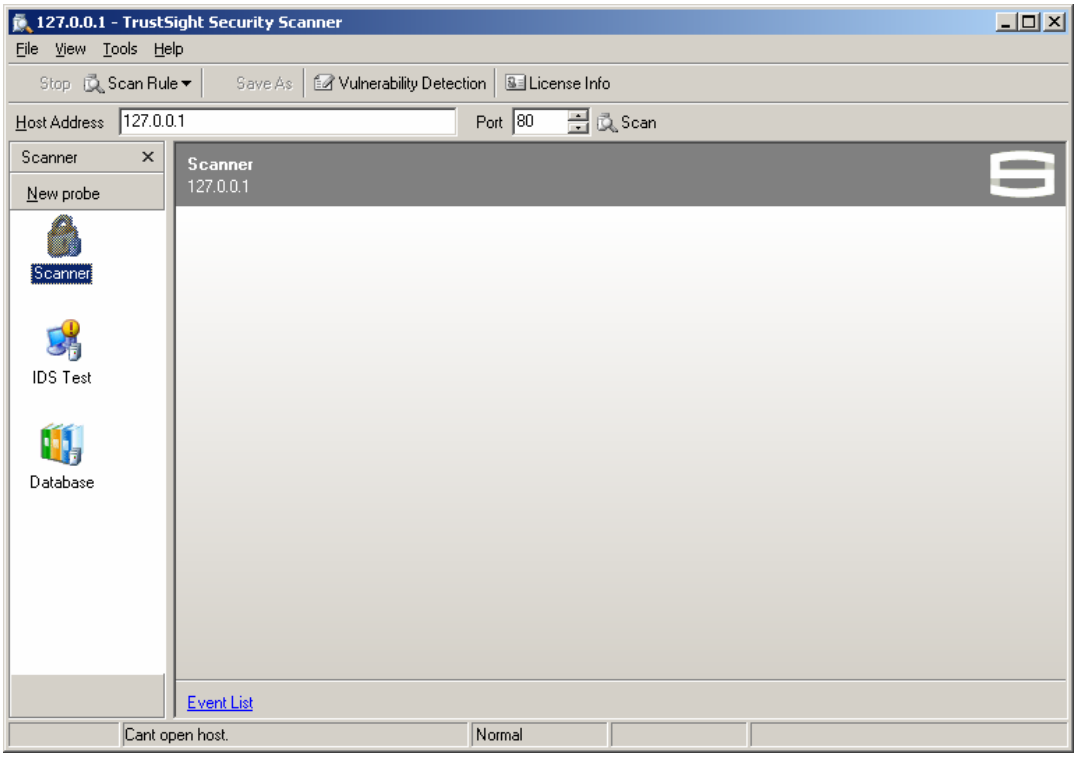
Instalacijska .exe datoteka ovog alata može se dohvatiti sa adrese http://www.syhunt.com. Pokretanjem ove datoteke započinje jednostavan instalacijski postupak, unutar kojega je potrebno prihvatiti licenčni ugovor i odabrati komponente paketa koje će se instalirati. Prozor unutar kojega se odabiru komponente alata prikazan je na Slici 1.



Slika 1: *Prozor za odabir komponenata TrustSight Security Scanner-a*

TrustScan Security Scanner alat moguće je pokretati na bilo kojoj Microsoft Windows platformi, a za potrebe rada program zahtjeva 20 MB slobodne radne memorije, jednaku količinu prostora na tvrdom disku i naravno, mrežni priključak.

Nakon jednostavnog postupka instalacije, automatski se otvara sučelje *scanner*-a (**Slika 2**). U lijevom prozoru smješten je odabir opcija, dok se u glavnom prozoru prati postupak skeniranja i pregledavaju rezultati.

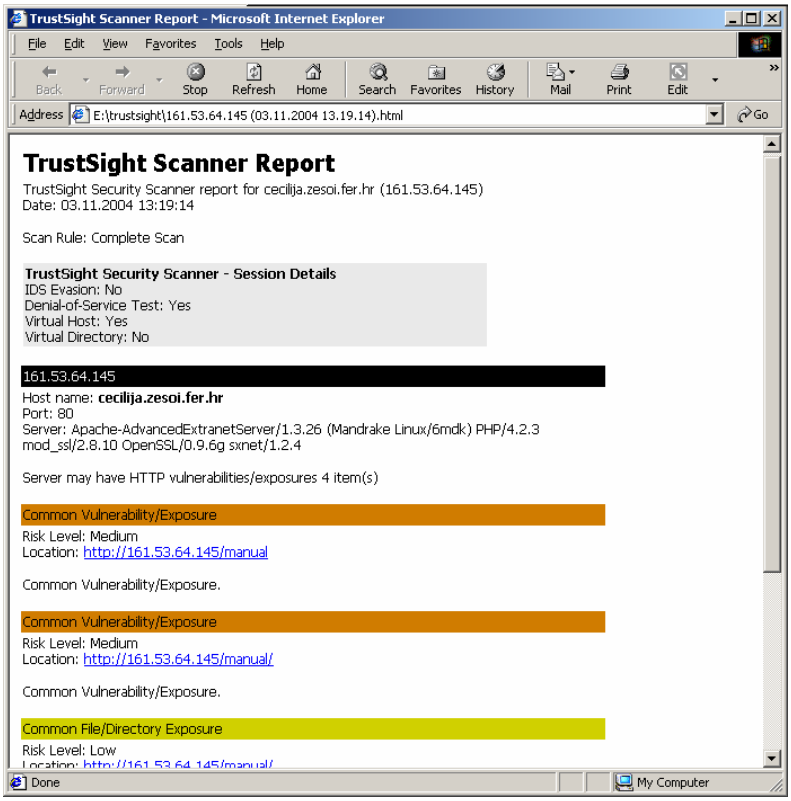


Slika 2: *Sučelje TrustSight Security Scanner alata*

Postupak skeniranja Web poslužitelja ovim alatom je sljedeći:

1. Unutar View->Vulnerability Detection izbornika potrebno je podesiti parametre skeniranja, tj. uključiti vrste testova koje će se primijeniti. Posebnu pozornost potrebno je obratiti prilikom korištenja *Denial-of-Service* testova, budući da zbog svoje prirode takvi testovi mogu uzrokovati nasilan prekid rada ispitivanog poslužitelja. Isto vrijedi i za korisnički definirane testove, ukoliko se unutar njih nalaze DoS testovi. Ukoliko se na ciljanoj mreži želi izbjeći detekcija skeniranja od strane IDS sustava, potrebno je dodatno uključiti "IDS Evasion" opciju, koja će upite nastojati oblikovati tako da prolaze neprimjećeno. Ipak, potrebno je naglasiti da u ovakvom načinu rada skener ne daje maksimalne rezultate. Za prikaz konačnih rezultata u HTML obliku potrebno je uključiti opciju "Create report".
2. Unutar izbornika Tools->Exploits->Special Options podešavaju se dodatne opcije koje se tiču načina skeniranja udaljenog poslužitelja. Između ostaloga, ovdje je moguće podesiti alat tako da pokuša identificirati direktorije na Web poslužitelju ili npr. konfiguracijske greške i dostupne datoteke koje sadrže zaporke.
3. Odabir Web preglednika kojeg će TrustSight Scanner nastojati oponašati prilikom skeniranja udaljenog poslužitelja obavlja se u izborniku Tools->Preferences. Osim toga, u ovom izborniku moguće je podesiti i virtualni direktorij na Web poslužitelju, kojeg će alat prilikom skeniranja pokušati pregledati.
4. Ukoliko se na zadanoj IP adresi nalazi Web poslužitelj sa više pokrenutih virtualnih Web-ova, skeneru je potrebno napomenuti koji od virtualnih poslužitelja se želi testirati. Adresa virtualnog poslužitelja definira s unutar izbornika Tools->Advanved->Misc. Options.
5. Nakon podešavanja svih parametara skeniranja, u glavnom prozoru programa, unutar polja Host Address, upisuje se IP adresa ciljanog računala i podešava mrežni port na kojem se nalazi testirani Web poslužitelj.

Po završenom skeniranju Web poslužitelja generira se izvještaj u HTML obliku (**Slika 3**), kojeg je potrebno pohraniti na disk i analizirati.



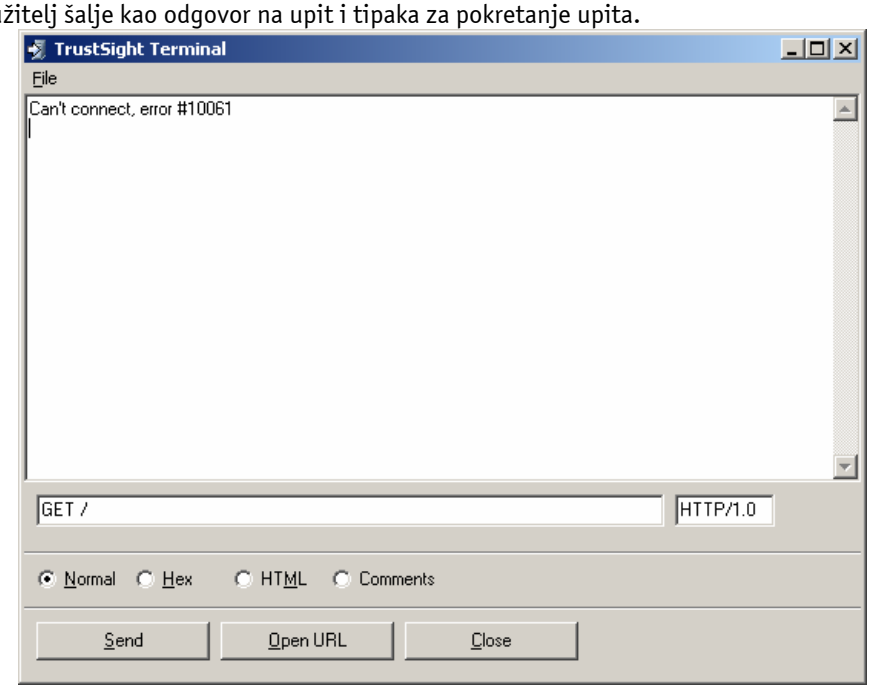
Slika 3: *Izvještaj sa rezultatima skeniranja*

Ranjivosti su poredane po stupnju opasnosti i sukladno tome označene različitim bojama. Uz svaku otkrivenu ranjivost dan je kratak opis i, ukoliko postoji, link na konkretnu Web stranicu.

4. Dodatne mogućnosti alata

4.1. Terminal za ručno ispitivanje

U direktoriju u kojeg se instalira TrustSight Security Scanner nalazi se i izvršna datoteka Stclient.exe, koja predstavlja jednostavan terminal za ručno ispitivanje Web poslužitelja i aplikacija. **Slika 4** prikazuje prozor terminala koji se sastoji od polja za unos zahtjeva, prozora za prikaz HTML koda kojeg Web poslužitelj šalje kao odgovor na upit i tipaka za pokretanje upita.

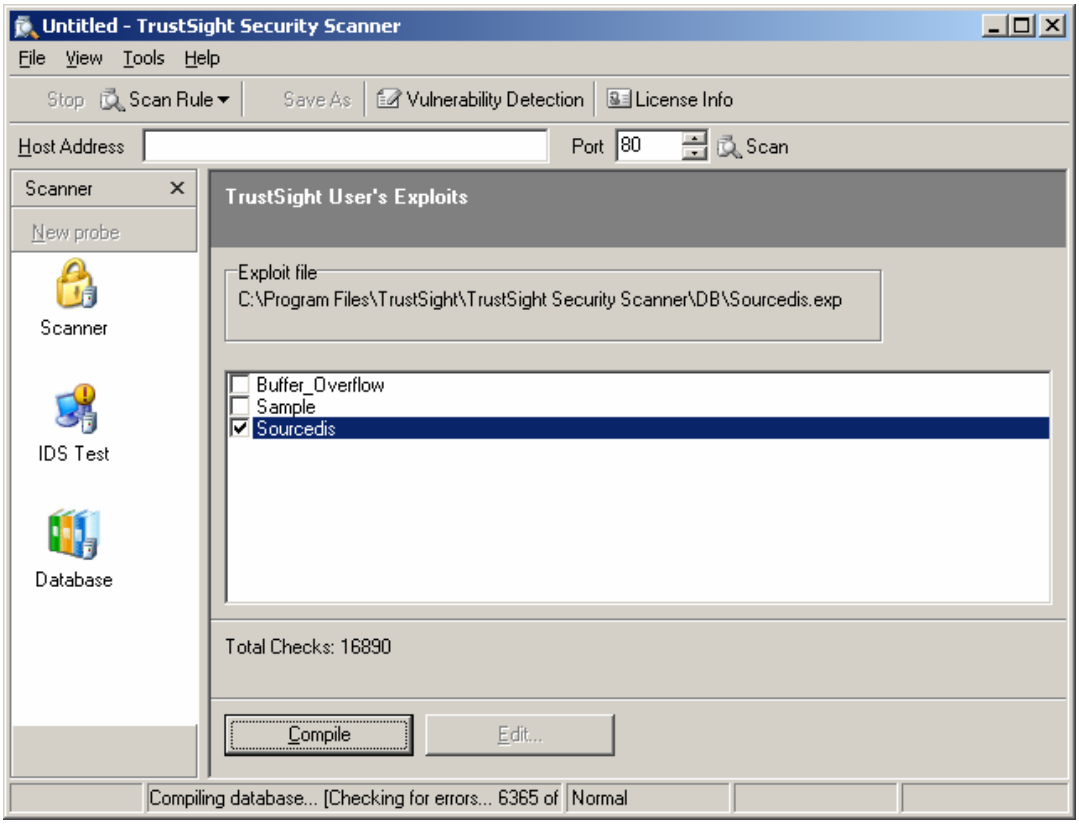


Slika 4: *Sučelje terminala za ručno ispitivanje sigurnosti Web aplikacija*

Odgovor je moguće pregledavati u normalnom obliku (čisti HTML kod), unutar Hex editora, kao Web stranicu (unutar ugrađenog Web preglednika), a pomoću posebnog filtra moguće je promatrati i samo komentare koji se nalaze unutar HTML koda.
Pritiskom na tipku Open URL zadana adresa otvara se unutar uobičajenog Web preglednika na sustavu.

4.2. Definiranje vlastitih testova

Unutar TrustSight Security Scanner alata administratorima je, u svrhu fleksibilnosti, ostavljena mogućnost definiranja vlastitih pravila skeniranja. Na taj način je prilikom skeniranja moguće na Web aplikaciju primijeniti proizvoljne testove koji odgovaraju specifičnim sigurnosnim potrebama korisnika.
Datoteke s proizvoljnim definicijama skeniranja smještaju se u poddirektorij Db glavnog instalacijskog direktorija alata. Sve datoteke s pravilima prikazati će se u glavnom prozoru programa odabirom opcije **Exploits->TrustSight's user exploits** iz **Tools** izbornika, nakon čega je moguće odabrati koje od datoteka će alat koristiti prilikom skeniranja. Potrebno je napomenuti da sve kreirane datoteke moraju nositi nastavak .exp ili se u suprotnom neće prikazati unutar prozora za odabir.



Slika 5: *Prozor za odabir korisnički definiranih pravila skeniranja*

Svaki zapis u datoteci sastoji se od upita i odgovora koji se očekuje od poslužitelja. Na primjer redak #GET /sample #500 podrazumijeva da se poslužitelju šalje upit za prikazom /sample direktorija, a kao rezultat se očekuje kod 500 (tj. greška na poslužitelju). Ukoliko u retku nije naveden očekivani odgovor, skener će pretpostaviti da se kao odgovor očekuje kod 200 koji označava da je na upit odgovoreno.

Jednostavna datoteka koja bi omogućavala provjeru specifičnog propusta unutar Microsoftovog IIS poslužitelja sadržavala bi samo jedan redak

```
#GET /index~1.sht
```

Nešto kompliciraniji redak poput

```
/sample.exe? * * HEAD 200 9 a
```

rezultirao bi upitom tipa

```
HEAD /sample.exe?aaaaaaaaa, uz koji se kao odgovor očekuje kod 200.
```

Datoteka sa pravilima koja bi omogućavala provođenje jednostavnog napada prepisivanjem spremnika izgledala bi ovako:

```
#INF Buffer Overflow
/sample.exe? * * GET 200 9 a

#INF Buffer Overflow 2
/sample.exe? * * HEAD 200 9 a

#INF Buffer Overflow 3
/sample.dll?data1= &data2=Hi * GET 200 9 A
```

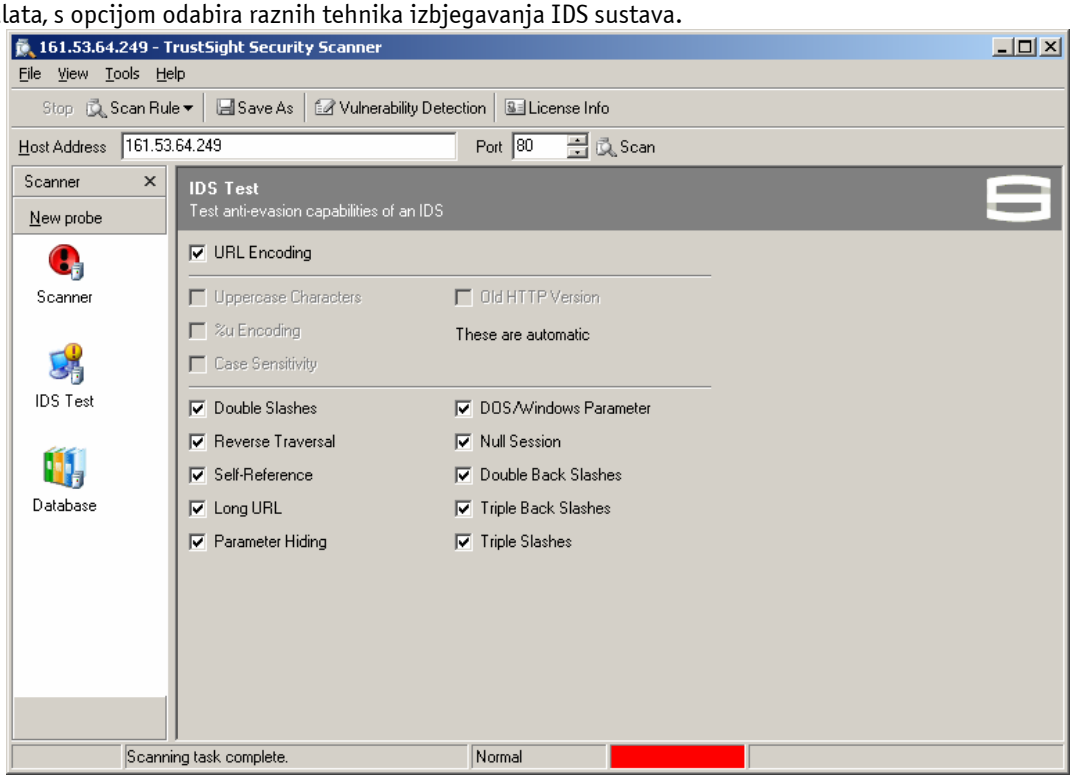
Korištenje ove opcije iskusnim korisnicima omogućuje prilagođavanje alata u svrhu automatiziranog otkrivanja ranjivosti unutar specifičnih, "*custom made*", Web aplikacija.

4.3. Korištenje *Proxy* poslužitelja

Još jedna od dodatnih mogućnosti ovog alata je i korištenje *proxy* poslužitelja preko kojeg je moguće izvoditi skeniranje tako da se prikrije stvarna IP adresa računala koje ga provodi. Odabir opcija za podešavanje *proxy* poslužitelja nalazi se unutar izbornika Tools->Network Settings...
U zadana polja potrebno je upisati IP adresu i odgovarajući mrežni port na kojem se nalazi *proxy* poslužitelj, kao i eventualnu lozinku za prijavljivanje na *proxy* poslužitelj.
Unutar ovog izbornika moguće je upisati i korisničko ime i lozinku koje će skener koristiti ukoliko na ispitivanom poslužitelju naiđe na direktorije koji za pristup zahtijevaju autorizaciju.

4.4. Izbjegavanje IDS sustava

Kao i većina sličnih alata, TrustSight Security Scanner koristi nekoliko tehnika izbjegavanja IDS sustava. Korištenje ove opcije može biti vrlo korisno, budući da se prilikom skeniranja Web poslužitelja automatski može provjeriti i funkcioniranje filtara na IDS sustavu.
Ova opcija uključuje se u izborniku View->Vulnerability Detection->IDS evasion, a izbor metoda izbjegavanja obavlja se pritiskom na link IDS Test u krajnjem lijevom prozoru. **Slika 6** prikazuje prozor alata, s opcijom odabira raznih tehnika izbjegavanja IDS sustava.



Slika 6: *Prozor za podešavanje parametra izbjegavanja IDS sustava*

Korisniku su na izbor ponuđene gotovo sve poznate metode izbjegavanja IDS sustava, kao što su npr.:

- **Kodiranje URL-a** (engl. *URL Encoding*) – zamjena znakova unutra URL-a znakovima oblika %xx, gdje x predstavlja broj u heskadecimalnom brojevnom sustavu.
- **Korištenje dvostrukog "/" znaka** (engl. *Double slashes*) – pokušaj zavaravanja IDS sustava korištenjem kombinacije / znakova unutar URL-a.
- **Referenciranje na trenutni direktorij** (engl. *Self-Reference*) – pokušaj neovlaštenog pristupa korištenjem referenci oblika '../' unutar URL-a. Na taj način, zahtjev oblika http://www-ime_poslužitelja.com/./cgi-bin, koji je u osnovi identičan zahtjevu http://www-ime_poslužitelja.com/cgi-bin, prošao bi nezapaženo od strane IDS sustava.
- **Skrivanje parametara** (engl. *Parameter Hiding*) – Skrivanje neovlaštenog zahtjeva unutar korisničkih parametara koji se prosljeđuju poslužitelju.

- **Korištenje dugačkih URL-ova** (engl. *Long URL*) – Skrivanje neovlaštenog zahtjeva unutar dugačkih URL-ova. Ovom tehnikom iskorištava se propust u konfiguraciji IDS sustava koji su podešeni tako da pregledavanju samo prvih nekoliko okteta svakog HTTP upita.
- **Korištenje Null znaka** (engl. *Null Session*) – Zaobilaženje provjere zahtjeva korištenjem NULL znaka unutar URL-a.
- **Korištenje višestrukih "/" i "\" znakova** – izbjegavanje IDS sustava korištenjem upita sintakse `/cgi-bin\primjer.cgi`, koji se smatraju legalnima na Microsoftovim Web poslužiteljima.

Više detalja o tehnikama izbjegavanja IDS sustava može se pronaći u dokumentu "Anti-IDS sustavi" koji se nalazi na službenim Web stranicama CARNet CERT-a.

5. Zaključak

TrustSight Securitiy Scanner je vrlo pouzdan i robustan alat, koji u velikoj mjeri olakšava postupak ispitivanja sigurnosti Web aplikacija. Velik broj mogućnosti koje nudi, kao i velika baza ranjivosti koja je korisniku na raspolaganju, čini ovaj alat jednim od vodećih u svojoj grupi, a ukupnom dojmu pridonosi i jednostavno grafičko sučelje koje olakšava provođenje skeniranja.

Alat je u potpunosti kompatibilan s CVE (engl. *Common Vulneravility Exposure*) listom ranjivosti, što manje iskusnim korisnicima olakšava prepoznavanje i ispravno tumačenje propusta pronađenih na Web poslužitelju i pratećim aplikacijama. Ipak, korištenje alata preporučuje se isključivo kvalificiranom osoblju, budući da loše podešeni parametri skeniranja mogu uzrokovati pojavljivanje vrlo velikog broja lažnih ranjivosti u konačnom izvještaju, kao i nasilni prekid rada testiranog Web poslužitelja.