

# Blind Cross-Site-Scripting

WaffleJS – November 6<sup>th</sup> 2019

I'm Interested In:



I Like:



I Love:



OWASP

Open Web Application  
Security Project

A7

:2017

13

Cross-Site Scripting (XSS)

Threat Agents

Attack Vectors

Security Weakness

Impacts

App. Specific

Exploitability: 3

Prevalence: 3

Detectability: 3

Technical: 2

Business ?

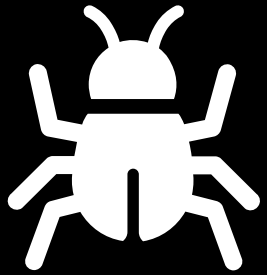
Automated tools can detect and exploit all three forms of XSS, and there are freely available exploitation frameworks.

XSS is the second most prevalent issue in the OWASP Top 10, and is found in around two-thirds of all applications.

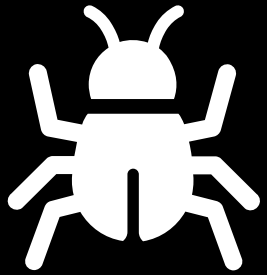
Automated tools can find some XSS problems automatically, particularly in mature technologies such as PHP, J2EE / JSP, and ASP.NET.

The impact of XSS is moderate for reflected and DOM XSS, and severe for stored XSS, with remote code execution on the victim's browser, such as stealing credentials, sessions, or delivering malware to the victim.

<https://github.com/OWASP/Top10>

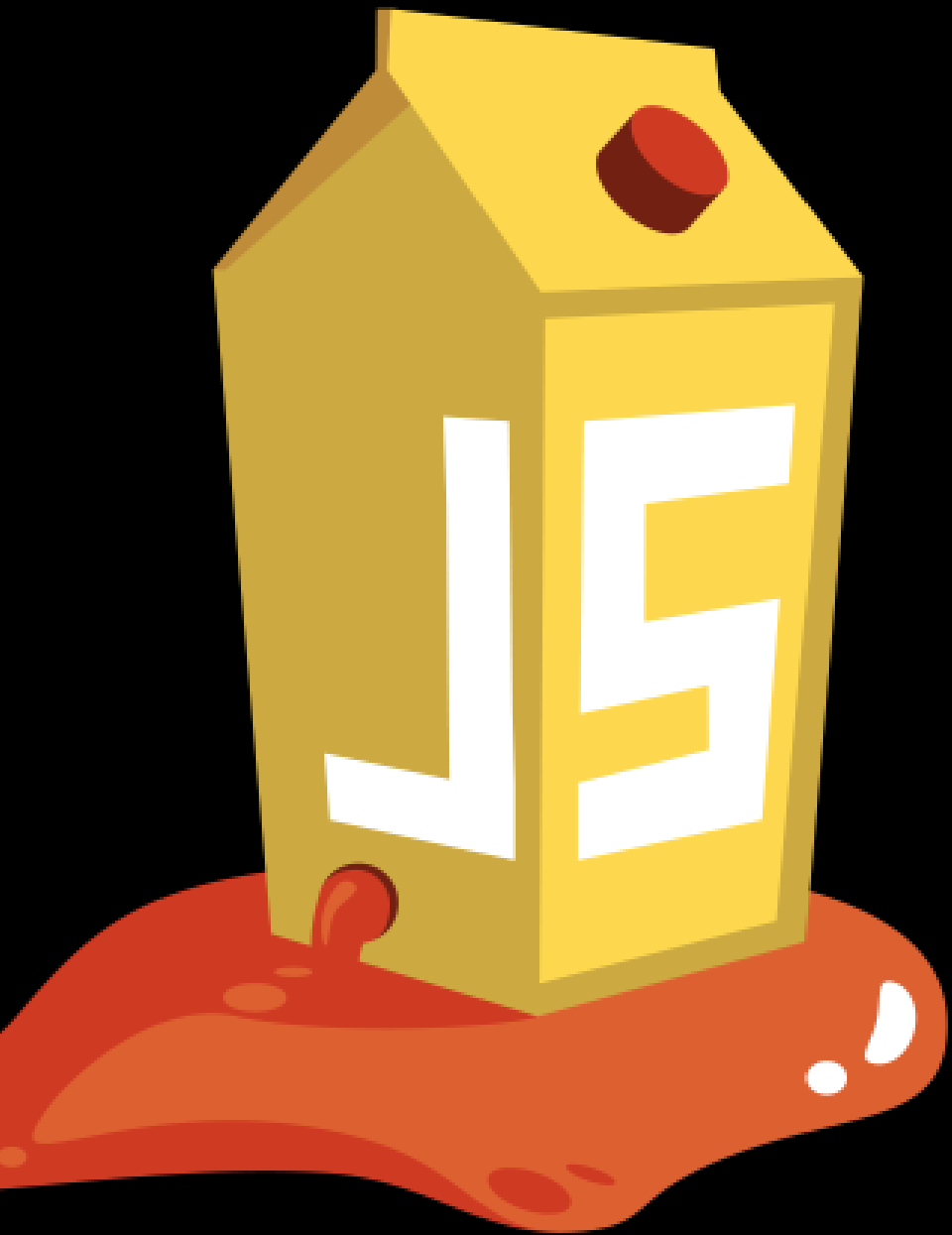


Cross-Site-Scripting (XSS) Is When  
User-Input Is Interpreted As Code In  
The Browser



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

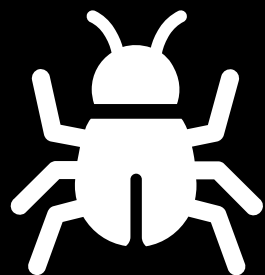
\* Out-Of-Band (OOB)



# Setting The Scene:

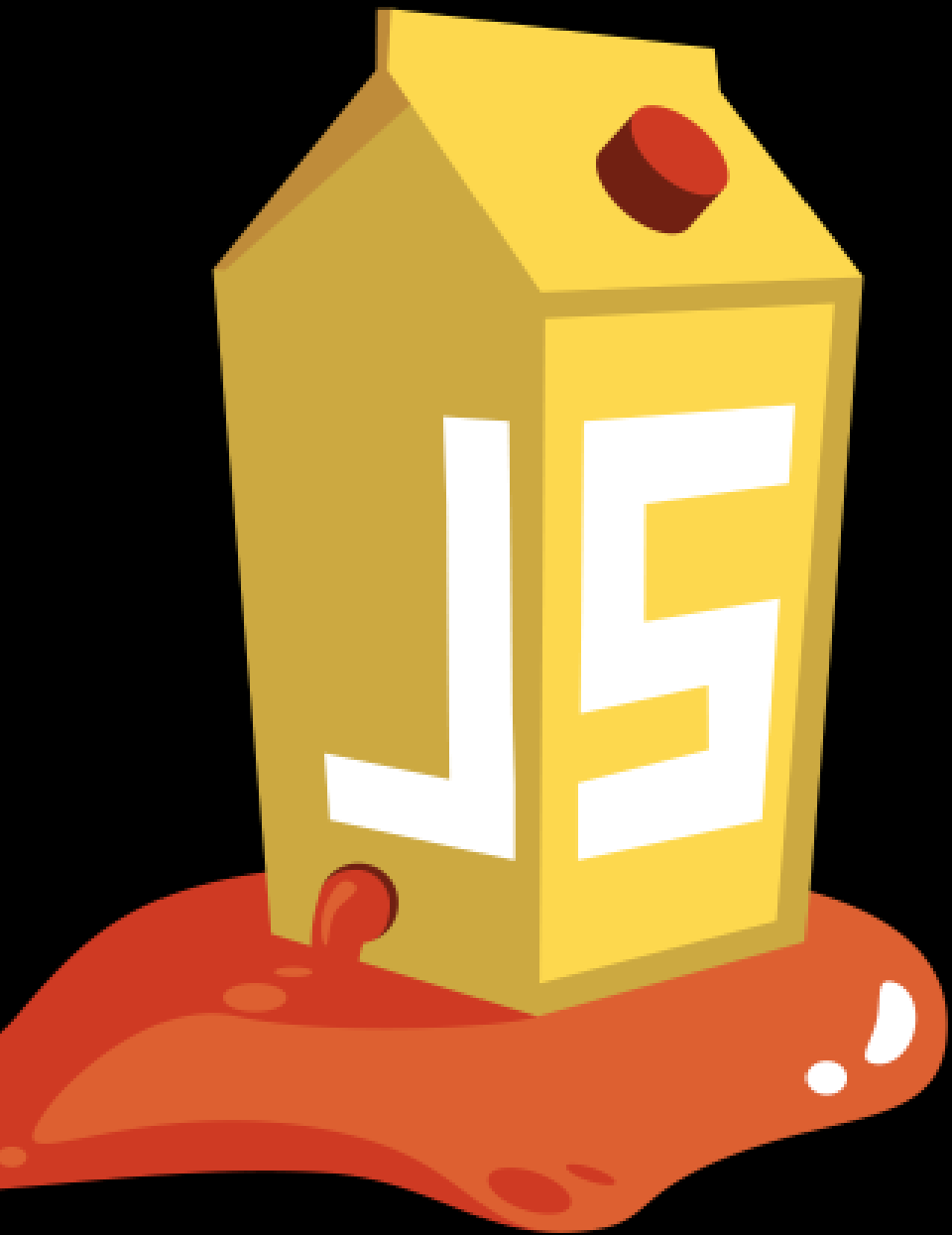
---

- 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...



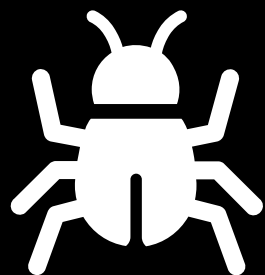
Demo





# 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!