

(Ne)bezbednost banaka u Srbiji

Dejan Levaja

Network Security Solutions

<http://www.netsec.rs>

O nama

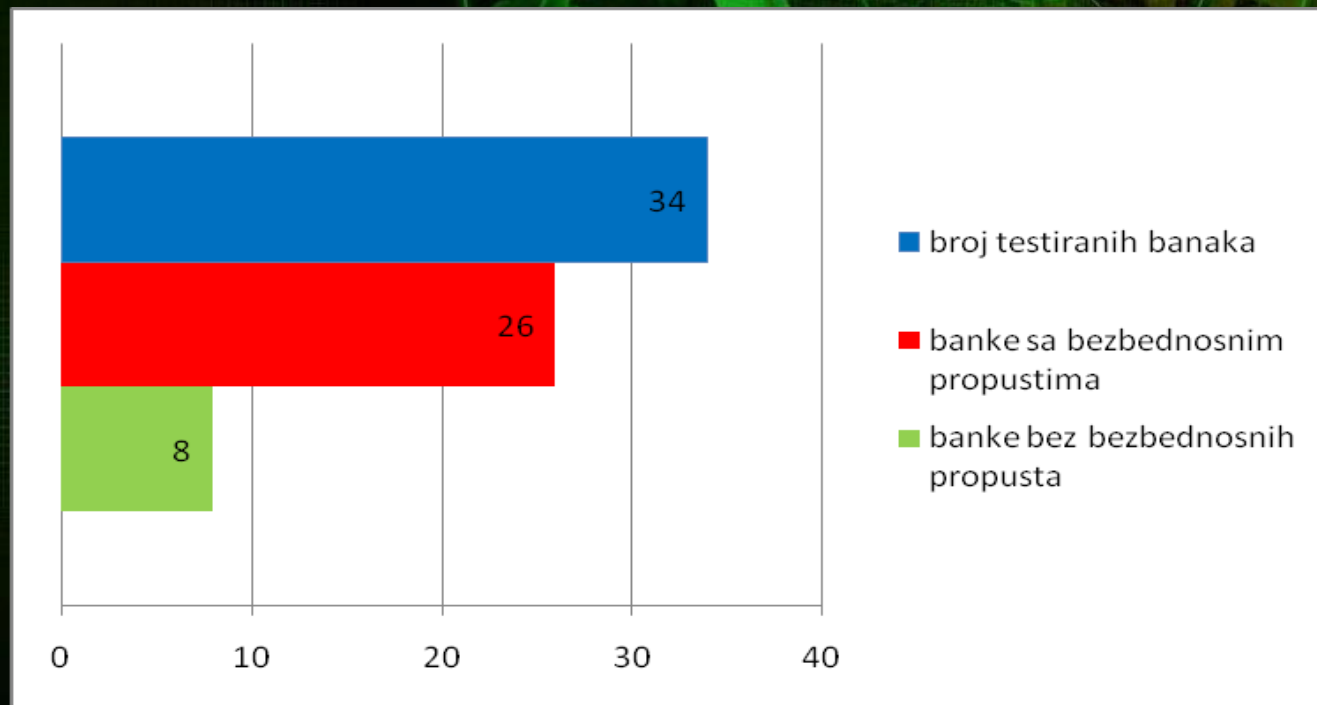
- Network Security Solutions :: <http://www.netsec.rs>
 - Bavimo se isključivo bezbednošću informacionih sistema
 - projektovanje
 - implementacije
 - održavanje
 - Ethical Hacking (testiranje bezbednosti)
 - istraživanje
 - secunia, bugtraq, milw0rm (sada *exploit-db.com*)
 - Microsoft Security Researchers Acknowledgement
 - tools
 - BackTrack4
 - Nessus
 - OWASP
 - edukacija

Uvod

- Dva jednostavna pitanja:
 - Da li vam je ikada “provaljeno” u sistem?
 - Kako znate?

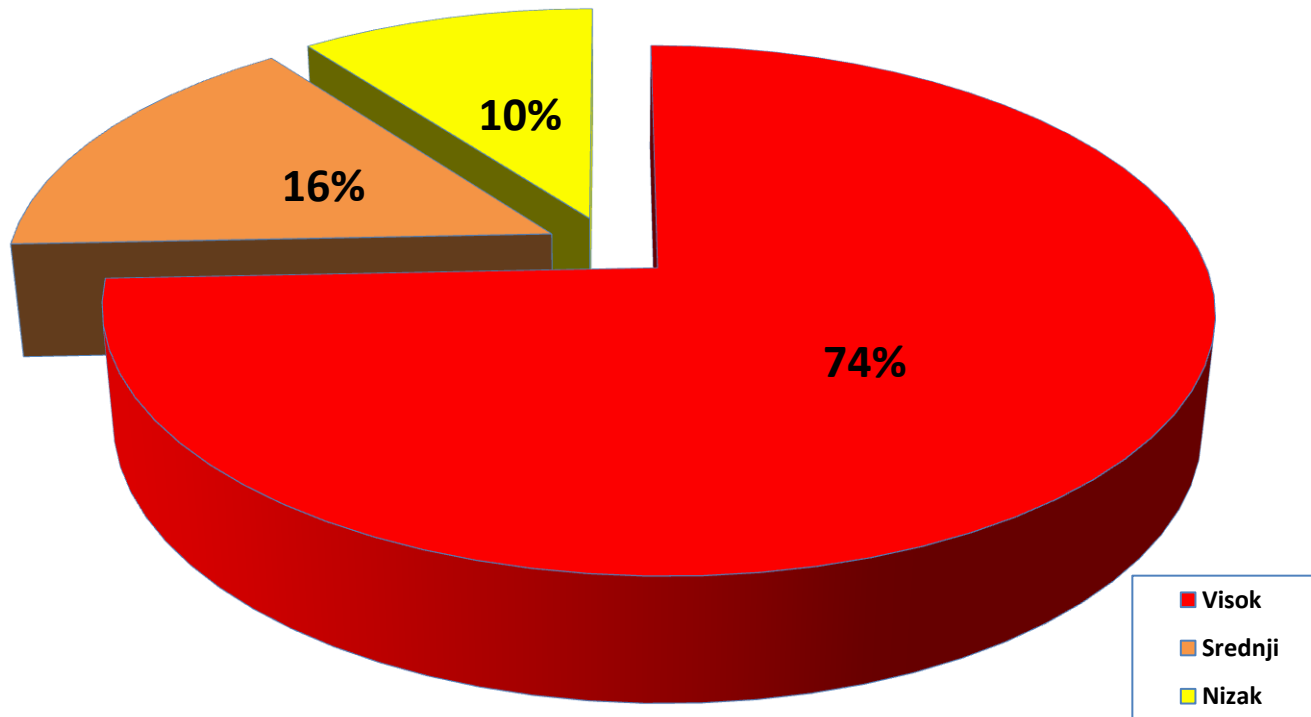
Istraživanje

- Istraživanje - avgust 2009.
- 34 banke
- neinvazivne tehnike (<http://netsec.rs/71/dokumenti.html>)
- 10 minuta po sajtu



Ranjivosti po nivou rizika

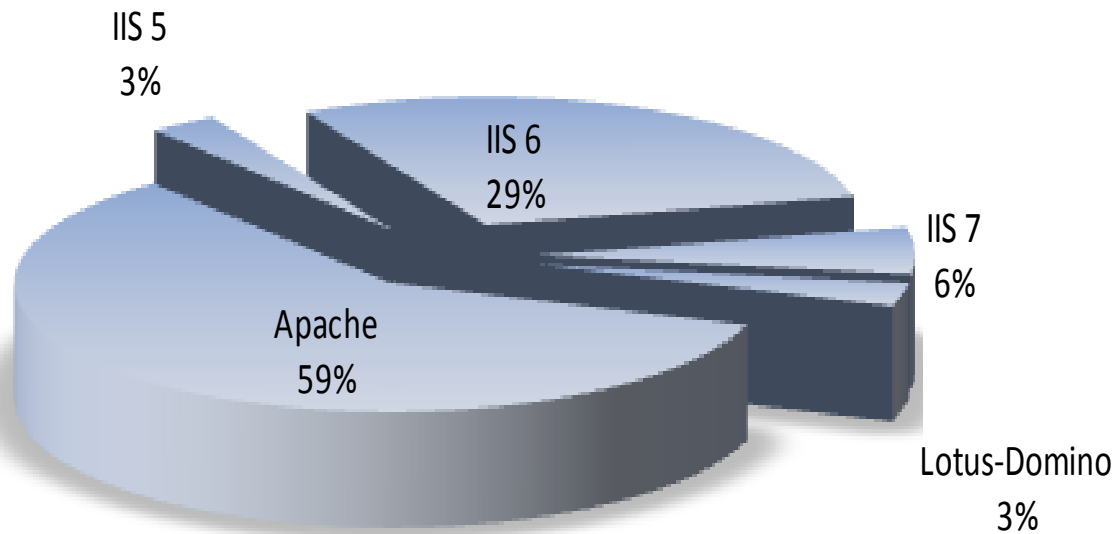
- 39 ranjivosti



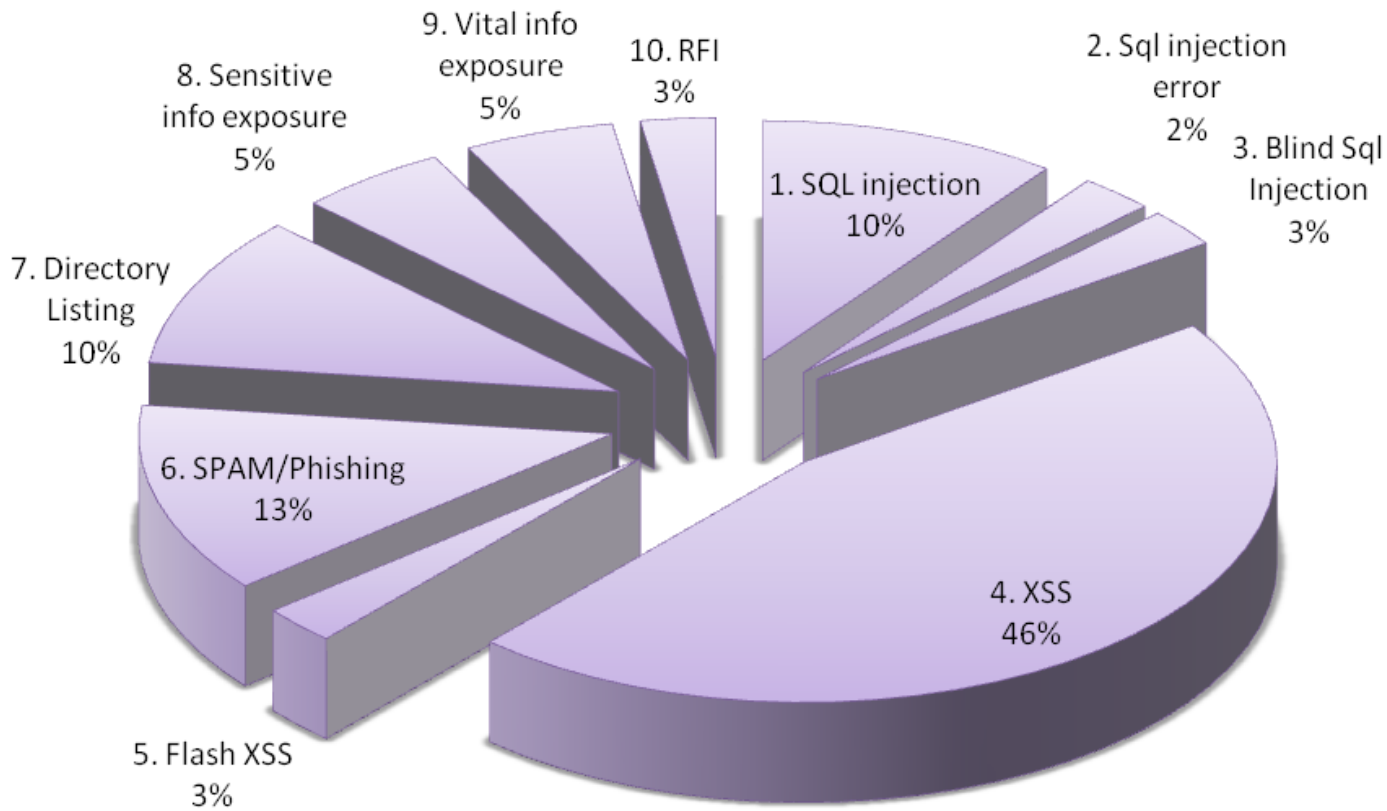
Web serveri

- Apache, IIS, Lotus Domino...

Web serveri



Detalji propusta



Potencijalna zloupotreba

- Otkrivanje tehničkih detalja o informacionim sistemima banaka.
- Lažno predstavljanje i korišćenja servera za neautorizovano slanje email poruka klijentima u ime banke.
- Krađa identiteta i akreditiva za pristup aplikacijama za elektronsko bankarstvo .
- Direktan pristup poverljivim informacijama i računima korisnika.
- _____ dodajte svoju ideju...

Eventualna rešenja

- ISO/IEC 27001, 27002
- PCI DSS
- Edukacija IT osoblja
- Redovno testiranje bezbednosti sistema
 - ne obeležavajte svoj sajt kao bezbedan!
 - testirajte sistem [redovno]!
 - testirajte svoje pentestere [povremeno]!





dejan.levaja@netsec.rs