OWASP JUICE SHOP & OWASP TOP 10

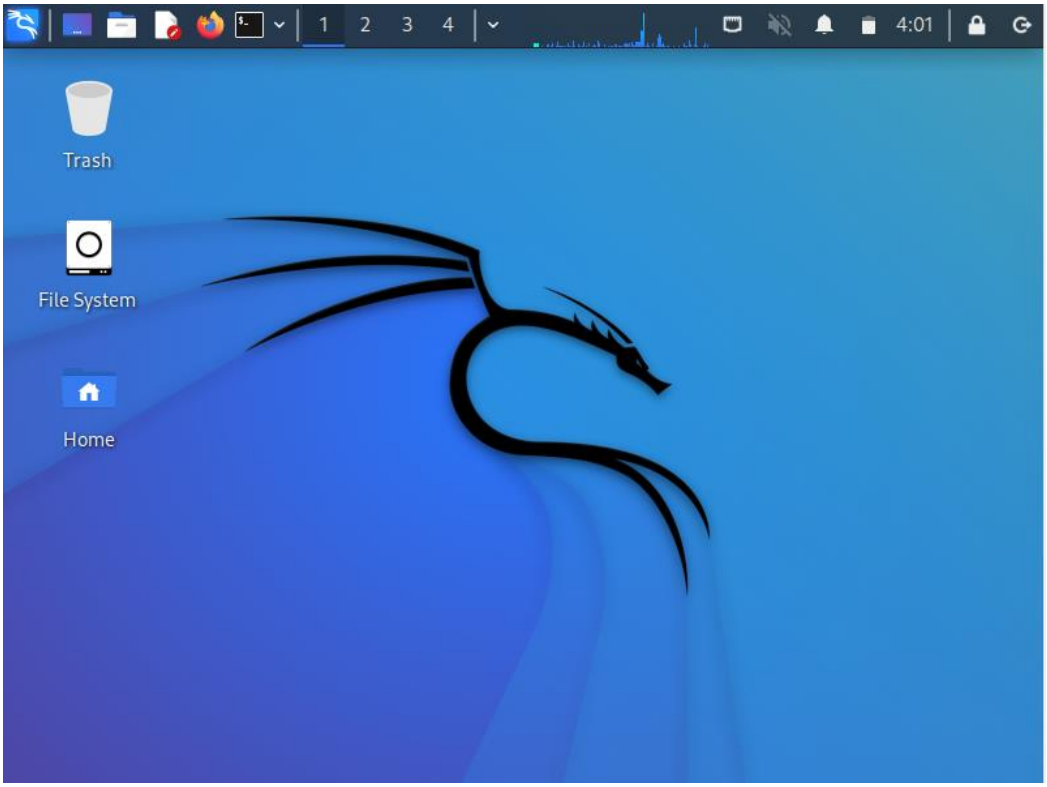
Tugas Keamanan Jaringan Minggu 1

FEBRUARY 26, 2023

FAJAR YUNUS AFIFFUDIN
NRP 3122640049

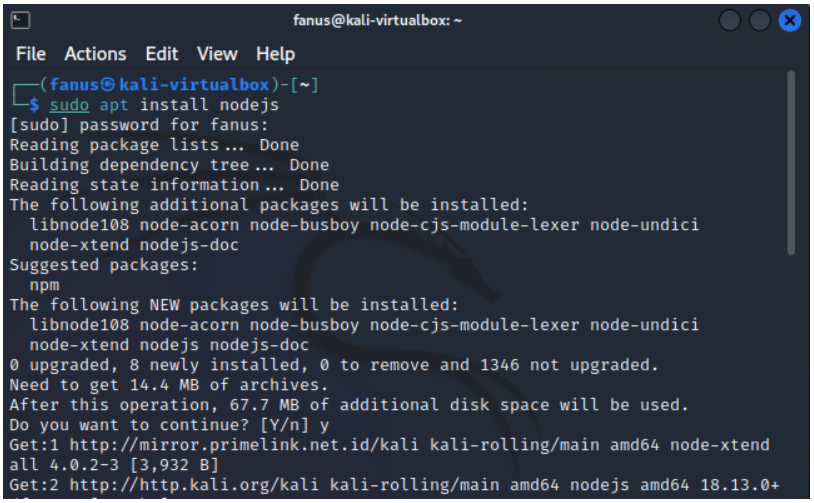
TUGAS 1 : Step Instalasi OWASP Juice Shop

1. Siapkan Server / VM
   - Siapkan server / vm untuk menhosting website Juice Shop
     Untuk praktikum ini, saya melakukan instalasi OWASP Juice Shop di VM khusus untuk hosting menggunakan distro Kali Linux.

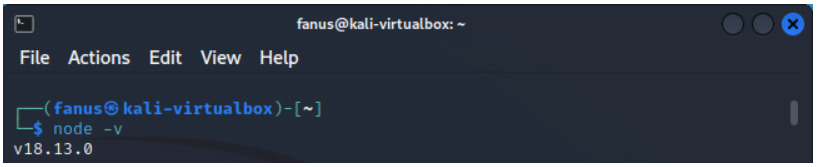


   -

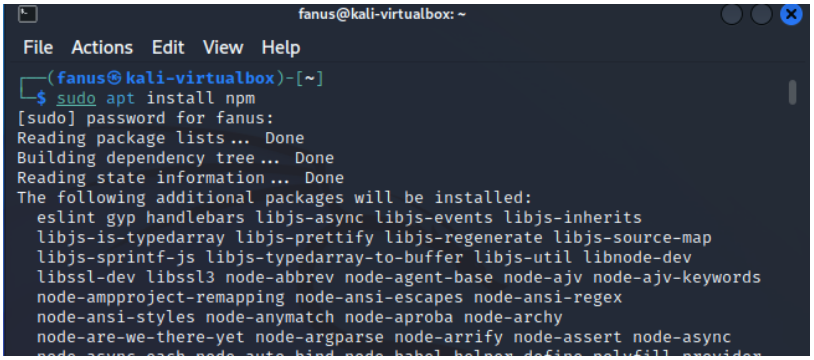
2. Untuk menjalankan OWASP juice shope memerlukan Node Js dan NPM. Install Node js pada server.
   - Install Node js dengan “sudo apt install nodejs”.



     Tunggu proses instalasi hingga selesai.
   - Untuk mengecek apakah node js sudah terinstall, bisa menggunakan perintah “node -v”

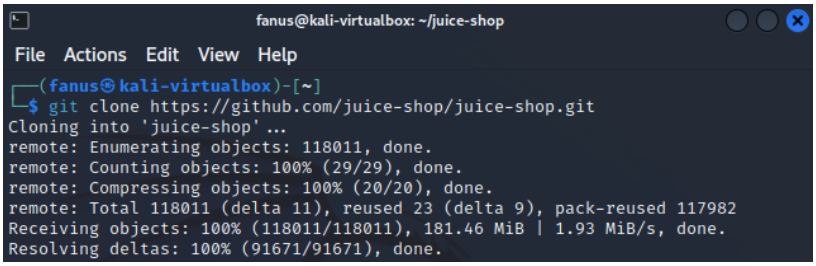


3. Setelah menginstall node js, install npm
   - Install NPM dengan “sudo apt npm”.

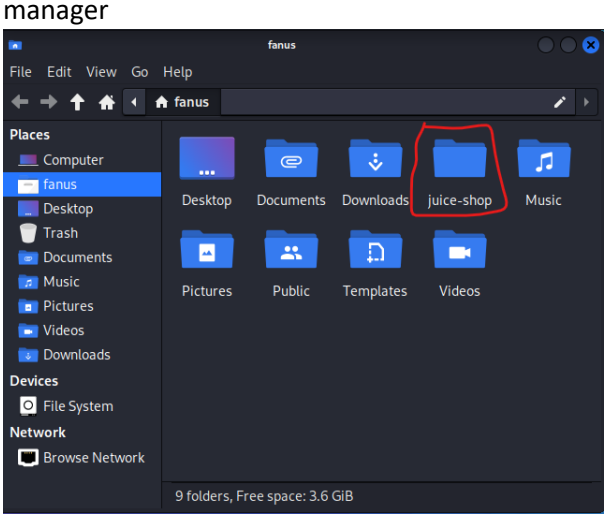


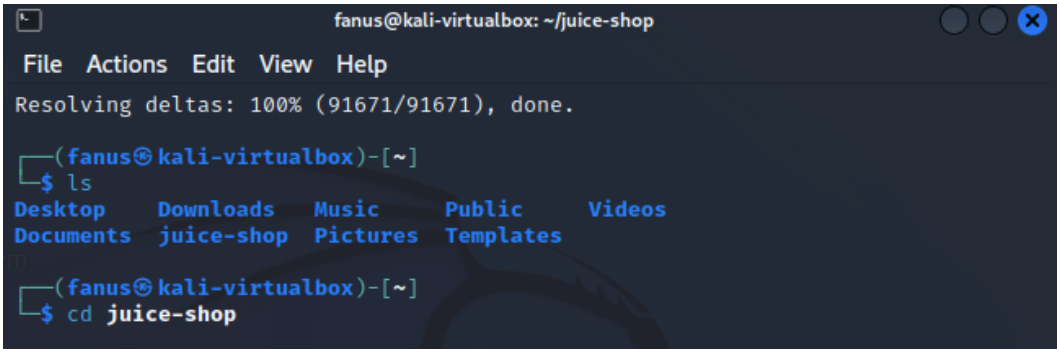
   - Untuk mengecek apakah npm sudah terinstall menggunakan perintah “npm -v”.

4. Download project OWASP Juice Shop melalui git. https://github.com/juice-shop/juice-shop.git

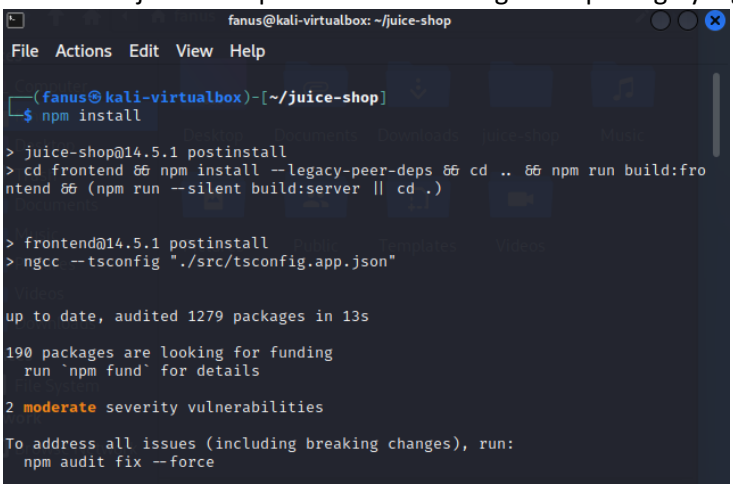


5. Setelah project terdownload masuk ke directory project dengan sintax “cd nama-directory” Sebelumnya pastikan directory project sudah terdownload dengan sintax “ls” atau melalui file manager

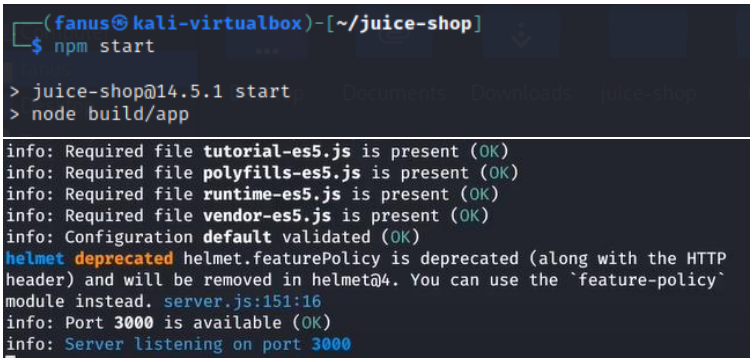




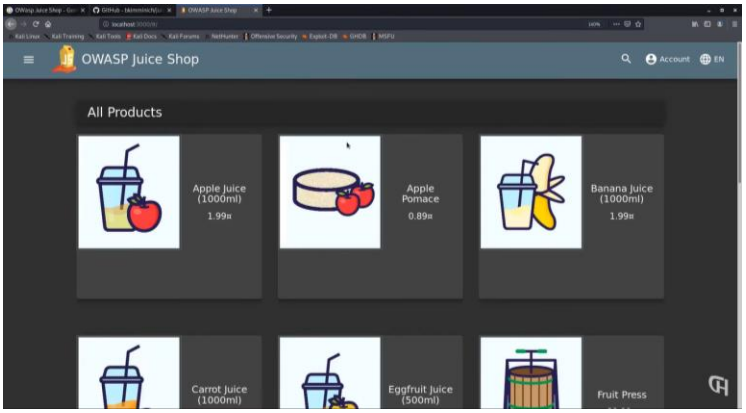
6. Setelah itu jalankan npm start untuk menginstall package yang tersedia di node module



7. Setelah package terinstall jalankan owasp juice shop dengan “npm run”



Maka website sudah bisa diakses.

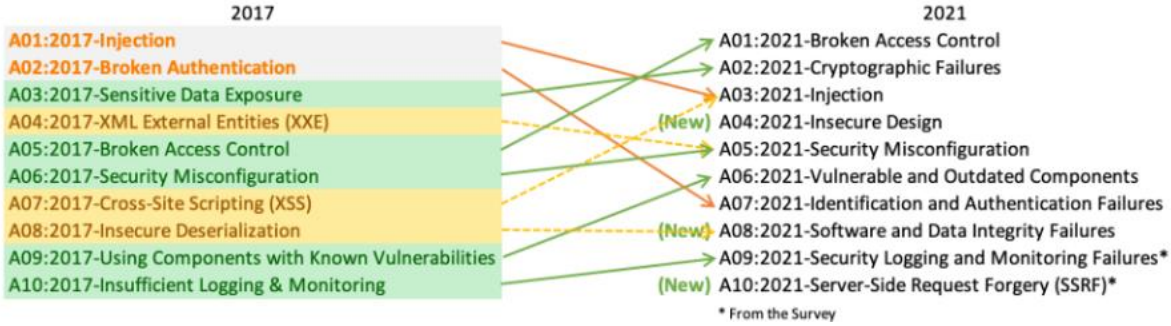


TUGAS 2 : Hubungan Antara OWASP 10 2022 dengan juice shop

Jawab :

1. OWASP Juice Shop adalah aplikasi web tidak aman yang paling modern dan canggih, yang mana aplikasi web ini biasa digunakan dalam pelatihan keamanan. **Di dalam juice shop, mencakup 10 kerentanan yang sering terjadi dan harus segera diatasi oleh sysadmin.**
2. OWASP Top 10 adalah panduan konvensional yang dapat digunakan oleh pemrogram dan tim keamanan aplikasi web untuk mengatasi kerentanan. Meskipun tidak mencakup semua risiko kerentanan, OWASP Top 10 dapat mengidentifikasi berbagai macam risiko keamanan yang sering terjadi dan harus segera diatasi oleh aplikasi web. OWASP Top 10 adalah standar keamanan dasar, terutama untuk aplikasi baru namun dapat juga digunakan pada aplikasi yang sudah cukup tua karena OWASP Top 10 menyediakan daftar checklist keamanan.

- Berdasarkan dari penjelasan OWASP TOP 10, OWASP 10 2022 adalah 10 daftar kerentanan teratas pada tahun 2022
- Berikut merupakan daftar OWASP TOP 10



- A01:2021-Broken Access Control
  Penyerang 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.
- A02:2021 Cryptographic Failures (Kegagalan Kriptografi)
  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.
- 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.
- A04:2021 Insecure Design (Kekurangan pada Desain)
- A05:2021 Security Misconfiguration (Kelemahan Konfigurasi Keamanan)
- A06:2021 Vulnerable and Outdated Components (Komponen yang rentan dan kadaluarsa)
- A07:2021 Identification and Authentication Failures (Kegagalan Identifikasi dan Autentikasi)

- A08:2021 Software and Data Integrity Failures (Kegagalan Perangkat Lunak dan Keutuhan Data)
- A09:2021 Security Logging and Monitoring Failures (Kegagalan pada keamanan logging dan monitoring data)
- A10:2021 Server-Side Request Forgery (SSRF)

-