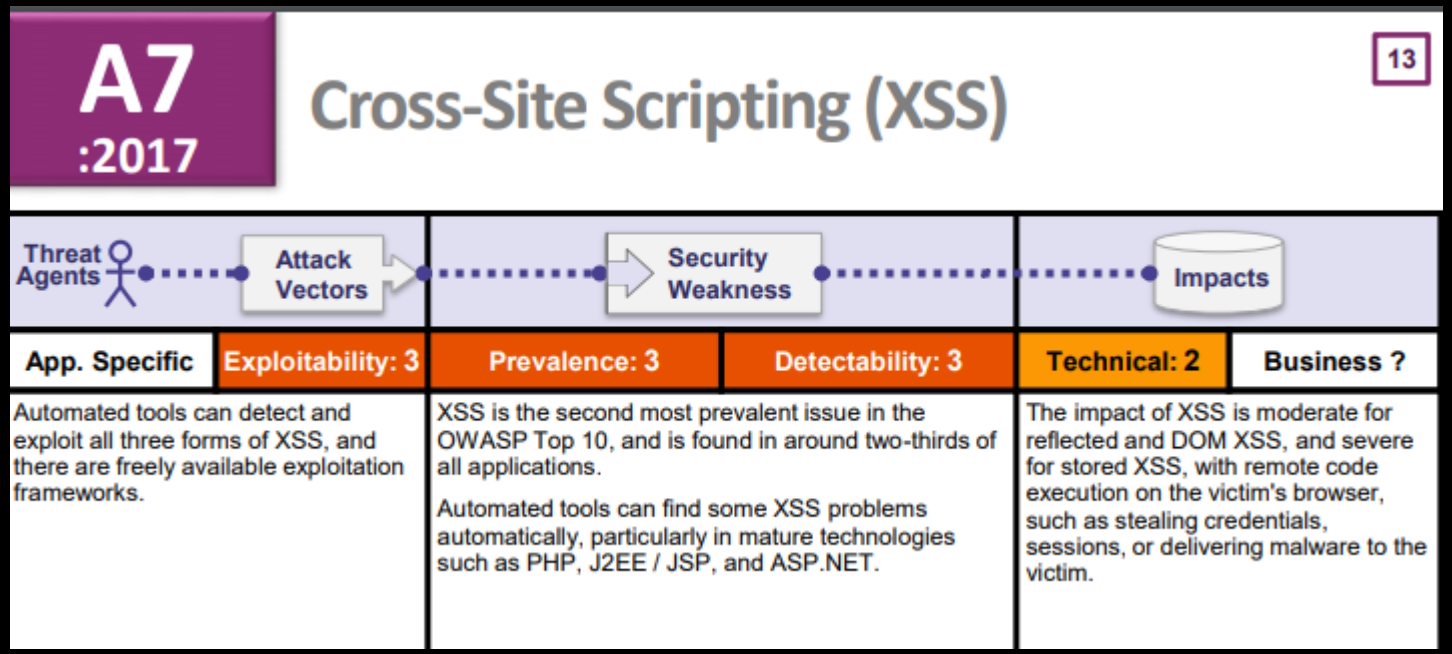
Blind Cross-Site-Scripting

WaffleJS – November 6th 2019

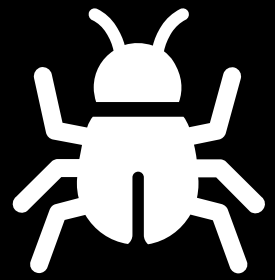
I’m Interested In:

I Like:

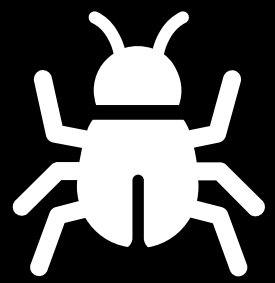
I Love:



https://github.com/OWASP/Top10

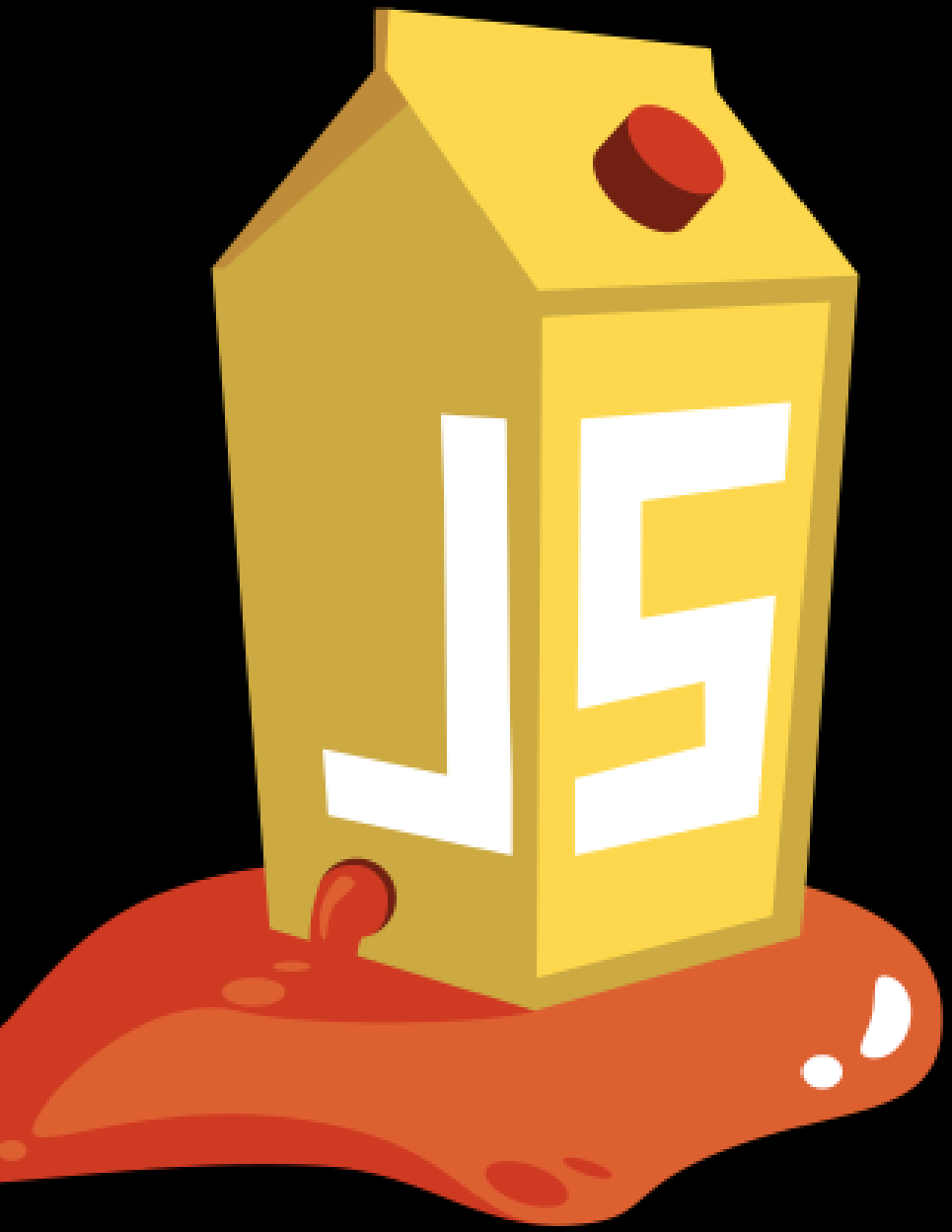


Cross-Site-Scripting (XSS) Is When User-Input Is Interpreted As Code In The Browser



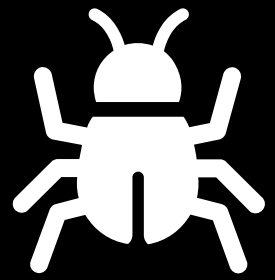
Blind Cross-Site-Scripting (bXSS) Is When User-Input Is Interpreted As Code In The Browser

* Out-Of-Band (OOB)

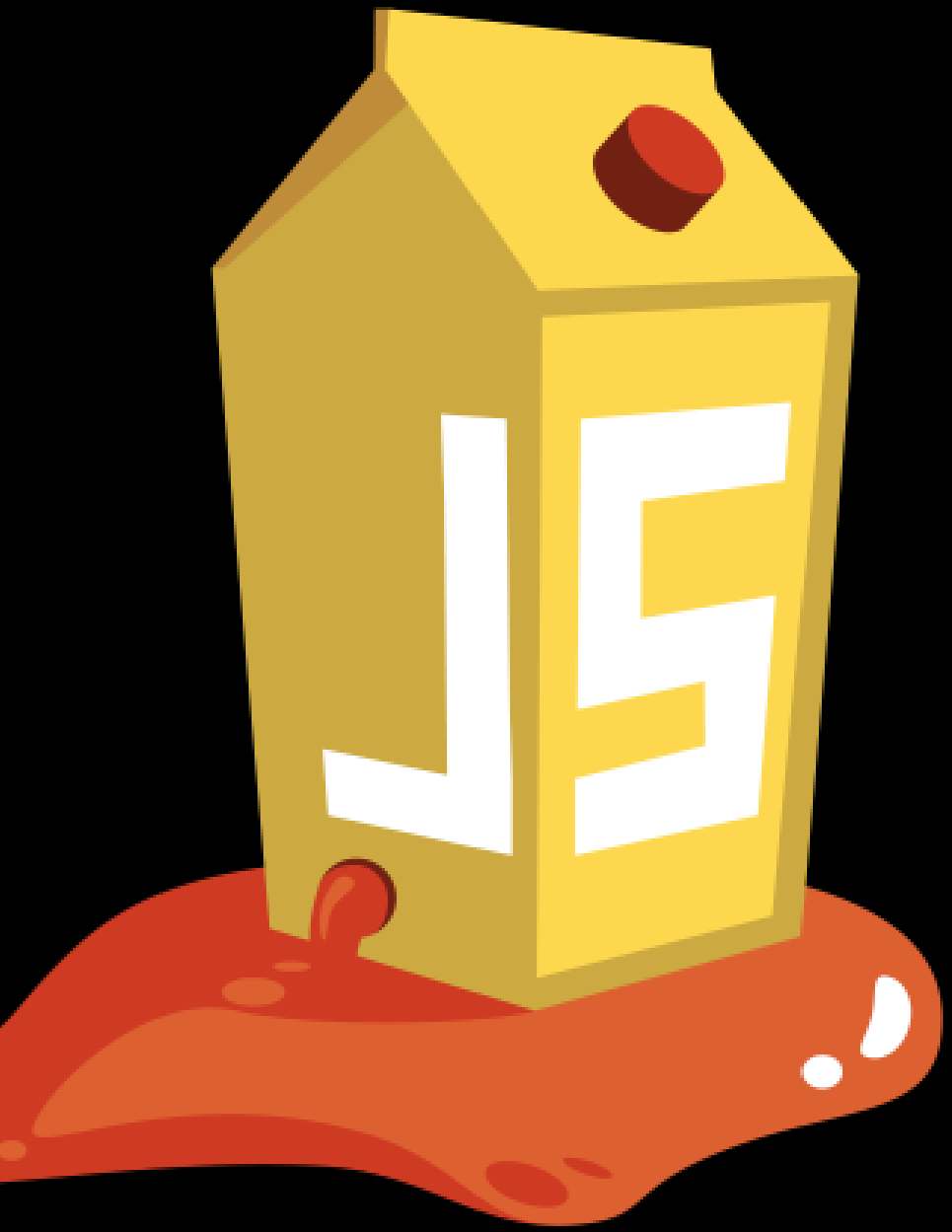


Setting The Scene:

- I run a website that sells juice (Juice Shop)
- This website allows for Users to register
- Only admins can see the registered users in /administration
- An attacker tries to XSS their username
- Let’s see if they succeed…

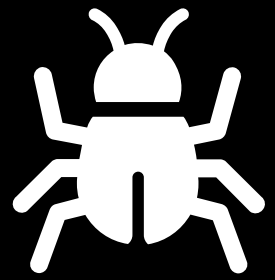


Demo



bXSS To The Rescue!

- The attacker could not see that their payload fired ☹
- This is because it happens OOB
- We need to find a way to alert the attacker to say the payload has been rendered, common ways:
  - Use an img
  - Load external JavaScript
  - Redirect via location.href
- Let’s look at popular utilities to do this for us:



Demo

Resources:

Tools:

- https://xsshunter.com/
- https://github.com/lewisardern/bxss

Reading:

- https://github.com/OWASP/Top10
- https://portswigger.net/web-security/cross-site-scripting/cheat-sheet
- https://ardern.io/2019/06/20/payload-bxss/

Vuln App:

- https://github.com/bkimminich/juice-shop

Thanks!