1st Week Task

Name: Muhammad Bin Qasim

Strengthening Security Measures for a Web Application

Report Document

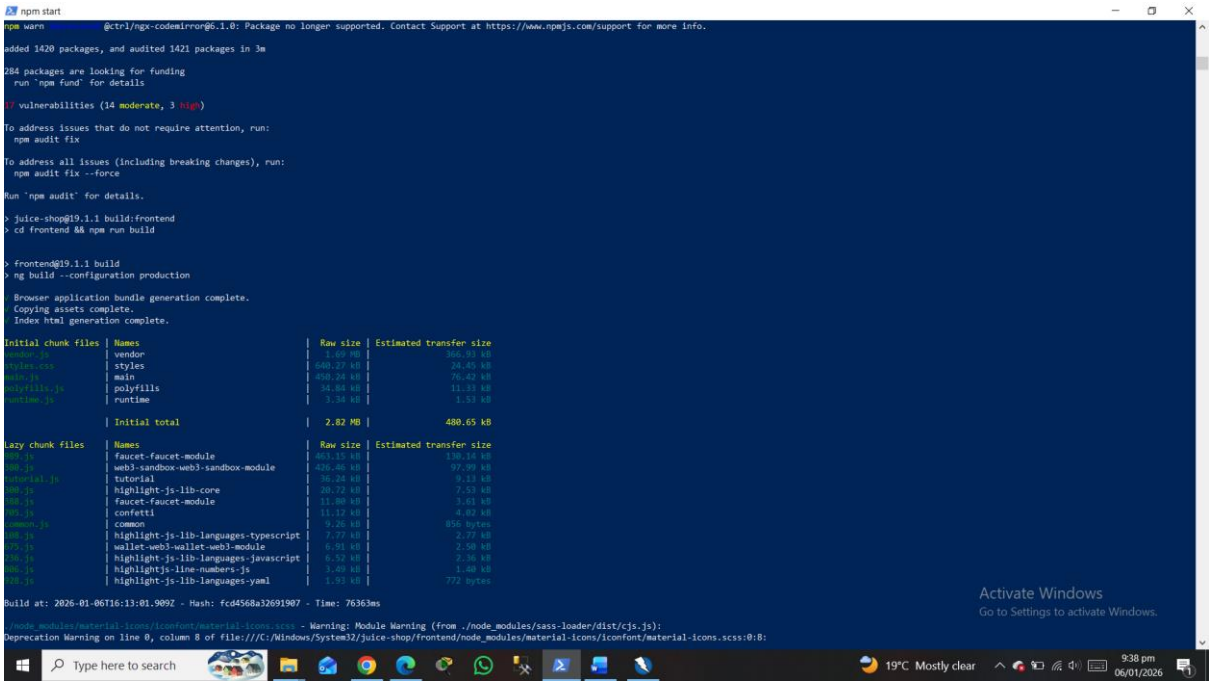
System Setup and Compilation:

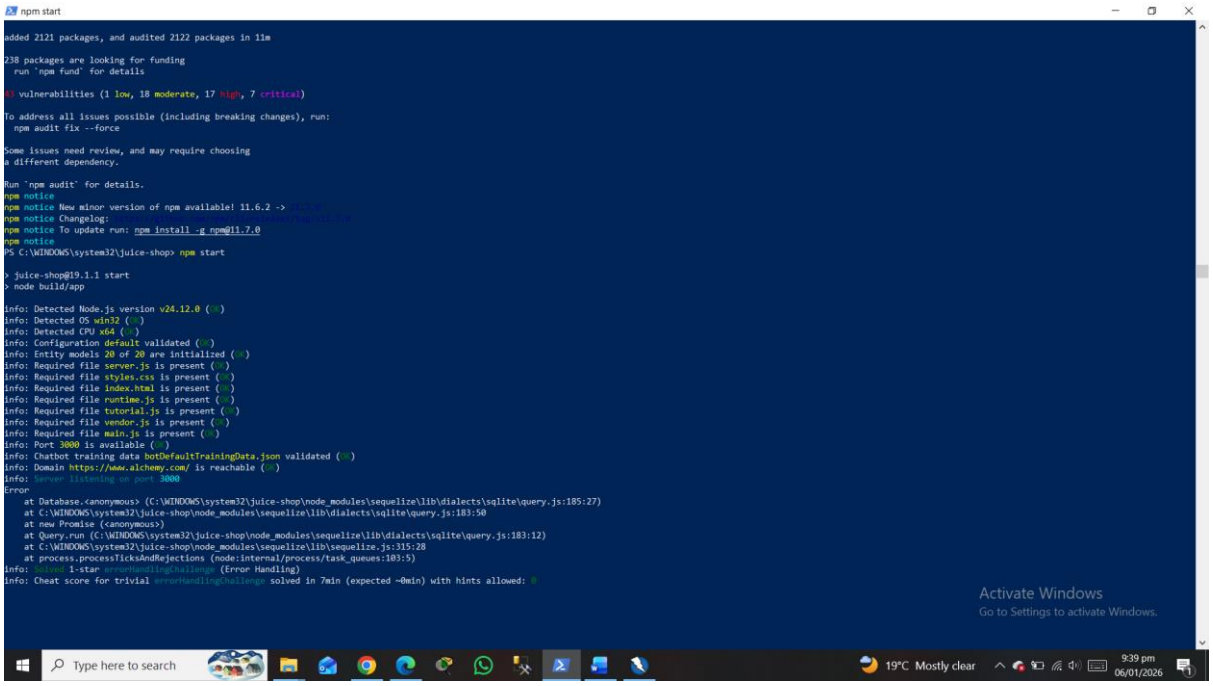
The first two images show the technical behind the scenes process of getting the website ready to run on a local computer.

1. Building the Application: Run command npm start. This process gathers all the necessary code files and prepares them for the browser.

2. Vulnerability Alerts: Even during setup, the system warns that there are vulnerabilities in the underlying software packages. One image shows 17 vulnerabilities, while another shows 43, including some labelled as critical.

3. Successful Launch: The system confirms the server is active and listening on Port 3000. This means the website is now live and can be accessed at http://localhost:3000.


npm start
npm warn @ctrl/ngx-codemirror@6.1.0: Package no longer supported. Contact Support at https://www.npmjs.com/support for more info.
added 1420 packages, and audited 1421 packages in 3m
284 packages are looking for funding
run `npm fund` for details
17 vulnerabilities (14 moderate, 3 high)
To address issues that do not require attention, run:
npm audit fix
To address all issues (including breaking changes), run:
npm audit fix --force
Run `npm audit` for details.
> juice-shop@19.1.1 build:frontend
> cd frontend && npm run build
> frontend@19.1.1 build
> ng build --configuration production
Browser application bundle generation complete.
Copying assets complete.
Index html generation complete.
Initial chunk files | Names | Raw size | Estimated transfer size
vendor.js | vendor | 7.69 MB | 366.33 kB
styles.css | styles | 640.27 kB | 24.45 kB
main.js | main | 450.24 kB | 76.42 kB
polyfills.js | polyfills | 34.84 kB | 11.33 kB
runtime.js | runtime | 3.34 kB | 1.53 kB
Initial total | 2.82 MB | 480.65 kB
Lazy chunk files | Names | Raw size | Estimated transfer size
909.js | faucet-faucet-module | 463.15 kB | 130.14 kB
100.js | web3-sandbox-web3-sandbox-module | 426.46 kB | 97.99 kB
tutorial.js | tutorial | 36.24 kB | 9.13 kB
309.js | highlight-js-lib-core | 20.72 kB | 7.53 kB
888.js | faucet-faucet-module | 11.80 kB | 3.61 kB
705.js | confetti | 11.12 kB | 4.02 kB
common.js | common | 9.26 kB | 856 bytes
108.js | highlight-js-lib-languages-typescript | 7.77 kB | 2.77 kB
975.js | wallet-web3-wallet-web3-module | 6.91 kB | 2.50 kB
936.js | highlight-js-lib-languages-javascript | 6.52 kB | 2.36 kB
806.js | highlightjs-line-numbers-js | 3.49 kB | 1.40 kB
928.js | highlight-js-lib-languages-yaml | 1.93 kB | 772 bytes
Build at: 2026-01-06T16:13:01.909Z - Hash: fcd4568a32691907 - Time: 76363ms
./node_modules/material-icons/iconfont/material-icons.scss - Warning: Module Warning (from ./node_modules/sass-loader/dist/cjs.js):
Deprecation Warning on line 0, column 8 of file:///C:/Windows/System32/juice-shop/frontend/node_modules/material-icons/iconfont/material-icons.scss:0:8:
Activate Windows
Go to Settings to activate Windows.
Type here to search
19°C Mostly clear
9:38 pm
06/01/2026


npm start
added 2121 packages, and audited 2122 packages in 11m
238 packages are looking for funding
run `npm fund` for details
83 vulnerabilities (1 low, 18 moderate, 17 high, 7 critical)
To address all issues possible (including breaking changes), run:
npm audit fix --force
Some issues need review, and may require choosing
a different dependency.
Run `npm audit` for details.
npm notice
npm notice New minor version of npm available! 11.6.2 ->
npm notice Changelog:
npm notice To update run: npm install -g npm@11.7.0
npm notice
PS C:\WINDOWS\system32\juice-shop> npm start
> juice-shop@19.1.1 start
> node build/app
info: Detected Node.js version v24.12.0 (OK)
info: Detected OS win32 (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 styles.css is present (OK)
info: Required file index.html is present (OK)
info: Required file runtime.js is present (OK)
info: Required file tutorial.js is present (OK)
info: Required file vendor.js is present (OK)
info: Required file main.js is present (OK)
info: Port 3000 is available (OK)
info: Chatbot training data botDefaultTrainingData.json validated (OK)
info: Domain https://www.alchemy.com/ is reachable (OK)
info: Server listening on port 3000
Error
at Database.<anonymous> (C:\WINDOWS\system32\juice-shop\node_modules\sequelize\lib\dialects\sqlite\query.js:185:27)
at C:\WINDOWS\system32\juice-shop\node_modules\sequelize\lib\dialects\sqlite\query.js:183:50
at new Promise (<anonymous>)
at Query.run (C:\WINDOWS\system32\juice-shop\node_modules\sequelize\lib\dialects\sqlite\query.js:183:12)
at C:\WINDOWS\system32\juice-shop\node_modules\sequelize\lib\sequelize.js:315:28
at process.processTicksAndRejections (node:internal/process/task_queues:103:5)
info: Solved 1-star errorHandlingChallenge (Error Handling)
info: Cheat score for trivial errorHandlingChallenge solved in 7min (expected ~0min) with hints allowed: 0
Activate Windows
Go to Settings to activate Windows.
Type here to search
19°C Mostly clear
9:39 pm
06/01/2026

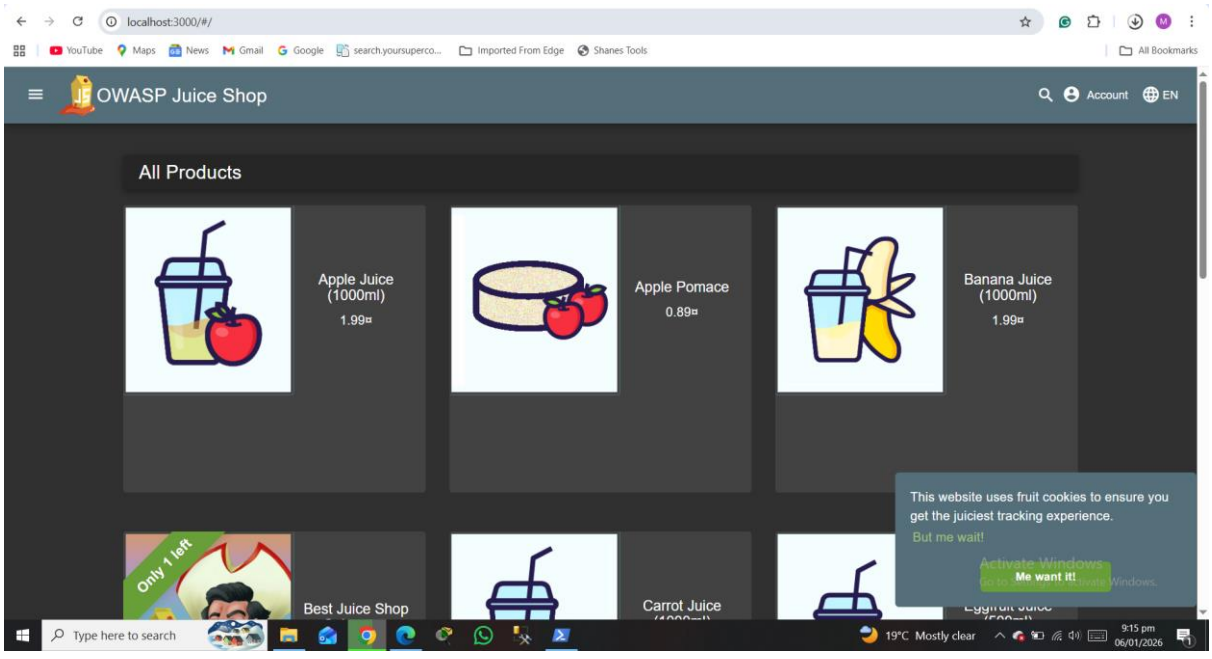
Exploring the Web Interface:

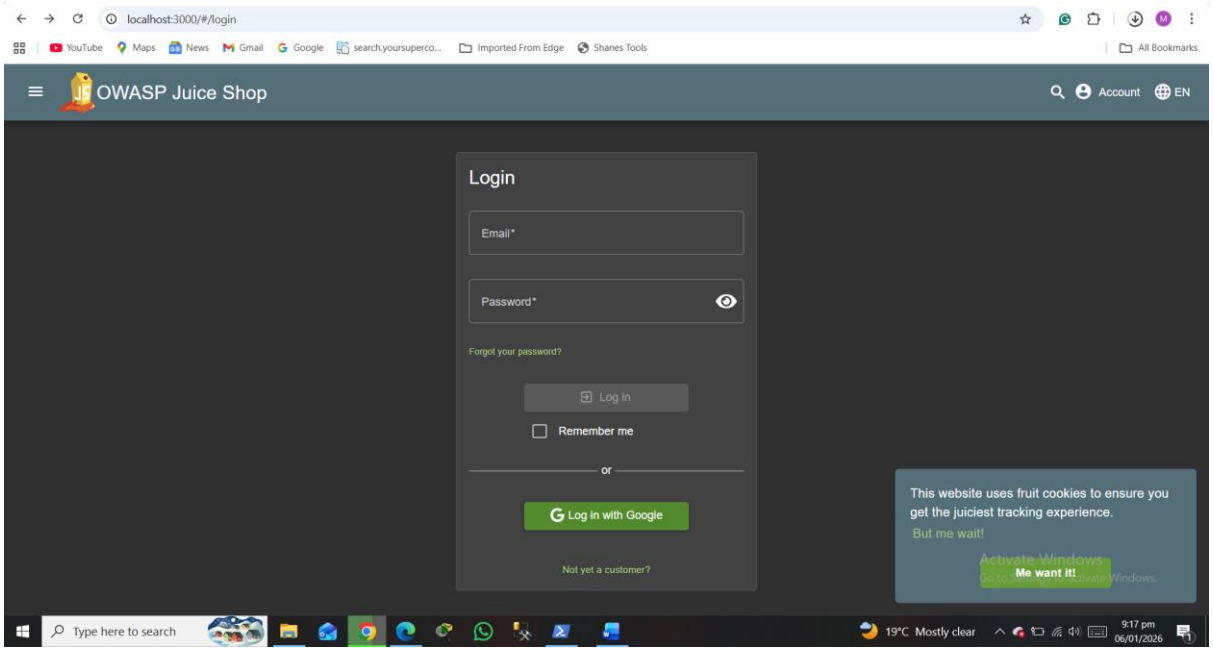
The next few images show the actual OWASP Juice Shop website as seen by a regular user.

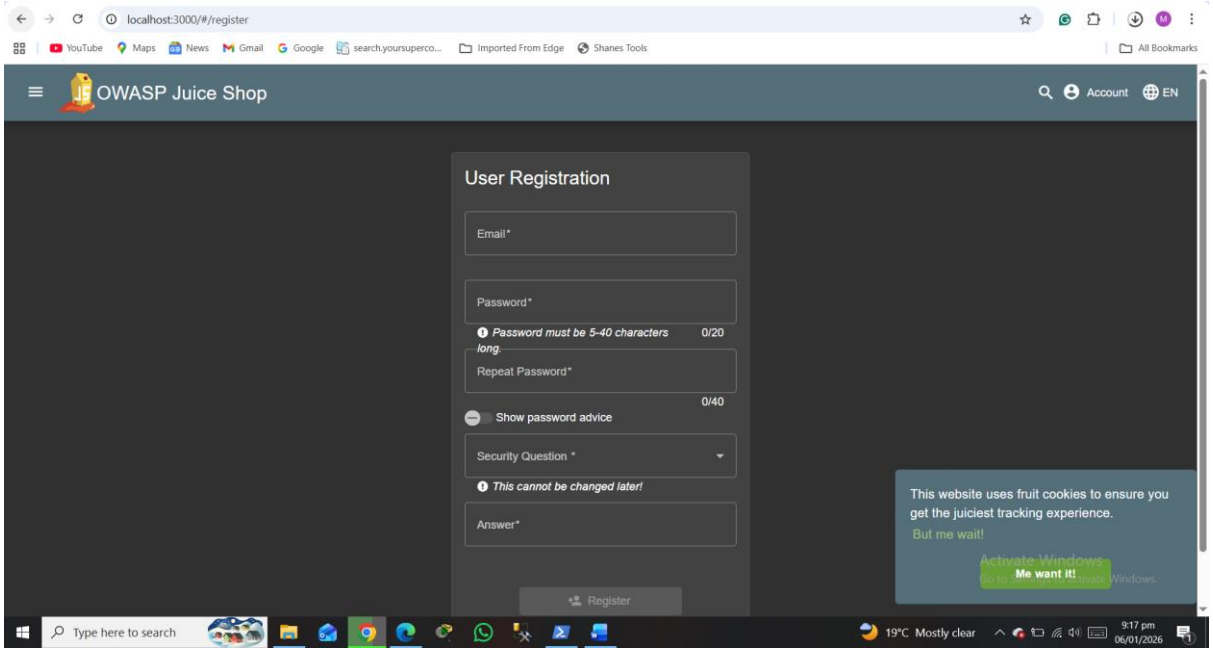
1. Homepage: A shop interface displaying products like Apple Juice, Banana Juice, etc.

2. User Accounts: There are standard forms for User Registration and Login, where people would normally enter an email and password to create an account.

3. Cookie Notice: A pop-up at the bottom of the screen mentions fruit cookies, a play on words regarding web cookies used for tracking.




localhost:3000/#/login
OWASP Juice Shop
Account
EN
Login
Email*
Password*
Forgot your password?
Log in
Remember me
or
Log in with Google
Not yet a customer?
This website uses fruit cookies to ensure you get the juiciest tracking experience.
But me wait!
Me want it!
Type here to search
19°C Mostly clear
9:17 pm
06/01/2026


localhost:3000/#/register
OWASP Juice Shop
Account
EN
User Registration
Email*
Password*
Password must be 5-40 characters long.
0/20
Repeat Password*
0/40
Show password advice
Security Question *
This cannot be changed later!
Answer*
Register
This website uses fruit cookies to ensure you get the juiciest tracking experience.
But me wait!
Me want it!
Type here to search
19°C Mostly clear
9:17 pm
06/01/2026

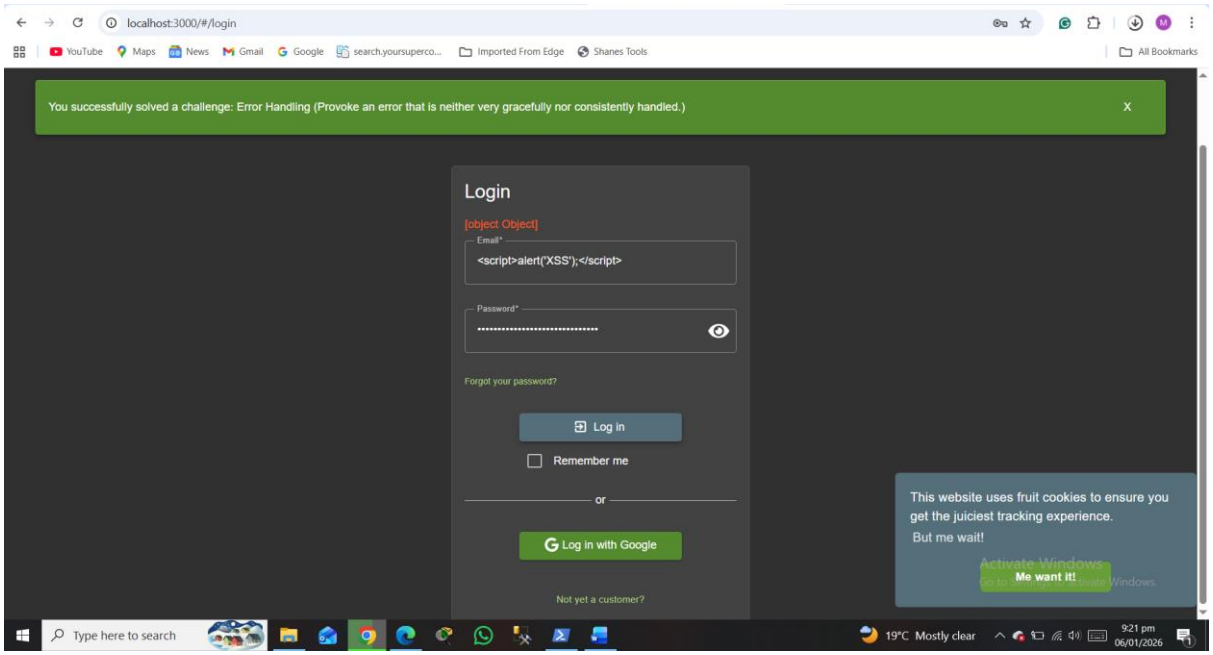
Security Testing:

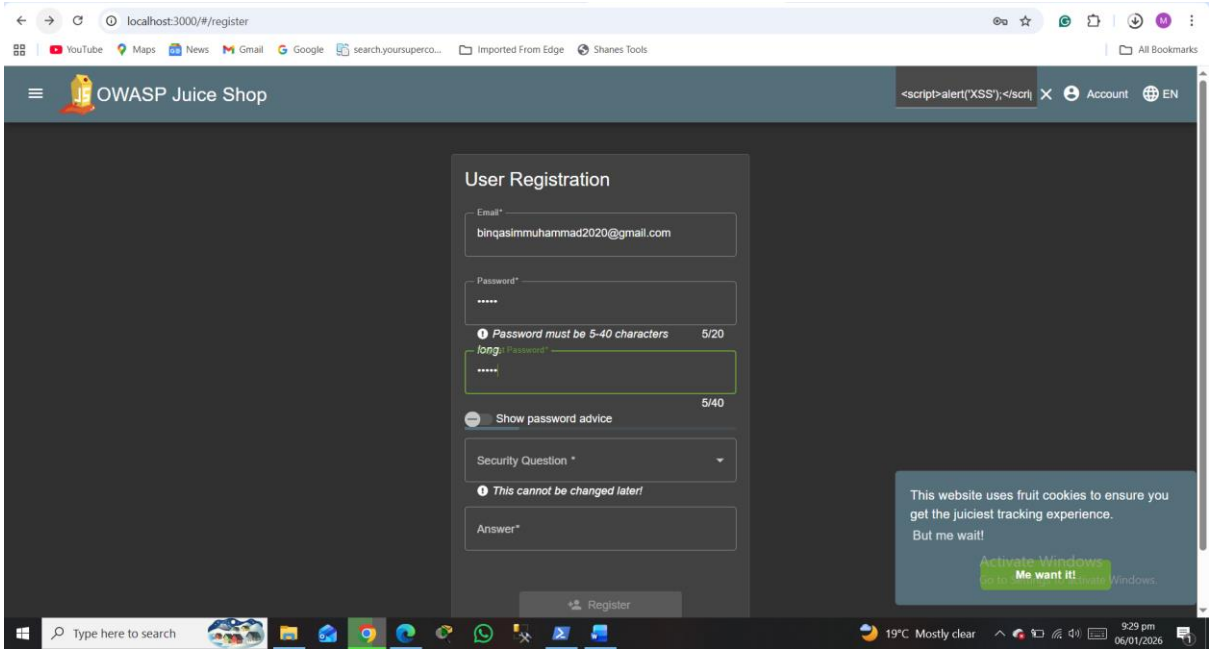
The image show that I attempting to break the website using common hacking techniques.

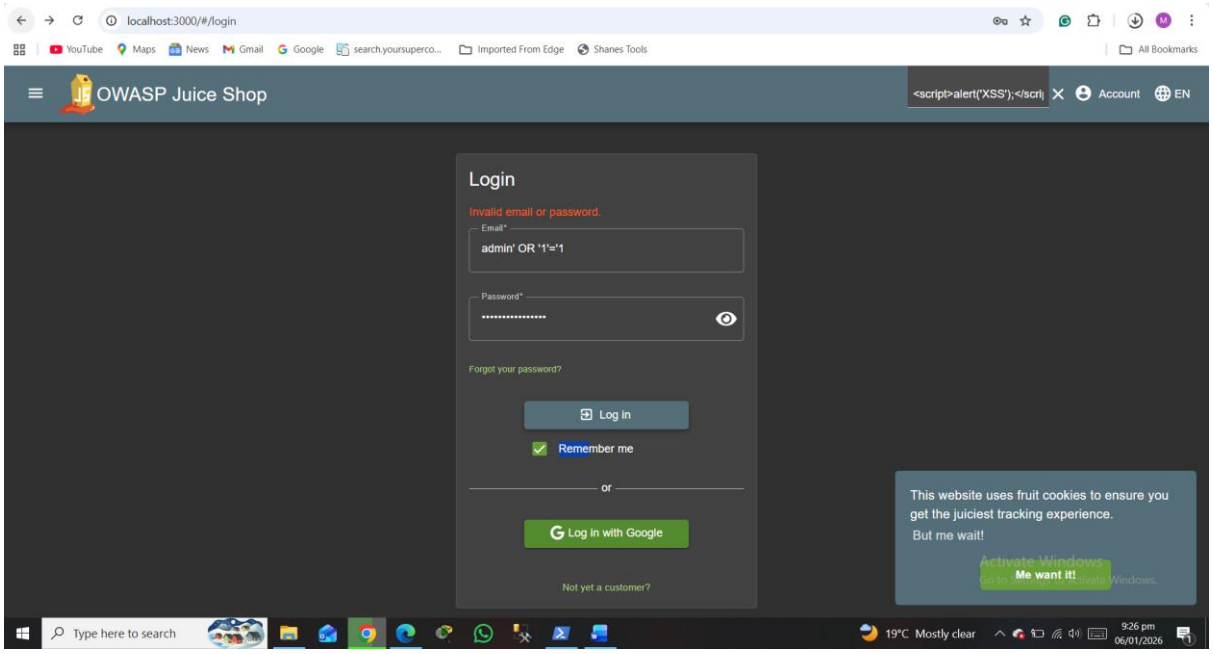
1. Error Handling Challenge: I successfully trigger an error that isn't handled properly by the website. A green banner appears at the top saying: You successfully solved a challenge: Error Handling.

2. Cross-Site Scripting (XSS): I type <script>alert('XSS');</script> into the email field. This is a test to see if the website will accidentally run malicious code entered by me.

3. SQL Injection: In the login box, I enter admin' OR '1'='1. This is a famous trick used to bypass password requirements by confusing the website's database into thinking the login is always valid.




localhost:3000/#/register
OWASP Juice Shop
<script>alert('XSS');</scri
Account
EN
User Registration
Email*
binqasimmuhammad2020@gmail.com
Password*
Password must be 5-40 characters
5/20
long
5/40
Show password advice
Security Question *
This cannot be changed later!
Answer*
Register
This website uses fruit cookies to ensure you get the juiciest tracking experience.
But me wait!
Me want it!
Type here to search
19°C Mostly clear
9:29 pm
06/01/2026


localhost:3000/#/login
OWASP Juice Shop
<script>alert('XSS');</scri
Account
EN
Login
Invalid email or password.
Email*
admin' OR '1'='1
Password*
Forgot your password?
Log in
Remember me
or
Log in with Google
Not yet a customer?
This website uses fruit cookies to ensure you get the juiciest tracking experience.
But me wait!
Me want it!
Type here to search
19°C Mostly clear
9:26 pm
06/01/2026

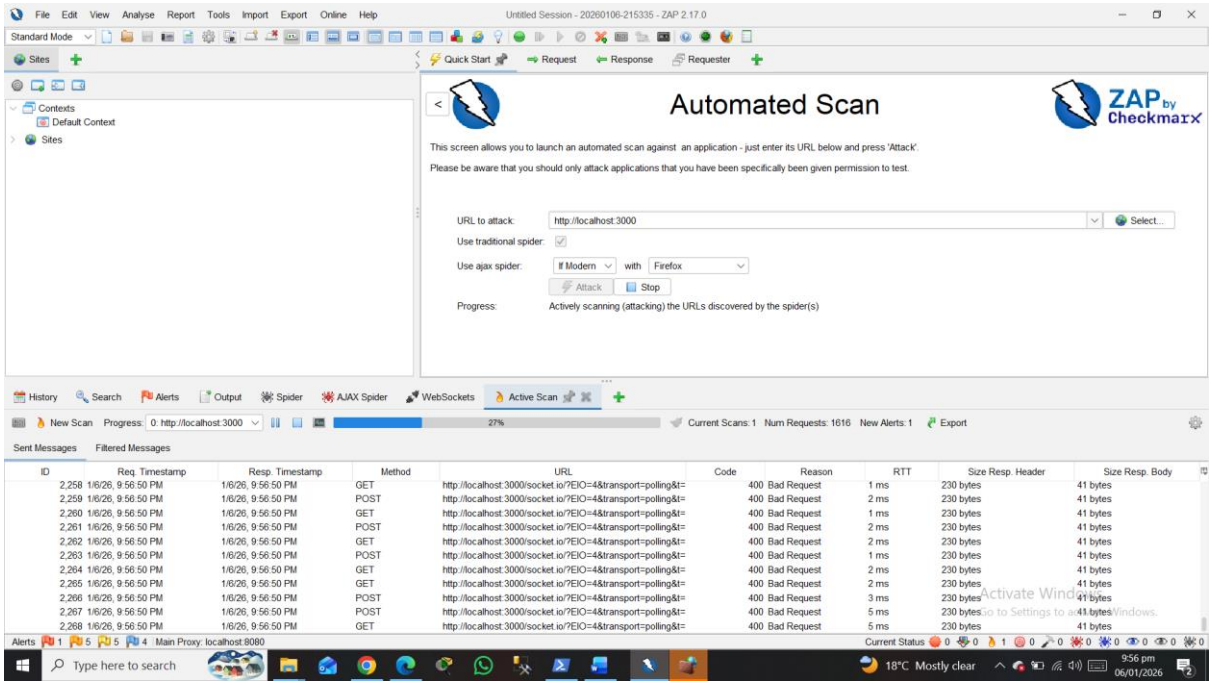
Automated Security Scanning:

The final image shows a professional security tool called ZAP (Zed Attack Proxy).

1. Automated Scan: I programmed this tool to automatically attack http://localhost:3000.

2. Scanning Progress: The tool is shown at 27% completion. It is rapidly sending hundreds of requests to the website to find every possible security weakness.

3. Results: The bottom of the screen lists various Bad Requests. Code 400, indicating the tool is finding ways the website reacts poorly to unusual data.



At Last:

I have completed my first week of tasks and gained a lot of new knowledge. Even though I could not finish the ZAP scanning process due to some web bad request errors, but still understand the basic concept of the tool. I learned that ZAP is used for automated security testing to find weaknesses in a website quickly. I am happy with what I have learned about setup and manual hacking so far.
