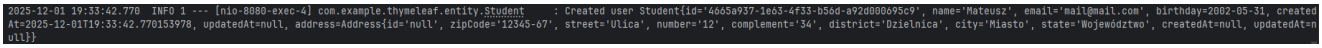
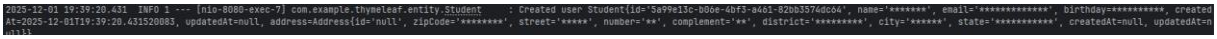
Name	E-mail	Age	Birthday	Street	District	City	State	Created at	Actions
Mateusz	mail@mail.com	23	31/05/2002	Ulica	Dzielnica	Miasto	Województwo	01/12/2025 19:33:42	

Tworzenie nowego użytkownika przed wprowadzonymi zmianami:



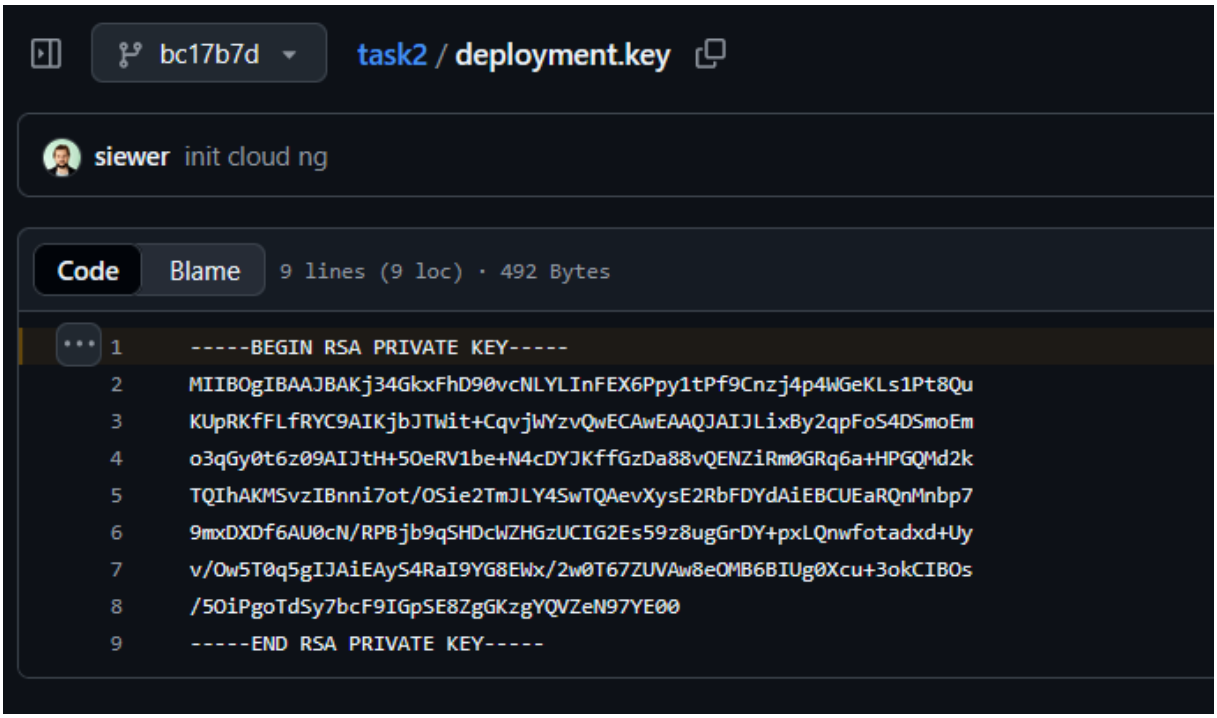
Po zmianach:

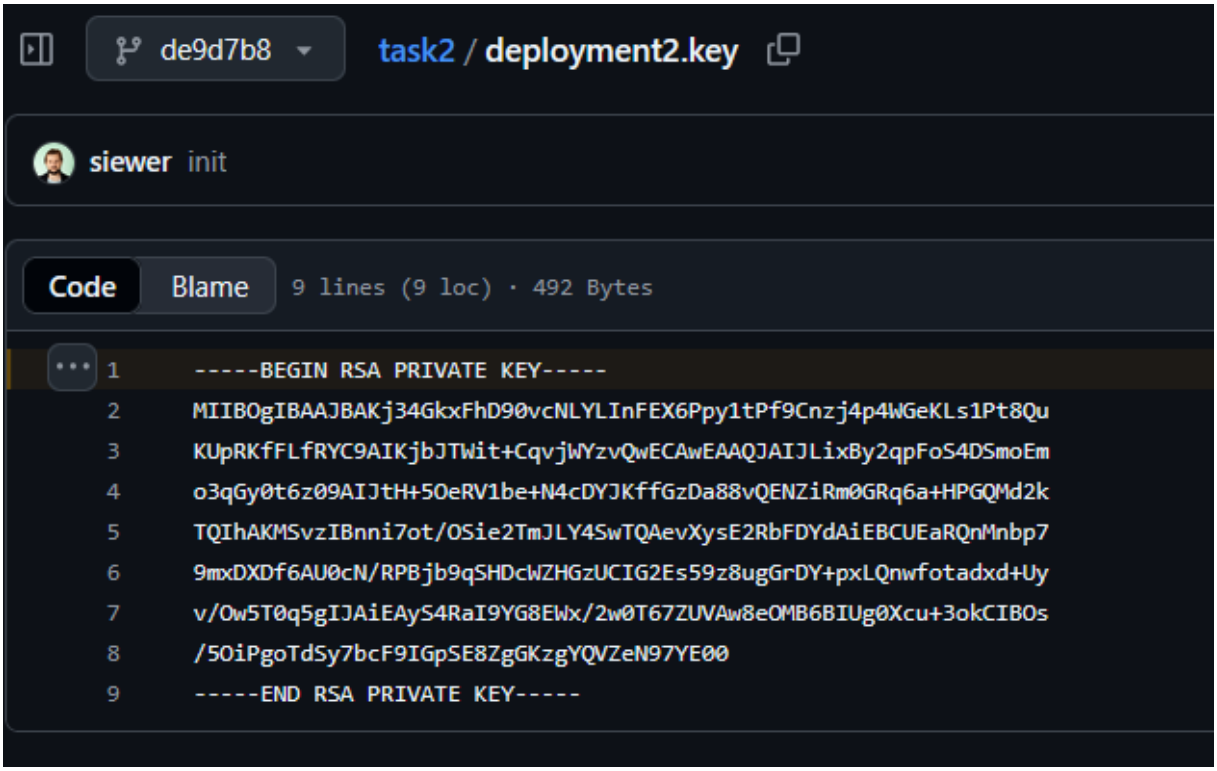


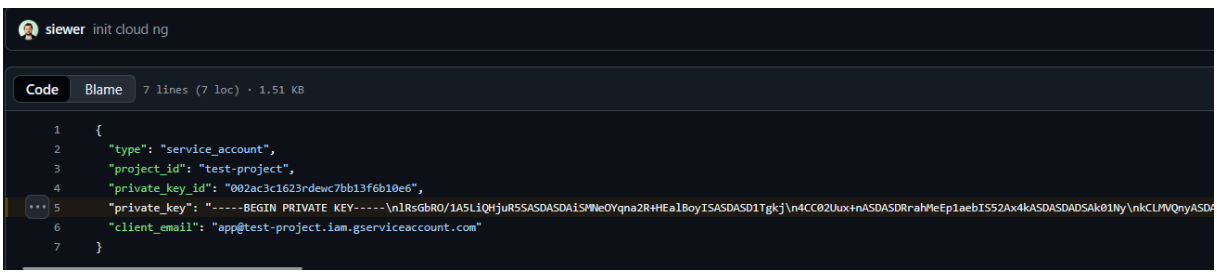
Zadanie 2

```
PS C:\Programowanie\TBO\task2> docker run -v C:\Programowanie\TBO\task2:/path zricethezav/gitleaks:latest detect --source="/path" -v

    ○
    │╲
    │ ○
    ○ ▒
    ▒   gitleaks

Finding:     -----BEGIN RSA PRIVATE KEY-----
MIIBOgIBAAJBAKj34GkxFhD90vcNLYLInFEX6Ppy1tPf9Cnzj4p4WGeKLs1Pt8Qu
KUp...
Secret:      -----BEGIN RSA PRIVATE KEY-----
MIIBOgIBAAJBAKj34GkxFhD90vcNLYLInFEX6Ppy1tPf9Cnzj4p4WGeKLs1Pt8Qu
KUp...
RuleID:      private-key
Entropy:     5.875154
File:        deployment2.key
Line:        1
Commit:      de9d7b8cb63bd7ae741ec5c9e23891b71709bc28
Author:      Grzegorz Siewruk
Email:       gsiewruk@gmail.com
Date:        2023-11-15T12:49:39Z
Fingerprint: de9d7b8cb63bd7ae741ec5c9e23891b71709bc28:deployment2.key:private-key:1
Link:        https://github.com/MalkowskiM/task2/blob/de9d7b8cb63bd7ae741ec5c9e23891b71709bc28/deployment2.key#L1

Finding:     -----BEGIN RSA PRIVATE KEY-----
MIIBOgIBAAJBAKj34GkxFhD90vcNLYLInFEX6Ppy1tPf9Cnzj4p4WGeKLs1Pt8Qu
KUp...
Secret:      -----BEGIN RSA PRIVATE KEY-----
MIIBOgIBAAJBAKj34GkxFhD90vcNLYLInFEX6Ppy1tPf9Cnzj4p4WGeKLs1Pt8Qu
KUp...
RuleID:      private-key
Entropy:     5.875154
File:        deployment.key
Line:        1
Commit:      bc17b7ddc46f46fff175aed55d68e11bb48166cc
Author:      Grzegorz Siewruk
Email:       gsiewruk@gmail.com
Date:        2023-11-15T12:52:32Z
Fingerprint: bc17b7ddc46f46fff175aed55d68e11bb48166cc:deployment.key:private-key:1
Link:        https://github.com/MalkowskiM/task2/blob/bc17b7ddc46f46fff175aed55d68e11bb48166cc/deployment.key#L1
```

```
Finding:     "private_key": "-----BEGIN PRIVATE KEY-----\nlRsGbRO/1A5LiQHjuR5SASDASDAiSMNeOYqna2R+HEalBoyISASDASD1Tgkj\n4CC02Uux+...\n",
Secret:      -----BEGIN PRIVATE KEY-----\nlRsGbRO/1A5LiQHjuR5SASDASDAiSMNeOYqna2R+HEalBoyISASDASD1Tgkj\n4CC02Uux+...
RuleID:      private-key
Entropy:     5.917361
File:        awscredentials.json
Line:        5
Commit:      bc17b7ddc46f46fff175aed55d68e11bb48166cc
Author:      Grzegorz Siewruk
Email:       gsiewruk@gmail.com
Date:        2023-11-15T12:52:32Z
Fingerprint: bc17b7ddc46f46fff175aed55d68e11bb48166cc:awscredentials.json:private-key:5
Link:        https://github.com/MalkowskiM/task2/blob/bc17b7ddc46f46fff175aed55d68e11bb48166cc/awscredentials.json#L5
```



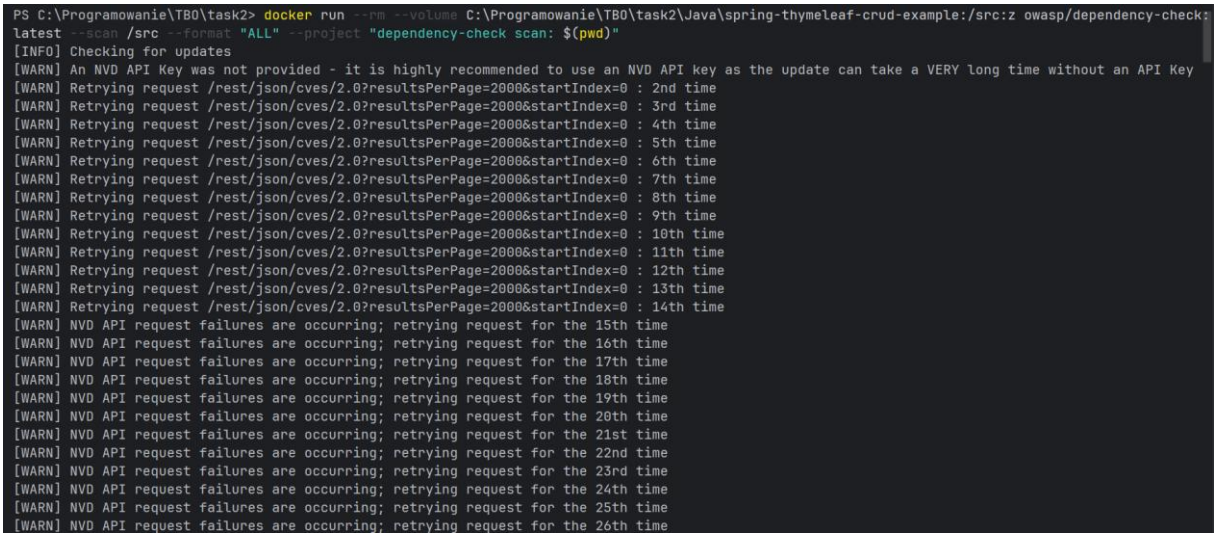


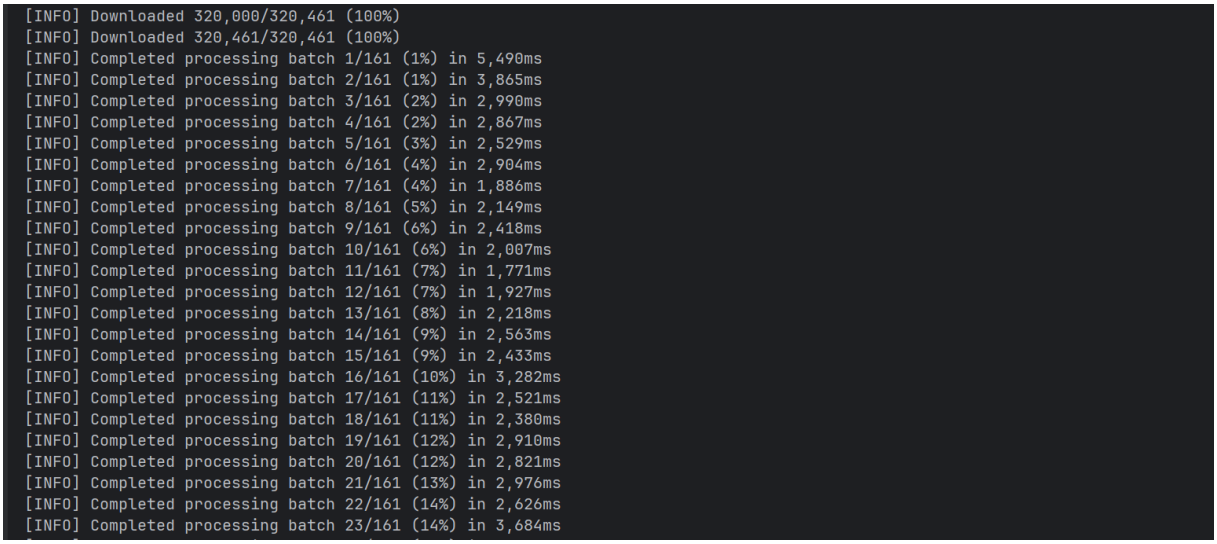


Gitleaks wykrył jedynie prawdziwe wycieki

Zadanie 3

docker run --rm --volume C:\Programowanie\TBO\task2\Java\spring-thymeleaf-crud-example:/src:z owasp/dependency-check:latest --scan /src --format "ALL" --project "dependency-check scan: $(pwd)"





```
[INFO] Completed processing batch 160/161 (99%) in 593ms
[INFO] Completed processing batch 161/161 (100%) in 82ms
[INFO] Updating CISA Known Exploited Vulnerability list: https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json
[INFO] Begin database defrag
[INFO] End database defrag (10190 ms)
[INFO] Check for updates complete (1628823 ms)
[INFO]

Dependency-Check is an open source tool performing a best effort analysis of 3rd party dependencies; false positives and false negatives may exist i
n the analysis performed by the tool. Use of the tool and the reporting provided constitutes acceptance for use in an AS IS condition, and there are
 NO warranties, implied or otherwise, with regard to the analysis or its use. Any use of the tool and the reporting provided is at the user's risk.
In no event shall the copyright holder or OWASP be held liable for any damages whatsoever arising out of or in connection with the use of this tool,
 the analysis performed, or the resulting report.


   About ODC: https://dependency-check.github.io/DependencyCheck/general/internals.html
   False Positives: https://dependency-check.github.io/DependencyCheck/general/suppression.html
```

```
[INFO] Analysis Started
[INFO] Finished File Name Analyzer (0 seconds)
[WARN] Analyzing `/src/src/main/resources/static/vendors/jquery-mask/package-lock.json` - however, the node_modules directory does not exist. Please
 run `npm install` prior to running dependency-check
[WARN] Analyzing `/src/target/classes/static/vendors/jquery-mask/package-lock.json` - however, the node_modules directory does not exist. Please run
 `npm install` prior to running dependency-check
[INFO] Finished Node.js Package Analyzer (0 seconds)
[INFO] Finished Dependency Merging Analyzer (0 seconds)
[INFO] Finished Hint Analyzer (0 seconds)
[INFO] Finished Version Filter Analyzer (0 seconds)
[INFO] Created CPE Index (4 seconds)
[INFO] Finished CPE Analyzer (5 seconds)
[INFO] Finished False Positive Analyzer (0 seconds)
[INFO] Finished NVD CVE Analyzer (0 seconds)
[INFO] Finished Node Audit Analyzer (1 seconds)
[INFO] Finished RetireJS Analyzer (7 seconds)
[WARN] Disabling OSS Index analyzer due to missing user/password credentials. Authentication is now required: https://ossindex.sonatype.org/doc/-req
-required
[INFO] Finished Vulnerability Suppression Analyzer (0 seconds)
[INFO] Finished Known Exploited Vulnerability Analyzer (0 seconds)
[INFO] Finished Dependency Bundling Analyzer (0 seconds)
[INFO] Finished Unused Suppression Rule Analyzer (0 seconds)
[INFO] Analysis Complete (14 seconds)
[INFO] Writing XML report to: /src/./dependency-check-report.xml
[INFO] Writing HTML report to: /src/./dependency-check-report.html
[INFO] Writing JSON report to: /src/./dependency-check-report.json
[INFO] Writing CSV report to: /src/./dependency-check-report.csv
[INFO] Writing SARIF report to: /src/./dependency-check-report.sarif
```

```
[INFO] Writing JENKINS report to: /src/./dependency-check-jenkins.html
[INFO] Writing JUNIT report to: /src/./dependency-check-junit.xml
[INFO] Writing GITLAB report to: /src/./dependency-check-gitlab.json
```

DEPENDENCY-CHECK

How to read the report | Suppressing false positives | Getting Help: github issues

Project: dependency-check scan: C:\Programowanie\TBO\task2

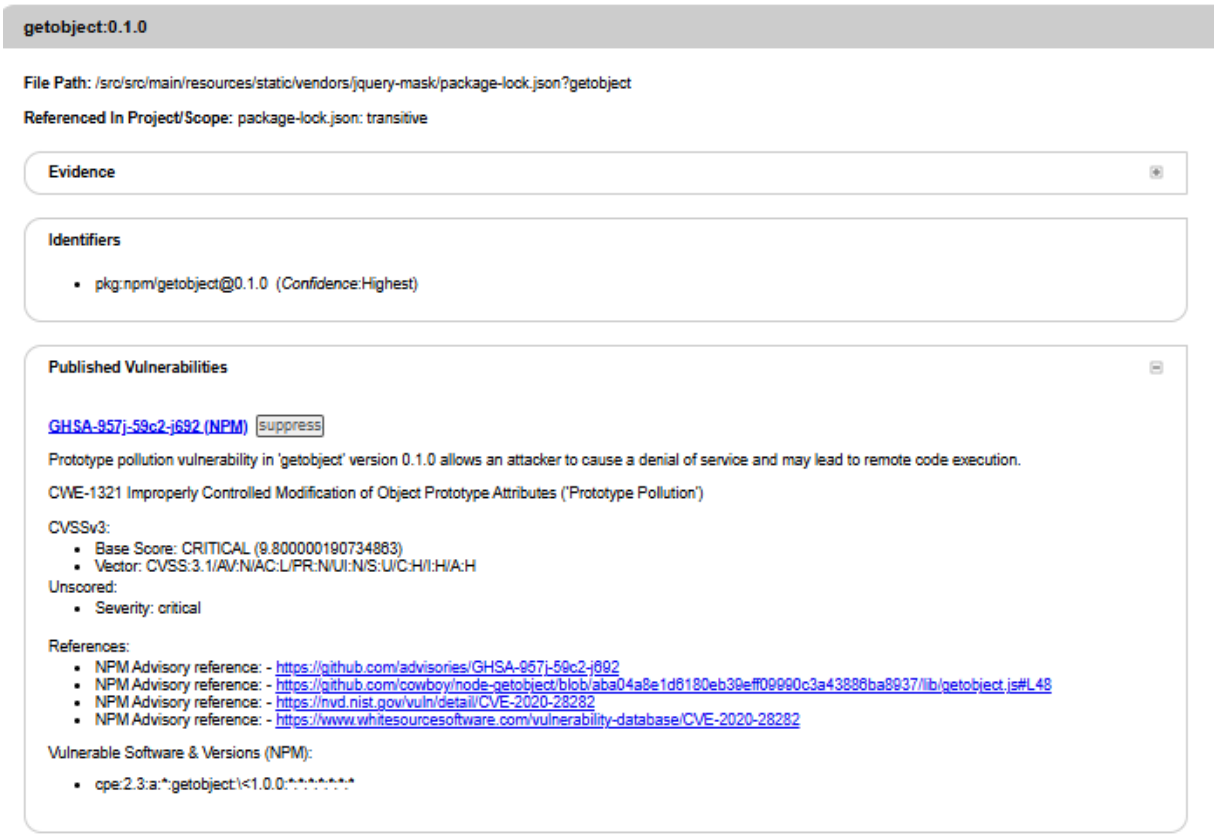
Scan Information (show all):

- *dependency-check version*: 12.1.9
- *Report Generated On*: Sun, 7 Dec 2025 17:35:42 GMT
- *Dependencies Scanned*: 103 (59 unique)
- *Vulnerable Dependencies*: 25
- *Vulnerabilities Found*: 33
- *Vulnerabilities Suppressed*: 0
- ...

Summary

Summary of Vulnerable Dependencies (click to show all)

Dependency	Vulnerability IDs	Package	Highest Severity	CVE Count	Confidence	Evidence Count
ajv:6.10.2		pkg:npm/ajv@6.10.2	MEDIUM	1		3
brace-expansion:1.1.8		pkg:npm/brace-expansion@1.1.8	LOW	1		3
debug:3.2.6		pkg:npm/debug@3.2.6	LOW	1		3
debug:4.1.1		pkg:npm/debug@4.1.1	LOW	1		3
form-data:2.3.3		pkg:npm/form-data@2.3.3	CRITICAL	1		3
getobject:0.1.0		pkg:npm/getobject@0.1.0	CRITICAL	1		3
grunt:1.0.4		pkg:npm/grunt@1.0.4	HIGH	3		3
hosted-git-info:2.5.0		pkg:npm/hosted-git-info@2.5.0	MEDIUM	1		3
https-proxy-agent:2.2.2		pkg:npm/https-proxy-agent@2.2.2	MEDIUM	1		3
js-yaml:3.13.1		pkg:npm/js-yaml@3.13.1	MEDIUM	1		3
json-schema:0.2.3		pkg:npm/json-schema@0.2.3	CRITICAL	1		3
lodash:4.17.15		pkg:npm/lodash@4.17.15	HIGH	3		3
minimatch:3.0.4		pkg:npm/minimatch@3.0.4	HIGH	1		3
minimist:0.0.8		pkg:npm/minimist@0.0.8	CRITICAL	2		3
minimist:1.2.0		pkg:npm/minimist@1.2.0	CRITICAL	2		3
on-headers:1.0.2		pkg:npm/on-headers@1.0.2	LOW	1		3
qs:6.5.2		pkg:npm/qs@6.5.2	HIGH	1		3
request:2.88.0		pkg:npm/request@2.88.0	MEDIUM	1		3
semver:5.4.1		pkg:npm/semver@5.4.1	HIGH	1		3
send:0.16.1		pkg:npm/send@0.16.1	MEDIUM	1		3
serve-static:1.13.1		pkg:npm/serve-static@1.13.1	MEDIUM	1		3
shelljs:0.3.0		pkg:npm/shelljs@0.3.0	HIGH	2		3
tough-cookie:2.4.3		pkg:npm/tough-cookie@2.4.3	MEDIUM	1		3
trim-newlines:1.0.0		pkg:npm/trim-newlines@1.0.0	HIGH	1		3
ws:6.2.1		pkg:npm/ws@6.2.1	HIGH	2		3



W pakiecie **getobject:0.1.0** wykryto podatność typu **Prototype Pollution** (mogącą prowadzić do RCE/DoS) oznaczoną jako **krytyczna.** Wykorzystanie podatności jest możliwe po przekazaniu złośliwych danych wejściowych, które są następnie przetwarzane przez funkcję ustawiającą właściwości w obiekcie (np. setKey() lub podobną funkcję z logiki biblioteki getobject) bez odpowiedniej walidacji kluczy. Po analizie w badanej aplikacji biblioteka getobject jest używana jako zależność przejściowa w pliku package-lock.json, co oznacza, że jest używana przez inną zależność, a nie ma bezpośredniej informacji o tym, która konkretna metoda jest wykorzystywana przez aplikację, dlatego nie można stwierdzić, że prawdopodobieństwo wykorzystania tej podatności jest minimalne.