

Frenemies



NoScript vs for Web Developers

noscript.net



about:me

- ✓ Giorgio Maone (@ma1)
- ✓ Software developer & hacker
- ✓ Code Contributor & Security Group member @ **Mozilla**
- ✓ WASWG invited expert @ **W3C**
- ✓ #9 @ “Most Dangerous People on the Internet” (© RSnake)
- ✓ Dad, most of the time @ **Home**
- ✓ Creator & maintainer of the **NoScript** browser add-on



about:NoScript

- ✓ JavaScript permission manager
- ✓ Embedded content blocker (plugins, media...)
- ✓ XSS filter
- ✓ Application Boundaries Enforcer (ABE)
- ✓ ClearClick (Clickjacking protection)
- ✓ HTTPS enhancements
- ✓ Usability helpers
- ✓ ...



about:talk

- ✓ Good practices appraisal
- ✓ Cheap tricks shaming
- ✓ Usability extras showcase
- ✓ Future directions
- ✓ Help & feedback requests



Tweet your questions

#ns4dev



Flexible Permissions for **JavaScript** and **Embedded Content**

Java, Flash, Silverlight, Acrobat Reader and any other plugin,
HTML5 media (<video>, <audio>, APIs),
WebGL, XSLT, Web Fonts,
Frames (optionally)



Firefox

Jobs, Robots, Capitalism, Inequality, And...

techcrunch.com/2013/08/24/jobs-robots-capitalism-inequality-and-you/

HOME STARTUPS MOBILE GADGETS EUROPE VIDEO MORE

HOT TOPICS YAHOO APPLE FACEBOOK TWITTER GOOGLE MICROSOFT

UMN

DISRUPT EUROPE 2013 OCTOBER 28-29 ARENA BERLIN BUY TICKETS NOW


Comment +1 487

Jobs, Robots, Capitalism, Inequality, And You

JON EVANS

Saturday, August 24th, 2013

Comments

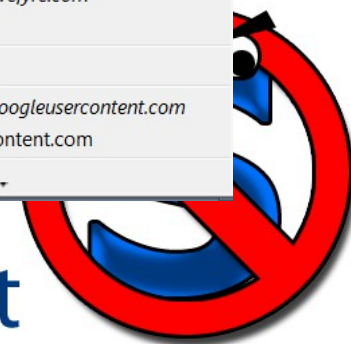


Maybe I'm wrong. Maybe everything will be fine. Maybe the "widening gap between rich and poor" is temporary. Maybe the steady growth in the proportion of jobs that are part-time and/or low-paid will soon reverse.

Or maybe the idea that all the homeless need are old laptops and a few JavaScript textbooks is not unlike the claim that new technologies automatically create new jobs for everyone. Maybe, unless something drastic changes, most people are totally screwed.

Scripts Partially Allowed, 3/23 (gstatic.com, google.com, techcrunch.com) | <SCRIPT>: 78 | <OBJECT>: 1

- Forbid techcrunch.com
- Temporarily allow gravatar.com
- Allow gravatar.com
- Temporarily allow scorecardresearch.com
- Allow scorecardresearch.com
- Temporarily allow gravity.com
- Allow gravity.com
- Temporarily allow optimizely.com
- Allow optimizely.com
- Temporarily allow facebook.net
- Allow facebook.net
- Temporarily allow quantserve.com
- Allow quantserve.com
- Temporarily allow adsonar.com
- Allow adsonar.com
- Temporarily allow aolcdn.com
- Allow aolcdn.com
- Temporarily allow linkedin.com
- Allow linkedin.com
- Temporarily allow twitter.com
- Allow twitter.com
- Temporarily allow wordpress.com
- Allow wordpress.com
- Temporarily allow wp.com
- Allow wp.com
- Temporarily allow chartbeat.com
- Allow chartbeat.com
- Temporarily allow google-analytics.com
- Allow google-analytics.com
- Temporarily allow livefyre.com
- Allow livefyre.com
- Forbid google.com
- Temporarily allow googleusercontent.com
- Allow googleusercontent.com
- Forbid gstatic.com



WTF?



Main use cases for this mess

- ✓ Content mash-ups
- ✓ CDNs
- ✓ External trackers/analytics
- ✓ Advertisement networks
- ✓ ... add yours #ns4devMess



Keep it tight

- ✓ *Depend* on just 1 domain...
- ✓ ... or use subdomains
- ✓ Sharding is less important nowadays
- ✓ cloudfront.net raw inclusions suck



Meet middle-click (or shift+click)



Firefox

OWASP

owasp.org: Security and Privacy Info

noscript.net/about/owasp.org;owasp.org

duck duck go search



owasp.org

Security and Privacy Info

This service is **experimental** and far from being complete yet.

Currently it provides links to other resources helping to assess the security and privacy trustworthiness of [owasp.org](#).

- [WOT Scorecard](#) about owasp.org
- [McAfee SiteAdvisor® rating](#) for owasp.org
- [Webmaster Tips Site Information](#) about owasp.org
- [Safe Browsing Diagnostic](#) on owasp.org
- [hpHost Report](#) on owasp.org

We hope to keep adding new tools and features over the time, making trust-based decisions easier for NoScript users.

Privacy Disclaimer

NOSCRIPT.NET does not retain any personal-identifiable record about your "Security and Privacy Info" queries.



Keep it visible

- ✓ Be clear about required/optional
- ✓ Take advantage of placeholders
- ✓ “Enable JavaScript” redirected page is EVIL
- ✓ Avoid nested inclusions
- ✓ cloudfront.net raw inclusions suck!



Poor man CDNs OMG!

- ✓ “Cheap” setups like including jQuery plugins from their code repositories get mercilessly broken by NoScript
- ✓ NoScript blocks script and CSS inclusions with **download-specific content-type** headers and/or **Content-disposition: attachment**
- ✓ This should be mandatory in any browser (even without **X-Content-Type-Options: nosniff**)
- ✓ Very important to NoScript users (github, googlecode...)



Less Painful Script Blocking?

- ✓ Attempt to “fix” JavaScript navigation (links, drop-down menus, submit buttons, redirections)
- ✓ Framebusting emulation
- ✓ Forcing <NOSCRIPT> elements visible for blocked inclusions
- ✓ Lots of other minor stuff, but most important...



Script Surrogates

- ✓ Similar to GreaseMonkey scripts but different :)
- ✓ Blocking aware (triggered also by inclusion blocking)
- ✓ Can modify the execution environment, emulating missing scripts and even built-in objects
- ✓ Can replace remote scripts with local alternatives (RFE by Richard Stallman)
- ✓ hackademix.net/2011/09/29/script-surrogates-quick-reference/



Abusive Ideas

- ✓ Abusing “Stallman's” surrogates to cache jQuery and other common libraries locally
- ✓ Abusing WHOIS to create “batch allow” groups
- ✓ Abusing (?) data- attributes on <SCRIPT> elements to provide useful metadata
- ✓ Tweet your #ns4devIdea

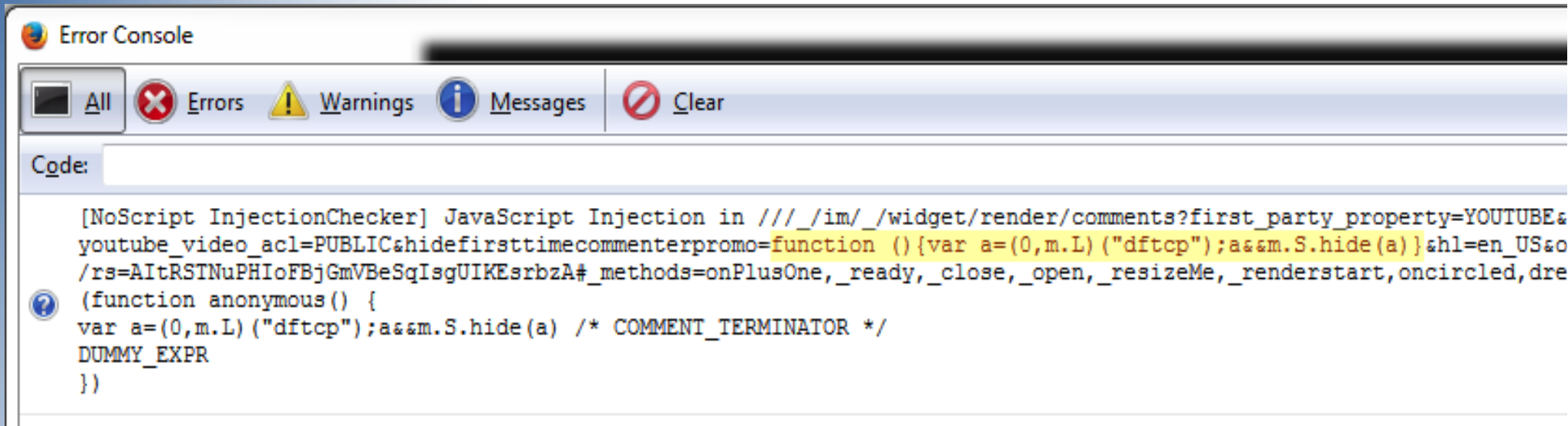


Anti-XSS Filter

- ✓ (Ab)uses Gecko's HTML parser and the SpiderMonkey JavaScript engine to check for suspicious payloads
- ✓ Desktop version filters / Android version blocks
- ✓ Checks for many “exotic” encodings and complex attack scenarios (e.g. Ebay's custom URL encoding, omographic attacks, multiple omomimous parameters concatenations...)
- ✓ Examines thoroughly the request, but ignores the response (pro: **safest**; con: more **false positives**)



XSS false positives



The screenshot shows a browser's Error Console with the following content:

```
[NoScript InjectionChecker] JavaScript Injection in ///_im/_/widget/render/comments?first_party_property=YOUTUBE&youtube_video_acl=PUBLIC&hidefirsttimecommenterpromo=function () {var a=(0,m.L) ("dftcp");a&&$.S.hide(a)}&hl=en_US&o/rs=AItrSTNuPHIoFBjGmVBeSqIsgUIKEsrbzA#_methods=onPlusOne,_ready,_close,_open,_resizeMe,_renderstart,onclicked,dre  
?  
(function anonymous() {  
var a=(0,m.L) ("dftcp");a&&$.S.hide(a) /* COMMENT_TERMINATOR */  
DUMMY_EXPR  
})
```

...as seen on Youtube!



Please post data, not code

- ✓ Avoid fancy cross-site POSTs (and GETs!)
- ✓ JSON & XML are OK
- ✓ JavaScript & HTML are bad
- ✓ Base64 “obfuscation” is useless



HTTPS Enhancements

- ✓ Automatic or manual cookie management (against “Cookie Monster” attacks on badly implemented HTTPS sites)
- ✓ HTTPS enforcing
- ✓ HTTPS-dependent permissions (with TOR-specific setting)



HTTPS Enhancements

Trivia

EFF's HTTPS Everywhere mostly reuses
NoScript's HTTPS enforcing code



HTTPS Enhancements

Developer Advices

- ✓ Avoid bouncing back user to HTTP
- ✓ Use HSTS



Application Boundaries Enforcer (ABE)

- ✓ A Web Application Firewall in a browser
- ✓ The advantage of more context (e.g. origin or DOM)
- ✓ Anti-CSRF
- ✓ Resistant to DNS-rebinding
- ✓ Default rule to block cross-zone request, protects LAN and local resources such as SOHO firewalls
- ✓ noscript.net/abe



Application Boundaries Enforcer (ABE)

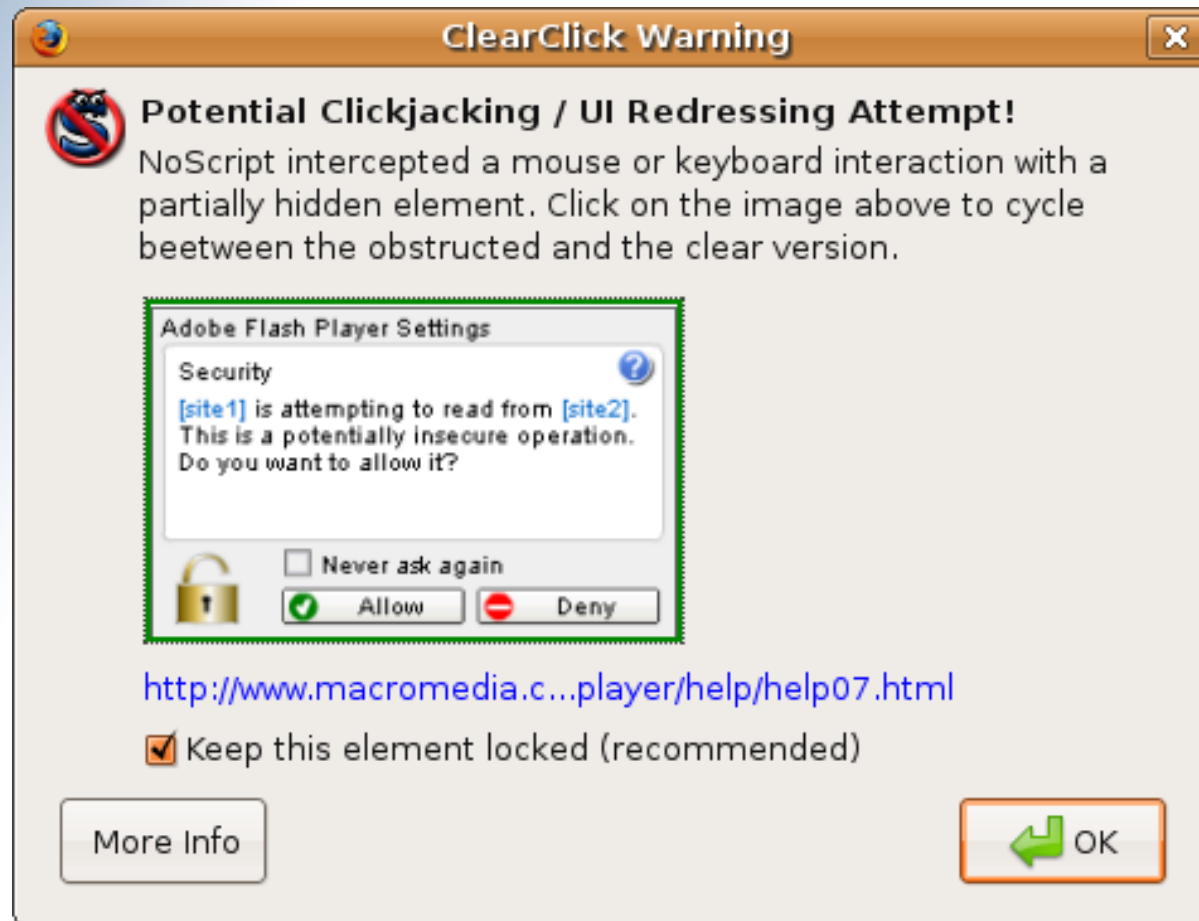
Developer Advices

- ✓ Experiment protecting your own applications
- ✓ Avoid “hotel Wi-Fi” nightmare setups
- ✓ Live without cross-zone requests



ClearClick

the ClickJacking Killer



ClearClick

the ClickJacking Killer

- ✓ Based on screenshots comparison
- ✓ Additional countermeasures against timing attacks
- ✓ Additional cursorjacking protection
- ✓ Built-in false positive reporting facility



ClearClick

the ClickJacking Killer

Developer Advices

- ✓ Alert your gfx/front-end people
- ✓ Avoid cross-site content overlapping
- ✓ Be careful with CSS filters/translucency on frames



~~ClearClick~~ UI Security

coming soon to a browser near you

- ✓ On its way to standardization by the W3C's Web Applications Security Work Group
- ✓ www.w3.org/TR/UISecurity/ (working draft)
- ✓ Extends CSP
- ✓ Opt-in from the embedded content
- ✓ Includes a *frame-options* directive and a reporting-only mode



Future Plans

- ✓ Merging Android and desktop versions
- ✓ Hacking Blink to make a serious NoScript Chrome viable
- ✓ Hacking Firefox OS to make any browser extension (and therefore NoScript) viable
- ✓ NoScript Enterprise Edition



Engagement Rules

- ✓ Use noscript.net/forum for usability bug reports, RFEs and general discussions
- ✓ Use private email for any security-sensitive report: anything causing a mismatch between NoScript users' security expectations and reality
- ✓ Please **use PGP to encrypt all your security reports**
- ✓ Avoid reporting on Facebook, Twitter & C.!



Questions?



Thank You!

- ✓ giorgio@maone.net
- ✓ hackademix.net
- ✓ [@ma1](#)
- ✓ noscript.net

