CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Internet Explorer 7 vs Mozilla Firefox 3

CCERT-PUBDOC-2008-07-233

CERT.hr u suradnji s LSS

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi.

Rezultat toga rada je i ovaj dokument, koji je nastao suradnjom CARNet CERT–a i LS&S–a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

CARNet CERT, www.cert.hr

Nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, www.LSS.hr

Laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. Uvod

Web preglednik je programski paket koji se koristi za prikaz i interakciju s tekstom, slikama, video i audio zapisima te drugim informacijama koje se tipično nalaze na web stranicama, a mogu se koristiti i za pristup informacijama sa web poslužitelja u privatnoj mreži ili sadržaju datotečnog sustava. Danas postoji veliki broj web preglednika, od kojih su poznatiji Mozilla Firefox, Safari, Konqueror, Opera, Flock, Internet Explorer, Epiphany i AOL Explorer .

Zasad najpoznatiji i najčešće korišteni su Internet Explorer i Mozilla Firefox pa će u ovom dokumentu biti dana usporedba upravo tih preglednika, opisane specifičnosti, kao i nedostaci svakog od njih, a poseban će naglasak biti na sigurnosti i mogućnostima zloporabe pojedinih sigurnosnih nedostataka istih. Na kraju će biti dan pregled metoda za implementaciju sigurnosti kod spomenutih preglednika, od kojih su poznatije onemogućavanje Active X kontrola, tzv. *phishing* filtri, prošireni SSL (eng. Secure Sockets Layer) i dr.

2. Općenito o pregledniku Internet Explorer

Internet Explorer preglednik je grafički preglednik tvrtke Microsoft, koji standardno od 1995. godine dolazi u paketu s Microsoft Windows operacijskim sustavima. Od 1999. godine Internet Explorer postaje najrašireniji web preglednik.

Prvi je put izdan kao dio dodatnog paketa Plus! za Windows 95 operacijski sustav, a kasnije su inačice izdane kao besplatni paketi ili dijelovi paketa za održavanje (eng. *service pack*) te su uključene u OEM (eng. *Original equipment manufacturer*) izdanja Windows 95 i kasnijih inačica Windows operacijskih sustava.

Inačica 7.0 izdana je 18. listopada 2006. godine, a dostupna je u obliku nadogradnje za Windows XP Service Pack 2, Windows Server 2003 sa Service Pack 1 ili kasnijim paketom, Windows Vistu i Windows Server 2008 sustave. Uključuje ispravke za prethodno otkrivene sigurnosne propuste, poboljšanja u podršci različitih web standarda, tzv. pregled pomoću tabulatora (eng. *tabbed browsing*) i brojne druge dodatke. S inačicom 7, Internet Explorer odvaja se od Windows ljuske – za razliku od prethodnih inačica, Active X kontrola više nije dio Windows Explorer procesa, već se pokreće na odvojenom procesu Internet Explorera. Time je dobiveno na sigurnosti preglednika, budući da se razni zlonamjerni programi i virusi često distribuiraju putem ActiveX kontrola. Ova izmjena uvjetuje manje ovlasti ActiveX kontrola nad operacijskim sustavom pa tako one predstavljaju manju opasnost za sustav.

Izvorno izdanje inačice 7 zahtijevalo je prije instalacije prolaz WGA (eng. *Windows Genuine Advantage*) provjere operacijskog sustava, koja je trebala spriječiti piratstvo, a radi na sljedeći način: kad korisnik prvi put posjećuje Microsoftove stranice za nadogradnju ili preuzimanje programa, mora obaviti validaciju svojeg primjerka Windows sustava, na način da preuzme ActiveX kontrolu koja će obaviti odgovarajuće akcije. Nakon toga može nastaviti sa preuzimanjem željenih programa, a posebna datoteka (licenca) sprema se na računalo za buduću verifikaciju. Međutim, u listopadu 2007. godine, Microsoft je maknuo taj zahtjev te je time nova inačica postala dostupna svim korisnicima.

2.1. Karakteristike i mogućnosti preglednika Internet Explorer 7

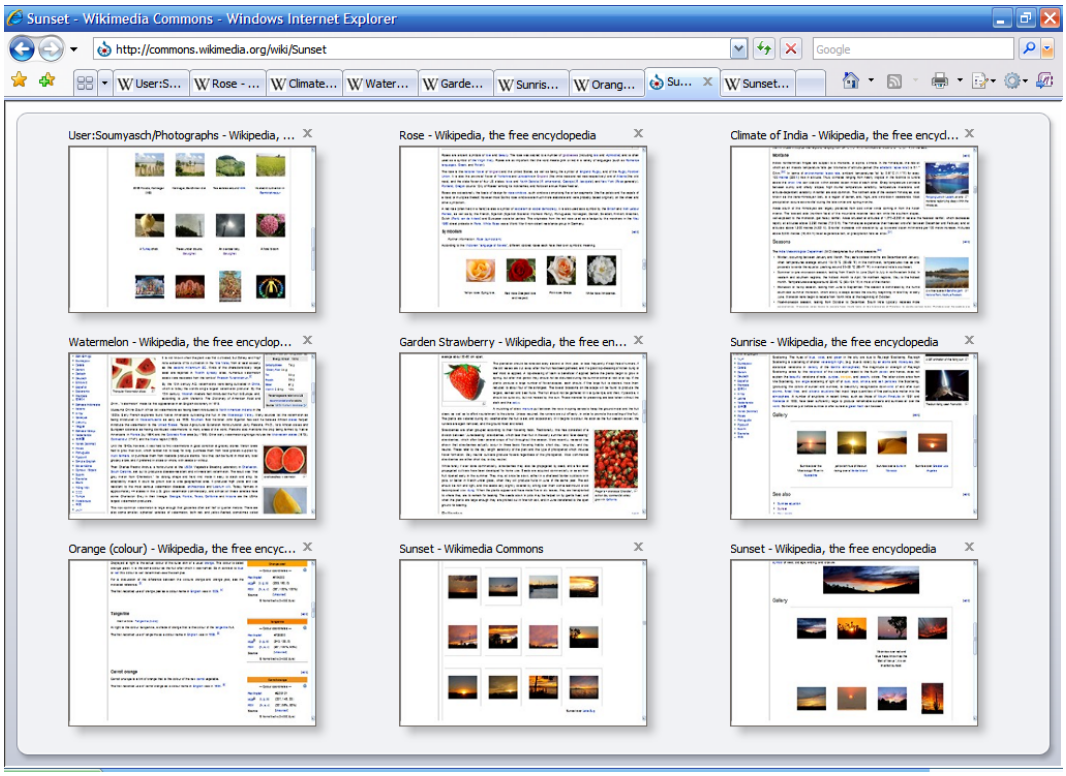
Velik dio temeljne arhitekture Internet Explorer preglednika je s izlaskom inačice 7.0 znatno izmijenjen (kao što je komponenta za automatsko iscrtavanje, sigurnosno okruženje i sl.). Djelomice kao rezultat sigurnosnih poboljšanja, Internet Explorer preglednik je sad samostalna aplikacija (za razliku od prethodnih inačica ugrađenih u Windows ljusku) i tako više nema mogućnost obavljanja funkcija datotečnog preglednika. Nova inačica tako ima manje ovlasti nad operacijskim sustavom, što dodatno povećava sigurnost preglednika, odnosno samog operacijskog sustava.

Na Windows Vista operacijskom sustavu, Internet Explorer radi u posebnom - zaštićenom načinu rada, koji mu onemogućava pristup ostatku operacijskog ili datotečnog sustava. Kad radi u takvom načinu rada, Internet Explorer ne može dobiti ovlasti pisanja u datoteke i tzv. *registry* zapisnik izvan direktorija korisničkog profila, što ima za cilj sprečavanje instalacije zlonamjernih programa (eng. *spyware*) na korisničko računalo. Iako je većina sigurnosnih mogućnosti Internet Explorer 7 preglednika dostupna i za druge inačice Windows sustava, zaštićeni je način rada omogućen samo kod Vista sustava, budući da se temelji na sigurnosnim mogućnostima same Vista inačice operacijskog sustava.

2.2. Novosti u odnosu na prethodne inačice

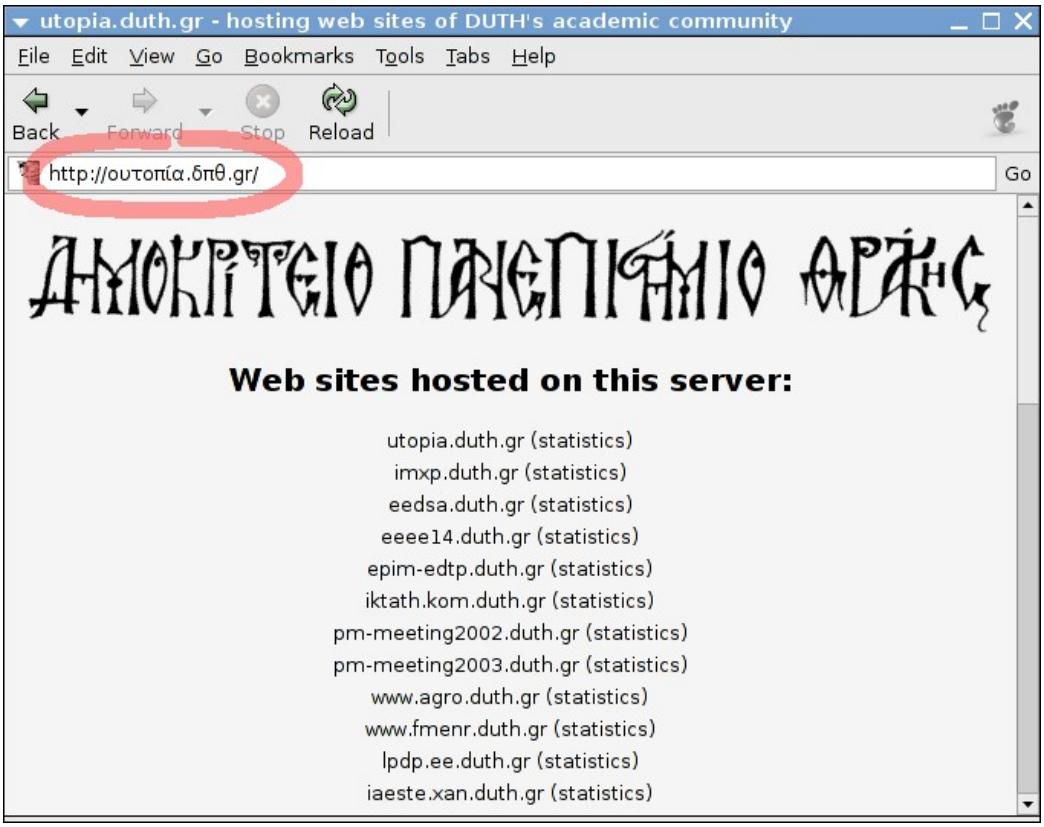
Najznačajnije izmjene i dopune u odnosu na starije inačice navedene su u nastavku.

- Iz sigurnosnih razloga, Internet Explorer više nije integriran u Windows Explorer ljusku. Lokalne datoteke pisane u Internet Explorer 7 pregledniku otvaraju se pomoću Windows Explorer ljuske, a stranice tipkane u Windows Explorer ljusci otvaraju se korištenjem podrazumijevanog web preglednika.
- Za Windows Vista sustave dostupan je i novi, zaštićeni način rada (eng. *Protected Mode*), u kojem preglednik radi s manjim ovlastima od ovlasti ograničenog korisničkog računa. Na taj način može pisati samo u direktorij privremenih Internet datoteka i ne može instalirati nove programe niti mijenjati konfiguraciju operacijskog sustava bez komunikacije putem "posredničkog" procesa. Iako je većina sigurnosnih mogućnosti Internet Explorer 7 preglednika dostupna i za druge inačice Windows sustava, zaštićeni je način rada omogućen samo kod Vista sustava, budući da se temelji na novim sigurnosnim mogućnostima koje postoje tek kod Vista inačica operacijskog sustava.
- Inačica 7 podržava pregledavanje pomoću tabulatora, odnosno mogućnost pregleda više stranica u istom prozoru, pri čemu je svaka stranica na svom tabulatoru. Osim toga, korisnicima je omogućeno i ručno preuređivanje tabulatora povlačenjem i ispuštanjem na željeno mjesto (eng. *drag and drop*). Sljedeća slika prikazuje opisanu opciju.



Slika 1: Pregledavanje stranica pomoću tabulatora

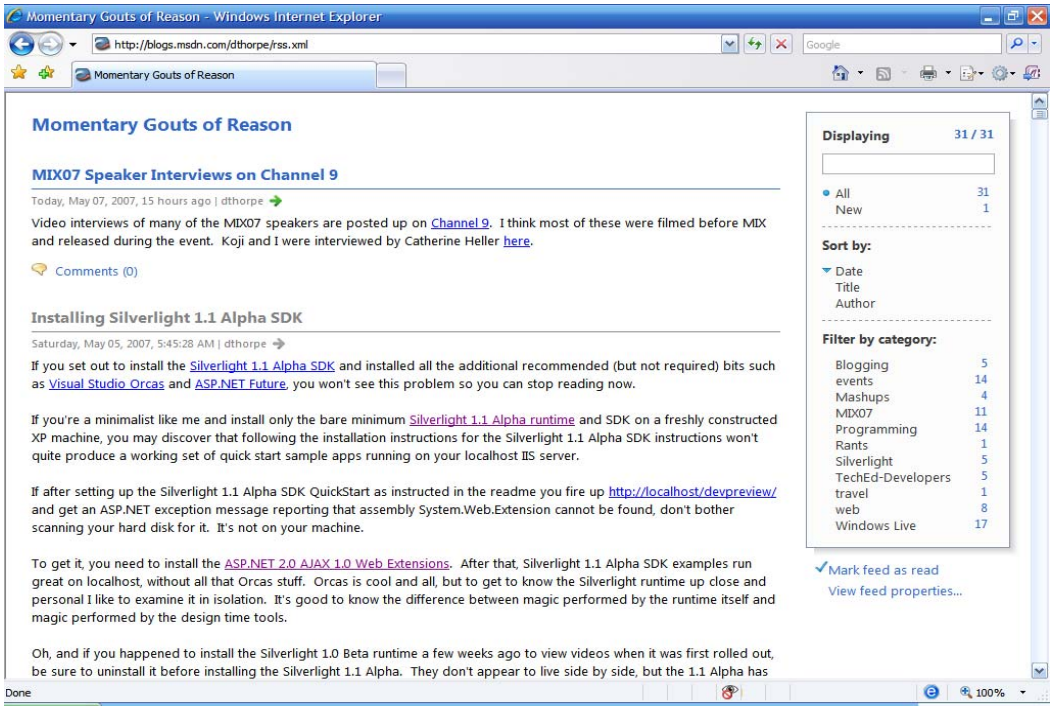
- Dodana je i potpora internacionalnom imenovanju domena (eng. *internationalized domain names*), s uključenom zaštitom od ometanja (eng. *spoofing*). Ako korisnik posjeti stranicu čije je ime na stranom jeziku (sadrži nelatinične znakove), stranica će biti prikazana u tzv. *punycode* načinu kodiranja, koji omogućava pretvorbu *Unicode* znakovnih nizova u abecedu s manjim skupom znakova dozvoljenih za korištenje u imenima računala. Isto tako, nelatinični se znakovi mogu (s nekim ograničenjima) prikazivati i u kombinaciji s latiničnim znakovima. U potonjem se slučaju *punycode* koristi ako računalo nema instaliranu potporu za nelatinične znakove. Ovaj dodatak omogućava sprečavanje tzv. *spoofing* napada, u kojima se neki znakovi zamjenjuju sa sličnim znakovima iz druge abecede. Primjer stranice čiji naziv sadrži nelatinične znakove nalazi se na sljedećoj slici:



Slika 2: Primjer internacionalnog imenovanja domena

- Dodano je polje za pretraživanje (eng. *search box*), koje korisnicima omogućava i ručno dodavanje pružatelja rezultata pretraživanja, kao što su Google, Altavista, Yahoo!, Live Search, Wikipedia i dr.

- Dodana je integrirana komponenta za čitanje novosti (eng. *feed reader*), što korisnicima omogućava čitanje web novosti bez korištenja dodatnih RSS čitača (slika 3). Mogućnosti ovog integriranog čitača uključuju automatsko otkrivanje novih informacija i pronalaženje ažuriranih informacija čak i kada preglednik nije pokrenut.



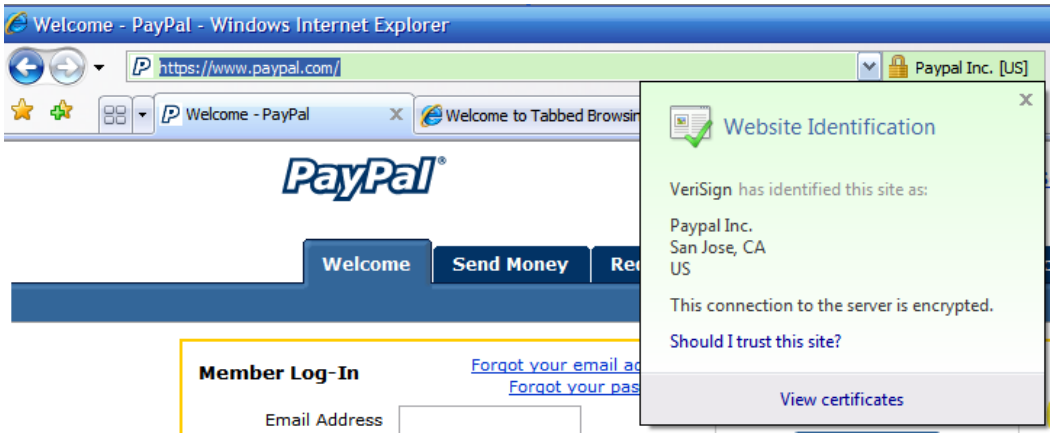
Slika 3: Integrirani RSS čitač

- Opcija *ActiveX Opt-In* blokira ActiveX kontrolu, osim ako joj je dopuštena instalacija. Ova mogućnost povećava sigurnost neprovjerenih i ranjivih kontrola. Korisnik može uključiti ili isključiti spomenutu opciju korištenjem tzv. *Add-on Manager* komponente.
- U novoj su inačici prisutna i brojna poboljšanja u ostvarenju brojnih standarda, kao što su CSS (eng. *Cascading Style Sheets*), DOM (eng. *Document Object Model*) i HTML (eng. *HyperText Markup Language*).
- Ispravljen je i poznati problem rezanja desnog dijela web stranice prilikom ispisa, a osim toga, dodana je i opcija "sažimanja" stranice kako bi više teksta stalo na istu stranicu. Obnovljeno je i sučelje za pregled ispisa (eng. *Print Preview*), gdje novo sučelje korisnicima omogućava povlačenje margina i neposredan pregled rezultata.
- Dodana je mogućnost zumiranja stranice, koja povećava sadržaj stranice i tako omogućava lakše čitanje na većim ekranima.
- Tzv. "*ClearType*" opcija prikaza teksta može biti omogućena ili onemogućena, neovisno o tipu operacijskog sustava koji se koristi. *ClearType* je Microsoftova implementacija tehnologije za iscrtavanje, koja uzima u obzir fizička svojstva ekrana. Razvijena je s namjerom da poboljša prikaz teksta na određenim tipovima računalnih ekrana, posebno LCD monitorima s ravnim ekranom.
- Dodan je tzv. *Phishing Filter,* koji nudi zaštitu od *phishing* napada i drugih web stranica koje se smatraju opasnim po korisnika koji bi na njima trebali upisivati svoje osobne podatke. Kad je ova opcija omogućena, svaka se stranica koju korisnik posjećuje provjerava uz pomoć liste poznatih, prethodno prijavljenih zlonamjerno oblikovanih stranica, koja se nalazi na Microsoftovom poslužitelju. Ako je stranica pronađena na listi, filtar blokira pristup stranici, a korisnika se o tome obavještava u obliku upozorenja koje mu se ispisuje na ekranu. Ako

stranica još nije na popisu poznatih zlonamjerno oblikovanih, odnosno korisnik je prvi koji ju je otkrio prilikom pretraživanja, na ekranu mu se pojavljuje žuto upozorenje u sigurnosnoj statusnoj traci, koja se nalazi pokraj adresne trake. Nakon toga, korisnik može klikom na ispisano upozorenje obavijestiti nadležne o otkrivenoj stranici, koja će se nakon toga dodati na listu postojećih zlonamjernih sjedišta. *Phishing* filter nije automatski omogućen, već se korisnika pita o njegovom uključivanju prilikom pokretanja Internet Explorer 7 preglednika.

- Adresna i statusna traka se pojavljuju u svim prozorima, a koristi se i različito bojanje adresne trake, što ima za cilj naglasiti pouzdanost posjećene stranice. Kad korisnik utipka adresu stranice koja ima neodgovarajući sigurnosni certifikat, traka postaje crvena i automatski se sprečava navigacija na tu stranicu (što korisnik može izmijeniti eksplicitnim potvrđivanjem željene navigacije), ako stranica ne koristi nikakvu enkripciju traka postaje bijela, a ako stranica koristi snažne sigurnosne certifikate, traka postaje zelena.
- Adresna traka više ne dozvoljava izvođenje JavaScripta na praznim (*about:blank*) stranicama, iako razlog za tu izmjenu nije objavljen. Ova je mogućnost i dalje podržana na ostalim stranicama, što omogućava ispravan rad tzv. *bookmarklet* appleta**.** Bookmarkleti su malene računalne aplikacije, spremljene kao URL adresa oznake za nalaženje stranice (eng. *bookmark*) u web pregledniku ili kao poveznica na web stranici.
- Opcija "*Delete Browsing History*" briše u jednom koraku sve podatke o prethodno posjećenim stranicama, a moguće je obrisati i samo pojedine podatke (samo kolačiće i sl.). Prije inačice 7, ovaj se postupak obavljao u nekoliko koraka, u kojima su korisnici morali zasebno birati brisanje pregledničke privremene memorije, tzv. kolačića (eng. *cookie*), spremljenih podataka i zaporki i sl. Ova je mogućnost korisna za osiguranje privatnosti u okruženjima s više korisnika.
- Opcija "*Fix My Settings*" omogućava provjeru izmijenjene postavke prilikom pokretanja preglednika te obavještava korisnika putem informacijske trake ako je trenutno stanje postavke nesigurno. Također, klikom na opciju "*Fix My Settings*" na informacijskoj traci korisnici mogu izmijeniti postavke u sigurno stanje, odnosno podrazumijevano (eng. *default*) stanje srednje razine sigurnosti.
- Uklonjeni su stari protokoli i tehnologije, između ostalog i DHTML kontrola za izmjenu web stranica (samo za Windows Vista sustave), što ima za cilj smanjenje površine za izvođenje sigurnosnih napada. DHTML je izraz koji označava umijeće izrade dinamičkih i interaktivnih web stranica, kombiniranjem različitih tehnologija, kao što su HTML, CSS, DOM i JavaScript.
- Jačina (veličina) šifri je za Windows Vista sustav 256 bita, dok je za ostale sustave 128 bita. Za usporedbu, prethodne su inačice podržavale 128-bitnu veličinu šifri, pri čemu je bilo potrebno instalirati dopunski paket (eng. *service pack*).

- Uključena je i podrška za proširene validacijske certifikate (eng. *Extended Validation Certificates*, EV). Kad stranica sadrži takav certifikat, adresna se traka boji zeleno.



Slika 4: Primjer stranice s EV certifikatom

- Dodana opcija "*Reset Internet Explorer settings*" briše sve privremene datoteke, onemogućava preglednicke dodatke te mijenja sve izmijenjene postavke na tvorničke. Može se koristiti ako preglednik, zbog izmjene određenih postavki, postane neupotrebljiv.
- U odnosu na prošlu inačicu postoje i razlike u količini memorijskih i sistemskih resursa koji su potrebni za instalaciju – primjerice 64MB RAM (eng. *random access memory*) memorije umjesto minimalnih 32 MB kod prethodne inačice te 233MHz procesor umjesto 66MHz kod inačice 6.
- Dodana je i mogućnost pokretanja preglednika bez instaliranih dodataka, što se postiže odabirom opcije "*No Add-ons*".

U sljedećoj su tablici navedene najznačajnije izmjene u pojedinim inačicama Internet Explorer 7 preglednika.

Inačica	Datum izdavanja inačice	Značajnije izmjene
7.0 Beta 1	27. srpanj 2005.	Dodana podrška za alfa kanal, ispravljeni neki CSS propusti, dodano pregledavanje pomoću tabulatora.
7.0 Beta 2 Preview	31. siječanj 2006.	Ispravljeni dodatni CSS propusti, dodana integracija RSS platforme i *Quick Tabs* opcija.
7.0 Beta 2	24. travanj 2006.	Ispravljeni još neki CSS propusti i propusti vezani uz kompatibilnost aplikacije.
7.0 Beta 3	29. lipanj 2006.	Ispravljeni problemi s iscrtavanjem za CSS.
7.0 RC 1	24. kolovoz 2006.	Postignuta poboljšanja u performansama, stabilnosti, sigurnosti, kompatibilnosti aplikacije i konačnim CSS korekcijama.
7.0	18. listopad 2006.	Finalno izdanje.

Tablica 1: Pregled razvoja preglednika Internet Explorer 7

3. Općenito o pregledniku Mozilla Firefox

Mozilla Firefox je besplatni web preglednik, pisan u programskim jezicima: C++, XUL, XBL i JavaScript. Podržan je na većini današnjih popularnih platformi (Microsoft Windows, Mac OS X, Linux te brojnim drugim sustavima nalik operacijskom sustavu Unix), a dostupan je i na preko više od 45 jezika. Nakon preglednika Internet Explorer (kojeg je u lipnju 2008. koristilo 54% korisnika), Mozilla je drugi najpopularniji web preglednik na svijetu (41% korisnika). Koristi besplatan programski paket Gecko (autora *Netscape Communications Corporation*) za prikaz web sadržaja (XML, HTML, slikovne datoteke i dr.). Neke od mogućnosti koje pruža preglednik Mozilla Firefox su sljedeće:

- pregledavanje korištenjem tabulatora,
- kontrola pravopisa (na engleskom jeziku),
- inkrementalno pretraživanje,
- dodatak za upravljanje prijenosom podataka,
- integrirani program za pretraživanje i dr.

Više o svakoj od spomenutih opcija bit će riječi u nastavku. Razvojni programeri koji se bave razvojem preglednika Firefox nastoje izgraditi preglednik koji pruža najbolje mogućnosti pretraživanja Interneta i prilagođen je najširoj populaciji. Osim prethodno spomenutih opcija, Mozilla Firefox nudi i mogućnost nadopunjavanja funkcionalnosti raznim dodacima (više od 2000 dodataka) od kojih su najpopularniji:

- *NoScript* - za onemogućavanje prikaza *JavaScript, Java, Flash* i drugog skriptnog sadržaja,
- *Tab Mix Plus* - za dodavanje raznih prilagodljivih opcija tabulatorima,
- *FoxyTunes* - prilagodba programa za pregled audio i video sadržaja,
- *Adblock Plus* - za postavljanje filtara, omogućava blokiranje prikaza različitih sadržaja kao što su reklame i sl.,
- *DownThemAll!* - omogućava jednostavno zaustavljanje i ponovno pokretanje preuzimanja datoteka, bez gubitka informacija, kao i brzo preuzimanje putem jednog klika na poveznice sadržane na trenutnoj web stranici i
- *Web Developer* - alati za uređivanje i ispravljanje pogrešaka, namijenjeni razvojnim programerima.

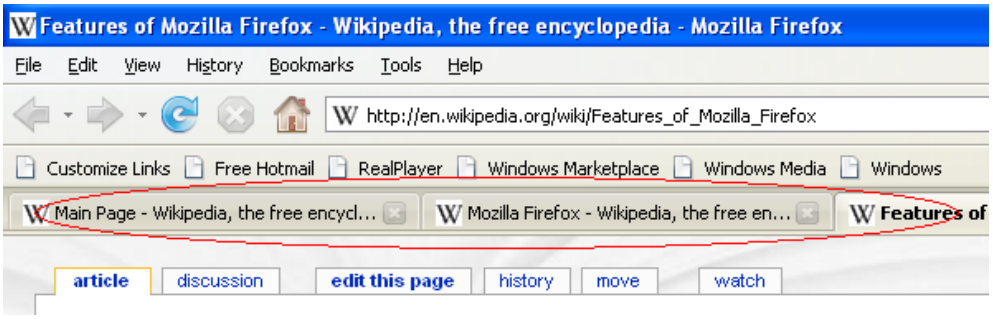
Podržava i velik broj web standarda, kao što su HTML, XML, XHTML, SVG, CSS, ECMAScript (JavaScript), DOM; MathML, DTD, XSLT, XPath, PNG slikovne datoteke sa tzv. alfa transparentnošću i dr.

Inačica 3.0.1, izdana je 16. srpnja 2008. godine.

3.1. Karakteristike i mogućnosti preglednika Mozilla Firefox 3

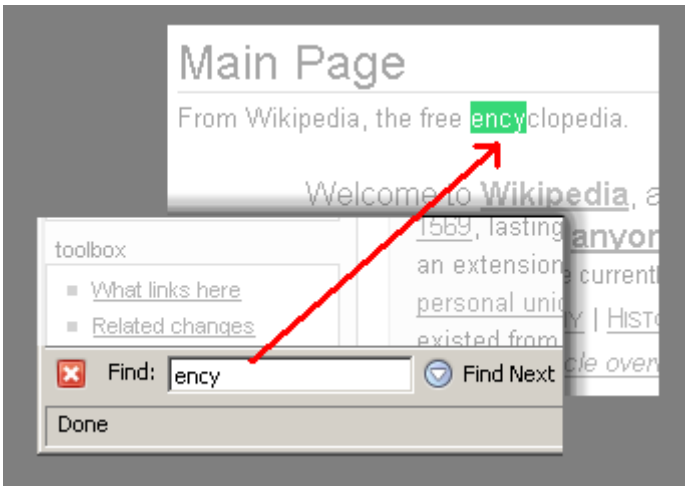
Najznačajnije i najzanimljivije opcije koje pruža Firefox preglednik su sljedeće:

- Mozilla Firefox podržava pregledavanje više web stranica u istom prozoru, između kojih se navigacija vrši korištenjem tabulatora. Osim toga, omogućeno je i postavljanje nekoliko URL adresa kao osnovnih stranica (eng. *homepage*), pri čemu se sve stranice automatski otvaraju u različitim tabulatorima.



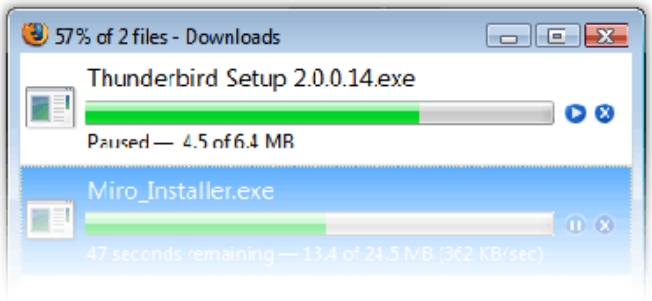
Slika 5: Pregled pomoću tabulatora

- Ugrađen kontrolor pravopisa (eng. *spell checker*) dopušta unos teksta direktno u web stranicu kao zapis u dnevniku (eng. *blog*) ili web-temeljenu poruku elektroničke pošte, pri čemu se vrši kontrola pravopisa, pogreški kod tipkanja i sl.
- Inkrementalno pretraživanje omogućava pretraživanje neposredno prilikom utipkavanja ključnih riječi – kako korisnik unosi riječi za pretraživanje, Firefox automatski prikazuje moguće rezultate, još prije završetka unosa.



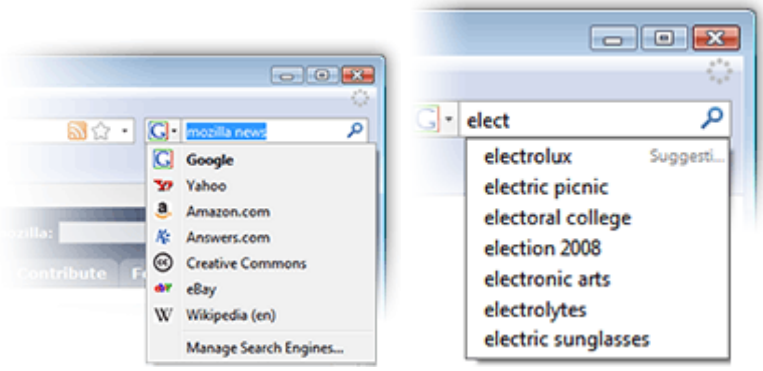
Slika 6: Prikaz rezultata pretraživanja prilikom unosa teksta

- Novi program za upravljanje prijenosom podataka (eng. *download manager*) omogućava jednostavno i sigurno preuzimanje datoteka. Ima mogućnost zaustavljanja i ponovnog pokretanja, što funkcionira i kod neočekivanih situacija, kao što je rušenje sustava i sl.



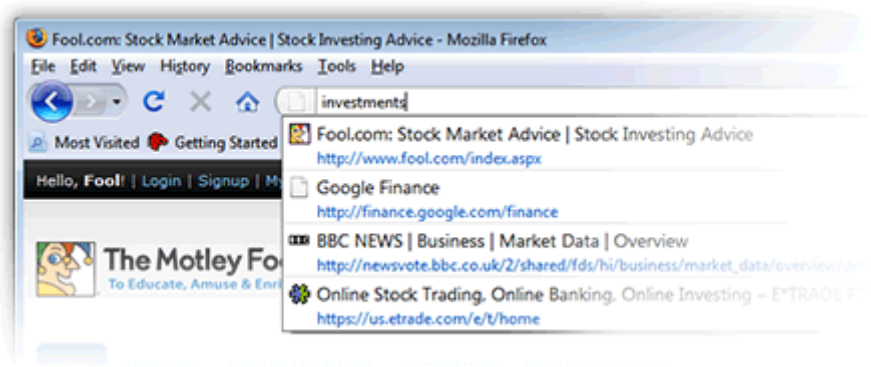
Slika 7: Program za upravljanje preuzimanjem datoteka

- Firefox posjeduje i brojne mogućnosti pretraživanja, kao što je prikaz prijedloga ključnih riječi prilikom unosa u polje za pretraživanje, odabir željenog web programa za pretraživanje (*Google, Yahoo!, Amazon.com* i dr.) iz integrirane trake za pretraživanje i sl.



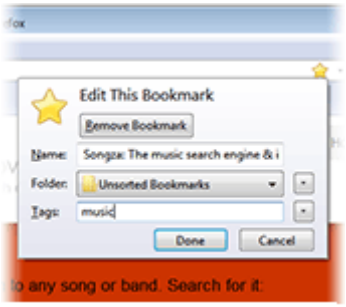
Slika 8: Mogućnosti pretraživanja

- Jedna od popularnijih mogućnosti je i pametna adresna traka (eng. *smart location bar*), koja prilikom unosa URL adrese, osim pretraživanja povijesti pristupa web stranicama, pretražuje oznake (eng. *bookmarks*) i pokušava pronaći potrebnu adresu. Osim toga, omogućena je i navigacija na stranicu putem unosa naslova umjesto URL adrese.



Slika 9: Pametna adresna traka

- Dodana je i mogućnost obnavljanja postojećih oznaka (eng. *live bookmarks*). Postojeće se oznake automatski nadopunjuju u stvarnom vremenu i tako korisnicima omogućavaju pristup najnovijim informacijama. Osim toga, omogućeno je i jednostavno uređivanje oznaka, jednim klikom na zvjezdicu u adresnoj traci.



Slika 10: Uređivanje oznaka

3.2. Novosti u odnosu na prethodne inačice

Jedna od najvećih izmjena u pregledniku Firefox 3 je implementacija nadograđenog programa za prikaz sadržaja – Gecko 1.9. Nova Gecko inačica u odnosu na prethodne uklanja brojne nedostatke (kao što su nedostaci vezani uz izmjenu atributa elemenata <object> i <embed> pomoću JavaScripta i sl.), pokazuje bolje performanse i implementira nova web aplikacijska sučelja. Dodatno, zahvaljujući ovim izmjenama, Firefox 3 je prvi puta uspješno položio tzv. Acid2 test, a pokazuje i bolje rezultate na Acid3 testu. Za usporedbu, Internet Explorer zasad ne uspijeva proći spomenute testove. Riječ je o testovima koji se koriste za otkrivanje ranjivosti kod prikaza sadržaja web stranica, pri čemu Acid2 test testira podršku za HTML i CSS web standarde, dok Acid3 testira korištenje JavaScript i DOM standarda.

Osim toga, dodana je i podrška za rukovanje protokolima temeljenim na webu te podrška za web aplikacije koje nisu spojene na Internet.

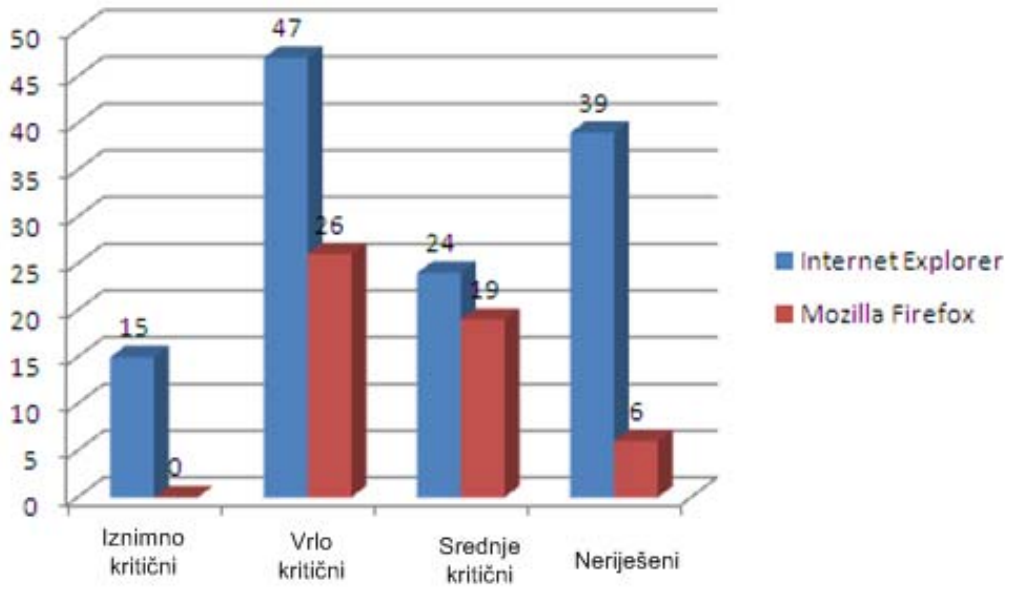
Od izmjena vezanih uz samo sučelje, najznačajnije su izmjene programa za prijenos datoteka, dodavanje programa za upravljanje dodacima (eng. *plug-in manager*) i instalaciju programskih paketa (eng. *package manager*). Program za upravljanje zaporkama u novoj inačici pita korisnika o spremanju zaporke nakon same prijave, a ne prije prolaska autorizacijskog postupka, što je bio slučaj u prethodnim inačicama i često je završio spremanjem pogrešne zaporke zbog grešaka u tipkanju i sl. Prethodno spomenuta opcija označavanja stranica (što kasnije omogućava pretraživanje i po naslovu, kao i pretraživanje oznaka umjesto samo povijesti pristupa stranicama) također je novost u inačici Firefox 3. Izmijenjen je i podrazumijevani izgled preglednika, koji je različit za različite operacijske sustave, dodane su nove ikone i dr.

4. Sigurnost web preglednika

Web preglednici, koliko god metoda zaštite od raznih sigurnosnih prijetnji implementirali, ipak sadrže komponente zbog kojih su posebno ranjivi na nekoliko tipova sigurnosnih napada. Neki od najpoznatijih napada na web preglednike su tzv. *phishing* napadi, napadi pokretanjem proizvoljnog programskog koda, napadi iskorištavanjem nepravilnosti AcitveX kontrola, uskraćivanje usluga rušenjem preglednika i sl. Razloga za takav ishod je više – kod nekih web preglednika više se pažnje posvećuje izradi raznih novih opcija za kvalitetnije pretraživanje pa manje vremena/resursa ostaje za posvećivanje sigurnosnim problemima. S druge strane, zlonamjerni korisnici ne čekaju – neprestano dolazi do novih vrsta sigurnosnih napada pa koliko se god trudili poboljšati zaštitu web preglednika, proizvođači su nekako uvijek korak u zaostatku.

4.1. Sigurnost Internet Explorera vs. sigurnost Mozille Firefox

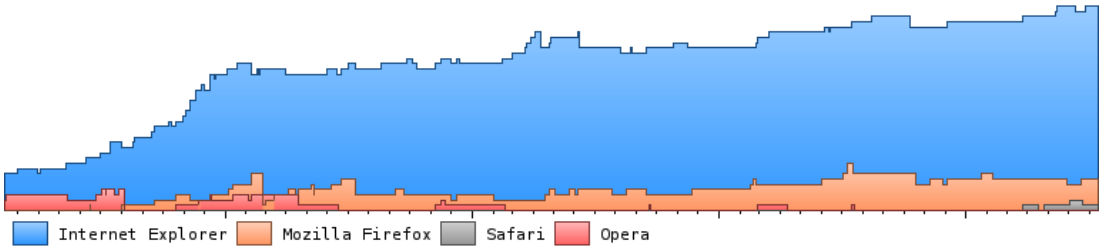
Prema izvještaju istraživačkog tima *Secunia*, izdanom 3. lipnja 2008. godine, Internet Explorer ima zabilježenih 135 izvješća o ranjivostima, od kojih je 24 označeno srednje teškim propustima, 47 je kritičnih propusta i 15 ekstremno kritičnih. Zasad je ostalo 39 neriješenih problema, od kojih je 10 označeno srednje teškim i 1 kritičnim. S druge strane, zabilježeno je 70 sigurnosnih izvješća Mozilla Firefox preglednika – 19 srednje teških propusta, 26 kritičnih i 0 ekstremno kritičnih. Također postoje i zasad neriješeni problemi i to 6 problema, od kojih je jedan srednje težine i jedan kritičan.



Slika 11: Odnos prijavljenih ranjivosti Internet Explorer i Mozilla Firefox preglednika

Osim toga, prema istraživanjima *Secunia* tima, ranjivosti preglednika Firefox su često manje kritične od onih u Internet Exploreru. Isto tako, sigurnosni propusti preglednika Mozilla Firefox se najčešće uklanjaju vrlo brzo. Prema istraživanjima tima *Symantec*, zakrpe za ranjivosti Firefox preglednika izdaju se u prosjeku 1 dan nakon što su ranjivosti objavljene, dok se na izdavanje zakrpe za Internet Explorer čeka u prosjeku 9 dana.

Sljedeća slika prikazuje odnos ranjivosti nekoliko web preglednika od 2004. godine do danas, gdje je vidljivo kako Internet Explorer ima zabilježeno daleko najviše ranjivosti, iako je Mozilla Firefox odmah sljedeći po broju propusta.



Slika 12: Usporedba sigurnosti nekoliko web preglednika

Na slici je vidljiva usporedba i s drugim popularnim web preglednicima – Opera i Safari. U istom razdoblju, Safari je imao prijavljeno samo 5 sigurnosnih propusta, od kojih su 4 proglašena vrlo kritičnima, dok je jedan, zasad još uvijek neriješen, označen manje kritičnim. Opera je imala prijavljeno nešto više – 65 sigurnosnih propusta, od kojih je 16 bilo vrlo kritičnih, 20 srednje kritičnih i 1 ekstremno kritičan. Sve prijavljene ranjivosti su uklonjene.

4.1.1. Sigurnosni propusti i njihova zloporaba

Jedna od poznatijih ranjivosti koje se javljaju kod web preglednika je sigurnosni propust JavaScript komponente, koja može dovesti do izmjene proizvoljnih memorijskih lokacija. Navođenjem korisnika na navigaciju na posebno oblikovanu web stranicu napadač može iskoristiti ovakvu ranjivost za rušenje preglednika ili pokretanje proizvoljnog programskog koda. Takva mu situacija omogućava umetanje virusa ili drugih zlonamjernih programa u ranjivo računalo. Slična je ranjivost (čija uspješna zloporaba omogućava uzrokovanje istih problema) uočena kod preglednika Firefox, a vezana je uz nepravilnosti u radu programa za prikaz web sadržaja (eng. *layout engine*).

I Internet Explorer posjeduje nedostatke u radu JavaScript komponente koje je moguće iskoristiti navođenjem korisnika na otvaranje web stranice s posebno oblikovanim JavaScript kodom. Ovakvi nedostaci omogućavaju pokretanje proizvoljnog programskog koda, a samim i time druge načine kompromitacije ranjivog sustava, kao što je pristup nekim potencijalno osjetljivim informacijama, izmjena određenih postavki, stjecanje povećanih ovlasti i sl.

Do pokretanja proizvoljnog programskog koda može doći i iskorištavanjem ranjivosti ActiveX kontrola. ActiveX kontrole su specifične funkcije ili setovi funkcija koje se koriste za izgradnju funkcionalnosti web preglednika i drugih aplikacija. Korištenjem ActiveX kontrola omogućena je enkapsulacija pojedinih dijelova funkcionalnosti, što omogućava višekratno korištenje i ugradnju istih i u druge aplikacije. Iskorištavanjem nedostataka korištenih kontrola napadač može kompromitirati osjetljivi sustav, budući da su razni zlonamjerni programi distribuirani putem ActiveX kontrola u web stranicama. Međutim, ActiveX kontrole su u nekim slučajevima neophodne i vrlo korisne, primjerice kod posjeta stranicama *Windows Update* ili *Security Updates*, pomoću kojih Microsoft svojim korisnicima omogućava pristup datotekama sigurnosnih nadogradnji.

Web preglednici ranjivi su i na tzv. *phishing* napade. *Phishing* napadi uključuju aktivnosti kojima zlonamjerni napadači korištenjem lažiranih poruka elektroničke pošte i lažiranih web stranica financijskih organizacija pokušavaju korisnike navesti na otkrivanje osjetljivih osobnih podataka kao što su korisnička imena i zaporke, PIN brojevi, brojevi kreditnih kartica i sl. Dakle ovdje se radi o primjeru korištenja tehnika socijalnog inženjeringa za zavaravanje korisnika. Borba protiv *phishing* napada uključuje povećanje osviještenosti korisnika, razne tehničke mjere i sl.

4.1.2. Kritični sigurnosni propusti novih inačica preglednika

Secunia je zasad objavila 3 sigurnosne preporuke za preglednik Mozilla Firefox 3.0, među kojima nema neispravljenih nedostataka. Internet Explorer ima objavljeno 29 sigurnosnih preporuka, od kojih za njih 10 nisu objavljene sigurnosne zakrpe.

Sva 3 sigurnosna propusta preglednika Mozilla Firefox 3 bila su označena vrlo kritičnima. Radilo se o sljedećim nedostacima:

- Prvi je nedostatak bio vezan uz inačicu Firefox paketa namijenjenu Mac OS X operacijskom sustavu, a mogao se iskoristiti za pokretanje proizvoljnog programskog koda oslobađanjem neinicijaliziranog pokazivača pomoću posebno oblikovane GIF (eng. *Graphics Interchange Format*) slikovne datoteke.
- Druga je preporuka obuhvaćala nekoliko kritičnih sigurnosnih propusta, koji su zlonamjernim korisnicima omogućavali izvođenje tzv. *spoofing* napada, zaobilaženje određenih sigurnosnih ograničenja te pokretanje proizvoljnog skriptnog koda.
- Konačno, treća je ranjivost bila vezana uz neodgovarajuću implementaciju CSS standarda, a napadačima je omogućavala izvođenje napada pokretanjem proizvoljnog programskog koda.

Od objavljenih preporuka za Internet Explorer, samo u 2008. godini objavljeno je 7 preporuka – 3 vrlo kritična propusta, 1 srednje kritičan i 3 nekritična. Veliki problem predstavlja činjenica da 3 od objavljenih 7 propusta još uvijek nisu ispravljena. Otkriveni kritični nedostaci bili su sljedeći:

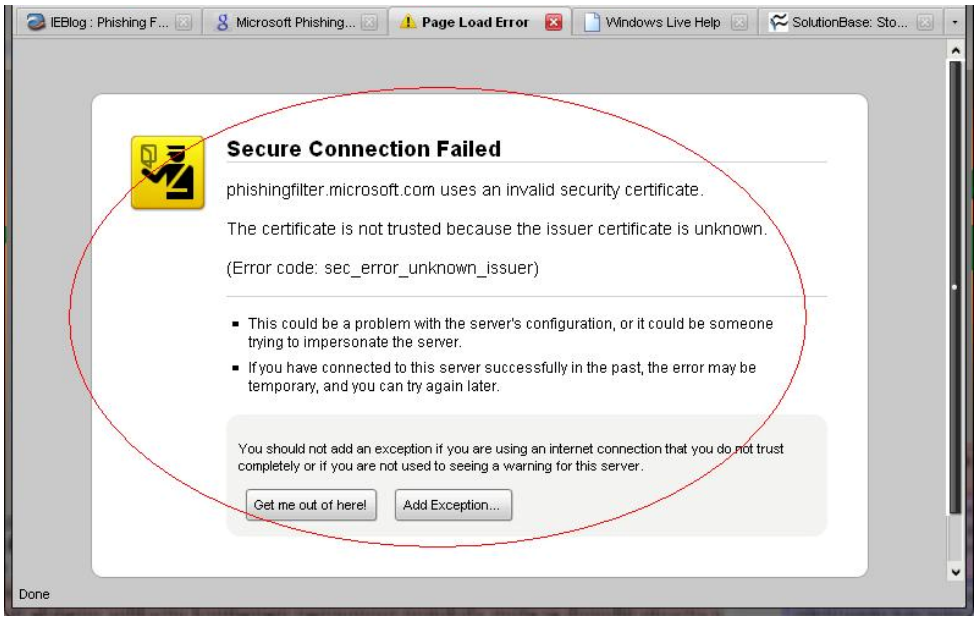
- Prvi je nedostatak vezan uz nepravilnosti u implementaciji DOM standarda, a može se iskoristiti za pokretanje proizvoljnog programskog koda.
- Drugi propust uzrokovan je pogreškama koje se manifestiraju prilikom obrade tokova podataka, a napadaču omogućava pokretanje proizvoljnog programskog koda. Uspješna zlouporaba pritom uključuje navođenje korisnika na posjet zlonamjerno oblikovane web stranice.
- Treća je preporuka obradila nekoliko sigurnosnih nedostataka vezanih uz implementaciju HTML i DOM standarda te obradu slikovnih datoteka. Ovih se nekoliko ranjivosti može iskoristiti za izmjenu proizvoljnih memorijskih lokacija (eng. *memory corruption*).

4.2. Sigurnosne metode preglednika Mozilla Firefox

Mozilla Firefox koristi razne metode zaštite od sigurnosnih prijetnji kao što su:

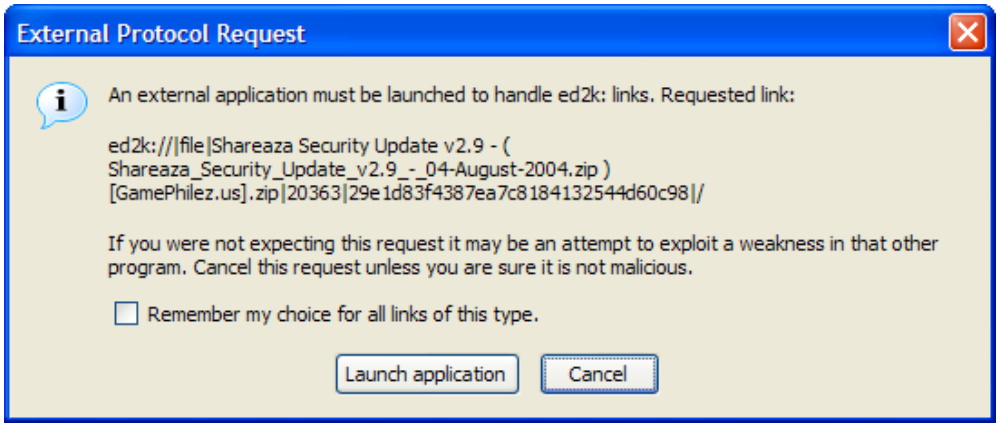
- Tzv. *sandbox* sigurnosni model, koji ograničava skripte u pristupu podacima s drugih web stranica, odnosno podacima iz drugih izvora. Najčešće se koristi za pokretanje nekih vanjskih programa, kojima se pruža samo ograničen set resursa i tako se omogućava njihovo sigurnije pokretanje.
- SSL/TLS (eng. *Secure Sockets Layer/Transport Layer Security*) zaštita sa snažnom enkripcijom u komunikaciji sa web poslužiteljima, pri čemu se koristi HTTPS protokol. SSL se, kao i većina modernih sigurnosnih protokola, temelji na kriptografiji. Kad je uspostavljena SSL sjednica, poslužitelj počinje komunikaciju objavom javnog ključa klijentu. Inicijalno se ne koristi nikakva enkripcija, tako da obje strane komunikacije (a i potencijalni prisluškivači) mogu pročitati taj ključ, ali nakon razmjene inicijalnih informacija, klijent može poslati poslužitelju informaciju na način da ju nitko drugi ne može dekodirati. Klijent generira 46 okteta slučajnih podataka, formira ih u jedan, vrlo velik broj, kriptira te podatke javnim ključem poslužitelja i šalje poslužitelju tako dobiven rezultat. Samo poslužitelj (uz pomoć svog privatnog ključa) može dekodirati primljenu informaciju i odrediti 46 okteta izvornih podataka. Takva se dijeljena tajna dalje koristi za generiranje skupine konvencionalnih RC4 šifri za enkripciju ostatka sjednice.
- Podrška za web aplikacije koje koriste pametne kartice za postupke autentikacije.

- Detektor *phishing* napada – Firefox preglednik svakodnevno nadograđuje svoju bazu podataka o lažiranim web stranicama i ako korisnik pokuša otvoriti lažiranu stranicu koja bi trebala biti sigurna (kao npr. stranica banke i sl.), preglednik zaustavlja taj pokušaj i ispisuje upozorenje korisniku.



Slika 13: Upozorenje o pristupu lažiranoj stranici

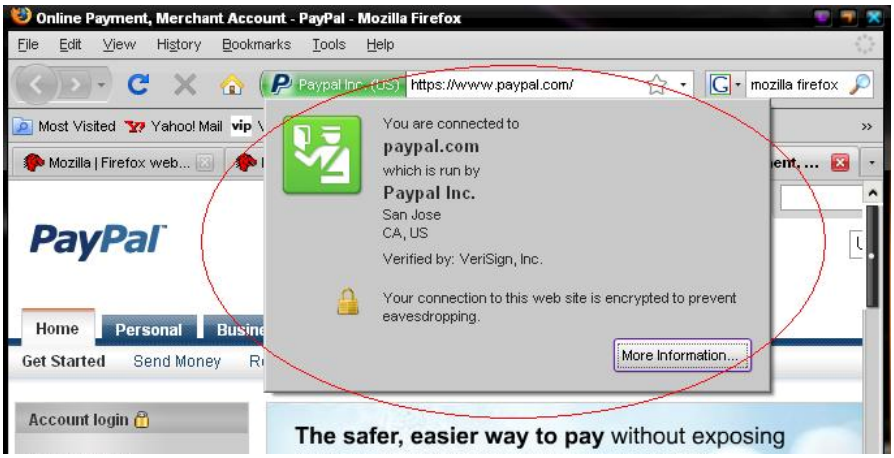
- Opcija za sigurno rukovanje korištenim eksternim protokolima – ako Firefox ne prepoznaje protokol koji se koristi u korisničkom zahtjevu, pregledava listu sigurnih protokola koji se koriste u slične svrhe; ako traženi protokol nije na listi, korisnik prima upozorenje nakon kojeg može ipak odabrati pokretanje eksterne aplikacije ili odustati od tog pokušaja. Ako korisnik ipak odluči pokrenuti eksternu aplikaciju korištenjem nesigurnog protokola, može se dogoditi situacija u kojoj se takav protokol iskorištava za zlouporabu neke sigurnosne ranjivosti operacijskog sustava Windows. Primjer upozorenja dan je na sljedećoj slici.



Slika 14: Upozorenje o korištenju eksternog protokola

- Mogućnost brisanja svih privatnih podataka i kolačića sa samo jednim klikom miša.

- Mogućnost provjere informacija o web stranici prije upisa ikakvih osobnih podataka – nudi se mogućnost provjere broja prethodnih posjeta stranici, spremljenih zaporki i sl. Opcija se koristi klikom na ikonu stranice (u adresnoj traci), pri čemu jedan klik ispisuje informacije o identitetu stranice, a drugi klik detaljnije informacije o prethodnim posjetima stranici i dr.



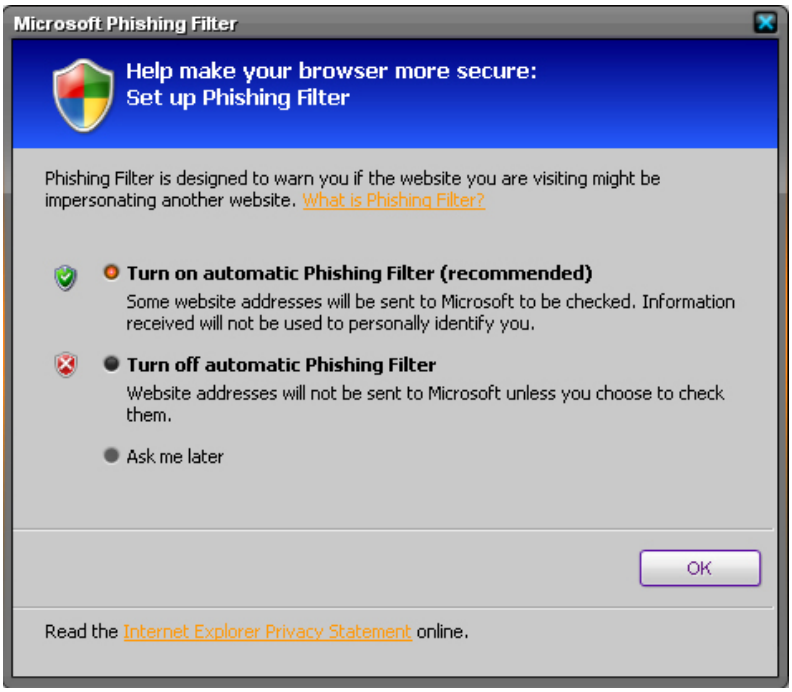
Slika 15: Provjera informacija o web stranici

- Integracija s antivirusnim programom – prilikom preuzimanja datoteke s Interneta, antivirusni program automatski provjerava da li se radi o nekom zlonamjernom programu, crvu i sl.

4.3. Sigurnosne metode preglednika Internet Explorer

Iako se Internet Explorer i dalje smatra jednim od nesigurnijih, ako ne i najnesigurnijim web preglednikom današnjice, inačica 7 ima implementirane nove, poboljšane metode zaštite od sigurnosnih napada. Neke od njih su sljedeće:

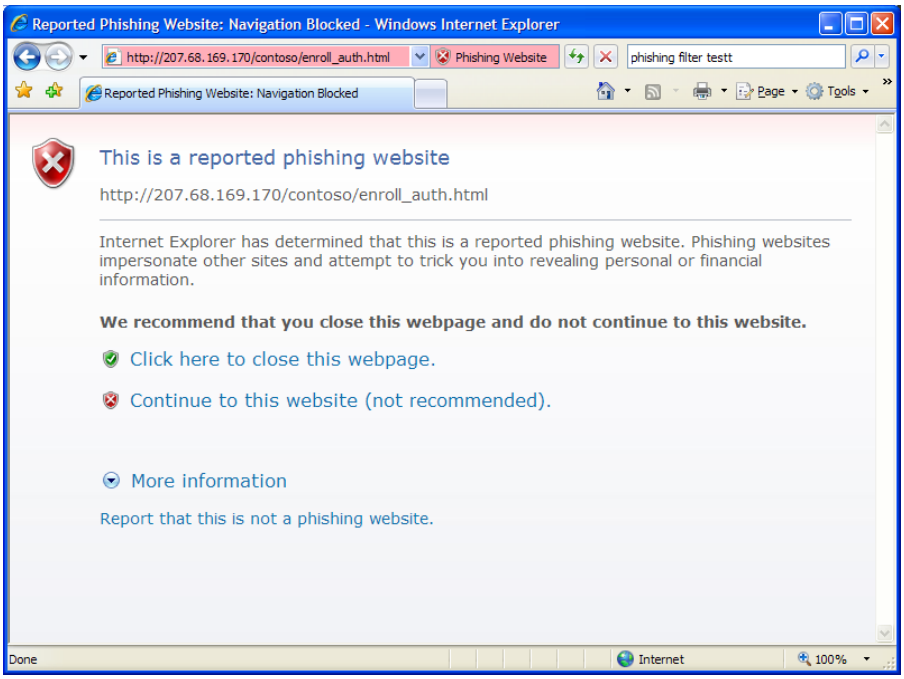
- Za Internet Explorer 7 namijenjen Windows Vista operacijskim sustavima postoje 2 načina obrane od sigurnosnih napada – kontrola korisničkih računa (eng. *User Account Control*) i rad u tzv. zaštićenom načinu (eng. *Protected-mode IE*). Kontrola korisničkih računa zahtijeva od korisnika potvrđivanje bilo kakve akcije koja bi mogla utjecati na stabilnost sigurnosti sustava. Provodi se čak i ako je korisnik prijavljen na sustav kao administrator. Iako zaštićeni način rada ne osigurava zaštitu od svih vrsta napada, značajno umanjuje mogućnost napada pisanjem, izmjenom ili uništavanjem podataka te instalacijom zlonamjerno oblikovanog koda na korisničkom računalu. Jedna od novosti kod Windows Vista sustava je svrstavanje procesa i drugih objekata u određene razine integriteta. Programi koji se spajaju na Internet (kao što su web preglednici) podložniji su sigurnosnim napadima jer preuzimaju nesiguran sadržaj iz neprovjerenih izvora. Iz tog se razloga Internet Explorer u zaštićenom načinu rada označava kao proces niske razine integriteta te mu se dodjeljuju manje ovlasti kako bi se smanjila mogućnost izmjena i napada putem istog.
- *Phishing* filter – omogućava korisnicima provjeru posjećenih stranica u potrazi za *phishing*, odnosno lažiranim stranicama, pri čemu se automatski mogu provjeravati sve stranice koje korisnik posjećuje ili je moguće provjeravati samo one stranice za koje postoji sumnja da su lažirane. Odabir jedne od spomenutih opcija vrši se u prozoru prikazanom sljedećom slikom.



Slika 16: Phishing filter

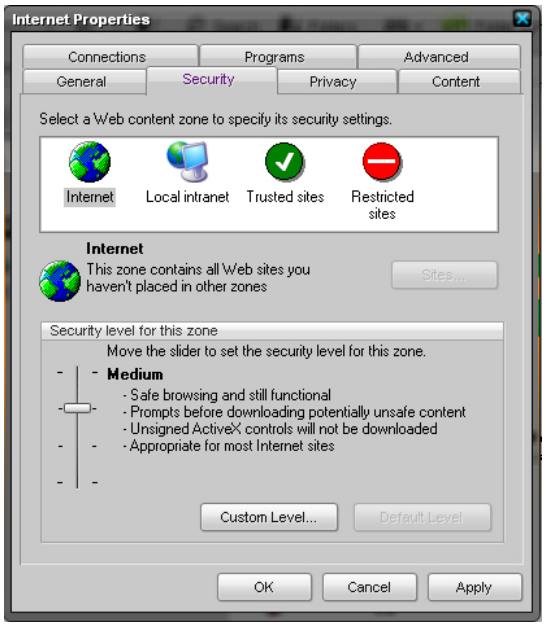
U slučaju otvaranja lažirane stranice, filter automatski detektira napad, miče preglednik s takve stranice i generira upozorenje za korisnika. Ako detektirana stranica nije na popisu lažiranih stranica na Microsoft poslužitelju, korisnik ima mogućnost prijavljivanja pronađene stranice. Filtar ne provjerava sve URL adrese na poslužitelju, već samo one koje se ne nalaze na popisu prihvatljivih adresa ili su iz nekog razloga sumnjive. Neki su korisnici kritizirali *phishing* filter tvrdeći da ga je lako prevariti. Jedan od načina na koji je to moguće izvesti je preusmjeravanjem stranice koja je na listi lažiranih na drugu stranicu (koja nije na listi). Sve dok i nova stranica ne bude blokirana, napad ostaje aktivan. To znači da napadači mogu i dalje koristiti iste poruke elektroničke pošte (kojima su prethodno navodili korisnike na otvaranje zlonamjerno

oblikovanih web stranica) jednostavnim premještanjem na novi poslužitelj. Problem kod ovog filtra je što na taj način korisnicima daje lažan osjećaj sigurnosti iako ga je moguće zaobići, što je neki put gore od nedostatka ikakve zaštite.



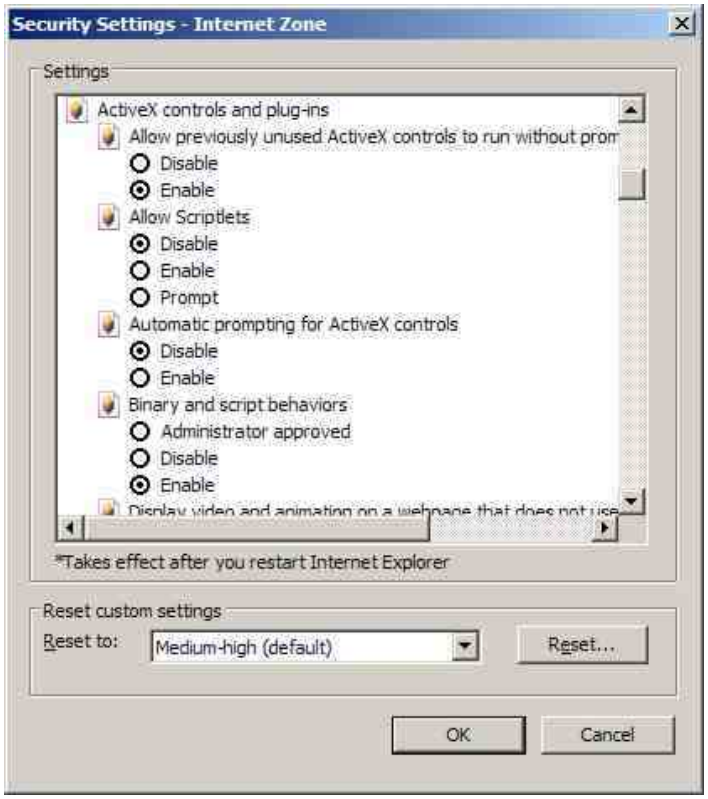
Slika 17: Phishing filter

- ActiveX kontrole koje nisu provjerene i označene sigurnima više se ne pokreću automatski, već su automatski onemogućene zahvaljujući novoj *ActiveX opt-in* opciji. Internet Explorer sve web-stranice smješta u jednu od četiri sigurnosne zone: Internet, lokalni intranet, sigurne stranice ili stranice s ograničenim pristupom. Sigurnosne postavke web stranice određene su zonom u kojoj se ona nalazi. Dodavanje web stranice u određenu zonu omogućuje nadzor nad razinom sigurnosti koja se na toj stranici koristi. Primjerice, ako korisnik posjeduje popis web stranica koje često posjećuje te im potpuno vjeruje, treba ih dodati u zonu sigurnih stranica. Na sljedećoj je slici prikazan prozor za izmjenu postavki sigurnosnih zona, do kojeg se dolazi sljedećim putem: *Start->Control Panel->Internet Options->Security*.



Slika 18: Sigurnosne zone

Opcija *ActiveX opt-in* je omogućena u Internet zoni i zoni ograničenih stranica, a automatski onemogućena u Intranetu i zoni sigurnih stranica, što se, naravno, može izmijeniti. Osim toga, pruža se i mogućnost ograničavanja pojedinih ActiveX kontrola, odnosno moguće je odrediti na kojim će se stranicama (eng. *site locking*) ili u kojim sigurnosnim zonama (eng. *zone locking*) kontrole pokretati.



Slika 19: Opcije za rukovanje ActiveX kontrolama

- Postoji i ugrađena funkcionalnost za sprečavanje tzv. *cross-domain* napada – kod inačice 7 skriptama je omogućeno pokretanje samo u originalnom sigurnosnom kontekstu, čak i ako su preusmjerene u drugu sigurnosnu domenu.
- Korisnici preglednika Internet Explorer 7 mogu lakše odrediti je li neka web stranica zaštićena SSL/TLS zaštitom i prikupiti informacije o digitalnim certifikatima koje stranica posjeduje. Ova se opcija naziva proširena validacija SSL certifikata (eng. *Extended Validation SSL Certificates*) i do nje se dolazi klikom na ikonu s desne strane adresne trake (žuti lokot). Navigacijom na stranice zabilježene kao sigurne adresna traka boji se u zeleno.

Slika 20: EV SSL certifikati

- Dodana su i 3 nova zapisnička ključa, tzv. *Feature Control Keys*, čija je zadaća da spriječe HTML od prikupljanja korisničkih osobnih podataka. Isto tako, omogućeno je i jednostavno brisanje svih informacija o posjećenim web stranicama, privremenim datotekama, zaporkama, privremenoj memoriji i sl.

Slika 21: Brisanje osjetlijviih informacija

- Internet Explorer 7 podržava internacionalne znakove, ali kako bi se spriječili napadi zamjenom znakova sličnim znakovima, preglednik upozorava korisnika kako se na određenoj stranici radi o stranom jeziku.

5. Zaključak

Sigurnosni su napadi postali svakodnevica. Provode se na razne načine i uzrokuju brojne probleme u radu računalnih sustava. Jedna od češćih meta napadača su web preglednici – ranjivi na tzv. *phishing* napade (napade korištenjem lažiranih poruka elektroničke pošte i lažiranih web stranica financijskih organizacija za navođenje korisnika na otkrivanje osjetljivih osobnih podataka), napade pokretanjem proizvoljnog programskog koda (do kojih dolazi radi nedostataka u radu JavaScript komponente, zlonamjerno oblikovanih ActiveX kontrola i dr.) ili rušenjem preglednika, što je oblik napada uskraćivanja usluga (eng. *Denial of Service*) i sl.

U ovom su dokumentu uspoređene karakteristike dva najpoznatija web preglednika – Internet Explorer i Mozilla Firefox, točnije inačica Internet Explorer 7 i Mozilla Firefox 3. Svaki od preglednika posjeduje prednosti i mane, a međusobno se razlikuju u mnogim karakteristikama - omogućuju različitu količinu opcija, razlikuju se u jednostavnosti korištenja, dizajnu i sl. Ono što je posebno bitno jest da se razlikuju i u sigurnosti, odnosno načinu na koji je implementirana zaštita od sigurnosnih napada i uspješnosti tih implementacija.

Istraživanja pokazuju kako je Internet Explorer, iako inačica 7 sadrži znatna poboljšanja na području sigurnosti, ipak dosta nesigurniji za korištenje od preglednika Mozilla Firefox. Tome u prilog ide odnos broja objavljenih sigurnosnih propusta u pojedinom pregledniku, brzina kojom su ti propusti ispravljeni, prolaznost na obavljenim sigurnosnim testiranjima i dr.

Ipak, Internet Explorer je i dalje jedan od najpopularnijih i najčešće korištenih web preglednika pa je izričito važno podići svijest korisnika o sigurnosnim problemima na koje mogu naići i metodama kojima se mogu zaštititi od istih.

6. Reference

[1] Extended Validation SSLCertificates, http://www.microsoft.com/windows/products/winfamily/ie/ev/default.mspx, srpanj 2008.

[2] Internet Explorer 7, http://en.wikipedia.org/wiki/Internet_Explorer_7, srpanj 2008.

[3] Mozilla beefs up security with Firefox 3, http://www.securityfocus.com/brief/631, srpanj 2008.

[4] Phishing filter in IE7, http://blogs.msdn.com/ie/archive/2005/09/09/463204.aspx, srpanj 2008.

[5] 10 things you should know about Internet Explorer 7 security, http://articles.techrepublic.com.com/5100-10878_11-6130844.html, srpanj 2008.

[6] Internet Explorer 6, http://en.wikipedia.org/wiki/Internet_Explorer_6, srpanj 2008.

[7] Windows Internet Explorer, http://www.microsoft.com/windows/products/winfamily/ie/default.mspx, srpanj 2008.

[8] ActiveX, http://en.wikipedia.org/wiki/ActiveX_control, srpanj 2008.

[9] Phishing, http://en.wikipedia.org/wiki/Phishing, srpanj 2008.

[10] Firefox 3 Beta Release Notes, http://www.mozilla.com/en-US/firefox/3.0b1/releasenotes/, srpanj 2008.

[11] Check out IE 7's security features, http://articles.techrepublic.com.com/5100-10878_11-6078324.html?tag=rbxccnbtr1, srpanj 2008.

[12] Get the details on Internet Explorer 7's security improvements, http://articles.techrepublic.com.com/5100-10878_11-6128517.html?tag=rbxccnbtr1, srpanj 2008.

[13] Mozilla Firefox, http://en.wikipedia.org/wiki/Mozilla_Firefox, srpanj 2008.

[14] Firefox 3, http://wiki.mozilla.org/Firefox3, srpanj 2008.

[15] Comparison of web browsers, http://en.wikipedia.org/wiki/Comparison_of_web_browsers, srpanj 2008.

[16] Features of Mozilla Firefox, http://en.wikipedia.org/wiki/Features_of_Mozilla_Firefox, srpanj 2008.

[17] Firefox Features, http://www.mozilla.com/en-US/firefox/features/, srpanj 2008.

[18] Web browser security summary, http://www.webdevout.net/browser-security, srpanj 2008.