SIGURNOST SAJTOVA CRNOGORSKIH BANAKA

SECURITY OF THE WEB SITES OF THE MONTENEGRIN BANKS

SAŠA VUJOŠEVIĆ,
Ekonomski fakultet Podgorica

Apstrakt: *Kao najjednostavniji vid elektronskog bankarstva može se smatrati prezentovanje banke na Internetu. Putem svoga sajta, banke se reklamiraju, a vrše i komunikaciju sa klijentima. Zato je, za kredibilitet banke, veoma važna sigurnosna komponenta sajta, tj. obezbjeđivanje sajta od raznih kompromitovanja. Takođe, ukoliko je sajt neke banke podložan nekoj od ranjivosti, u nekim slučajevima može doći i do krađe povjerljivih podataka o klijentima. U ovom radu, prikazani su otkriveni propusti na sajtovima crnogorskih banaka i dati predlozi za njihovo otklanjanje.*
Ključne riječi*: elektronsko bankarstvo, sigurnost, ranjivosti*

Abstract: *As the simplest form of electronic banking can be considered presentation of the bank on the Internet. Through its website, the bank is advertising, and communicateing with it's clients. Therefore, for the credibility of the bank, an important security component of the site, is securing the site from various vulnerabilities. Also, if the site of a bank is a subject to any of the vulnerabilities, in some cases may come to the theft of confidential customer data. In this paper, we show omissions that were discovered on the sites of Montenegrin banks and give suggestions for their elimination.*
Key words*: electronic banking, security, vulnerability.*

JEL Classification: G 21; L 81; L 86;
Review; Recived:October 03, 2010

1. Uvod

Uvođenjem elektronskog bankarstva za banke više nije dovoljno da fizički čuvaju svoje podatke bilo u papirnom, bilo u elektronskom obliku, već zbog novonastale mogućnosti povezivanja sa klijentima (preko Interneta ili na neki drugi način) i sam server se mora bolje obezbijediti. Zaštita ovih servera je ranije bila relativno jednostavna, pošto su oni bili fizički odvojeni od „ostatka svijeta" i moglo im je pristupiti samo ovlašćeno osoblje pomoću odgovarajućeg klijentskog softvera. Razvoj Interneta i troslojne klijent/server arhitekture doveli su do toga da su mnogi serveri baza podataka „otvoreni za svijet", tj. korisnici mogu da im pristupe preko posebne aplikacije koja se izvršava na web serveru, a da pri tom koriste samo web pretraživač.

Sajt banke ne mora da sadrži podatke o klijentima, ali baza podataka na sajtu za elektronska plaćanja ih definitivno čuva. Korišćenjem ranjivosti zlonamjerna osoba može doći do povjerljivih informacija, čak i u prvom slučaju (sajt banke, koji je odvojen od sajta za elektronska plaćanja), kada to nisu informacije vezane za račune i naloge klijenata, ali koje se, dalje, nekom drugom tehnikom (npr. društvenim inžinjeringom) mogu iskoristiti za dobijanje drugih informacija.

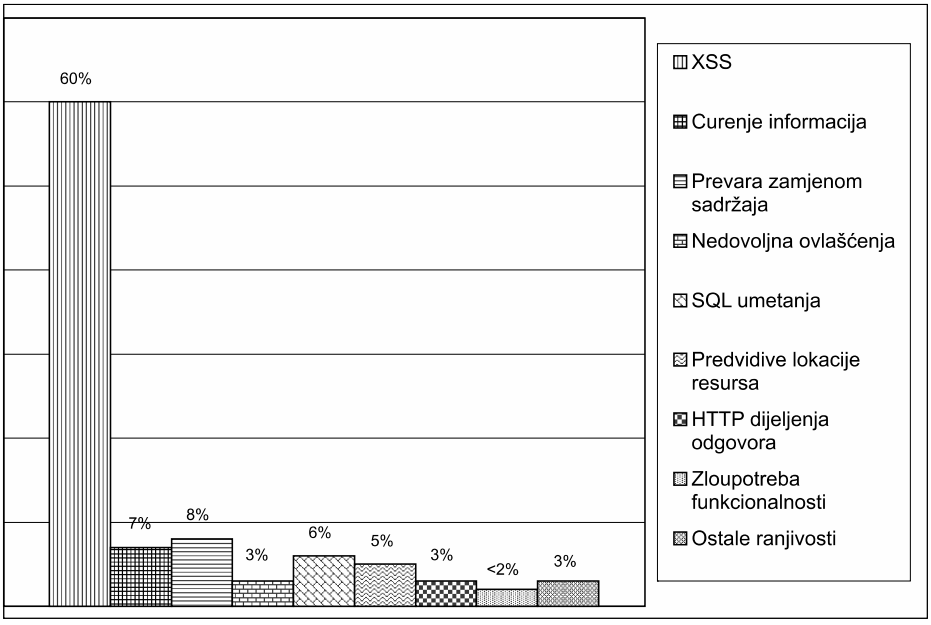
Razvojem raznih tehnologija, omogućeno je pravljenje sajtova sa dinamičkim sadržajem. Time su prodavci došli do nove mogućnosti prezentovanja svoje robe i usluga, ali, sa druge strane, hakerima se otvorio čitav svijet novih mogućnosti. Poslednjih godina banke sve više koriste mogućnosti Interneta. U početku samo kao vid prezentacije banke, a kasnije i u vidu nuđenja usluge elektronskog bankarstva. Kako je Internet nesiguran komunikacioni kanal, razvijene su razne tehnike i protokoli koji omogućavaju sigurnu razmjenu transakcija. Međutim, osim transakcija, banke moraju brinuti i o sigurnosti sajtova, pogotovo o sajtovima za Internet bankarstvo.

Ukoliko neovlašćeni korisnik kompromituje sajt za Internet bankarstvo, to može doći do osjetljivih informacija o korisnicima poput brojeva računa, brojeva kartica itd. Iako se na regularnim sajtovima ne čuvaju osjetljivi podaci, već su to, uglavnom, podaci vezani za promociju banke, ako sajt ima slabosti, zlonamjerni korisnik i ovdje može doći do pojedinih podataka o korisnicima, koje bi, eventualno, kasnije iskoristio za neku drugu vrstu napada. Čak i ako ne dođe do osjetljivih podataka, može mijenjanjem ili obaranjem sajta nanijeti štetu banci. Za potrebe ovog rada ispitani su svi sajtovi crnogorskih banaka, uočene određene ranjivosti i predložena rešenja za njihovo otklanjanje.

2. Vrste ranjivosti

Postoji više ranjivosti vezanih za slabosti sajtova. Najčešće korišćene, po istraživanju WhiteHat Securitya [6] prikazane su grafikonom sa slike 1. Sami napadi zavise i od web platforme, s obzirom da se pojedine vrste napada mogu primijeniti samo na određenim platformama. Različiti napadi eksploatišu različite sigurnosne propuste na različitim platformama. Možemo primijetiti da je veliki broj sajtova pokazao više tipova ranjivosti, kao i da je najzastupljenija ranjivost tipa XSS (eng. *Cross Site Scripting*).

Slika 1: Uporedni prikaz najčešćih ranjivosti (6)



Kao najkritičnija vrsta napada može se smatrati umetanje SQL[1] upita (eng. *SQL injection*). Ovdje se radi o korišćenju slabosti u web aplikaciji, tako da napadač modifikovanjem SQL upita koje web aplikacija šalje bazi podataka, može otkriti osjetljive podatke ili izvesti neku nedozvoljenu radnju nad njima. Umetanjem SQL naredbi, napadač može da preuzme potpunu kontrolu nad povjerljivim podacima u bazi [5]. Sledeća po kritičnosti je XSS ranjivost [3,5], a u navedenom istraživanju je ustanovljena na čak 60% sajtova u svijetu.

Ranjivosti mogu nastati iz različitih razloga. To može biti posledica nedovoljno dobro održavanog servera, starihz verzija softvera ili čak pogrešno podešenih parametara. Ipak, one najopasnije, posledica su loše napisanog kôda web aplikacije, koji ne provjerava ulazne parametre na pravi način. Čak i ako su propusti identifikovani, to ne znači da ih je lako otloniti. Kao rezultat toga, važno je da se analiziraju vrste i težine ranjivosti i da se otklone, u zavisnosti od stepena rizika i potencijalne zloupotrebe. Neke organizacije kao primarni cilj postavljaju otkljanjanje „lakših" slabosti kako bi pokazali napredak u reduciranju ranjivosti. Drugima je prioritet otklanjanje prijetnji „velike" težine, kako bi se smanjio ukupni rizik. Takođe, na nekoj platformi se problemi lakše rešavaju nego na drugim.

Otklanjanje slabosti nije jednostavno i u zavisnosti od platforme i tipa ranjivosti, po spomenutom istraživanju WhiteHat Securitya, može da traje i više mjeseci. Na primjer, za otklanjanje ranjivosti tipa SQL injekcije potrebno prosječno 54 dana.

3. Ranjivosti sajtova crnogorskih banaka

U prethodnom poglavlju spomenute su ranjivosti od koga boluje priličan broj sajtova u svijetu. U ovom poglavlju analiziraćemo ranjivosti sajtova crnogorskih banaka. Za ispitivanje ranjivosti korišćen je alat *Acunetix Web Vulnerability Scanner* [1].

Kada se vrši ispitivanje ranjivosti, treba imati u vidu da je to moguće raditi na 3 načina:

- Uz kompletno poznavanje strukture sajta i web aplikacije (bijela kutija, eng. *white box*);
- Uz djelimično poznavanje strukture sajta i web aplikacije(siva kutija, eng. *gray box*);
- Bez ikakvih informacija o strukturi sajta i web aplikaciji (crna kutija, eng. *black box*).

Stručnjaci za sigurnost u banci bi trebalo da ispitivanja sprovode na prvi ili drugi način, pošto on garantuje veću sigurnost. Treći način predstavlja neku vrstu crne kutije i najbolje odgovara stvarnosti. Naime, napadač (ukoliko nema insajderske informacije), nema saznanja o dizajnu sistema pa mu pristupa kao crnoj kutiji, pokušavajući da nađe „rupe" u njoj, kroz koje bi kompromitovao

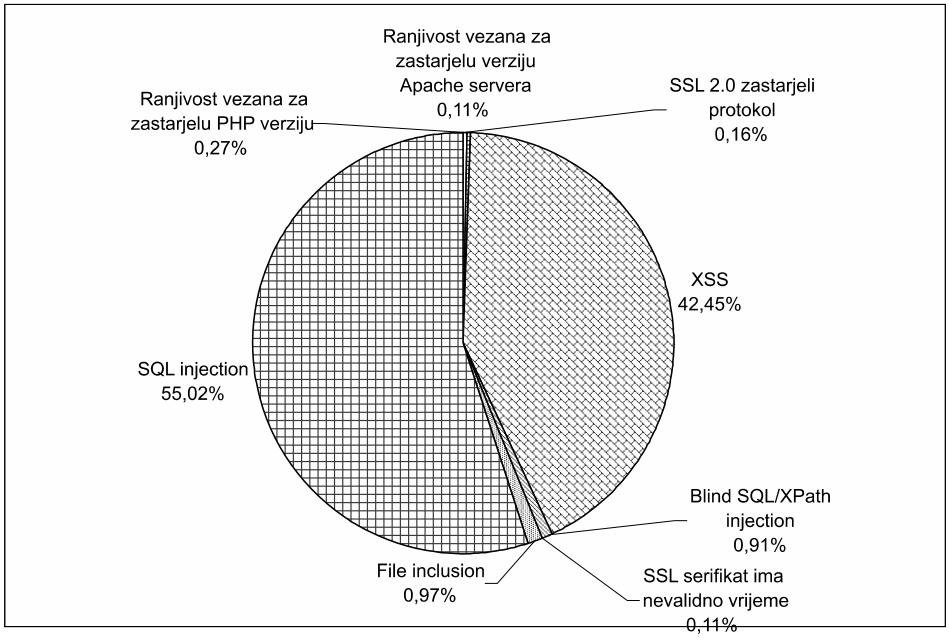
[1] (*eng. Structured Query Language*) je specijalizovani programski jezik koji omogućava smještanje, čitanje i manipulisanje podacima smještenih u relacionim bazama podataka.

sajt. Za potrebe ovog rada, istraživanju se pristupilo na treći način. Ispitujući sajtove svih crnogorskih banaka ukupno je identifikovano 10 klasa kritičnih ranjivosti, 10 klasa ranjivosti srednjeg rizika i 10 klasa malog rizika. Koristeći bilo koju od kritičnih ranjivosti, zlonamjerni korisnik bi mogao da kompromituje sajt banke. Od dizajna same web aplikacije, koja kontroliše sajt, zavisi u kom obimu bi to kompromitovanje bilo. Neke ranjivosti srednjeg rizika, vješt haker može iskoristiti za kompromitovanje sajta, a u najmanju ruku može doći do informacija pomoću kojih može efikasnije iskoristiti neku drugu ranjivost. Ranjivosti malog rizika se ne mogu direktno iskoristiti, ali mogu pomoći da se, pomoću njih, dođe do nekih podataka, koji bi doprinijeli eksploataciji neke druge, opasnije ranjivosti. Ukupno je evidentirano 1861 kritičnih ranjivosti, 82 ranjivosti srednjeg rizika i 1207 ranjivosti malog rizika. Pritom, ranjivosti nisu ravnomjerno raspoređene. Na primjer, kod 4 banke nisu pronađene kritične ranjivosti, dok ih samo jedna ima preko 1000!

3.1. Kritične ranjivosti

Na regularnim sajtovima crnogorskih banaka, detektovano je 1861 kritičnih ranjivosti. Neke od kritičnih ranjivosti se mogu vrlo lako riješiti. Naime, čak 5 klasa pronađenih kritičnih ranjivosti su posledica starih verzija Apache web servera ili PHP-a. Jednostavnom instalacijom najnovijih verzija softvera, otklonile bi se i te slabosti. Na grafikonu sa slike 2. dat je uporedni prikaz, u procentima, kritičnih ranjivosti otkrivenih na sajtovima crnogorskih banaka. Ranjivosti, koje suštinski iskorišćavaju različite propuste na web serveru, ali koje se rešavaju instalacijom nove verzije, svrstali smo u istu kategoriju. Slično je urađeno i za ostale softverske propuste (npr. verzija PHP-a). Pošto je u ispitivanju, kod samo jedne banke, konstatovano više od polovine svih kritičnih ranjivosti, radi boljeg upoređivanja sa svjetskim trendovima, napravljen je i uporedni prikaz kritičnih ranjivosti, izuzimajući tu banku (slika 3).

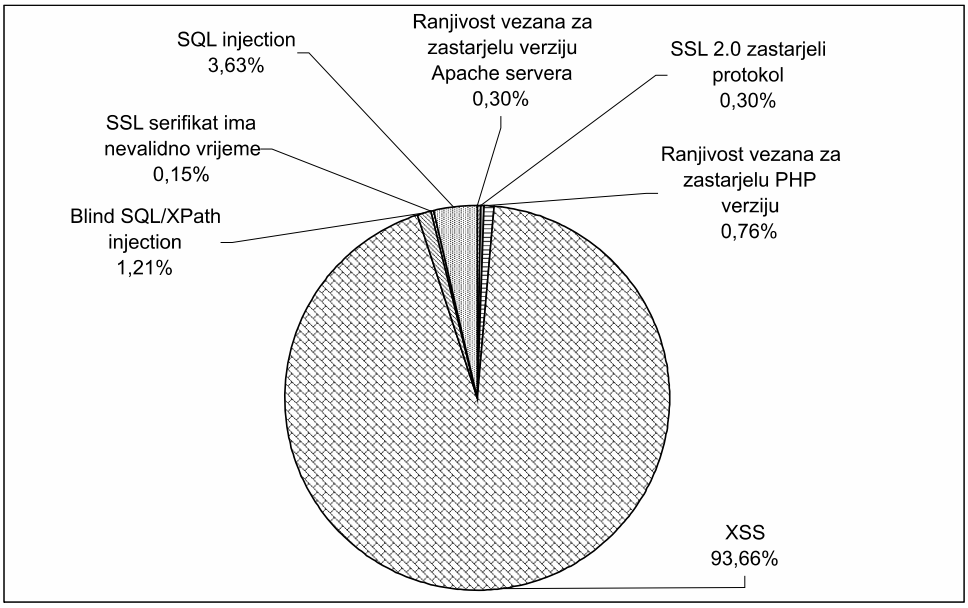
Slika 2 : % zastupljenost kritičnih ranjivosti na sajtovima crnogorskih banaka (sopstveno istraživanje)



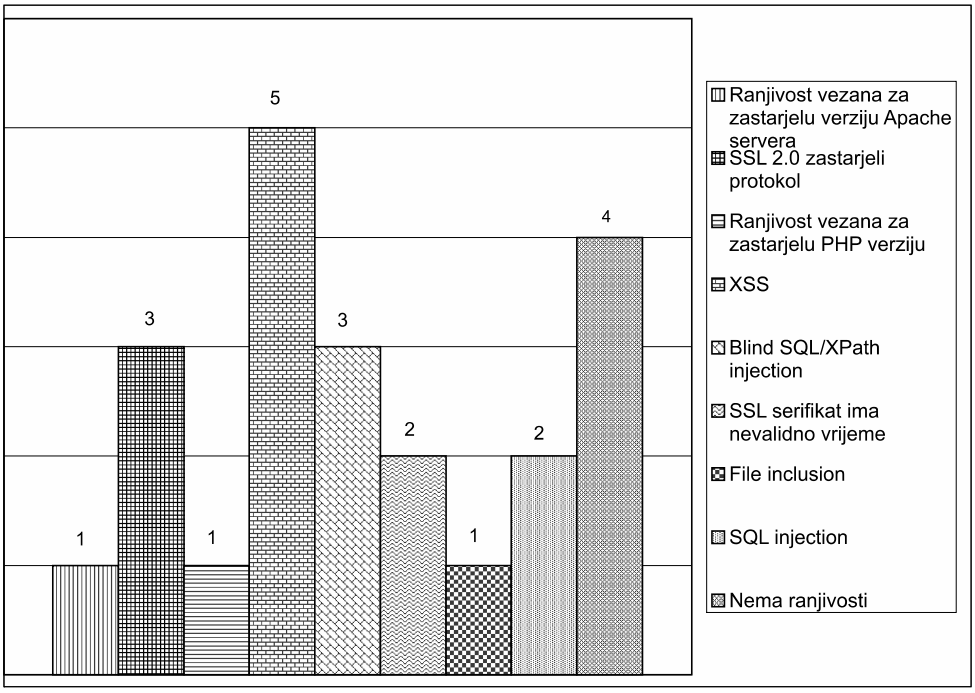
Kao vjerovatno najopasniji tip ranjivosti, SQL injection je zasupljen sa nevjerovatnih 56%. Kako se SQL injection napadom direktno dobija pristup bazi podataka, to zlonamjerni korisnik praktično može doći do svih podataka. Radi poređenja, vidimo sa slike 1., da se u svijetu SQL injection ranjivost nalazi na oko 6% sajtova, a u finansijskim institucijama, zbog prirode posla, ovaj procenat je daleko manji, pa 56% kod naših banaka izgleda još nevjerovatnije. Ipak, najveći broj ovih ranjivosti je identifikovan kod spomenute banke, pa slika 3. daje realniju sliku.

Vidi se da se broj SQL injection ranjivosti sveo na neku razumnu cifru (mada i dalje preveliku za finansijske institucije), ali je broj XSS ranjivosti ogroman, čak 93,66%, nasuprot svjetskog prosjeka od oko 60%. Kod 4 banke nisu pronađene kritične ranjivosti. Ukupno je identifikovano 10 vrsta kritičnih ranjivosti koje smo svrstali u 8 klasa. Na grafikonu sa slike 4. vidi se kod koliko banaka je identifikovana određena kritična ranjivost.

Slika 3 : % zastupljenost kritičnih ranjivosti na sajtovima crnogorskih banaka, izuzimajući banku sa najviše ranjivosti (sopstveno istraživanje)



Slika 4 : Broj banaka kod kojih je otkrivena određena kritična ranjivost (sopstveno istraživanje)

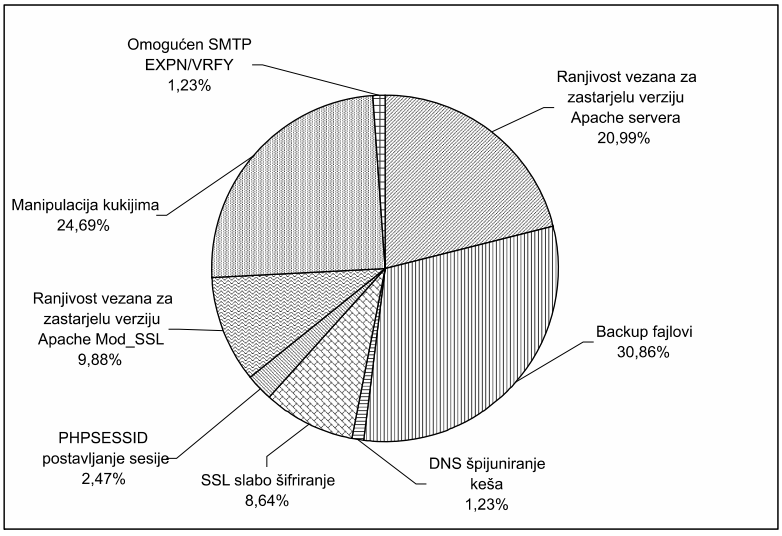


Gornja slika daje bolju procjenu. Gotovo pola banaka je pokazalo slabosti na XSS napade. Onih ogromnih 56% SQL injection ranjivosti su identifikovane kod samo 2 banke. Četiri banke nemaju kritičnih ranjivosti. Interesantno je još da napomenemo da je na 4 sajta pronađeno više od 100 kritičnih ranjivosti, a još jedan ih ima 95.

3.2. Ranjivosti srednjeg rizika

Na sajtovima crnogorskih banaka nađeno je 82 ranjivosti srednjeg rizika. Slično kao kod kritičnih ranjivosti, neke možemo svrstati u istu klasu ranjivosti, tako da se njihova rasprostranjenost može prikazati grafički (slika 5.).

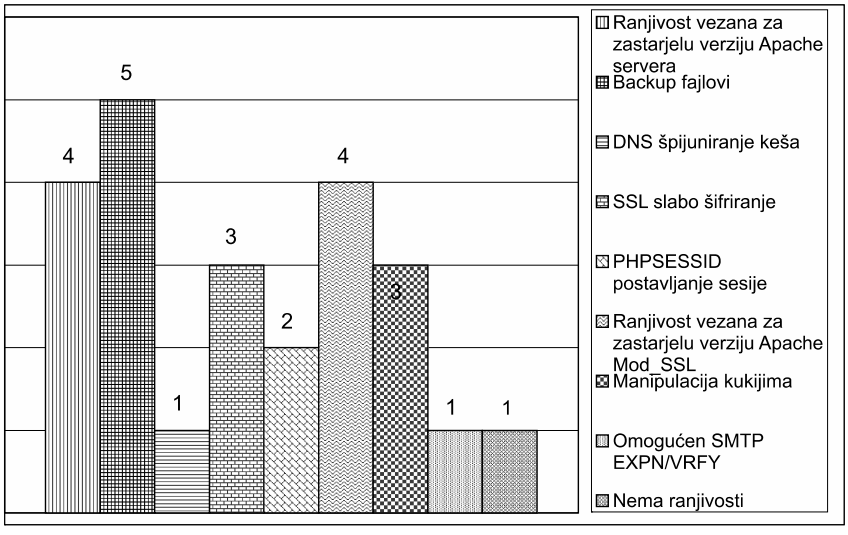
Slika 5 : % zastupljenost ranjivosti srednjeg rizika na satovima crnogorskih banaka *(sopstveno istraživanje)*



Iako je na nekom sajtu konstatovana kriitična ranjivost, to ipak ne znači da zlonamjerni korisnik može da napravi veliku štetu. To, između ostaloga, zavisi i od dizajna same web aplikacije. Nasuprot tome, može se ispostaviti da neka ranjivost srednjeg rizika nosi daleko veći rizik. Na primjer, od ranjivosti prikazanih na slici 5., to se može ispostaviti za backup fajlove, u zavisnosti od toga koji su fajlovi čuvani. To mogu biti neki fajlovi sa lozinkama ili neke skripte, koje će pokrenuti zlonamjerni korisnik. Druga, potencijalno opasna prijetnja može biti manipulacija kukijima, u zavisnosti od toga za što su predviđeni. Takođe, propusti u SMTP (mail protokol), može napadaču omogućiti da dođe do adresa klijenata, a time i potencijalnih žrtvi za phishing napade.

Slično kao u prethodnom poglavlju prikazaćemo i odnos ranjivosti po broju banaka (slika 6).

Slika 6 : Broj banaka kod kojih je otkrivena određena ranjivost srednjeg rizika (sopstveno istraživanje)

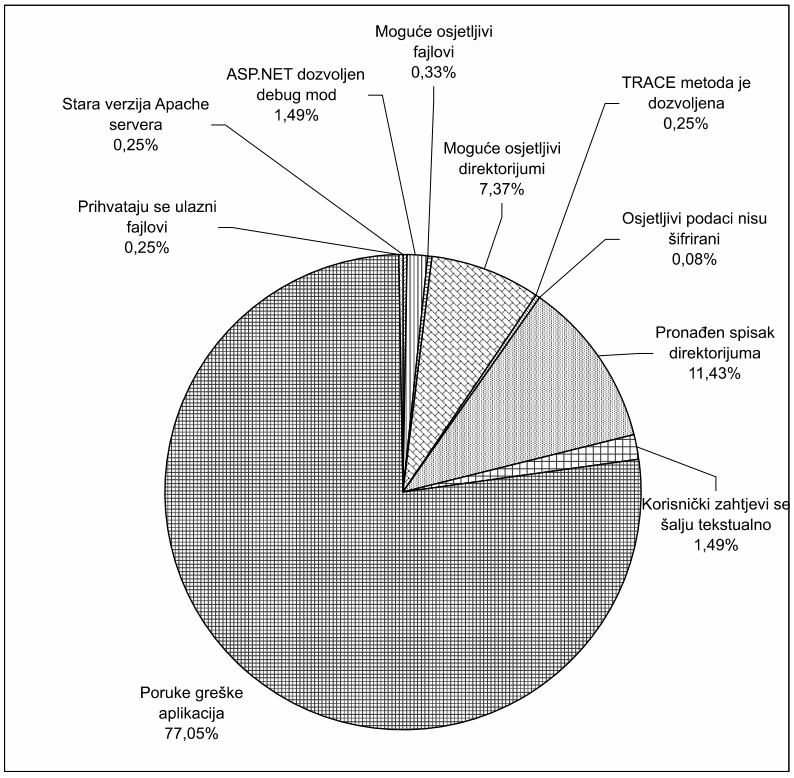


Napomenimo da samo kod jedne banke nije ustanovljena ranjivost srednjeg rizika, dok je kod banke sa najviše različitih tipova ranjivosti, pronađeno 7 tipova sa ukupno 17 različitih ranjivosti.

3.3. Ranjivosti malog rizika

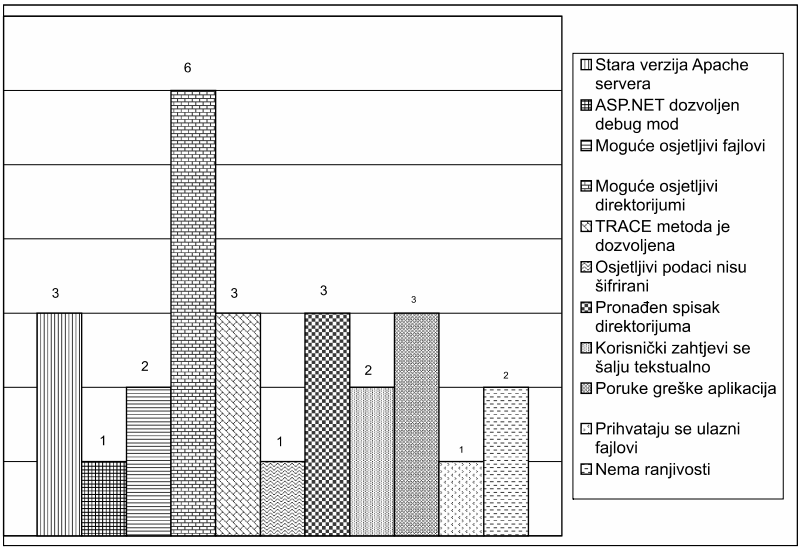
Na sajtovima crnogorskih banaka utvrđeno je 1207 ranjivosti malog rizika. Kao i u prethodnim slučajevima i ovdje ćemo slične ranjivosti uvrstiti u istu klasu ranjivosti, pa se njihova rasprostranjenost može prikazati grafički (slika 7.).

Slika 7 : % zastupljenost ranjivosti malog rizika na satovima crnogorskih banaka (sopstveno istraživanje)



Navedene ranjivosti se ne mogu direktno eksploatisati. Ipak, napadač može da, zahvaljujući ovim slabostima, dođe do nekih podataka, koji mu mogu pomoći da efikasnije zloupotrijebi neku opasniju ranjivost. Na primjer, koristeći prihvatanje ulaznih fajlova, napadač može smjestiti zlonamjernu datoteku na server. Ranjivosti po bankama prikazane su na slici 8.

Slika 8 : Broj banaka kod kojih je otkrivena određena ranjivost malog rizika (sopstveno istraživanje)



Uočava se da je ranjivost „moguće osjetljivi direktorijumi“ najzastupljenija – kod 6 banaka. Ipak, treba imati u vidu da se ova ranjivost odnosi na direktorijume koji nisu direktno povezani sa sajtom, pa je rizik u direktnoj vezi sa njihovim sadržajem. Kod dva sajta nisu pronađene slabosti malog rizika, a kod najranjivijeg sajta je pronađena 471 ranjivost razvrstanih u 7 različitih klasa.

5. Zaključak

Testirano je 11 sajtova crnogorskih banaka. Ukupno je nađeno 3149 ranjivosti, od čega je čak 1.861 kritična ranjivost, srednjeg rizika je 81 a malog rizika 1.207. Broj od 1861 kritične ranjivosti može se shvatiti kao alarmantan. Iako ovi sajtovi nisu povezani sa računima klijenata, ipak njihovim kompromitovanjem i banka i klijenti mogu da pretrpe štetu. U najmanju ruku, zlonamjerni korisnik može da kompromituje sajt postavljajući na njega razne nepoželjne materijale (reklame, porno sadržaj...), čime banka gubi na kredibilitetu. Takođe, u zavisnosti od sadržaja samog sajta, zlonamjerni korisnik može doći i do povjerljivih podataka, koje će, eventualno, iskoristiti za nalaženje ranjivosti na mnogo važnijem sajtu – za elektronsko bankarstvo. Preporuka bi bila da se, što je moguće brže otklone ove ranjivosti. Mišljenja smo, da bi trebalo krenuti od najkritičnijih, pa tek nakon njihovog otklanjanja, preći na ranjivosti manjeg rizika. Već je spomenuto da se neke kritične ranjivosti lako rešavaju instalacijom i pažljivim podešavanjem poslednjih verzija softvera, a time bi se, automatski, riješio i dio ranjivosti malog i srednjeg rizika. Na primjer, kod sajta jedne crnogorske banke, uočene su kritične ranjivosti samo toga tipa. Kako ranjivost navedenog tipa nije posledica slabosti web aplikacije, čudi inertnost IT sektora spomenute banke.

Druge slabosti (npr. SQL injection i XSS), zahtijevaju intervenciju u kôdu web aplikacije, pa je otklanjanje ovih slabosti poželjno raditi u saradnji sa timom koji je razvio aplikaciju. Nakon otklanjanja kritičnih ranjivosti može se pristupiti otklanjanju ostalih. Naravno, svemu mora da prethodi detaljno ispitivanje ranjivosti. Banke u tu svrhu mogu unajmiti profesionalna preduzeća, koja se bave ispitivanjem sigurnosti ili kupovinom specijalizovanog softvera i svojim stručnjacima izvršiti detekciju. Nakon otkrivanja ranjivisti slijedi teži dio – njihovo otklanjanje. Kako ove ranjivosti postoje već duže vrijeme, postavlja se pitanje da li su ih banke uopšte svjesne? Takođe, vjerovatno je da bi se uz poznati dizajn softvera (napadi po principu „bijele kutije“) otkrila još neka ranjivost. Isto tako, eksploatacijom neke ranjivosti i eventualnim upadom u sistem, mogla bi se naći još neka ranjivost.

Za potrebe ovog rada, ranjivosti su samo konstatovane, ne pokušavajući da se eksploatacijom neke, otkriju nove, tako da se sa sigurnošću ne može znati, u kolikoj mjeri postojeće slabosti mogu kompromitovati sajt banke. Radi poređenja s okruženjem, može se navesti slično istraživanje sprovedeno u Srbiji od strane *Network Security Solutionsa* u saradnji sa kompanijom *Microsoft Software* krajem 2009. godine [4]. Od 34 testirane banke pronađeni su kod 26 banaka bezbijednosni propusti. Ipak, u navedenom istraživanju svaki sajt je testiran po 10 minuta na osnovne ranjivosti, dok je istraživanje sprovedeno za potrebe ovog rada trajalo, u zavisnosti od potencijalnih slabosti i veličine sajta, od par sati do više dana, po banci, tako da bi se, dužim ispitivanjem, vjerovatno pronašla još neka kritična ranjivost. Međutim i ovo ispitivanje govori o prevelikom broju slabosti, pogotovo za sajtove finansijskih institucija. Na kraju, treba primijetiti da sigurnost nije statitčko stanje, već proces koji traje, pa ga kao takvog i treba posmatrati. Sistem treba često provjeravati, uočene slabosti što brže otklanjati, a ukoliko je došlo do zloupotrebe pokušati analizom tzv. log fajlova i sličnih zapisa da se identifikuje napadač[2] i problemi riješe pravnim putem.

Literatura

[1] Acunetix: http://www.acunetix.com/

[2] Cross, M., Palmer, S., Kapinos, S., Petkov, P. D., Meer, H., Shields, R., Muttik, I., Temmingh, R., Web Application Vulnerabilities Detect, Exploit, Prevent, Syngress Publishing, Inc., 2007.

[3] Grossman, J. Hansen R., Petkov P. D., Rager A., XSS Attacks: Cross Site Scripting Exploits and Defense, Syngress Publishing, Inc., 2007.

[4] Network Security Solutions, „Statistika bezbednosnih propusta web prezentacija banaka u Srbiji“, decembar 2009.: http//www.netsec.rs

[5] Shema, M., Seven Deadliest Web Application Attacks, Syngress Publishing, Inc., 2010.

[6] WhiteHat Security: „WhiteHat Website Security Statistic Report“, Spring 2010, 9th Edition: http://www.whitehatsec.com/

[2] Nauka koja se bavi otkrivanjem tragova nastalih kiber kriminalom zove se računarska forenzika (eng. *computer forensic*).

Conclusion

Research was conducted over 11 sites of Montenegrin banks. A total of 3149 vulnerabilities had been founded, of which 1861 were a critical vulnerabilities, the 81 medium-risks and 1207 of low risk. The number of critical vulnerabilities of 1861 can be seen as alarming. Although these sites are not related to client accounts, but compromising them, the bank and customers can suffer damage. At least, malicious user can compromise the site by putting on it a variety of unwanted materials (ads, porn content, etc), which makes the bank to lose its credibility. Also, depending on the content of the site, malicious users can get in possession of confidential data, which will possibly be used to find vulnerabilities in a much more important site - for electronic banking. The recommendation would be to, as soon as possible, eliminate the vulnerabilities. By our opinion, process of elimination should start from the most critical, and only after their removal, move to a smaller risk vulnerabilities. It has already been mentioned that certain critical vulnerabilities can be easily solved by careful installation and setup of the last version of the software, and therefore would be automatically solved a part of the vulnerability of small and medium-risk level. For example, at the site one of a Montenegrin banks, there has been identified only that type of a critical vulnerabilities. Vulnerability of the mentioned type is not a result of weaknesses in web applications; therefore it surprises inertness of the IT sector of the aforementioned banks.

Other weaknesses (such as SQL injection and XSS), requires an intervention in code of web application, so it is desirable to eliminate them in a collaboration with a team that developed the application. After elimination of critical it can be accessed to elimination of the other vulnerabilities. Of course, everything must be preceded by a detailed examination of vulnerability. Banks for this purpose can hire a professional company, which deals with examining the vulnerabilities, or purchase specialized software and with its own experts carry out detection. After discovering vulnerabilities, it follows the difficult part - their elimination. As these vulnerabilities have existed for some time, the main question is whether the banks were aware of them at all? Also, it is likely that with well-known designed software (attacks on the principle of "white box"), can be revealed some other vulnerability. Similarly, with the exploitation of some vulnerability and potential intrusion into the system, it can be found some other vulnerability.

For the purposes of this paper, vulnerabilities are just diagnosed, without trying to exploit some of them, to discover new ones, so it certainly can not know to what extent the existing weaknesses could compromise the website of the bank. In comparison with the others in region, a similar survey has been conducted in Serbia by Network Security Solutions in collaboration with Microsoft software in end of 2009.[4]. Out of 34 tested banks, in 26 banks were found various vulnerabilities. However, in that study each site was tested only for 10 minutes, just for basic vulnerabilities, while the research conducted for the purpose of this work, depending on the potential weaknesses and the size of the site, was long from a few hours to several days, depending on the bank, so probably with a longer time of investigation it would be possible to find some new critical vulnerability. However, even this investigation presents too many weaknesses, especially for the sites of financial institutions.Finally, it should be noted that security is not static dimension, but an ongoing process, and as such it should be considered. The system should be more often checked, detected weaknesses to be remove as quickly as possible, and if it has been any kind of misuse, try with analysis of log files and other records to identify the attacker[3] and solve problems through legal channels.

[3] the science of detecting traces generated cyber crime, is called computer forensics.