

Test browserů

Surfujete **PO INTERNETU BEZPEČNĚ**? Chip vám ukáže, jak hackeři a zloději dat zneužívají bezpečnostní problémy browserů a také jak se v tomto případě bránit...

CLAUDIO MÜLLER

Používáte starý prohlížeč bez záplat? Pak to u vás mají hackeři snadné: k vašim soukromým datům se mohou dostat stejně snadno jako do domu s otevřenými okny a dveřmi. Je překvapivé, že většina uživatelů stále používá Internet Explorer 7, a nezanedbatelné procento uživatelů dokonce i jeho předchůdce s číslem 6. Tyto prohlížeče jsou totiž ve srovnání s konkurencí pomalejší, méně vybavené a především zranitelnější. Přitom alternativ je k dispozici více než dost: Firefox, Opera, stále více příznivců nachází v poslední době i Safari od Applu, a dokonce i novinka od Googlu – Chrome – vypadá nadějně.

V současné době, kdy hackeři pracují jako profesionálové a honbu za daty provádějí skutečně ve velkém, už není volba prohlížeče jen otázkou toho, zda „se mi líbí“. Především pokud je počítač vašim „pracovním nástrojem“, nebo z něj dokonce ovládáte svůj bankovní účet, měla by být volba prohlížeče důležitým rozhodnutím. My vám ukážeme, jak jednotlivé browsery ob stojí v přímém srovnání nejen z hlediska funkcí, ale především z hlediska bezpečnosti.

Riziko při surfování

V našich článcích na téma bezpečnosti doporučujeme těm nejnáročnějším uživatelům použití bezpečnostního balíku, který dokáže počítač komplexně zabezpečit – od portů až po e-mailovou schránku. Pravda ale je, že ani nejlepší bezpečnostní software nedokáže zabránit zneužití zranitelností v prohlížeči. Nejnebezpečnější hrozba se skrývá pod zkratkou XSS (cross-site scripting). Ten totiž zahrnuje celou řadu možností, jak v prohlížeči spustit nebezpečný kód. Obrázek vpravo ukazuje, jak mohou hackeři využít tento typ útoku k získání vašich soukromých dat.

První typ útoku infiltrovat škodlivý skript do dynamicky generovaných odkazů, které jsou podobné výsledkům z vyhledávačů. Pokud uživatel na takto „upravený“ link klikne, kód se spustí a z počítače uživatele ukradne vybranou „session“ cookie. Její pomocí může hacker zís-

SHRNUTÍ

Petr Kratochvíl, redaktor Chipu



Vybírejte pečlivě

Klasické útoky na počítač jsou dávno minulostí. Nyní jsou dvě třetiny útoků namířeny přímo proti webovým aplikacím. Jejich hlavním a nejdůležitějším cílem je pochopitelně brána k webu – internetový prohlížeč. A právě z tohoto důvodu je úroveň bezpečnosti browseru jedním z nejdůležitějších faktorů pro bezpečný počítač. Je neuvěřitelné, že i přes trístní výsledky ve většině testů je Internet Explorer (verze 6, 7 i 8) stále dominantním prohlížečem. Argumenty ve stylu „Stejně si prohlížím jen stále stejné weby“ jsou ve světle nových triků hackerů jen naivní představou. Ano, tisíce uživatelů opravdu surfují s IE bez větších problémů – je však jen otázkou času, kdy se objeví první útok na jejich data...

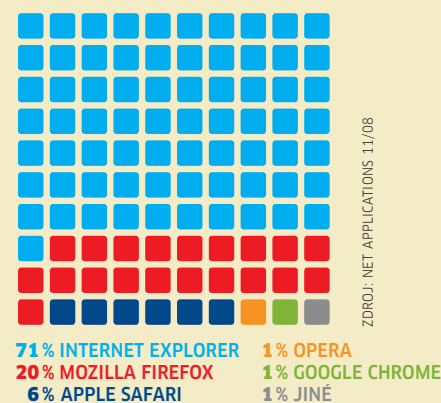
Upozornění: Ačkoliv jsou v testu zařazeny dvě beta verze, rozhodně nedoporučujeme jejich nasazení „v běžném provozu“.

kat plný přístup k vybranému účtu, dokud je uživatel přihlášen. Nejhorší je to, že celá stránka (do které byl infiltrován link) je originální – pochopitelně kromě infikované URL. I z tohoto důvodu patří tento typ útoku mezi nečastější se opakující. Druhý typ útoku je charakteristický uložením škodlivého kódu přímo na serveru, a to také na delší dobu. V praxi jde o případ, kdy hacker umístí škodlivý kód například do diskuze nebo do návštěvní knihy serveru. Každý uživatel, který si tuto položku přečte, spustí kód v prohlížeči. Stejně jako v prvním případě i tento typ útoku je možný jen u serverů s bezpečnostními mezerami.

Nicméně zločinci se nyní zaměřují také na hledání zranitelností v doplňcích prohlížečů – například ActiveX, Flash nebo QuickTime, které jsou nutné pro zobrazení dynamických prvků nebo přehrání multimediálních formátů. A právě pomocí mezer v těchto doplňcích se hackeři pokouší získat přístup do systému. Největší procento útoků je zaměřeno na ActiveX komponenty, které jsou podporovány pouze

ROZŠÍŘENÍ BROWSERŮ

Před šesti roky používalo více než 90 procent uživatelů Internet Explorer. Nyní má již více než třetina uživatelů nainstalován alternativní produkt. Z hlediska statistik je nutné ještě podotknout, že údaje o podílu jednotlivých prohlížečů jsou ovlivněny jak geograficky (např. v Evropě nebo i v ČR je podíl Firefoxu větší), tak i odborně (na IT serverech je podíl alternativních prohlížečů mnohem větší).



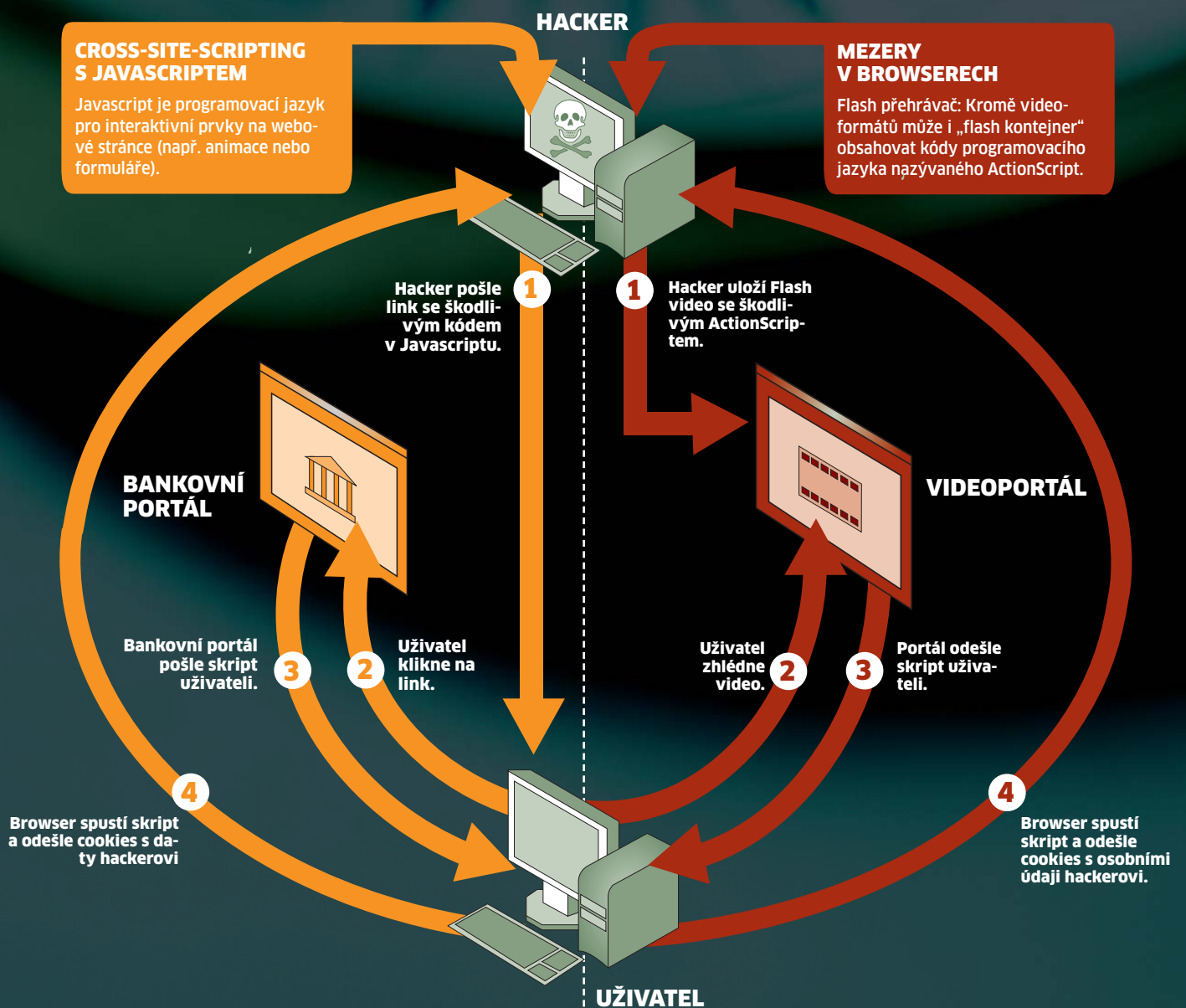
v IE. Tyto komponenty jsou oblíbeným cílem i proto, že mají velmi často přidělenou celou řadu přístupových práv, které hackerovi průnik do systému usnadňují. Jiné komponenty (jako například Java applety) často běží odděleně v tzv. sandboxu, spolupracují s prohlížečem a k samotnému systému obvykle přístup nemají. Všechny prohlížeče umožňují kompletní vypnutí všech zmiňovaných komponent, dokonce ani instalace QuickTime rozšíření nebo Flashe není nutností. Tak proč riskovat?

Aktivní obsah: Bez něj je to těžké

Pokud se rozhodnete vypnout zobrazování „aktivního obsahu“, brzy zjistíte, že se vám správně zobrazí jen zlomek webů. Statické HTML stránky obsahující jen text a obrázky jsou už dávno minulostí. Všechny dynamické prvky – například animace, otevírající se nabídky, prezentace – se v prohlížeči zobrazují jen pomocí „aktivního obsahu“. Tyto prvky jsou naprogramovány v různých (i kriptovacích) jazycích. Nejčastější bývá použití Javy nebo Javascriptu, a proto ni-



Dva způsoby, jakými vám hackeři mohou ukrást vaše data



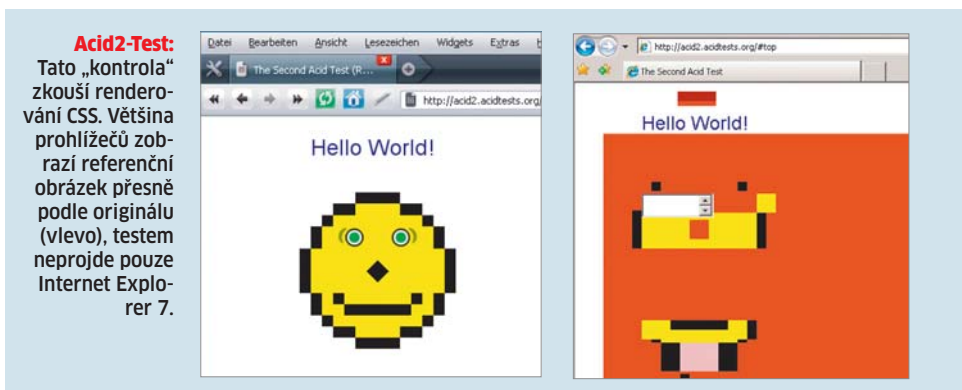
koho nepřekvapí, že všechny prohlížeče v testu podporují oba zmiňované jazyky. Důležité: Zatímco Javascriptu prohlížeč „rozumí“ bez problémů, Java musí být spuštěna ve specifickém prostředí a výsledky pro prohlížeč „přeloženy“. Toto prostředí bývá do prohlížeče obvykle integrováno jako plug-in.

Ve srovnání se statickými weby mají ty dynamické výhodu v nabídce více funkcí a lepšího pohodlí. Nevýhoda: Nezávisle na zmiňovaném bezpečnostním riziku mají dynamické weby většinou ještě jednu nevýhodu, a to mnohem větší velikost. Pokud jsou navíc přidány komplikované kaskádové styly (CSS), které nabízejí další možnosti vizuální „konfigurace“ stránky, může být nahrávání stránky opravdu dlouhé...

Pravda je, že poměrně často bývají nejslabším článkem řetězu „renderovací“ jádra v prohlížečích. Ta se starají o správné zobrazování jednotlivých standardů (HTML, XML a také zmiňovaných CSS) a hrají hlavní roli v závodu v rychlosti zobrazení webu. My jsme otestovali, který z prohlížečů je nejen bezpečný a pohodlný, ale také rychlý.

Šest prohlížečů pod mikroskopem: Bezpečnost především

K nejdůležitějším kritériím z hlediska bezpečnosti patří i ochrana soukromí. Browsersy si obvykle do cache ukládají přihlašovací údaje, položky formulářů a historii surfování, kde mohou být tyto informace snadnou kořistí hackerů a zlodějů dat. Tomu se lze bránit používáním speciálního surfovacího modu. V něm se do cache browseru neukládají žádná data a surfování lze považovat za částečně anonymní (úplně anonymity lze dosáhnout „skrytím“ IP adresy například pomocí proxy serveru). Tento „anonymní mod“ nabízí už dlouhou dobu browser Safari od Applu, teprve nedávno se pak k němu připojily i browsersy Internet Explorer 8 a Chrome (v beta verzích). V Opeře tato funkce schází a ve Firefoxu se s anonymním surfova-



cím modem počítá až ve verzi 3.1 – pro verzi 3 je k dispozici „jen“ rozšíření. Pro pořádek je ale nutné podotknout, že jak Opera, tak Firefox nabízejí velmi dobrý „management“ cookies a celou řadu možností, jak při surfování kontrolovat soukromá data.

V současné době patří antiphishingový filtr k základní výbavě prohlížeče, v jeho kvalitě jsou ale stále velké rozdíly. Například Firefox, Opera a Safari rozpoznají přibližně 80 procent phishingových webů uvedených na webu www.phishtank.com. Ve srovnání s nimi je na tom se svými 40 procenty Internet Explorer 8 velmi špatně a překvapivě je, že si vede dokonce i hůře než jeho předchůdce s číslem 7. Na druhou stranu, Internet Explorer 8 je jediným prohlížečem v testu, který nabízí integrovanou XSS ochranu. Ta by měla uživatele chránit před škodlivým kódem na webových stránkách a zabránit jiným typům špehování. Ve Firefoxu sice tato funkce integrována není, k dispozici je ale rozšíření, které vám tuto ochranu nabídne (rozšíření najdete i na našem DVD).

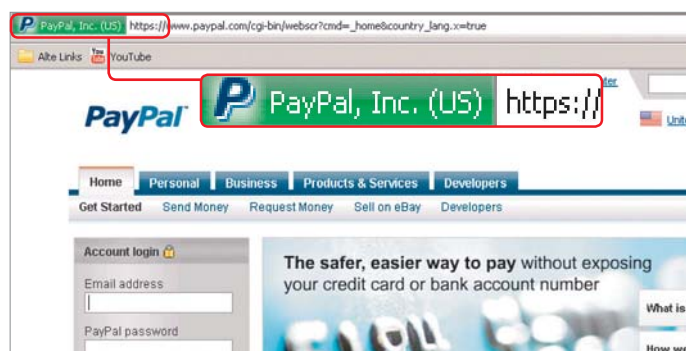
Smutným faktem tedy je, že jeden z nejpoužívanějších prohlížečů, Internet Explorer 7, nenabízí ani XSS ochranu, ani anonymní mod a výkon jeho antiphishingového filtru je podprůměrný. Navíc podle bezpečnostních expertů ze serveru Secunia také obsahuje nejvíce bez-

pečnostních mezer, z nichž nemalá část stále ještě není opravena. To je další důvod, proč se IE7 zdaleka vyhnout. Navíc ve výkonnostních testech za zbytkem „závodního pelotonu“ žalostně zaostával – a to jak v „SunSpider“ testu, tak i při testování CSS.

Rychlost: Rychlé počítače a staré stroje

Pomocí „SunSpider“ testu jsme zkoumali výkon javascriptového enginu – což by mělo leccos naznačit o rychlosti prohlížeče při zpracování komplikovanějších webových stránek. Tento „benchmark“, který se skládá z 26 samostatných „minitestů“, můžete vyzkoušet i sami ve svém prohlížeči (najdete ho na adrese www2.webkit.org/perf/sunspider-0.9/sunspider.html). Stačí jen v dolní části stránky kliknout na »Start Now!«, a za pár minut poznáte, jak si ve srovnání stojí váš prohlížeč. Další test, test CSS, zjišťuje rychlost, jakou dokáže prohlížeč pracovat s kaskádovými styly – ukazuje rychlost zpracování stránky s graficky náročnými styly. I výsledek tohoto testu byl pro nás překvapením, protože i zde Internet Explorer 8 výrazně zaostal za ostatními. Na opačném konci výsledkové listiny příjemně překvapil prohlížeč Chrome, který se po boku Safari dostal na absolutní vrchol výkonnostních testů. Oba zmiňované

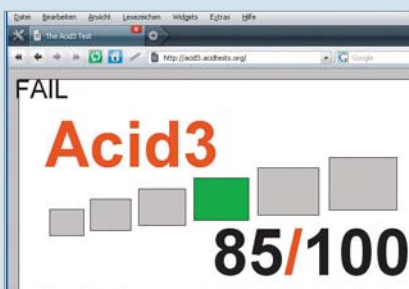
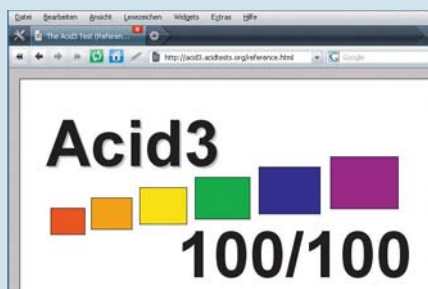
Phishing: Takto hackeři vytváří chytré napodobeniny internetových stránek.



Originál: Všimněte si rozpoznání pravosti stránky pomocí autentizační funkce v adresním řádku (zelené pole) a zabezpečeného (https) připojení.



Kopie: Záhadné URL odhaluje napodobeninu webu. Díky zkopírování grafických prvků je jinak vzhled webu více než přesvědčivý...



Acid3-Test: Tento test zkouší, jak se prohlížeč dokáže vypořádat s dynamickými prvky specifikace Web 2.0. Podrobnější informace včetně samotného testu najdete na adrese www.webstandards.org/action/acid3/.

prohlížeče totiž porazily ostatní „závodníky“ rozdílem několika tříd.

Pohodlí: Příjemné surfování

Bývá obvyklé, že nejrychlejší sportovní vozy nejsou zrovna ideální pro delší pohodlné cestování. Podobně lze i testovací verzi prohlížeče Chrome označit spíše za rychlý a spolehlivý nástroj pro internetové puristy. Běžný uživatel zde bude postrádat pohodlnou správu záložek, náhledy webů nebo ukládání skupin odkazů. Nepříjemné také je, že v prohlížeči chybí funkce pro individuální nastavení (povolení) aktivních prvků. To lze provést pouze na úrovni jednotlivých webů. V Opeře a Firefoxu je tento „problém“ vyřešen mnohem lépe. I z celkového pohledu na komfort surfování jsou na tom oba zmiňované browsery mnohem lépe než Google Chrome. Září především Opera, která má již v základní verzi

působivou nabídku funkcí. Jinou cestou jde Firefox, který toho sice „v základu“ tolik neumí, ale pomocí více než pěti tisíc rozšíření ho lze označit za nejpřizpůsobivější prohlížeč.

Příjemné zlepšení jsme zaznamenali u Internet Exploreru 8, který na rozdíl od svého předchůdce nabízí správce rozšíření, obnovu záložek nebo ochranu proti pádu – podobně jako v browseru Chrome zde tvoří každý ja-nel separátní proces.

Ačkoliv byl Google Chrome v testu nejrychlejší, teprve až finální verze nabídne skutečně praktické a pohodlné surfování. Na Internet Exploreru 8 je vidět, že se snaží držet krok s konkurencí, ale ne vždy se mu to daří. Teprve dvojice našich vítězů přesně splňuje naše požadavky na ideální prohlížeč – bezpečně a rychle surfování jako základ a rozsáhlou nabídku funkcí jako bonus... **AUTOR@CHIP.CZ**

NA DVD

BROWSERY A INTERNETOVÉ NÁSTROJE

- Mozilla Firefox** ► jeden ze dvou nejlepších prohlížečů
- Opera** ► bezpečný browser pro náročné uživatele
- Adblock Plus** ► nástroj na blokování reklamy
- All in-One Sidebar** ► komfortní lišta s praktickými funkcemi
- CustomizeGoogle** ► optimalizuje vyhledávání Googlu
- DownThemAll** ► nástroj na stahování
- FlashBlock** ► blokuje spouštění Flashe
- IE7Pro** ► rozšíření pro Internet Explorer
- NoScript** ► rozšíření pro blokování Javascriptu
- noXSS** ► doplněk chránící před útokem typu XSS
- Speed Dial** ► rychlý přístup k oblíbeným webům
- VDownloader** ► nástroj na stahování multimédií
- WinHTTrack** ► ukládání kompletních webových stránek
- WOT (Web of Trust)** ► rozpoznává nebezpečné stránky
- Bezpečný browser** ► přenosná verze prohlížeče Firefox, doplněná o rozšíření a nabízející bezpečně a rychle surfování; ideální pro použití na cizích počítačích nebo v internetových kavárnách

NA DVD: Programy k tomuto článku najdete na DVD pod indexem **BROWSERY**.

Bezpečnost internetových prohlížečů: Vítězové a poražení

	1. MÍSTO	1. MÍSTO	3. MÍSTO	4. MÍSTO	5. MÍSTO	6. MÍSTO
Program	Firefox 3.0	Opera 9.6	Safari 3.2	Chrome 0.3 (Beta)	Internet Explorer 8 Beta 2	Internet Explorer 7
Výrobce	Mozilla Foundation	Opera Software	Apple	Google	Microsoft	Microsoft
Internet	www.mozilla-europe.org	www.opera.com	www.apple.com	www.google.com	www.microsoft.com	www.microsoft.com
Celkové hodnocení	86 	86 	77 	69 	65 	42
Mezery v zabezpečení (celkem/neuzavřené)*	28/1	41/0	26/2	11/0	0/0	67/9
Rozpoznané phishingové weby (přibližně)*	80 %	80 %	80 %	70 %	40 %	60 %
Soukromý mod	-	-				-
Možnost blokování aktivních prvků*	rozsáhlá	velmi rozsáhlá	malá	žádná	rozsáhlá	rozsáhlá
Detekce XSS	typ 0 a 1**	-	-	-	typ 1	-
SunSpider test - Javascript (sekund)	2,8 s	3,4 s	3,3 s	1,3 s	7,6 s	26,7 s
CSS test (milisekund)	185 ms	115 ms	26 ms	33 ms	448 ms	342 ms
Zabraná RAM (5 oken)	94 MB	94 MB	104 MB	113 MB	127 MB	126 MB
DNS Prefetching	-	-	-		-	-
Test ACID2	prošel	prošel	prošel	prošel	prošel	neprošel
Test ACID3 (max. 100)	71	85	75	78	21	12
Možnost rozšíření	vynikající	dobrá	sotva možná	nelze	dobrá	dobrá
Správa záložek	velmi rozsáhlé možnosti	velmi rozsáhlé možnosti	rozsáhlé možnosti	malé možnosti	velké možnosti	jen částečná

* k 17.11. 2008 (zdroj: www.secunia.com, www.securityfocus.com)

** pomocí doplňku <https://addons.mozilla.org/cs/firefox/addon/9517>

Špičková třída (100-90) Vyšší třída (89-75)
 Střední třída (74-45) Než doporučit (44-0)
 Všechna hodnocení v bodech (max. 100)

ano
 ne