

# **INSTAL OWASP JUICE SHOP**



**DI SUSUN OLEH :**

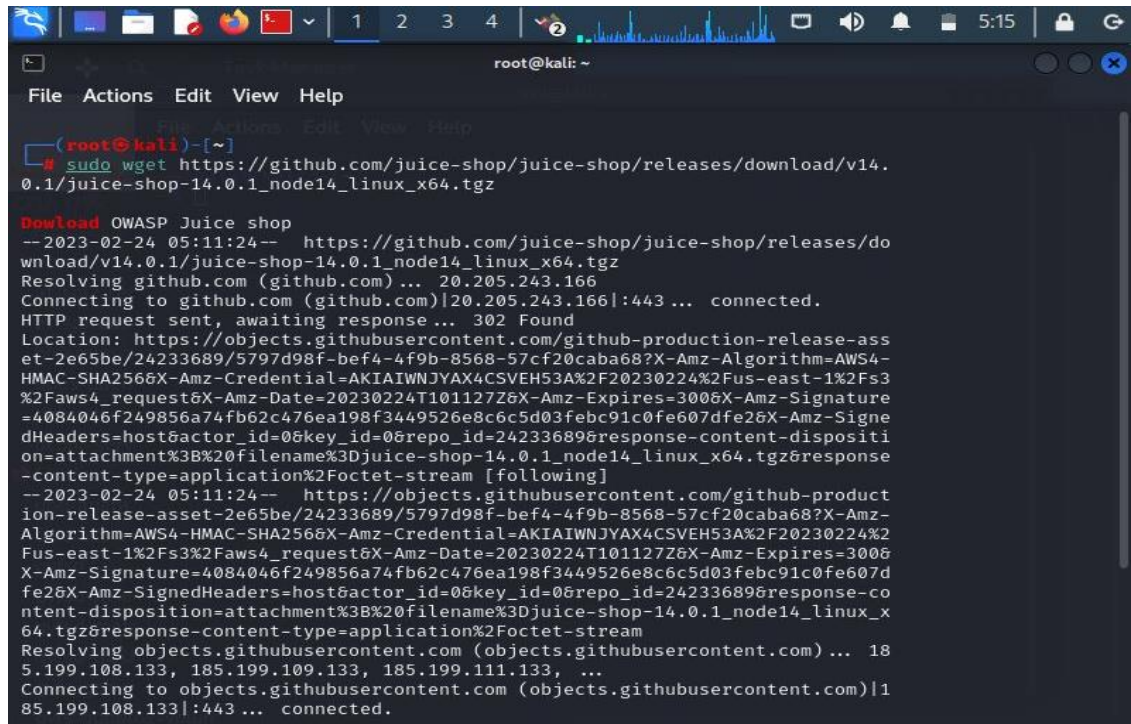
Nadya Indah Trisnawati

3122640034

**PROGRAM STUDI TEKNIK INFORMATIKA  
DEPARTEMEN TEKNIK INFORMATIKA DAN KOMPUTER  
POLITEKNIK ELEKTRONIKA NEGERI SURABAYA**

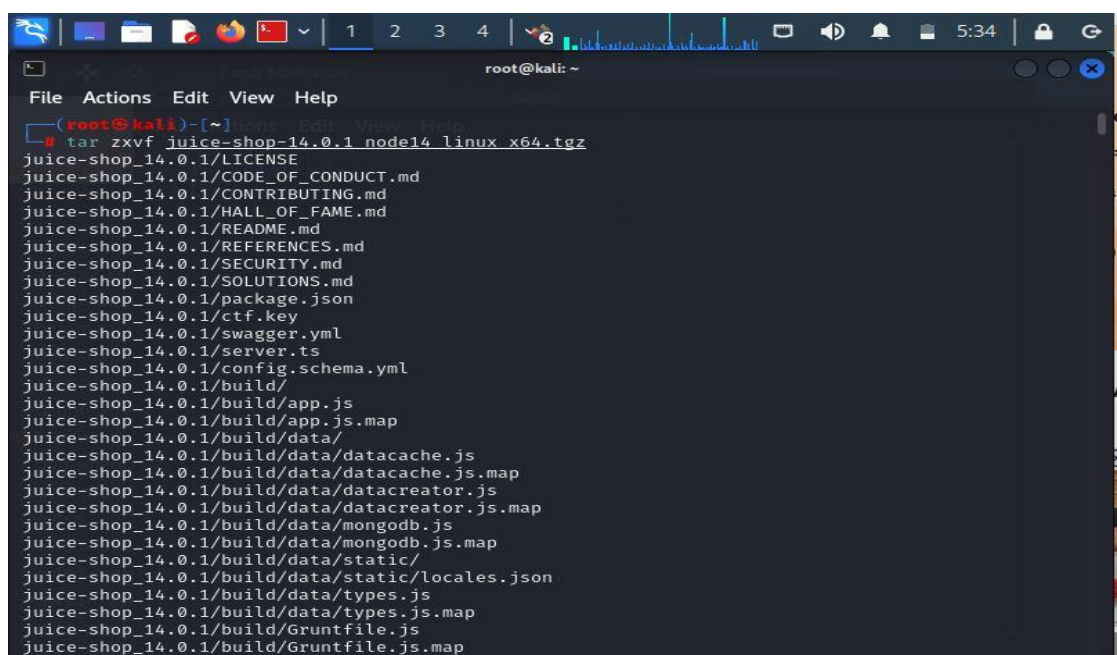
## 1. Download OWASP Juice Shop

- Menginstal OWASP Juice Shop versi terbaru 14.0.1 dari halaman resmi GitHub. menggunakan perintah `wget` untuk mengunduh file di lokasi yang di inginkan. Dengan cara klik kanan pada versi OWASP yang ingin di unduh dan memilih opsi "copy link address atau copy link location".
- Membuka Terminal Kali Linux dan menggunakan `cd` command untuk menavigasi ke lokasi tempat mengunduh file OWASP Juice Shop. menggunakan sintaks di bawah ini untuk mengunduh file zip pada sistem.



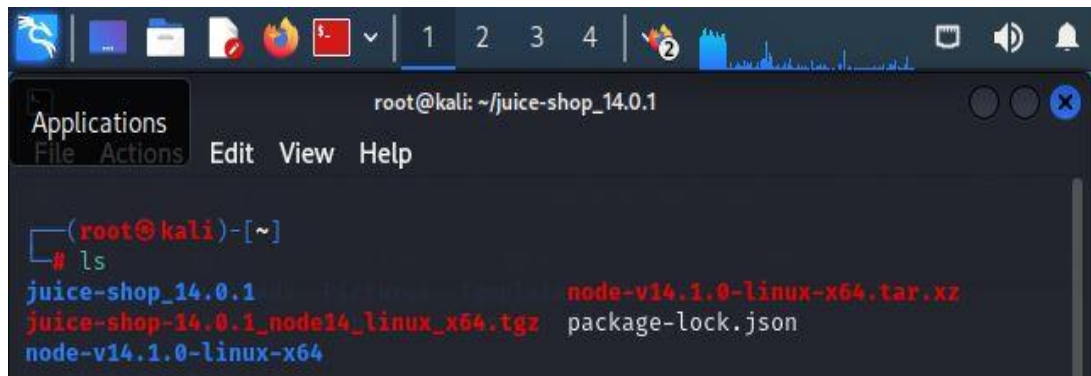
```
root@kali: ~  
File Actions Edit View Help  
(root@kali)~  
# sudo wget https://github.com/juice-shop/juice-shop/releases/download/v14.0.1/juice-shop-14.0.1_node14_linux_x64.tgz  
  
Download OWASP Juice shop  
--2023-02-24 05:11:24-- https://github.com/juice-shop/juice-shop/releases/download/v14.0.1/juice-shop-14.0.1_node14_linux_x64.tgz  
Resolving github.com (github.com)... 20.205.243.166  
Connecting to github.com (github.com)|20.205.243.166|:443 ... connected.  
HTTP request sent, awaiting response... 302 Found  
Location: https://objects.githubusercontent.com/github-production-release-asset-2e65be/24233689/5797d98f-bef4-4f9b-8568-57cf20caba68?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIWNYAX4CSVEH53A%2F20230224%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20230224T101127Z&X-Amz-Expires=300&X-Amz-Signature=4084046f249856a74fb62c476ea198f3449526e8c6c5d03febc91c0fe607dfe26X-Amz-SignedHeaders=host&actor_id=0&key_id=0&repo_id=24233689&response-content-disposition=attachment%3B%20filename%3Djuice-shop-14.0.1_node14_linux_x64.tgz&response-content-type=application%2Foctet-stream [following]  
--2023-02-24 05:11:24-- https://objects.githubusercontent.com/github-production-release-asset-2e65be/24233689/5797d98f-bef4-4f9b-8568-57cf20caba68?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIWNYAX4CSVEH53A%2F20230224%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20230224T101127Z&X-Amz-Expires=300&X-Amz-Signature=4084046f249856a74fb62c476ea198f3449526e8c6c5d03febc91c0fe607dfe26X-Amz-SignedHeaders=host&actor_id=0&key_id=0&repo_id=24233689&response-content-disposition=attachment%3B%20filename%3Djuice-shop-14.0.1_node14_linux_x64.tgz&response-content-type=application%2Foctet-stream  
Resolving objects.githubusercontent.com (objects.githubusercontent.com)... 185.199.108.133, 185.199.109.133, 185.199.111.133, ...  
Connecting to objects.githubusercontent.com (objects.githubusercontent.com)|185.199.108.133|:443 ... connected.
```

- Extract file dalam format “zip”, menggunakan perintah `unzip` seperti pada gambar.



```
root@kali: ~  
File Actions Edit View Help  
(root@kali)~  
# tar xzvf 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  
juice-shop_14.0.1/build/data/mongodb.js  
juice-shop_14.0.1/build/data/mongodb.js.map  
juice-shop_14.0.1/build/data/static/  
juice-shop_14.0.1/build/data/static/locales.json  
juice-shop_14.0.1/build/data/types.js  
juice-shop_14.0.1/build/data/types.js.map  
juice-shop_14.0.1/build/Gruntfile.js  
juice-shop_14.0.1/build/Gruntfile.js.map
```

- d. File yang telah di extract dapat dilihat pada versi aplikasi web.

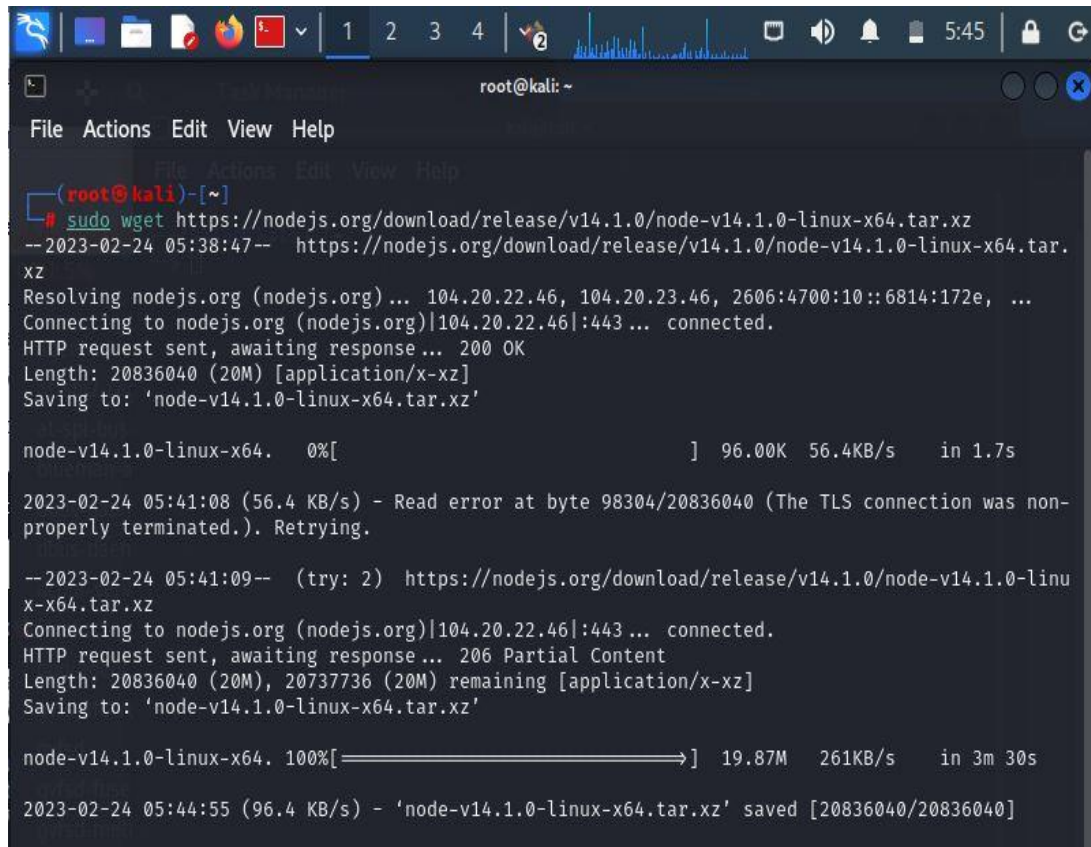


```
root@kali: ~/juice-shop_14.0.1
Applications
File Actions Edit View Help

(root@kali)-[~]
# ls
juice-shop_14.0.1 node-v14.1.0-linux-x64.tar.xz
juice-shop-14.0.1_node14_linux_x64.tgz package-lock.json
node-v14.1.0-linux-x64
```

## 2. Menginstal Node JS dan NPM

- a. Menginstal versi Node JS dengan alamat "NodeJS for x64 Linux systems" yang mirip dengan versi OWASP Juice Shop 14.0.1, yaitu mengunduh Node JS dengan versi 14. Menginstal Node JS dengan perintah wget seperti gambar dibawah.



```
root@kali: ~
File Actions Edit View Help

(root@kali)-[~]
# sudo wget https://nodejs.org/download/release/v14.1.0/node-v14.1.0-linux-x64.tar.xz
--2023-02-24 05:38:47-- https://nodejs.org/download/release/v14.1.0/node-v14.1.0-linux-x64.tar.xz
Resolving nodejs.org (nodejs.org)... 104.20.22.46, 104.20.23.46, 2606:4700:10::6814:172e, ...
Connecting to nodejs.org (nodejs.org)|104.20.22.46|: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-x64.  0%[          ] 96.00K  56.4KB/s  in 1.7s

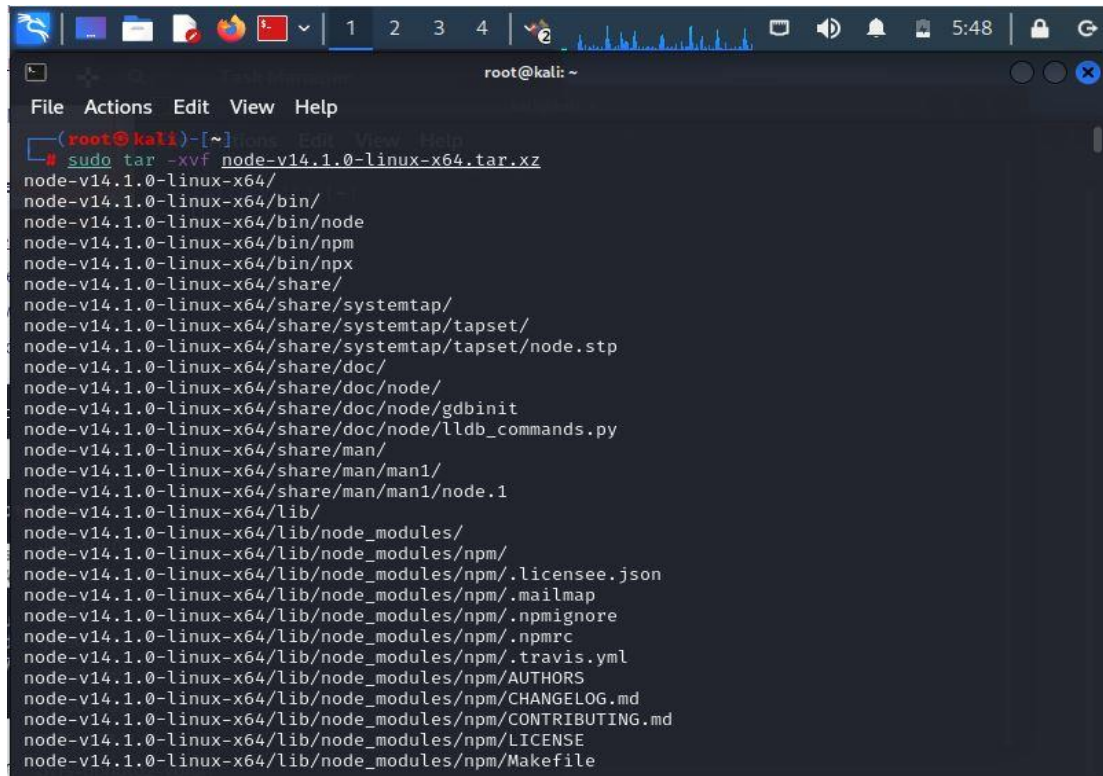
2023-02-24 05:41:08 (56.4 KB/s) - Read error at byte 98304/20836040 (The TLS connection was non-
properly terminated.). Retrying.

--2023-02-24 05:41:09-- (try: 2) https://nodejs.org/download/release/v14.1.0/node-v14.1.0-linu
x-x64.tar.xz
Connecting to nodejs.org (nodejs.org)|104.20.22.46|:443 ... connected.
HTTP request sent, awaiting response... 206 Partial Content
Length: 20836040 (20M), 20737736 (20M) remaining [application/x-xz]
Saving to: 'node-v14.1.0-linux-x64.tar.xz'

node-v14.1.0-linux-x64. 100%[=====>] 19.87M  261KB/s  in 3m 30s

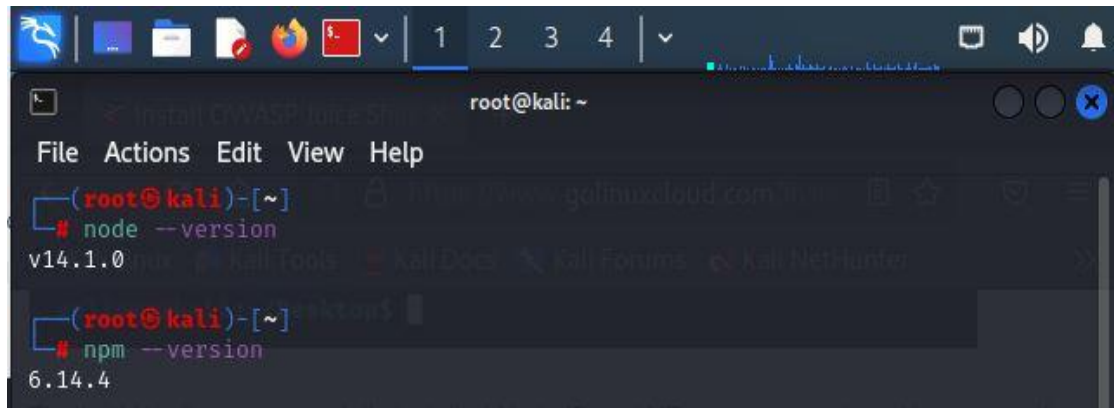
2023-02-24 05:44:55 (96.4 KB/s) - 'node-v14.1.0-linux-x64.tar.xz' saved [20836040/20836040]
```

- b. Extract isi file yang telah di install menggunakan perintah tar.



```
root@kali: ~  
File Actions Edit View Help  
(root@kali)~  
# sudo 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  
node-v14.1.0-linux-x64/lib/node_modules/npm/.npmrc  
node-v14.1.0-linux-x64/lib/node_modules/npm/.travis.yml  
node-v14.1.0-linux-x64/lib/node_modules/npm/AUTHORS  
node-v14.1.0-linux-x64/lib/node_modules/npm/CHANGELOG.md  
node-v14.1.0-linux-x64/lib/node_modules/npm/CONTRIBUTING.md  
node-v14.1.0-linux-x64/lib/node_modules/npm/LICENSE  
node-v14.1.0-linux-x64/lib/node_modules/npm/Makefile
```

- c. Akan muncul folder “node” baru yang dibuat di sistem. Beberapa file yang harus disalin dari folder yang baru di extract ke di rektori /usr untuk menginstal Node JS dan NPM. Node JS dan NPM telah berhasil di install.

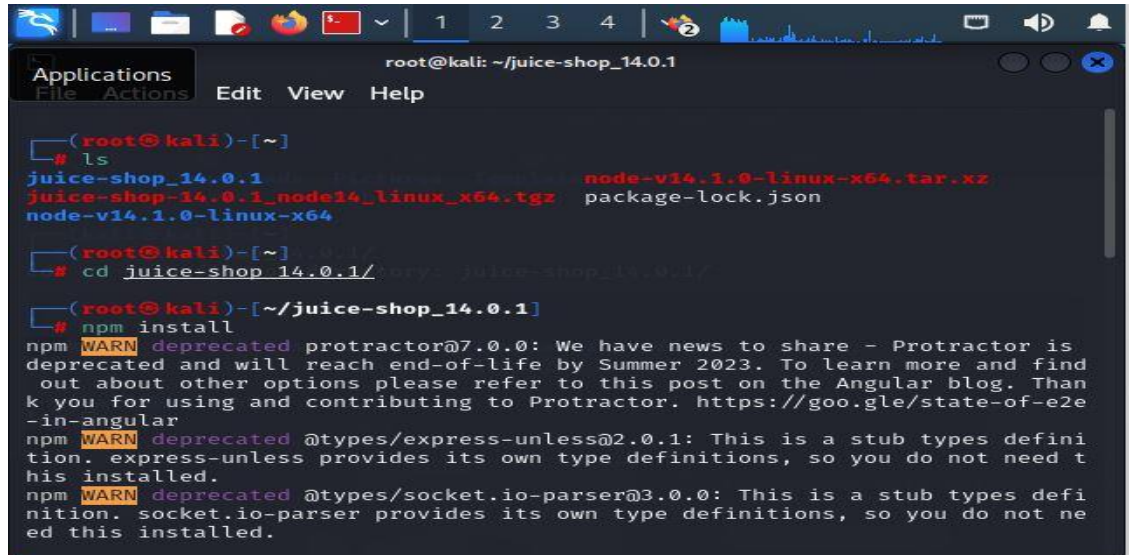


```
root@kali: ~  
File Actions Edit View Help  
(root@kali)~  
# node --version  
v14.1.0  
(root@kali)~  
# npm --version  
6.14.4
```



### 3. Instal Node Dependencies

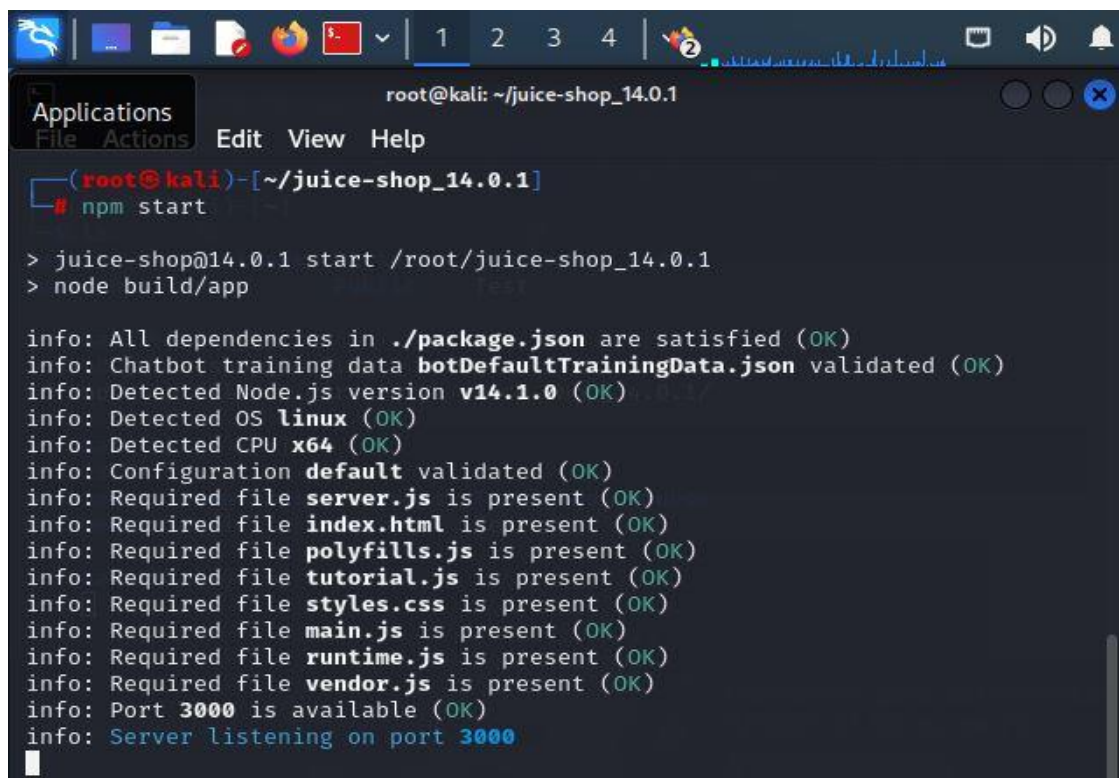
- a. Menggunakan perintah “cd” untuk mengubah direktori ke folder tersebut. Kemudian menjalankan perintah untuk menginstal paket Node yang diperlukan untuk menjalankan OWASP Juice Shop.



```
root@kali: ~/juice-shop_14.0.1
# ls
juice-shop_14.0.1  node-v14.1.0-linux-x64.tar.xz
juice-shop-14.0.1_node14_linux_x64.tgz  package-lock.json
node-v14.1.0-linux-x64

# cd juice-shop_14.0.1/
# npm install
npm WARN deprecated protractor@7.0.0: We have news to share - Protractor is deprecated and will reach end-of-life by Summer 2023. To learn more and find out about other options please refer to this post on the Angular blog. Thank you for using and contributing to Protractor. https://goo.gle/state-of-e2e-in-angular
npm WARN deprecated @types/express-unless@2.0.1: This is a stub types definition. express-unless provides its own type definitions, so you do not need this installed.
npm WARN deprecated @types/socket.io-parser@3.0.0: This is a stub types definition. socket.io-parser provides its own type definitions, so you do not need this installed.
```

- b. Setelah selesai, menjalankan perintah seperti pada gambar untuk menjalankan OWASP Juice Shop.

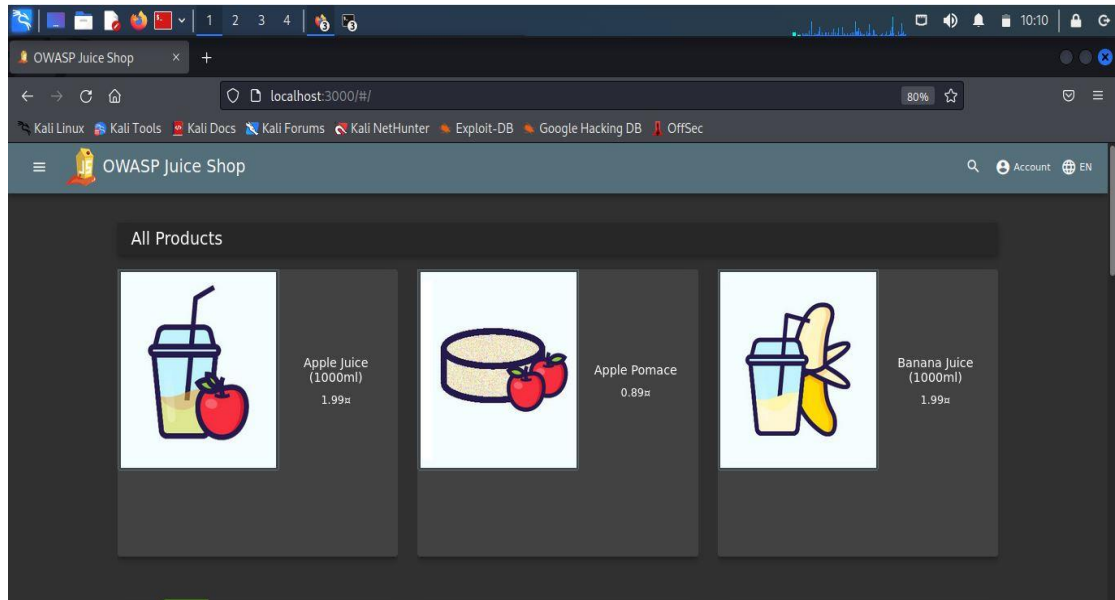


```
root@kali: ~/juice-shop_14.0.1
# npm start

> juice-shop@14.0.1 start /root/juice-shop_14.0.1
> node build/app

info: All dependencies in ./package.json are satisfied (OK)
info: Chatbot training data botDefaultTrainingData.json validated (OK)
info: Detected Node.js version v14.1.0 (OK)
info: Detected OS linux (OK)
info: Detected CPU x64 (OK)
info: Configuration default validated (OK)
info: Required file server.js is present (OK)
info: Required file index.html is present (OK)
info: Required file polyfills.js is present (OK)
info: Required file tutorial.js is present (OK)
info: Required file styles.css is present (OK)
info: Required file main.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: Server listening on port 3000
```

- c. Pada perintah ini akan memulai aplikasi web pada port 3000. Namun, jika terdapat aplikasi lain yang berjalan di port tersebut, dapat memilih menggunakan port lain seperti 3001. Membuka browser dan memasukkan URL seperti gambar dibawah untuk mengakses aplikasi web.
- d. Setelah itu, akan muncul halaman web sederhana seperti gambar dibawah yang menampilkan beberapa jus buah yang dapat dibeli. Dan OWASP Juice Shop telah berhasil di install.



#### **4. Hubungan Antara OWASP 10 dengan Aplikasi Juice Shop**

Hubungan antara OWASP Top 10 2022 dan Juiceshop adalah bahwa aplikasi Juiceshop didesain untuk mencontohkan sejumlah besar kerentanan yang ada pada daftar OWASP Top 10, sehingga pengguna dapat belajar bagaimana menemukan, mengeksploitasi, dan mengatasi kerentanan keamanan pada aplikasi web. Aplikasi Juiceshop dilengkapi dengan beberapa kerentanan yang paling umum ditemukan pada aplikasi web, seperti Injection, Broken Authentication and Session Management, Cross-Site Scripting (XSS), dan Broken Access Control.

Dengan menggunakan aplikasi Juiceshop, pengguna dapat mempraktikkan teknik-teknik pengujian keamanan seperti penetrasi, serangan brute-force, dan pengujian penetrasi manual untuk melihat seberapa mudahnya untuk mengeksploitasi kerentanan keamanan pada aplikasi web. Dengan demikian, Juiceshop dapat menjadi alat yang berguna bagi pengembang dan profesional keamanan untuk meningkatkan kemampuan mereka dalam mengidentifikasi, mengeksploitasi, dan mengatasi kerentanan keamanan pada aplikasi web.

#### **5. 10 Kerentanan Populer Pada Aplikasi Web (OWASP 10)**

OWASP (Open Web Application Security Project) adalah sebuah organisasi nirlaba yang berfokus pada peningkatan keamanan aplikasi web. OWASP mengeluarkan daftar OWASP Top 10 yang mencakup 10 kerentanan paling umum yang ditemukan pada aplikasi web. Berikut adalah penjelasan singkat tentang OWASP Top 10:

1. Injection  
Kerentanan ini terjadi ketika aplikasi menerima input yang tidak valid dari pengguna, yang dapat menyebabkan penggunaan kode berbahaya atau manipulasi database.
2. Broken Authentication and Session Management  
Kerentanan ini terjadi ketika mekanisme otentikasi dan manajemen sesi di aplikasi tidak diatur dengan benar, sehingga memungkinkan serangan oleh pengguna yang tidak sah.
3. Cross-Site Scripting (XSS)  
Kerentanan ini terjadi ketika aplikasi menerima input yang tidak valid dari pengguna yang memungkinkan serangan skrip berbahaya di browser pengguna.
4. Broken Access Control  
Kerentanan ini terjadi ketika aplikasi tidak membatasi akses pengguna ke sumber daya yang seharusnya tidak dapat diakses.
5. Security Misconfiguration  
Kerentanan ini terjadi ketika konfigurasi aplikasi tidak dilakukan dengan benar, sehingga memungkinkan serangan oleh penyerang.
6. Insecure Cryptographic Storage  
Kerentanan ini terjadi ketika data sensitif disimpan dalam format yang mudah dipecahkan oleh penyerang.
7. Insufficient Transport Layer Protection

Kerentanan ini terjadi ketika komunikasi antara server dan klien tidak dilindungi dengan benar.

8. Insufficient Logging and Monitoring

Kerentanan ini terjadi ketika aplikasi tidak mencatat atau memonitor aktivitas yang mencurigakan atau aneh, sehingga tidak dapat mendeteksi atau mengatasi serangan.

9. Insecure Communication

Kerentanan ini terjadi ketika aplikasi menggunakan protokol komunikasi yang rentan terhadap serangan.

10. Using Components with Known Vulnerabilities

Kerentanan ini terjadi ketika aplikasi menggunakan komponen yang telah diketahui memiliki kerentanan keamanan, yang dapat dimanfaatkan oleh penyerang.