

**LAPORAN RESMI**  
**PRAKTIKUM KEAMANAN JARINGAN**  
**A06 VULNERABLE COMPONENT**



Oleh :

**Tarisa Dinda Deliyanti      3122640037**

**Fisabili Maghfirona Firdaus 3122640051**

**D4 LJ Teknik Informatika B**

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

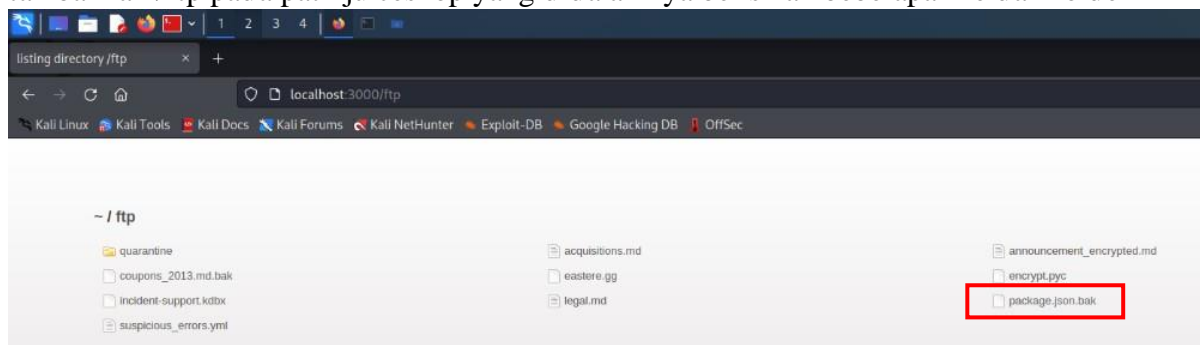
Vulnerable Component terjadi ketika terdapat sebuah komponen yang yang berbahaya, sudah tidak lagi disupport dan komponen yang sudah tertinggal, komponen yang dimaksud adalah OS, server, DBMS, API library, dan semua komponen yang terdapat pada aplikasi.

Untuk mengatasi vulnerable component dapat dilakukan dengan cara :

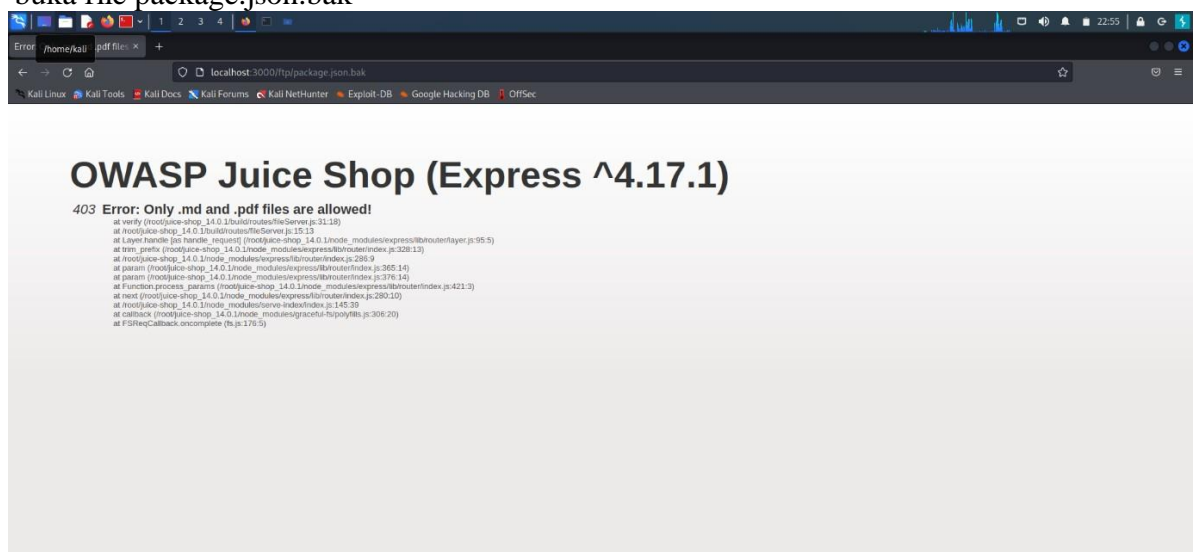
1. Menghapus dependensi, fitur, component, file, dan dokumen yang tidak diperlukan
2. Gunakan komponen dari link official atau resmi
3. Monitoring library dan komponen yang digunakan

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

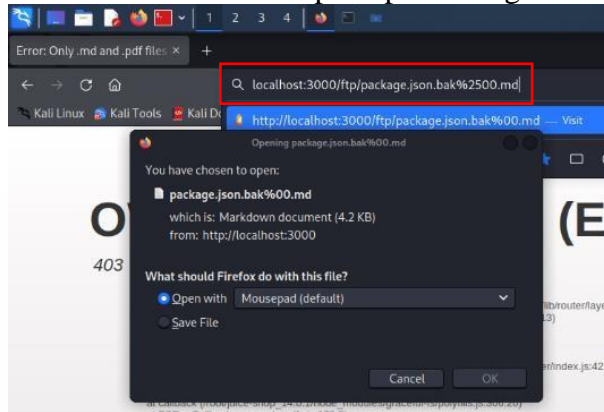
1. tambahkan /ftp pada path juiceshop yang didalamnya berisikan beberapa file dan folder



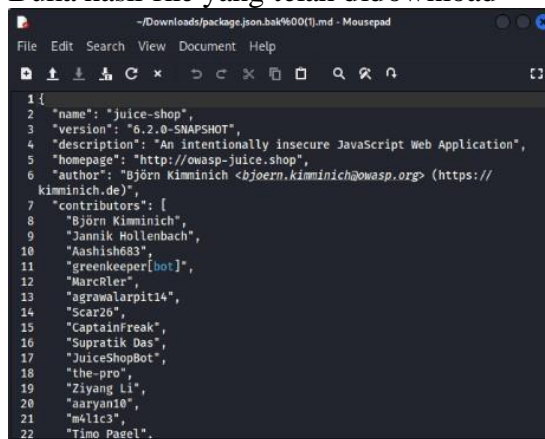
2. buka file package.json.bak



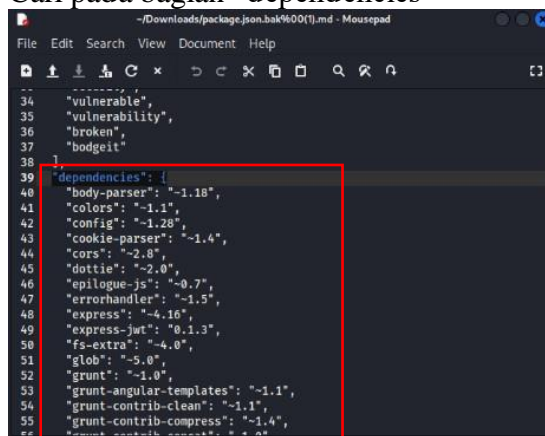
3. Tambahkan %2500.md pada path url agar file dapat diakses



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

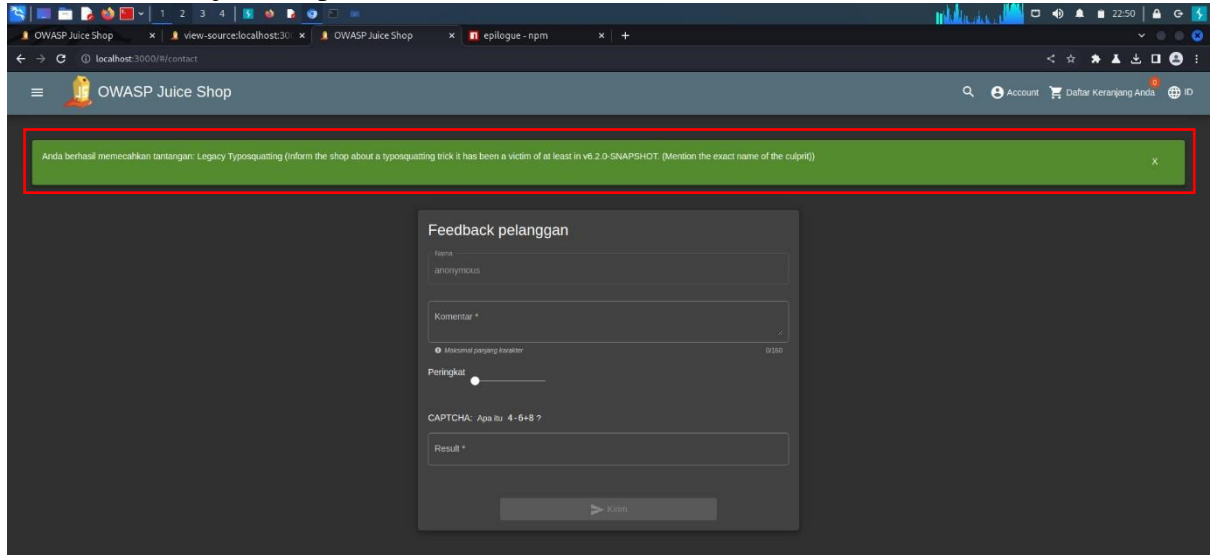
The screenshot shows the npmjs website for the 'body-parser' package. The package is version 1.20.2, published 3 months ago, and has 12 dependencies, 22,579 dependents, and 72 versions. The description states it is a body parsing middleware that parses incoming request bodies in a middleware before your handlers, available under the 'req.body' property. A note mentions that 'req.body' 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' and the 'Homepage' is 'github.com/expressjs/body-parser#readme'. The 'Weekly Downloads' are 28,370,209.

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 states it is a module for creating flexible REST endpoints and controllers from Sequelize models in Express or Restify apps. The 'Install' section shows the command 'npm i epilogue-js'. The 'Repository' is 'github.com/dchester/epilogue' and the 'Homepage' is 'github.com/dchester/epilogue#readme'. The 'Weekly Downloads' are 6. The 'Version' is 0.7.3 and the 'License' is MIT. The 'Issues' are 60 and the 'Pull Requests' are 11. The 'Last publish' is 6 years ago. The 'Collaborators' section shows the package owner. The 'Getting Started' section shows a code snippet for using the package with Sequelize. A warning message states: '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!'

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 mencurigakan tersebut ke dalam feedbackjuiceshop



Dan hasilnya percobaan demonstrasi typosquatting telah selesai