State of The Art

1. What did others?

A considerable number of vulnerable web applications already existed before the Juice Shop was created. When Juice Shop came to life there were only server-side rendered applications. But Rich Internet Application (RIA) or Single Page Application (SPA) style applications were already a commodity at that time. Juice Shop was meant to fill that gap. Many of the existing vulnerable web applications were very rudimental in their functional scope. So, the aim of the Juice Shop also was to give the impression of a functionally complete e-commerce application that could actually exist like this in the wild, because it is written entirely in JavaScript (Node.js, Express, Angular), while the others (BWAPP, DVWA, Mutillidae II) are written in PHP.

2. Names in the field

The OWASP Juice Shop has been created by **Björn Kimminich** and is developed, maintained and translated by a team of volunteers.

With more than 10 years of experience in security consulting, **Dafydd Stuttard** specializes in the penetration testing of web applications. His interests include developing tools to facilitate all kinds of software security testing. Under the alias “PortSwigger,” Dafydd created the popular Burp Suite of web application hacking tools; he continues to work actively on Burp’s development.

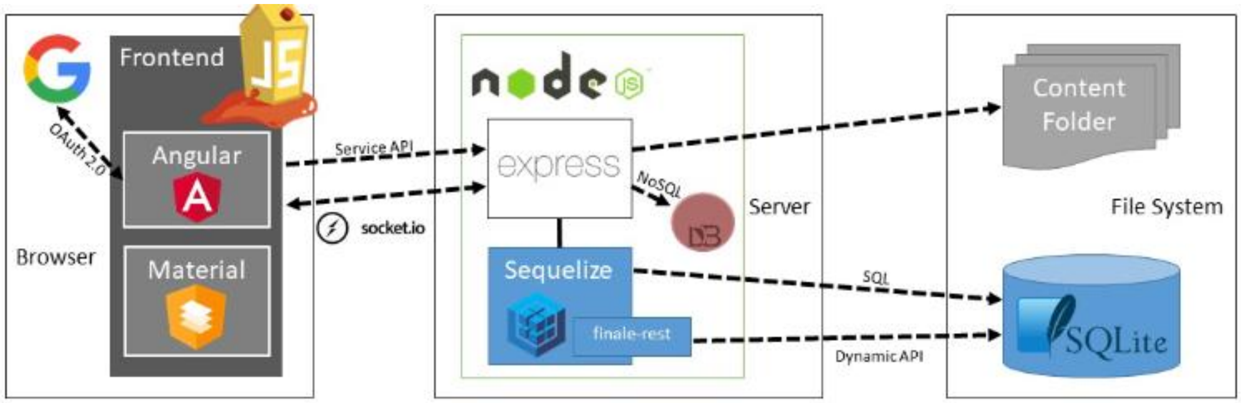
Marcus Pinto is cofounder of MDSec, developing and delivering training courses in web application security. Marcus has 11 years of experience in attack-based security assessment and penetration testing. He has worked extensively with large-scale web application deployments in the financial services industry. Marcus has been developing and presenting database and web application training courses since 2005 at Black Hat and other worldwide security conferences, and for private-sector and government clients.

Simon Bennetts also plays an important role in this field because he is the creator of the world's most popular application security scanner. ZAP, now part of the OWASP Foundation.

3. Architecture

The OWASP Juice Shop is a pure web application implemented in JavaScript and TypeScript. In the frontend the popular Angular framework is used to create a so-called Single Page Application. The user interface layout is implementing Google's Material Design using Angular Material components. It uses Angular Flex-Layout to achieve responsiveness. JavaScript is also used in the backend as the exclusive programming language: An Express application hosted in a Node.js server delivers the client-side code to the browser. It also provides the necessary backend functionality to the client via a RESTful API. As an underlying database a light-weight SQLite was chosen, because of its file-based nature.

As an additional data store a MarsDB is part of the OWASP Juice Shop. It is a JavaScript derivate of the widely used MongoDB NoSQL database and compatible with most of its query/modify operations. The application also offers convenient user registration via OAuth 2.0 so users can sign in with their Google accounts. The following diagram shows the high-level communication paths between the client, server and data layers:



4. Results

It can be used in security trainings, awareness demos, CTFs and as a guinea pig for security tools! Juice Shop encompasses vulnerabilities from the entire OWASP Top Ten along with many other security flaws found in real-world applications!

5. Methodology

We will use the Juice Shop OWASP to show how important it is to be aware of the web application vulnerabilities.

The following methodology, in this research, is used to determine the degree of security in web application servers involving the following steps. First, we will scan through the websites of each targeted destination and list all found vulnerabilities. Then, we will segregate the found vulnerabilities into three types according to their degree of severity, namely: High, Medium, Low. Finally, each type of vulnerability will be presented on a web application.

6. Related Articles and books

Dafydd Stuttard, Marcus Pinto, *The Web Application Hacker's Handbook - Finding and Exploiting Security Flaws*, 2nd Edition, John Wiley & Sons, 2011

https://portswigger.net/web-security

https://www.researchgate.net/publication/283180137_Systematic_Review_of_Web_Application_Security_Vulnerabilities_Detection_Methods

https://owasp.org/www-project-top-ten/

https://www.acunetix.com/websitesecurity/sql-injection/

https://www.indusface.com/blog/owasp-top-10-mitigation-techniques/

7. Resources and tools

The following tools and tehnology will help us in identifying vulnerabilities in Juice Shop:

- Python 3
- Kali Linux
- Burpsuite
- ZAP
- Hydra
- John the Ripper
- Hashcat
- W3af
- SQLMap
- Retire JS