Statistika bezbednosnih propusta web prezentacija banaka u Srbiji

Network Security Solutions d.o.o.
http//www.netsec.rs
office@netsec.rs

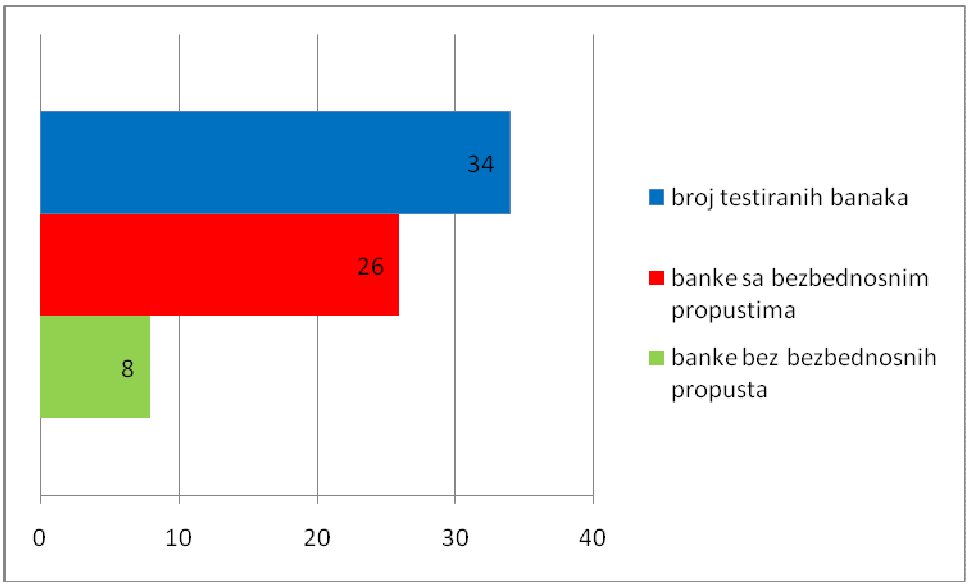
Beograd, 2009. god.

Sadržaj

Uvod

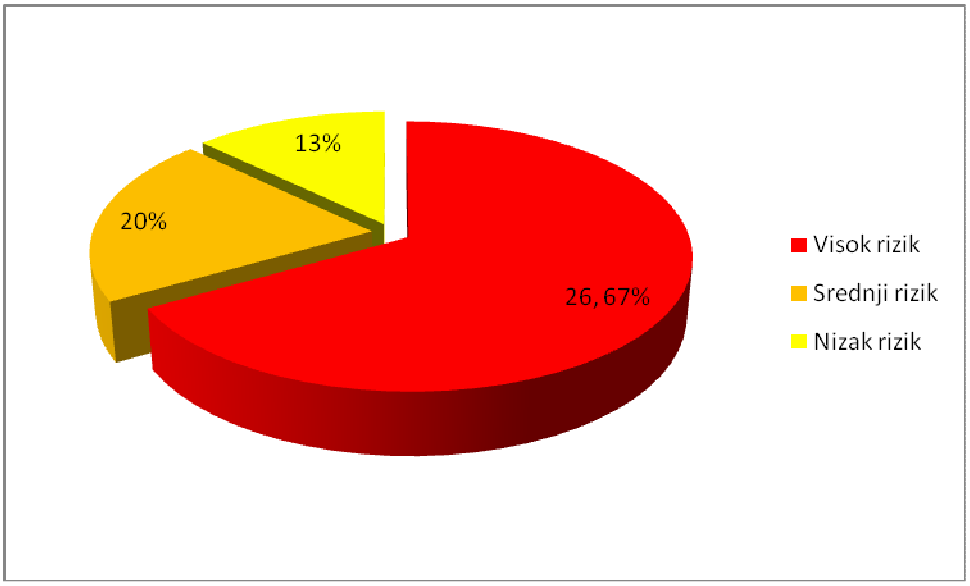
U cilju kreiranja statistike bezbednosti web sajtova banaka u Srbiji, testirane su sve web prezentacije koje se mogu naći na lokaciji "Udruženje banaka Srbije": http://www.ubs-asb.com/s/Clanice.htm, ukupno: 34.

Od 34 web prezentacije na samo 8 nisu pronađeni sigurnosni propusti u roku od 10 minuta. Sve pronađene ranjivosti spadaju u TOP 10 bezbednosnih propusta po međunarodno priznatoj OWASP listi (http://www.owasp.org/).



Slika: Banke sa i bez propusta

Od 39 pronađenih propusta 26 možemo smatrati kritičnim jer omogućavaju izvršavanje malicioznih napada koji direktno mogu naneti štetu korisnicima i/ili samoj web prezentaciji.



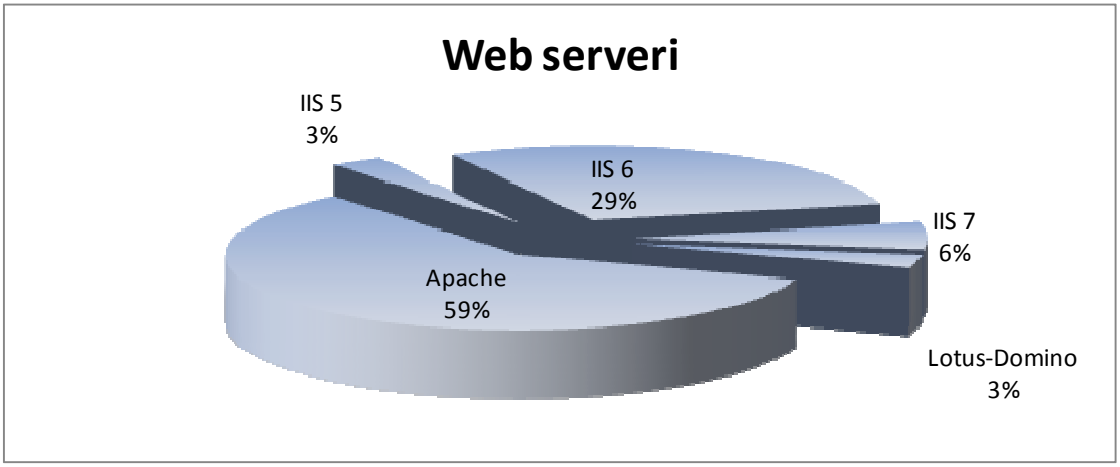
Slika: Raspodela ranjivosti po kategorijama

Napomena:
Konsultanti firme **Network Security Solutions d.o.o.** ni u jednom trenutku nisu imali neovlašćen pristup serveru niti podacima. **Nisu** testirane "E-banking" aplikacije , operativni sistemi servera, kao ni aktivna mrežna oprema. Korišćene su isključivo neinvazivne tehnike testiranja. Više o navedenim tehnikama: (http://netsec.rs/UserFiles/File/Testiranje%20Web%20Aplikacija%20neinvazivnim%20tehnikama.pdf).
Za svaku web prezentaciju utrošeno je po **10 minuta**.

Tehnički detalji

- Rezultati testiranja su dobijeni korišćenjem uobičajnih metoda (posete web prezentacija kroz web čitač) i korišćenjem neinvazivnih test vrednosti za manipulisanje parametrima.
- Samo jedna web aplikacija radi pod “SSL”-om a 12 koriste “Google Analytics”.
- “SSL” može da posluži kao odlična zaštita u “Man-in-the-middle” napadima.
- Korišćenje javno dostupnih i besplatnih servisa može dovesti do iznenadnih prekida u radu, kao i “curenja” informacija.

Sledeći grafik pokazuje procenat tipova web servera koje koriste pomenute prezentacije:



Klasifikacija propusta

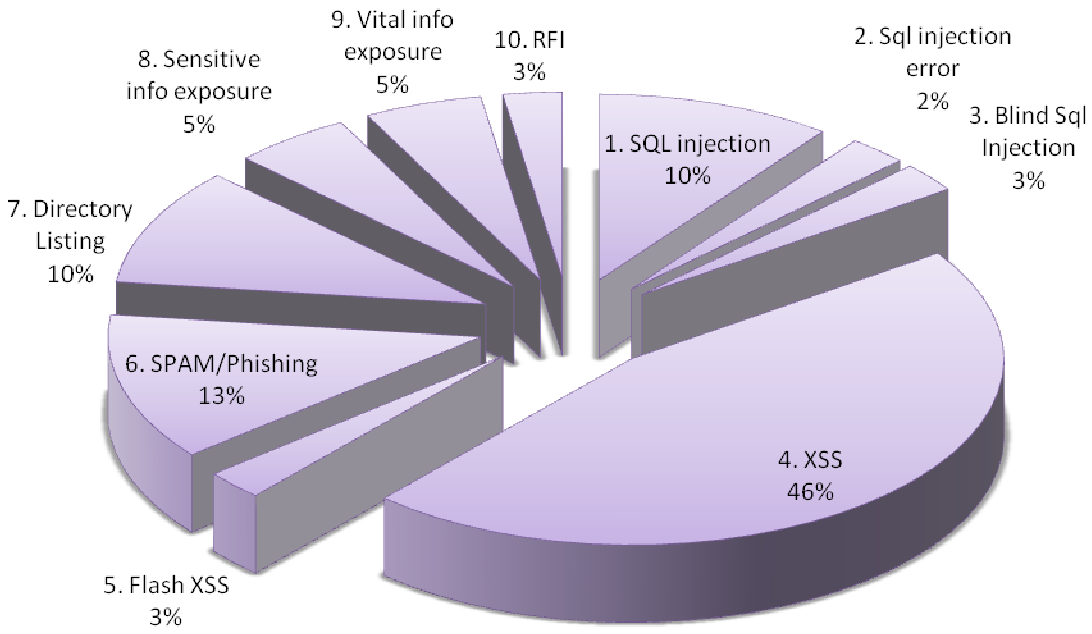
Dole su navedeni propusti koji su pronadjeni na web prezentacijama, njihov kratki opis i svrha eksploatacije:

1. Izmena SQL upita (eng. SQL injection)
2. Izmena SQL upita u cilju dobijanja vitalnih informacija iz poruka o greškama
3. Izmena SQL upita bez “vidljivih” promena (eng. Blind SQL injection)
4. Izmena i izvršavanje HTML/Script koda u okviru stranice (eng. Cross Site Scripting - XSS)
5. Izmena parametara Flash aplikacija u cilju izvršavanja HTML/Script koda
6. Izmena parametara formi za slanje email poruka, sa ciljem slanja “SPAM” ili “Phishing” poruka
7. Uključena opcija pregleda direktorijuma koja omogućava pristup vitalnim fajlovima
8. Otkrivanje vitalnih informacija nižeg nivoa (interne adrese, komentari, …)
9. Otkrivanje vitalnih informacija višeg nivoa (šifre)
10. Učitavanje udaljenih resursa (eng. Remote File Include)

Napomena:
Konsultanti firme Network Security Solutions d.o.o. ni u jednom trenutku nisu pokušali da izvrše eksploataciju ovih propusta tako da su moguće greške u rezultatima zbog netačnih podataka.

Detalji propusta

Ukupno je pronađeno 39 sigurnosnih propusta. Procentualna podela se može videti na sledećem grafiku:



Zaključak

Pronađeni propusti potencijalno omogućavaju široku lepezu napada kako na korisnike tako i na sisteme testiranih banaka i to od otkrivanja tehničkih detalja o informacionim sistemima banaka, lažnog predstavljanja i korišćenja servera za neautorizovano slanje email poruka korisnicima a u ime banke, preko krađe identiteta i akreditiva za pristup aplikacijama za elektronsko bankarstvo do direktnog pristupa poverljivim informacijama i računima korisnika što može dovesti do krađe ličnih podataka i novca.
Iako mnogi od ovih napada podrazumevaju određene preduslove da bi bili uspešno izvedeni, iskustvo govori da strpljiv napadač pre ili kasnije uspe da ih stvori.
Kompanija Network Security Solutions d.o.o. preporučuje poštovanje ISO/IEC 27001/27002 i PCI-DSS standarda kao osnova za uspostavljanje bezbednih informacionih sistema.