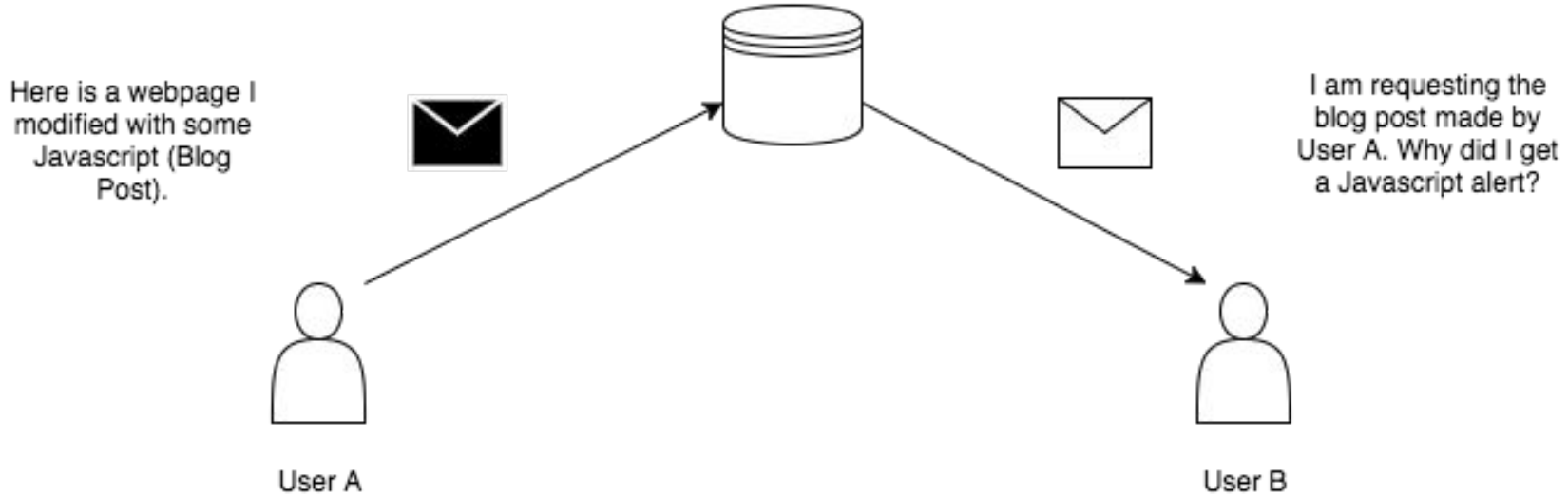
Web Security Primer - XSS

An Antiquated Example

Joseph Parker Diamond
HackUTK
Fall 2016

The Premise

- Cross-site scripting or “XSS” is a web vulnerability where Javascript from a end-user is passed through a website to another end-user.
- A Diagram



The Premise

- A client’s web browser does not always distinguish between what “should” be within a comment field and valid HTML.
- If the web server does not want HTML in comments, it should be the one sanitizing inputs!
- But, relying on ***other*** people to be secure is a dangerous game...

A Simple Example

- Consider Google’s Gruyere vulnerable web app -- it is a practice/testing ground for web application penetration testing
- It contains a place to post “snippets” that are supplied by end users.
- It seems that <script> tags are not escaped/poorly stripped...

Demo Time!

Follow along at: https://google-gruyere.appspot.com/

You may need to use an older browser, enable pop-ups, and/or disable some protections (your browser tries to protect you a fair bit)

The Bottom Line

Yes, pop-ups are annoying, but is that the extent of the danger? No.

XSS can possibly:

- Steal Session Cookies
- Access Stored Passwords
- Rewrite HTML on the Page
- Etc (hackers use their imagination)

Obviously, this is bad -- sanitize your inputs.

Countermeasures

- Tag stripping -- Usually a variant of “strip_tags(string data)” for languages
- Escape non-letter characters in data, use various encoding schemes properly
- Cheat-Sheets:
  - https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet
  - https://www.owasp.org/index.php/DOM_based_XSS_Prevention_Cheat_Sheet