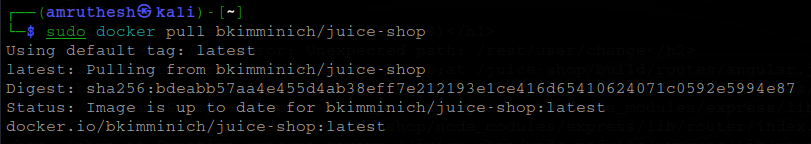
Amruthesh - 241059041

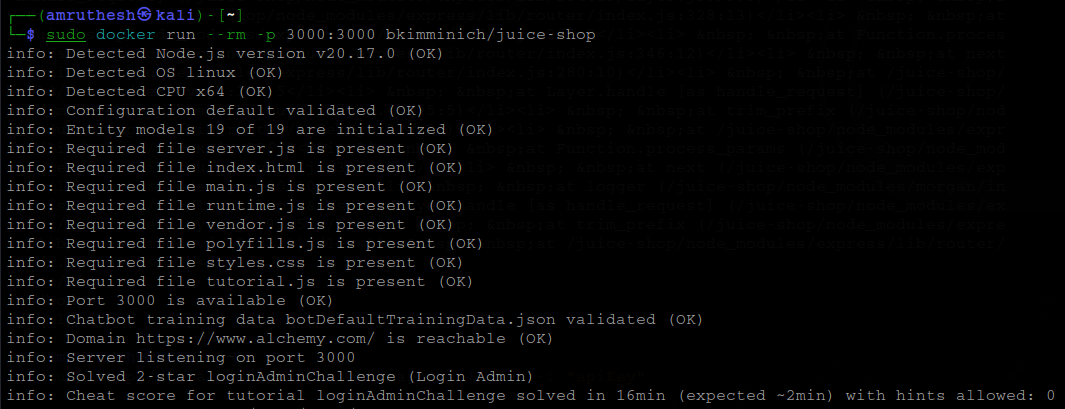
Cybersecuirty  MSIS

Juiceshop lab internals

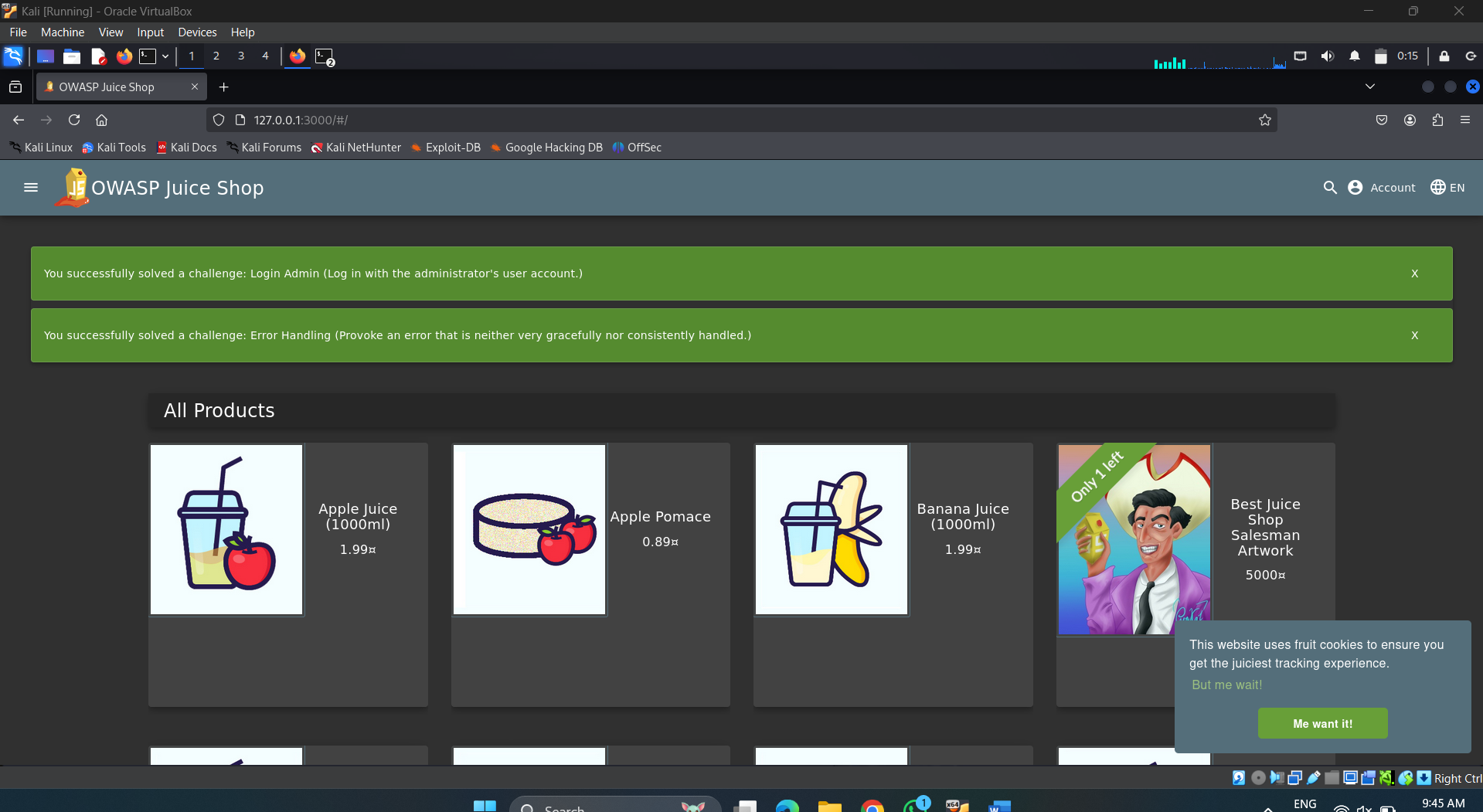
**Pull JuiceShop through Docker**

****

**Run the JuiceShop**

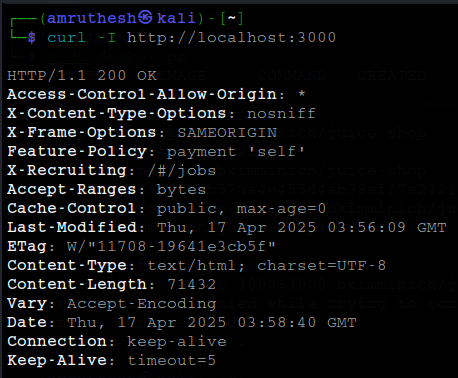
****

**Open it in the Browser**

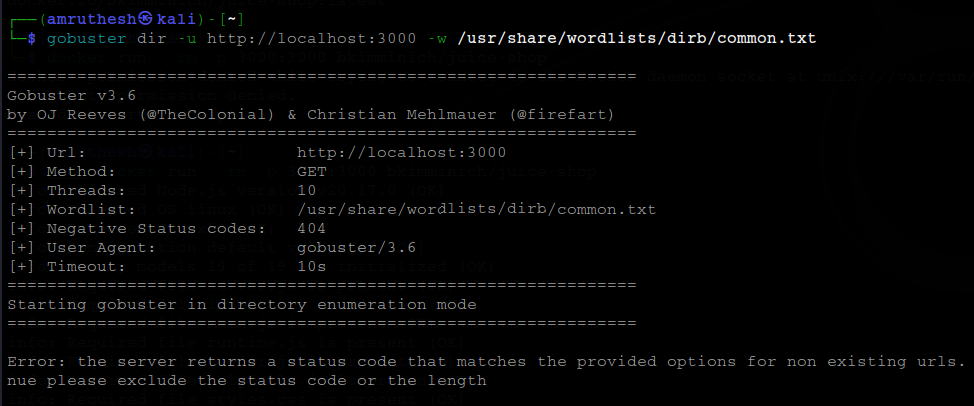
****

**Information Gathering (Reconnaissance) on Juice Shop**

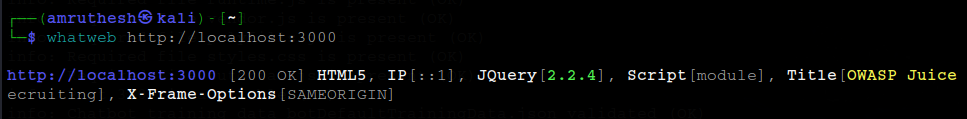
**Banner Grabbing**

****

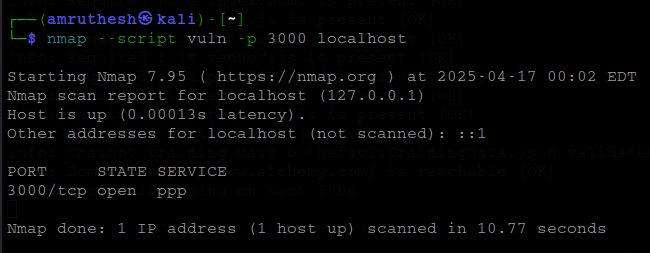
**Directory and File Enumeration**

****

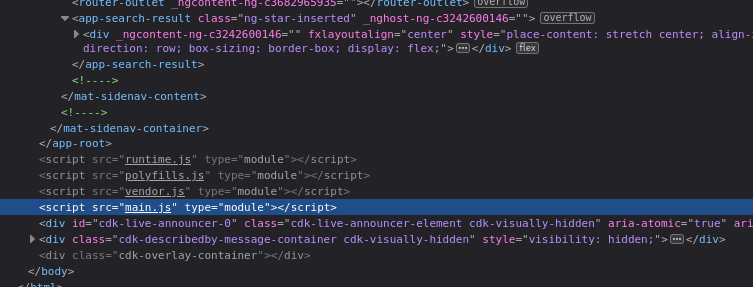
**Identify Technologies Used**

****

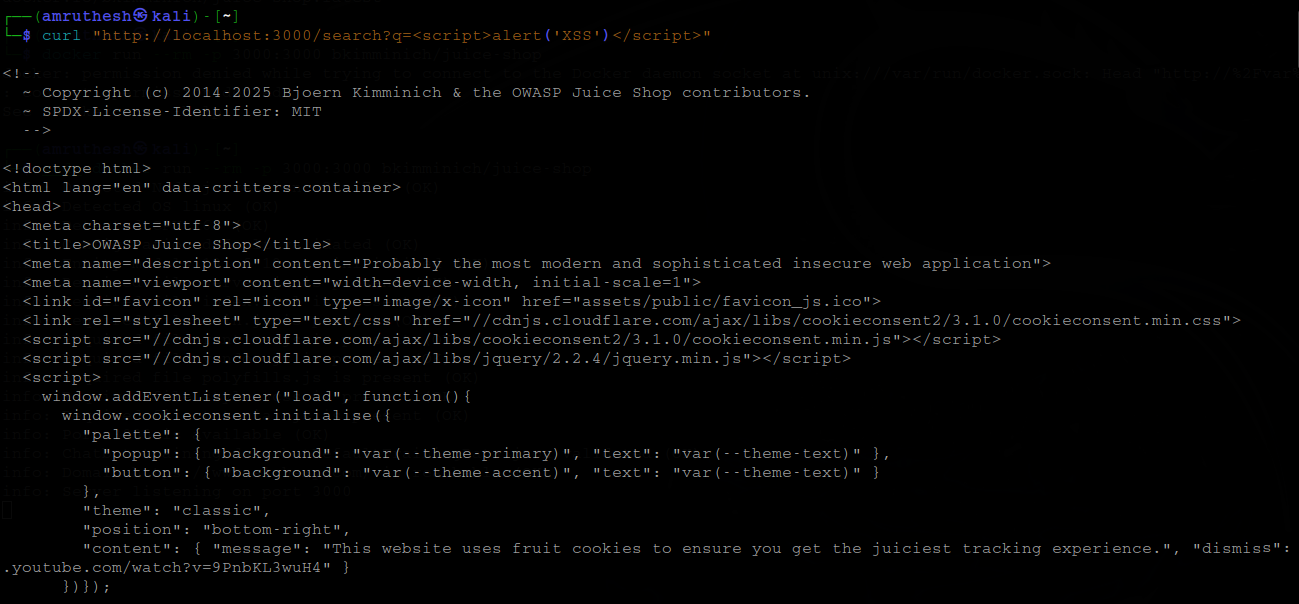
**Vulnerability Scan (using Nmap scripts):**

****

**Gather info from inspect element**

****

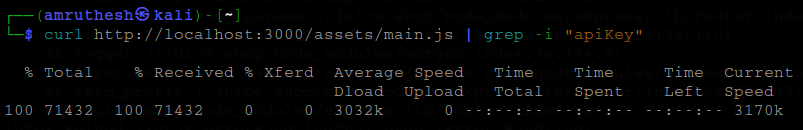
**Web Server Vulnerabilities in Juice Shop  
Cross-Site Scripting (XSS)**

****

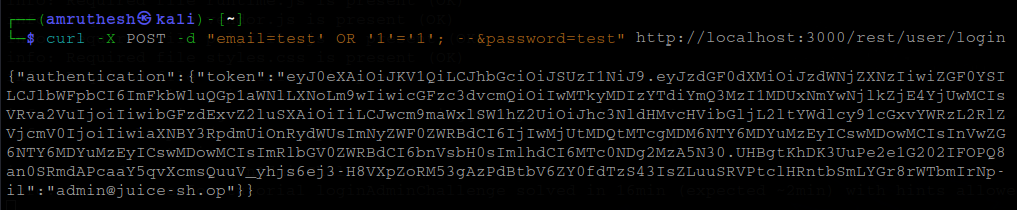
**Cross-Site Request Forgery (CSRF)**

****

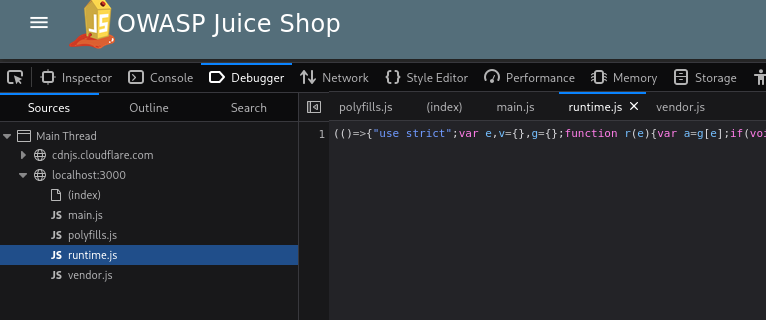
**Sensitive Information in URLs or JavaScript Files**

****

**SQL Injection (SQLi)**

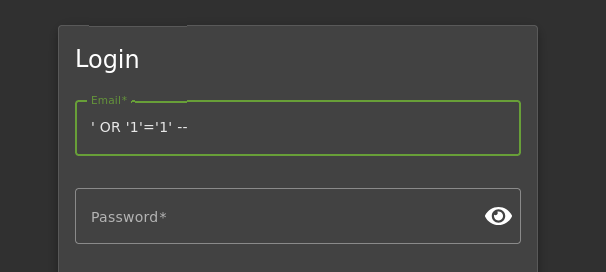
****

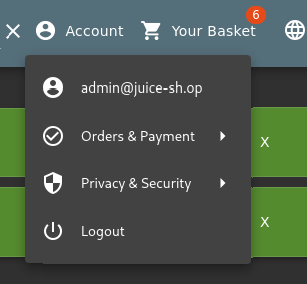
**Easily Accessible JS/Config files**

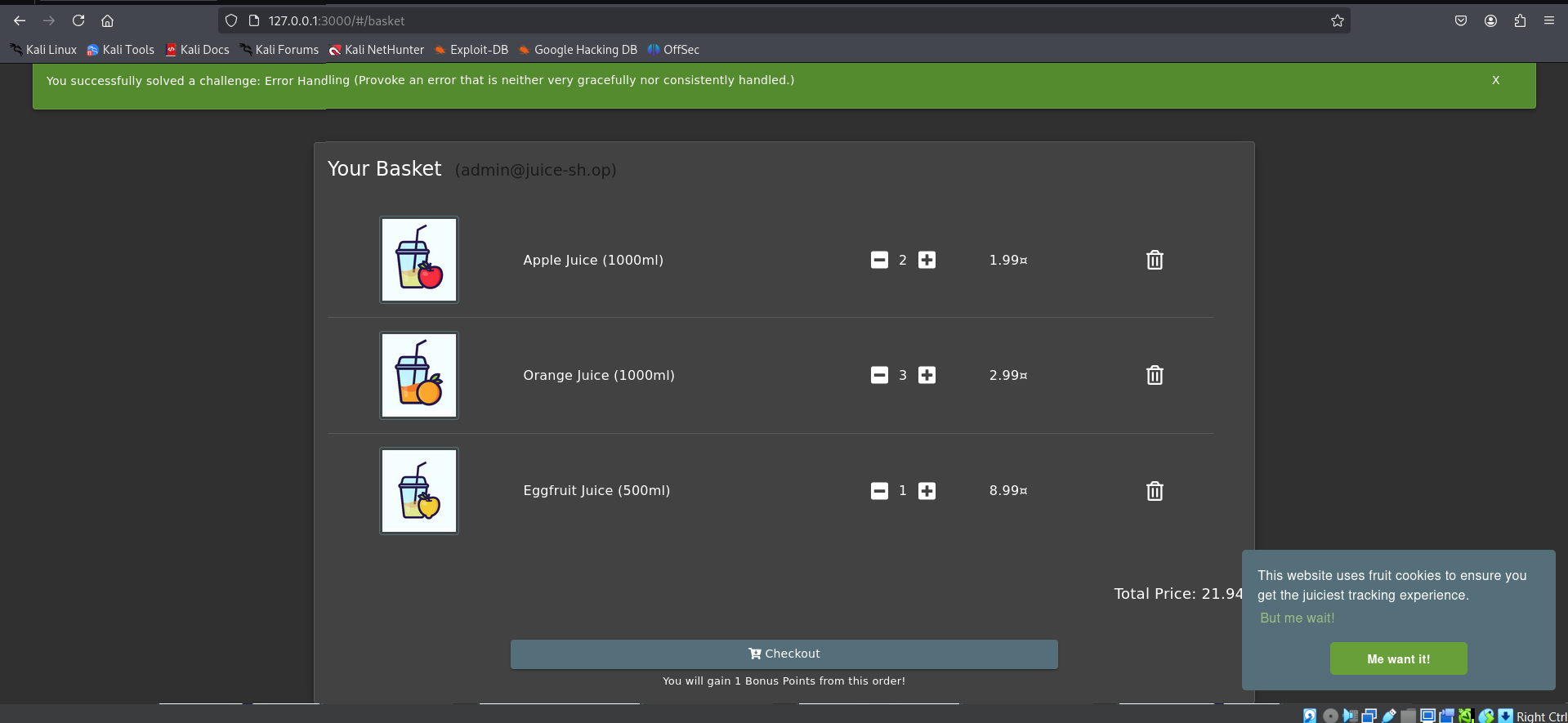
****

**Exploits / Payloads on Juice Shop**

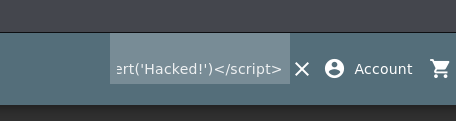
**SQL Injection (Login Bypass)**

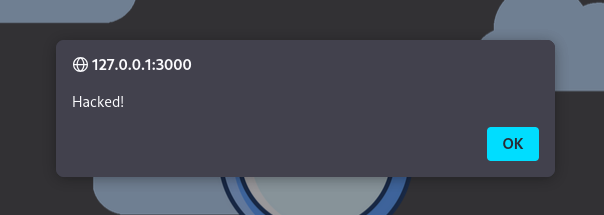
****

****

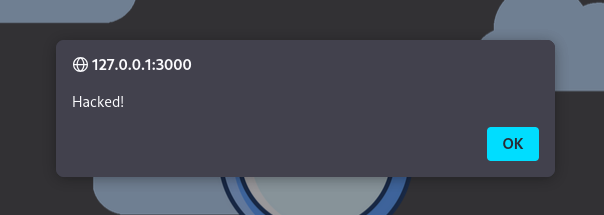
****

**Reflected XSS in Search Bar**

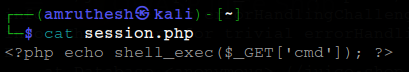
****

****

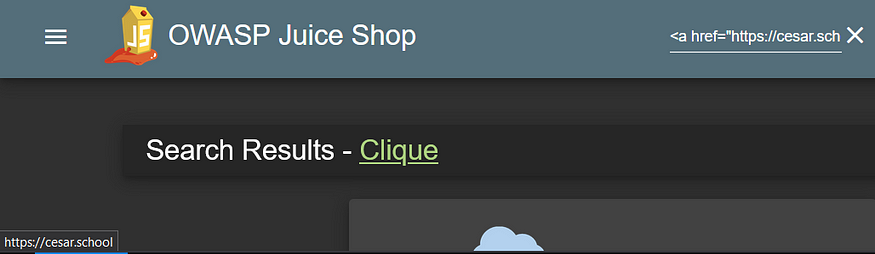
**Try Different Variations of XSS Payloads**

****

**Exploiting Insecure File Upload**

****

**Simple Redirect Link**

****