OMU
HACKERS

/dmuhackers

@dmuhackers

DMU HACKERS

XSS & Juice Shop

Disclaimer

Don't do illegal shit

Overview

- Announcements
- XSS
- Juice Shop
- Today's activity

DMU Cyber Week 2021

- 1st - 5th March (Enhancement Week)

- Events:
  - Nettitude Red Team CTF,
  - Datathon Competition,
  - DMU CYRAN Red V Blue Exercise,
  - Prof. Allan Cook: “Practice Makes Perfect: Preparing and rehearsing for a cyber incident before it happens

- Register at: http://bit.ly/eventbriteDMUCyberWeek

Bellingcat

- “Bellingcat is an independent international collective of researchers, investigators and citizen journalists using open source and social media investigation to probe a variety of subjects”
- 11th March, 6-7pm in usual session time.
- Hosted here on discord
- Register interest on the DMU Hackers FB page event

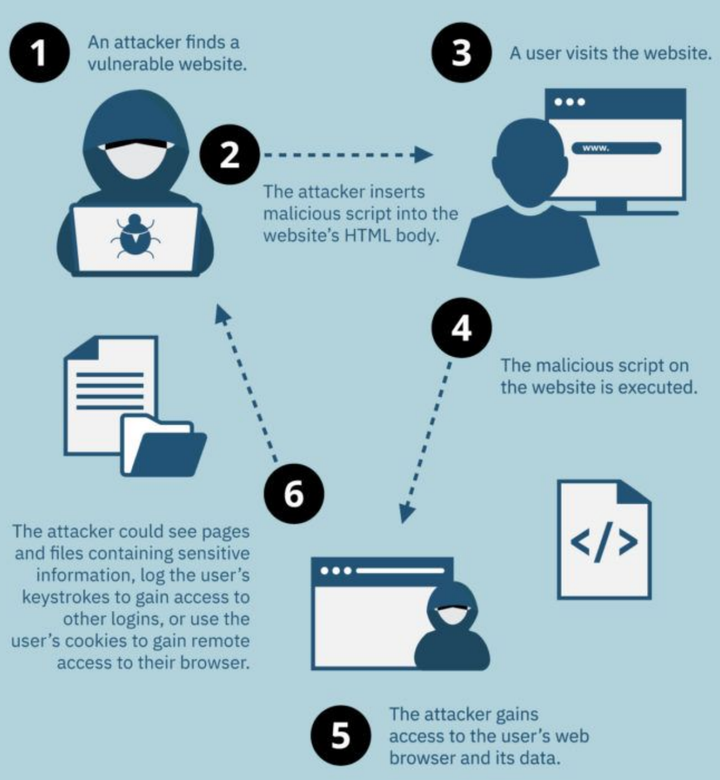
We want to hear from you!

What is XSS?

- Cross-site scripting - an OWASP top 10 vulnerability

- XSS attacks occur when
    - Data enters a web app via an untrusted source, likely through a web request
    - Data is included in dynamic content sent to a user - without being checked/cleared for malicious content
- Malicious content sent to a web browser is often JavaScript, but could be HTML, Flash, or other browser executable code.

Continued: What is XSS?

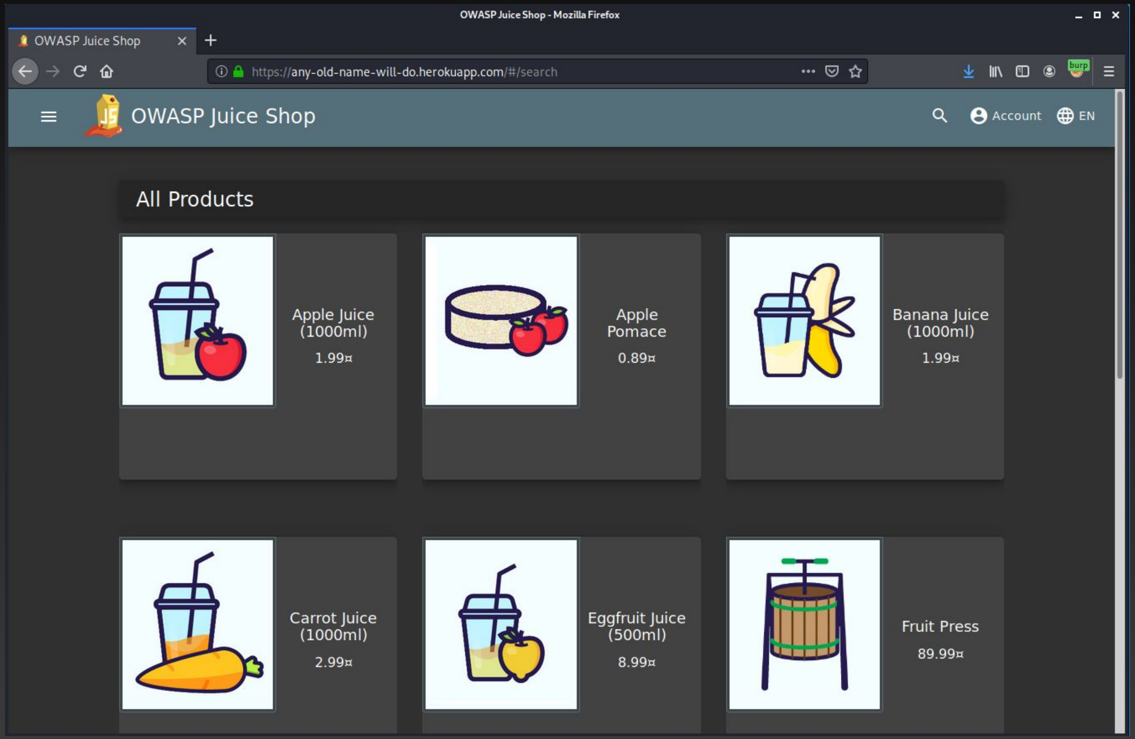

1
An attacker finds a vulnerable website.
2
The attacker inserts malicious script into the website's HTML body.
3
A user visits the website.
www.
4
The malicious script on the website is executed.
5
The attacker gains access to the user's web browser and its data.
6
The attacker could see pages and files containing sensitive information, log the user's keystrokes to gain access to other logins, or use the user's cookies to gain remote access to their browser.
</>

3 main types:

- Reflected XSS, where the malicious script comes from the current HTTP request.
- Stored XSS, where the malicious script comes from the website's database.
- DOM-based XSS, where the vulnerability exists in client-side code rather than server-side code.

What was Juice Shop again?

- From the OWASP Foundation (Open Web Application Security Project)
- An insecure web application for security training, awareness demos, CTFs, and for testing security tools.
- Contains many real-world vulnerabilities, including the OWASP top 10 (i.e. SQLi and XSS)
- Can host through a browser using a free heroku account
- Find more at -
  - Juice Shop:
    - https://owasp.org/www-project-juice-shop/
  - OWASP:
    - https://owasp.org/



OWASP Juice Shop - Mozilla Firefox

OWASP Juice Shop

https://any-old-name-will-do.herokuapp.com/#/search

OWASP Juice Shop

All Products

Apple Juice (1000ml) 1.99¤

Apple Pomace 0.89¤

Banana Juice (1000ml) 1.99¤

Carrot Juice (1000ml) 2.99¤

Eggfruit Juice (500ml) 8.99¤

Fruit Press 89.99¤

Today's activity

Juice Shop XSS challenges:
http://bit.ly/XSSandJuiceShop