LAPORAN TUGAS
WORKSHOP KECERDASAN BUATAN

OWASP 10 – Juice Shop

Oleh:

Nama	:	Fisabili Maghfirona Firdaus
NRP	:	3122640051
Kelas	:	LJ D4 IT-B

POLITEKNIK ELEKTRONIKA NEGERI SURABAYA

Kampus ITS, Jl. Raya ITS, Keputih, Kec. Sukolilo, Kota SBY,

Jawa Timur 60111

Telepon +62 31 594 7280 Fax. +62 31 594 6114

E-mail: *humas@pens.ac.id* Website: *pens.ac.id*

SURABAYA

2023

OWASP - Juice Shop

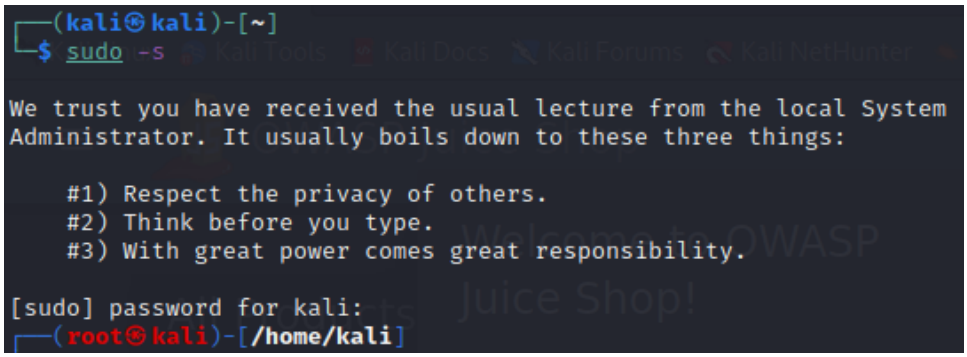
OWASP Juice Shop merupakan sebuah aplikasi web yang dikembangkan sebagai platform untuk melakukan pengujian serta pembelajaran dalam kerentanan keamanan dalam website, termasuk pengujian penetrasi hingga peretasan. OWASP – Juice Shop termasuk ke dalam platform yang canggih dibandingkan dengan platform lain karena telah memiliki kerentanan yang sering dimiliki dalam aplikasi web biasanya, dirangkum dalam daftar OWASP Top 10 Vulnerabilities:

1. Broken Access Control
2. Cryptographic Failures
3. Injection
4. Insecure Design
5. Security misconfigurations
6. Vulnerable and Outdated Components
7. Identification and authentication failures
8. Software and Data Integrity Failures
9. Security Logging and Monitoring Failures
10. Server-side Request Forgery

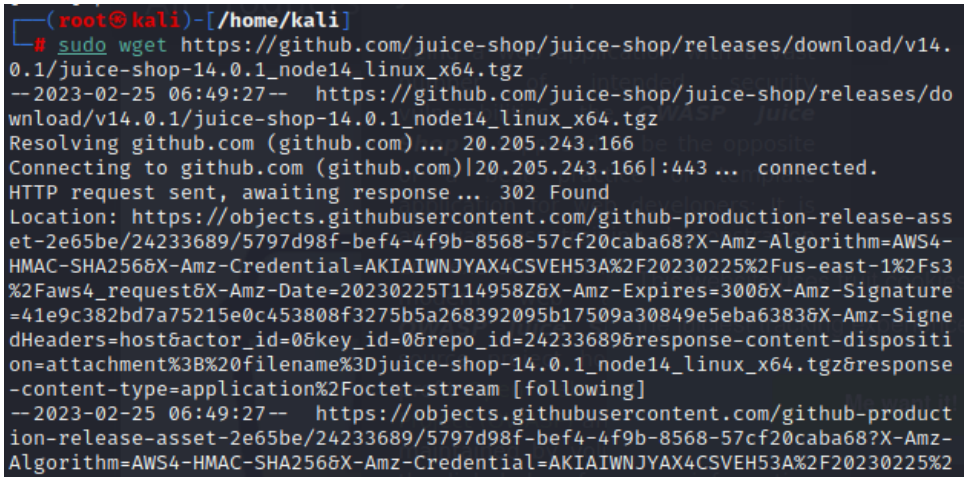
Instalasi Juice Shop pada Kali LINUX

Pada percobaan ini, akan digunakan Kali LINUX dan NodeJS sebagai sistem operasi dan web servernya.

1. Melakukan login pada Super User untuk kontrol sistem melalui terminal.
   Login pada Super User di terminal dibutuhkan untuk mengakses kontrol sistem menggunakan terminal.



2. Melakukan pengambilan package pada online repository Juice Shop di Github.
   Karena package Juice Shop masih belum ada pada sistem, dilakukan pengambilan package dari repository luar.



3. Melakukan ekstraksi package Juice Shop.
   Setelah package diunduh, maka perlu diekstrak terlebih dahulu menggunakan ekstraksi pada terminal.

```
┌──(root㉿kali)-[/home/kali]
└─# tar zxvf juice-shop-14.0.1_node14_linux_x64.tgz
juice-shop_14.0.1/LICENSE
juice-shop_14.0.1/CODE_OF_CONDUCT.md
juice-shop_14.0.1/CONTRIBUTING.md
juice-shop_14.0.1/HALL_OF_FAME.md
juice-shop_14.0.1/README.md
juice-shop_14.0.1/REFERENCES.md
juice-shop_14.0.1/SECURITY.md
juice-shop_14.0.1/SOLUTIONS.md
juice-shop_14.0.1/package.json
juice-shop_14.0.1/ctf.key
juice-shop_14.0.1/swagger.yml
juice-shop_14.0.1/server.ts
juice-shop_14.0.1/config.schema.yml
juice-shop_14.0.1/build/
juice-shop_14.0.1/build/app.js
juice-shop_14.0.1/build/app.js.map
juice-shop_14.0.1/build/data/
juice-shop_14.0.1/build/data/datacache.js
juice-shop_14.0.1/build/data/datacache.js.map
juice-shop_14.0.1/build/data/datacreator.js
juice-shop_14.0.1/build/data/datacreator.js.map
```

4. Melakukan pengambilan package NodeJS pada online repository.
   Hal yang sama dengan package Juice Shop juga dilakukan pada NodeJS, yaitu mengambil dari luar sistem.

```
┌──(root㉿kali)-[/home/kali]
└─# wget https://nodejs.org/download/release/v14.1.0/node-v14.1.0-linux-x64.tar.xz

--2023-02-25 06:51:34--  https://nodejs.org/download/release/v14.1.0/node-v14.1.0-linux-x64.tar.xz
Resolving nodejs.org (nodejs.org)... 104.20.23.46, 104.20.22.46, 2606:4700:10::6814:162e, ...
Connecting to nodejs.org (nodejs.org)|104.20.23.46|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 20836040 (20M) [application/x-xz]
Saving to: 'node-v14.1.0-linux-x64.tar.xz'

node-v14.1.0-linux- 100%[===================>]  19.87M  1.55MB/s    in 12s

2023-02-25 06:51:47 (1.72 MB/s) - 'node-v14.1.0-linux-x64.tar.xz' saved [20836040/20836040]
```

5. Melakukan ekstraksi package NodeJS.
   Setelah package berhasil didownload, dilakukan ekstraksi dengan cara yang sama pada NodeJS.

```
┌──(root㉿kali)-[/home/kali]
└─# tar -xvf node-v14.1.0-linux-x64.tar.xz
node-v14.1.0-linux-x64/
node-v14.1.0-linux-x64/bin/
node-v14.1.0-linux-x64/bin/node
node-v14.1.0-linux-x64/bin/npm
node-v14.1.0-linux-x64/bin/npx
node-v14.1.0-linux-x64/share/
node-v14.1.0-linux-x64/share/systemtap/
node-v14.1.0-linux-x64/share/systemtap/tapset/
node-v14.1.0-linux-x64/share/systemtap/tapset/node.stp
node-v14.1.0-linux-x64/share/doc/
node-v14.1.0-linux-x64/share/doc/node/
node-v14.1.0-linux-x64/share/doc/node/gdbinit
node-v14.1.0-linux-x64/share/doc/node/lldb_commands.py
node-v14.1.0-linux-x64/share/man/
node-v14.1.0-linux-x64/share/man/man1/
node-v14.1.0-linux-x64/share/man/man1/node.1
node-v14.1.0-linux-x64/lib/
node-v14.1.0-linux-x64/lib/node_modules/
node-v14.1.0-linux-x64/lib/node_modules/npm/
node-v14.1.0-linux-x64/lib/node_modules/npm/.licensee.json
node-v14.1.0-linux-x64/lib/node_modules/npm/.mailmap
node-v14.1.0-linux-x64/lib/node_modules/npm/.npmignore
```

6. Melakukan penyalinan data environment NodeJS.
   Setelah data terekstrak, maka data environment NodeJS dipindahkan ke dalam user directory agar dapat diakses oleh sistem.

```
┌──(root㉿kali)-[/home/kali]
└─# cp -r node-v14.1.0-linux-x64/{bin,include,lib,share} /usr/
```

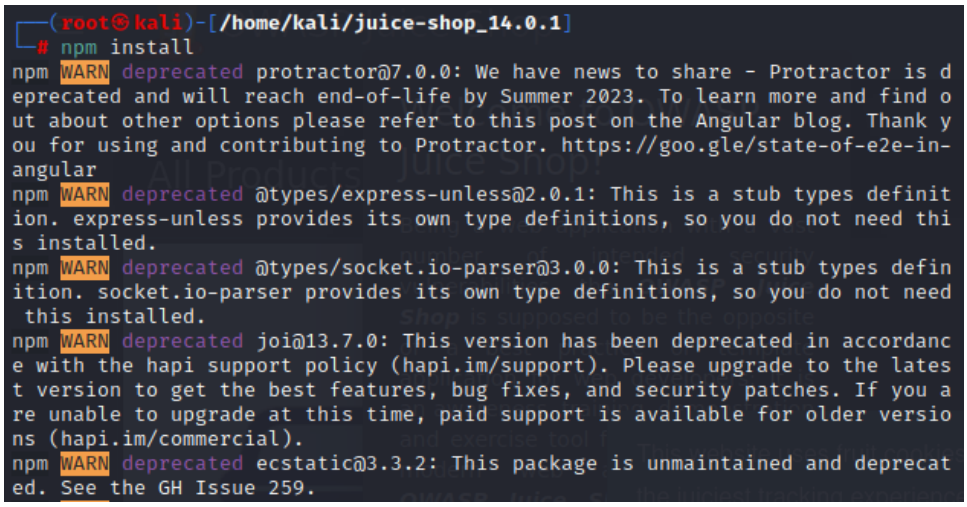
7. Masuk ke dalam direktori Juice Shop.
   Setelah itu, masuk ke dalam direktori hasil ekstraksi Juice Shop.

```
┌──(root㉿kali)-[/home/kali]
└─# ls
Desktop             juice-shop-14.0.1_node14_linux_x64.tgz  Pictures
Documents           Music                                   Public
Downloads           node-v14.1.0-linux-x64                  Templates
juice-shop_14.0.1   node-v14.1.0-linux-x64.tar.xz           Videos
```

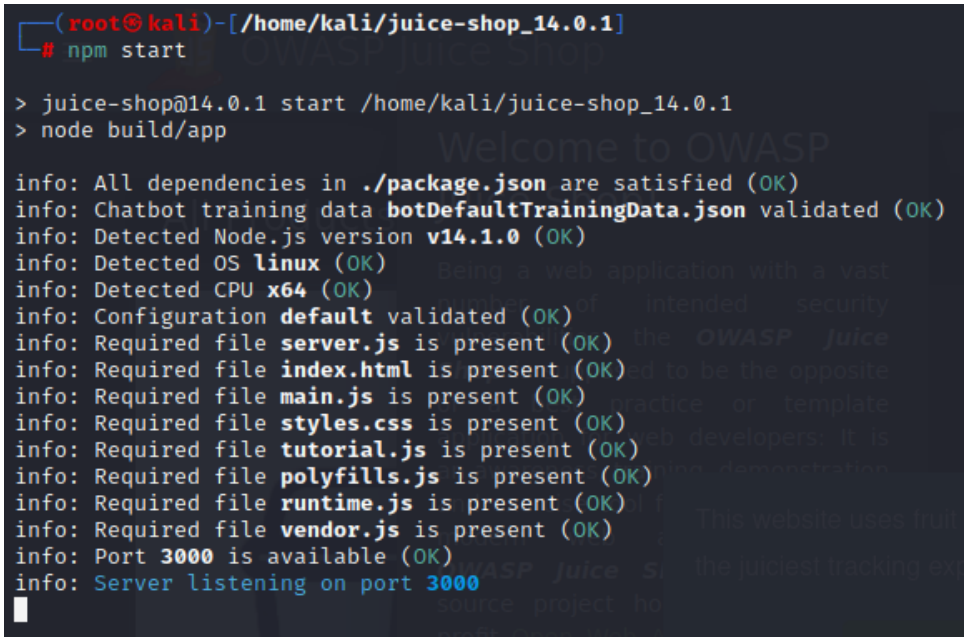
```
┌──(root㉿kali)-[/home/kali]
└─# cd juice-shop_14.0.1

┌──(root㉿kali)-[/home/kali/juice-shop_14.0.1]
└─# ls
build                data              lib               REFERENCES.md  uploads
CODE_OF_CONDUCT.md   encryptionkeys    LICENSE           routes         views
config               frontend          models            SECURITY.md
config.schema.yml    ftp               node_modules      server.ts
CONTRIBUTING.md      HALL_OF_FAME.md   package.json      SOLUTIONS.md
ctf.key              i18n              README.md         swagger.yml
```

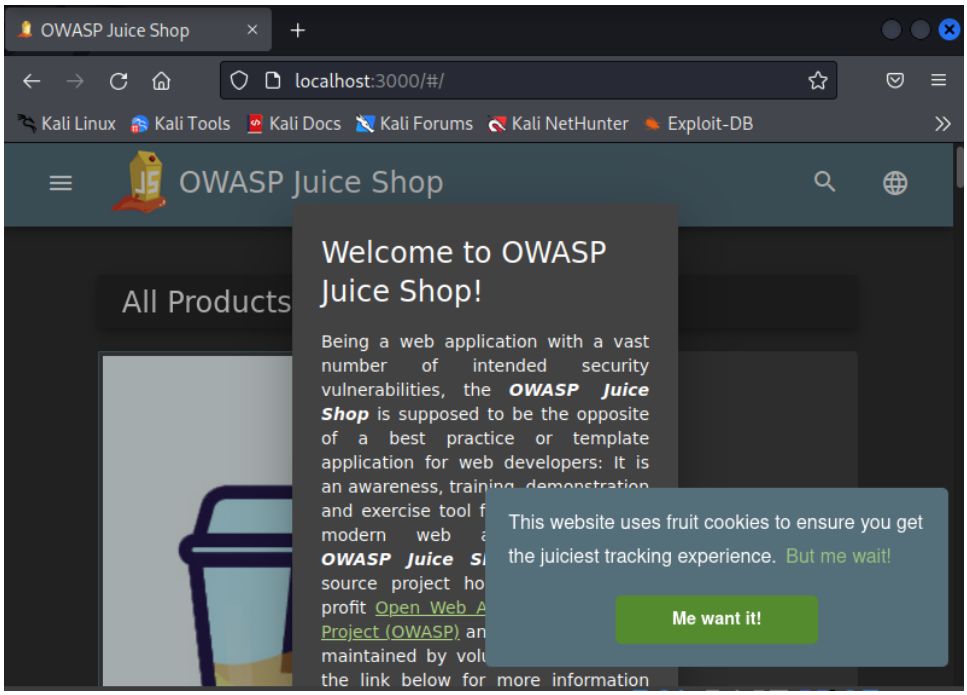
8. Memasang NodeJS pada Juice Shop.
   Kemudian melakukan instalasi NodeJS pada direktori Juice Shop sebagai web server.



9. Menjalankan service Juice Shop menggunakan NodeJS.
   Setelah selesai, service Juice Shop dapat langsung dijalankan dengan melakukan run pada direktori Juice Shop.



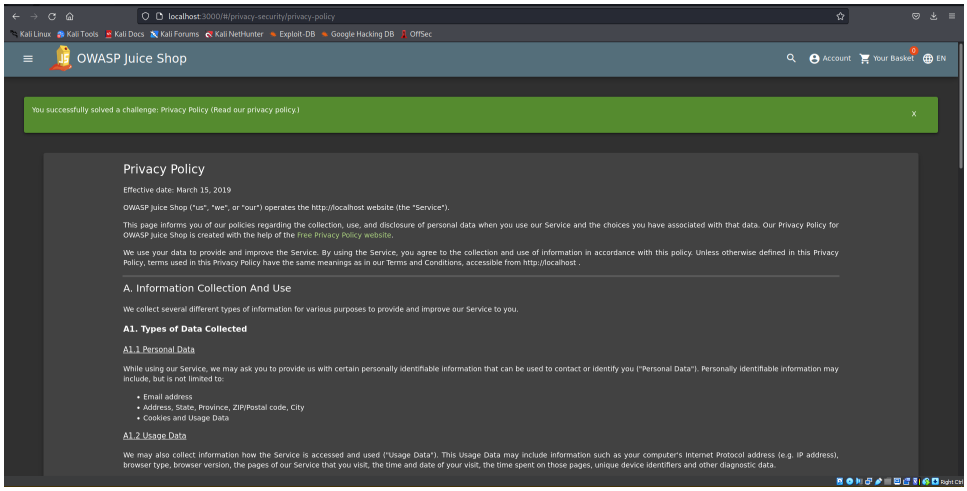
10. Membuka web service dari host yang disediakan NodeJS.
    Service web dapat diakses dengan menginputkan host dan port yang digunakan untuk NodeJS.


OWASP Juice Shop
localhost:3000/#/
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
OWASP Juice Shop
All Products
Welcome to OWASP Juice Shop!
Being a web application with a vast number of intended security vulnerabilities, the OWASP Juice Shop is supposed to be the opposite of a best practice or template application for web developers: It is an awareness, training, demonstration and exercise tool f
modern web a
OWASP Juice S
source project ho
profit Open Web A
Project (OWASP) an
maintained by volu
the link below for more information
This website uses fruit cookies to ensure you get the juiciest tracking experience. But me wait!
Me want it!

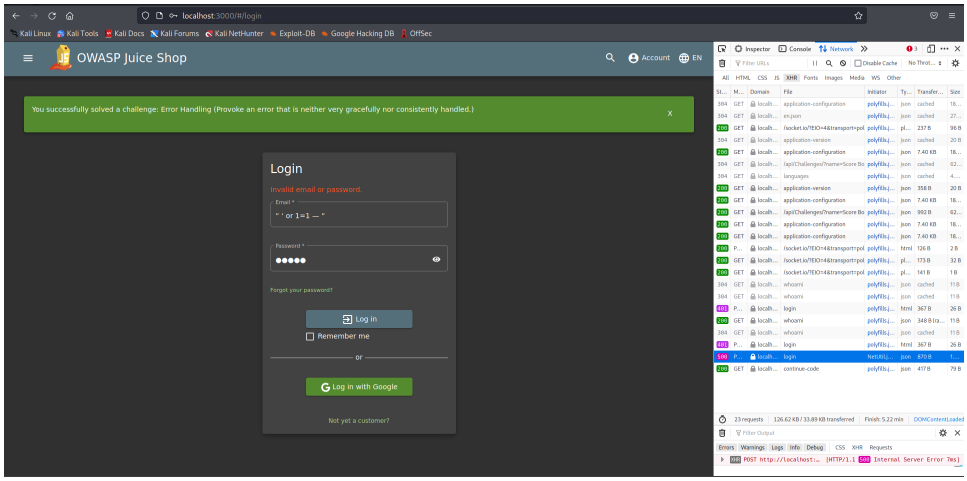
Juice Shop Challenges

Pada Juice Shop akan terdapat beberapa challenge yang bisa dilakukan untuk memahami beberapa vulnerability yang telah didaftarkan pada OWASP 10. Berikut adalah beberapa di antaranya.

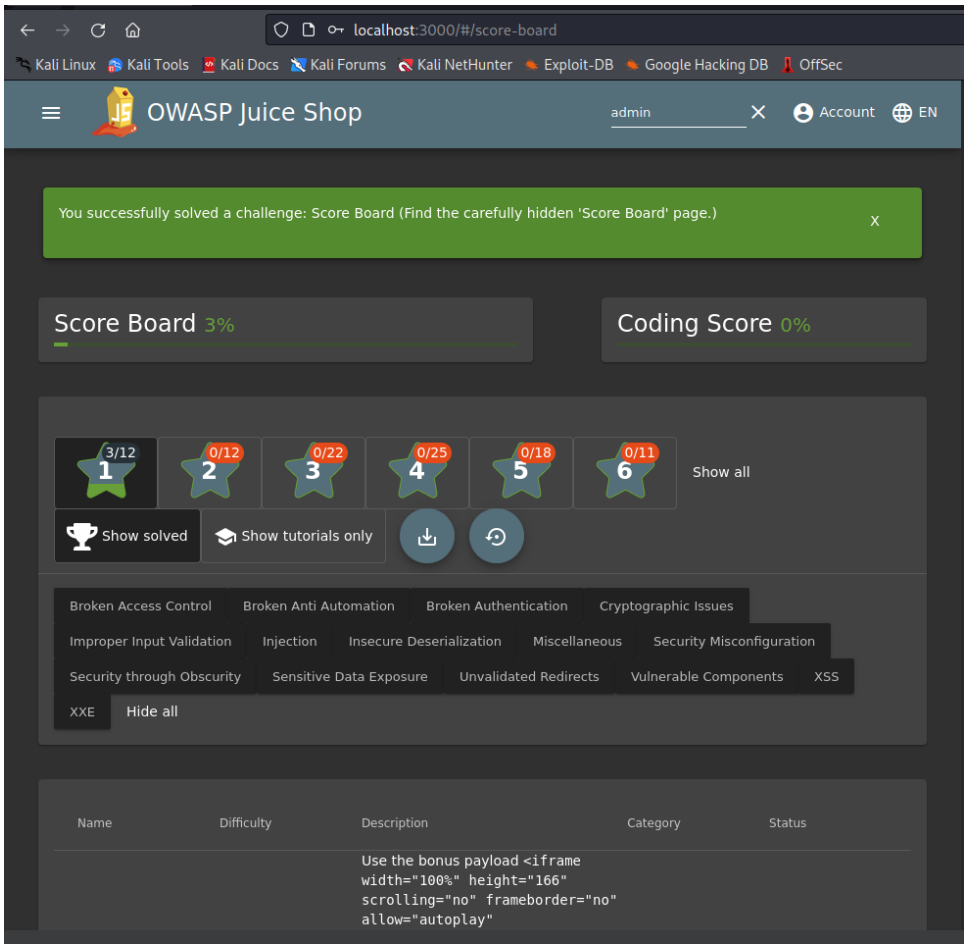
1. Privacy Policy
   Didapatkan dengan membuka Privacy Policy yang berada pada navigasi dan pada menu yang muncul pada navigasi tersebut.



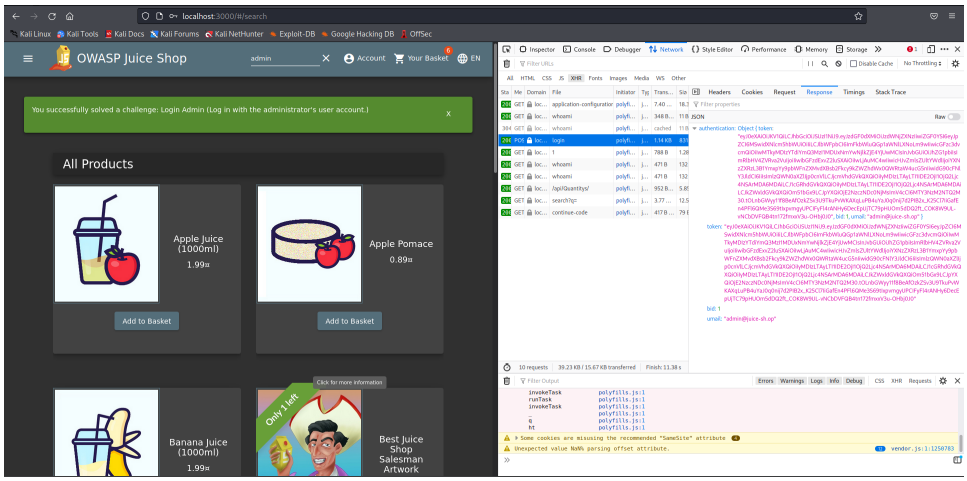
2. Error Handling
   Didapatkan dengan melakukan handling pada beberapa error yang muncul, dan mengalihkan error tersebut ke tahap yang lainnya. Pada challenge ini dapat dilakukan dengan menggunakan console browser ataupun aplikasi lainnya.

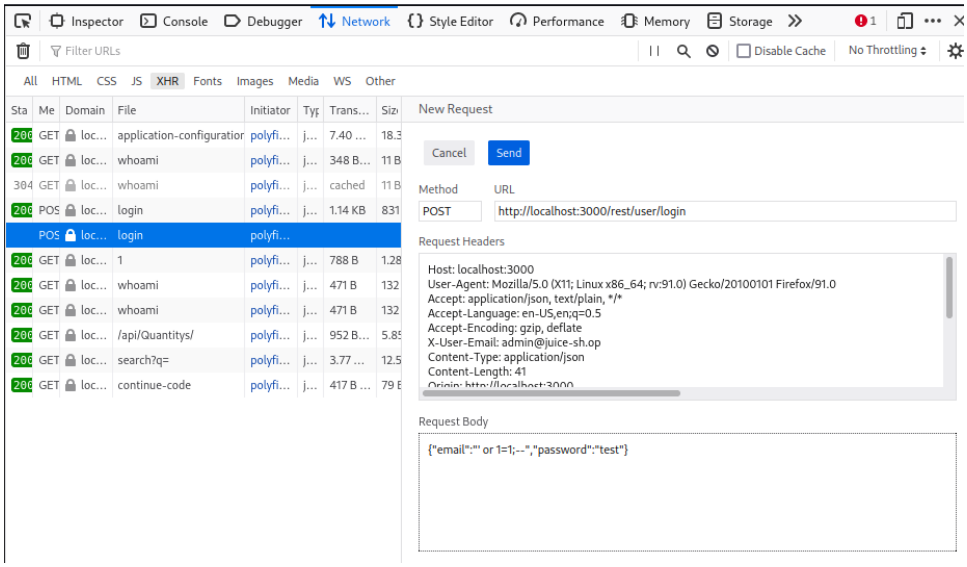


3. Score Board
   Score Board didapatkan dengan mencoba membuka beberapa directory web source pada console yang cukup tersembunyi pada baris kode web. Setelah menemukannya, dapat langsung menggabungkan URL yang telah ada.

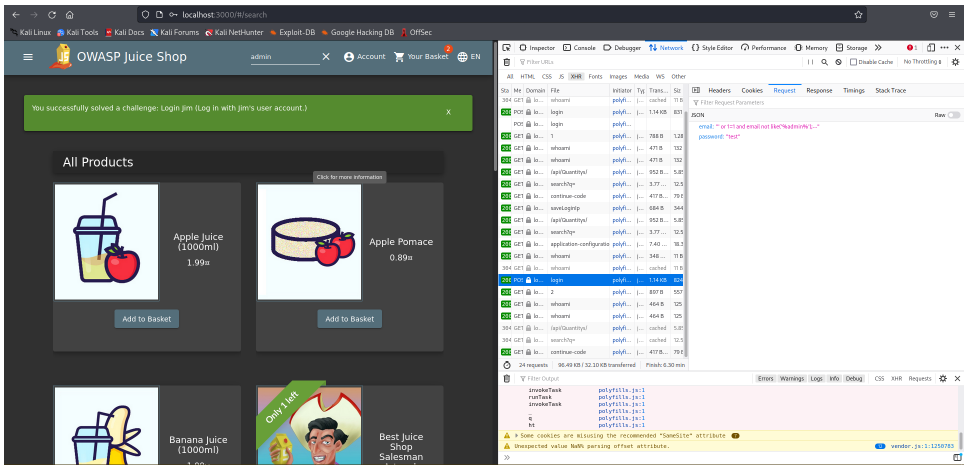


4. Access Admin Login
   Login Admin dapat dilakukan setelah beberapa kali mencoba mencari kode role dari Admin website, dan ditemukan sebagai “1”. Karena form pada login dapat juga melakukan compile masukan, maka dilakukan pemaksaan login menggunakan role admin.

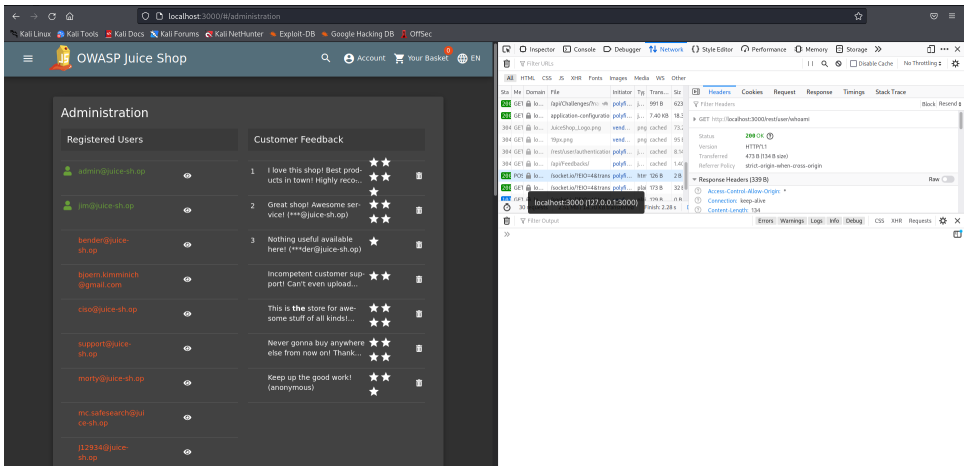




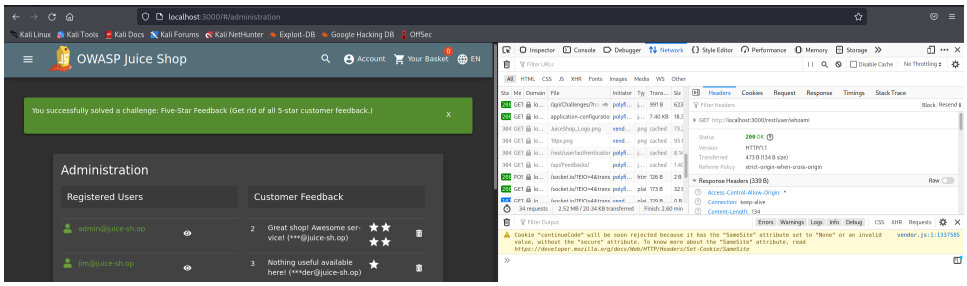
5. Login menggunakan akun milik Jim (salah satu user)
   Akun milik Jim dapat diakses dengan cara yang kurang lebih sama dengan login admin, namun bedanya adalah melakukan pemaksaan agar kredensial yang login bukanlah admin, dan akun milik Jim terdapat pada urutan yang atas, sehingga diambil.



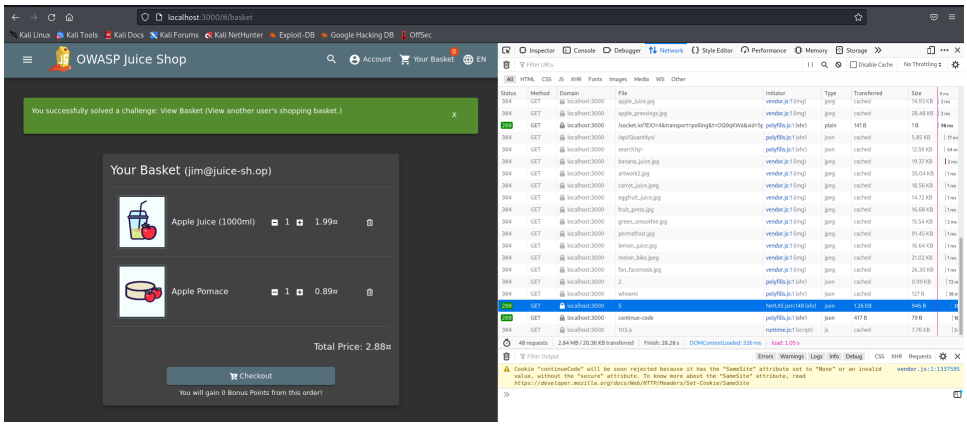
6. Mengakses halaman Administration
   Halaman Administration dapat diakses setelah melihat beberapa rute tersembunyi yang sebenarnya dapat diakses oleh role admin. Halaman ini dapat dilihat pada console yang menampilkan halaman aksesnya.



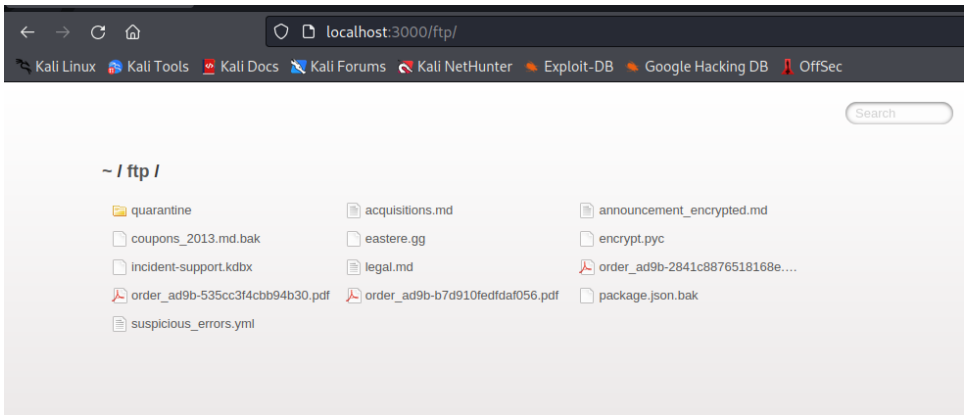
7. Menghapus salah satu review
   Pada halaman administrasi, admin dapat menghapus salah satu review untuk menyelesaikan salah satu challenge dan melihat bahwa challenge telah selesai pada console.

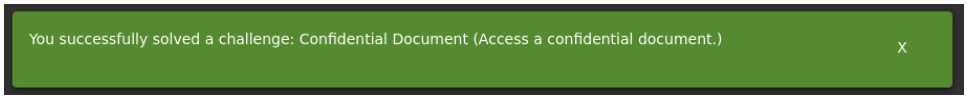


8. Melihat keranjang orang lain
   User dapat melihat keranjang user lain dengan melakukan injeksi pada masukan url di console. Keranjang akan dibagi menjadi ID, sehingga dengan memasukkan ID maka keranjang user lain dapat diakses.

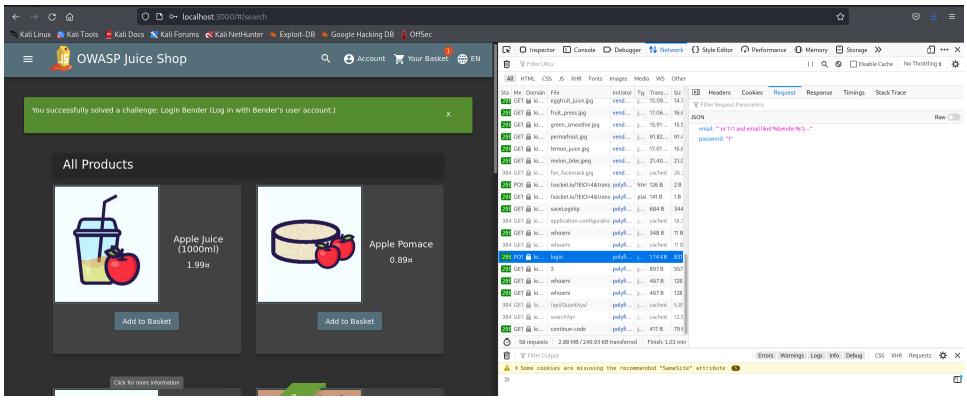


9. Mengakses FTP web
   Pada struktur web, dapat dilihat bahwa terdapat halaman FTP yang memiliki beberapa file di dalamnya, dan dapat diakses melalui URL langsung.



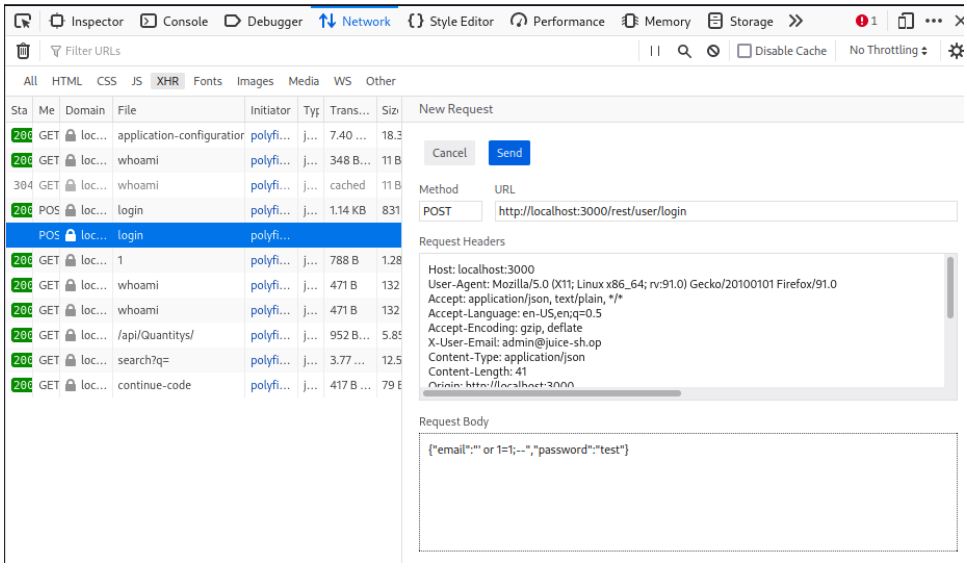


10. Login menggunakan akun Bender
    Akun ini dapat diakses dengan menggunakan cara yang hampir sama dengan kedua akun lainnya. Namun untuk mengakses dapat melakukan spesifikasi menggunakan nama user yang dapat dilihat melalui console.

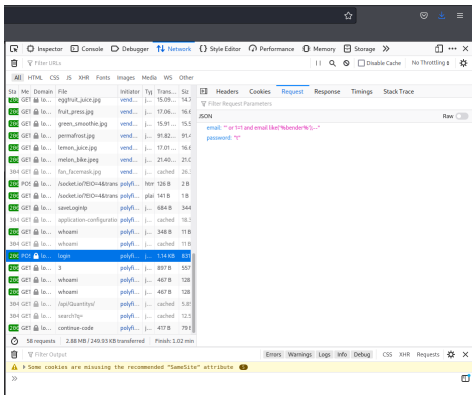


OWASP 10 in Juice Shop

1. Broken Access Control
   Kerusakan atau kesalahan dalam izin kontrol akses data yang menyebabkan dapat diaksesnya suatu data yang seharusnya tidak bisa diakses.
   Pada hasil penelitian di Juice Shop ini, ditemukan kerentanan Broken Access Control pada bagian pemasukan email yang dapat dilakukan dengan memasukkan perintah yang membawa role dari user, contohnya adalah dengan memaksa untuk masuk menggunakan role admin, “1”.



2. Cryptographic Failures
   Kesalahan dalam melakukan enkripsi atau dekripsi pada kunci data sensitif, misal akses token, login ID, dan sebagainya.
   Pada penelitian kali ini, didapati bahwa kesalahan dalam Cryptographic terdapat pada enkripsi di akun milik Jim dan Bender yang dapat diakses dengan memasukkan injeksi untuk memanggil username tanpa disertai password.



3. Injection
   Eksploitasi kerentanan dengan melakukan input data tambahan ke dalam sistem produk (web / server) baik berupa input perintah ataupun sebuah file yang dapat merubah kinerja sistem dari dalam.
   Pada web ini, hampir semua percobaan yang dilakukan adalah dengan melakukan injeksi pada kode di beberapa bagian, seperti untuk mengakses akun, hingga untuk mengubah aktivitas dalam web.

4. Insecure Design
   Kesalahan dalam pengembangan sistem yang terjadi mulai dari design. Kesalahan desain ini kemudian dapat dimanfaatkan dengan melakukan eksploitasi struktur desain mana yang tidak kuat atau lemah dalam pengamanannya.
   Pada website ini masih terdapat beberapa design / arsitektur web yang kurang baik, seperti bagian FTP yang dapat langsung diakses oleh guest.

5. Security misconfigurations
   Terjadi kesalahan pengaturan atau konfigurasi keamanan yang menyebabkan beberapa data menjadi lebih kompleks dan susah dijalankan dengan optimal dan menyebabkan beberapa kerentanan pada sistem yang tidak mampu berjalan dengan optimal.
   Pada percobaan ini ditemui bahwa langkah preventif untuk keamanan web masih belum sempurna, contohnya pada pengaksesan beberapa bagian penting seperti akun, yang masih bisa dilakukan meski hanya login menggunakan masukan role, dan langkah preventif yang dilakukan hanya mengalihkan halaman.

6. Vulnerable and Outdated Components
   Penggunaan komponen pada produk yang kurang jelas latar belakangnya atau komponen yang tidak memiliki pembaruan dalam pengembangannya sehingga mungkin keamanannya telah dapat dieksploitasi, sementara komponen tidak lagi dapat memperbaharui perlindungan.
   Pada percobaan ini ditemui bahwa ada beberapa komponen yang masih menggunakan metode lama dan mengakibatkan komponen cukup lama untuk loading.

7. Identification and authentication failures
   Kesalahan dalam proses identifikasi dan autentikasi sebuah masukan yang berakibat pada bebasnya suatu masukan dapat dijalankan di dalam sistem.
   Pada hal ini, percobaan melakukan bypass akun masih dapat dilakukan dan aktivitas mencurigakan user masih tidak dilakukan tindakan preventif. Contohnya adalah user Jim dapat melihat keranjang belanja milik user Bender yang seharusnya tidak bisa dilakukan.

8. Software and Data Integrity Failures
   Penggunaan perangkat atau data tambahan yang tidak terjamin integritasnya sehingga dapat menyebabkan hal yang tidak diinginkan terjadi.
   Pada percobaan kali ini penulis belum dapat membuktikan apakah failure ini ada atau belum.

9. Security Logging and Monitoring Failures
   Kesalahan dalam melakukan pemantauan dan pengawasan log atau history dari setiap aktivitas aneh yang terjadi pada sistem yang dibiarkan terjadi tanpa ada filter atau penyaringan yang benar.
   Pada percobaan kali ini penulis belum dapat membuktikan apakah failure ini ada atau belum.

10. Server-side Request Forgery
    Eksploitasi yang dilakukan dengan merequest atau men-generate data tanpa dilakukan verifikasi yang benar karena data yang direquest hampir sama dengan data yang ada.
    Pada penelitian ini, hampir semua percobaan dapat dilakukan karena melakukan request melalui console pada server side, termasuk dalam mengakses akun, melihat keranjang user lain, menambah item pada keranjang orang lain, admin mengubah review orang lain pada suatu produk, dan lain sebagainya.