

# Bezbednost internet sajtova banaka u Srbiji

Ivan Marković  
Network Security Solutions  
<http://netsec.rs/>

Beograd - iSEC 2011

# O nama / Projektovanje, Implementacija, Održavanje, Ethical Hacking (testiranje bezbednosti)

**Network Security Solutions d.o.o.** je nastala iz potrebe da se kompanijama jugoistočne Evrope pruži svetski nivo usluga vezanih za IT bezbednost. Svetski priznati stručnjaci zaposleni u Network Security Solutions rade na ispunjavanju misije kompanije - podizanju svesti o IT bezbednosti i zaštiti informacionih sistema klijenata.

Ponosni smo na našu listu referenci, istraživanja i alata, koja je rezultat godina rada u ovoj oblasti i verujemo da je kredibilitet stečen tokom tih godina najbolja preporuka našim budućim klijentima.

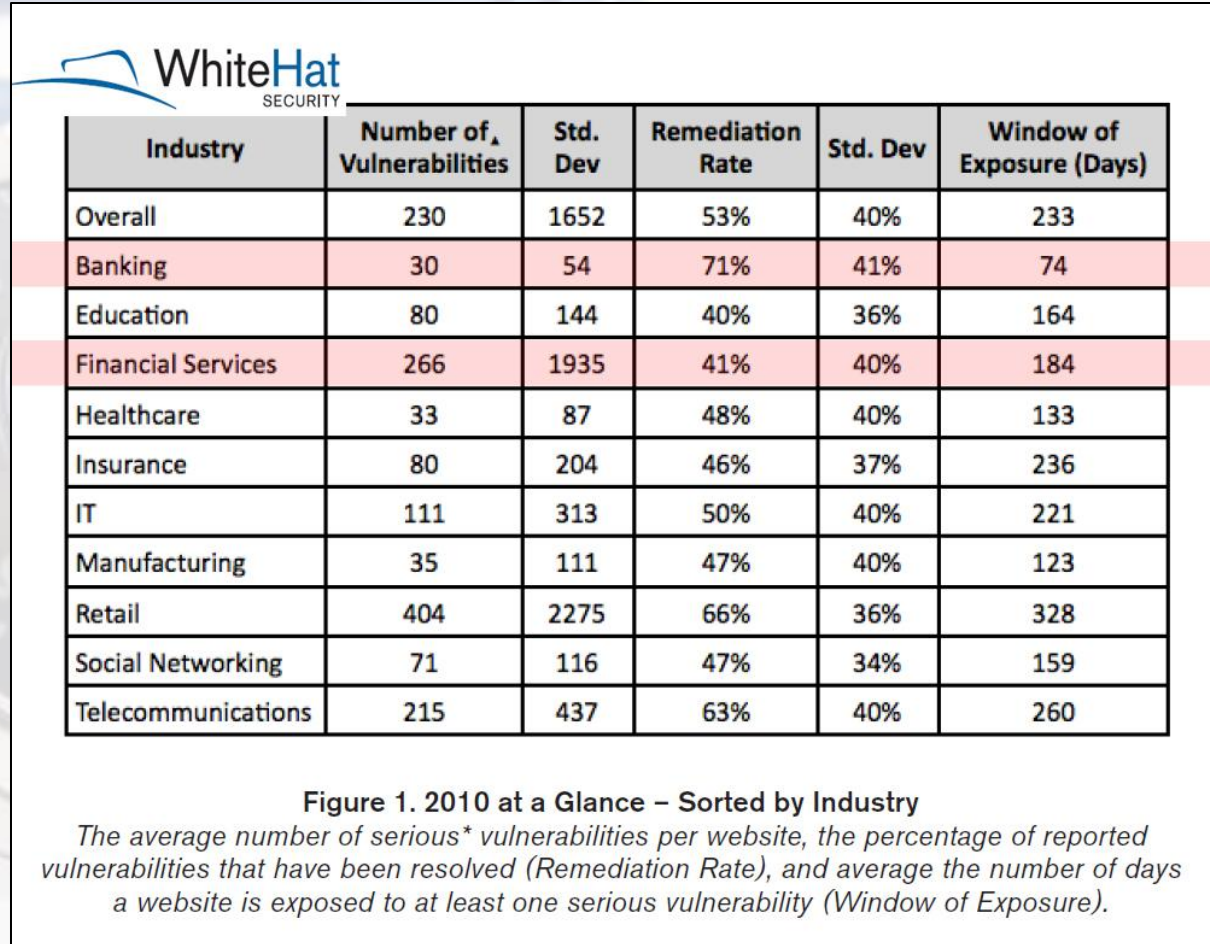


# Ciljevi prezentacije

- Skretanje pažnje na globalne i lokalne probleme vezane za bezbednost podataka i sistema
- Analiza situacije u bankama na teritoriji Srbije
- Edukacija i pronalaženje rešenja

# Globalni problem

- Efikasan, siguran i brz protok podataka
- Cena implementacije i održavanje
- Aplikacije će uvek imati bezbedonosne propuste
- Redovna obuka i specijalizacije zaposlenih
- Odabir pravih alata za poslovanje i zaštitu



# Lokalni problem

- Globalni problemi
- +
- Pravni okviri
- Standardi (ISO 27001, PCI/DSS)
- **Nizak nivo svesti o potencijalnim problemima (Security Awareness)**
- Nepostojanje precizno utvrđenih internih procedura



Someone discovered my  
**PASSWORD.**  
Now I have to rename my dog.

Use strong passwords. A simple password, such as your pet's name, is not sufficient protection. Hackers systematically check every possible word to decipher passwords in no time.

 Watch for an online awareness program  
**PUBLIC JOBS: PRIVATE DATA**

Minnesota STATE COLLEGE  
100 UNIVERSITY AVENUE  
MANKATO, MN 56001

© 2010 Minnesota State College and University System. All rights reserved.

# Uvod u stvarno stanje

- Da li Vam je ikada “provaljeno” u sistem?
- Kako znate?
- Koliko je bila šteta?
- Kako ste je sanirali ?
- Šta ste preduzeli da se obezbedite u budućnosti?

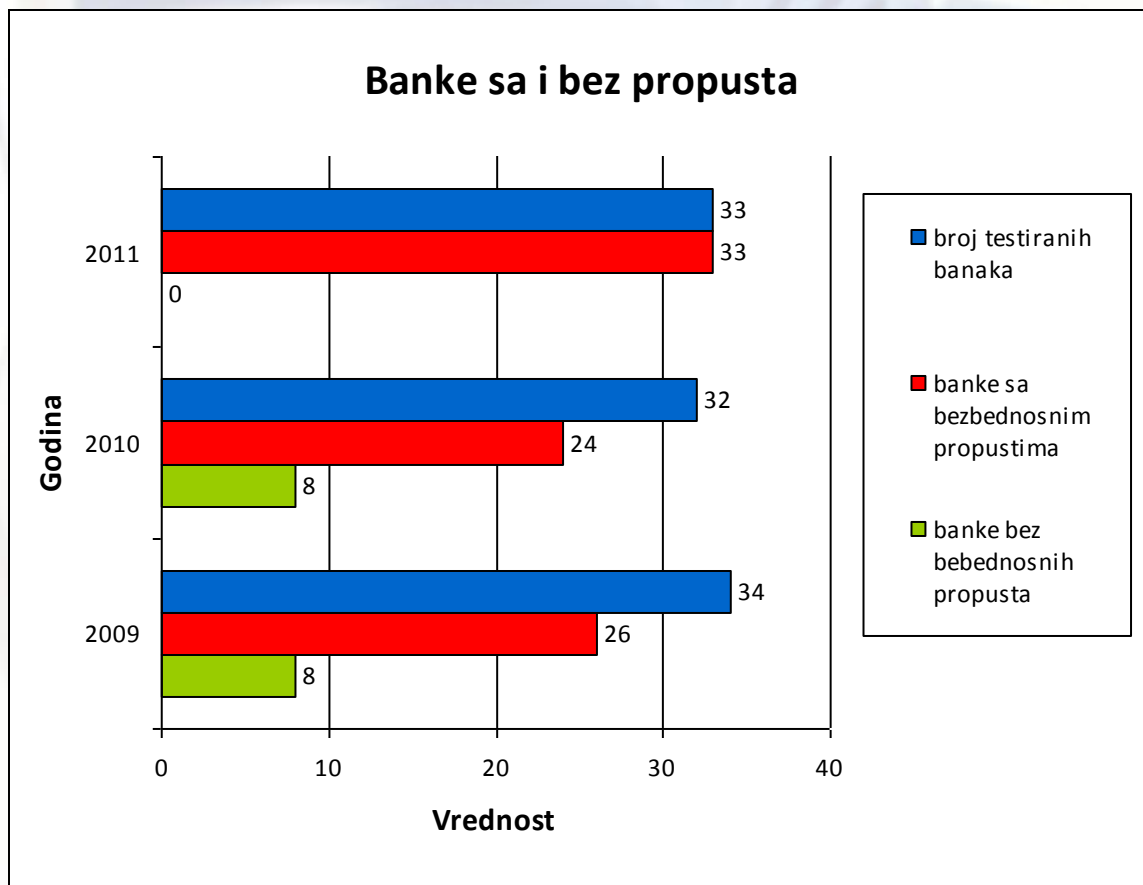
# Banke u Srbiji

- Neinvazivne tehnike testiranja / 10 minuta
- Statistika bezbednosnih propusta web prezentacija banaka
- Analiza dokumenata na web sajtovima banaka

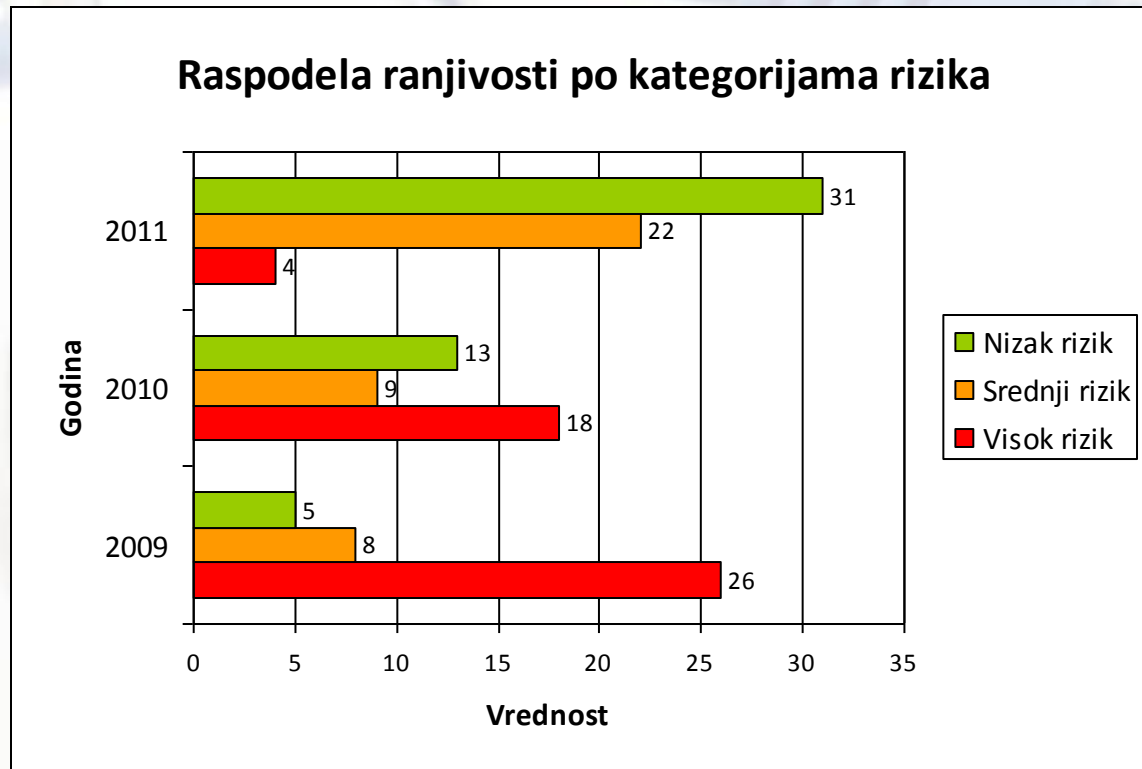
# Banke u Srbiji / Neinvazivne tehnike testiranja / 10 minuta

- 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.

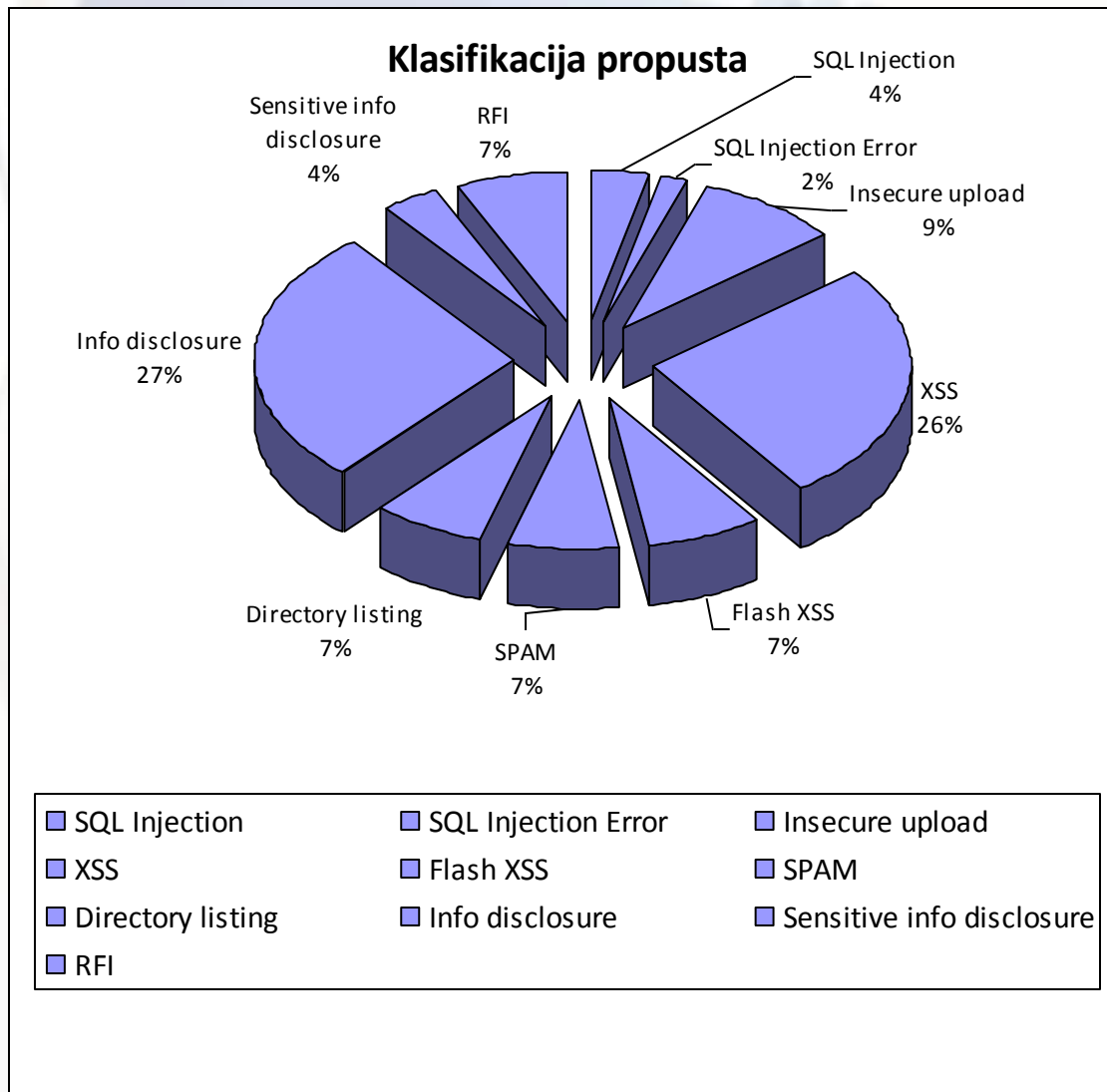
# Banke u Srbiji / Banke sa i bez propusta



# Banke u Srbiji / Podela propusta po riziku



# Banke u Srbiji / Klasifikacija propusta



# Banke u Srbiji / Zanimljive informacije

- Tri web prezentacije rade pod “SSL”-om (ili bar delimično)
- Dvadeset i četiri koriste udaljene biblioteke poput “*Google Analytics*” –a
- 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
- Neke banke imaju demo sisteme na istim pod mrežama gde se nalaze i produkioni sistemi
- A neke banke omogućavaju pristup i nakon gašenja naloga
- ...

# Banke u Srbiji / Analiza dokumenata

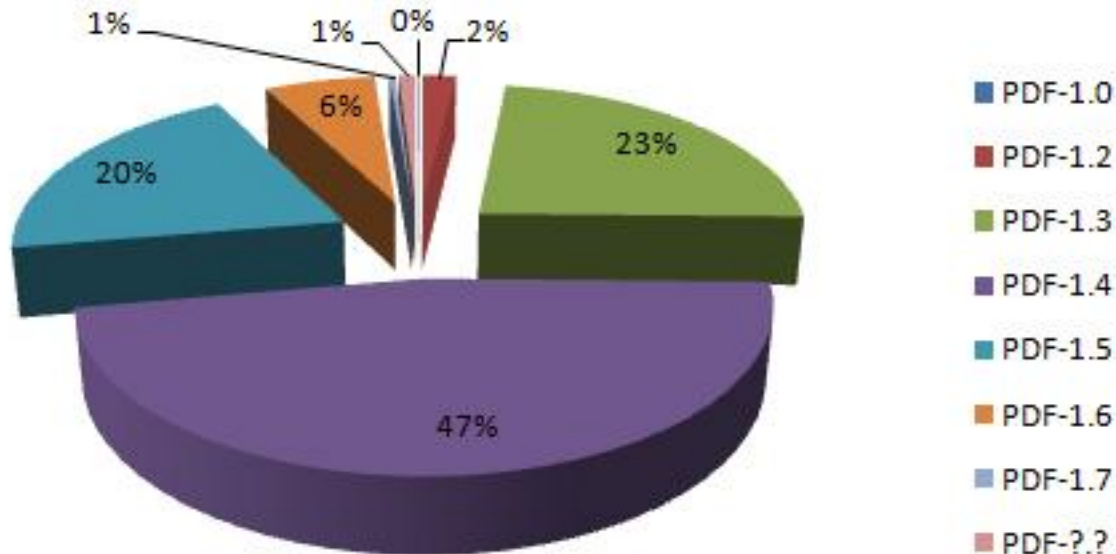
Testiranje dokumenata obuhvata analizu atributa svakog dokumenta sa ciljem pronalazjenja detalja koji mogu otkriti vitalne informacije vezane za:

- verzije aplikacija koje se koriste na internim sistemima za kreiranje ovih dokumenata
- autora dokumenta
- komentara u vezi sa revizijama
- informacijama vezanim za vreme koje je provedeno za rad na dokumentu
- informacijama o štampanju dokumenata
- ...

# Banke u Srbiji / Analiza dokumenata

- Analizirano 5713 dokumenata
- PDF 5235 / MS Office 478
- ~800 atributa autora / ~500 ličnih podataka

## Verzije PDF dokumenata



# Banke u Srbiji / Scenario

- Verzije web servera i tehnologija
- Verzije instaliranih aplikacija
- Spisak zaposlenih
- Manipulacija podacima web prezentacije
- Slanje email poruka putem web sajta banke
- ...

Interesantno ?



# Banke u Srbiji / Posledice eksploatacije

- Krađa indentiteta korisnika
- Lažiranje podataka o proizvodima, korisnicima
- Pristup vitalnim korisničkim podacima (transakcije, kartice, ...)
- Iskorišćavanje web prezentacije za serviranje zabranjenog sadržaja (warez, xxx, ...)
- Iskorišćavanje web prezentacije za "black" SEO tehnike
- Iskorišćavanje web prezentacije za serviranje malicioznog koda (virusi, spyware, 0-day, ...)
- Pretvaranje web prezentacije u "zombie" nekog BOTNET sistema
- Zabrana funkcionisanja web prezentacije od strane pretraživača
- Zabrana funkcionisanja web prezentacije od strane ISP-a
- Zabrana funkcionisanja web prezentacije od strane nadležnih organa reda
- I najvažnije gubitak poverenja korisnika!

# Rešenje



## ❖ Problem

- Nerazumevanje tehnologija
- Loše projektovan informacijski sistem
- Loše projektovan poslovni sistem
- Nepoštovanje standarda, ušteda ?
- One man show !

## ❖ Rešenje

- Profesionalni pristup problemu kroz obuku i poštovanje standarda!
- Primena pravih alata!

# Pitanja?

Ivan Marković, <[ivan.markovic@netsec.rs](mailto:ivan.markovic@netsec.rs)>  
Network Security Solutions, Beograd  
<http://netsec.rs/>

# Hvala! 😊

Ivan Marković, <[ivan.markovic@netsec.rs](mailto:ivan.markovic@netsec.rs)>  
Network Security Solutions, Beograd  
<http://netsec.rs/>