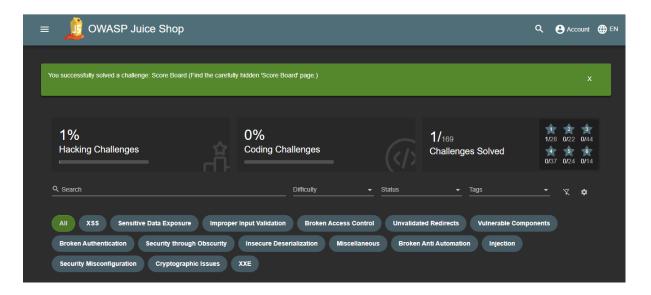
# Report - Owasp juice-shop

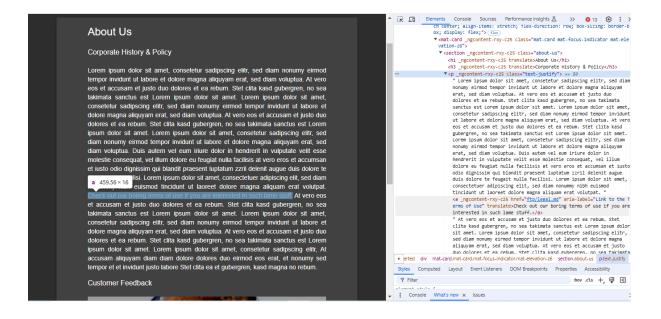
Hamma Abdessamad - GL

### Scoreboard, sensitive data exposure:

The scoreboard offers a clear view of completed and remaining challenges, allowing for efficient tracking of progress made.



The "About Us" page presents the Juice Shop team with their photos and respective roles in the company. When examining the HTML source code of this page, an interesting reference to the /ftp directory can be discovered.



The exploration of the /ftp directory reveals access to two confidential documents: legal.md and acquisitions.md. These files are directly accessible by manipulating the URL

juice-shop-330813791524.us-central1.run.app/ftp/acquisitions.md

- # Planned Acquisitions
- > This document is confidential! Do not distribute!

Our company plans to acquire several competitors within the next year. This will have a significant stock market impact as we will elaborate in detail in the following paragraph:

Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.

Our shareholders will be excited. It's true. No fake news.

← → C

juice-shop-330813791524.us-central1.run.app/ftp/legal.md

#### # Legal Information

Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.

Duis autem vel eum iriure dolor in hendrerit in vulputate velit esse molestie consequat, vel illum dolore eu feugiat nulla facilisis at vero eros et accumsan et iusto odio dignissim qui blandit praesent luptatum zzril delenit augue duis dolore te feugait nulla facilisi. Lorem ipsum dolor sit amet, consectetuer adipiscing elit, sed diam nonummy nibh euismod tincidunt ut laoreet dolore magna aliquam erat volutpat.

Ut wisi enim ad minim veniam, quis nostrud exerci tation ullamcorper

## <u>Developer file backup</u>:

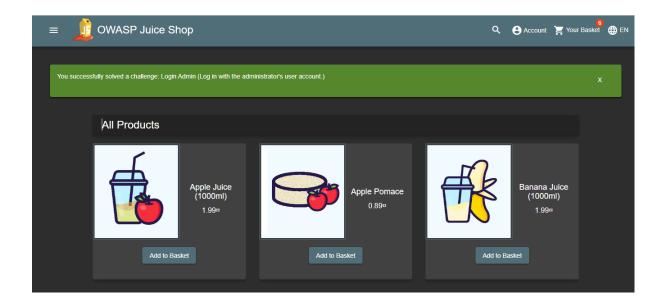
The package json bak file in the /ftp directory appears inaccessible at first, as the application blocks files with sensitive extensions for security reasons. However, by employing URL encoding and adding the null byte sequence (%00) encoded as %25%30%30 at the end of the filename, we can successfully bypass these

restrictions and access the backup file, revealing valuable development configuration details.

```
** package.json.bak%00.md X
C: > Users > User > Downloads > *** package.json.bak%00.md
         "name": "juice-shop",
         "version": "6.2.0-SNAPSHOT",
         "description": "An intentionally insecure JavaScript Web Application",
         "homepage": "http://owasp-juice.shop",
         "author": "Björn Kimminich <bjoern.kimminich@owasp.org> (https://kimminich.de)",
         "contributors": [
           "Björn Kimminich",
           "Jannik Hollenbach",
           "Aashish683",
  10
           "greenkeeper[bot]",
           "MarcRler",
           "agrawalarpit14",
           "Scar26",
           "CaptainFreak",
           "Supratik Das",
           "JuiceShopBot",
           "the-pro",
           "Ziyang Li",
           "aaryan10",
           "m4l1c3",
           "Timo Pagel",
          'private": true,
         "keywords": [
           "web security",
           "web application security",
```

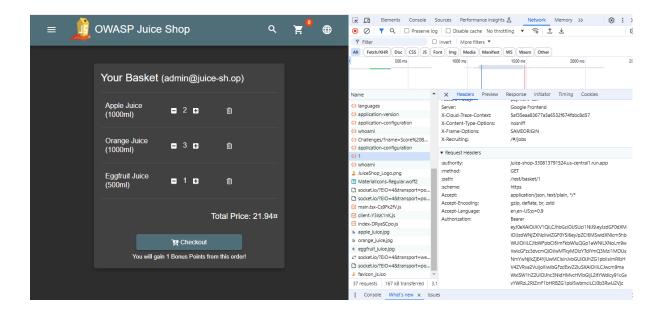
# Injection:

By entering the crafted input "admin' or 1=1 --" in the email field of the login form, a classic SQL injection vulnerability is exploited. This injection works by manipulating the SQL query to always evaluate to true through the 'or 1=1' condition, while the double dash (--) comments out the remaining query logic, effectively bypassing the password verification and granting access to the admin account.

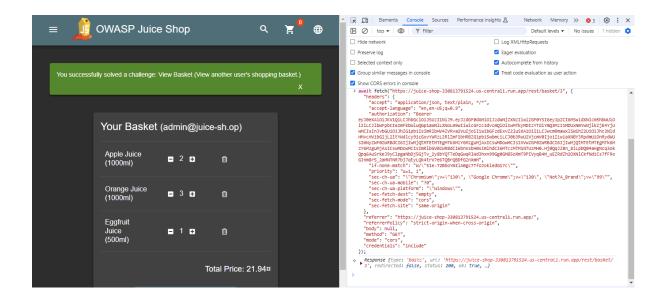


### Broken Access control:

When adding items to the shopping basket, the application sends POST requests containing both the productld and basketld parameters. Through inspection of these requests using the browser's developer tools, the structure of these basket manipulation calls becomes apparent.



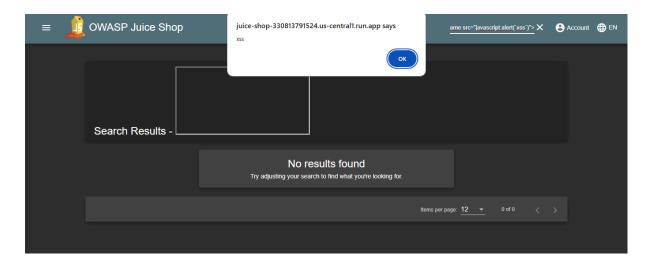
By modifying the basketId parameter in the request to different numerical values, any user can access and manipulate baskets belonging to other customers. This modification can be performed through a simple request parameter change, demonstrating how the application fails to validate basket ownership.



## Other challenges:

#### DOM XSS:

The search functionality in Juice Shop contains a DOM-based Cross-Site Scripting vulnerability, where user input from the search bar is directly injected into the page's HTML without proper sanitization. This allows malicious JavaScript code to be executed in the context of other users' browsing sessions, potentially compromising their interaction with the application.



#### **Bully chatbot:**

The Bully Chatbot challenge in Juice Shop demonstrates a vulnerability in the Support Chat feature where the bot can be manipulated into revealing sensitive information.

