

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:


```
2025-12-01 19:33:42.770 INFO 1 --- [nio-8080-exec-4] com.example.thymeleaf.entity.Student : Created user Student(id='4b5e937-16b3-4f33-b5ed-492d098095c9', name='Mateusz', email='mail@mail.com', birthday=2002-05-31, createdAt=2025-12-01T19:33:42.770153978, updatedAt=null, address=Address(id='null', zipCode='12345-07', street='Ulica', number='12', complement='34', district='Dzielnica', city='Miasto', state='Województwo', createdAt=null, updatedAt=null))
```

Po zmianach:

```
2025-12-01 19:39:20.431 INFO 1 --- [nio-8080-exec-7] com.example.thymeleaf.entity.Student : Created user Student(id='5a99e13c-b0ee-40f3-ae61-82bb3574dc0e', name='*****', email='*****', birthday=*****, createdAt=2025-12-01T19:39:20.431520083, updatedAt=null, address=Address(id='null', zipCode='*****', street='*****', number='**', complement='**', district='*****', city='*****', state='*****', createdAt=null, updatedAt=null))
```

Zadanie 2

```
PS C:\Programowanie\TB0\task2> docker run -v C:\Programowanie\TB0\task2:/path zricethezav/gitleaks:latest detect --source="/path" -v
```



```
Finding: -----BEGIN RSA PRIVATE KEY-----
MII80gIBAAJBAKj34GkxFhD90vcNLYLInFEX6Ppy1tPf9Cnzj4p4W6eKls1Pt8Qu
KUp...
Secret: -----BEGIN RSA PRIVATE KEY-----
MII80gIBAAJBAKj34GkxFhD90vcNLYLInFEX6Ppy1tPf9Cnzj4p4W6eKls1Pt8Qu
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/Ma1kowsk1M/task2/blob/de9d7b8cb63bd7ae741ec5c9e23891b71709bc28/deployment2.key#L1

Finding: -----BEGIN RSA PRIVATE KEY-----
MII80gIBAAJBAKj34GkxFhD90vcNLYLInFEX6Ppy1tPf9Cnzj4p4W6eKls1Pt8Qu
KUp...
Secret: -----BEGIN RSA PRIVATE KEY-----
MII80gIBAAJBAKj34GkxFhD90vcNLYLInFEX6Ppy1tPf9Cnzj4p4W6eKls1Pt8Qu
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/Ma1kowsk1M/task2/blob/bc17b7ddc46f46fff175aed55d68e11bb48166cc/deployment.key#L1

Finding: "private_key": "-----BEGIN PRIVATE KEY-----\n\u0000R0/1A5LiQHjuR5SASDASDAiSMNe0Yqna2R+HEalBoyISASDASD1Tgkj\n4CC02Uux+...\n",
Secret: -----BEGIN PRIVATE KEY-----\n\u0000R0/1A5LiQHjuR5SASDASDAiSMNe0Yqna2R+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/Ma1kowsk1M/task2/blob/bc17b7ddc46f46fff175aed55d68e11bb48166cc/awscredentials.json#L5
```

bc17b7d

task2 / deployment.key

siewer

init cloud ng

Code

Blame

9 lines (9 loc) · 492 Bytes

1

-----BEGIN RSA PRIVATE KEY-----

2

MIIBOgIBAAJBAKj34GkxFhD90vcNLYLInFEX6Ppy1tPf9Cnzj4p4WGeKLs1Pt8Qu

3

KUpRKfFLfRYC9AIKjbJTWit+CqvjWYzvQwECAwEAAQJAIJLixBy2qpFoS4DSmoEm

4

o3qGy0t6z09AIJtH+50eRV1be+M4cDYJKffGzDa88vQENZiRm0GRq6a+HPGQMd2k

5

TQIhAKMSvzIBnni7ot/OSie2TmJLY4SwTQAevXysE2RbFDYdAiEBCUEaRQnMnbp7

6

9mxDXDf6AU0cN/RPBjb9qSHDcWZHGzUCIG2Es59z8ugGrDY+pxLQnwfotadxd+Uy

7

v/Ow5T0q5gIJAiEAyS4RaI9YG8EWx/2w0T67ZUVAw8eOMB6BIUg0Xcu+3okCIB0s

8

/50iPgoTdSy7bcF9IGpSE8ZgGKzgYQVZeN97YE00

9

-----END RSA PRIVATE KEY-----

de9d7b8

task2 / deployment2.key

siewer

init

Code

Blame

9 lines (9 loc) · 492 Bytes

1

-----BEGIN RSA PRIVATE KEY-----

2

MIIBOgIBAAJBAKj34GkxFhD90vcNLYLInFEX6Ppy1tPf9Cnzj4p4WGeKLs1Pt8Qu

3

KUpRKfFLfRYC9AIKjbJTWit+CqvjWYzvQwECAwEAAQJAIJLixBy2qpFoS4DSmoEm

4

o3qGy0t6z09AIJtH+50eRV1be+M4cDYJKffGzDa88vQENZiRm0GRq6a+HPGQMd2k

5

TQIhAKMSvzIBnni7ot/OSie2TmJLY4SwTQAevXysE2RbFDYdAiEBCUEaRQnMnbp7

6

9mxDXDf6AU0cN/RPBjb9qSHDcWZHGzUCIG2Es59z8ugGrDY+pxLQnwfotadxd+Uy

7

v/Ow5T0q5gIJAiEAyS4RaI9YG8EWx/2w0T67ZUVAw8eOMB6BIUg0Xcu+3okCIB0s

8

/50iPgoTdSy7bcF9IGpSE8ZgGKzgYQVZeN97YE00

9

-----END RSA PRIVATE KEY-----

siewer

init cloud ng

Code

Blame

7 lines (7 loc) · 1.51 KB

1

{

2

"type": "service_account",

3

"project_id": "test-project",

4

"private_key_id": "002ac3c1623rdewc7bb13f6b10e6",

5

"private_key": "-----BEGIN PRIVATE KEY-----\nIRsGbrO/1ASLIQHjR5SASDASDA1SMNeOYqna2RHEa1BoyISASDASD1Tgkj\n4CC02Uux+nASDASDRrahMeEp1aebIS52Ax4kASDASDADSak01Ny\nnkCLMVQnyASD",

6

"client_email": "app@test-project.iam.gserviceaccount.com"

7

}

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)"`

```
PS C:\Programowanie\TBO\task2> 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] Checking for updates
[WARN] An NVD API Key was not provided - it is highly recommended to use an NVD API key as the update can take a VERY long time without an API Key
[WARN] Retrying request /rest/json/cves/2.0?resultsPerPage=2000&startIndex=0 : 2nd time
[WARN] Retrying request /rest/json/cves/2.0?resultsPerPage=2000&startIndex=0 : 3rd time
[WARN] Retrying request /rest/json/cves/2.0?resultsPerPage=2000&startIndex=0 : 4th time
[WARN] Retrying request /rest/json/cves/2.0?resultsPerPage=2000&startIndex=0 : 5th time
[WARN] Retrying request /rest/json/cves/2.0?resultsPerPage=2000&startIndex=0 : 6th time
[WARN] Retrying request /rest/json/cves/2.0?resultsPerPage=2000&startIndex=0 : 7th time
[WARN] Retrying request /rest/json/cves/2.0?resultsPerPage=2000&startIndex=0 : 8th time
[WARN] Retrying request /rest/json/cves/2.0?resultsPerPage=2000&startIndex=0 : 9th time
[WARN] Retrying request /rest/json/cves/2.0?resultsPerPage=2000&startIndex=0 : 10th time
[WARN] Retrying request /rest/json/cves/2.0?resultsPerPage=2000&startIndex=0 : 11th time
[WARN] Retrying request /rest/json/cves/2.0?resultsPerPage=2000&startIndex=0 : 12th time
[WARN] Retrying request /rest/json/cves/2.0?resultsPerPage=2000&startIndex=0 : 13th time
[WARN] Retrying request /rest/json/cves/2.0?resultsPerPage=2000&startIndex=0 : 14th time
[WARN] NVD API request failures are occurring; retrying request for the 15th time
[WARN] NVD API request failures are occurring; retrying request for the 16th time
[WARN] NVD API request failures are occurring; retrying request for the 17th time
[WARN] NVD API request failures are occurring; retrying request for the 18th time
[WARN] NVD API request failures are occurring; retrying request for the 19th time
[WARN] NVD API request failures are occurring; retrying request for the 20th time
[WARN] NVD API request failures are occurring; retrying request for the 21st time
[WARN] NVD API request failures are occurring; retrying request for the 22nd time
[WARN] NVD API request failures are occurring; retrying request for the 23rd time
[WARN] NVD API request failures are occurring; retrying request for the 24th time
[WARN] NVD API request failures are occurring; retrying request for the 25th time
[WARN] NVD API request failures are occurring; retrying request for the 26th time

[WARN] NVD API request failures are occurring; retrying request for the 31st time
[INFO] NVD API has 320,459 records in this update
[INFO] Downloaded 10,000/320,459 (3%)
[INFO] Downloaded 20,000/320,459 (6%)
[INFO] Downloaded 30,000/320,459 (9%)
[INFO] Downloaded 40,000/320,459 (12%)
[INFO] Downloaded 50,000/320,459 (16%)
[INFO] Downloaded 60,000/320,459 (19%)
[INFO] Downloaded 70,000/320,459 (22%)
[INFO] Downloaded 80,000/320,459 (25%)
[INFO] Downloaded 90,000/320,461 (28%)
[INFO] Downloaded 100,000/320,461 (31%)
[INFO] Downloaded 110,000/320,461 (34%)
[INFO] Downloaded 120,000/320,461 (37%)
[INFO] Downloaded 130,000/320,461 (41%)
[INFO] Downloaded 140,000/320,461 (44%)

[INFO] Downloaded 320,000/320,461 (100%)
[INFO] Downloaded 320,461/320,461 (100%)
[INFO] Completed processing batch 1/161 (1%) in 5,490ms
[INFO] Completed processing batch 2/161 (1%) in 3,865ms
[INFO] Completed processing batch 3/161 (2%) in 2,990ms
[INFO] Completed processing batch 4/161 (2%) in 2,867ms
[INFO] Completed processing batch 5/161 (3%) in 2,529ms
[INFO] Completed processing batch 6/161 (4%) in 2,904ms
[INFO] Completed processing batch 7/161 (4%) in 1,886ms
[INFO] Completed processing batch 8/161 (5%) in 2,149ms
[INFO] Completed processing batch 9/161 (6%) in 2,418ms
[INFO] Completed processing batch 10/161 (6%) in 2,007ms
[INFO] Completed processing batch 11/161 (7%) in 1,771ms
[INFO] Completed processing batch 12/161 (7%) in 1,927ms
[INFO] Completed processing batch 13/161 (8%) in 2,218ms
[INFO] Completed processing batch 14/161 (9%) in 2,563ms
[INFO] Completed processing batch 15/161 (9%) in 2,433ms
[INFO] Completed processing batch 16/161 (10%) in 3,282ms
[INFO] Completed processing batch 17/161 (11%) in 2,521ms
[INFO] Completed processing batch 18/161 (11%) in 2,380ms
[INFO] Completed processing batch 19/161 (12%) in 2,910ms
[INFO] Completed processing batch 20/161 (12%) in 2,821ms
[INFO] Completed processing batch 21/161 (13%) in 2,976ms
[INFO] Completed processing batch 22/161 (14%) in 2,626ms
[INFO] Completed processing batch 23/161 (14%) in 3,684ms
```

```
[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 in 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/-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 is an open source tool performing a best effort analysis of 3rd party dependencies; false positives and false negatives may exist in the analysis performed by the tool. Use of the tool and the reporting provided constitutes acceptance.

[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

getobject:0.1.0

File Path: /sro/sro/main/resources/static/vendors/jquery-mask/package-lock.json?getobject

Referenced In Project/Scope: package-lock.json: transitive

Evidence

Identifiers

- pkg:npm/getobject@0.1.0 (Confidence: Highest)

Published Vulnerabilities

[GHSA-957j-59c2-j692 \(NPM\)](#)

Prototype pollution vulnerability in 'getobject' version 0.1.0 allows an attacker to cause a denial of service and may lead to remote code execution.

CWE-1321 Improperly Controlled Modification of Object Prototype Attributes ("Prototype Pollution")

CVSSv3:

- Base Score: CRITICAL (9.800000190734883)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Unscored:

- Severity: critical

References:

- NPM Advisory reference: - <https://github.com/advisories/GHSA-957j-59c2-j692>
- NPM Advisory reference: - <https://github.com/cowboy/node-getobject/blob/aba04a8e1d6180eb30eff09990c3a43886ba8937/lib/getobject.js#L48>
- NPM Advisory reference: - <https://nvd.nist.gov/vuln/detail/CVE-2020-28282>
- NPM Advisory reference: - <https://www.whitesourcesoftware.com/vulnerability-database/CVE-2020-28282>

Vulnerable Software & Versions (NPM):

- ope:2.3.a:*getobject\<1.0.0:*****

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.