

KEAMANAN JARINGAN

OWASP Juice Shop



OLEH :

Mochammad Jauhar Ulul Albab

NRP : 3122640044

PROGRAM STUDI TEKNIK INFORMATIKA

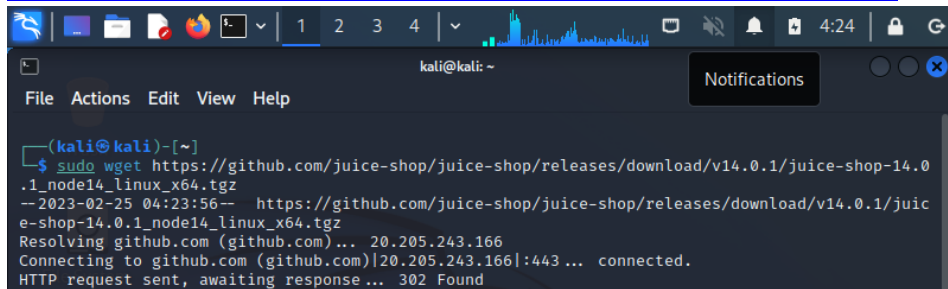
DEPARTEMEN TEKNIK INFORMATIKA DAN KOMPUTER

POLITEKNIK ELEKTRONIKA NEGERI SURABAYA

2022/2023

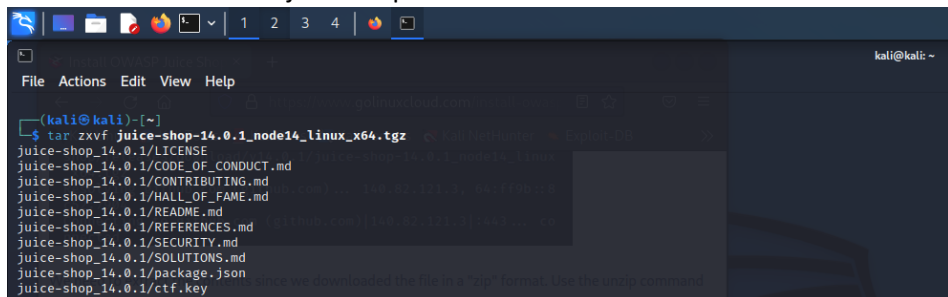
A. INSTALASI JUICE SHOP

1. Download juice shop pada linux dengan cara
"sudo wget https://github.com/juice-shop/juice-shop/releases/download/v14.0.1/juice-shop-14.0.1_node14_linux_x64.tgz"



```
(kali@kali)-[~]
$ sudo wget https://github.com/juice-shop/juice-shop/releases/download/v14.0.1/juice-shop-14.0.1_node14_linux_x64.tgz
--2023-02-25 04:23:56-- 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
```

2. Ekstrak hasil download juice shop



```
(kali@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
```

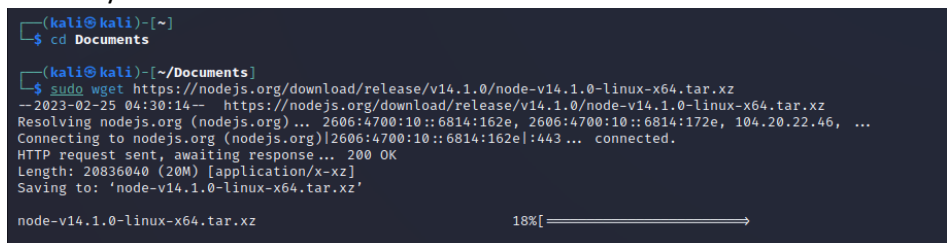
Hasil ekstrak



```
(kali@kali)-[~]
$ ls
Desktop  Documents  Downloads  juice-shop_14.0.1  juice-shop-14.0.1_node14_linux_x64.tgz  Music  Pictures  Public  Templates  Videos
```

3. Download dan install NodeJS dan NPM

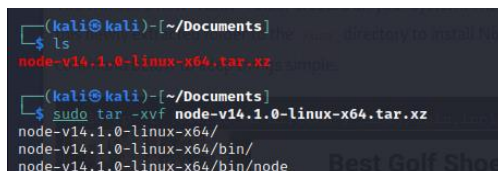
Disini saya menaruh hasil download di folder Documents



```
(kali@kali)-[~]
$ cd Documents
(kali@kali)-[~/Documents]
$ sudo wget https://nodejs.org/download/release/v14.1.0/node-v14.1.0-linux-x64.tar.xz
--2023-02-25 04:30:14-- https://nodejs.org/download/release/v14.1.0/node-v14.1.0-linux-x64.tar.xz
Resolving nodejs.org (nodejs.org)... 2606:4700:10::6814:162e, 2606:4700:10::6814:172e, 104.20.22.46, ...
Connecting to nodejs.org (nodejs.org)|2606:4700:10::6814:162e|: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.tar.xz                               18%[=====>]
```

Kemudian ekstrak hasil download

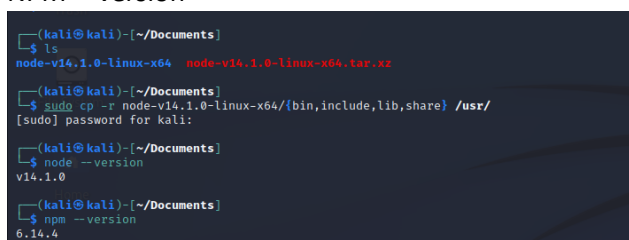


```
(kali@kali)-[~/Documents]
$ ls
node-v14.1.0-linux-x64  node-v14.1.0-linux-x64.tar.xz
(kali@kali)-[~/Documents]
$ sudo tar -xvf node-v14.1.0-linux-x64.tar.xz
node-v14.1.0-linux-x64/
node-v14.1.0-linux-x64/bin/
node-v14.1.0-linux-x64/bin/node
```

Kemudian copy kan folder hasil ekstraksi ke system dan lakukan pengecekan apakah NodeJS dan NPM telah terinstall pada system dengan menggunakan

Node --version

NPM --version



```
(kali@kali)-[~/Documents]
$ ls
node-v14.1.0-linux-x64  node-v14.1.0-linux-x64.tar.xz
(kali@kali)-[~/Documents]
$ sudo cp -r node-v14.1.0-linux-x64/{bin,include,lib,share} /usr/
[sudo] password for kali:
(kali@kali)-[~/Documents]
$ node --version
v14.1.0
(kali@kali)-[~/Documents]
$ npm --version
6.14.4
```

4. Install dependencies NPM pada folder juice shop yang sudah didownload dengan memasuki folder juice shop terlebih dahulu

```
(kali@kali)~$ ls
Desktop  Documents  Downloads  juice-shop_14.0.1  juice-shop-14.0.1_node14_linux_x64.tgz  Music  package-lock.json  Pictures  Public  Templates  Videos

(kali@kali)~$ cd juice-shop_14.0.1

(kali@kali)~/juice-shop_14.0.1$ npm install
npm ERR! code EAI_AGAIN
npm ERR! errno EAI_AGAIN
npm ERR! request to https://registry.npmjs.org/safe-buffer failed, reason: getaddrinfo EAI_AGAIN registry.npmjs.org
npm ERR! A complete log of this run can be found in:
npm ERR! /home/kali/.npm/_logs/2023-02-25T10_02_51_578Z-debug.log
```

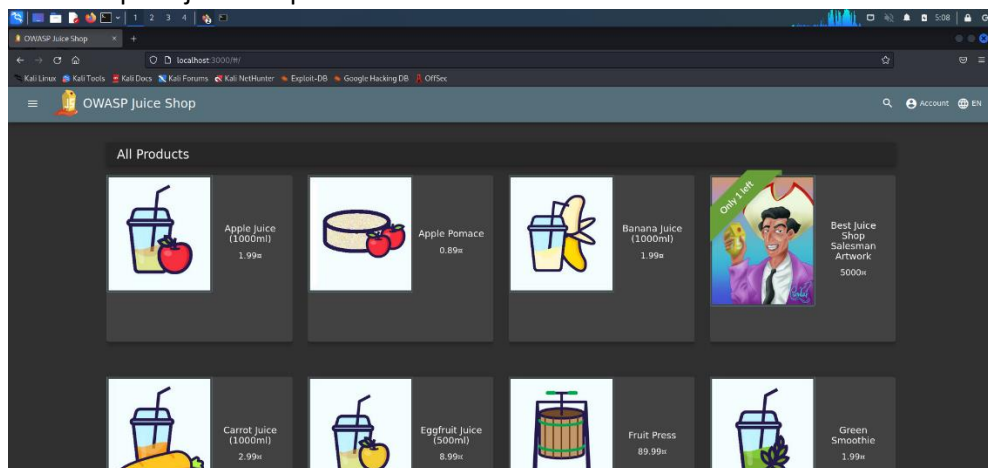
5. Jalankan NPM pada folder juiceshop agar juiceshop dapat diakses

```
(kali@kali)~/juice-shop_14.0.1$ npm start

> juice-shop@14.0.1 start /home/kali/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 tutorial.js 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: Required file styles.css is present (OK)
info: Required file index.html is present (OK)
info: Required file polyfills.js is present (OK)
info: Port 3000 is available (OK)
info: Server listening on port 3000
```

Hasil tampilan juice shop



B. HUBUNGAN OWASP 10 DENGAN JUICESHOP

Juice shop merupakan web aplikasi yang dapat digunakan sebagai pelatihan mengenai keamanan sebuah aplikasi web OWASP 10, karena juice shop merupakan aplikasi web modern yang memiliki keamanan rendah dan mencakup semua kelemahan yang ada pada OWASP 10

C. 10 KERENTANAN APLIKASI WEB

1. Injeksi

Serangan injeksi dapat terjadi pada hal-hal seperti database (SQL, noSQL), sistem operasi, atau server (melalui protokol seperti LDAP). Mereka terjadi ketika data yang tidak bersahabat dikirim ke interpreter sebagai bagian dari kueri atau perintah. Data ini kemudian mengelabui interpreter agar menjalankan perintah yang seharusnya

terlarang bagi orang luar. Itu juga dapat digunakan untuk mengakses data pribadi tanpa otentikasi yang tepat.

2. Kerusakan Autentikasi

Autentikasi yang rusak mengacu pada contoh ketika fungsi autentikasi dan sesi manajemen diterapkan secara tidak benar. Kredensial seperti kata sandi, kunci, atau token sesi dapat dicegat dan mengasumsikan identitas pengguna lain.

3. Terpaparnya Data yang Bersifat Sensitif

Eksposur data sensitif terjadi ketika aplikasi web dan API gagal melindungi data sensitif seperti informasi keuangan atau perawatan kesehatan. Data yang terlindungi secara lemah ini dapat dengan mudah dicuri oleh penyerang untuk melakukan penipuan, pencurian identitas, dan kejahatan lainnya.

Jika situs web tidak menggunakan sertifikat SSL/TLS berkualitas untuk semua halaman, maka penyerang dapat memantau lalu lintas, mengubah koneksi dari HTTPS ke HTTP, dan kemudian mencuri sesi cookie untuk mendapatkan akses. Contoh lainnya adalah hash yang kurang.

4. XML EXTERNAL ENTITIES (XXE)

Serangan semacam ini menargetkan aplikasi web yang mengurai input XML. Prosesor XML yang lebih lama atau tidak dikonfigurasi dengan benar dapat mengevaluasi referensi entitas eksternal (seperti hard drive) dalam dokumen XML. Hal ini dapat mengelabui pengurai XML agar mengirimkan data ke entitas eksternal yang tidak sah, yang kemudian dapat mengirim data sensitif langsung ke peretas.

5. Kontrol Akses Rusak

terjadi ketika pembatasan tentang apa yang diizinkan/tidak diizinkan oleh pengguna yang diberlakukan autentikasi secara tidak benar. Serangan kemudian dapat memanfaatkan untuk mendapatkan fungsionalitas yang tidak sah, termasuk mengakses dan mengubah akun pengguna, file sensitif, data pengguna, hak akses, dan banyak lagi.

6. Kesalahan Konfigurasi Keamanan

kerentanan paling umum pada Daftar OWASP Top Ten dan biasanya disebabkan oleh penggunaan konfigurasi/kredensial default atau menampilkan pesan kesalahan yang panjang dan tidak perlu. Pesan-pesan ini berpotensi mengungkapkan kerentanan dalam aplikasi.

7. CROSS-SITE SCRIPTING (XSS)

Jenis kerentanan ini merupakan hasil dari sesi manajemen yang lemah dan terjadi saat aplikasi web memungkinkan pengguna menambahkan kode khusus ke URL atau situs yang akan ditampilkan kepada orang lain. Kode JavaScript berbahaya kemudian dapat dijalankan di browser mereka.

8. Deserialisasi yang Tidak Aman

Deserialization memungkinkan peretas untuk mengeksekusi kode berbahaya di server. Meskipun kerentanan tidak mengakibatkan eksekusi kode jarak jauh, penyerang masih dapat menggunakannya untuk melakukan tindakan seperti serangan berulang, serangan injeksi, dan serangan eskalasi hak istimewa.

9. Penggunaan Komponen Dengan Kerentanan yang Tidak Diketahui

Web developer sering menggunakan komponen yang ada dalam aplikasi untuk menghindari pekerjaan yang berlebihan sambil menyediakan fungsionalitas yang dibutuhkan. Penyerang akan mencari kerentanan di dalam komponen ini yang dapat mereka manfaatkan untuk melakukan serangan pada aplikasi itu sendiri. Komponen populer dapat digunakan di ratusan ribu situs, dan satu kerentanan dapat membuat semuanya berisiko.

10. Pencatatan & Pemantauan yang Tidak Memadai

Pencatatan (logging) dan pemantauan harus dilakukan secara rutin untuk membantu memastikan keamanan web bekerja maksimal. Kegagalan mampu meningkatkan risiko serangan yang dapat terjadi dan menghambat waktu respons situs Anda. Hal ini pada gilirannya memberi penyerang cukup banyak waktu untuk merusak, mengekstrak, atau menghancurkan data, beralih ke sistem lain, dan mengacak-acak semua yang ada di dalamnya.