Statistika bezbednosnih propusta web prezentacija banaka u Srbiji / godina 2011

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

Beograd, 2011. god.

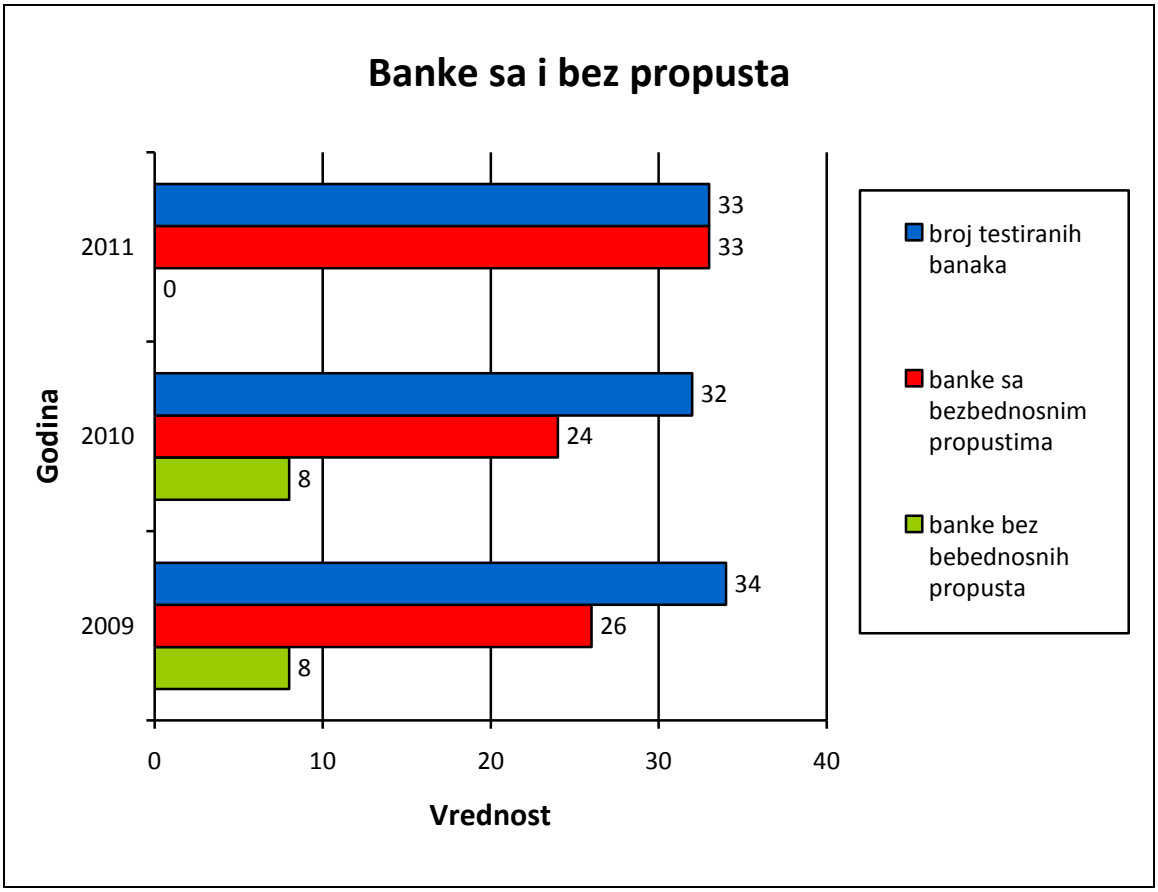
NETWORK SECURITY SOLUTIONS

Sadržaj

Uvod

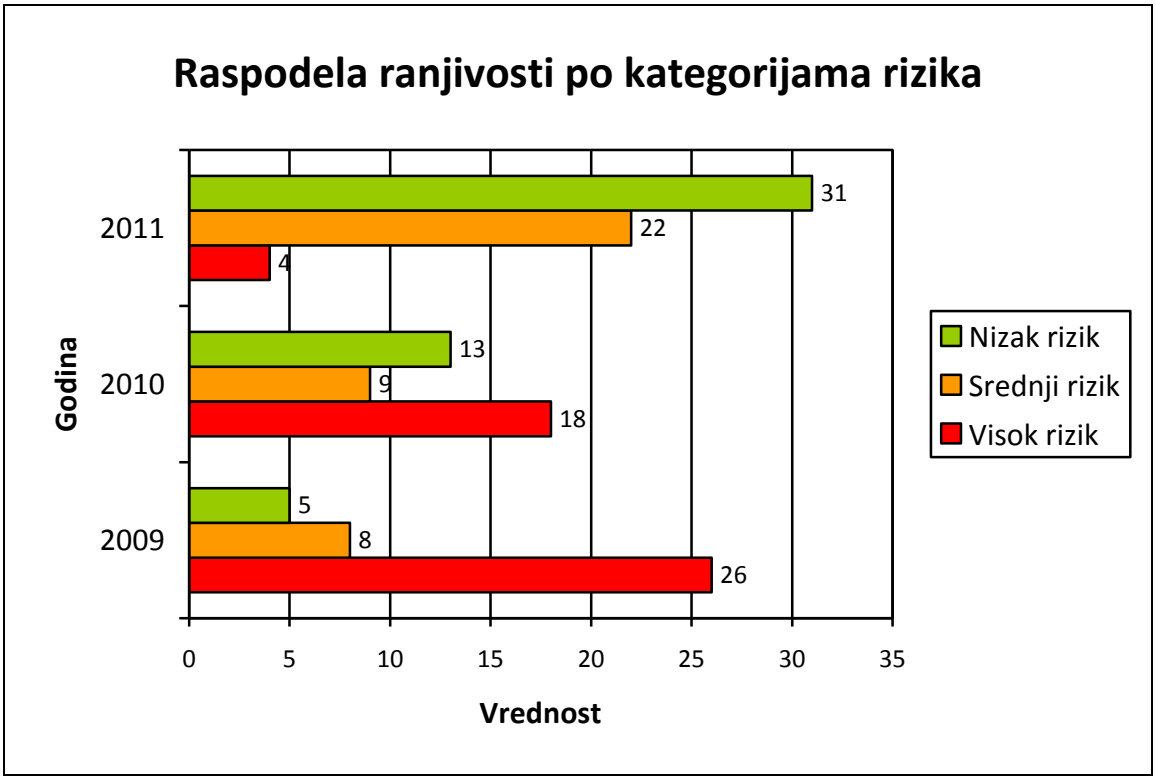
U cilju kreiranja statistike bezbednosti web sajtova banaka u Srbiji, testirane su sve web prezentacije koje se mogu naći na lokaciji “Udruženje banaka Srbije”: http://www.ubs-asb.com/Default.aspx?tabid=66, ukupno: 33.

U roku od 10 minuta, po web lokaciji, pronađeni su propusti na svim web prezentacijama članica udruženja. Pronađene ranjivosti između ostalog spadaju i u TOP 10 bezbednosnih propusta po međunarodno priznatoj OWASP listi (http://www.owasp.org/).



Od 57 pronađenih propusta, u godini 2011, 4 možemo smatrati kritičnim jer potencijalno omogućavaju pristup izvornom kodu, podacima o bazi podataka i manipulaciju podacima u bazi podataka.

Propusti koji dozvoljavaju izvršavanje HTML i SCRIPT koda, kao i propusti koji omogućavaju slanje EMAIL poruka sa web servera banaka svrstani su u kategoriju srednjeg rizika.



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 možete pročitati u dokumentu „**Testiranje Web Aplikacija neinvazivnim tehnikama - Network Security Solutions 2009**".

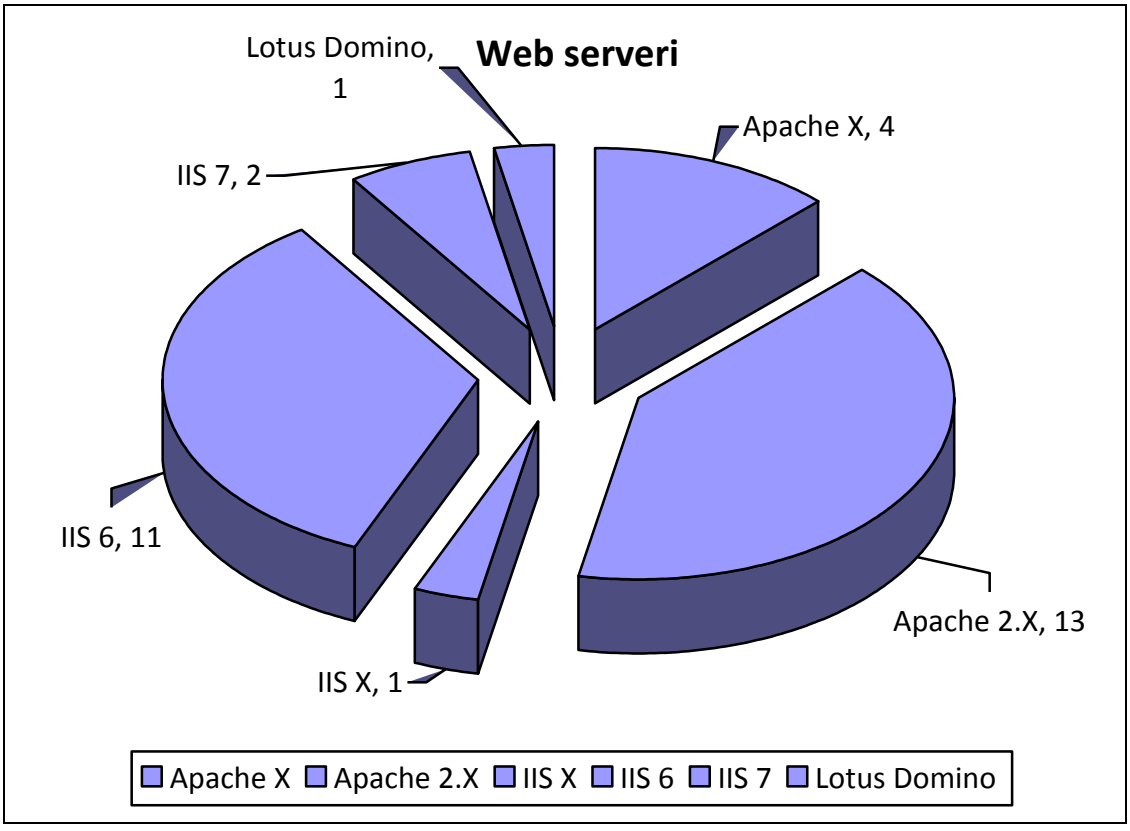
Za svaku web prezentaciju utrošeno je po 10 minuta. I tokom testiranja korišćen je samo *internet browser*.

Tehnički detalji

- Rezultati testiranja su dobijeni korišćenjem uobičajnih metoda (posete web prezentacija kroz web čitač) i korišćenjem neinvazivnih test vrednosti za manipulisanje parametrima.
- Tri web prezentacije rade pod "SSL"-om (ili bar delimično)
- Dvadeset i četiri koriste udaljene biblioteke poput "*Google Analytics*"' –a
- "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 do "curenja" informacija.

- Određene prezentacije koriste gotova rešenja poput: *Active Z CMS, cMASS, Drupal, ECMS, gPortal,* ***Joomla 1.5****, MODx, Omnicom OCP, TYPO3*
- Tehnologije koje se koriste su: ASP, ASP.NET, Microsoft Share Point, Microsoft Office Web Server, JSP, Notes Storage Facility, DAV/2, **PHP 4.x**, PHP 5.x
- Korišćenje javno dostupnih rešenja može da poveća opasnost od napada, a otkrivanje korišcenih tehnologija potencijalnom napadaču pomaže u biranju alata i pristupa.

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:

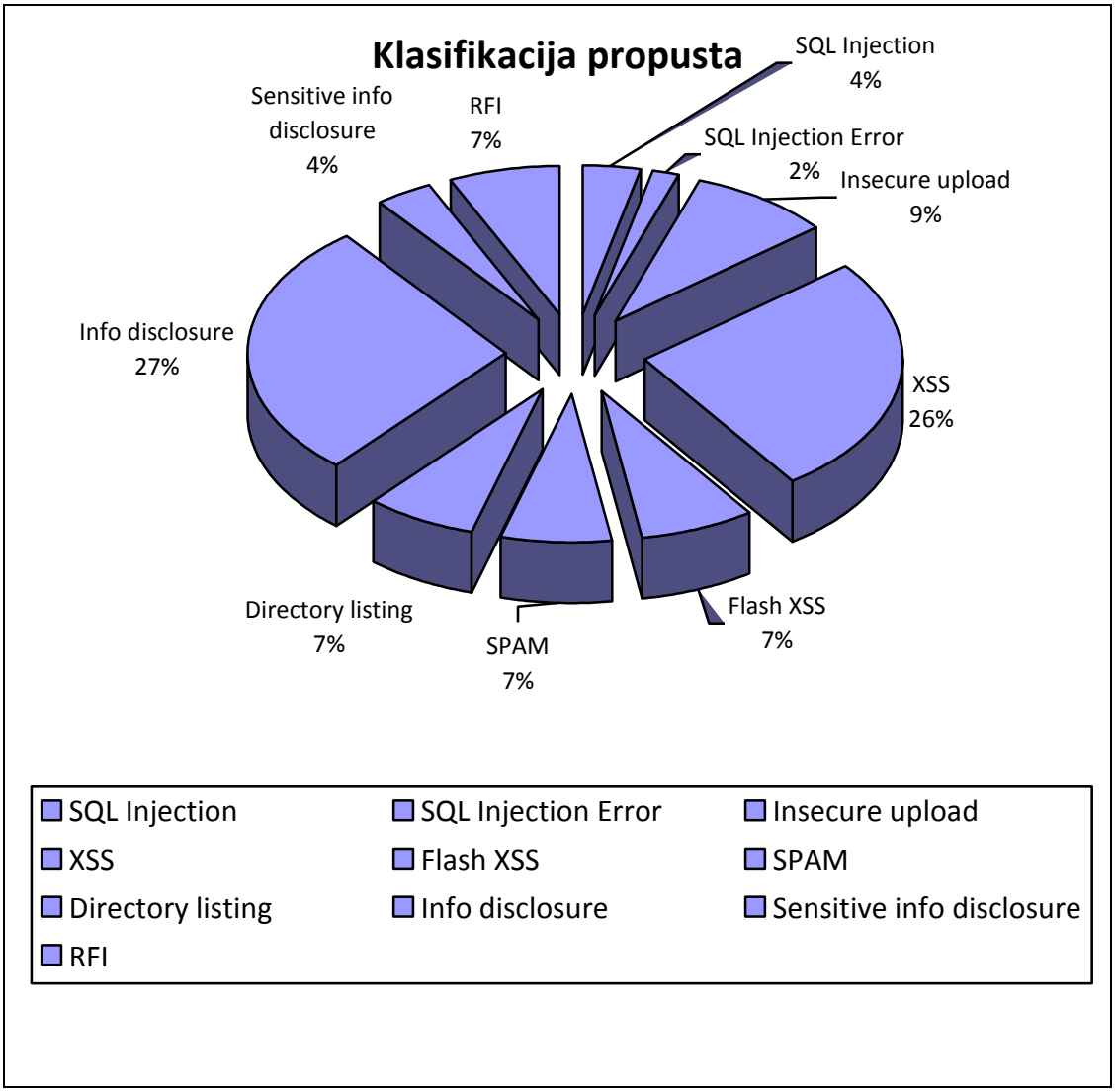
1. Izmena SQL upita (eng. SQL injection)
2. Izmena SQL upita u cilju dobijanja vitalnih informacija iz poruka o greškama
3. Nebezbedan *upload* fajlova (otkrivanje *upload* lokacija, slanje izvršnih fajlova)
4. Izmena i izvršavanje *script* koda u okviru stranice (eng. Cross Site Scripting - XSS)
5. Izmena parametara Flash aplikacija u cilju izvršavanja *script* koda
6. Izmena parametara formi za slanje email poruka, sa ciljem slanja *SPAM* i/ili *PHISHING* poruka
7. Uključena opcija pregleda direktorijuma koja omogućava pristup vitalnim fajlovima
8. Otkrivanje vitalnih informacija nižeg nivoa (interne adrese, stranice za logovanje, …)
9. Otkrivanje vitalnih informacija višeg nivoa (šifre, korisnički podaci)
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 57 bezbednosnih 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.

Linkovi:

http://netsec.rs/71/dokumenti.html
https://www.pcisecuritystandards.org/