





CERT.hr

Sadržaj

4	ZAK	LJUČAK	12
	3.2	SUČELJE <i>NoScripta</i>	9
	3.1	Kako <i>NoScript</i> štiti korisnike	8
3	KOR	IŠTENJE ALATA <i>NOSCRIPT</i>	8
2	INST	TALACIJA ALATA <i>NOSCRIPT</i>	4
1	UVO	D	3

Ovaj dokument izradio je Laboratorij za sustave i signale Zavoda za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Ovaj dokument vlasništvo je Nacionalnog CERT-a. Namijenjen je javnoj objavi te se svatko smije njime koristiti i na njega se pozivati, ali isključivo u izvornom obliku, bez izmjena, uz obvezno navođenje izvora podataka. Korištenje ovog dokumenta protivno gornjim navodima povreda je autorskih prava CARNET-a, a sve navedeno u skladu je sa zakonskim odredbama Republike Hrvatske.



1 Uvod

U današnje vrijeme, "web" je gotovo postao sinonim za "internet". Kada smo za računalom, korištenje interneta većinom se zapravo svodi na korištenje web stranica, od tražilice *Google*, preko društvenih mreža kao što su *Facebook* i *Twitter*, do brojnih portala s vijestima i slično.

Zato ni ne čudi da je jedan od glavnih načina kako kibernetički kriminalci napadaju korisnike upravo preko web stranica. Funkcionalnosti na webu koje nam omogućavaju napredne, interaktivne sadržaje (npr. *JavaScript* kôd), ujedno su i glavni alat kriminalaca u napadima na korisnike.

Problem je u tome što korisnici ne mogu jednostavno isključiti *JavaScript* kôd i slične funkcionalnosti. Iako bi time korisnici zaista bili sigurniji, većina web stranica tada više ne bi funkcionirala. Zato je potrebno rješenje koje će selektivno blokirati zlonamjerni sadržaj (npr. zlonamjerni *JavaScript* kôd), a dopustiti sav ostali sadržaj kako bi web stranice funkcionirale.

Jedno od najboljih rješenja takvog tipa je dodatak web pregledniku (engl. *add-on/extension*) zvan *NoScript*. Već *NoScriptovo* ime otkriva da je glavna funkcionalnost ovog dodatka selektivno blokiranje *JavaScript* kôda i sličnih funkcionalnosti. *NoScript* korisnicima daje kontrolu da sami odaberu koji se sadržaj na webu smije izvršavati. Tako korisnici mogu zabraniti izvršavanje sumnjivog (potencijalno opasnog) sadržaja, a dopustiti izvršavanje sadržaja iz izvora/domena kojima vjeruju. Nažalost, takav pristup u kojem korisnik sam bira koji elementi web stranice se smiju izvršavati zahtijeva znanje i dodatni trud krajnjeg korisnika, pa zbog toga *NoScript* većinom koriste samo tehnički napredni korisnici kojima je izrazito bitna sigurnost na webu.

NoScript je izvorno bio dostupan samo za web preglednik *Mozilla Firefox*, no nedavno je postao dostupan i za web preglednik *Google Chrome*.



2 Instalacija alata NoScript

Instalacija *NoScripta* prilično je jednostavna – neovisno o web pregledniku kojega korisnik koristi, prvo je potrebno posjetiti <u>službenu web stranicu dodatka</u> i tamo kliknuti na tipku *Install* na lijevom dijelu web stranice.



Time će korisnik, ovisno o korištenom web pregledniku (*Mozilla Firefox* ili *Google Chrome*), biti preusmjeren na odgovarajuću službenu web stranicu za preuzimanje dodataka.

Ako korisnik koristi web preglednik *Mozilla Firefox*, otvorit će se web stranica *Firefox*. *Add-ons*, gdje treba kliknuti na tipku *Add to Firefox*.

🍀 NoScript Security Suite – Get this E 🗙 🕂			
→ C' 🏠 (i) 🗍 🔒 Moz	illa Foundation (US) https://addons.mozilla.org/en-US/firefox/addon/no	oscript/ 🗉 🚥 🗹 🏠	III\ 🗉 📽
-		Extension Workshop 🗗	Developer Hub
Firefox Add-ons	Explore <u>Extensions</u> Themes More v	Q Find a	idd-ons $ ightarrow$
~			
	2 Recommended) 1,503,159 <u>2,928</u> Users <u>Reviews</u>	<u>★</u> ★★ <u>×</u> 4.4 Stars
NoScript Security	Suite	<u>5</u>	2,087
hy Giorgia Maona	Suite	3	178
by Glorgio Maorie		2	145
The best cocurity you can get in a web brown		1 🛨 📃	165
Allow active content to run only from sites yo	ou trust, and protect yourself against + Add to Firefox		
XSS other web security exploits. Disabled and can't reinstall? <u>https://tinyurl</u> .	com/moz-ext-cert		
Rate your experience	Screenshots		



Zatim će se pojaviti manji prozor u kojem treba kliknuti *Add* za davanje odgovarajućih dozvola za rad dodatku *NoScript*.

Image: NoScript Security Suite – Get this : x +					
← → C û	S) https://addons.mozilla.org/en-US/firefox/addon/noscript/	▣ … ▽ ☆	III\ © © ≡		
Add NoScript? It requires your permission Access your data for a Access browser tabs Store unlinited amount Access browser activit Learn more about permission	on to: Il websites cy cettings cy client-side data y during navigation silons	Extension Workshop 🗗 Develope Q Find add-ons	r Hub (2) Register or Log in		
Add	Gancel	1,503,159 <u>2,928</u> Users <u>Reviews</u>	4.4 Stars		
NoScript Security Suite by Giorgio Maone The best security you can get in a web browser! Allow active content to run only from sites you trust, and protee other web security exploits. Disabled and can't reinstall? https://tinyurl.com/moz-ext-cert	t yourself against XSS	5 ★ 4 ★ 3 ★ 2 ★ 1 ★	2.087 353 178 145 165		
Rate your experience	Screenshots				
How are you enjoying NoScript Security Suite ? Log in to rate this extension	Hinhi critical Hinhi critical Crisis Sine Scripting System access Vender Patch Honis Frefox 1.xx 				

U zadnjem koraku instalacije za preglednik Mozilla Firefox, moguće je odabrati da dodatak *NoScript* bude aktivan i u privatnim prozorima (engl. *private windows*) označavanjem okvira (engl. *check-box*) *Allow this extension to run in Private Windows*.

😻 NoScript Security Suite – Get this E 🗙 🕂		<u>_</u> _×
← → C û û û A Mozilla Foundation (US) https://addons.mozilla.org/en-US/firefox/addon/noscript/	▣ … ⊠ ☆	II\ ₪ © \$ Ξ
Firefox Add-ons explore <u>extensions</u> Themes More ~	Extension Script has be Manage your as	een added to Firefox. dd-ons by clicking ♣ in the ☰ menu. ktension to run in Private Windows Qkay, Got It
Recommended	1,503,159 2,928 Users <u>Reviews</u>	4.4 Stars
NoScript Security Suite by Giorgio Maone The best security you can get in a web browser! Allow active content to run only from sites you trust, and protect yourself against XSS other web security exploits. Disabled and can't reinstall? <u>https://tinyurl.com/moz-ext-cert</u>	5 ★ 4 ★ 3 ★ 2 ★ 1 ★	2.087 353 178 145 165
Rate your experience Screenshots How are you enjoying NoScript Security Suite? How are you enjoying NoScript Security Suite? Log in to rate this extension For moto Yendor Patch		



Ako korisnik koristi web preglednik *Google Chrome*, onda će ga poveznica sa službene stranice dodatka *NoScript* odvesti na *Chrome web store* gdje za instalaciju treba kliknuti na tipku *Add to Chrome*.





Zatim će se pojaviti manji prozor u kojem treba kliknuti *Add Extension* za davanje odgovarajućih dozvola za rad dodatku *NoScript*.

🚡 NoScript - Chrome Web Store 🗙 🕂			
\leftarrow \rightarrow C \triangleq chrome.google.com/webstore/detail/	noscript/doojmbjmlfjjnbmnoijecmcbfeoakpjm/		☆ 👶 :
🚡 chrome web store	Add "NoScript"?	×	🗱 Sign in
Home > Extensions > NoScript	It can: Read and change all your data on the websites you v Change your privacy-related settings	visit	
NoScript	Add extensi	on Cancel	Add to Chrome
Offered by: Hackademix	ty 🛛 🔔 49,338 users		
	Overview Reviews Suppo	rt Related	
C → C ■ https://eta C → C ■ https://eta	Chel International - Breaking News, US News, World News and Corporation Mannelm X & Noscript - Javatic X & Noscript - Edition to ton concorn US Politics (Business Editor comments Sport Trans S Now Martin S & S Now Martin S & S & S Now Martin S & S & S Now Martin S & S & S & S & S & S & S & S & S & S	Video-Chromium - C × a Developer Dable: × C NH Internations: × + & S & S T NH Internations: × + S T N () () ()	
Tł	hird time lucky?	No. - Antibios and pane kell St. - population science St. - population science St. - population science St. - polation science	
	Fundel to punish gay sax adultory with death by st Make seven stab Fajceket by impart Fapet impart of adapt/ Druss taw facets Milling persons are in the seven if the seven stab for the seven facets Milling persons are in the	and Trump and Comey clash over Mueller probe outcome and the second second second and the second second second second file Wenebook the statistics where the statistics of the second second second music second second second second second second second second second second second second second second second s	
British PM May v	Hill bring her ill-stared Brexit deal for a series Cohinet minister indicates and series Cohinet minister indicates and series Cohinet minister indicates and series	new 15th Century Indiates a characterial sh't just Damler to build Smart cars in China	

Neovisno o korištenom web pregledniku, nakon opisanog postupka instalacije će se u gornjem desnom kutu web preglednika pojaviti ikona *NoScripta*, koja prikazuje broj blokiranih elemenata. Prelaskom pokazivača preko ikone *NoScripta* prikazuju se dodatne informacije o blokiranim elementima.



3 Korištenje alata NoScript

U ovom će poglavlju prvo biti konceptualno objašnjeno kako *NoScript* štiti korisnike, a zatim će biti opisane njegove funkcije kroz sučelje.

3.1 Kako NoScript štiti korisnike

NoScriptova uloga je selektivno blokiranje nekih funkcionalnosti na webu (npr. *JavaScripta, Jave, Flasha, Silverlighta* i sl.) koje se, unatoč svojim legitimnim svrhama, često koriste i za napade na računalo korisnika.

Idealno, *NoScript* bi zaustavio izvršavanje svih zlonamjernih sadržaja na webu, te bi u isto vrijeme dopustio izvršavanje preostalog sadržaja (koji nije zlonamjeran) kako bi korisnik mogao pregledavati web bez ikakvih poteškoća. Problem je u tome što nema laganog načina za saznati koji je sadržaj zlonamjeran, a koji nije. Zato će, nakon instalacije, *NoScript* automatski blokirati gotovo sav *JavaScript, Java, Flash, Silverlight* i sl. kôd na webu, jer su takve funkcionalnosti česti izvori napada. Uloga korisnika je tada selektivno odobriti neke izvore kôda (domene) kojima korisnik vjeruje, nakon čega će *NoScript* dopustiti izvršavanje kôda/sadržaja samo iz tih izvora. Tako će u konačnici biti dopušteno izvršavanje kôda isključivo s domena kojima korisnik vjeruje, a sav ostali kôd, uključujući zlonamjerni kôd, bit će blokiran.

Primjerice, otvaranjem stranice <u>Nacionalnog CERT-a</u>, automatski će biti blokiran sav JavaScript kôd s domena *cert.hr, facebook.com, facebook.net* i *google-analytics.com*. U ovom primjeru, korisnik bi mogao dopustiti izvršavanje kôda s domene *cert.hr* kako bi web stranica normalno funkcionirala (jer je pretpostavka da kôd s te domene nije zlonamjeran, a potreban je za funkcioniranje stranice), a preostali kôd s *Facebook* i *Google* domena ostaviti blokiranim (s ciljem zadržavanja više razine privatnosti).



Kako korisnik ne bi morao svaki put ispočetka odobravati domene, *NoScript* će zapamtiti domene koje korisnik označi kao pouzdane (engl. *trusted*), odnosno nepouzdane (engl. *untrusted*). Primjerice, jednom kada korisnik označi domenu *cert.hr* kao pouzdanu, a domenu *google-analytics.com* kao nepouzdanu, na svakoj web stranici će biti dopušteno izvršavanje kôda s domene *cert.hr*, te neće biti dopušteno izvršavanje kôda s domene *google-analytics.com*. Unatoč tome, glavni nedostatak *NoScripta* je taj što korisnik mora steći naviku redovitog odobravanja svake nove domene/izvora kôda kojemu vjeruje, jer u suprotnom će previše funkcionalnosti biti blokirano i velik dio web stranica uopće neće raditi. To će svakako u nekoj mjeri usporiti korisnika u svakodnevnom pregledavanju weba, no ipak, ovakav će pristup pružiti izrazito visoku razinu zaštite koja mnogima opravdava dodatni napor.

CERT.hr

3.2 Sučelje NoScripta

Kao što je prethodno navedeno, nakon instalacije se u gornjem desnom kutu pojavljuje ikona *NoScripta*, a klikom na nju prikazuje se glavno sučelje.

eb APIs 🗙 🕂				
				🔤 Q 🛧 🥏 🖊 🚱
× C 🔇				S! 🎵 🔇 🐻
S DEFAULT	S	s 😒	S	unizg.hr
S DEFAULT	5	S 😒	S.	google-analytics.com
🔇 ≲ S TRUSTEI	0	8	S.	gstatic.com
S DEFAULT	5	S 😒	S.	npmcdn.com

U prvom redu glavnog sučelja vidljive su sljedeće ikone:

- 1. 🗙 zatvori izbornik
- 2. **C** ponovno učitaj stranicu
- 3. 🚳 dodatne postavke
- 4. 🚫 omogući blokiranje skripti na svim stranicama
- 5. 🥂 ukini sve zabrane za stranicu u ovom *tabu*
- 6. 🔃 označi sve blokirane izvore na stranici privremeno pouzdanima
- 7. 💦 prestani smatrati pouzdanima izvore označene kao "privremeno pouzdane"

Ispod tog reda, u sučelju je prikazan popis izvora (domena) s kojih trenutna web stranica pokušava učitati resurse (npr. *JavaScript* kôd). Ako se pored domene nalazi i simbol lokota, to označava da veza koristi HTTPS.

Dio sučelja kojega korisnik najviše koristi je upravo popis domena u kojemu je moguće klikom na odgovarajuću ikonu označiti stupanj pouzdanosti domene kao:

- 🔇 zadan (engl. *default*),
- So privremeno pouzdan (engl. *temporarily trusted*),
- **S** pouzdan (engl. *trusted*),
- 🔇 nepouzdan (engl. *untrusted*),
- 🕵 prilagođen (engl. *custom*).



U uobičajenom korištenju *NoScripta*, ako nakon otvaranja web stranice neke funkcionalnosti ne rade, korisnik će otvoriti glavno sučelje *NoScripta*, pogledati s kojih sve izvora (domena) web stranica pokušava učitati kôd, te će, po svojoj procjeni, označiti neke od tih izvora kao pouzdane ili kao privremeno pouzdane kako bi se samo željeni kôd učitao i izvršio, dok bi sav ostali kôd ostao blokiran iz sigurnosnih razloga.

Klikom na ikonu za otvaranje dodatnih postavki () moguće je preciznije provjeriti, i po potrebi izmijeniti, što točno *NoScript* dozvoljava izvorima koji su označeni kao zadani (engl. *default*), pouzdani (engl. *trusted*), odnosno nepouzdani (engl. *untrusted*).

U zadanom (engl. *default*) načinu su nakon instalacije dopušteni elementi iz kategorija *frame, fetch* i *other*, a svi ostali elementi (npr. *JavaScript* ili WebGL kôd) su blokirani.

General Per-site Pe	ermissions Appearance	Advanced	
Disable restriction	ns globally (dangerous) 🛛 🗖	Temporarily set top-level sites to	TRUSTED 🗖 Cascade top
Preset customizati	on (for all the sites sharing a	n preset)	
S DEFAULT	S TRUSTED		
Allow			
🗖 script 🗖 obje	ect 🥅 media 🔽 frame	🗖 font 🔲 webgl 🔽 fetch	🔽 other

U pouzdanom (engl. *trusted*) načinu su nakon instalacije dopušteni svi elementi. Ako korisnik označi domenu kao privremeno pouzdanu, *NoScript* u tom slučaju koristi iste postavke kao da je domena označena kao pouzdana, ali samo za vrijeme trajanja sjednice (engl. *session*) preglednika. Nakon zatvaranja i ponovnog otvaranja preglednika, postavke za privremeno pouzdane domene vraćaju se na izvornu vrijednost.

General Per-site Permissi	ions Appearance Advan	ced	
C Disable restrictions glob	oally (dangerous) 🗖 Tempor	arily set top-level sites to TRUSTED	Cascade top
Preset customization (for	all the sites sharing a preset)	
SDEFAULT	S TRUSTED		
Allow			
🔽 script 🔽 object 🔽	🗹 media 🔽 frame 🔽 font	🔽 webgl 🔽 fetch 🔽 other	

U nepouzdanom (engl. *untrusted*) načinu su inicijalno onemogućene sve vrste elemenata.

General Per-site Permiss	ions Appearance	Advanced	
Disable restrictions glob	bally (dangerous) 🛛	Temporarily set top-level sites	to TRUSTED 🗖 Cascade top
Preset customization (for	r all the sites sharing	a preset)	
SDEFAULT	S TRUSTED		
Allow			
🗖 script 📕 object 🦷	media 🗖 frame	🗖 font 📕 webgl 📕 fetch	🗖 other



U dodatnim postavkama moguće je i pregledati te izmijeniti popis domena/izvora kojima je zadana razina pouzdanosti (pouzdan, privremeno pouzdan, nepouzdan...). Nakon instalacije već postoji manja lista domena označenih kao pouzdane (kako nakon instalacije *NoScripta* ne bi sve često korištene web stranice prestale raditi), no korisnik ih u ovom izborniku može po potrebi izmijeniti ili ukloniti.



Još jedna korisna funkcionalnost je uvoz i izvoz postavki *NoScripta*, dostupnih putem tipki *Import* i *Export* u sučelju za dodatne postavke. Uvozom i izvozom je moguće pohraniti i prenijeti sve postavke *NoScripta* iz jednog web preglednika/računala na drugo. Izvozom će *NoScript* generirati tekstualnu datoteku koju korisnik zatim preuzme, pohrani, te po potrebi uveze u novu instalaciju *NoScripta*.

Ceneral	Der-cite Dermi	scions Annearanc	e Advanced	NoScri	Version 11.0.2	
General	rei-site reinit	SSIONS Appearance	Auvanceu	1		
🗖 Disab	le restrictions gl	obally (dangerous)	Temporarily	set top-level sites	to TRUSTED	
🗆 Casca	ade top documer	nt's restrictions to sub	odocuments			
Preset	customization (f	or all the sites shari	ng a preset)			
	AULT	S TRUSTED				
Allow						
🔽 📈 scri	ipt 🔽 object	🔽 media 🔽 frame	e 🔽 font 🔽	webgl 🔽 fetch	🔽 other	



4 Zaključak

Većini ljudi je korištenje web stranica važna aktivnost svakog dana. Na webu nas čekaju razne prijetnje: zlonamjerno oglašavanje (engl. *malvertising*), iskorištavanje ranjivosti i *exploit kitovi, cross-site scripting* (XSS) napadi, prikupljanje informacija i profiliranje korisnika (engl. *fingerprinting*), *Clickjacking, Tabnabbing, Cross-site request forgery* (CSRF) napadi...

Nema lakog načina da se istovremeno i zaštitimo od većine prijetnji i zadržimo svu funkcionalnost i bogatstvo modernog weba temeljenog na *JavaScriptu* i sličnim tehnologijama. No za one koji su spremi uložiti trud, dostupan je *NoScript* – dodatak web preglednicima *Mozilla Firefox* i *Google Chrome* koji korisnicima daje kontrolu da precizno odrede koji dijelovi web stranice se smiju izvršavati, a koji ne. Korištenje *NoScripta* ipak zahtijeva osnovno razumijevanje tehnologije web stranica, te će redovito odobravanje domena/izvora sadržaja nažalost usporiti korisnika u svakodnevnom pregledavanju weba, no razina zaštite koju *NoScript* tada pruža nema alternative.