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
✔ ...

Frenemies: NoScript for Web Developers - #ns4dev
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)
Frenemies: NoScript for Web Developers - ns4dev
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)
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, dropdown menus, submit buttons, redirections)

✔ Framebusting emulation

✔ Forcing <NOSCRIPト> 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

...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

Potential Clickjacking / UI Redressing Attempt!
NoScript intercepted a mouse or keyboard interaction with a partially hidden element. Click on the image above to cycle between the obstructed and the clear version.

Adobe Flash Player Settings
Security
[site1] is attempting to read from [site2]. This is a potentially insecure operation. Do you want to allow it?

- Never ask again
- Allow
- Deny

http://www.macromedia.com/player/help/help07.html

Keep this element locked (recommended)

More Info  OK
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