Web Security Shorts

Browser Bookmarklets Security

UNIVERSITY of WASHINGTON

Browser bookmarklet security

- What are bookmarklets?
- How do they work?
- Why use them?
- What is the concern?
- How to use bookmarklets wisely?
- Bookmarklets and content-security-policy

What are bookmarklets?

- a browser bookmark that adds functionality to a page by inserting JavaScript
- also known as favelets

How do they work?

- created like a standard bookmark
- but instead of *http:* prefixing the location field, *javascript:* is used and custom script inserted
- bookmarklets are scoped to the active page unlike extensions that can access browser features
- the user creates/installs and controls initiation

Why use them?

- easy way for a user to add custom functionality to a page
- easy way for third parties to offer some functionality without the overhead of creating an extension
- demo

What is the concern?

- the browser will treat a bookmarklet as a trusted source and will execute its script
- 3rd-party bookmarklets may contain malicious code working behind the scenes. For example, code that
  - transmits session tokens, passwords, sensitive information to an attacker's site
  - implements redirection
  - manipulates content in undesired way

Using 3rd-party bookmarklets wisely - 1 of 2

- only use bookmarklets from a trustworthy source (brand or developer)
- ensure the site offering the bookmarklet is not a phishing site impersonating the trustworthy source

Using 3rd-party bookmarklets wisely - 2 of 2

- If there is a code repo, is it maintained and updated regularly and recently?
- If you are a developer, evaluate the code itself - is it doing what you expect it will do?
- Once installed, refrain from activating 3rd-party bookmarklets on pages with sensitive information

What about content-security-policy?

- Content Security Policy (CSP) adds a layer of security via the configuration of content-security-policy HTTP header enabled on the web server
- So can owners of sites with sensitive data use CSP to block bookmarklets, specifically preventing inline scripts thru the script-src directive? ....

Bookmarklets and content-security-policy

- Impact of CSP script-src directive on bookmarklets a mix - the specs discourage browsers from enforcing compliance on bookmarklets
- "Policy enforced on a resource SHOULD NOT interfere with the operation of user-agent features like addons, extensions, or bookmarklets. These kinds of features generally advance the user's priority over page authors, as espoused in [HTML-DESIGN]." https://www.w3.org/TR/CSP3/#extensions
- But some browsers will enforce compliance so there is inconsistent behaviour out there

Further reading and references

- Wikipedia bookmarklet article
- Creating a bookmarklet
- CSP: specs
- CSP: script-src

Thanks!

Peter Giles
gilesp@uw.edu

Pete Graff
pgraff@uw.edu

Jeane Marty
jeanem@uw.edu