

LAPORAN RESMI PRAKTIKUM KEMANAN JARINGAN

INSTALASI OWASP JUICE SHOP



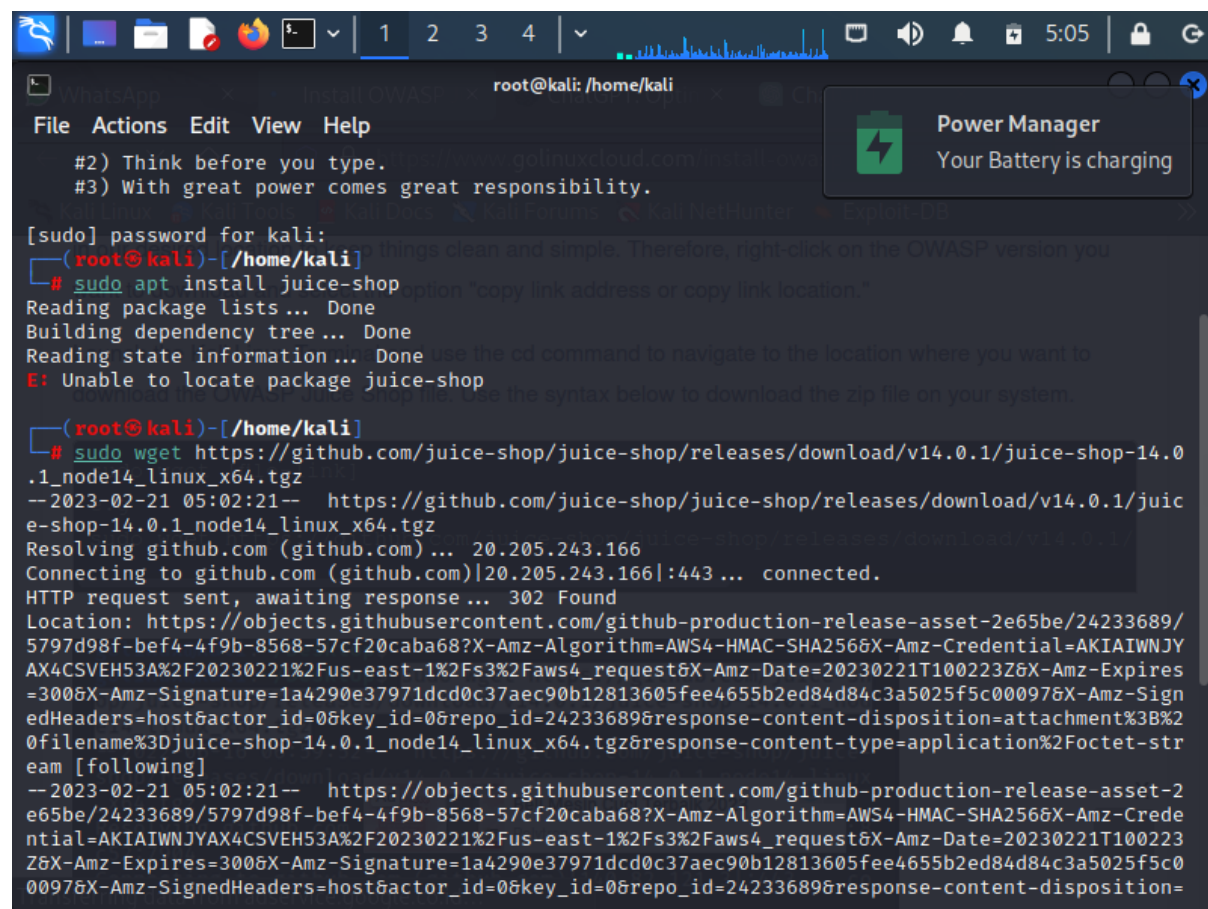
**Dosen :
Dr. Ferry Astika Saputra ST, M.Sc
Oleh :
Septiana Dyah Anissawati
D4 LJ Teknik Informatika B
3122640031**

**POLITEKNIK ELEKTRONIKA NEGERI SURABAYA
TAHUN AJARAN
2022/2023**

Jelaskan proses instalasi aplikasi WEB dengan kerentanan OWASP JUICE SHOP <https://owasp.org/www-project-juice-shop/> pada web server yang dijalankan diatas sembarang OS dengan virtualisasi VMWARE ataupun Virtual Box. Jelaskan juga hubungan anantara OWASP 10 2022 dengan aplikasi Juiceshop ! Jelaskan juga 10 kerentanan yang populer di aplikasi web (OWASP 10)

1. Download OWASP 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
```



```
root@kali: /home/kali
File Actions Edit View Help
#2) Think before you type.
#3) With great power comes great responsibility.

[sudo] password for kali:
(root@kali)-[/home/kali]
# sudo apt install juice-shop
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
E: Unable to locate package juice-shop

(root@kali)-[/home/kali]
# sudo wget https://github.com/juice-shop/juice-shop/releases/download/v14.0.1/juice-shop-14.0.1_node14_linux_x64.tgz
--2023-02-21 05:02:21-- 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=AKIAIWNJYAX4CSVEH53A%2F20230221%2Fus-east-1%2Fawslogs%3Fawslogs-request&X-Amz-Date=20230221T100223Z&X-Amz-Expires=300&X-Amz-Signature=1a4290e37971dcd0c37aec90b12813605fee4655b2ed84d84c3a5025f5c00976X-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]
--2023-02-21 05:02:21-- https://objects.githubusercontent.com/github-production-release-asset-2e65be/24233689/5797d98f-bef4-4f9b-8568-57cf20caba68?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIWNJYAX4CSVEH53A%2F20230221%2Fus-east-1%2Fawslogs%3Fawslogs-request&X-Amz-Date=20230221T100223Z&X-Amz-Expires=300&X-Amz-Signature=1a4290e37971dcd0c37aec90b12813605fee4655b2ed84d84c3a5025f5c00976X-Amz-SignedHeaders=host&actor_id=0&key_id=0&repo_id=24233689&response-content-disposition=
```

Deskripsi :

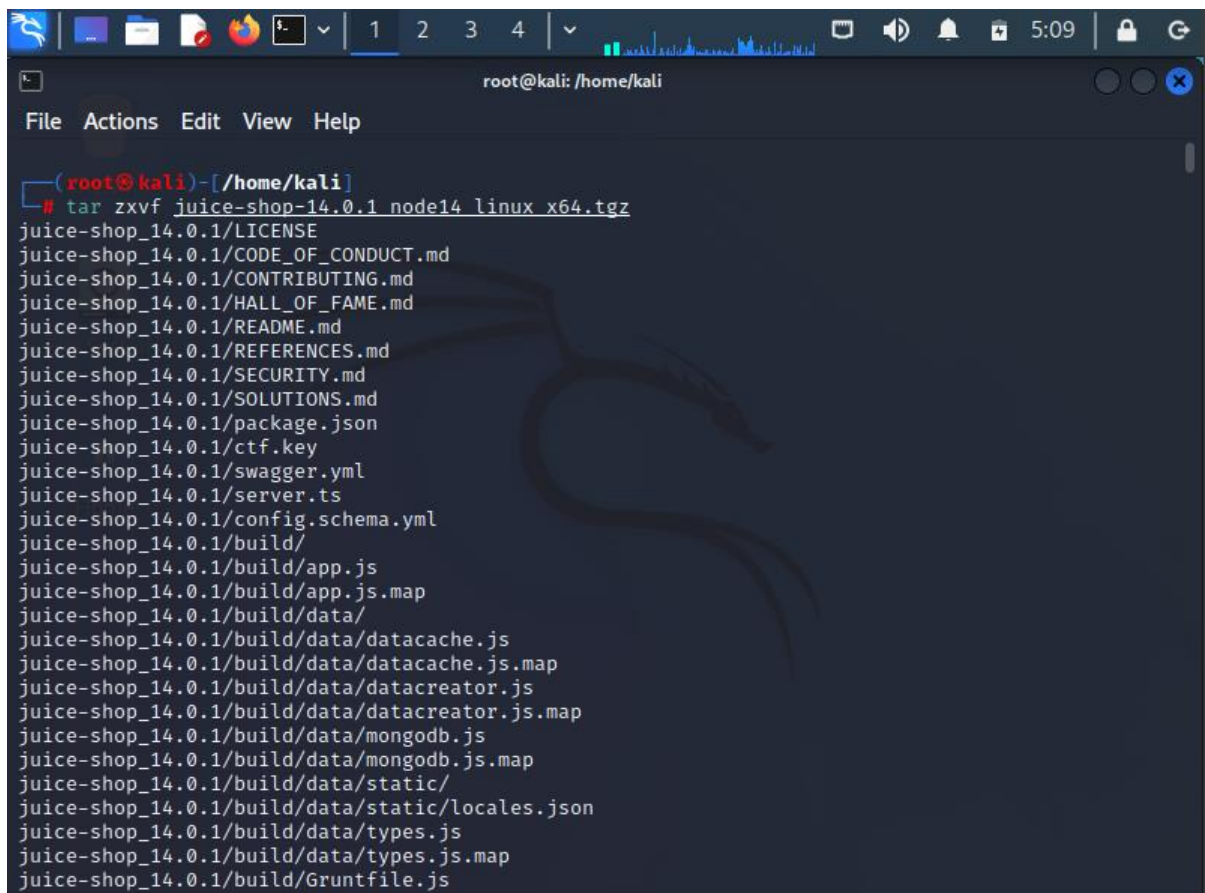
Code "sudo wget https://github.com/juice-shop/juice-shop/releases/download/v14.0.1/juice-shop-14.0.1_node14_linux_x64.tgz" adalah perintah terminal Linux yang bertujuan untuk mengunduh file "juice-shop-14.0.1_node14_linux_x64.tgz" dari repositori GitHub pada alamat yang diarahkan oleh URL "https://github.com/juice-shop/juice-shop/releases/download/v14.0.1/".

Perintah "wget" adalah singkatan dari "web get", yang merupakan perintah untuk mengunduh file dari internet melalui terminal. Sementara itu, kata "sudo" adalah perintah untuk meminta izin administrator dalam mengakses dan menjalankan perintah tersebut.

File yang diunduh dalam perintah tersebut adalah file arsip berformat "tar.gz" yang berisi aplikasi web bernama "Juice Shop". Juice Shop sendiri adalah aplikasi web yang dirancang untuk tujuan pembelajaran keamanan siber, di mana pengguna dapat mempelajari dan mencoba untuk mengeksploitasi kerentanan keamanan yang ada pada aplikasi tersebut.

Dengan mengunduh file tersebut, pengguna dapat memasang dan menjalankan aplikasi Juice Shop pada sistem operasi Linux mereka, sehingga dapat mempelajari tentang keamanan siber dan mencoba teknik-teknik hacking secara aman.

```
Tar zxvf juice-shop-14.0.1_node14_linux_x64.tgz
```

A screenshot of a terminal window on a Kali Linux system. The window title is 'root@kali: /home/kali'. The terminal shows the command 'tar zxvf juice-shop-14.0.1_node14_linux_x64.tgz' being executed. The output lists the contents of the archive, including LICENSE, CODE_OF_CONDUCT.md, CONTRIBUTING.md, HALL_OF_FAME.md, README.md, REFERENCES.md, SECURITY.md, SOLUTIONS.md, package.json, ctf.key, swagger.yml, server.ts, config.schema.yml, and a build directory with various JavaScript files and maps. The background of the terminal has a faint Kali Linux dragon logo.

```
root@kali: /home/kali
File Actions Edit View Help

(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
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
```

Deskripsi :

Code "tar zxvf juice-shop-14.0.1_node14_linux_x64.tgz" adalah perintah terminal Linux untuk mengekstrak atau menge-"unzip" arsip (file kompresi) dengan format "tar.gz" bernama "juice-shop-14.0.1_node14_linux_x64.tgz" menggunakan perintah "tar" pada sistem operasi Linux.

Lebih rinci, perintah "tar" pada dasarnya adalah perintah untuk membuat, menampilkan, mengekstrak, atau memodifikasi arsip file dalam sistem Linux. Dalam perintah di atas, "zxvf" adalah opsi atau argumen perintah tar yang digunakan untuk mengekstrak arsip file yang dikompresi menggunakan gzip.

Lebih rinci, opsi "z" digunakan untuk menunjukkan bahwa arsip yang akan di-ekstrak di-kompres dengan gzip, opsi "x" digunakan untuk menunjukkan bahwa perintah tar harus digunakan untuk mengekstrak atau menge-"unzip" file, opsi "v" digunakan untuk memberikan output informasi yang lebih detail saat perintah dieksekusi, dan opsi "f" digunakan untuk menunjukkan nama file arsip yang akan diekstrak.

Dalam kasus perintah di atas, "juice-shop-14.0.1_node14_linux_x64.tgz" adalah nama file arsip yang akan di-ekstrak, dan perintah tersebut akan mengekstrak arsip tersebut ke direktori tempat perintah tersebut dijalankan.

Secara keseluruhan, perintah "tar zxvf juice-shop-14.0.1_node14_linux_x64.tgz" digunakan untuk mengekstrak arsip file "juice-shop-14.0.1_node14_linux_x64.tgz" ke dalam

direktori tertentu pada sistem operasi Linux, sehingga pengguna dapat menggunakan aplikasi Juice Shop pada sistem operasi Linux mereka.

2. Install NodeJs and NPM

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

```
(root@kali)-[/home/kali]
# sudo wget https://nodejs.org/download/release/v14.1.0/node-v14.1.0-linux-x64.tar.xz
--2023-02-21 05:11:12-- 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-x64. 100%[=====>] 19.87M 128KB/s in 5m 47s

2023-02-21 05:17:06 (58.7 KB/s) - 'node-v14.1.0-linux-x64.tar.xz' saved [20836040/20836040]
```

Deskripsi :

Code "sudo wget https://nodejs.org/download/release/v14.1.0/node-v14.1.0-linux-x64.tar.xz" adalah perintah terminal Linux yang bertujuan untuk mengunduh file arsip berformat "tar.xz" yang berisi instalasi paket dari Node.js pada sistem operasi Linux.

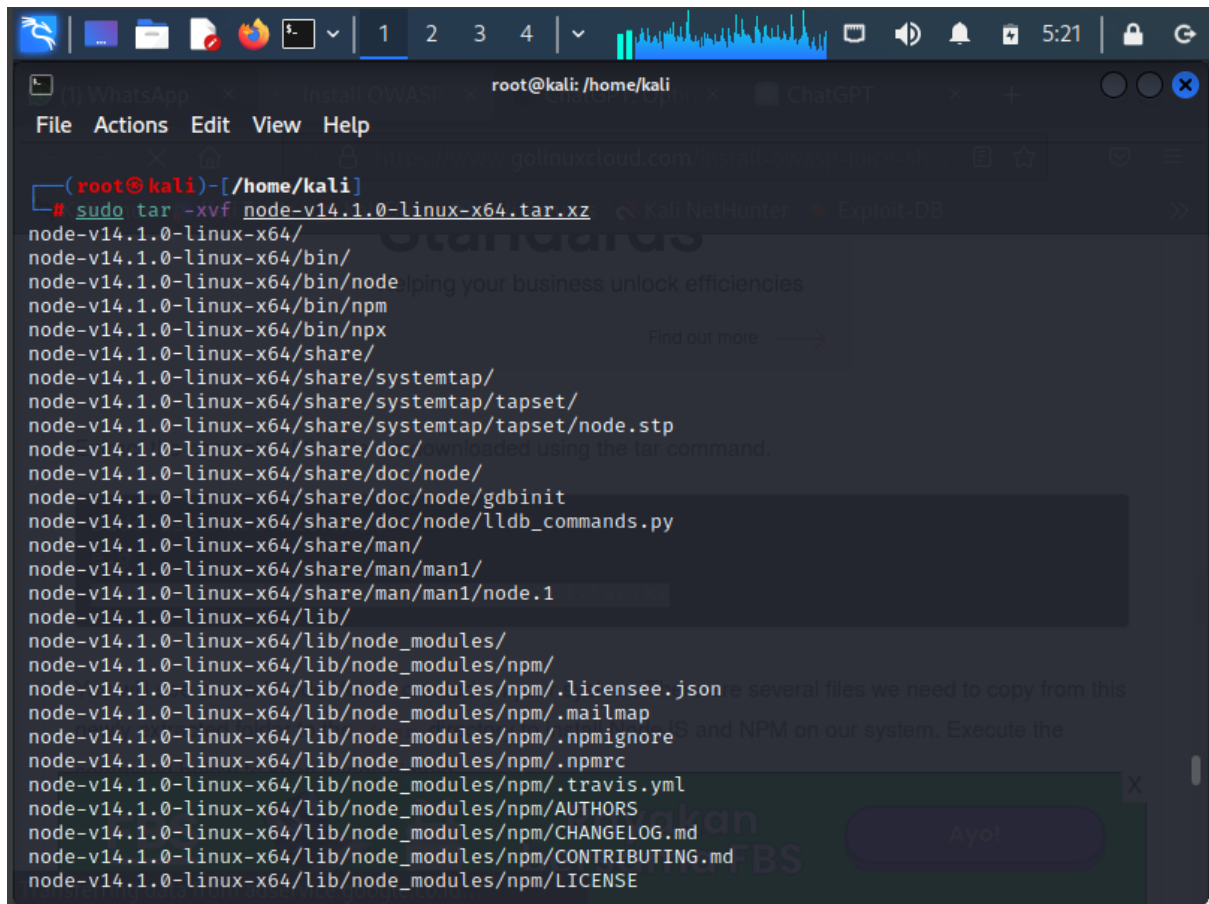
Node.js adalah platform perangkat lunak yang digunakan untuk membangun aplikasi berbasis jaringan. Dalam konteks perintah ini, versi yang akan diunduh adalah versi 14.1.0 yang ditujukan untuk sistem operasi Linux dengan arsitektur 64-bit.

Perintah "wget" pada dasarnya digunakan untuk mengunduh file dari internet, sedangkan opsi "sudo" pada perintah tersebut berfungsi untuk meminta izin administrator dalam mengakses dan menjalankan perintah tersebut.

Dalam perintah di atas, URL "https://nodejs.org/download/release/v14.1.0/" menunjukkan tempat unduh untuk versi Node.js 14.1.0, dan "node-v14.1.0-linux-x64.tar.xz" adalah nama file arsip yang akan diunduh. File tersebut kemudian disimpan pada direktori tempat perintah tersebut dijalankan.

Setelah file berhasil diunduh, langkah selanjutnya adalah mengekstrak arsip tersebut dan menginstal Node.js pada sistem operasi Linux, agar pengguna dapat memulai pengembangan aplikasi dengan menggunakan Node.js.

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


A terminal window on a Kali Linux system. The user is at the root prompt in the directory /home/kali. They have just executed the command 'sudo tar -xvf node-v14.1.0-linux-x64.tar.xz'. The terminal output lists the contents of the archive, including directories like bin, share, lib, and man, and various files like node, npm, npx, systemtap, tapset, node.stp, node/gdbinit, node/lldb_commands.py, node/man, node/man1, node/lib, node_modules, node_modules/npm, node_modules/npm/.licensee.json, node_modules/npm/.mailmap, node_modules/npm/.npmignore, node_modules/npm/.npmrc, node_modules/npm/.travis.yml, node_modules/npm/AUTHORS, node_modules/npm/CHANGELOG.md, node_modules/npm/CONTRIBUTING.md, and node_modules/npm/LICENSE.

```
(root@kali)-[/home/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
```

Dekripsi :

Code "sudo tar -xvf node-v14.1.0-linux-x64.tar.xz" adalah perintah terminal Linux untuk mengekstrak arsip "tar.xz" yang telah diunduh sebelumnya dengan perintah "wget" pada sistem operasi Linux.

Perintah "tar" pada dasarnya adalah perintah untuk membuat, menampilkan, mengekstrak, atau memodifikasi arsip file dalam sistem Linux. Opsi "-xvf" yang digunakan dalam perintah tersebut berguna untuk mengekstrak arsip yang telah diunduh. Opsi "-x" berfungsi untuk mengekstrak file dari arsip, opsi "-v" menampilkan output informasi tentang proses ekstraksi, dan opsi "-f" digunakan untuk menunjukkan file arsip yang akan diekstrak.

Dalam perintah di atas, "node-v14.1.0-linux-x64.tar.xz" adalah nama file arsip yang akan diekstrak. Perintah "sudo" digunakan untuk meminta izin administrator dalam mengakses dan menjalankan perintah tersebut. Setelah dijalankan, perintah tersebut akan mengekstrak arsip tersebut ke dalam direktori tempat perintah tersebut dijalankan.

Setelah berhasil mengekstrak arsip, pengguna dapat mulai menginstal Node.js pada sistem operasi Linux, sehingga mereka dapat menggunakan platform tersebut untuk mengembangkan aplikasi jaringan.

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

A terminal window on a Kali Linux system. The user is at the root prompt in the directory /home/kali. They have just executed the command 'sudo cp -r node-v14.1.0-linux-x64/{bin,include,lib,share} /usr/'. The terminal output shows the command being executed and a prompt character '#' indicating the command has finished.

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

Dekripsi :

Code "sudo cp -r node-v14.1.0-linux-x64/{bin,include,lib,share} /usr/" adalah perintah terminal Linux yang bertujuan untuk menyalin (copy) folder "bin", "include", "lib", dan "share" dari direktori "node-v14.1.0-linux-x64" ke direktori "/usr/" pada sistem operasi Linux.

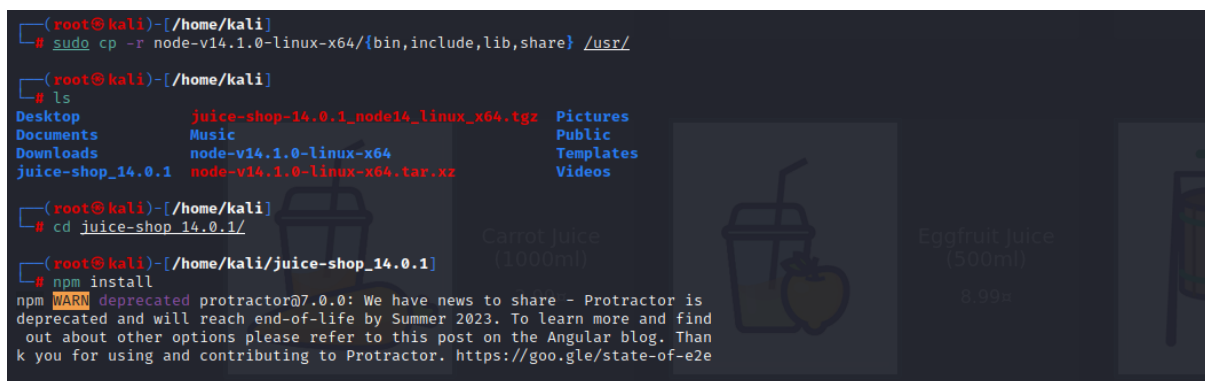
Perintah "cp" pada dasarnya adalah perintah untuk menyalin file atau folder dalam sistem Linux. Opsi "-r" yang digunakan dalam perintah tersebut berguna untuk menyalin folder beserta seluruh isi di dalamnya, termasuk sub-folder dan file-file di dalamnya. Perintah "sudo" digunakan untuk meminta izin administrator dalam mengakses dan menjalankan perintah tersebut.

Dalam perintah di atas, tanda kurung kurawal "{bin,include,lib,share}" digunakan untuk memungkinkan pengguna menentukan beberapa folder yang akan disalin sekaligus dalam satu kali perintah. Setelah itu, direktori "node-v14.1.0-linux-x64" yang berisi folder-folder tersebut, diikuti dengan direktori tujuan "/usr/", yang merupakan direktori sistem pada Linux.

Dengan menjalankan perintah ini, folder-folder "bin", "include", "lib", dan "share" dari direktori Node.js akan disalin ke direktori "/usr/" pada sistem operasi Linux. Hal ini berguna untuk mengaktifkan Node.js pada sistem operasi dan memungkinkan pengguna untuk menggunakan Node.js pada sistem operasi Linux.

3. Install Node Dependencies

```
npm install
```



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

(root@kali)-[/home/kali]
# ls
Desktop      juice-shop-14.0.1_node14_linux_x64.tar.gz  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]
# 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
```

Deskripsi :

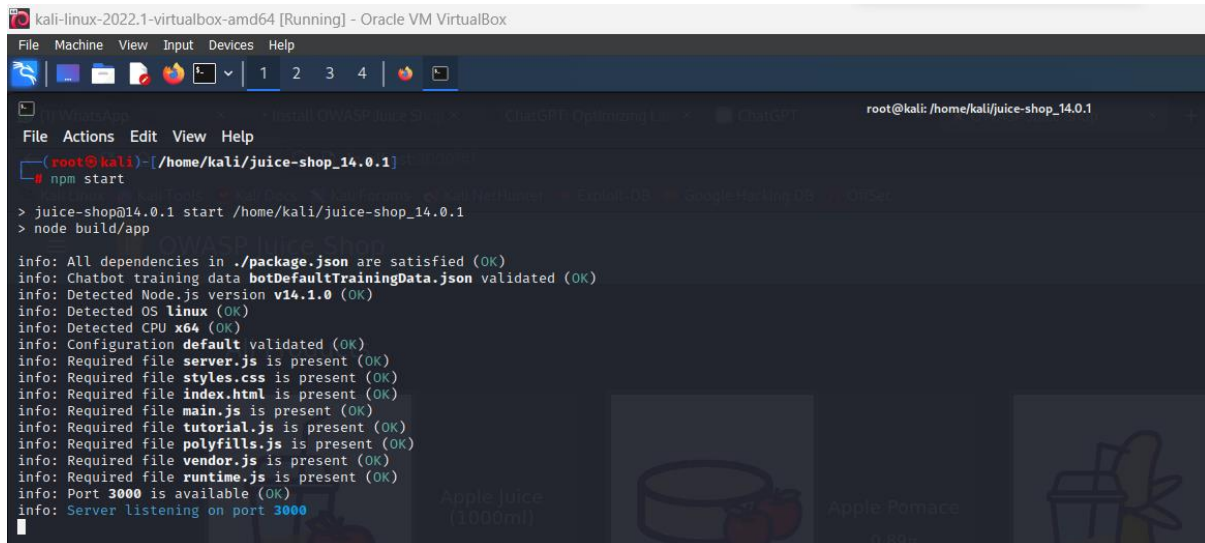
Code "npm install" adalah perintah yang digunakan pada terminal untuk menginstal paket atau modul Node.js yang dibutuhkan oleh sebuah proyek atau aplikasi. NPM (Node Package Manager) adalah manajer paket yang digunakan oleh Node.js untuk mengelola dan menginstal modul/modul JavaScript.

Setelah perintah "npm install" dijalankan pada direktori proyek, NPM akan membaca file package.json pada proyek tersebut dan menginstal semua dependensi yang diperlukan oleh proyek tersebut. File package.json menyimpan daftar dependensi (modul/modul JavaScript) yang diperlukan oleh proyek beserta versi modul yang dibutuhkan.

Perintah "npm install" akan menginstal modul-modul tersebut pada folder "node_modules" pada direktori proyek. Pengguna dapat memasang versi tertentu dari modul atau menginstal modul secara global pada seluruh sistem dengan menambahkan argumen pada perintah "npm install". Selain itu, pengguna juga dapat menghapus modul yang tidak diperlukan lagi dengan perintah "npm uninstall".

Dengan menjalankan perintah "npm install", pengguna dapat dengan mudah menginstal semua dependensi yang dibutuhkan oleh proyek atau aplikasi Node.js, sehingga aplikasi tersebut dapat berjalan dengan baik pada sistem operasi yang ditargetkan.

npm start



```
kali-linux-2022.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali: /home/kali/juice-shop_14.0.1
File Actions Edit View Help
(root@kali)-[/home/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 styles.css is present (OK)
info: Required file index.html is present (OK)
info: Required file main.js is present (OK)
info: Required file tutorial.js is present (OK)
info: Required file polyfills.js is present (OK)
info: Required file vendor.js is present (OK)
info: Required file runtime.js is present (OK)
info: Port 3000 is available (OK)
info: Server listening on port 3000
```

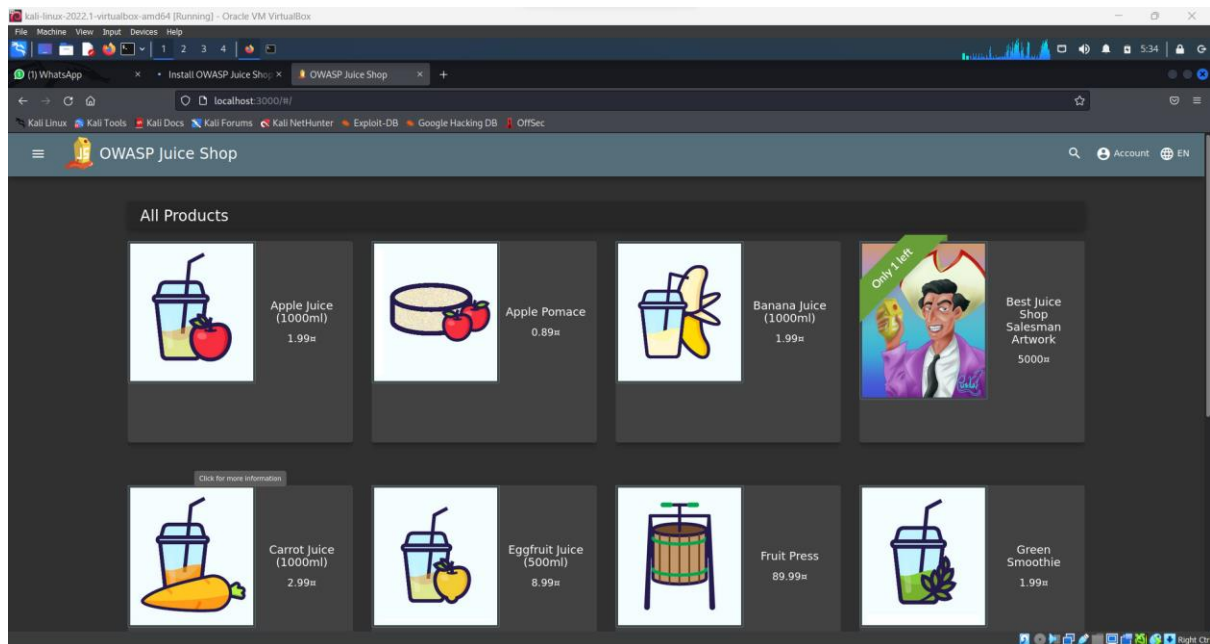
Deskripsi :

Code "npm start" adalah perintah yang digunakan pada terminal untuk menjalankan aplikasi atau proyek Node.js yang memiliki script "start" pada file package.json. Script "start" adalah script yang akan dijalankan oleh Node.js ketika perintah "npm start" dijalankan pada terminal.

Biasanya, script "start" pada file package.json akan menjalankan perintah atau file utama yang menjadi entry point dari aplikasi Node.js. Misalnya, jika file utama dari aplikasi Node.js bernama "index.js", maka script "start" pada package.json akan menjalankan perintah "node index.js" untuk menjalankan aplikasi.

Dalam beberapa kasus, script "start" pada package.json juga dapat diubah untuk menjalankan perintah atau file yang berbeda, tergantung pada kebutuhan proyek atau aplikasi.

Dengan menjalankan perintah "npm start", pengguna dapat menjalankan aplikasi atau proyek Node.js dengan mudah. Perintah "npm start" akan membaca file package.json pada direktori proyek, mengecek script "start" pada file tersebut, dan menjalankan perintah atau file yang diatur pada script "start". Hal ini memudahkan pengguna dalam menjalankan dan menguji aplikasi atau proyek Node.js pada sistem operasi yang ditargetkan.



OWASP Top 10 adalah daftar risiko keamanan yang paling sering terjadi pada aplikasi web yang dirilis oleh Open Web Application Security Project (OWASP). Daftar ini dikeluarkan secara periodik untuk membantu para pengembang aplikasi web dan peneliti keamanan dalam mengidentifikasi dan memperbaiki kerentanan keamanan pada aplikasi web.

Juice Shop adalah aplikasi web yang dirancang untuk digunakan sebagai platform pembelajaran dan pengujian keamanan aplikasi web. Aplikasi ini memiliki fitur-fitur yang mengimplementasikan beberapa risiko keamanan pada daftar OWASP Top 10, sehingga para pengguna Juice Shop dapat belajar tentang keamanan aplikasi web sambil mencoba menyelesaikan tantangan yang disediakan.

Hubungan antara OWASP Top 10 2022 dan Juice Shop adalah bahwa Juice Shop menawarkan berbagai tantangan keamanan yang terkait dengan beberapa risiko keamanan pada daftar OWASP Top 10. Dengan menggunakan Juice Shop, para pengguna dapat belajar tentang risiko keamanan yang sering terjadi pada aplikasi web dan belajar cara mengidentifikasi dan memperbaiki kerentanan tersebut.

Dalam hal ini, Juice Shop dapat digunakan sebagai alat pembelajaran yang efektif dalam mempelajari risiko keamanan pada aplikasi web yang terkait dengan daftar OWASP Top 10 2022. Para pengguna Juice Shop dapat memperdalam pengetahuan mereka tentang risiko keamanan yang sering terjadi pada aplikasi web, sehingga mereka dapat lebih siap dalam menghadapi tantangan keamanan pada aplikasi web di dunia nyata.

Contohnya, salah satu tantangan pada Juice Shop adalah "Broken Authentication and Session Management" yang merupakan risiko keamanan nomor 2 pada daftar OWASP Top 10. Tantangan ini menantang para pengguna untuk menemukan kerentanan pada autentikasi dan manajemen sesi pada aplikasi web.

Dengan menggunakan Juice Shop, para pengguna dapat menguji dan meningkatkan kemampuan mereka dalam mengidentifikasi dan memperbaiki kerentanan keamanan pada aplikasi web yang terkait dengan OWASP Top 10. Oleh karena itu, Juice Shop dapat digunakan sebagai alat pembelajaran yang efektif dalam mempelajari dan memahami risiko keamanan pada aplikasi web yang sering terjadi.

OWASP Top 10 adalah daftar kerentanan keamanan pada aplikasi web yang paling umum dan sering terjadi. Berikut ini adalah 10 kerentanan yang terdapat pada daftar OWASP Top 10:

- a. **Injection:** Kerentanan injeksi terjadi ketika input yang dimasukkan oleh pengguna tidak divalidasi dengan benar, sehingga memungkinkan serangan injeksi seperti SQL injection dan Command injection.
- b. **Broken Authentication and Session Management:** Kerentanan ini terjadi ketika sistem otentikasi dan manajemen sesi tidak diatur dengan benar, sehingga memungkinkan serangan seperti brute force, session hijacking, dan session fixation.
- c. **Cross-Site Scripting (XSS):** Kerentanan XSS terjadi ketika aplikasi web tidak memvalidasi data masukan pengguna dengan benar, sehingga memungkinkan serangan pengacauan situs web atau pencurian data pengguna.
- d. **Broken Access Control:** Kerentanan ini terjadi ketika aplikasi web tidak memvalidasi dan mengontrol akses yang tepat pada sumber daya dan fitur tertentu, sehingga memungkinkan pengguna untuk mengakses data atau fitur yang tidak seharusnya mereka akses.
- e. **Security Misconfiguration:** Kerentanan ini terjadi ketika sistem atau aplikasi web tidak dikonfigurasi dengan benar, sehingga memungkinkan serangan seperti akses yang tidak sah, peretasan, atau pencurian data.
- f. **Insecure Cryptographic Storage:** Kerentanan ini terjadi ketika data sensitif disimpan dengan cara yang tidak aman, sehingga memungkinkan serangan seperti pencurian data atau identitas.
- g. **Insufficient Transport Layer Protection:** Kerentanan ini terjadi ketika aplikasi web tidak menggunakan enkripsi atau perlindungan lapisan transport yang memadai, sehingga memungkinkan serangan seperti sniffing, man-in-the-middle, atau pengiriman ulang.
- h. **Insecure Direct Object References:** Kerentanan ini terjadi ketika aplikasi web tidak memvalidasi akses ke objek langsung, sehingga memungkinkan pengguna untuk mengakses data yang seharusnya tidak mereka akses.
- i. **Cross-Site Request Forgery (CSRF):** Kerentanan ini terjadi ketika aplikasi web tidak memvalidasi permintaan yang diterima dari sumber yang tidak sah, sehingga memungkinkan pengguna untuk melakukan tindakan yang tidak seharusnya mereka lakukan.
- j. **Using Components with Known Vulnerabilities:** Kerentanan ini terjadi ketika aplikasi web menggunakan komponen yang sudah diketahui rentan, sehingga memungkinkan serangan seperti peretasan atau pencurian data.

Demikianlah 10 kerentanan yang sering terjadi pada aplikasi web yang ada di daftar OWASP Top 10. Penting bagi pengembang dan pengguna aplikasi web untuk memahami dan mengantisipasi kerentanan-kerentanan tersebut guna mencegah serangan-serangan keamanan yang berbahaya.