Sveučilište u Splitu-Sveučilišni odjel za stručne studije

Sigurnost računala i podataka

**ZAŠTITA WEB PREGLEDNIKA**

Autor: Filip Bikić

Split,Studeni,2018.godina

**SADRŽAJ:**

*1.Što je web preglednik?*

*2.Povijest web preglednika*

*3.Mračne strane web preglednika*

*4.Kako se zaštititi?*

*5.Usporedba web preglednika*

*6.Tips and tricks*

*7.Zaključak*

*8.Literatura*

**1.Što je web preglednik?**

**Web preglednik** je program koji korisniku omogućuje pregled web-stranica i multimedijalnih sadržaja vezanih uz njih.

Svaki web preglednik je **interpreter**. Dakle, stranica je pisana u kodu koji web preglednik nakon toga interpretira kao nešto svakome razumljivo.

Web preglednici rade na taj način što sa web stranica učitavaju HTML (Hypertext Markup Language) dokumente, a nakon toga prikazuju isti na izlaznom uređaju - monitoru.

Internetske preglednike opisuju sljedeće osobine: brzina, sigurnost, dokumentacija za podršku i pomoć, mogućnosti i jednostavnost korištenja.

Svi glavni web preglednici omogućavaju korisniku da otvori više informacijskih resursa u isto vrijeme ili u različitim prozorima preglednika ili u različitim karticama u istom prozoru. Glavni preglednici uključuju blokere skočnih prozora za sprječavanje neželjenog iskakanja prozora, bez pristanka korisnika.

Većina preglednika podržava HTTPS i nude brz i jednostavan način za brisanje web cache, povijest preuzimanja, formu i traženje povijesti, kolaćiće i povijest pregledavanja.

Web preglednici sastoje se od korisničkog interfacea, rasporeda motora , renderirajućih motora, JavaScript prevoditelja, UI backenda, umrežavajućih komponenti i podataka komponente upornosti. Ove komponente ostvaruju različite funkcije web preglednika i zajedno pružaju sve mogućnosti web preglednika.

Novije generacije web preglednika podržavaju HTML5 standard.

Neki od internetskih preglednika koji se danas koriste su:

* Safari
* Google chrome
* Microsoft edge
* Mozilla firefox
* Opera

**2.Povijest web preglednika**

HTML kao meta-jezik kojim se hipertekstualni dokumenti mogu opisivati je izmislio Tim Berners-Lee (djelatnik CERN-a) 1990/1991. godine.

Prvi preglednici su bili strogo tekstualni, a veliku promjenu je 1993.godine donio *NCSA Mosaic* - koji je izvorno bio UNIX aplikacija ali je ubrzo prenijet i na druge operativne sustave.

1994. godine je Marc Andreesen (voditelj projekta *NCSA Mosaic*) pokrenuo vlastitu tvrtku - *Netscape* i izdao *Netscape Navigator*.

Ubrzo nakon toga je i Microsoft izbacio *Internet explorer* (*IE*) - čime je započet *rat preglednika*.

Zahvaljujući činjenici što je IE dolazio predinstaliran s *Windowsima* Microsoft je uspio postići da se danas koristi u više od 80% računala.

Netscape je odgovorio tako što je izvorni kod Netscape-a pretvorio u otvoreni kod (tj. *open source*), no to nije uspjelo zaustaviti opadanje zastupljenosti tog preglednika. Ipak, iz tog poteza se razvio internetski preglednik kojeg danas većina stručnjaka drži kao najboljeg i najsigurnijeg - *Mozilla* i njegovih izvedenica kao što je Firefox.

Od tekstualnih preglednika još uvijek se, iako u vrlo malom postotku, koriste *Lynx* i *Links*.

Na Linuxu je popularan još i Konqueror, a na Macintosh OS X se često koristi Safari.

**3.Mračne strane web preglednika:**

Web preglednici kao svaki drugi programi imaju svoje **sigurnosne rupe,** koje određeni individualci, kao i firme koriste za nanošenje štete korisnicima u svoju korist.

Neki od najčešćih kriminalnih aktivnosti na webu su :

-Krađa identiteta

-Krađa podataka

-Narušavanje privatnosti

-Prosljeđivanje virusa

Većina ovih veoma zlonamjernih aktivnosti se dešava svakodnevno na webu i potrebno je biti oprezan kako i mi ne bih postali žrtva „cybercrime-a“.

Večina ovih aktivnosti se provodi koristeći dijelove JS ili php koda koji su u mogučnosti prikupljati naše osobne podatke, kao i naše bankovne podatke za daljnju zloupotrebu.

Pop-up reklame, web bugovi, Clickjacking, HTTP cookies, zombie cookies, phishing su samo dio naše internet svakodnevice koji pokušavaju probiti našu sigurnosti i remetiti našu privatnost.

HTTP cookies omogučuju pohranu naših podataka prilikom ispunanja formi, što omogučuje lak pristup našim podatcima.

Web bugovi služe za pračenje naših internet aktivnosti s čim narušavaju našu privatnost.

Pop-up reklame,Phishing i cklickjacking su samo jedni od načina zavaravanja korisnika u autentičnost stranice dok se izad toga nalazi neautorizirana osoba koja samo čeka da mu pružimo svoje osobne podatke za daljnju zloupotebu.

**4.Kako se zaštititi?**

Zaštita web preglednika je ograničena.

Nemoguće je uspostaviti regulaciju cijelog internet sadržaja i nemoguće je napisati neprobojni softver.

Iz gore navedenih razloga najbolja zaštita je sam korisnik koji u svakom trenutku mora biti svjestan opasnosti i predvidjeti neželjeni sadržaj.

Naravno da developeri web preglednika nisu prepustili sav posao nama, razvijene su razne kvalitetne metode zaštite koje odrađuju svoj posao dobro,a neke od nih su:

-HTTPS Protokol

-Sandbox model

-VPN

HyperText Transfer Protocol Secure (**HTTPS**) je internetski protokol nastao kombinacijom protokola **HTTP** s protokolom **SSL/TLS**.

Ovaj protokol omogućava kriptiranu komunikaciju i sigurnu identifikaciju web poslužitelja mreže. HTTPS veze često se koriste za novčane transakcije na World Wide Webu i ostale povjerljive transakcije u korporativnim informacijskim sustavima.

Sandbox model je uveden od strane Google chrome-a, a danas ga koriste svi web preglednici.

Ideja je da je lokalni kod siguran i ima pristup svim lokalnim datotekama i podatcima, dok vanjski kod (kod skinut s interneta prilikom učitavanja stranice) se smatra nesigurnim i njemu se odvaja posebni prostor u memoriji za izvedbu, s tim da mu je onemogučen pristup važnim resursima kao što je naprimjer File system.

**VPN** je ime za računalnu mrežu koja spaja daleke mreže koristeći javne komunikacijske mreže kao što je internet.

VPN daje upraviteljima mreža i krajnjim korisnicima sigurnost od prisluškivanja i upadanja drugih korisnika (namjerno ili nehotično) kroz korištenje tehnoloških rješenja kao što su tunelski protokoli i šifriranje.

VPN se koristi i za spajanje različitih mreža, poput dvije IPv6 mreže preko spojne IPv4 mreže.

**5.Usporedba web preglednika**

Danas je najpopularniji Google chrome preglednik koji drži čak ~54% tržišta (54% ljudi koji koriste web preglednike koriste Google chrome).

Najveća konkurencija Chromu su Mozila Firefox,Opera,Safari,Microsoft Edge.

To što je Google Chrome najkorišteniji ne znači da je najbolji.

Svi web preglednici su danas više-manje slični ali postoje manje različitosti.

Svi preglednici od gore navedenih imaju redovite update-ove i svi koriste safe browsing, kojeg je razvio google,a služi za blokiranje nesigurnih web stranica i sadržaja prilikom skidanja (downloadanja).

Google chrome je prvi razvio Sandbox model i iako ga danas svi preglednici koriste Google Chrome ima najbolju implementaciju Sandbox modela iz tog razloga Google Chrome glasi za najsigurniji preglednik po pitanju sigurnusti, ali isto tako glasi i sa „najkontorverzniji“ preglednik po pitanju privatnosti. Google Chrome je closed-source s toga javnost nema uvid u njegovo implementaciju.

Microsoft Edge ima lošiji Sandbox model od samog Google Chrome-a, ali zato ima bolju zaštitu privatnosti, zbog upotrebe „Tracking protection“. Tracking protection onemogučava rad dijelovima koda koji su zaslužni za promatranje naših internet aktivnosti, što ubrzava web preglednik i donekle daje na zaštiti privatnosti. Microsoft Edge je također closed-soruce.

Mozilla Firefox glasi za najbolji web preglednik iako nije najkorišteniji, zaštita sigurnosti je na razini Google chromea, a zaštita privatnosti je bolja od svih browsera, zbog korištenja Tracking protection-a (Firefox je prvi uveo Tracking protection), ali još više zbog toga što je open-source, stoga javnost ima uvid u kod u svakom momentu.

**6.Tricks and tips**

Svi web preglednici podržavaju razne ekstenzije i vamo čemo navesti neke koje glase za najbolje trenutno na tržištu:

-LastPass

-Disconnect

-ScriptSafe

-Ghostery

-HTTPS everywhere

-Adblock plus

LastPass je softver koji nam omogučuje pohranu lozinki. Ukoliko ne želimo koristiti iste lozinke iznova,a nemamo praktičan način za zapamtiti svakiu lozinku svakog accounta LastPass je najbolja opcija. On osim što simulira neprobojni trezor za sve naše lozinka, daje i mogučnost generiranja „Teško probojnih“ lozinki uz pomoć naprednog algoritma. Također pruža opciju slanja lozinki i osjetljivih podataka sigurnim kanalima.

Disconnect je jedna od najpopularnijih sigurnostih aplikacija na tržištu. Aplikacija je tolko uspješna da ju je sam Googla makao s Google play-a više puta. Osnovne funkcionalnosti, kao mogučnost skeniranja web preglednika,safe browsing,brisanje kolačića,itd.. su omugučene u besplatnoj verziji aplikacije, dok premium verzija ima i upotrebu VPN-a, tracking protection, maskiranje lokacije,bolja konekcija, itd...

ScriptSafe je ekstenzija koja blokira sve <SCRIPT>, <OBJECT>, <EMBED>, <IFRAME>, <FRAME>, <APPLET>, <AUDIO>, <VIDEO>, <NOSCRIPT>, <IMG> elemente, kao I web bugove, s čim se postiže veća sigurnost i brzina preglednika. Međutim loša strana ove ekstenzije,iako odlično obavlja svoj posao je što večina stranica neće izgledati kako su izgledale, a neke se čak neće moći učitati. Naravno ScriptSafe nudi opciju da se njihov kod ne primjenjuje na određene stranice s čim je taj problem lako rješiv.

Ghostery je Google chrome ekstenzija koja kopira tracking protection mehanizam. Princip je identičan, onemogučava djelove koda koji su zaduženi za pračenje naše web aktivnosti, s čim se dobiva na zaštiti privatnosti i brzini preglednika.

HTTPS everywhere je možda I najkorisnija ekstenzija koja pronalazi siguran put do poslužitelja. Recimo da unosimo neki URL, tj. Želimo posjetiti neku stranicu, HTTPS everywhere će se pobrinuti da neđe sigurnu enkriptiranu HTTPS konekciju, a ne nekriptiranu HTTP konekciju.

Adblock plus je najpopuliranija ekstenzija s ove liste i možda čak I najpraktičnija. Kao što I samo ime kaže njena funkcionalnost je opisana blokiranjem neželjenih reklama,oglasa,pop-up reklama, s čim se postiže na većoj brzini preglednika, većoj sigurnosti od nasjedanja na lažne oglase, lakšem i lijepšem snalaženju i izlistavanju sadržaja web stranice.

**7.Zaključak**

Internet je neizbježno mjesto svake prosječne osobe u današnjem svijetu.

Veći dio svjetske populacije danas ima pristup internetu što maksimalno olakšava svakodnevni život pojedinca.

Danas sve što se može učiniti uživo može i preko interneta, s toga je njegova važnost neosporiva.

Za pristup internetu potreban nam je internetski preglednik.

Iako je internet pun raznih pogodnosti,zabavnog,edukacijskog i jedinstvenog sadržaja, tako je pun i „cyber kriminalaca“,bili oni individualci ili kompanije, koji pokušavaju narušiti sigurnost i privatnost pojidinih korisnika WorldWideWeb-a.

Web preglednici pružaju pristojnu zaštitu protiv takvih kriminalaca, ali kao što ništa nije savršeno, tako nije ni njihov otpor.

Preglednici osim samih integriranih načina zaštite pružaju i optimalnu podlogu za instaliranje dodatnih ekstenzija koje će nam pripomoći pri samoj zaštiti sigurnosti i privatnosti.

Na kraju krajeva odluka je na nama, mi kao korisnici smo najbolja zaštita i naše odluke će najviše utjecati na našu sigurnost, bez obzira koji preglednik koristili i kakva njegova zaštita bila ukoliko mi ne možemo predvijedjeti potencijalnu opasnost, naša sigurnost će biti ugrožena.

**8.Literatura**

* https://www.seminarsonly.com/computer%20science/Browser-Security.php
* https://en.wikipedia.org/wiki/Web\_browser
* https://en.wikipedia.org/wiki/Browser\_security
* <https://www.cloudwards.net/most-secure-web-browser/>
* <https://www.expressvpn.com/blog/best-browsers-for-privacy/>
* https://www.nextvation.com/10-browser-security-plugins-using/