

## *NoScript*

CERT.hr-PUBDOC-2019-10-390

## Sadržaj

<b>1</b>	<b>UVOD</b> .....	<b>3</b>
<b>2</b>	<b>INSTALACIJA ALATA <i>NOSCRIPT</i></b> .....	<b>4</b>
<b>3</b>	<b>KORIŠTENJE ALATA <i>NOSCRIPT</i></b> .....	<b>8</b>
3.1	KAKO <i>NoScript</i> ŠTITI KORISNIKE .....	8
3.2	SUČELJE <i>NOSCRIPTA</i> .....	9
<b>4</b>	<b>ZAKLJUČAK</b> .....	<b>12</b>

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.

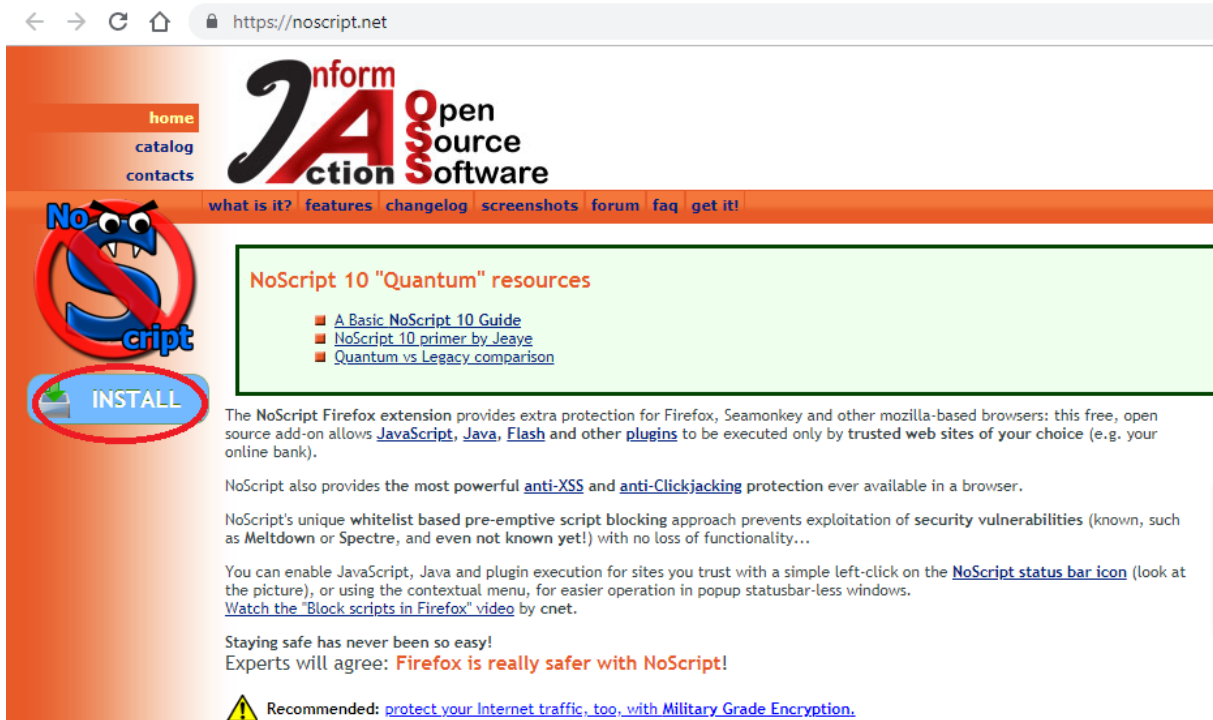
Problem je u tome što korisnici ne mogu jednostavno isključiti *JavaScript* kôd i slične funkcionalnosti. Iako bi time korisnici zaista bili sigurniji, većina web stranica tada više ne bi funkcionirala. Zato je potrebno rješenje koje će selektivno blokirati zlonamjerni sadržaj (npr. zlonamjerni *JavaScript*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

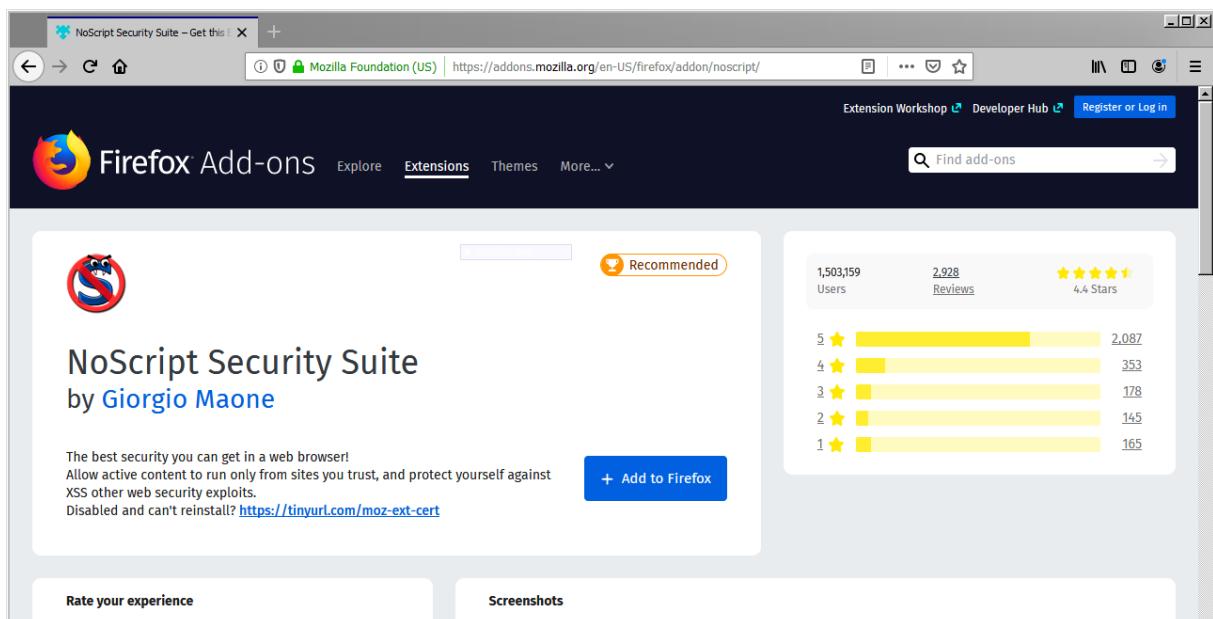
## 2 Instalacija alata NoScript

Instalacija *NoScripta* prilično je jednostavna – neovisno o web pregledniku kojega korisnik koristi, prvo je potrebno posjetiti [službenu web stranicu dodatka](#) i tamo kliknuti na tipku **Install** na lijevom dijelu web stranice.

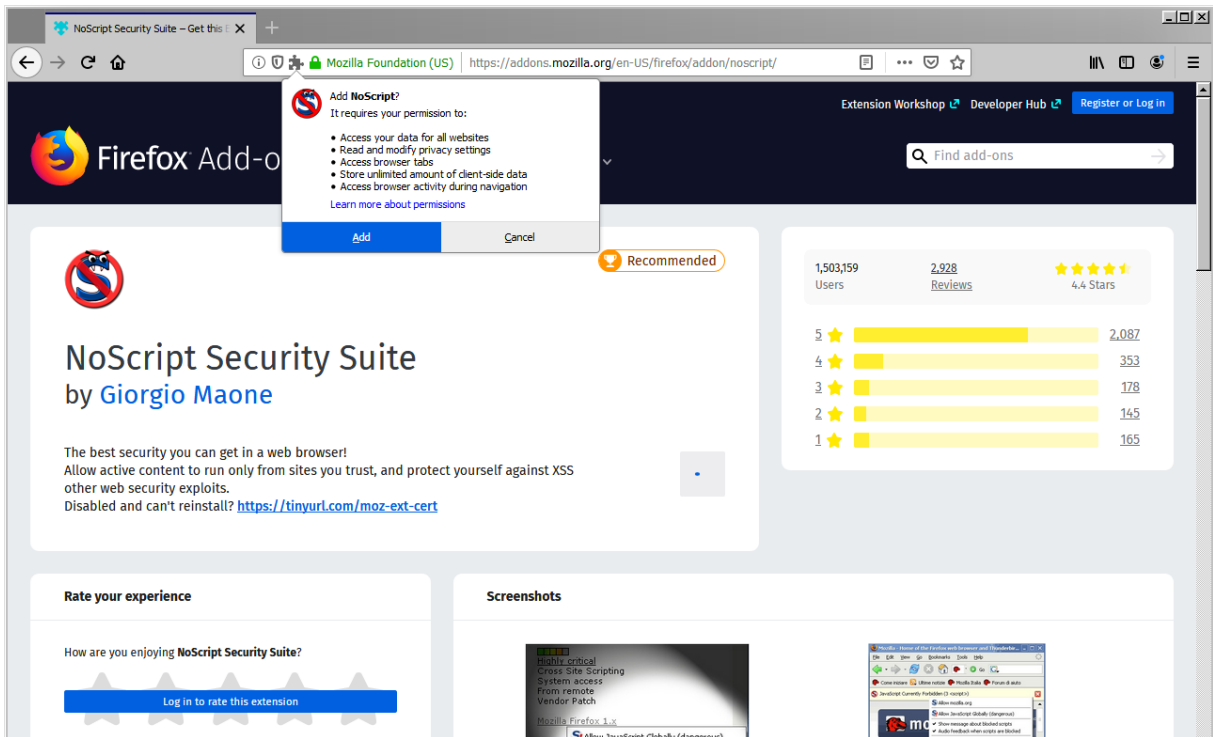


Time će korisnik, ovisno o korištenom web pregledniku (*Mozilla Firefox* ili *Google Chrome*), biti preusmjeren na odgovarajuću službenu web stranicu za preuzimanje dodatka.

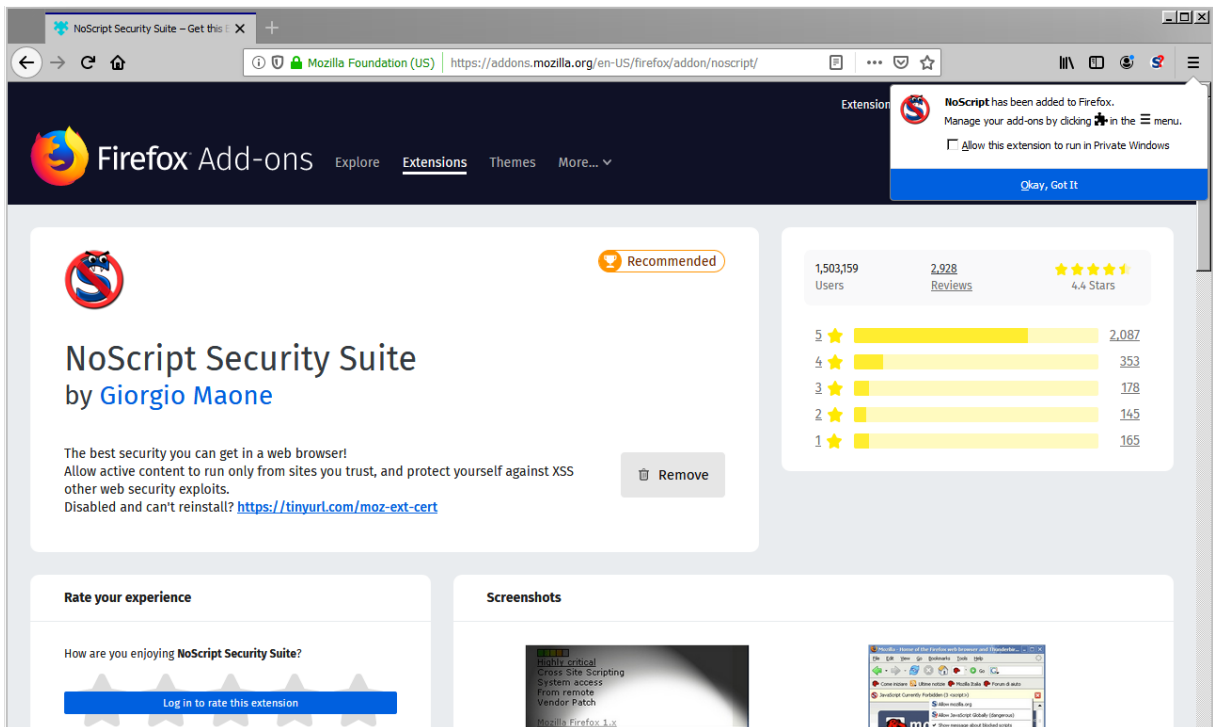
Ako korisnik koristi web preglednik *Mozilla Firefox*, otvorit će se web stranica *Firefox Add-ons*, gdje treba kliknuti na tipku **Add to Firefox**.



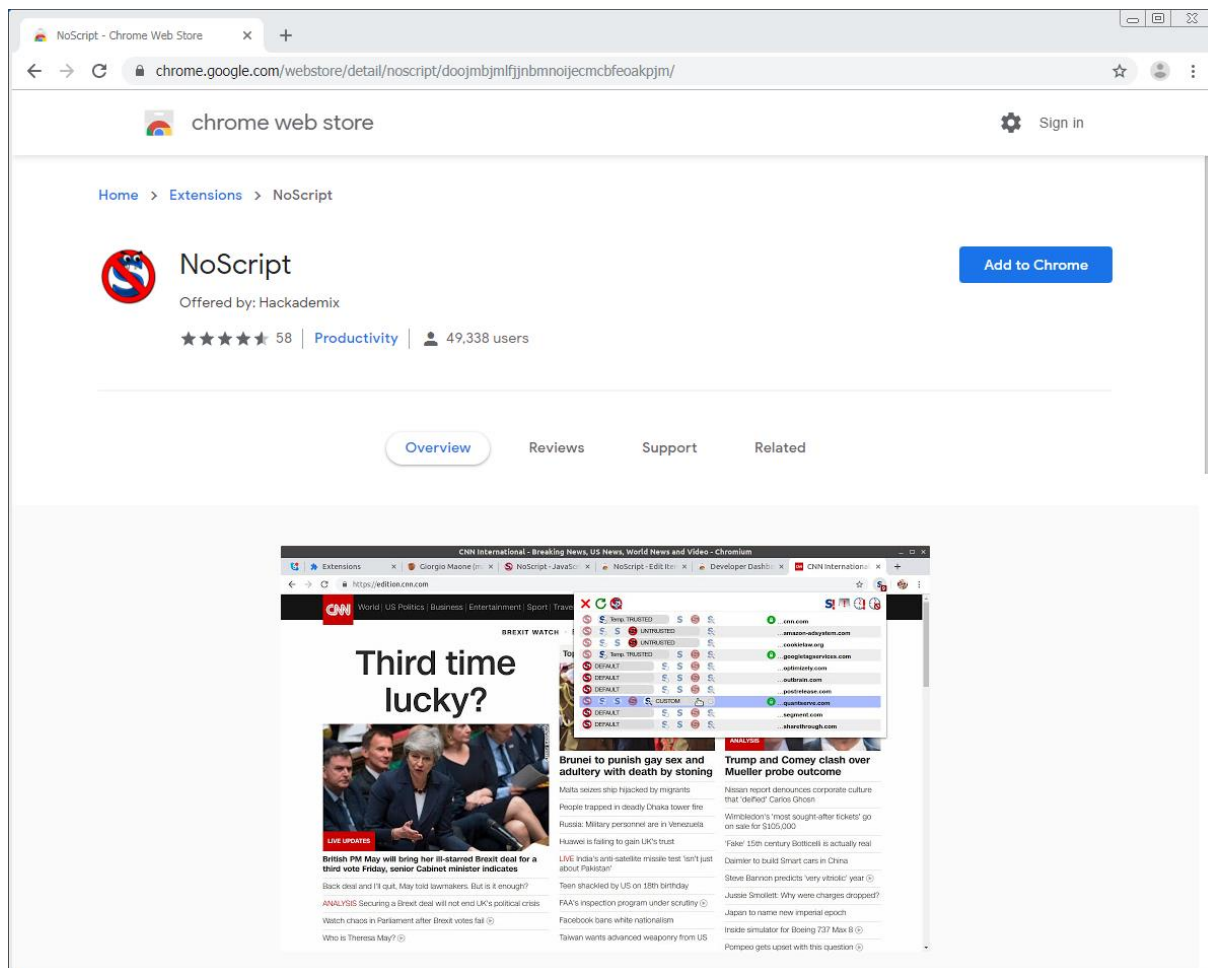
Zatim će se pojaviti manji prozor u kojem treba kliknuti **Add** za davanje odgovarajućih dozvola za rad dodatku *NoScript*.



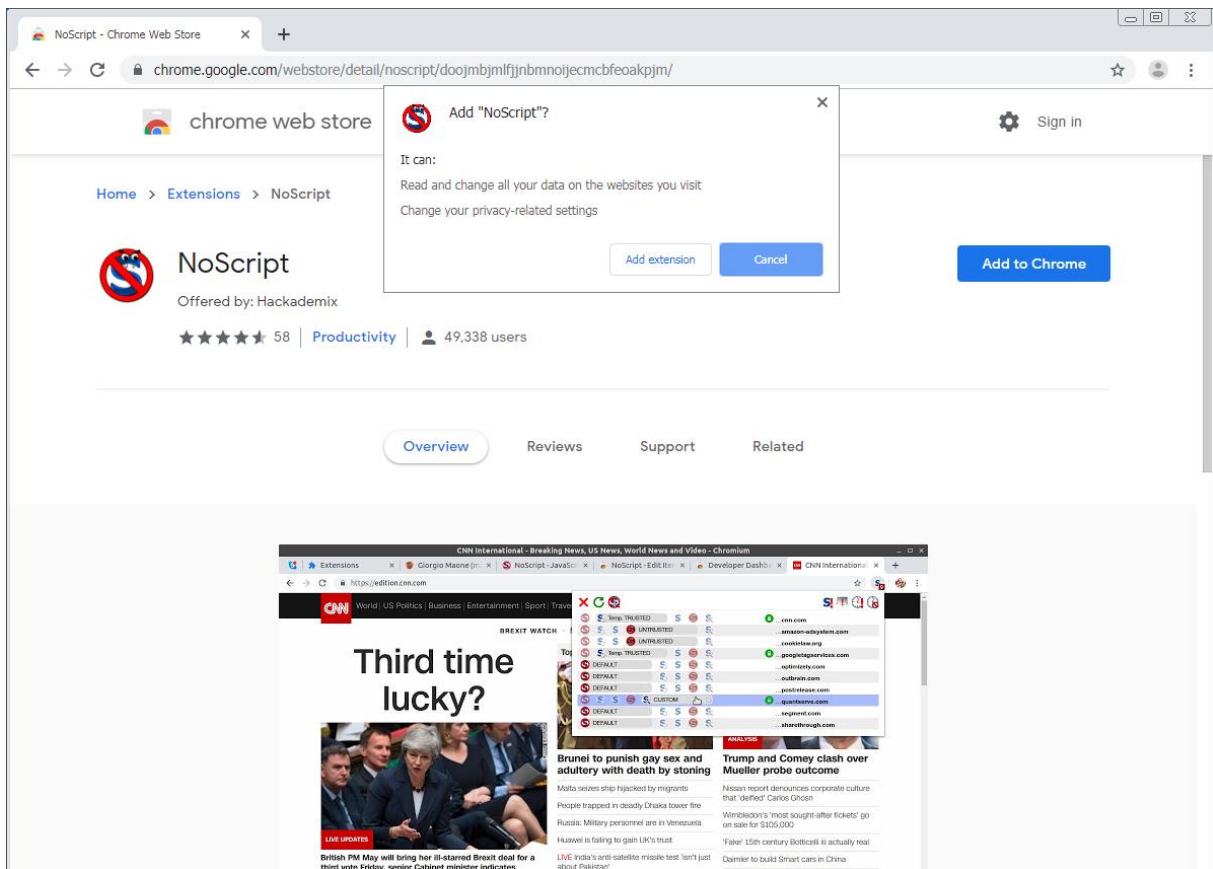
U zadnjem koraku instalacije za preglednik Mozilla Firefox, moguće je odabrati da dodatak *NoScript* bude aktivan i u privatnim prozorima (engl. *private windows*) označavanjem okvira (engl. *check-box*) **Allow this extension to run in Private Windows**.



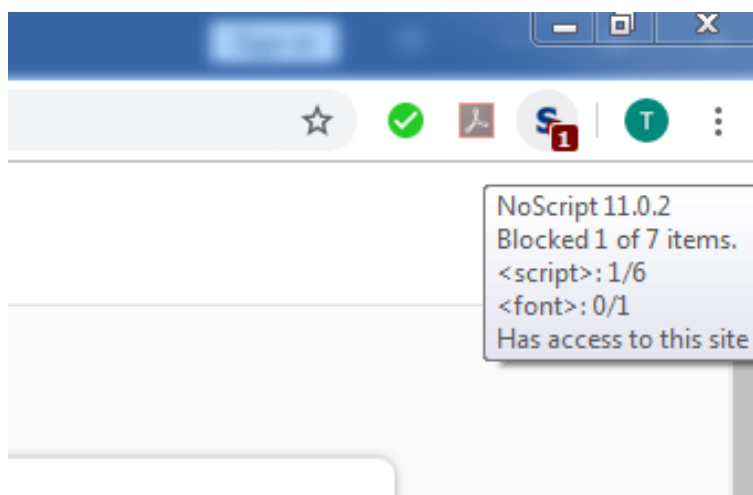
Ako korisnik koristi web preglednik *Google Chrome*, onda će ga poveznica sa službene stranice dodatka *NoScript* odvesti na *Chrome web store* gdje za instalaciju treba kliknuti na tipku **Add to Chrome**.



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



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*

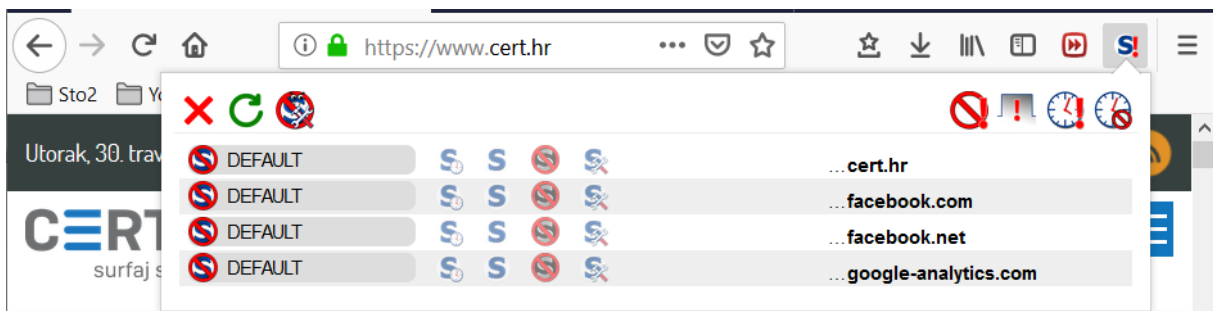
U ovom će poglavlju prvo biti konceptualno objašnjeno kako *NoScript* štiti korisnike, a zatim će biti opisane njegove funkcije kroz sučelje.

#### 3.1 Kako *NoScript* štiti korisnike

*NoScript*ova uloga je selektivno blokiranje nekih funkcionalnosti na webu (npr. *JavaScripta*, *Java*, *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 zlonamjerna) kako bi korisnik mogao pregledavati web bez ikakvih poteškoća. Problem je u tome što nema laganog načina za saznati koji je sadržaj zlonamjerna, 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 zlonamjerna kôd, bit će blokiran.

Primjerice, otvaranjem stranice [Nacionalnog CERT-a](https://www.cert.hr), 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 zlonamjerna, a potreban je za funkcioniranje stranice), a preostali kôd s *Facebook* i *Google* domena ostaviti blokiranim (s ciljem zadržavanja više razine privatnosti).

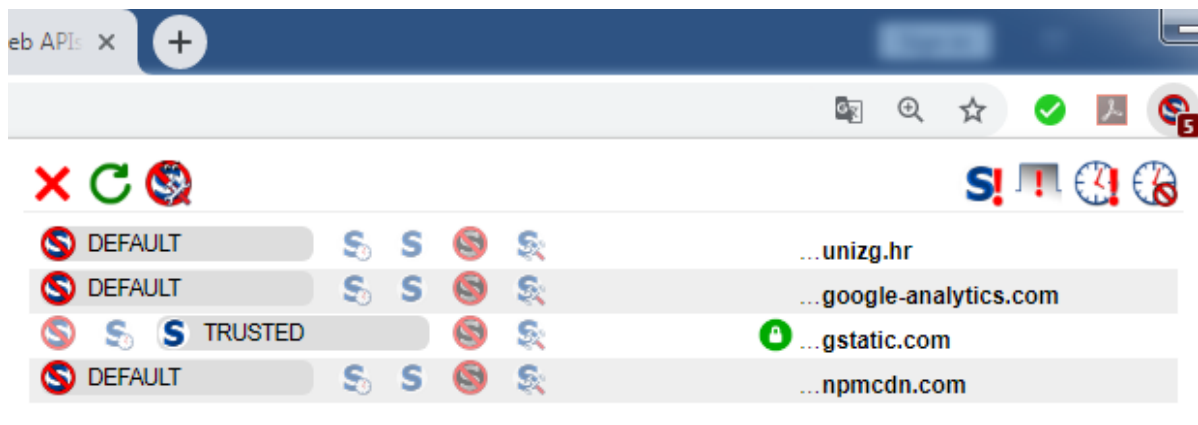


Kako korisnik ne bi morao svaki put ispočetka odobravati domene, *NoScript* će zapamtiti domene koje korisnik označi kao pouzdane (engl. *trusted*), odnosno nepouzdanu (engl. *untrusted*). Primjerice, jednom kada korisnik označi domenu *cert.hr* kao pouzdanu, a domenu *google-analytics.com* kao nepouzdanu, 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.



### 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.



U prvom redu glavnog sučelja vidljive su sljedeće ikone:


1. – zatvori izbornik
2. – 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.

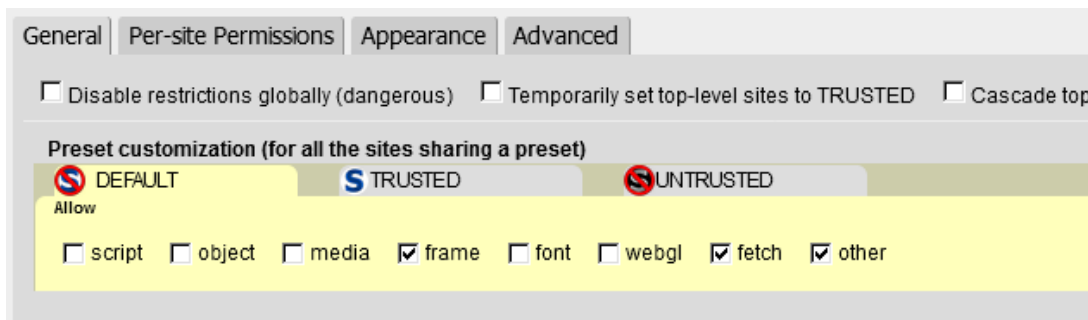
Dio sučelja kojega korisnik najviše koristi je upravo popis domena u kojemu je moguće klikom na odgovarajuću ikonu označiti stupanj pouzdanosti domene kao:

- – zadan (engl. *default*),
- – privremeno pouzdan (engl. *temporarily trusted*),
- – pouzdan (engl. *trusted*),
- – nepouzdan (engl. *untrusted*),
- – prilagođen (engl. *custom*).

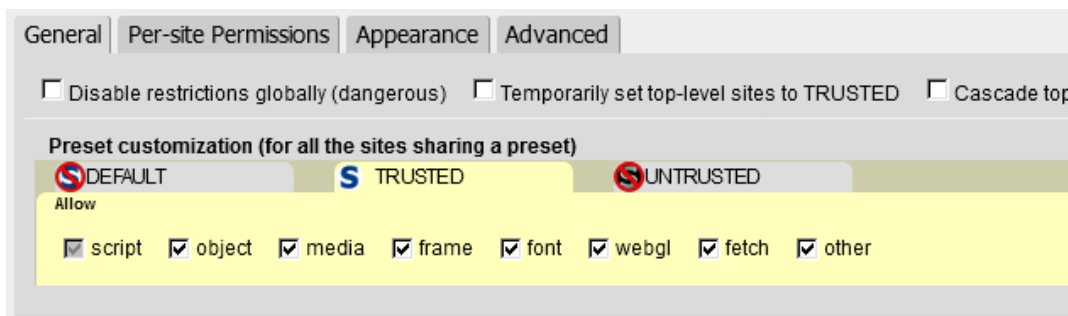
U uobičajenom korištenju *NoScripta*, ako nakon otvaranja web stranice neke funkcionalnosti ne rade, korisnik će otvoriti glavno sučelje *NoScripta*, pogledati s kojih sve izvora (domena) web stranica pokušava učitati kôd, te će, po svojoj procjeni, označiti neke od tih izvora kao pouzdane ili kao privremeno 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 nepouzdana (engl. *untrusted*).

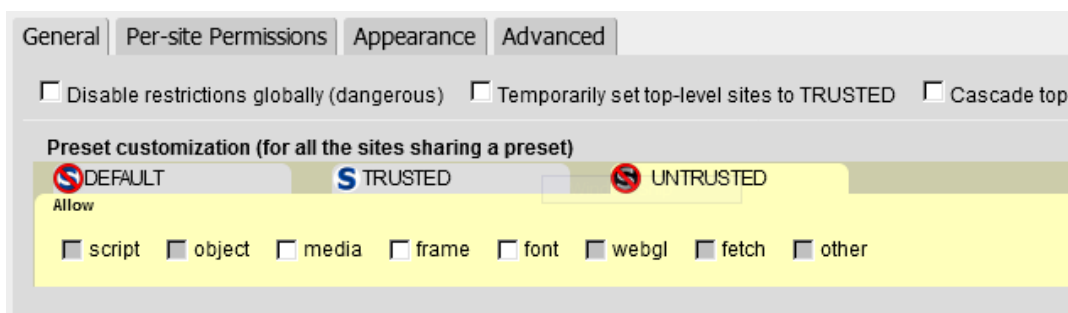
U zadanom (engl. *default*) načinu su nakon instalacije dopušteni elementi iz kategorija *frame*, *fetch* i *other*, a svi ostali elementi (npr. *JavaScript* ili *WebGL* kôd) su blokirani.



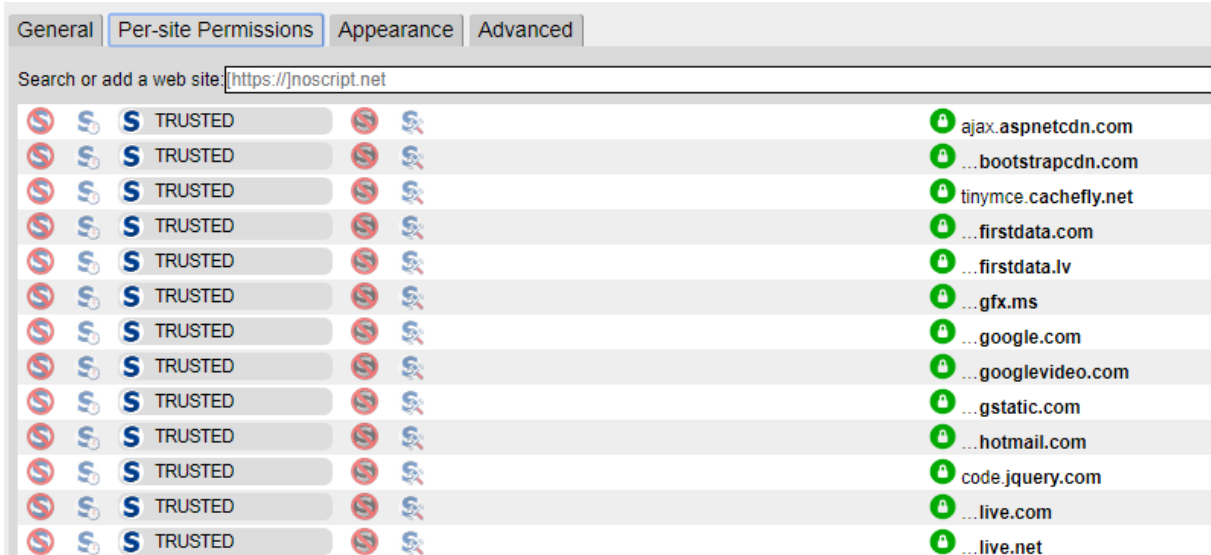
U pouzdanom (engl. *trusted*) načinu su nakon instalacije dopušteni svi elementi. Ako korisnik označi domenu kao privremeno pouzdanu, *NoScript* u tom slučaju koristi iste postavke kao da je domena označena kao pouzdana, ali samo za vrijeme trajanja sjednice (engl. *session*) preglednika. Nakon zatvaranja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



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



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*.



## 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.