

**Network Security Solutions d.o.o**

# Testiranje Web Aplikacija neinvazivnim tehnikama

**Beograd 2009.**

<http://www.netsec.rs>  
[office@netsec.rs](mailto:office@netsec.rs)

## Sadržaj

Network Security Solutions.....	2
O kompaniji.....	2
Istraživanje.....	2
Alati.....	2
Obuka.....	2
Tehnike testiranja.....	3
SQL injection, SQL error.....	3
Blind SQL injection.....	3
Cross Site Scripting (XSS).....	4
SPAM.....	4
Directory Listing.....	4
Information disclosure.....	5
Remote File Include (RFI).....	5

## Network Security Solutions

### O kompaniji

**Network Security Solutions** je jedna od malog broja kompanija u ovom delu Evrope, čiji je primarni poslovni fokus bezbednost informacionih sistema. Kompanija u svoje klijente ubraja poznate privatne, vladine i finansijske kuće, kao što su Microsoft, Dunav Osiguranje AD, Pepsi Srbija, EFG Eurobank, Univerzal i Opportunity banka, MUP Srbije i druge, za koje je radila bezbednosna rešenja od revizije i testiranja postojećih, preko projektovanja i implementacije novih, do održavanja već implementiranih sistema, uključujući mehanizme za detekciju i prevenciju napada, digitalnu zaštitu podataka, anti-virusnu zaštitu i drugo.

### Istraživanje

**Network Security Solutions** se izdvaja i istraživanjem na polju IT bezbednosti, te su kao rezultat toga pronađeni sigurnosni propusti u operativnim sistemima, komercijalnim i programima otvorenog koda, popularnim sistemima za video nadzor, web aplikacijama i sajtovima *Fortune 500* kompanija kao što su Microsoft, Yahoo, Oracle i brojne druge. Istraživački radovi su objavljeni na inostranim referentnim lokacijama poput Bugtraq, SecurityFocus i Secunie.

### Alati

Kompanija **Network Security Solutions** za potrebe obavljanja posla razvija i svoje softverske alate. Naš "*DFP Scanner*" je od inostranih kolega svrstan u TOP 10 skenera u svetu u svojoj kategoriji i kao i *WMAT (Web Mail Attack Tool)* alat predstavlja našu firmu na najnovijoj Linux *BackTrack* distribuciji.

Najpopularniji softverski alati za testiranje ranjivosti sistema kao što je na primer "*Nessus*", koriste u svom radu, između ostalog i testove zasnovane na istraživanjima naše kompanije.

### Obuka

Zaposleni u kompaniji svoje znanje stečeno kroz dugogodišnje bavljenje bezbednošću informacionih sistema prenose kolegama kroz različite kurseve, stručne radionice i predavanja.

"*Testiranje bezbednosti sistema – Ethical Hacking*" je kurs koji polaznicima omogućava upoznavanje sa realnim hakerskim tehnikama, kao i metodama odbrane od takvih napada, a osmišljen je u potpunosti od strane naših stručnjaka i prvi je kurs tog tipa u našoj zemlji.

## Tehnike testiranja

Prilikom procene bezbednosti web aplikacija mogu se koristiti razne tehnike koje u manjoj ili većoj meri mogu ostaviti trag ili posledice testiranja. Kako bi potpuno prevazišli potencijalne probleme možemo koristiti takozvane neinvazivne tehnike koje nam omogućavaju manipulaciju funkcijama web aplikacija, bez namere da ih ugrozimo u bezbedonosnom smislu ili da ostvarimo pristup podacima.

Tehnike se uglavnom svode na specifične konstrukcije zahteva, takozvane test vrednosti koje se prosleđuju isključivo kroz *browser*.

Pogledajte primere tehnika koje se koriste kako bi pronašli određene tipove propusta:

### SQL injection, SQL error

- Ovi tipovi napada dozvoljavaju manipulaciju SQL upitima ka bazi podataka, kao i otkrivanje vitalnih informacija koje mogu biti pročitane prilikom pogrešno podešenog sistema za prikaz grešaka.

Test vrednosti (u okviru HTTP zahteva):

```
'
%
';
%';
“,'
```

### Blind SQL injection

- Ovaj tip propusta dozvoljava manipulaciju SQL upita bez vizuelnog prikazivanja podataka.

Test vrednosti (u okviru HTTP zahteva):

```
[vrednost parametra]+1
([vrednost parametra]+1)
([vrednost parametra]+X)
```

## Cross Site Scripting (XSS)

- Ovi tipovi propusta dozvoljavaju ubacivanje i izvršavanje malicioznog HTML i/ili Script koda u okviru korisničke sesije.

Test vrednosti (u okviru HTTP zahteva):

```
"test  
<test  
test>  
'test  
<'test"  
<test'"  
<test>
```

## SPAM

- Ovi tipovi propusta omogućavaju manipulaciju web formama koje imaju opcije slanja email poruka. Njihova eksploatacija omogućava slanje SPAM/PHISHING poruka sa adrese "proverenog" posiljaoca.

Test vrednosti (u okviru HTTP zahteva):

```
%0d%0a  
\r\n  
,  
;
```

Dodatne metode uključuju pregled HTML izvornog koda stranica u potrazi za sakrivenim ulaznim vrednostima.

## Directory Listing

- Ova opcija web servera omogućava pregled svih fajlova u direktorijumu ukoliko ne postoji "glavni" fajl.

Testiranje se vrši jednostvanim pozivom bilo kog direktorijuma na web serveru, npr style/.

## Information disclosure

- Ova klasa propusta otkriva vitalne informacije web aplikacije, web servera i/ili korisnika aplikacije.

Testiranje se svodi na čitanje HTML izvorog koda stranica u potrazi za:

- a) HTML komentarima koje su ostavili programeri ili dizajneri
- b) Internim putanjama koje su ostale prilikom prebacivanja aplikacije na javni server
- c) Informacijama koje otkrivaju verzije pojedinih delova sistema ili celog sistema
- d) Skrivenim HTML ulaznim vrednostima
- c) Putanjama ka *backup* fajlovima
- e) ...

## Remote File Include (RFI)

- Ovaj tip propusta omogućava učitavanje udaljenih resursa.

Testiranje se vrši promenom jednog karaktera u okviru zahteva kako bi se uočila razlika u odzivu aplikacije.

Ovo su osnovne tehnike za otkrivanje sigurnosnih propusta u web aplikacijama, bez nanošenja štete i korišćenja dodatnih alata. Sve test vrednosti se prosleđuju kroz forme ili HTTP zahteve u okviru *browsera*. Na osnovu odziva aplikacije možemo zaključiti da li postoji određeni propust ili ne.

Posebno treba obratiti pažnju na izbegavanje višestrukog ponavljanja ovih zahteva kako bi izbegli detektovanje od strane ugrađenih odbrambenih sistema ili kako bi izbegli takozvani *Denial of Service* napad.

Dugogodišnje iskustvo u testiranju web aplikacija može da potvrdi da su ove metode u 90% slučajeva bile efikasne.