ACTA ECONOMICA
Година X, број 17 / јун 2012
ISSN 1512-858X

ПРЕГЛЕДНИ ЧЛАНАК

УДК: 004.738.5:339(497.16)
DOI: 10.7215/ACE1217083V

Саша Вујошевић[1]

Анализа слабости електронског банкарства у Црној Гори

The analysis of electronic banking weaknesses in Montenegro

Резиме

Развојем интернета електронско банкарство добија нову димензију. Захваљујући ниским цијенама интернетских трансакција, посљедњих година интернетско и онлајн банкарство постају главни банкарски канали. Једноставност коришћења, доступност средствима у било које вријеме и брзина трансакција учиниле су ову врсту трансакција веома популарном, поготово код млађе популације. С друге стране, интернет је несигуран канал, па се због тога велика пажња мора посветити сигурности. За потребе овог рада урађено је истраживање у оквиру кога су испитани готово сви системи за електронско банкарство црногорских банака. Приказане су уочене рањивости и дати предлози за њихово отклањање.

***Кључне ријечи**: електронско банкарство, сигурност, рањивости.*

Summary

Development of the Internet brings a new dimension to e-banking. Thanks to low-cost Internet transactions, in recent years, Internet banking and online banking have become the main channels. Simplicity of use, availability of funds at any time, as well as a speed of transactions have made this type of transaction very popular, especially among the younger population. On the other hand, the Internet is inse-

[1] Економски факултет Подгорица - Универзитет Црне Горе, Црна Гора, vsasa@ac.me

cure channel, and therefore great attention must be paid to some security aspects. For the purpose of this paper, we conducted a research in which we tested almost all systems for electronic banking in Montenegrin banks. We also identified some particulars vulnerabilities and proposed suggestions for their elimination.

***Key words**: electronic banking, security, vulnerability.*

1. Увод

Развој и могућности интернета учиниле су тај ресурс посебно интересантним за банке. Међутим, због отвореног типа ове „мреже свих мрежа", за експлоатацију овог ресурса, било је потребно да се развије технологија која ће повезати позадинско пословање банке са корисницима који банци приступају преко Интернета. Тај дио се стара да прихвати кориснике са Интернета и да сервисира њихове захтјеве, а да се не угрозе подаци у банци, комуницирајући са банкарским апликацијама преко система заштићеног различитим хардвером и софтвером.

Ширењем техничко-технолошке инфраструктуре, банке су корисницима почеле да стављају на располагање поједине банкарске сервисе, попут прегледа рачуна и других сервиса који немају могућност промјене стања. Даљим технолошким развојем и увођењем напреднијих хардверских и софтверских сигурносних механизама банке уводе већи број сервиса, па чак и плаћања путем интернета.

Увођењем електронског банкарства за банке више није довољно да физички чувају своје податке било у папирном било у електронском облику, већ због новонастале могућности повезивања са клијентима (преко интернета или на неки други начин) и сам сервер се мора боље обезбиједити. Заштита ових сервера је раније била релативно једноставна, пошто су они били физички одвојени од „остатка свијета" и могло им је приступити само овлашћено особље, помоћу одговарајућег клијентског софтвера. Развој интернета и трослојне клијент/сервер архитектуре, довели су до тога да су многи сервери база података „отворени за свијет", тј. корисници могу да им приступе преко посебне апликације која се извршава на веб серверу, а да при том користе само веб претраживач.

Развојем разних технологија, омогућено је прављење сајтова са динамичким садржајем. Тиме су продавци дошли до нове могућности презентовања своје робе и услуга, али, са друге стране, хакерима се отворио читав свијет нових могућности.

Посљедњих година банке све више користе могућности интернета. У почетку само као вид презентације банке, а касније и у виду нуђења услуге електронског банкарства. Како је интернет несигуран комуникациони

канал, развијене су разне технике и протоколи који омогућавају сигурну размјену трансакција. Међутим, осим трансакција, банке морају бринути и о сигурности сајтова, поготово о сајтовима за интернетско банкарство.

Уколико неовлашћени корисник компромитује сајт за интернетско банкарство, он може доћи до осјетљивих информација о корисницима - попут бројева рачуна, бројева картица итд. Иако се на регуларним сајтовима не чувају осјетљиви подаци, већ су то, углавном, подаци везани за промоцију банке, ако сајт има слабости, злонамјерни корисник и овдје може доћи до појединих података о корисницима, које би, евентуално, касније искористио за неку другу врсту напада. Чак и ако не дође до осјетљивих података, може мијењањем или обарањем сајта нанијети штету банци.

Познати стручњак за сигурност, професор на *Purdue* универзитету, Eugene Spafford је рекао: „Коришћење криптографије на интернету еквивалентно је ангажовању блиндираног аута да пренесе информације са кредитне картице од некога ко живи у картонској кутији до друге особе која живи на клупи у парку“ [1]. Из ове изјаве, може се извести закључак да није довољно обезбиједити сигурне трансакције између банке и клијента (тј. неке фирме и клијента), већ се мора водити рачуна и о рачунарима између којих се трансакција одвија. Наравно, свака страна је дужна да води рачуна о сопственој сигурности, али, ипак, због осјетљивости информација, банчин сервер мора бити неупоредиво боље заштићен. Наиме, злоупотребом података на клијентовом рачунару биће оштећен само тај клијент, а крађом података са сервера банке (предузећа) угрожени су сви клијенти (или већина клијената).

Веб апликације, преко којих клијенти врше комуникацију са банком, представљају дистрибуиране клијент/сервер системе, који се изводе и на корисниковом, тј. клијентском рачунару (енг. *client-side*) и на *веб серверу* (енг. *server-side*). Иако је констатовано да је свака страна одговорна за обезбјеђивање своје сигурности, ипак би банке, у најмању руку, морале даураде све што је до њих, и макар скину одговорност са себе за евентуалне злоупотребе клијентовог рачунара и, касније, као посљедицу тога и његовог налога код банке. Наиме, у неким случајевима није потпуно јасно, да ли је искључиво клијентова грешка што је био жртва одређене врсте напада.

У овом раду анализиране су слабости на серверској страни система за електронско банкарство готово свих црногорских банака, уочене одређене рањивости и предложена решења за њихово отклањање. Такође, скренута је пажња на слабости на клијентској страни, а које су посљедица неажурности банака.

2. Сигурност клијенске стране

Огроман број рачунара, поготово они који су на мрежи, свакодневно је изложен различитим врстама злонамјерних напада. Неки од тих напада су директно повезани са покушајима нелегалног присвајања разних личних података, чиме би се, евентуално, злоупотријебили за даље неовлашћено пријављивање на банчине сервере или пак, извршила нека плаћања. Према истраживању *Lavasofta* [2] између 100 и 150 милиона рачунара је под директном контролом хакера.

Постоји много различитих начина на који злонамјерна особа може доћи до података са рачунара жртве. У овом раду осврнућемо се само на оне технике, које се касније могу искористити за лажно пријављивање код банака, а које су остварене упадом у рачунар жртве. Дакле, фокус је на крађи идентитета[2], и то путем корисниковог рачунара. Овдје ћемо обрадити неколико статистички најчешћих и најефикаснијих метода, чији се резултати касније могу експлоатисати у циљу коришћења банковног рачуна жртве.

Постоје два начина крађе идентитета. Први је да се подаци украду директно из базе података банке, продавнице итд. Често су у крађу укључени и запослени или бивши запослени[3]. Код овакве крађе корисници чији идентитет покушава да се украде, не могу на то утицати – то је на институцији која чува податке. Једина ствар коју корисник може да уради је често провјеравање свог рачуна и обављених трансакција. Други начин крађе идентитета је када нападач информације украде директно од жртве или преваром дође до њих. У већини случајева други начин је пуно једноставни и, сходно томе, много популарнији код злонамјерних корисника.

Према извјештају Anti Phishing Working Group (APWG), на крају 2009. године 47,87% рачунара је било заражено неким злонамјерним програмом за крађу идентитета [3].

Пецање (енг. *phishing*[4]) представља један од најчешћих начина за покушај преотимања идентитета. Овдје се преваром, комбиновањем са друштвеним инжињерингом, долази до разних осјетљивих података (бројеви рачуна, број банковне картице, итд).

Типична превара путем пецања почиње када корисник прими електронску пошту, која изгледа једнако као мејл његове банке. У мејлу је, најчешће,

[2] Крађа идентитета *„настаје када неко користи ваше личне податке без дозволе, како би починио превару или неки други злочин"* (америчка Савезна трговинска комисија [4]).

[3] Према истраживању PricewaterhouseCoopers из 2005, преко 50% информатичких злоупотреба дошло је од стране запослених или бивших запослених. У истраживању из 2007, тај број се повећао на око 61% [5].

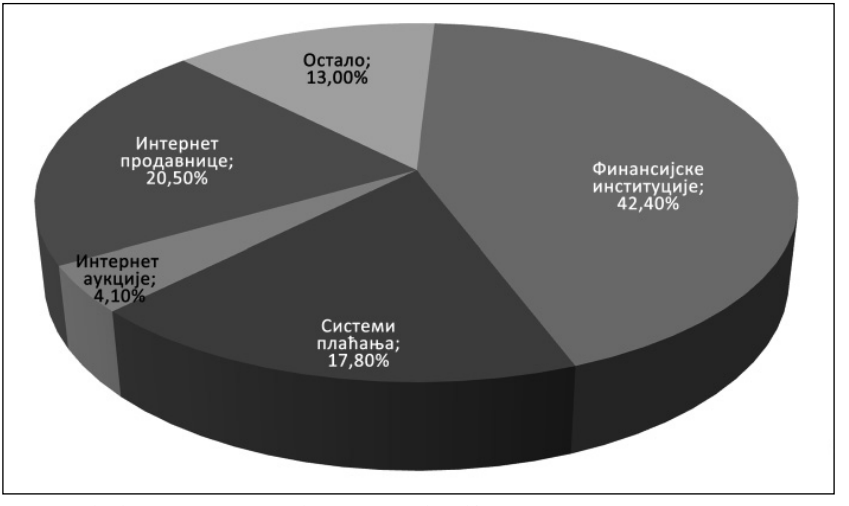
[4] *Phishing*, израз који је настао 1996, а добио је назив као алузија на *fishing* (пецају се информације), комбинованом са хакерским термином за проваљивање (*phreaking*). Ријечи *fishing* и *phishing* се у енглеском језику исто изговарају, а *phishing* се код нас преводи као пецање.

неко обавјештење везано за кориснички рачун (наводно су непотпуни или нетачни подаци) у коме се тражи да се корисник мора хитно јавити ради ажурирања података. То „ажурирање" се обавља путем линка који се налази у мејлу и кликом на њега корисник би требао да буде преусмјерен на сајт банке. Наравно, он се не преусмјерава на сајт банке, већ на сајт нападача, који изгледа идентично банчином сајту. Ту ће корисник попунити одређене обрасце у којима се, између осталог, тражи и број његове картице. Након тога, нападач има све потребне жртвине податке, а жртву може, ради смањивања сумње, преусмјерити на легалан банчин сајт.

Као што је већ речено, највећи број *phishing* напада почиње слањем имејла. Иако се имејл може послати унапријед одабраној жртви, углавном се тако не ради. Наиме, нападач за слање електронске поште, обично користи исте методе које се користе за слање спама[5]. Коришћењем тих техника нападач може, у веома кратком времену (пар сати или, чак минута), да достави припремљене мејлове на милионе адреса. Уколико су му циљна група клијенти једне банке, то може урадити далеко брже.

Циљне групе за *phishing* нападе могу бити различите, али су то најчешће корисници финансијских институција, неког система плаћања, онлајн аукције или неке онлајн трговине. На графикону са слике 1 приказане су, процентуално, најчешће нападани сектори.

Слика 1. *Најчешће нападани сектори, пецањем*



Извор: Phishing Activity Trends Report 2nd Half 2011 [3]

Очигледно су најчешће крађе идентитета корисника разних финансијских институција и система плаћања преко 70%. Иако корисници имају све

[5] Нежељена пошта. Разним техникама њени пошиљаоци, тзв. спамери, шаљу исте рекламне емаилове на десетине хиљада мејл адреса, до којих су дошли неким другим техникама.

више информација о нападима ове врсте, пецање је и даље врло популарна и успјешна метода крађе. По истраживању *APWG-a, око* 5% послатих *phishing* имејлова успијева у намјери да од корисника извуче личне податке [3]. По истраживању *Lavasofta* [2] чак 46,03% корисника интернета је било жртва *phishing* напада.

3. Сертификати

Пословање преко Интернета се мора обезбиједити неким криптографским техникама и протоколима. Један од најзаступљенијих протокола у свијету је SSL протокол, који обезбјеђује сигурну комуникацију путем несигурног канала и успоставља сигурну комуникацију између банке и клијента. Све црногорске банке, које пружају услуге електронског банкарства, ту сигурну везу успостављају управо путем SSL протокола. Истина, поједине банке за коришћење е-банкинга (поготово за предузећа) имају и додатни ниво заштите у виду додатног софтвера, паметних картица, или предефинисаних сигурносних кодова.

Крајем 2004. године, у Црној Гори почео је са радом и сервисни центар за електронско пословање *E-ton*, основан као заједничка инвестиција: *Телеком Црна Гора* и информатичке компаније *Rexit Solutions* из Београда. Компанија је замишљена да, између осталог, издаје и извршне аутентификационе сертификате, чиме би клијентима наших банака гарантовали да је успостављена конекција баш са жељеном банком. Да ли је баш тако?

Сâм SSL протокол, преко кога клијенти са црногорским банкама успостављају сигурну конекцију, јесте сигуран онолико колико то данашња теорија и пракса показују. Није доказано да су имплементирани алгоритми непробојни[6], али вишегодишња пракса показује да му се може вјеровати. У том смислу, црногорске банке не заостају за свјетским и можемо сматрати да је сама трансакција довољно сигурна.

На први поглед, успостављена веза је сигурна и даља размјена података је безбједна. И заиста, као што је већ речено, сама трансакција је обезбијеђена SSL протоколом и као таква сматра се сигурном. Једино питање које се овдје може поставити јесте: да ли је заиста успостављена конекција са траженом банком. Наиме, у тренутку успостављања конекције, претраживач од банчиног сервера тражи валидну потврду да је сајт са којим је успостављена конекција управо тражени сајт.

Сертификат је једино што клијенту гарантује да је успостављена конекција баш тражена конекција. Отуда и потреба да сертификате издају про-

[6] 2008. године откривене су слабости унутар SSL протокола, у оквиру МД5 функције, и уз помоћ 200 паралелно повезаних Sony playstationa 3, тим криптографа је у *Laboratory for Cryptologic Algorithms at EPFL*, успио је да креира лажни CA [6].

вјерена ауторизациона тијела. Сâм веб претраживач препознаје валидне сертификате издате од стране признатих ауторизационих тијела. Нажалост, у Црној Гори постоје банке које имају невалидне сертификате (табела 1) и управо клијенти тих банака могу постати жртве пецања.

Табела 1: *Број валидних и невалидних сертификата банака у Црној Гори*

	Август 2011	2012
Валидни	2	9
Самопотписани	4	2
Непознат издавач	5	0

Извор: Сопствено истраживање

Напоменимо да 2005. године, након што су увеле електронско банкарство, ни једна банка у Црној Гори није имала валидан сертификат, а тек септембра 2011. године добављањем врховног сертификата од *Go Daddy Secure Certification Authoritya*, E-mon је својим клијентима обезбиједио валидни сертификат.

4. Рањивости сајтова

Постоји више рањивости везаних за слабости сајтова. Најчешће коришћене су сљедеће:

- Напад подметањем SQL[7] упита (енг. *SQL injection*);
- XSS напад (енг. *Cross-site scripting*);
- CSRF напад (енг. *Cross-Site Request Forgery*);
- Напад CRLF[8] уметањем;
- Напад промјеном директоријума;
- Напади везани за аутентикацију;
- Цурење информација;
- Напади везани за прекорачења промјењивих;
- Напади на сесије итд.

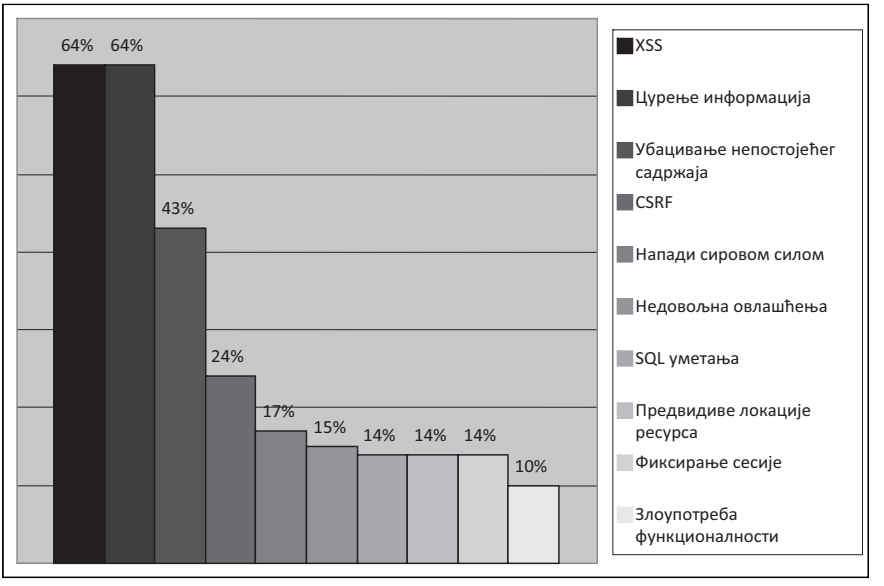
Постоји више рањивости везаних за слабости сајтова. Најчешће коришћене, по истраживању WhiteHat Securitya [8] приказане су графиконом са слике 2. Сами напади зависе и од веб платформе, с обзиром да се поједине врсте напада могу примијенити само на одређеним платформама. Различити напади експлоатишу различите сигурносне пропусте на различитим

[7] SQL (*eng. Structured Query Language*) је специјализовани програмски језик који омогућава смјештање, читање и манипулисање подацима смјештених у релационим базама података. SQL је најраширенији језик за релационе базе података који користи већина данашњих веб апликација. Примјери релацијских база података којима се управља путем SQL-а су Oracle, Microsoft Access, MS SQL Server, MySQL, Filemaker Pro itd. Детаљи о SQL језику могу се наћи у нпр. [7].

[8] CR (eng. C*arriage return*) – Ентер; LF (енг. *Line feed*) – нови ред.

платформама. Можемо примијетити да је велики број сајтова показао више типова рањивости, као и да је најзаступљенија рањивост типа XSS (енг. *Cross Site Scripting*).

Слика 2: *10 најчешћих рањивости*



Извор: WhiteHat Website Security Statistic Report [8]

Такође по истраживању WhiteHat Securitya за претходну годину [9] и поређењем са посљедњим, уочава се раст свих рањивости – изузимајући XSS - ни једна рањивост није премашивала 10%.

Као најкритичнија врста напада може се сматрати уметање SQL[9] упита (енг. *SQL injection*). Овдје се ради о коришћењу слабости у веб апликацији, тако да нападач модификовањем SQL упита које веб апликација шаље бази података, може открити осјетљиве податке, или извести неку недозвољену радњу над њима. Уметањем SQL наредби, нападач може да преузме потпуну контролу над повјерљивим подацима у бази [10]. Сљедећа по критичности је XSS рањивост [10,11], а у наведеном истраживању је установљена на чак 64% сајтова у свијету.

Рањивости могу настати из различитих разлога. То може бити посљедица недовољно добро одржаваног сервера, старих верзија софтвера, или чак погрешно подешених параметара. Ипак, оне најопасније, посљедица су лоше написаног кôда веб апликације, који не провјерава улазне параметре на прави начин.

[9] (*Енг. Structured Query Language*) је специјализовани програмски језик који омогућава смјештање, читање и манипулисање подацима смјештених у релационим базама података.

Чак и ако су пропусти идентификовани, то не значи да их је лако отклонити. Као резултат тога, важно је да се анализирају врсте и тежине рањивости и да се отклоне у зависности од степена ризика и потенцијалне злоупотребе. Неке организације као примарни циљ постављају откључање „лакших" слабости како би показали напредак у редуцирању рањивости. Другима је приоритет отклањање пријетњи „велике" тежине, како би се смањио укупни ризик. Такође, на некој платформи се проблеми лакше рјешавају него на другим.

Отклањање слабости није једноставно и у зависности од платформе и типа рањивости, по споменутом истраживању WhiteHat Securitya [11], може да траје и више мјесеци. На примјер, за отклањање рањивости типа SQL инјекције потребно је просјечно 54 дана.

5. Рањивости сајтова за електронско банкарство у Црној Гори

Доношењем Закона о електронској трговини 2004. године [12] и Закона о електронском потпису 2005. године [13], стекли су се услови за електронско пословање у Црној Гори. Иако се и само презентовање банака на Интернету може сматрати неком врстом електронског пословања, „право" електронско банкарство почиње крајем 2004. године, увођењем е-банкинг сервиса за грађане у Euromarket банци. Ова банка се почетком 2006. године спојила са Монтенегро банком и настала је *NLB Montenegrobanka*.

Убрзо након тога, у току 2005. године, готово све банке у Црној Гори почињу да пружају неку врсту електронског банкарства.

Данас у Црној Гори послује 11 лиценцираних банака [14]:

1. Црногорска комерцијална банка АД Подгорица member of OTP Group,
2. Хипотекарна банка АД Подгорица,
3. Societe Generale banka Montenegro AD,
4. Инвест банка Монтенегро АД Подгорица,
5. Прва банка Црне Горе АД Подгорица, основана 1901. Године,
6. ERSTE Bank АД Подгорица,
7. Атласмонт банка АД Подгорица,
8. NLB Montenegrobanka АД Подгорица,
9. Комерцијална банка АД Будва,
10. Hypo Alpe-Adria Bank АД Подгорица,
11. First Financial Bank АД Подгорица.

Све наведене банке пружају услуге електронског банкарства[10]. Иако би правилнији термин, у случају црногорских банака, био интернетско бан-

[10] Није јасно да ли First Financial Bank има ову услугу или не. Наиме, на сајту банке, не постоје подаци о томе, али на сајту Е-мона се тврди да су започели и тај сервис. Личним претраживањем и методом покушаја, уписујући име које асоцира на банку, нађен је сајт на адреси

карство или онлајн банкарство, у овом дијелу ћемо га звати именом како га и саме банке нуде и рекламирају – *електронско банкарство*.

У претходнм дијелу рада размотрене су многе рањивости од којих болује приличан број сајтова у свијету. У овом дијелу анализираћемо рањивости сајтова за електронско банкарство црногорских банака.

За испитивање рањивости коришћен је алат *Acunetix Web Vulnerability Scanner* [15].

Када се врши испитивање рањивости, треба имати у виду да је то могуће радити на 3 начина:

1. Уз комплетно познавање структуре сајта и веб апликације (бијела кутија, енг. *white box*);
2. Уз дјелимично познавање структуре сајта и веб апликације (сива кутија, енг. *gray box*);
3. Без икаквих информација о структури сајта и веб апликацији (црна кутија, енг. *black box*).

Стручњаци за сигурност у банци би требало да испитивања спроводе на први или други начин, пошто он гарантује већу сигурност. Трећи начин представља неку врсту црне кутије и најбоље одговара стварности. Наиме, нападач (уколико нема инсајдерске информације), нема сазнања о дизајну система па му приступа као црној кутији, покушавајући да нађе „рупе“ у њој, кроз које би компромитовао сајт. За потребе овог рада, истраживању се приступило на трећи начин.

У току истраживања, испитано је 9 од 11 система за електронско банкарство. Наиме, још увијек није јасно да ли је First Finansial Bank почела званично да нуди услугу електронског банкарства. Друго, у тренутку испитивања једна од преосталих 10 банака је блокирала даље покушаје конекције са испитивачеве IP адресе. Ово се може схватити као једна од сигурносних мјера те банке, о чему ће, нешто касније, бити ријечи.

Од 9 испитаних система за интернетско банкарство црногорских банака идентификовано је 6 класа критичних рањивости, 4 класе рањивости средњег ризика и 5 класа рањивости малог ризика.

Укупно су евидентиране 43 критичне рањивости, 21 рањивост средњег ризика и 1115 рањивости малог ризика. На сајтовима са презентацијама банака откривено је неупоредиво више рањивисти. На примјер, нађена је 1861 критична рањивост [16]. Један од разлога мањег броја рањивости на системима за електронско банкарство је вјероватно SSL протокол, преко кога се обавља комуникација са овим сајтовима. Други разлог могу бити и сигурносни протоколи који дозвољавају ограничен број покушаја прија-

https://secure.emon24.net/ffb. Могуће је да је сервис још у тестној фази, а да ће убрзо бити званично покренут.

вљивања у неком временском интервалу (нпр. 3 или 5 покушаја за сат времена), а што ће дефинисати сама банка.

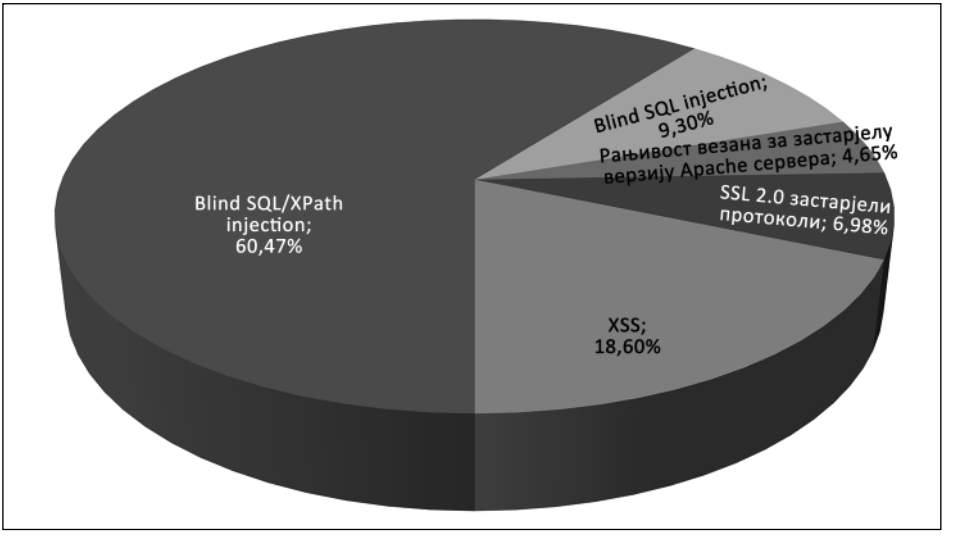
Могуће је да би уз детаљнију анализу број откривених рањивости био већи. Наиме, ограничавање броја покушаја јесте добра превентивна мјера, али упорном нападачу неће превише сметати. Рестартовањем рутера, биће му додијељена нова IP адреса, чиме ће поново моћи да покуша са нападима. Осим тога, постоји специјализован софтвер који то може радити у његово име, па предузете мјере готово да немају ефекта. Такође, поједини програми дозвољавају коришћење постављених листи прокси сервера, тако да се ни рутер не мора ресетовати.

На крају, као коментар против трајног блокирања IP адресе може бити сљедећи аргумент: уколико злонамјерни корисник услуга неког црногорског провајдера интернетских услуга изведе велики број покушаја напада, то ће банка блокирати велики број IP адреса, па може доћи до засићења, тј. може се десити да ни регуларан корисник не добије приступ (интернетски провајдер му је у тренутку додјељивања IP адресе додијелио неку од блокираних).

5.1. Критичне рањивости

На 9 испитаних сајтова за електронско банкарство, уочене су 43 критичне рањивости. Њихова расподјела, по класама, може се видјети на графикону са слике 3.

Слика 3: *Заступљеност критичних рањивости*



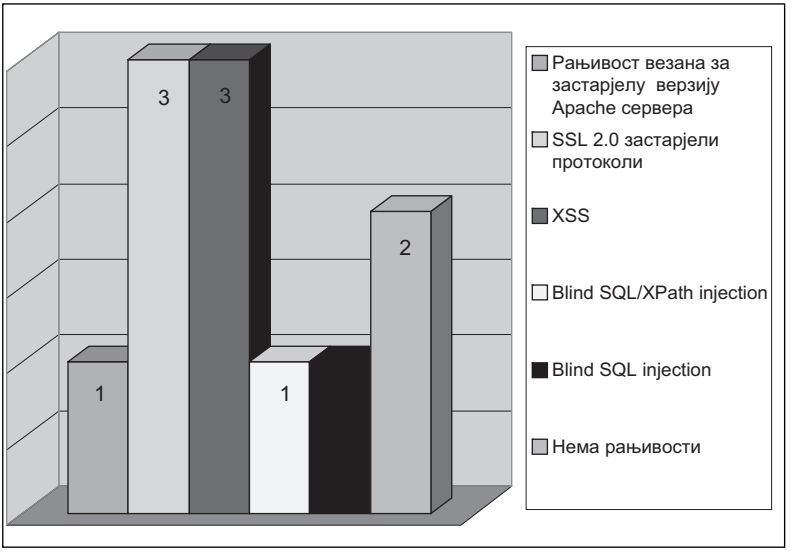
Извор: Сопствено истраживање

Интересантно је да примијетимо да је чак и на сајтовима за електронско банкарство, уочен одређени број критичних рањивости, које су посљедица застарјелих верзија софтвера. Оно што може помало да забрињава јесте присуство рањивости типа разних уметања (XSS или SQL injection), које се можда могу искористити без обзира на додатне заштите. Наиме, многе банке, осим уноса имена и лозинке, користе и додатну заштиту. Код неких банака је та заштита у виду паметне картице, код других у виду неког трећег параметра (тзв. предефинисаних рачуна). Углавном, за правна лица користи се већи ниво заштите и тамо је, као додатни ниво заштите, присутна паметна картица у комбинацији са читачем картица.

У зависности од структуре сајта и дизајна саме веб апликације, постоји могућност, без обзира на све додатне заштите, да се сајт компромитује. Тек детаљном анализом, приступом „бијеле кутије" и искључивањем аутоматског искључивања тестне IP адресе, добили би праву слику о слабостима сваког сајта. Чак и ове откривене би, могуће, довеле до нових, када би се искористиле.

Међутим, иако број уочених рањивости није ни приближно велики као код регуларних сајтова, поражавајућа је чињеница да од 9 анализираних сајтова, код само двије банке нису уочене критичне рањивости (слика 4).

Слика 4: *Број система за електронско банкарство, код којих је откривена одређена критична рањивост*



Извор: Сопствено истраживање

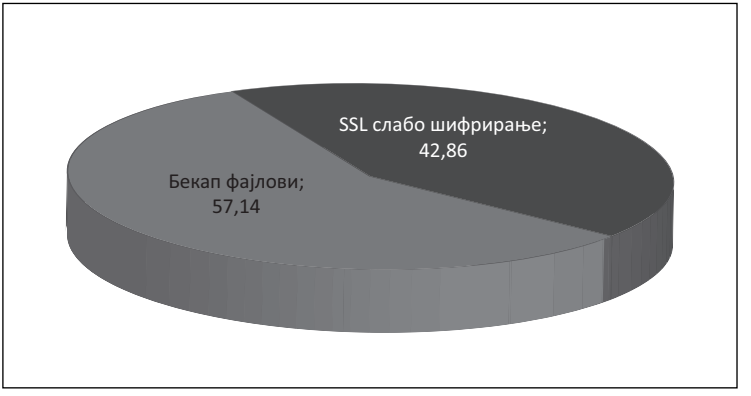
Посебно забрињавајуће дјелује присуство XSS и SQL *injection* (у разним варијантама) рањивости, које се сматрају за најопасније рањивости и чијом

експлоатацијом се може нанијети велика финансијска штета како банци, тако и њеним клијентима.

5.2. Рањивости средњег ризика

Испитујући системе за електронско банкарство, нађена је 21 критична рањивост. Њихова расподјела, по класама, може се видјети на графикону са слике 5. И овдје су неке рањивосте сличне природе смјештене у исту групу.

Слика 5: *Заступљеност рањивости средњег ризика*

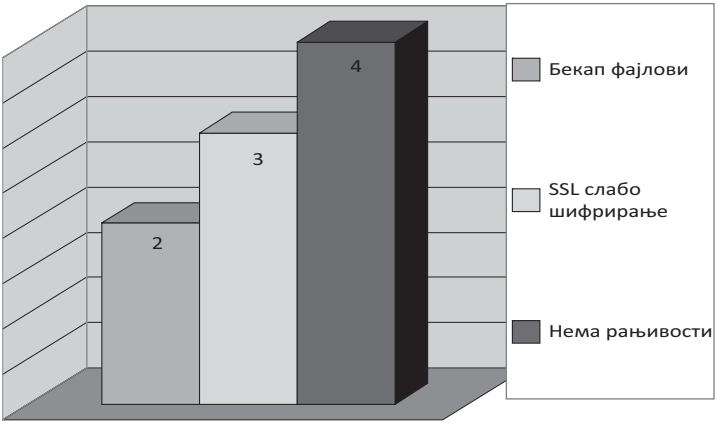


Извор: Сопствено истраживање

Трећина слабости је посљедица старе верзије *Apache* сервера, па се једноставном инсталацијом посљедње верзије, отклања ова рањивост.

И рањивости средњег ризика су нађене код готово свих банака (слика 6).

Слика 6: *Број сајтова за електронско банкарство, код којих је откривена одређена рањивост средњег ризика*



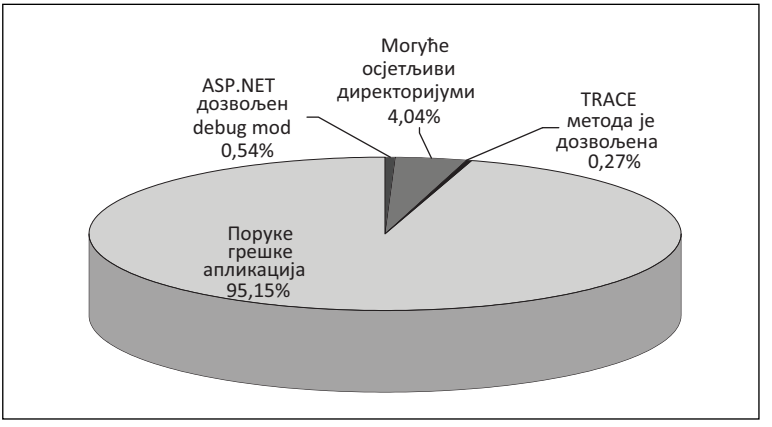
Извор: Сопствено истраживање

Слично као што је раније констатовано, зависно од дизајна софтвера и веб апликације, ове рањивости не морају бити опасне, али, исто тако, могу бити и веома ризичне. Праву процјену може урадити само тим који је програмирао веб апликацију, односно стручно лице које ће имати увид у дизајн веб апликације.

5.3. Рањивости малог ризика

Нађено је 1115 рањивости малог ризика. Већ је речено да се ове слабости не могу искористити за директно компромитовање сајта, али да могу довести до неких података, које ће олакшати злоупотребу неке рањивости већег ризика. На слици 7 приказан је удио уочених рањивости малог ризика.

Слика 7: *Заступљеност рањивости малог ризика*

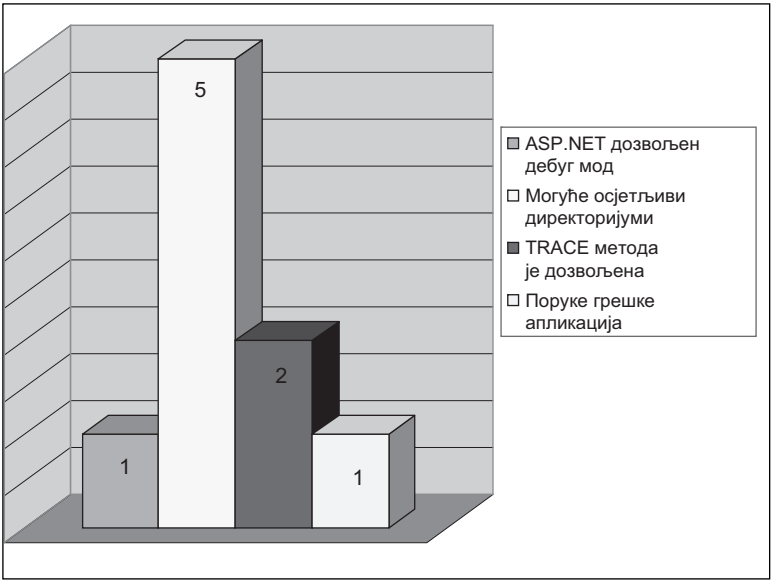


Извор: Сопствено истраживање

Највећи број рањивости малог ризика односи се на поруке о грешкама. Оне могу помоћи нападачу у организовању новог напада. Додатним програмирањем треба подесити веб апликацију да не јављају ове грешке. Остале грешке је лакше отклонити, једноставним подешавањем параметара.

Ако би рањивости малог ризика анализирали по банкама, тада слика 8 даје одговор о заступљености појединих рањивости.

Слика 8: *Број сајтова за електронско банкарство, код којих је откривена одређена рањивост малог ризика*



Извор: Сопствено истраживање

6. Закључак

Тестирано је 9 система за електронско банкарство црногорских банака. Укупно је нађено 1179 рањивости, од чега 43 критичне рањивости (табела 2).

Табела 2: *Рањивости откривене на сајтовима за е-банкарство црногорских банака*

Рањивост	Број откривених рањивисти
Критичне	43
Средњи ризик	21
Мали ризик	1115
Укупно	1179

Извор: Сопствено истраживање

Нађене 43 критичне рањивости носе далеко већи ризик од 1861 критичне рањивости откривене на регуларним сајтовима - на сајту за електронско банкарство директно су угрожени рачуни корисника.

Пошто се у овом случају ради о много осјетљивијим подацима него на регуларном сајту банке, свака банка би требала да уради детаљно испитивање на рањивости. При томе би требало да се користи модел „бијеле кутије“. Иако нападач, по правилу (ако нема инсајдерске информације), не

зна ништа о структури сајта, тј. напада по моделу „црне кутије“, ипак откривањем једне рањивости може доћи до сазнања за налажење нове. Отуда би се моделом „бијеле кутије“ обезбиједило налажење свих потенцијалних пропуста.

Након налажења, треба приступити њиховом отклањању. Неке рањивости, чак и критичне, једноставно се отклањају. На примјер рањивости које користе „рупе“ у старим верзијама софтвера, отклањају се инсталацијом посљедње верзије софтвера. Неке друге рањивости отклањају се једноставним подешавањем параметара. На примјер, на неким сајтовима одобрен је дебуг мод, па то нападач може покренути и искористити. Једноставним искључивањем, отклања се и та слабост.

Нажалост, неке рањивости није лако отклонити. Захтијевају дуготрајно тражење по кôду, па затим интервенцију. Ове интервенције најбезболније може урадити аутор софтвера.

Констатујмо овдје да је једна банка примијенила нов начин заштите лозинке (ПИН-а), уносом преко виртуалне тастатуре[11]. Тиме је онемогућен унос куцањем преко тастатуре, већ се поље за унос попуњава кликом миша по виртуелној тастатури. На овај начин се спречавају разни роботи, који би пробали велики број лозинки за кратко вријеме. Такође се користи као заштита од пецања, али се показало да ову врсту заштите побјеђују специјализовани злонамјерни програми – читачи тастатуре (енг. *keylogeri*).

Иако није све једноставно извести, лако је описати шта треба да уради банке.

Прво, треба инсталирати најновије верзије софтвера који користе. Затим би требало извршити тестирање на рањивости моделом „бијеле кутије“. Потом, треба уклонити све критичне рањивости. Овај дио може потрајати и више мјесеци и вјероватно се морају ангажовати специјализована предузећа. Након уклањања неке рањивости, треба опет вршити тестирање. Може се показати да је уклоњена још нека рањивост, али је, исто тако, интервенција у софтверу могла направити нову слабост.

И када су све слабости отклоњене, не треба сједети скрштених руку, већ се у одређеним интервалима поново мора вршити тестирање на рањивости. Као примјер може послужити и једна од испитиваних банака, код које су уочене критичне рањивости, али су све посљедица пропуста у старој верзији *Apache* сервера (верзија из 2003. године).

Дакле, уочени су одређени недостаци и безбједносни пропусти. Неки од уочених пропуста се могу врло лако отклонити, док за неке треба више времена и ангажовање стручне помоћи. Вријеме ће показати како банке реагу-

[11] Модел примјењују неке банке у свијету, још од 2005. године.

ју на поједине пропусте (и да ли их уопште констатују) и на који начин се то одражава на коришћење електронског банкарства и конкурентност банака.

Литература

1. Garfinkel S., Spafford, E. H., Web Security & Commerce, First Edition, O'Reilly, June 1997
2. Lavasoft: www.lavasoft.com
3. Anti Phishing Working Group – APWG, „Phishing Activity Trends Report 2nd Half 2011": http://www.antiphishing.org/
4. *„FTC, Department of Justice Halt Identity Theft Scam."*, Federal Trade Commission Press, 2004.: http://www.ftc.gov/opa/2004/03/phishinghilljoint.shtm
5. PricewaterhouseCoopers: http://www.pwc.com/
6. Sotirov, A., Stevens, M., Appelbaum, J., Lenstra, A., Molnar, D., Osvik, D.A., de Weger, B., „MD5 considered harmful today: Creating a rogue CA certificate", 25th Chaos Communication Congress, Berlin, December 2008.
7. Kline, K. E., ine, D., SQL in a Nutshell - A Desktop Quick Reference, O'Reilly & Associates
8. WhiteHat Security: „WhiteHat Website Security Statistic Report",Winter 2011, 11th Edition: http://www.whitehatsec.com/
9. WhiteHat Security: „WhiteHat Website Security Statistic Report", Spring 2010, 9th Edition: http://www.whitehatsec.com/
10. Grossman, J. Hansen R., Petkov P. D., Rager A., XSS Attacks: Cross Site Scripting Exploits and Defense, Syngress Publishing, Inc., 2007.
11. Shema, M., Seven Deadliest Web Application Attacks, Syngress Publishing, Inc., 2010.
12. Закон о електронској трговини, Сл. лист РЦГ, бр. 80/04
13. Закон о електронском потпису, Сл.лист РЦГ, бр: 55/03 и 31/05
14. ЦБЦГ – Централна Банка Црне Горе: http://www.cb-cg.org/
15. Acunetix: http://www.acunetix.com/
16. Вујошевић, С. Сигурност сајтова црногорских банака, Montenegrin Journal Of Economics, , Vol 6 No 12, 2010., str. 209-216, ISSN 1800-5845