

Network Security Solutions d.o.o.

Sinergija09 :: Akcija

Rezultati

24-Dec-09

Sadržaj

Uvod	2
Propusti po tipu	3
Legenda propusta	4
Propusti po riziku	6
Legenda rizika	6
Odnos rizik : broj web prezentacija sa datim nivoom rizika	7

Uvod

Network Security Solutions je u saradnji sa kompanijom **Microsoft Software** ove godine poklonila zainteresovanim firmama učesnicama Sinergije09, bez obzira na broj prijavljenih posetilaca konferencije, po jednu besplatnu osnovnu procenu bezbednosti web sajta.

Na osnovu istraživanja SANS instituta, više od 60% napada uočenih na Internetu su napadi na web aplikacije, a utvrđeno je i da preko 90% web prezentacija ima jedan ili više propusta sa OWASP TOP 10 liste. Bezbednosni propusti u web aplikacijama mogu imati za posledicu gubitak intelektualne svojine i podataka klijenata, kao i negativan uticaj na imidž kompanije, te prestanak izvršenja servisa i brojne druge sistemske, finansijske i zakonske konsekvence.

Firma **Network Security Solutions** je u toku ove akcije testirala 32 web prezentacije, od malih web prodavnica, preko sajtova pojedinih ministarstava do velikih finansijskih institucija.

Ni za jedan web sajt nismo bili u prilici da pošaljemo prazan izveštaj, a statistika kaže da po broju i nivou rizika bezbednosnih propusta pratimo svetske trendove.

Kao poseban podatak koji se ne nalazi u statistici, izdvojili bi smo to da se od velikog broja kompanija prijavljenih za Sinergiju09, samo mali broj odlučio da utvrdi da li su njihovi, kao i podaci njihovih klijenata bezbedni. To govori o velikoj i urgentnoj potrebi sprovođenja široke kampanje podizanja nivoa bezbednosne kulture (security awareness) u našoj zemlji.

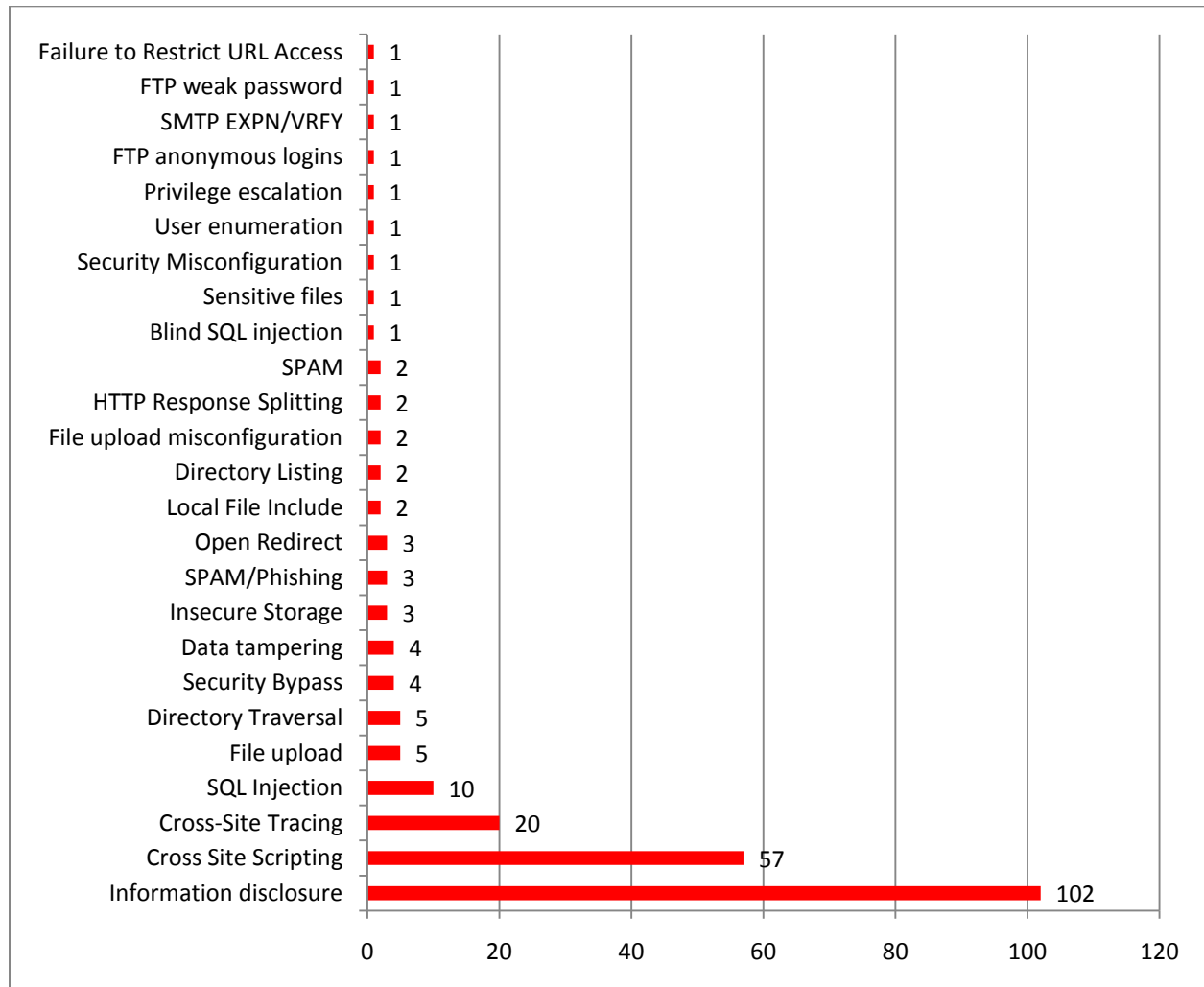
U nastavku izveštaja, možete videti grafikone ranjivosti po tipu, nivou rizika, kao i odnos broja prezentacija i kategorija rizika kao i kratak opis ranjivosti po tipu i opis nivoa rizika.

Network Security Solutions želi da se zahvali kompaniji **Microsoft Software** na podršci i organizaciji akcije besplatne procene bezbednosti, kao i svim firmama učesnicama.

Beograd, 24.12.2009. god.

Propusti po tipu

Na donjem grafikonu se mogu videti bezbednosni propusti po tipu.



Legenda propusta

Information disclosure

- Pristup informacijama čija važnost sama po sebi nije vitalna ali može da otkrije tragove za dalju istragu.

Blind SQL injection

- Manipulacija SQL upitima bez vizuelne kontrole napada.

Cross Site Scripting

- Izvršavanje HTML/SCRIPT koda u okviru korisničke sesije.

Sensitive files

- Pristup fajlovima koji sadrže vitalne informacije o sistemu, aplikaciji, korisnicima i slično.

Cross-Site Tracing

- Potencijalna eksploatacija TRACE HTTP metoda.

File upload

- Pristup opciji za upload fajlova na web server bez adekvatne provere tipa fajla.

Insecure Storage

- Čuvanje vitalnih informacija na klijent strani, čuvanje vitalnih informacija na javno dostupnom mestu.

Security Bypass

- Zaobilaženje ugrađenje zaštite.

Local File Include

- Ucitavanje fajlova sa lokalnih resursa.

Directory Traversal

- Neautorizovano prelaženje u direktorijume sistema iz direktorijuma web aplikacije.

SPAM/Phishing

- Ekploatacija kontakt formi sa mogućnošću kreiranja sadržaja po izboru napadača.

SQL Injection

- Manipulacija SQL upitima.

Directory Listing

- Listanje sadržaja fajlova u direktorijumu web sajta.

File upload misconfiguration

- Pristup opciji za upload fajlova na web server sa pogrešnom postavkom bezbednosnih opcija.

Data tampering

- Kreiranje lažnih podataka, u okviru određenog dela sistema, presretanjem zahteva.

Security Misconfiguration

- Pogrešno postavljeni sigurnosni parametri .

User enumeration

- Popis korisnika sistema.

Privilege escalation

- Eskalacija privilegija.

HTTP Response Splitting

- Manipulacija HTTP zahtevima.

Open Redirect

- Javna opcija redirekcije korisnika.

FTP anonymous logins

- Anonimno logovanje FTP korisnika.

SPAM

- Eksploatacija kontakt formi sa ciljem slanja SPAM poruka.

SMTP EXPN/VRFY

- Popis korisnika kroz SMTP opcije.

FTP weak password

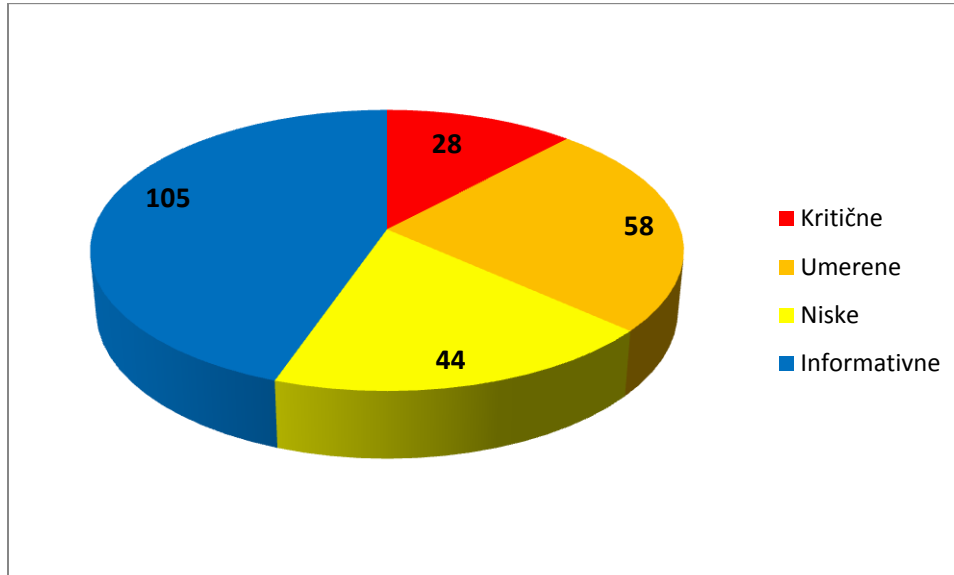
- Jednostavna FTP šifra.

Failure to Restrict URL Access

- Zaobilaznje zaštite direktnim pozivanjem resursa kroz URL.

Propusti po riziku

Na donjem grafikonu se vide bezbednosni propusti po kategoriji rizika.



Legenda rizika

Kritične ranjivosti

- U zavisnosti od tipa aplikacije označava pristup lokalnom sistemu, eskalaciju privilegija do najvišeg nivoa ili potencijalni pristup vitalnim informacijama o korisnicima/administratorima kroz eksploataciju određenog propusta.

Umerene ranjivosti

- Potencijalni pristup vitalnim informacijama o korisnicima/administratorima kroz eksploataciju određenog propusta uz otežane uslove eksploatacije. Pristup lokalnim resursima.

Niske ranjivosti

- Veoma teški uslovi eksploatacije propusta koji mogu da dovedu do pristupa vitalnim informacijama.

Informativne

- Pristup informacijama čija vaznost sama po sebi nije vitalna ali može da otkrije podatke koji omogućavaju bolju pripremu napada od strane napadača.

Odnos rizik : broj web prezentacija sa datim nivoom rizika

Na donjem grafikonu se može videti broj prezentacija koje su imale određene kategorije bezbednosnih rizika. Trećina testiranih web prezentacija ima kritične ranjivosti.

