

Week 1: Security Assessment

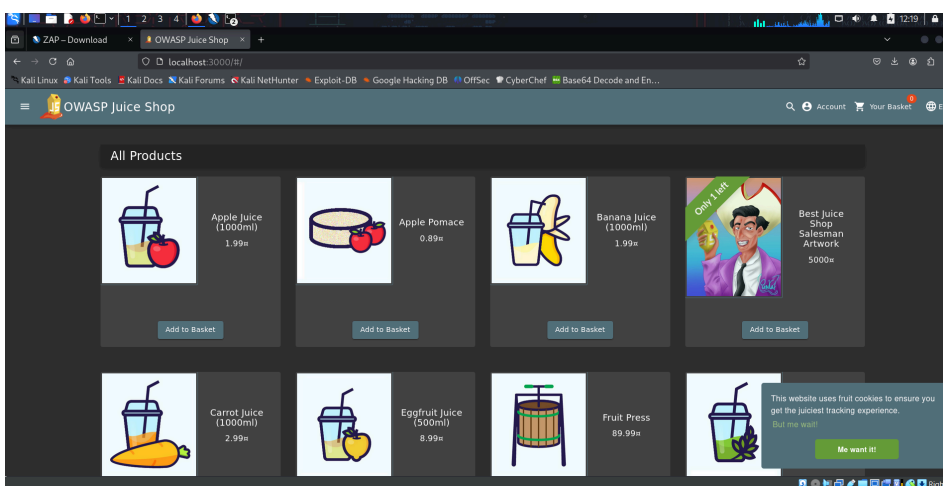
1. Understand the Application

```
(kali㉿kali)-[~/juice-shop]
$ npm start

> juice-shop@19.1.1 start
> node build/app

info: Detected Node.js version v20.19.0 (OK)
info: Detected OS linux (OK)
info: Detected CPU x64 (OK)
info: Configuration default validated (OK)
info: Entity models 20 of 20 are initialized (OK)
info: Required file server.js is present (OK)
info: Required file index.html is present (OK)
info: Required file main.js is present (OK)
info: Required file styles.css is present (OK)
info: Required file tutorial.js is present (OK)
info: Required file runtime.js is present (OK)
info: Required file vendor.js is present (OK)
info: Port 3000 is available (OK)
info: Domain https://www.alchemy.com/ is reachable (OK)
info: Chatbot training data botDefaultTrainingData.json validated (OK)
info: Server listening on port 3000
```

Web application was running locally

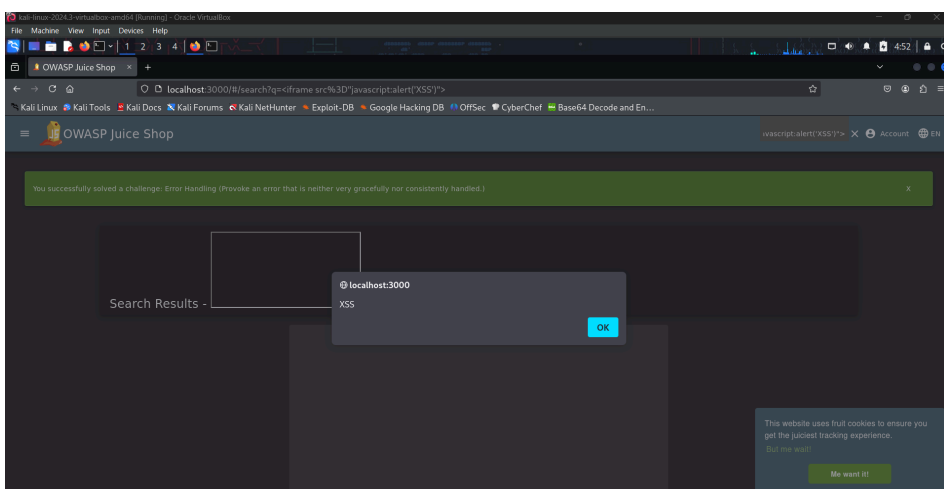


Juice Shop vulnerable web applications

2. Perform Basic Vulnerability Assessment

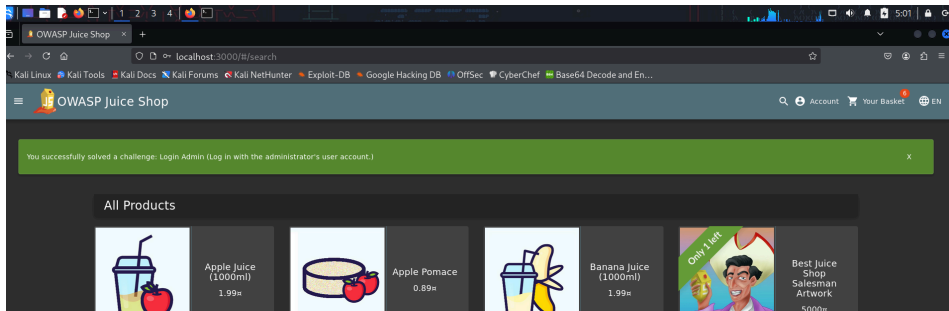
Vulnerabilities Found

- Reflected Cross-Site Scripting (XSS)
 - Location: Search Bar
 - Evidence: Executed `<iframe src="javascript:alert('XSS')">` to trigger a popup.



Note on Payload: The standard `<script>` payload was ineffective because the application inserts user input via `innerHTML`, which browsers do not execute. I successfully exploited the vulnerability using an `<iframe>` payload (`<iframe src="javascript:alert('XSS')">`), which leverages the `src` attribute to force JavaScript execution

- SQL Injection (Authentication Bypass)
 - Location: Login Page (Email Field)
 - Evidence: Logged in as Admin using payload 'OR 1=1 -- .



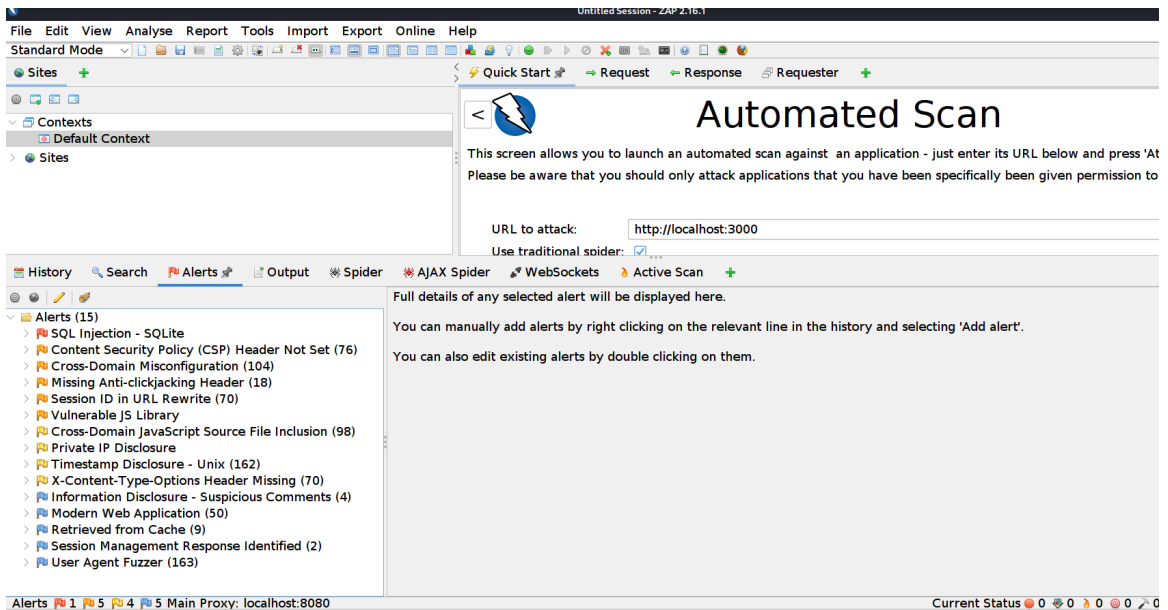
- Weak Password Hashing
 - Location: User Database
 - Evidence: Passwords are stored using MD5 (identified by 32-char hex strings). This algorithm is obsolete and vulnerable to cracking.

```
sqlite> SELECT email, password FROM Users;
admin@juice-sh.op|0192023a7bbd73250516f069df18b500
jim@juice-sh.op|e541ca7ecf72b8d1286474fc613e5e45
bender@juice-sh.op|0c36e517e3fa95aabf1bbfffc6744a4ef
bjoern.kimminich@gmail.com|6edd9d726cbdc873c539e41ae8757b8c
ciso@juice-sh.op|861917d5fa5f1172f931dc700d81a8fb
support@juice-sh.op|3869433d74e3d0c86fd25562f836bc82
morty@juice-sh.op|f2f933d0bb0ba057bc8e33b8ebd6d9e8
mc.safesearch@juice-sh.op|b03f4b0ba8b458fa0acdc02cdb953bc8
J12934@juice-sh.op|3c2abc04e4a6ea8f1327d0aae3714b7d
wurstbrot@juice-sh.op|9ad5b0492bbe528583e128d2a8941de4
amy@juice-sh.op|030f05e45e30710c3ad3c32f00de0473
bjoern@juice-sh.op|7f311911af16fa8f418dd1a3051d6810
bjoern@owasp.org|9283f1b2e9669749081963be0462e466
chris.pike@juice-sh.op|10a783b9ed19ea1c67c3a27699f0095b
accountant@juice-sh.op|963e10f92a70b4b463220cb4c5d636dc
uvogin@juice-sh.op|05f92148b4b60f7dacd04ccee8b8f1af
demo|fe01ce2a7fbac8fafaed7c982a04e229
john@juice-sh.op|00479e957b6b42c459ee5746478e4d45
emma@juice-sh.op|402f1c4a75e316afec5a6ea63147f739
stan@juice-sh.op|e9048a3f43dd5e094ef733f3bd88ea64
ethereum@juice-sh.op|2c17c6393771ee3048ae34d6b380c5ec
testing@juice-sh.op|b616a64605a07941fbd31868aea3b54b
sqlite> █
```

- The screenshot shows the OWASP Juice Shop application interface. At the top, a navigation bar contains a hamburger menu icon, the application logo, and the name "OWASP Juice Shop". On the right side of the navigation bar are links for "Account" and "EN". Below the navigation bar, a green banner displays the message: "You successfully solved a challenge: Error Handling (Provoke an error that is neither very gracefully nor consistently handled.)". Below this banner is a "Login" form. The form has a title "Login" and a label "object Object". It contains two input fields: "Email" with the value "<script>alert('XSS')</script>" and "Password" with a masked password represented by dots. There is a "Forgot your password?" link below the password field and a "Log in" button at the bottom.

- ```
Request Headers (1,392 KB) Raw
```
- |                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Accept:                    | text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Accept-Encoding:           | gzip, deflate, br, zstd                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Accept-Language:           | en-US,en;q=0.5                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Connection:                | keep-alive                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Cookie:                    | language=en; welcomebanner_status=dismiss; continueCode=gXWY6ZqWnJPaLzDVMvR53wkbI7voAJlfrGYtjR8p6NemQXXkG942BxOyEKr9q; token=eYJ0eXAIOUJKV1QiLCJhbGciOiJSUzI1NiJ9.eYJzdGFodXMmOiJqdWVwZjNXN2liZWZGF0YS16eyJpZC16MSwidXNlcml5bWUiOiilICJlbWVfb3Cl6lmFkbWluQGp1aWNLIXNoImNmYiwlicWcGFzc3dvcmlQIiJldiYMDlZlYTDiYmQ3MztlMTDUUXNmYmNjZjE4YjUwMClsInJvbGVuIGUoIHZGTpbisImRlbnHV4ZVRva2VuljoilwibGFZdExvZ2UsXAIOUllICJwcm9maWxlSW1hZ2UioiJhc3NidHMybWVibGljZ2ltYWRdlcy91cGxyYWRzLRlZmF1bHRBRzBG1pi5wbmciclCBjb3RwU2VjcmV0IjoiliwiaXBNY3RpdmlUOnRydWUSImNlYWZFOZWRBdCI6IjIwMjItMTgMDk6MDgzMDguMDguMDTM2ICswMDowMDwMcisVZWZFOZWRBdCI6IjIwMjItMTgMDk6MDgzMDguMDguMDTM2ICswMDowMDwMcisImRlbGV0ZWRBdCI6IjlnVsbsHosimlhdCI6MTc3MDg5MDQONH0.Dlhld8u-jEKHuEtKTC4tfA-FNCRX4izze-n8V2zTKyk3quhuux4j5tdaMuipVzg2p2gwcS7AJwrzh9d2NUJYluVNv6RX4vrUoo6on9-eODJEDBC4josyfaHL0vbnNQ643PlQ-dFxw5sqG67GQk6dLHWwRsFRFLUF5re-X9eTM |
| Host:                      | localhost:3000                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| If-Modified-Since:         | Thu, 12 Feb 2026 09:38:13 GMT                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| If-None-Match:             | W/"125f2-19c51371fd"                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Priority:                  | u=0,i                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Sec-Fetch-Dest:            | document                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Sec-Fetch-Mode:            | navigate                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Sec-Fetch-Site:            | none                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Sec-Fetch-User:            | ?1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Upgrade-Insecure-Requests: | 1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| User-Agent:                | Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

# OWASP ZAP: Automated scanner for web app vulnerabilities



## Areas of Improvement

- Input Sanitization: Implement strict validation using libraries like **validator** to prevent XSS and SQL Injection attacks .
- Secure Authentication: Upgrade password storage from weak MD5 to strong hashing algorithms like **bcrypt** and implement token-based authentication .
- Server Hardening: Configure secure HTTP headers using **helmet.js** and implement generic error messages to prevent information leakage .