

KEAMANAN JARINGAN

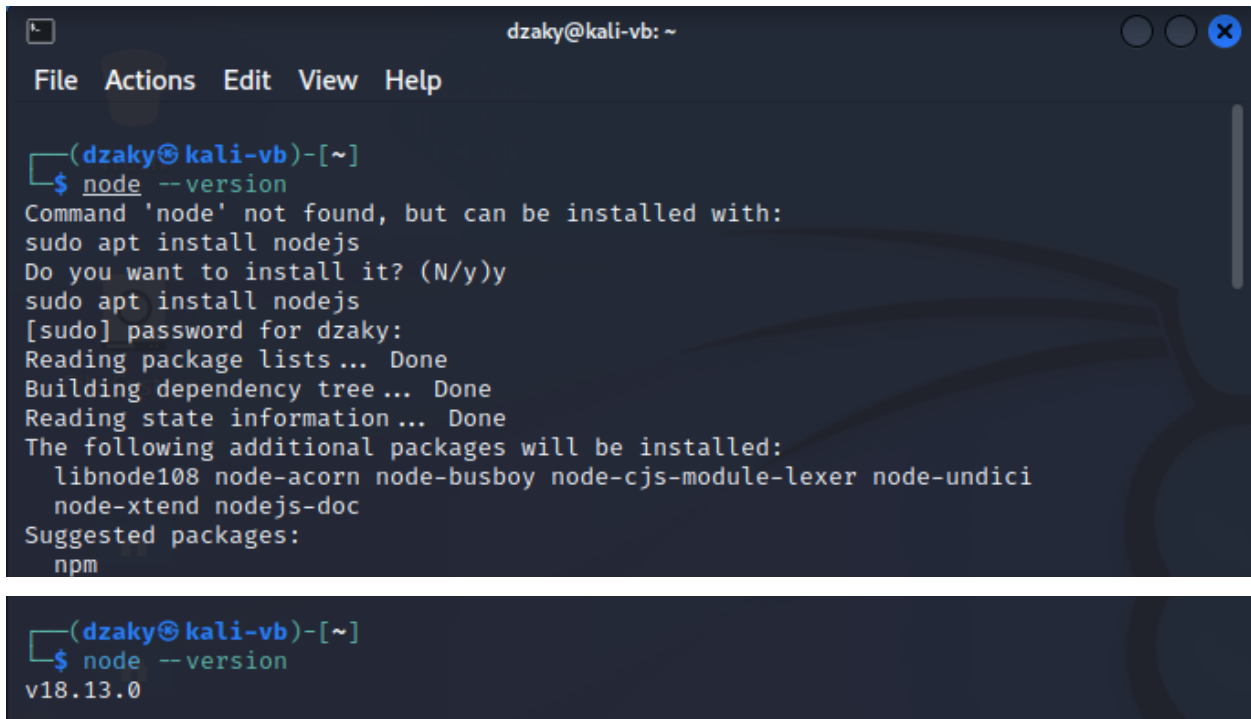


Disusun Oleh :
Muhammad Dzaky Mahfuzh
3122640050
D4 LJ B
Teknik Informatika

Politeknik Elektronika Negeri Surabaya
Kampus ITS Keputih Sukolilo Surabaya 60111
Telp. 031-5947280, 031-5946114, Fax:031-5946114

Task 1 Part 1: 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.

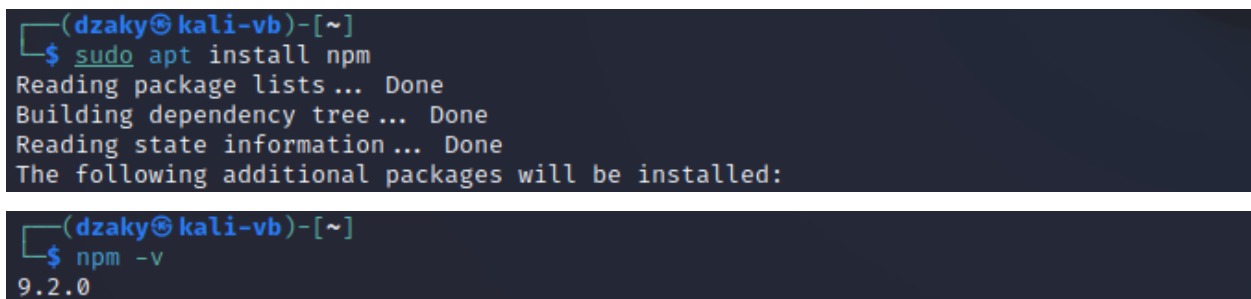
1. Buka terminal dan cek apakah sudah terinstall nodejs, dapat menggunakan command **node -version** atau **nodejs -v**. Apabila belum lakukan instalasi menggunakan command **sudo apt install nodejs** lalu tunggu sampai proses instalasi selesai.



```
(dzaky@kali-vb)-[~]
$ node --version
Command 'node' not found, but can be installed with:
sudo apt install nodejs
Do you want to install it? (N/y)y
sudo apt install nodejs
[sudo] password for dzaky:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libnode108 node-acorn node-busboy node-cjs-module-lexer node-undici
  node-xtend nodejs-doc
Suggested packages:
  npm

(dzaky@kali-vb)-[~]
$ node --version
v18.13.0
```

2. Setelah menginstall nodejs langkah selanjutnya adalah menginstall npm dengan menggunakan command **sudo apt install npm** dan tunggu sampai proses instalasi selesai.



```
(dzaky@kali-vb)-[~]
$ sudo apt install npm
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:

(dzaky@kali-vb)-[~]
$ npm -v
9.2.0
```

3. Lalu mengkloning aplikasi dari repository github dengan menggunakan command **git clone <https://github.com/juice-shop/juiceshop.git>** dan tunggu sampai proses kloning selesai.

```
(dzaky@kali-vb)-[~]
$ git clone https://github.com/juice-shop/juice-shop.git
Cloning into 'juice-shop' ...
remote: Enumerating objects: 118011, done.
remote: Counting objects: 100% (29/29), done.
remote: Compressing objects: 100% (20/20), done.
Receiving objects: 24% (28551/118011), 61.52 MiB | 890.00 KiB/s
```

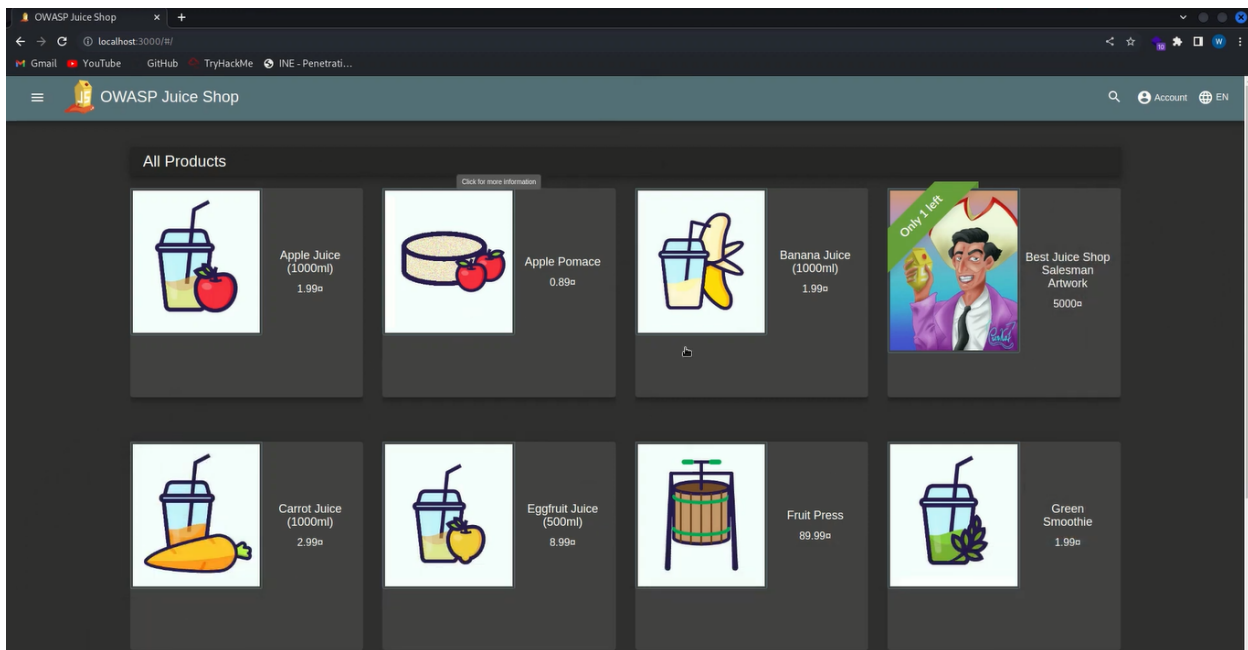
- Setelah proses selesai, silahkan cek menggunakan command **ls** untuk mengecek directory dan pastikan telah ada directory aplikasi juice-shop. Masuk ke directory juice-shop menggunakan command **cd juice-shop** lalu jalankan command **npm install** untuk menginstall juice-shop.

```
(dzaky@kali-vb)-[~]
$ ls
Desktop  Downloads  Music  Public  Videos
Documents  juice-shop  Pictures  Templates

(dzaky@kali-vb)-[~]
$ cd juice-shop

(dzaky@kali-vb)-[~/juice-shop]
$ npm install
```

- Setelah proses instalasi selesai jalankan command **npm start** lalu buka browser dan masukan localhost:3000 untuk mengakses web juice-shop.



Task 1 Part 2: Jelaskan hubungan anantara OWASP 10 2022 dengan aplikasi Juiceshop !

OWASP Juice Shop adalah Web Application Vulnerable yang digunakan untuk pembelajaran tentang Web Security. Dibangun dengan menggunakan bahasa JavaScript yang mencakup seluruh OWASP Top 10 atau kerentanan yang telah dirilis oleh OWASP.

Task 1 Part 3: Jelaskan 10 kerentanan yang populer di aplikasi web (OWASP 10)

1. A01:2021 Broken Access Control (Kelemahan Access Control)

34 Common Weakness Enumerations (CWEs) memetakan Broken Access Control lebih banyak terjadi pada aplikasi dibandingkan kategori lainnya. Penyerang dan peretas dapat mengakses sebuah sistem ketika autentikasi dan pembatasan akses tidak diterapkan dengan baik. Dengan kata lain, Broken Access Control memungkinkan entri yang tidak sah yang dapat mengakibatkan kerentanan data dan file yang bersifat sensitif. Kontrol akses yang lemah terkait manajemen kredensial dapat dihindari dengan metode coding yang unik dan tindakan khusus seperti mematikan akun administratif dan penggunaan autentikasi multi-faktor.

2. A02:2021 Cryptographic Failures (Kegagalan Kriptografi)

Fokus disini adalah pada API (Application Programming Interface) yang menghasilkan koneksi dan layanan pihak ketiga. Dalam hal ini, kegagalan kriptografi seperti layanan pihak ketiga termasuk Google Maps dapat memanfaatkan data transmisi yang tidak aman sehingga mendorong peretas untuk melakukan serangan. Kegagalan kriptografi menekankan pada kebocoran data sensitif dan sistem yang telah terinfeksi oleh peretas. Aktivitas seperti enkripsi data, manajemen sistem yang memadai, tokenisasi, dan menonaktifkan respon dapat mengurangi risiko kebocoran data pribadi.

3. A03:2021 Injection (Injeksi)

Injeksi mungkin terjadi apabila peretas memanipulasi kode yang tidak aman kemudian diinjeksikan kode buatan peretas tersebut kedalam program tertentu. Seringkali, karena program yang terinjeksi tidak dapat mengidentifikasi data terinjeksi tersebut, penyerang yang telah menginjeksi sistem dapat mengidentifikasi area yang aman serta informasi yang bersifat rahasia, karena sistem akan mengidentifikasi mereka sebagai pengguna yang terpercaya. Injeksi diantaranya adalah command injection (injeksi perintah), LDAP, CRLF, dan injeksi SQL. Pengujian OWASP dapat mengetahui kegagalan pada injeksi dan memberikan teknik perbaikan yang berlawanan.

4. A04:2021 Insecure Design (Kekurangan pada Desain)

Untuk desain yang tidak aman, OWASP menghadirkan daftar risiko terkait kekurangan desain. Insecure design merupakan pendekatan baru dalam survei 2021. Uji penetrasi telah terbukti dapat

digunakan untuk mengatasi kelemahan ini. Perusahaan harus meningkatkan penggunaan pemodelan ancaman, pola dan desain yang aman serta menyediakan referensi arsitektur.

5. A05:2021 Security Misconfiguration (Kelemahan Konfigurasi Keamanan)

Security Misconfiguration sangat diperlukan dalam OWASP Top 10 karena mampu menunjukkan perubahan pada perangkat lunak yang dapat dikonfigurasi. Kategori lainnya seperti XML External Entities (XXE) termasuk kedalam kategori ini. Hampir sama dengan kesalahan konfigurasi pada access controls, bagian ini juga mengatasi kesalahan pada konfigurasi yang dapat menimbulkan risiko signifikan dengan memberikan akses kepada penyerang untuk masuk kedalam sistem. Untuk menyelesaikan permasalahan tersebut, pengujian dinamis dapat membantu audit untuk menemukan kesalahan konfigurasi keamanan pada aplikasi Anda.

6. A06:2021 Vulnerable and Outdated Components (Komponen yang rentan dan kadaluarsa)

Peretas dapat menyerang dan memanipulasi keamanan kode serta API Anda. Serangan ini dapat dilakukan karena komponen pihak ketiga dan ketergantungan yang tidak aman. Ketika serangan seperti itu terjadi, analisis komposisi perangkat lunak dapat mengatasi permasalahan tersebut dari dalam sistem. Analisis memungkinkan pemrogram atau audit untuk mengidentifikasi komponen yang tidak aman sebelum sistem mempublikasikan aplikasinya.

7. A07:2021 Identification and Authentication Failures (Kegagalan Identifikasi dan Autentikasi)

Pada survei sebelumnya, faktor ini termasuk kedalam kesalahan autentikasi dan penerapan autentikasi serta manajemen sesi yang diimplementasikan secara tidak benar. Risiko yang signifikan dapat memungkinkan penyerang untuk menyalin peran dari identitas pengguna yang sah. Autentikasi multi-faktor merupakan pendekatan vital untuk mengurangi kelemahan pada autentikasi atau identifikasi dan kegagalan autentikasi. Penggunaan alat pemindai DAST dan SCA dapat mendeteksi dan mengatasi permasalahan yang mencakup kesalahan implementasi sebelum pemrogram mengaplikasikan kodenya.

8. A08:2021 Software and Data Integrity Failures (Kegagalan Perangkat Lunak dan Keutuhan Data)

Software and Data Integrity Failures merupakan kategori baru pada survei tahun 2021 yang menekankan pada keputusan terkait pembaruan perangkat lunak, CI/CD pipeline, dan data penting. Kategori ini merupakan salah satu dampak dari Common Vulnerability and Exposures/Common Vulnerability Scoring Sistem (CVE/CVSS). Perlu diketahui bahwa deserialisasi yang tidak aman sejak survei tahun 2017 termasuk kedalam kategori ini.

Deserialisasi mengacu pada pengambilan data atau objek sebelumnya yang tertulis atau tersimpan pada disk dan dapat digunakan untuk menjalankan kode pada sistem Anda atau terbuka untuk serangan lebih lanjut. Objek ini dapat terstruktur atau biner melalui desain konvensional seperti JSON dan XML. Seringkali, kegagalan terjadi ketika penyerang memanfaatkan data yang tidak terpercaya (untrusted data) untuk mengeksploitasi aplikasi tertentu, memulai penolakan layanan untuk menjalankan kode yang tidak terduga (unpredicted code) untuk mengubah perilaku sistem. Meskipun deserialisasi merupakan tugas yang cukup luas untuk diselesaikan, uji penetrasi dan penggunaan tools keamanan dapat mengatasi serangan tersebut. Pada kebanyakan kasus, pengguna harus menolak sumber yang tidak dapat dipercaya dan objek serial untuk melindungi sistem dari risiko serangan siber.

9. A09:2021 Security Logging and Monitoring Failures (Kegagalan pada keamanan logging dan monitoring data)

Kegagalan pada login dan praktek pemantauan yang tidak memadai dapat memicu risiko kesalahan manusia. Secara global, pelaku pengancaman bergantung pada kurangnya pemantauan dan pemulihan yang lambat untuk melakukan proses mereka, tanpa disadari dan tanpa reaksi. Konteks login dengan kegagalan pada login, kontrol akses dan validasi data dari server dapat mengidentifikasi aktivitas yang mencurigakan didalam sistem. Uji penetrasi juga dapat mengidentifikasi area dengan login yang tidak memadai.

10. A10:2021 Server-Side Request Forgery (SSRF)

Merupakan entri baru yang masuk kedalam list dan berfokus pada pengujian. Server-Side Request Forgery berkaitan dengan cakupan pengujian diatas rata-rata terhadap potensi eksploitasi dan dampak. Pada level ini, skenario dimana tim keamanan menuntut relevansi data juga penting.

Secara umum, pembaruan rutin digunakan untuk mengatasi kebutuhan yang beragam terkait keamanan aplikasi yang dihadapi oleh perusahaan. Pembaruan secara rutin merupakan usaha untuk membangun sebuah kerangka kerja yang berkelanjutan yang dapat membantu perusahaan membangun infrastruktur penting untuk menghindari risiko keamanan yang dihadapi perusahaan. Tujuannya meliputi teknisi keamanan, pemrogram, penegak hukum, auditor dan bahkan manajer program. Tool uji penetrasi aplikasi mudah digunakan dan mengintegrasikan pendekatan yang luas mencakup uji pengembangan (developing test) dan pengujian fungsi (functional test).