

LAPORAN RESMI
PRAKTIKUM KEAMANAN JARINGAN
A06 VULNERABLE COMPONENTS



Oleh :

Tarisa Dinda Deliyanti 3122640037

Fisabili Maghfirona Firdaus 3122640051

D4 LJ Teknik Informatika B

POLITEKNIK ELEKTRONIKA NEGERI SURABAYA
TAHUN AJARAN 2022/2023

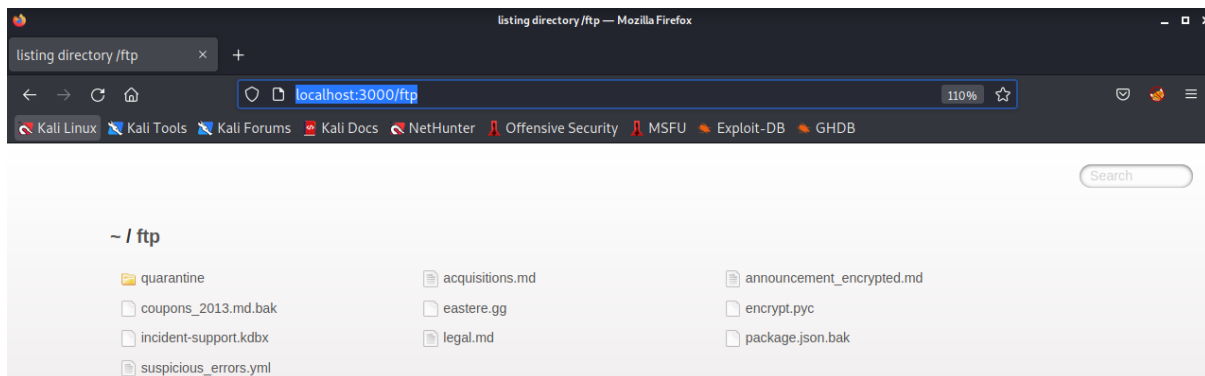
Vulnerable Components adalah komponen yang digunakan untuk membangun aplikasi yang telah usang atau memiliki kerentanan. Masalah ini juga ada di daftar 10 Teratas tahun 2017 dan telah mendapatkan posisi yang lebih baik: #6, sementara itu berada di posisi #9 di tahun 2017 dan diberi nama Using Components with Known Vulnerabilities. Percaya atau tidak, mengelola dependensi Anda adalah pekerjaan yang berat. Ini tidak sesederhana menjalankan perintah pembaruan atau mengunduh dependensi & paket yang diperbarui. Tapi lebih dari ini: aplikasi Anda mungkin rusak dengan perubahan terbaru, beberapa fitur mungkin tidak digunakan lagi, fungsi mungkin diganti namanya, dependensi mungkin ditinggalkan, perbaikan mungkin tidak berfungsi pada sistem Anda tanpa merusak beberapa dependensi lain, membuat malapetaka. Anda mendapatkan ide yang benar.

Percobaan

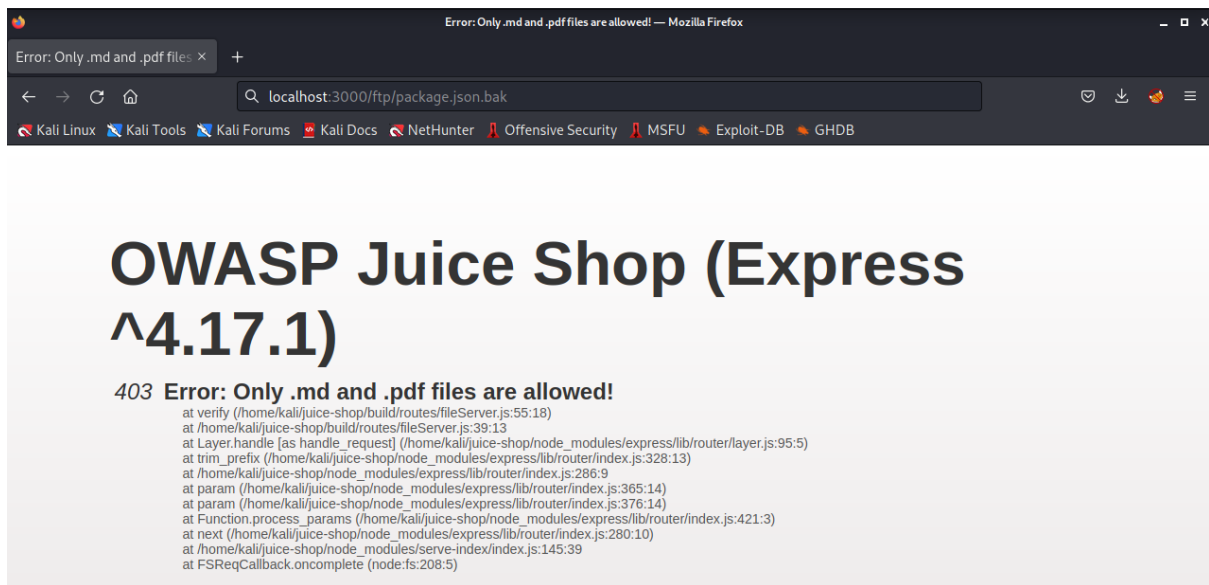
Percobaan dapat dilakukan dengan menggunakan Legacy Typosquatting.

Typosquatting yang juga disebut URL hijacking, sting site, atau fake URL, adalah bentuk cybersquatting, dan kemungkinan brandjacking yang bergantung pada kesalahan seperti kesalahan ketik yang dibuat oleh pengguna Internet saat memasukkan alamat situs web ke dalam browser web. Jika pengguna secara tidak sengaja memasukkan alamat situs web yang salah, mereka dapat diarahkan ke URL apa pun (termasuk situs web alternatif yang dimiliki oleh cybersquatter). Ini bisa merujuk ke google.com. Google.com adalah situs web berbahaya salah ketik yang bahkan dapat membahayakan komputer Anda dan menghapus ROM Anda dalam 30 detik.

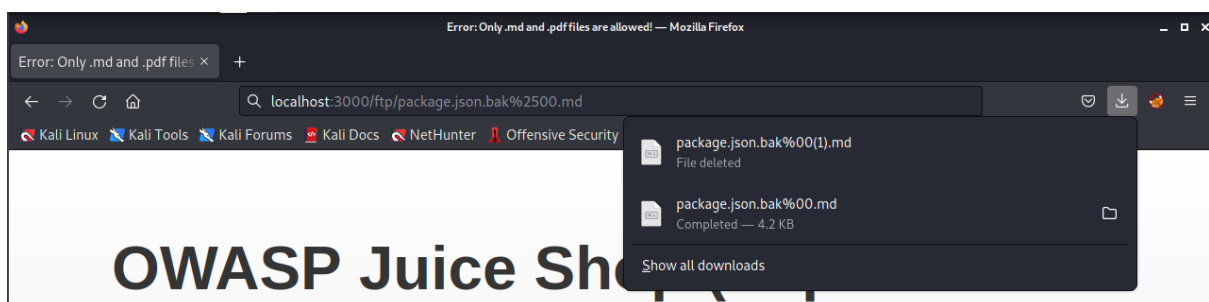
1. Langkah pertama kita pergi ke URL berikut <http://localhost:3000/ftp>



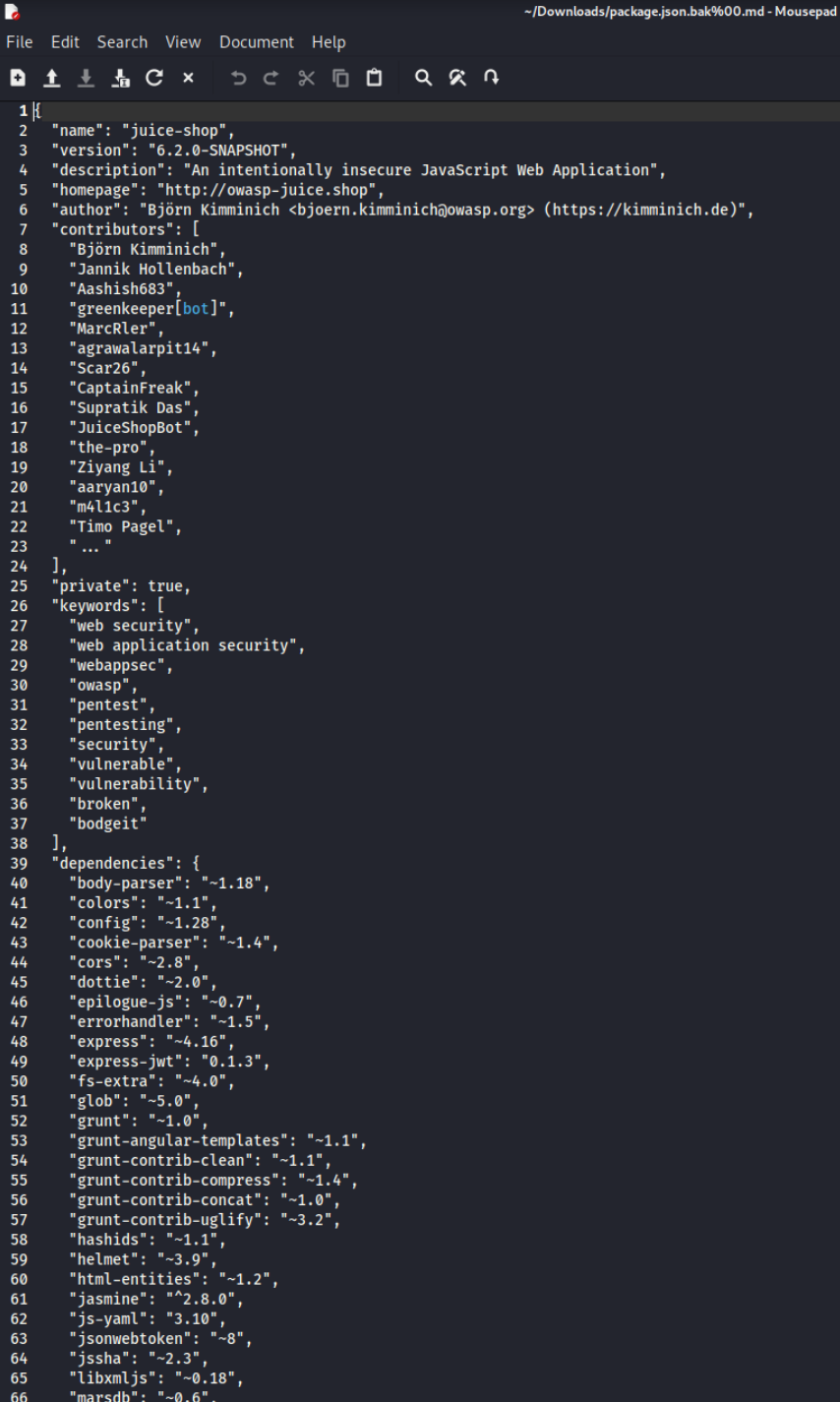
- Setelah itu kita akan ditunjukkan list file yang ada pada directory ftp ini seperti gambar diatas. Kita buka file yang bernama package.json.bak



- Kemudian akan muncul tampilan seperti pada gambar yang menampilkan error bahwa file tersebut tidak bisa dibuka. Ubah URL halaman package.json.bak menjadi seperti berikut <http://localhost:3000/ftp/package.json.bak%2500.md>



4. Lalu menjalankan URL tersebut yang akan mendownload file yang berisi package json website tersebut



The screenshot shows a text editor window titled "~Downloads/package.json.bak%00.md - Mousepad". The editor contains a JSON file for a project named "juice-shop". The file includes metadata like version, description, homepage, author, and contributors. It also lists various keywords related to web security and application security. A detailed list of dependencies is provided, including packages like "body-parser", "express", "jsonwebtoken", and "helmet".

```
1{
2  "name": "juice-shop",
3  "version": "6.2.0-SNAPSHOT",
4  "description": "An intentionally insecure JavaScript Web Application",
5  "homepage": "http://owasp-juice.shop",
6  "author": "Björn Kimminich <bjoern.kimminich@owasp.org> (https://kimminich.de)",
7  "contributors": [
8    "Björn Kimminich",
9    "Jannik Hollenbach",
10   "Aashish683",
11   "greenkeeper[bot]",
12   "MarcRler",
13   "agrawalarpit14",
14   "Scar26",
15   "CaptainFreak",
16   "Supratik Das",
17   "JuiceShopBot",
18   "the-pro",
19   "Ziyang Li",
20   "aaryan10",
21   "m4l1c3",
22   "Timo Pagel",
23   "... "
24 ],
25 "private": true,
26 "keywords": [
27   "web security",
28   "web application security",
29   "webappsec",
30   "owasp",
31   "pentest",
32   "pentesting",
33   "security",
34   "vulnerable",
35   "vulnerability",
36   "broken",
37   "bodgeit"
38 ],
39 "dependencies": {
40   "body-parser": "~1.18",
41   "colors": "~1.1",
42   "config": "~1.28",
43   "cookie-parser": "~1.4",
44   "cors": "~2.8",
45   "dottie": "~2.0",
46   "epilogue-js": "~0.7",
47   "errorhandler": "~1.5",
48   "express": "~4.16",
49   "express-jwt": "0.1.3",
50   "fs-extra": "~4.0",
51   "glob": "~5.0",
52   "grunt": "~1.0",
53   "grunt-angular-templates": "~1.1",
54   "grunt-contrib-clean": "~1.1",
55   "grunt-contrib-compress": "~1.4",
56   "grunt-contrib-concat": "~1.0",
57   "grunt-contrib-uglify": "~3.2",
58   "hashids": "~1.1",
59   "helmet": "~3.9",
60   "html-entities": "~1.2",
61   "jasmine": "^2.8.0",
62   "js-yaml": "3.10",
63   "jsonwebtoken": "~8",
64   "jssha": "~2.3",
65   "libxmljs": "~0.18",
66   "marsdb": "~0.6".
```

5. Dari file package json ini cek dependencies apa saja yang digunakan oleh aplikasi. Setelah itu salah satu dependencies yang sepertinya tidak seharusnya atau typo dalam penulisannya tetapi dapat digunakan yaitu yang bernama epilogue-js. Ketika buka pada website npm muncul tampilan sebagai berikut

epilogue-js - npm — Mozilla Firefox

epilogue-js - npm

https://www.npmjs.com/package/epilogue-js

Kali Linux Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU Exploit-DB GHDB

Nuclear Powered Mushroom Pro Teams Pricing Documentation


npm Search packages Search Sign Up Sign In

epilogue-js
0.7.3 • Public • Published 6 years ago

Readme Code Beta 3 Dependencies 2 Dependents 2 Versions

build unknown **Dependency Status**

Epilogue



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!

Install

```
> npm i epilogue-js
```

Repository

github.com/dchester/epilogue

Homepage

github.com/dchester/epilogue#readme

Weekly Downloads

8

Version	License
0.7.3	MIT

Issues	Pull Requests
60	11

Last publish
6 years ago

- Untuk package yang seharusnya digunakan adalah package epilogue bukan epilogue-js

The screenshot shows the npm package page for 'epilogue' in a Mozilla Firefox browser. The browser's address bar shows 'https://www.npmjs.com/package/epilogue'. The page header includes navigation links like 'Pro', 'Teams', 'Pricing', and 'Documentation'. The main content area displays the package name 'epilogue' with a 'DT' badge, version '0.7.1', and status 'Public'. It also shows 'Published 6 years ago'. Below this are links for 'Readme', 'Code', 'Beta', '3 Dependencies', '10 Dependents', and '19 Versions'. A 'build' button is labeled 'unknown'. The 'Install' section shows the command 'npm i epilogue'. The 'Repository' section points to 'github.com/dchester/epilogue'. The 'Homepage' section points to 'github.com/dchester/epilogue#readme'. A 'Weekly Downloads' chart shows 323 downloads. A table lists 'Version' (0.7.1) and 'License' (MIT). Another table lists 'Issues' (60) and 'Pull Requests' (11). The 'Last publish' date is '6 years ago'. The 'Getting Started' section contains a code snippet for setting up the package with Sequelize and Restify.

```
var Sequelize = require('sequelize'),
    epilogue = require('epilogue'),
    http = require('http');

// Define your models
var database = new Sequelize('database', 'root', 'password');
var User = database.define('User', {
  username: Sequelize.STRING,
  birthday: Sequelize.DATE
});

// Initialize server
var server, app;
if (process.env.USE_RESTIFY) {
  var restify = require('restify');
```

7. Informasikan temuan ini pada customer feedback untuk menyelesaikan challenge ini

The screenshot shows the OWASP Juice Shop Customer Feedback form. The form is titled 'Customer Feedback' and has a dark theme. It includes fields for 'Author' (set to 'anonymous'), 'Comment' (with the text 'epilogue.js' and a character count of 11/160), 'Rating' (a slider), and a CAPTCHA question 'What is 8-9*6 ?' with the answer '-46'. A 'Submit' button is at the bottom.

8. Berhasil mendapatkan notifikasi bahwa percobaan berhasil.

