

KEAMANAN JARINGAN OWASP

A06 – Vulnerable Component



OLEH :

Nadya Indah Trisnawati (3122640034)
Mochammad Jauhar Ulul Albab (3122640044)

PROGRAM STUDI TEKNIK INFORMATIKA
DEPARTEMEN TEKNIK INFORMATIKA DAN KOMPUTER
POLITEKNIK ELEKTRONIKA NEGERI SURABAYA

2022/2023

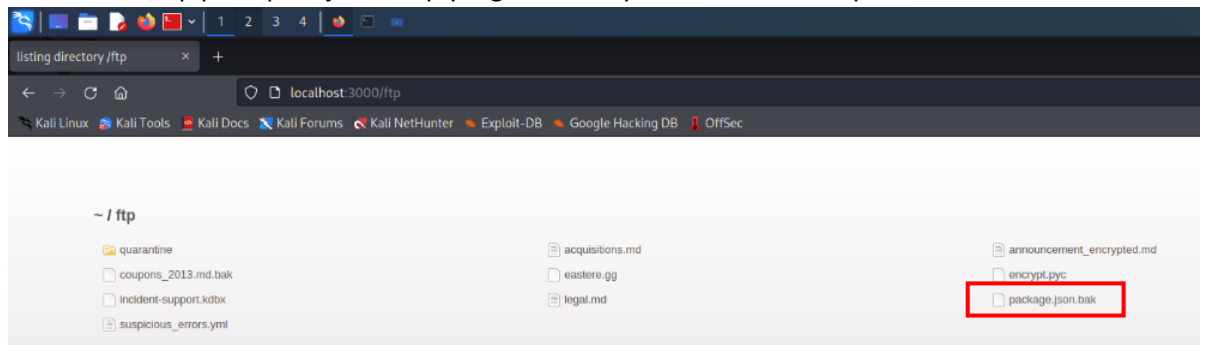
Vulnerable Component terjadi Ketika terdapat sebuah komponen yang yang berbahaya, sudah tidak lagi disupport dan komponen yang sudah tertinggal, komponen yang dimaksud adalah OS, server, DBMS, API library dan semua komponen yang terdapat pada aplikasi.

Untuk mengatasi vulnerable component dapat dilakukan dengan cara :

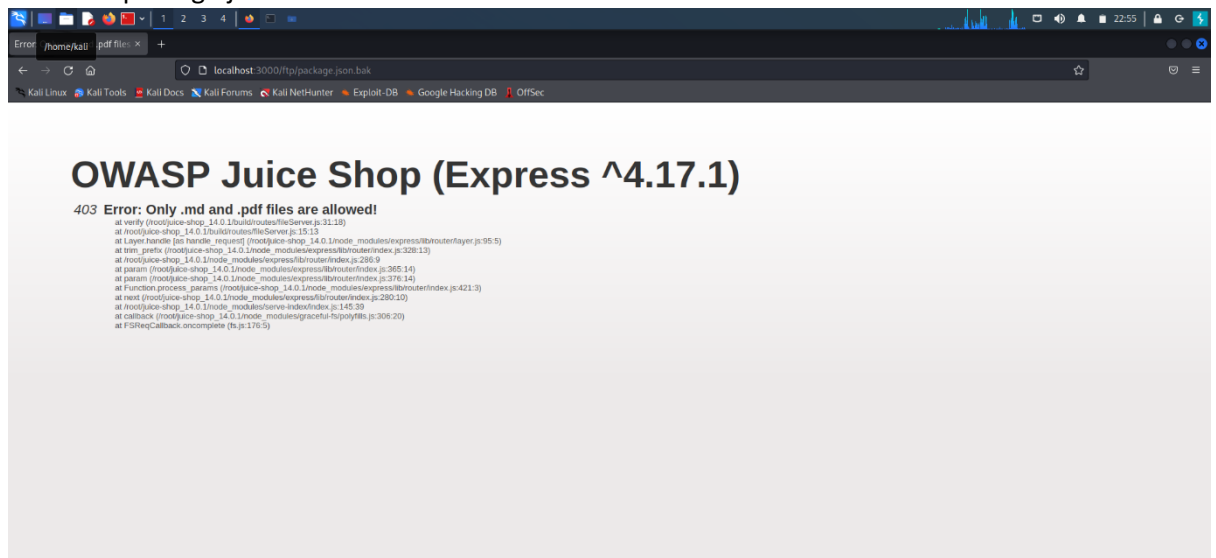
1. Menghapus dependensi, fitur, component, file dan dokumen yang tidak diperlukan
2. Gunakan komponen dari link official atau resmi
3. Monitoring library dan komponen yang digunakan

Untuk contoh serangan vulnerable component dapat dilakukan Legacy Typosquatting caranya adalah seperti berikut :

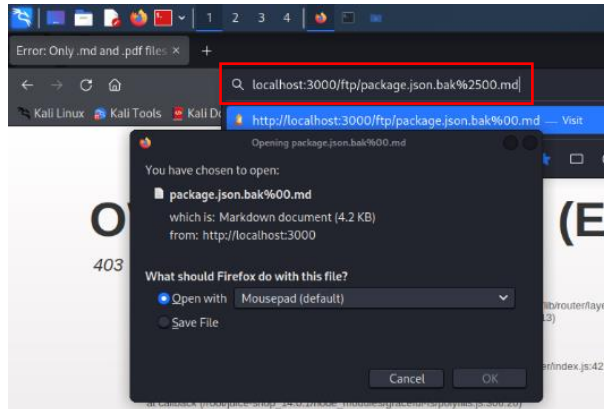
1. tambahkan /ftp pada path juiceshop yang didalamnya berisikan beberapa file dan folder



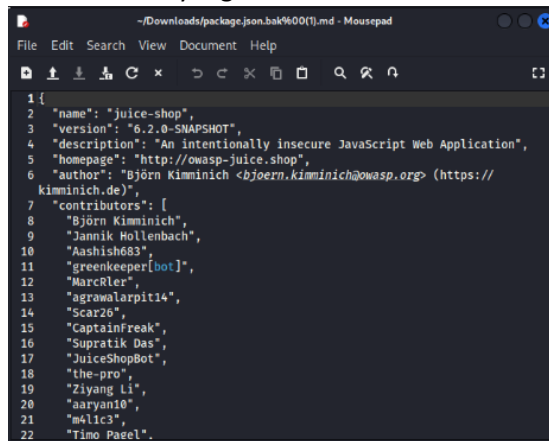
2. buka file package.json.bak



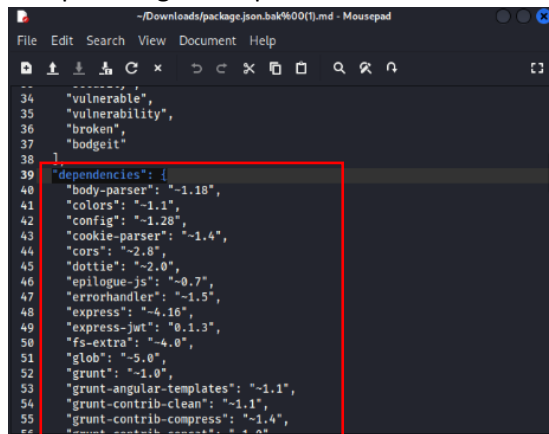
3. Tambahkan %2500.md pada path url agar file dapat diakses



4. Buka hasil file yang telah didownload



5. Cari pada bagian "dependencies"



6. Buka npmjs untuk melakukan pengecekan pada tiap dependencies apakah terdapat dependencies yang mencurigakan

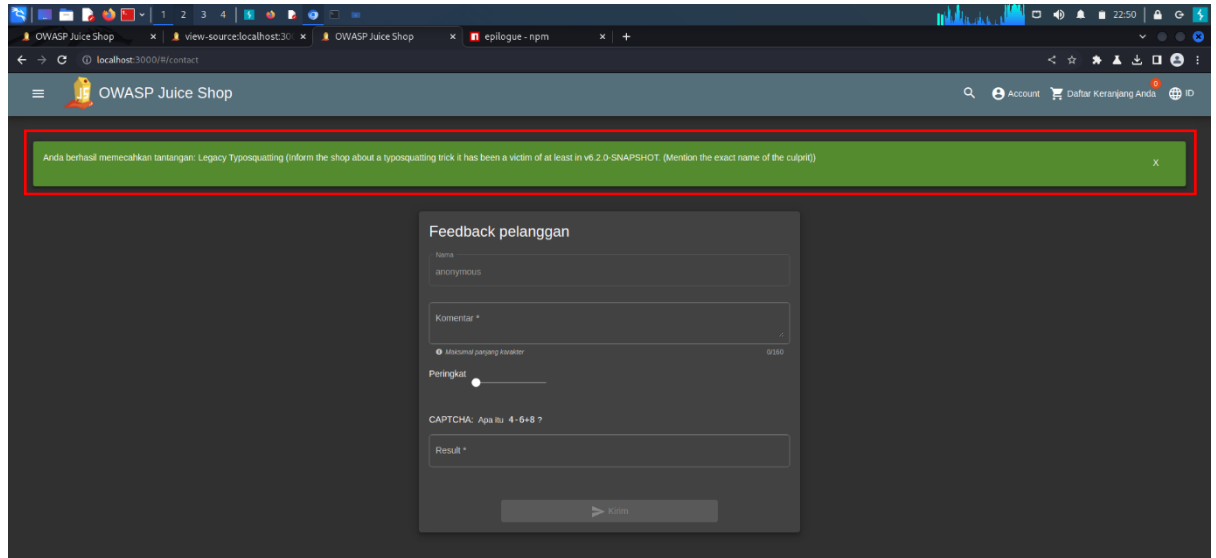
The screenshot shows the npmjs website for the 'body-parser' package. The package is version 1.20.2, published 3 months ago, and has 12 dependencies, 22,579 dependents, and 72 versions. The description states it is a Node.js body parsing middleware. A note mentions that the 'req.body' property is based on user-controlled input and should be validated. The 'Install' section shows the command 'npm i body-parser'. The repository is 'github.com/expressjs/body-parser'.

7. Disini saya menemukan terdapat dependencies yang mencurigakan yaitu epilogue-js yang dapat dilihat dari isi konten deskripsi pada website npmjs

The screenshot shows the npmjs website for the 'epilogue-js' package. The package is version 0.7.3, published 6 years ago, and has 3 dependencies, 2 dependents, and 2 versions. The description includes a warning: 'THIS IS NOT THE MODULE YOU ARE LOOKING FOR! Please use https://github.com/dchester/epilogue! This repository exists only for security awareness and training purposes to demonstrate the issue of typosquatting! Please read https://github.com/bkimminich/juice-shop/issues/368 and https://iamakulov.com/notes/npm-malicious-packages/ for more information!'. The 'Getting Started' section shows code for installing and using the package. The repository is 'github.com/dchester/epilogue'.

Terdapat pesan bahwa library ini bukan library yang ingin dicari dan library ini hanya dibuat untuk tujuan demonstrasi typosquatting.

8. Coba masukkan nama dependencies yang mencurigikan tersebut kedalam feedback juiceshop



Dan hasilnya percobaan demonstrasi typosquatting telah selesai