

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
```

```
(kali@kali)-[~]
$ sudo apt update

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

#1) Respect the privacy of others.
#2) Think before you type.
#3) With great power comes great responsibility.

[sudo] password for kali:
Get:1 http://mirror.primelink.net.id/kali kali-rolling InRelease [41.2 kB]
Get:2 http://mirror.primelink.net.id/kali kali-rolling/main amd64 Packages [1
9.5 MB]
Get:3 http://mirror.primelink.net.id/kali kali-rolling/main amd64 Contents (deb) [45.4 MB]
Get:4 http://mirror.primelink.net.id/kali kali-rolling/contrib amd64 Packages [116 kB]
Get:5 http://mirror.primelink.net.id/kali kali-rolling/contrib amd64 Contents (deb) [172 kB]
Get:6 http://mirror.primelink.net.id/kali kali-rolling/non-free amd64 Packages [222 kB]
Get:7 http://mirror.primelink.net.id/kali kali-rolling/non-free amd64 Contents (deb) [931 kB]
Fetched 66.4 MB in 37s (1,794 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
1826 packages can be upgraded. Run 'apt list --upgradable' to see them.
```

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
```

```
(kali@kali)-[~/Desktop]
$ sudo wget https://nodejs.org/download/release/v14.1.0/node-v14.1.0-linux-x64.tar.xz
--2023-02-25 09:06:53-- 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.tar.xz 100%[=====]
2023-02-25 09:07:03 (2.15 MB/s) - 'node-v14.1.0-linux-x64.tar.xz' saved [20836040/20836040]
```

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
```

```
(kali㉿kali)-[~/Desktop]
└─$ 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
```

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
```

```
(kali㉿kali)-[~/Desktop]
└─$ sudo cp -r node-v14.1.0-linux-x64/{bin,include,lib,share} /usr/

(kali㉿kali)-[~/Desktop]
└─$ node --version
v14.1.0

(kali㉿kali)-[~/Desktop]
└─$ npm --version
6.14.4
```

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
```

```
(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
--2023-02-25 12:15:27-- 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%2F20230225%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20230225T171528Z&X-Amz-Expires=300&X-Amz-Signature=08e3b31c22473bc5d276bd1c1b49ca316dc9b5710f57473a13244765d12289fd6X-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]
--2023-02-25 12:15:28-- 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%2F20230225%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20230225T171528Z&X-Amz-Expires=300&X-Amz-Signature=08e3b31c22473bc5d276bd1c1b49ca316dc9b5710f57473a13244765d12289fd6X-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)... 185.199.111.133
Connecting to objects.githubusercontent.com (objects.githubusercontent.com)|185.199.111.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 119567474 (114M) [application/octet-stream]
Saving to: 'juice-shop-14.0.1_node14_linux_x64.tgz'

juice-shop-14.0.1_node14_linux_x64.tgz      100%[=====]
2023-02-25 12:16:27 (1.95 MB/s) - 'juice-shop-14.0.1_node14_linux_x64.tgz' saved [119567474/119567474]
```

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/
```

```
(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
```

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

Mengecek Folder Hasil Ekstraksi

```
(root@kali)-[~]  
# ls  
juice-shop_14.0.1 juice-shop-14.0.1_node14_linux_x64.tgz
```

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

Langkah 3. Install Node Dependencies

Menginstall Paket Node pada Folder Aplikasi Web Juice Shop

```
npm install
```

```
(root@kali)-[~]  
# cd juice-shop 14.0.1  
  
(root@kali)-[~/juice-shop_14.0.1]  
# npm install  
npm WARN deprecated protractor@7.0.0: We have news to share - Protractor is  
r using and contributing to Protractor. https://goo.gle/state-of-e2e-in-ang  
npm WARN deprecated @types/express-unless@2.0.1: This is a stub types defin  
npm WARN deprecated @types/socket.io-parser@3.0.0: This is a stub types defi  
npm WARN deprecated joi@13.7.0: This version has been deprecated in accorda  
able to upgrade at this time, paid support is available for older versions  
npm WARN deprecated ecstatic@3.3.2: This package is unmaintained and deprec  
npm WARN deprecated hoek@5.0.4: This version has been deprecated in accorda  
able to upgrade at this time, paid support is available for older versions  
npm WARN deprecated topo@3.0.3: This module has moved and is now available  
npm WARN deprecated hoek@6.1.3: This module has moved and is now available  
npm WARN deprecated sane@4.1.0: some dependency vulnerabilities fixed, supp  
npm WARN deprecated w3c-hr-time@1.0.2: Use your platform's native performanc  
npm WARN lifecycle juice-shop@14.0.1~postinstall: cannot run in wd juice-sho  
)  
npm notice created a lockfile as package-lock.json. You should commit this  
npm WARN optional SKIPPING OPTIONAL DEPENDENCY: fsevents@~2.3.2 (node_module  
npm WARN notsup SKIPPING OPTIONAL DEPENDENCY: Unsupported platform for fseve  
added 1090 packages from 1036 contributors and audited 2146 packages in 47.3  
158 packages are looking for funding  
run `npm fund` for details  
found 79 vulnerabilities (14 low, 24 moderate, 28 high, 13 critical) in OWASP  
run `npm audit fix` to fix them, or `npm audit` for details
```

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
```

```
(root@kali) ~/juice-shop_14.0.1
# npm audit fix
npm WARN deprecated @npmcli/move-file@1.1.2: This functionality has been moved to @npmcli/fs

> sqlite3@5.1.4 install /root/juice-shop_14.0.1/node_modules/sqlite3
> node-pre-gyp install --fallback-to-build

[sqlite3] Success: "/root/juice-shop_14.0.1/node_modules/sqlite3/lib/binding/napi-v6-linux-glibc-x64/node_sqlit
npm WARN notsup Unsupported engine for npmlog@6.0.2: wanted: {"node": "^12.13.0 || ^14.15.0 || ≥16.0.0"} (current: "node": "v14.15.0")
npm WARN notsup Not compatible with your version of node/npm: npmlog@6.0.2
npm WARN notsup Unsupported engine for gauge@4.0.4: wanted: {"node": "^12.13.0 || ^14.15.0 || ≥16.0.0"} (current: "node": "v14.15.0")
npm WARN notsup Not compatible with your version of node/npm: gauge@4.0.4
npm WARN notsup Unsupported engine for are-we-there-yet@3.0.1: wanted: {"node": "^12.13.0 || ^14.15.0 || ≥16.0.0"} (current: "node": "v14.15.0")
npm WARN notsup Not compatible with your version of node/npm: are-we-there-yet@3.0.1
npm WARN notsup Unsupported engine for npmlog@6.0.2: wanted: {"node": "^12.13.0 || ^14.15.0 || ≥16.0.0"} (current: "node": "v14.15.0")
npm WARN notsup Not compatible with your version of node/npm: npmlog@6.0.2
npm WARN notsup Unsupported engine for are-we-there-yet@3.0.1: wanted: {"node": "^12.13.0 || ^14.15.0 || ≥16.0.0"} (current: "node": "v14.15.0")
npm WARN notsup Not compatible with your version of node/npm: are-we-there-yet@3.0.1
npm WARN notsup Unsupported engine for gauge@4.0.4: wanted: {"node": "^12.13.0 || ^14.15.0 || ≥16.0.0"} (current: "node": "v14.15.0")
npm WARN notsup Not compatible with your version of node/npm: gauge@4.0.4
npm WARN optional SKIPPING OPTIONAL DEPENDENCY: fsevents@2.3.2 (node_modules/fsevents):
npm WARN notsup SKIPPING OPTIONAL DEPENDENCY: Unsupported platform for fsevents@2.3.2: wanted {"os": "darwin", "arch": "x64"}

+ sqlite3@5.1.4
+ sequelize@6.29.0
+ replace@1.2.2
+ juicy-chat-bot@0.6.6
+ file-type@16.5.4
added 64 packages from 46 contributors, removed 16 packages and updated 83 packages in 58.733s

156 packages are looking for funding
  run `npm fund` for details

fixed 27 of 79 vulnerabilities in 2146 scanned packages
  11 vulnerabilities required manual review and could not be updated
  7 package updates for 41 vulnerabilities involved breaking changes
  (use `npm audit fix --force` to install breaking changes; or refer to `npm audit`)
```

Keterangan: “npm audit fix” digunakan untuk memperbaiki kerentanan atau masalah pada proses penginstalan 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
```

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

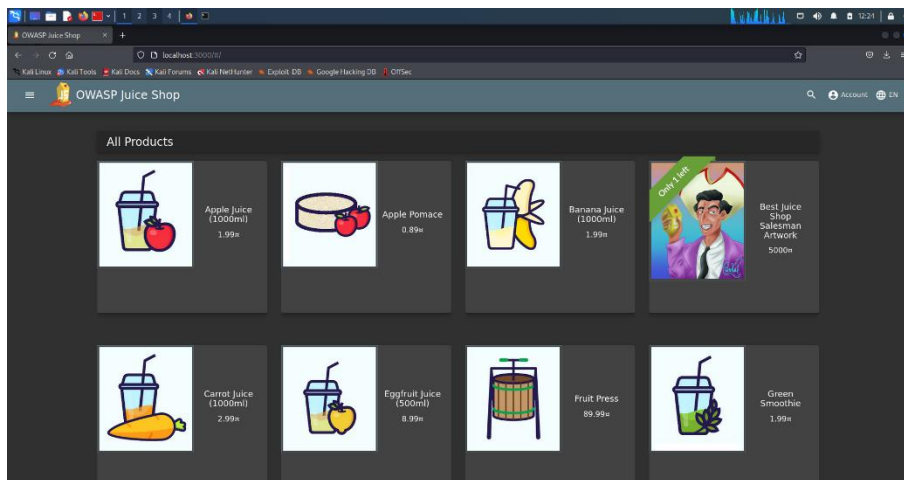
> juice-shop@14.0.1 start /root/juice-shop_14.0.1
> node build/app

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 styles.css is present (OK)
info: Required file polyfills.js is present (OK)
info: Required file tutorial.js is present (OK)
info: Required file runtime.js is present (OK)
info: Required file main.js is present (OK)
info: Required file index.html is present (OK)
info: Required file vendor.js is present (OK)
info: Port 3000 is available (OK)
info: Server listening on port 3000
```

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 perencanaan.

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.