Praktikum Keamanan Jaringan

Oleh:

Aldo Faiz Winarno (3122640039)

D4 LJ IT B

POLITEKNIK ELEKTRONIKA NEGERI SURABAYA

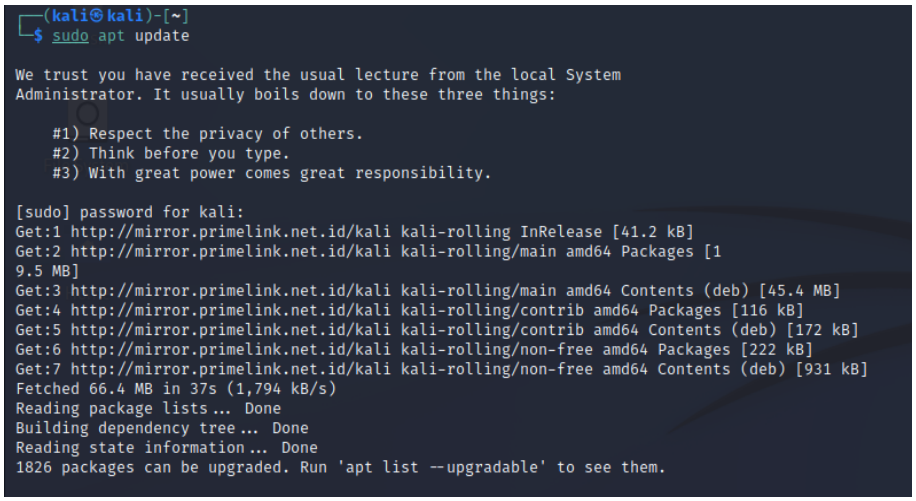
TAHUN 2023

Instalasi Aplikasi Web Juice Shop pada Kali Linux

Langkah 1. Instal NodeJS dan NPM

Mengupdate Kali Linux

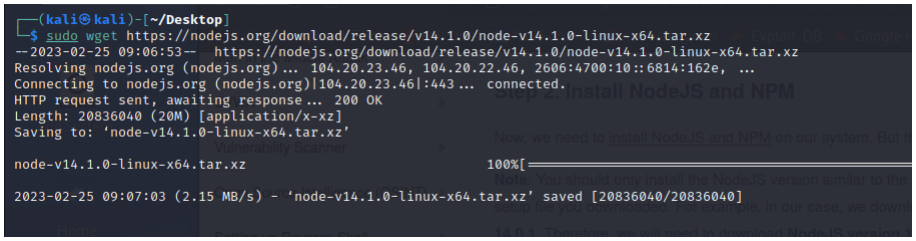
```
sudo apt update
```



Keterangan: Perintah tersebut digunakan untuk memperbaharui paket list program computer pada Linux.

Mendownload Nodejs

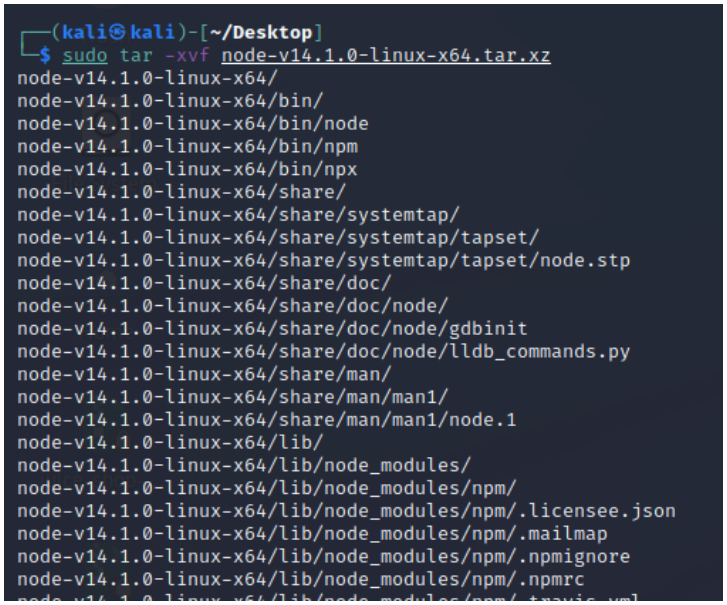
```
sudo wget https://nodejs.org/download/release/v14.1.0/node-v14.1.0-linux-x64.tar.xz
```



Keterangan: Mengunduh file NodeJS untuk sistem Linux x64 pada situs web resmi NodeJS menggunakan perintah “wget”.

Mengekstrak Folder Hasil Download Nodejs

```
sudo tar -xvf node-v14.1.0-linux-x64.tar.xz
```



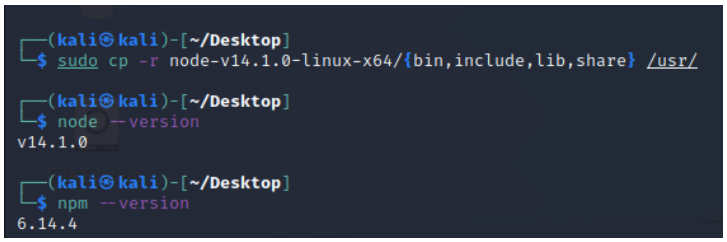
Keterangan: Mengekstrak folder hasil download nodejs dengan command “tar”.

Mengcopy Folder ke Sistem dan Mengecek Versi

```
sudo cp -r node-v14.1.0-linux-x64/{bin,include,lib,share} /usr/
```

```
node --version
```

```
npm --version
```

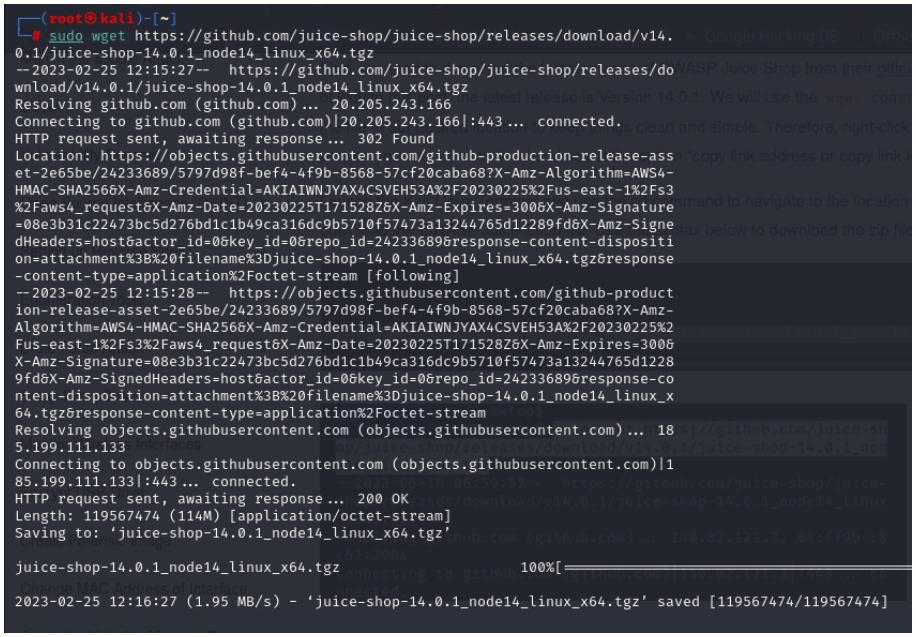


Keterangan: Memasukkan hasil install Nodejs dan NPM ke dalam system, kemudian mengecek versi nodejs dan npm. Pada gambar diatas v14.1.0 merupakan versi dari nodejs dan 6.14.4 merupakan versi dari npm.

Langkah 2. Mendownload Juice Shop

Mendownload Aplikasi Web Juice Shop

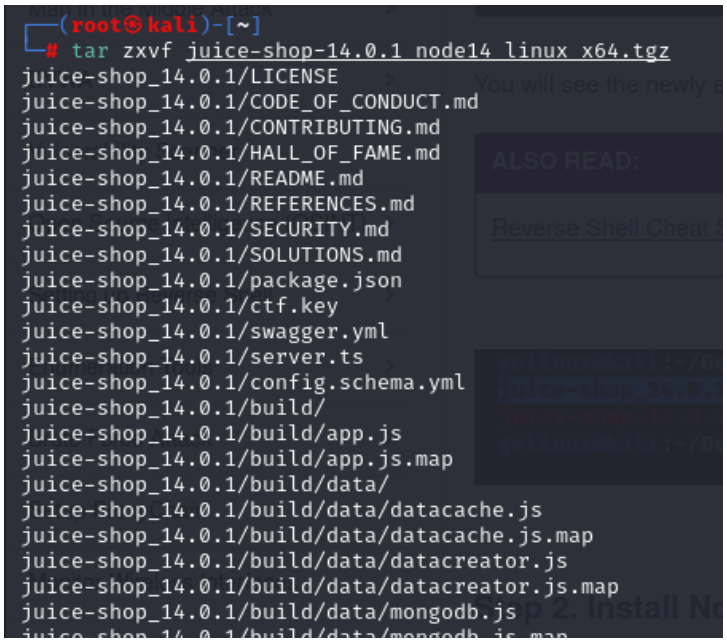
```
sudo wget https://github.com/juice-shop/juice-shop/releases/download/v14.0.1/juice-shop-14.0.1_node14_linux_x64.tgz
```



Keterangan: Sebelum mendownload OWASP Juice Shop perlu masuk kedalam root terlebih dahulu, kemudian mendownload OWASP Juice Shop melalui akun resmi github menggunakan perintah “wget”. Versi yang digunakan adalah 14.0.1.

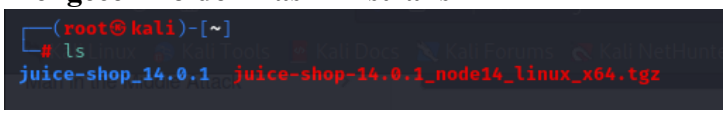
Mengekstrak Folder Hasil Download Aplikasi Web Juice Shop

```
sudo cp -r node-v14.1.0-linux-x64/{bin,include,lib,share} /usr/
```



Keterangan: Mengekstrak folder hasil download juice shop dengan command “tar”.

Mengecek Folder Hasil Ekstraksi

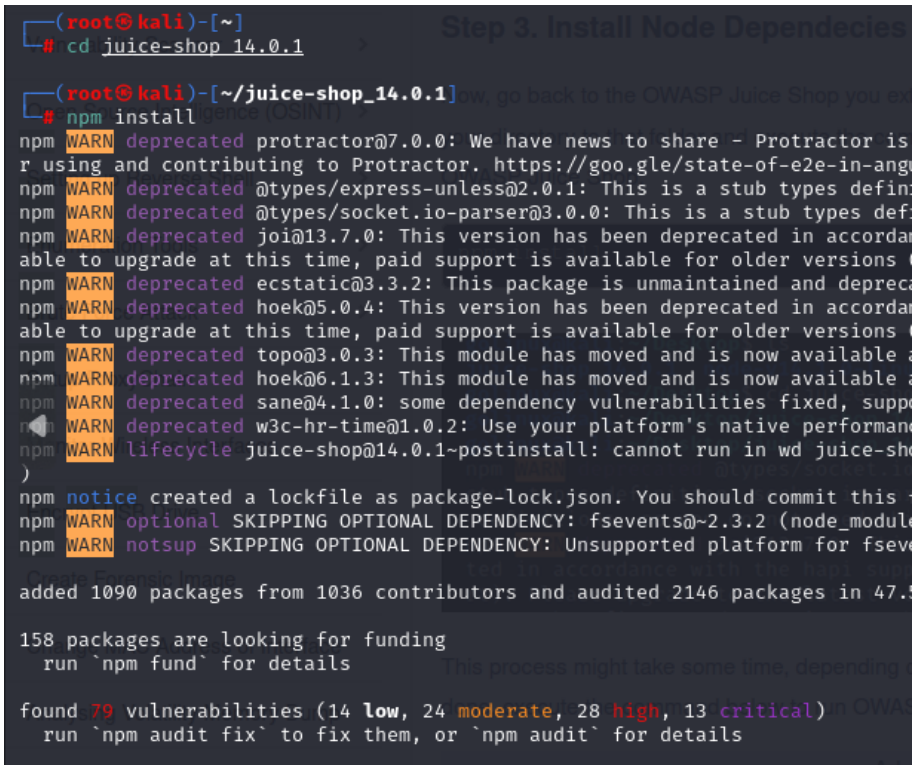


Keterangan: Untuk mengecek folder yang ada didalam dapat menggunakan command “ls”.

Langkah 3. Install Node Dependecies

Menginstall Paket Node pada Folder Aplikasi Web Juice Shop

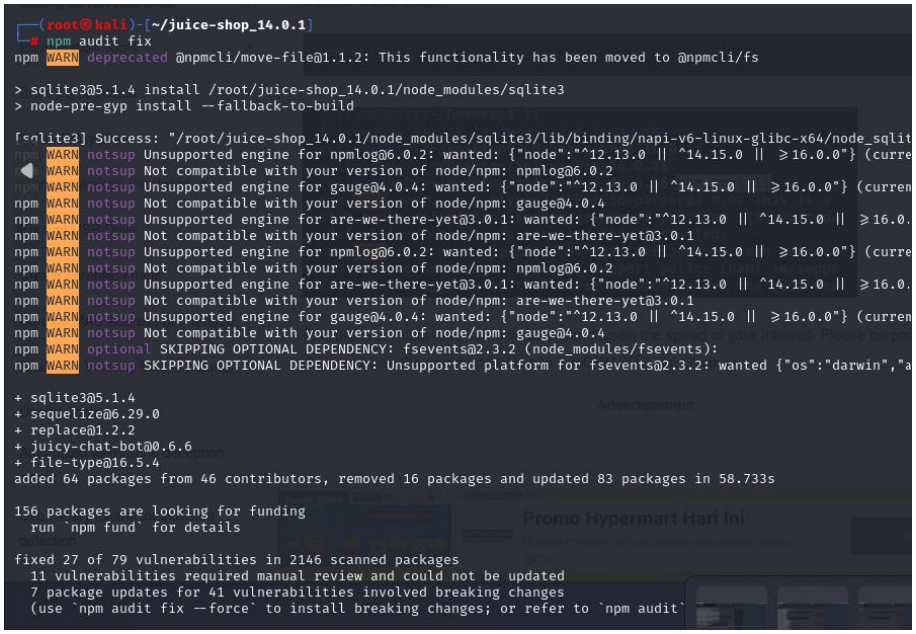
```
npm install
```



Keterangan: Sebelum menginstall paket node pada folder juice shop perlu untuk masuk kedalam folder juice shop dengan menggunakan command “cd”. Setelah masuk kedalam folder juice shop dapat memasukkan perintah “npm install”.

Memperbaiki Masalah Pada Proses Penginstallan Paket Node

```
npm audit fix
```



Keterangan: “npm audit fix” digunakan untuk memperbaiki kerentanan atau masalah pada proses penginstallan yang bertujuan mencegah hal-hal seperti kehilangan data, pemadaman layanan, dan akses tidak sah ke informasi sensitif.

Langkah 4. Menjalankan Aplikasi Web Juice Shop

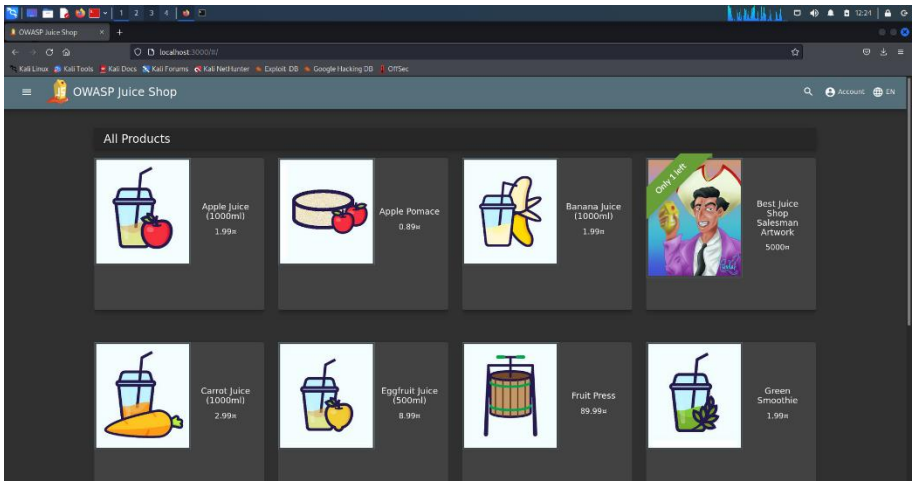
Menjalankan Aplikasi Web Juice Shop

```
npm start
```

Keterangan: Menjalankan aplikasi web juice shop menggunakan “npm start” dengan port 3000.

Tampilan Aplikasi Web Juice Shop

http://localhost:3000/



Keterangan: Membuka tampilan aplikasi web juice shop pada browser dengan memasukkan URL http://localhost:3000/ .

Hubungan Antara OWASP 10 2022 dengan Aplikasi Juice Shop

OWASP Top 10 adalah daftar risiko keamanan aplikasi web yang paling umum dan penting yang disusun oleh Organisasi Keamanan Aplikasi Web Terbuka (OWASP). Daftar ini diperbarui secara berkala untuk mencerminkan tren dan tantangan keamanan terbaru dalam pengembangan aplikasi web.

Sementara itu, Juice Shop adalah aplikasi web yang dirancang khusus sebagai contoh aplikasi yang rentan terhadap beberapa risiko keamanan dalam daftar OWASP Top 10. Aplikasi ini bertujuan untuk membantu pengembang dan profesional keamanan memahami bagaimana risiko keamanan pada daftar OWASP Top 10 dapat terjadi dalam praktiknya.

Oleh karena itu, OWASP Top 10 2022 dan Juice Shop saling terkait karena Juice Shop dirancang untuk menunjukkan contoh konkret tentang bagaimana risiko keamanan dalam OWASP Top 10 dapat terjadi dalam aplikasi web nyata. Dengan menggunakan Juice Shop, pengembang dan profesional keamanan dapat mempelajari cara mengidentifikasi, menghindari, dan memperbaiki masalah keamanan dalam aplikasi web mereka sendiri dengan mengacu pada OWASP Top 10.

10 Kerentanan yang Populer di Aplikasi Web (OWASP 10)

Broken Access Control
Kerentanan ini terjadi ketika sistem tidak memvalidasi atau memverifikasi akses pengguna terhadap sumber daya sistem yang dilindungi, sehingga penyerang dapat mengakses data atau fungsi yang seharusnya tidak dapat diakses.

Cryptographic Failures
Kerentanan keamanan pada sistem yang terkait dengan penggunaan yang salah atau tidak tepat pada teknik kriptografi yaitu teknik untuk melindungi informasi sensitif dengan mengubahnya menjadi format yang tidak dapat dimengerti oleh pihak yang tidak berwenang.

Injection
Kerentanan injeksi terjadi ketika input dari pengguna tidak divalidasi atau di-filter dengan benar, sehingga penyerang dapat memasukkan kode berbahaya atau perintah SQL yang merusak.

Insecure Design
Kerentanan yang merujuk pada kurangnya perancangan atau perencanaan keamanan pada level desain aplikasi web. Hal ini berarti aplikasi web memiliki celah keamanan yang dapat dimanfaatkan oleh penyerang karena tidak dipertimbangkan saat perancangan dan perancanaan.

Security Misconfiguration
Kerentanan ini terjadi ketika konfigurasi keamanan sistem tidak diatur dengan benar, seperti pengaturan default password, izin file yang tidak aman, atau koneksi jaringan yang tidak dienkripsi.

Vulnerable and Outdated Components
Kerentanan yang merujuk pada komponen atau library yang usang dan kurangnya pembaharuan yang digunakan dalam pembangunan aplikasi web .

Identification and Authentication Failures
Kerentanan ini terjadi ketika kontrol akses tidak diterapkan dengan benar pada fungsi autentikasi dan manajemen sesi, sehingga penyerang dapat mendapatkan akses ke akun pengguna atau melakukan serangan phishing.

Software and Data Integrity Failures
Kerentanan yang mengacu pada kegagalan dalam memastikan integritas dari software dan data pada aplikasi web. Integritas adalah kemampuan untuk memastikan bahwa data dan software tidak dirubah oleh pihak yang tidak berwenang dan tetap akurat serta utuh. Kegagalan dalam menjaga integritas dapat menghasilkan kesalahan pada aplikasi web dan membuka celah untuk serangan seperti penyusupan data (*data tampering*) dan perusakan data (*data destruction*).

Security Logging and Monitoring Failures
Kerentanan ini terjadi ketika sistem tidak memadai mencatat atau memantau aktivitas pengguna, sehingga sulit untuk mendeteksi dan mencegah serangan.

Server-Side Request Forgery
Kerentanan ini terjadi ketika penyerang dapat memanipulasi aplikasi untuk membuat permintaan jaringan dari server yang rentan, sehingga memungkinkan penyerang untuk mengakses sumber daya internal atau membuka celah untuk serangan lebih lanjut.