report

Tuesday, January 9, 2024
12:55 PM

Frontend:

SCA

Software Composition Analysis (SCA) provides visibility into the open source components and libraries being incorporated into the software that development teams create.

retireJS

There are lots of JavaScript libraries for use on the Web and in Node.JS apps. The availability of these libraries greatly simplifies development, but also increases the security risks. Because of rampant abuse of these libraries, attackers are concentrating on these libraries. Realizing the need for awareness, OWASP has included “Using Components with Known Vulnerabilities” as part of the OWASP Top 10 list.

RetireJS helps you in finding the insecure Javascript libraries in your code.

Embed retireJS into Gitlab CI/CD:

```
oast-RetireJS:
  stage: build
  image: node:alpine3.10
  script:
    - npm install
    - npm install -g retire # Install retirejs npm package.
    - retire --outputformat json --outputpath retirejs-report.json --severity high
    - cat retirejs-report.json
  artifacts:
    paths: [retirejs-report.json]
    when: always
```

```
$ cat retirejs-report.json
{"version":"4.3.4","start":"2024-01-09T20:00:43.360Z","data":[],"messages":[],"errors":[],"time":40.595}
```

osv-scanner

google/osv-scanner

Embed osv-scanner into Gitlab CI/CD:

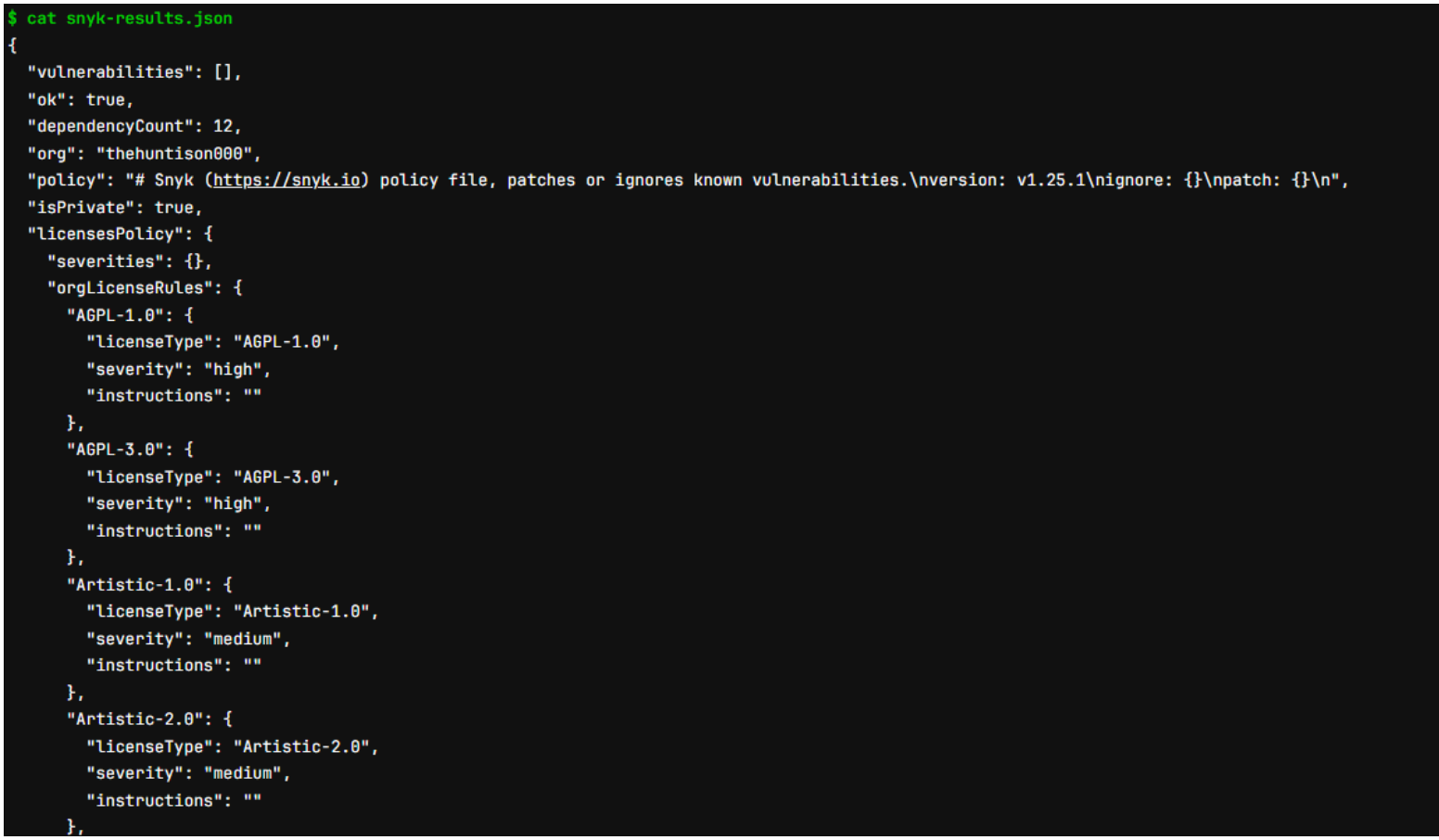
```
osv-scanner:
  stage: pre-build
  image: golang:1.21.1-alpine3.18
  before_script:
    - apk add npm
    - npm install
  script:
    - go install github.com/google/osv-scanner/cmd/osv-scanner@v1
    - osv-scanner .
```

```
$ osv-scanner .
Scanning dir .
Scanning /builds/mouad.tigmouti00/devsecops-frontend/ at commit 4d7b8e588e53e4abae976c8c788ce813a0baace3
Scanned /builds/mouad.tigmouti00/devsecops-frontend/package-lock.json file and found 847 packages
+-----------------------------------+------+-----------+-----------------+---------+-------------------+
| OSV URL                           | CVSS | ECOSYSTEM | PACKAGE         | VERSION | SOURCE            |
+-----------------------------------+------+-----------+-----------------+---------+-------------------+
| https://osv.dev/GHSA-67hx-6x53-jw92 | 9.3  | npm       | @babel/traverse | 7.21.5  | package-lock.json |
| https://osv.dev/GHSA-jchw-25xp-jwwc | 6.1  | npm       | follow-redirects | 1.15.2 | package-lock.json |
| https://osv.dev/GHSA-7fh5-64p2-3v2j | 5.3  | npm       | postcss         | 8.4.23  | package-lock.json |
| https://osv.dev/GHSA-c2qf-rxjj-qqgw | 5.3  | npm       | semver          | 5.7.1   | package-lock.json |
| https://osv.dev/GHSA-c2qf-rxjj-qqgw | 5.3  | npm       | semver          | 6.3.0   | package-lock.json |
| https://osv.dev/GHSA-c2qf-rxjj-qqgw | 5.3  | npm       | semver          | 7.4.0   | package-lock.json |
| https://osv.dev/GHSA-353f-5xf4-qw67 | 7.5  | npm       | vite            | 4.3.1   | package-lock.json |
+-----------------------------------+------+-----------+-----------------+---------+-------------------+
```

Snyk

Embed Snyk into Gitlab CI/CD:

```
oast-snyk:
  stage: build
  image: node:alpine3.10
  before_script:
    - wget -O snyk https://github.com/snyk/cli/releases/download/v1.1156.0/snyk-alpine
    - chmod +x snyk
    - mv snyk /usr/local/bin/
  script:
    - npm install
    - snyk auth 35589080-01a0-4492-af3d-82ee5f1140d0
    - snyk test --json > snyk-results.json
    - cat snyk-results.json
  artifacts:
    paths: [snyk-results.json]
    when: always
    expire_in: one week
```



```
$ cat snyk-results.json
{
  "vulnerabilities": [],
  "ok": true,
  "dependencyCount": 12,
  "org": "thehuntison000",
  "policy": "# Snyk (https://snyk.io) policy file, patches or ignores known vulnerabilities.\nversion: v1.25.1\nignore: {}\npatch: {}\n",
  "isPrivate": true,
  "licensesPolicy": {
    "severities": {},
    "orgLicenseRules": {
      "AGPL-1.0": {
        "licenseType": "AGPL-1.0",
        "severity": "high",
        "instructions": ""
      },
      "AGPL-3.0": {
        "licenseType": "AGPL-3.0",
        "severity": "high",
        "instructions": ""
      },
      "Artistic-1.0": {
        "licenseType": "Artistic-1.0",
        "severity": "medium",
        "instructions": ""
      },
      "Artistic-2.0": {
        "licenseType": "Artistic-2.0",
        "severity": "medium",
        "instructions": ""
      },
```


{
 "vulnerabilities": [],
 "ok": true,
 "dependencyCount": 12,
 "org": "thehuntison000",
 "policy": "# Snyk (https://snyk.io) policy file, patches or ignores known vulnerabilities.\nversion: v1.25.1\nignore: {}\npatch: {}\n",
 "isPrivate": true,
 "licensesPolicy": {
  "severities": {},
  "orgLicenseRules": {
   "AGPL-1.0": {
    "licenseType": "AGPL-1.0",
    "severity": "high",
    "instructions": ""
   },
   "AGPL-3.0": {
    "licenseType": "AGPL-3.0",
    "severity": "high",
    "instructions": ""
   },
   "Artistic-1.0": {
    "licenseType": "Artistic-1.0",
    "severity": "medium",
    "instructions": ""

```
},
"Artistic-2.0": {
  "licenseType": "Artistic-2.0",
  "severity": "medium",
  "instructions": ""
},
"CDDL-1.0": {
  "licenseType": "CDDL-1.0",
  "severity": "medium",
  "instructions": ""
},
"CPOL-1.02": {
  "licenseType": "CPOL-1.02",
  "severity": "high",
  "instructions": ""
},
"EPL-1.0": {
  "licenseType": "EPL-1.0",
  "severity": "medium",
  "instructions": ""
},
"GPL-2.0": {
  "licenseType": "GPL-2.0",
  "severity": "high",
  "instructions": ""
},
"GPL-3.0": {
  "licenseType": "GPL-3.0",
  "severity": "high",
  "instructions": ""
},
"LGPL-2.0": {
  "licenseType": "LGPL-2.0",
  "severity": "medium",
  "instructions": ""
},
"LGPL-2.1": {
  "licenseType": "LGPL-2.1",
  "severity": "medium",
  "instructions": ""
},
"LGPL-3.0": {
  "licenseType": "LGPL-3.0",
  "severity": "medium",
  "instructions": ""
},
"MPL-1.1": {
  "licenseType": "MPL-1.1",
  "severity": "medium",
  "instructions": ""
},
```

```
    "MPL-2.0": {
      "licenseType": "MPL-2.0",
      "severity": "medium",
      "instructions": ""
    },
    "MS-RL": {
      "licenseType": "MS-RL",
      "severity": "medium",
      "instructions": ""
    },
    "SimPL-2.0": {
      "licenseType": "SimPL-2.0",
      "severity": "high",
      "instructions": ""
    }
   }
  },
  "packageManager": "npm",
  "ignoreSettings": {
   "adminOnly": false,
   "reasonRequired": false,
   "disregardFilesystemIgnores": false
  },
  "summary": "No known vulnerabilities",
  "filesystemPolicy": false,
  "uniqueCount": 0,
  "projectName": "angular-16-crud",
  "displayTargetFile": "package-lock.json",
  "hasUnknownVersions": false,
  "path": "/builds/mouad.tigmouti00/devsecops-frontend"
}
```


SAST

Static application security testing is a type of software test used for inspecting and analyzing code to identify security vulnerabilities. Software security tools — such as static code analyzers — scan your code as it’s being written to identify potential weaknesses, errors and bugs.

TruffleHog

Embed TruffleHog into Gitlab CI/CD:

```
git-secrets:
  stage: build
  script:
    - docker run -v $(pwd):/src --rm hysnsec/trufflehog filesystem --directory=/src --json | tee trufflehog-output.json
    - cat trufflehog-output.json
  artifacts:
    paths: [trufflehog-output.json]
    when: always
    expire_in: one week
```

```
$ docker run -v $(pwd):/src --rm hysnsec/trufflehog filesystem --directory=/src --json | tee trufflehog-output.json
{"level":"info-0","ts":"2024-01-09T20:06:49Z","logger":"trufflehog","msg":"--directory flag is deprecated, please pass directories as arguments"}
{"level":"info-0","ts":"2024-01-09T20:06:49Z","logger":"trufflehog","msg":"running source","source_manager_worker_id":"XZwq5","with_units":true}
{"level":"info-0","ts":"2024-01-09T20:06:49Z","logger":"trufflehog","msg":"finished scanning","chunks":0,"bytes":0,"verified_secrets":0,"unverified_secrets":0,"scan_duration":"40.182481ms"}
```

Bandit

The Bandit is a tool designed to find common security issues in Python code.

To do this Bandit, processes each file, builds an AST, and runs appropriate plugins against the AST nodes. Once Bandit has finished scanning all the files it generates a report.

Embed Bandit into Gitlab CI/CD:

```
sast-bandit:
  stage: build
  before_script:
    - apk update
    - apk add --no-cache python3 py3-pip
  script:
    - pip3 install bandit==1.7.4 --break-system-packages
    - pip3 install requests --break-system-packages
    - bandit -r . -f json | tee bandit-output.json
    - cat bandit-output.json
    - whoami
    - hostname
  after_script:
    - python3 upload-results.py --host 0.0.0.0:8080 --api_key
3d49f5330984a68a20f4dc75a59bc313ddc3509d --engagement_id 1 --product_id 1 --lead_id 1 --
environment "Production" --result_file bandit-output.json --scanner "Bandit Scan"
  artifacts:
    paths: [bandit-output.json]
    when: always
```

```
$ bandit -r . -f json | tee bandit-output.json
[main]  INFO    profile include tests: None
[main]  INFO    profile exclude tests: None
[main]  INFO    cli include tests: None
[main]  INFO    cli exclude tests: None
{
  "errors": [],
  "generated_at": "2024-01-09T20:08:20Z",
  "metrics": {
    "_totals": {
      "CONFIDENCE.HIGH": 0,
      "CONFIDENCE.LOW": 0,
      "CONFIDENCE.MEDIUM": 0,
      "CONFIDENCE.UNDEFINED": 0,
      "SEVERITY.HIGH": 0,
      "SEVERITY.LOW": 0,
      "SEVERITY.MEDIUM": 0,
      "SEVERITY.UNDEFINED": 0,
      "loc": 0,
      "nosec": 0,
      "skipped_tests": 0
    }
  },
  "results": []
```

DAST

Dynamic Application Security Testing (DAST) is an application security testing methodology in which the application is tested at runtime to discover security vulnerabiltiies. DAST tools don't have access to the application and API's source code, so they detect vulnerabilities by performing actual attacks, similar to a real hacker.

Nikto

Nikto is a web server assessment tool. It's designed to find various default and insecure files, configurations, and programs on any type of web server.

Embed Nikto into Gitlab CI/CD:

```
nikto:
  stage: test
  script:
    - docker pull hysnsec/nikto
    - docker run --rm -v $(pwd):/tmp hysnsec/nikto -h http://192.168.75.132:8080 -o nikto-output.xml
    - cat nikto-output.xml
  artifacts:
    paths: [nikto-output.xml]
    when: always
```

```
$ docker run --rm -v $(pwd):/tmp hysnsec/nikto -h http://192.168.75.132:8081
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.75.132
+ Target Hostname:    192.168.75.132
+ Target Port:        8081
+ Start Time:         2024-01-09 20:55:42 (GMT0)
---------------------------------------------------------------------------
+ Server: No banner retrieved
+ /: Retrieved x-powered-by header: Express.
+ /: Retrieved access-control-allow-origin header: *.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME typ
e. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ 8102 requests: 0 error(s) and 4 item(s) reported on remote host
+ End Time:           2024-01-09 20:58:10 (GMT0) (148 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Nmap

Nmap (“Network Mapper”) is a free and open source (license) utility for network discovery and security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime.

Embed Nmap into Gitlab CI/CD:

```
nmap:
  stage: test
  script:
    - docker pull hysnsec/nmap
    - docker run --rm -v $(pwd):/tmp hysnsec/nmap -p 8080 192.168.75.132 -oX nmap-output.xml
    - nmap-output.xml
  artifacts:
    paths: [nmap-output.xml]
    when: always
```

```
$ docker run --rm -v $(pwd):/tmp hysnsec/nmap -sSVC -A -p 8081 192.168.75.132
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-09 20:59 UTC
Nmap scan report for 192.168.75.132
Host is up (0.00023s latency).
PORT     STATE SERVICE VERSION
8081/tcp open  http    Node.js (Express middleware)
|_http-title: ICCN-Project
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
Network Distance: 1 hop
TRACEROUTE (using port 8081/tcp)
HOP RTT     ADDRESS
1   0.21 ms 192.168.75.132
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.27 seconds
```

Zap

ZAP is an open-source web application security scanner to perform security testing (Dynamic Testing) on web applications. OWASP ZAP is the flagship OWASP project used

extensively by penetration testers. ZAP can also run in a daemon mode for hands-off scans for CI/CD pipeline. ZAP provides extensive API (SDK) and a REST API to help users create custom scripts.

Embed ZAP (Zed Atttack Proxy) into Gitlab CI/CD:

```
zap-baseline:
  stage: test
  script:
    - docker run --user $(id -u):$(id -g) -w /zap -v $(pwd):/zap/wrk:rw --rm
softwaresecurityproject/zap-stable:2.13.0 zap-baseline.py -t http://192.168.75.132:8080 -J zap-
output.json
    - cat zap-output.json
  artifacts:
    paths: [zap-output.json]
    when: always
```

```
$ zap-full-scan.py -t http://192.168.75.132:8081 -r report.html
Total of 15 URLs
PASS: Vulnerable JS Library (Powered by Retire.js) [10003]
PASS: In Page Banner Information Leak [10009]
PASS: Cookie No HttpOnly Flag [10010]
PASS: Cookie Without Secure Flag [10011]
PASS: Re-examine Cache-control Directives [10015]
PASS: Cross-Domain JavaScript Source File Inclusion [10017]
PASS: Content-Type Header Missing [10019]
PASS: Information Disclosure - Debug Error Messages [10023]
PASS: Information Disclosure - Sensitive Information in URL [10024]
PASS: Information Disclosure - Sensitive Information in HTTP Referrer Header [10025]
PASS: HTTP Parameter Override [10026]
PASS: Information Disclosure - Suspicious Comments [10027]
```

$ zap-full-scan.py -t http://192.168.75.132:8081 -r report.html
Total of 15 URLs
PASS: Vulnerable JS Library (Powered by Retire.js) [10003]
PASS: In Page Banner Information Leak [10009]
PASS: Cookie No HttpOnly Flag [10010]

PASS: Cookie Without Secure Flag [10011]
PASS: Re-examine Cache-control Directives [10015]
PASS: Cross-Domain JavaScript Source File Inclusion [10017]
PASS: Content-Type Header Missing [10019]
PASS: Information Disclosure - Debug Error Messages [10023]
PASS: Information Disclosure - Sensitive Information in URL [10024]
PASS: Information Disclosure - Sensitive Information in HTTP Referrer Header [10025]
PASS: HTTP Parameter Override [10026]
PASS: Information Disclosure - Suspicious Comments [10027]
PASS: Open Redirect [10028]
PASS: Cookie Poisoning [10029]
PASS: User Controllable Charset [10030]
PASS: User Controllable HTML Element Attribute (Potential XSS) [10031]
PASS: Viewstate [10032]
PASS: Directory Browsing [10033]
PASS: Heartbleed OpenSSL Vulnerability (Indicative) [10034]
PASS: Strict-Transport-Security Header [10035]
PASS: HTTP Server Response Header [10036]
PASS: X-Backend-Server Header Information Leak [10039]
PASS: Secure Pages Include Mixed Content [10040]
PASS: HTTP to HTTPS Insecure Transition in Form Post [10041]
PASS: HTTPS to HTTP Insecure Transition in Form Post [10042]
PASS: User Controllable JavaScript Event (XSS) [10043]
PASS: Big Redirect Detected (Potential Sensitive Information Leak) [10044]
PASS: Source Code Disclosure - /WEB-INF folder [10045]
PASS: HTTPS Content Available via HTTP [10047]
PASS: Remote Code Execution - Shell Shock [10048]
PASS: Content Cacheability [10049]
PASS: Retrieved from Cache [10050]
PASS: Relative Path Confusion [10051]
PASS: X-ChromeLogger-Data (XCOLD) Header Information Leak [10052]
PASS: Cookie without SameSite Attribute [10054]
PASS: X-Debug-Token Information Leak [10056]
PASS: Username Hash Found [10057]
PASS: GET for POST [10058]
PASS: X-AspNet-Version Response Header [10061]
PASS: PII Disclosure [10062]
PASS: Backup File Disclosure [10095]
PASS: Timestamp Disclosure [10096]
PASS: Hash Disclosure [10097]
PASS: Source Code Disclosure [10099]
PASS: User Agent Fuzzer [10104]
PASS: Weak Authentication Method [10105]
PASS: HTTP Only Site [10106]
PASS: Httpoxy - Proxy Header Misuse [10107]
PASS: Reverse Tabnabbing [10108]
PASS: Modern Web Application [10109]
PASS: Authentication Request Identified [10111]
PASS: Session Management Response Identified [10112]
PASS: Verification Request Identified [10113]
PASS: Absence of Anti-CSRF Tokens [10202]

PASS: Private IP Disclosure [2]
PASS: Anti-CSRF Tokens Check [20012]
PASS: HTTP Parameter Pollution [20014]
PASS: Heartbleed OpenSSL Vulnerability [20015]
PASS: Cross-Domain Misconfiguration [20016]
PASS: Source Code Disclosure - CVE-2012-1823 [20017]
PASS: Remote Code Execution - CVE-2012-1823 [20018]
PASS: External Redirect [20019]
PASS: Session ID in URL Rewrite [3]
PASS: Buffer Overflow [30001]
PASS: Format String Error [30002]
PASS: Integer Overflow Error [30003]
PASS: CRLF Injection [40003]
PASS: Parameter Tampering [40008]
PASS: Server Side Include [40009]
PASS: Cross Site Scripting (Reflected) [40012]
PASS: Session Fixation [40013]
PASS: Cross Site Scripting (Persistent) [40014]
PASS: Cross Site Scripting (Persistent) - Prime [40016]
PASS: Cross Site Scripting (Persistent) - Spider [40017]
PASS: SQL Injection [40018]
PASS: SQL Injection - MySQL [40019]
PASS: SQL Injection - Hypersonic SQL [40020]
PASS: SQL Injection - Oracle [40021]
PASS: SQL Injection - PostgreSQL [40022]
PASS: Possible Username Enumeration [40023]
PASS: SQL Injection - SQLite [40024]
PASS: Proxy Disclosure [40025]
PASS: Cross Site Scripting (DOM Based) [40026]
PASS: SQL Injection - MsSQL [40027]
PASS: ELMAH Information Leak [40028]
PASS: Trace.axd Information Leak [40029]
PASS: Out of Band XSS [40031]
PASS: .htaccess Information Leak [40032]
PASS: .env Information Leak [40034]
PASS: Hidden File Finder [40035]
PASS: Bypassing 403 [40038]
PASS: Spring Actuator Information Leak [40042]
PASS: Log4Shell [40043]
PASS: Exponential Entity Expansion (Billion Laughs Attack) [40044]
PASS: Spring4Shell [40045]
PASS: Server Side Request Forgery [40046]
PASS: Text4shell (CVE-2022-42889) [40047]
PASS: Source Code Disclosure - Git [41]
PASS: Source Code Disclosure - SVN [42]
PASS: Source Code Disclosure - File Inclusion [43]
PASS: Script Active Scan Rules [50000]
PASS: Script Passive Scan Rules [50001]
PASS: Path Traversal [6]
PASS: Remote File Inclusion [7]
PASS: Insecure JSF ViewState [90001]

PASS: Java Serialization Object [90002]
PASS: Sub Resource Integrity Attribute Missing [90003]
PASS: Insufficient Site Isolation Against Spectre Vulnerability [90004]
PASS: Charset Mismatch [90011]
PASS: XSLT Injection [90017]
PASS: Server Side Code Injection [90019]
PASS: Remote OS Command Injection [90020]
PASS: XPath Injection [90021]
PASS: Application Error Disclosure [90022]
PASS: XML External Entity Attack [90023]
PASS: Generic Padding Oracle [90024]
PASS: Expression Language Injection [90025]
PASS: SOAP Action Spoofing [90026]
PASS: Cookie Slack Detector [90027]
PASS: Insecure HTTP Method [90028]
PASS: SOAP XML Injection [90029]
PASS: WSDL File Detection [90030]
PASS: Loosely Scoped Cookie [90033]
PASS: Server Side Template Injection [90035]
PASS: Server Side Template Injection (Blind) [90036]
WARN-NEW: Directory Browsing [0] x 1
    http://192.168.75.132:8081/vendor.js/ (200 OK)
WARN-NEW: Missing Anti-clickjacking Header [10020] x 2
    http://192.168.75.132:8081/ (200 OK)
    http://192.168.75.132:8081 (200 OK)
WARN-NEW: X-Content-Type-Options Header Missing [10021] x 9
    http://192.168.75.132:8081/ (200 OK)
    http://192.168.75.132:8081 (200 OK)
    http://192.168.75.132:8081/favicon.ico (200 OK)
    http://192.168.75.132:8081/runtime.js (200 OK)
    http://192.168.75.132:8081/main.js (200 OK)
WARN-NEW: Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) [10037] x 11
    http://192.168.75.132:8081/ (200 OK)
    http://192.168.75.132:8081/robots.txt (404 Not Found)
    http://192.168.75.132:8081/sitemap.xml (404 Not Found)
    http://192.168.75.132:8081 (200 OK)
    http://192.168.75.132:8081/favicon.ico (200 OK)
WARN-NEW: Content Security Policy (CSP) Header Not Set [10038] x 2
    http://192.168.75.132:8081/ (200 OK)
    http://192.168.75.132:8081 (200 OK)
WARN-NEW: CSP: Wildcard Directive [10055] x 2
    http://192.168.75.132:8081/sitemap.xml (404 Not Found)
    http://192.168.75.132:8081/robots.txt (404 Not Found)
WARN-NEW: Permissions Policy Header Not Set [10063] x 9
    http://192.168.75.132:8081/ (200 OK)
    http://192.168.75.132:8081/sitemap.xml (404 Not Found)
    http://192.168.75.132:8081/robots.txt (404 Not Found)
    http://192.168.75.132:8081 (200 OK)
    http://192.168.75.132:8081/runtime.js (200 OK)
WARN-NEW: Cross-Domain Misconfiguration [10098] x 11

http://192.168.75.132:8081/ (200 OK)
http://192.168.75.132:8081/sitemap.xml (404 Not Found)
http://192.168.75.132:8081/robots.txt (404 Not Found)
http://192.168.75.132:8081 (200 OK)
http://192.168.75.132:8081/runtime.js (200 OK)
WARN-NEW: Dangerous JS Functions [10110] x 1
http://192.168.75.132:8081/vendor.js (200 OK)
WARN-NEW: CORS Misconfiguration [40040] x 11
http://192.168.75.132:8081 (200 OK)
http://192.168.75.132:8081/ (200 OK)
http://192.168.75.132:8081/main.js (200 OK)
http://192.168.75.132:8081/favicon.ico (200 OK)
http://192.168.75.132:8081/polyfills.js (200 OK)
WARN-NEW: Cloud Metadata Potentially Exposed [90034] x 1
http://192.168.75.132:8081/latest/meta-data/ (200 OK)
FAIL-NEW: 0 FAIL-INPROG: 0 WARN-NEW: 11 WARN-INPROG: 0 INFO: 0 IGNORE: 0 PASS: 125

Container Security

Container Scanning is often considered part of Software Composition Analysis (SCA). SCA can contain aspects of inspecting the items your code uses. These items typically include application and system dependencies that are almost always imported from external sources, rather than sourced from items you wrote yourself.

```
#Container Scanning
include:
  - template: Security/Container-Scanning.gitlab-ci.yml
container_scanning:
  variables:
    CS_IMAGE: mouadtigmouti/devsecops-backend
```

```
$ gtcs scan
[INFO] [2024-01-09 20:49:14 +0000] [container-scanning]  >  Remediation is disabled; /builds/mouad.tigmouti00/devsecops-frontend/Dockerfile cannot be fo
d. Have you set `GIT_STRATEGY` and
`CS_DOCKERFILE_PATH`?
See https://docs.gitlab.com/ee/user/application_security/container_scanning/#solutions-for-vulnerabilities-auto-remediation
[INFO] [2024-01-09 20:49:28 +0000] [container-scanning]  >  Scanning container from registry [MASKED]/devsecops-backend for vulnerabilities with severit
evel UNKNOWN or higher, with gcs 6.6.2 and Trivy Version: 0.48.1, advisories updated at 2024-01-09T12:13:28+00:00
```

STATUS	CVE SEVERITY	PACKAGE NAME	PACKAGE VERSION	CVE DESCRIPTION
Unapproved	Low	apt	2.2.4	It was found that apt-key in apt, all versions, do not correctly validate gpg keys with the master keyring, leading to a potential man-in-the-middle attack.
Unapproved	High	bash	5.1-2+b3	A flaw was found in the bash package, where a heap-buffer overflow can occur in valid parameter_transform. This issue may lead to memory problems.
Unapproved	Low	bash	5.1-2+b3	TEMP-0841856-B18BAF
Unapproved	Low	bsdutils	1:2.36.1-8+deb11u1	A flaw was found in the util-linux chfn and chsh utilities when compiled with Readline support. The Readline library uses an "INPUTRC" environment variable to get a path to the library config file. When the library cannot parse the specified file, it prints an error message containing data from the file. This flaw allows an unprivileged user to read root-owned files, potentially leading to privilege escalation. This flaw affects util-linux versions prior to 2.37.4.
Unapproved	Low	coreutils	8.32-4+b1	chroot in GNU coreutils, when used with --userspec, allows local users to escape to the parent session via a crafted TIOCSTI ioctl call, which pushes characters to the terminal's input buffer.
Unapproved	Low	coreutils	8.32-4+b1	In GNU Coreutils through 8.29, chown-core.c in chown and chgrp does no

Backend:

SCA

Software Composition Analysis (SCA) provides visibility into the open source components and libraries being incorporated into the software that development teams create.

retireJS

Embed retireJS into Gitlab CI/CD:

```
oast-RetireJS:
  stage: build
  image: node:alpine3.10
  script:
    - npm install
    - npm install -g retire # Install retirejs npm package.
    - retire --outputformat json --outputpath retirejs-report.json --severity high
    - cat retirejs-report.json
  artifacts:
    paths: [retirejs-report.json]
    when: always
```

```
$ cat retirejs-report.json
{"version":"4.3.4","start":"2024-01-09T15:31:01.504Z","data":[],"messages":[],"errors":[],"time":0.261}
```

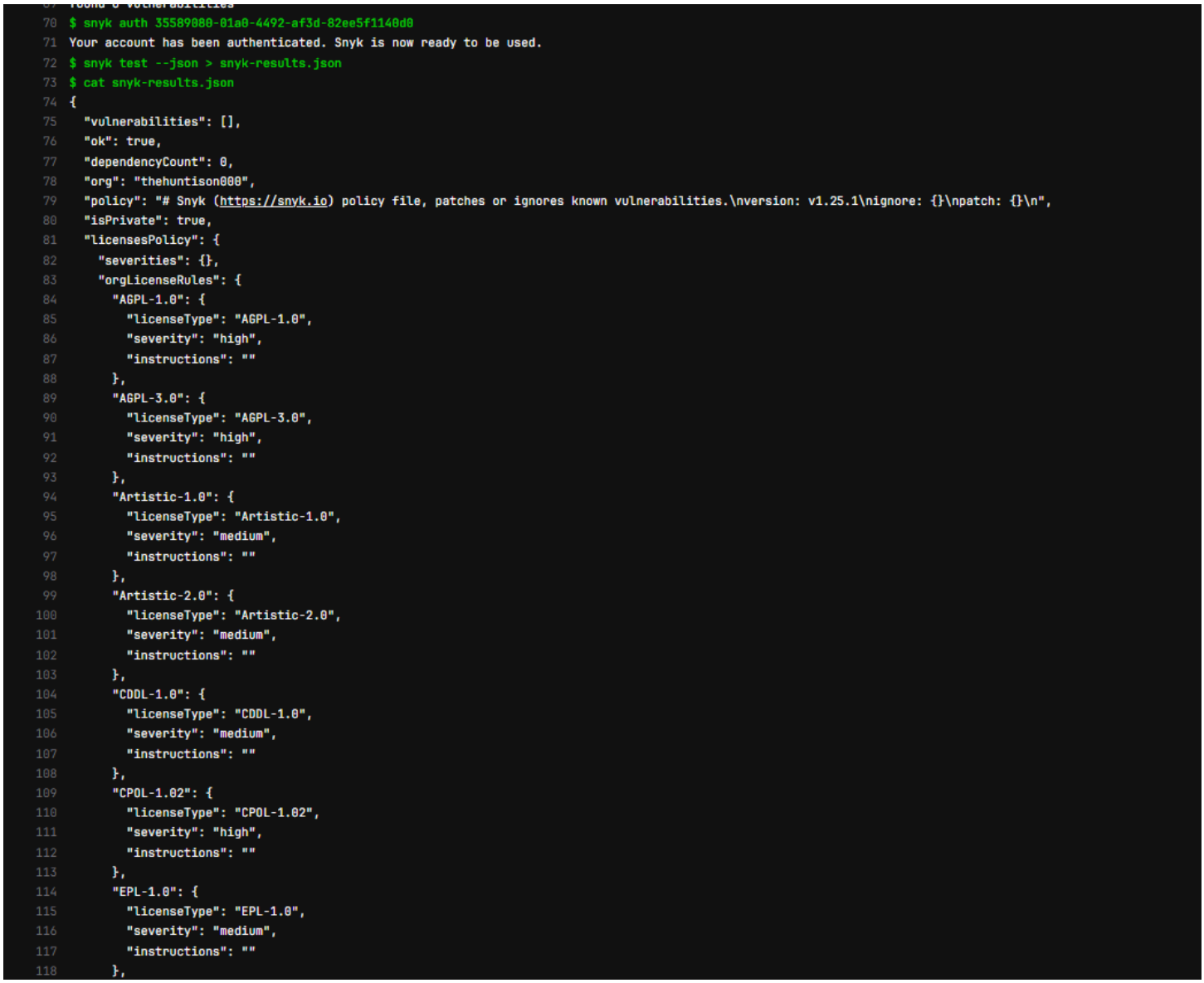
{"version":"4.3.4","start":"2024-01-09T15:31:01.504Z","data":[],"messages":[],"errors":[],"time":0.261}

Snyk

Embed Snyk into Gitlab CI/CD:

```
oast-snyk:
  stage: build
  image: node:alpine3.10
  before_script:
    - wget -O snyk https://github.com/snyk/cli/releases/download/v1.1156.0/snyk-alpine
    - chmod +x snyk
    - mv snyk /usr/local/bin/
  script:
    - npm install
    - snyk auth 35589080-01a0-4492-af3d-82ee5f1140d0
    - snyk test --json > snyk-results.json
    - cat snyk-results.json
  artifacts:
```

paths: [snyk-results.json]
when: always
expire_in: one week



$ cat snyk-results.json
{
"vulnerabilities": [],
"ok": true,
"dependencyCount": 0,
"org": "thehuntison000",
"policy": "# Snyk (https://snyk.io) policy file, patches or ignores known vulnerabilities.\nversion: v1.25.1\nignore: {}\npatch: {}\n",
"isPrivate": true,
"licensesPolicy": {
"severities": {},
"orgLicenseRules": {
"AGPL-1.0": {
"licenseType": "AGPL-1.0",

```
  "severity": "high",
  "instructions": ""
},
"AGPL-3.0": {
  "licenseType": "AGPL-3.0",
  "severity": "high",
  "instructions": ""
},
"Artistic-1.0": {
  "licenseType": "Artistic-1.0",
  "severity": "medium",
  "instructions": ""
},
"Artistic-2.0": {
  "licenseType": "Artistic-2.0",
  "severity": "medium",
  "instructions": ""
},
"CDDL-1.0": {
  "licenseType": "CDDL-1.0",
  "severity": "medium",
  "instructions": ""
},
"CPOL-1.02": {
  "licenseType": "CPOL-1.02",
  "severity": "high",
  "instructions": ""
},
"EPL-1.0": {
  "licenseType": "EPL-1.0",
  "severity": "medium",
  "instructions": ""
},
"GPL-2.0": {
  "licenseType": "GPL-2.0",
  "severity": "high",
  "instructions": ""
},
"GPL-3.0": {
  "licenseType": "GPL-3.0",
  "severity": "high",
  "instructions": ""
},
"LGPL-2.0": {
  "licenseType": "LGPL-2.0",
  "severity": "medium",
  "instructions": ""
},
"LGPL-2.1": {
  "licenseType": "LGPL-2.1",
  "severity": "medium",
```

```
      "instructions": ""
    },
    "LGPL-3.0": {
      "licenseType": "LGPL-3.0",
      "severity": "medium",
      "instructions": ""
    },
    "MPL-1.1": {
      "licenseType": "MPL-1.1",
      "severity": "medium",
      "instructions": ""
    },
    "MPL-2.0": {
      "licenseType": "MPL-2.0",
      "severity": "medium",
      "instructions": ""
    },
    "MS-RL": {
      "licenseType": "MS-RL",
      "severity": "medium",
      "instructions": ""
    },
    "SimPL-2.0": {
      "licenseType": "SimPL-2.0",
      "severity": "high",
      "instructions": ""
    }
   }
  },
  "packageManager": "npm",
  "ignoreSettings": {
    "adminOnly": false,
    "reasonRequired": false,
    "disregardFilesystemIgnores": false
  },
  "summary": "No known vulnerabilities",
  "filesystemPolicy": false,
  "uniqueCount": 0,
  "projectName": "package.json",
  "foundProjectCount": 1,
  "displayTargetFile": "package-lock.json",
  "hasUnknownVersions": false,
  "path": "/builds/mouad.tigmouti00/devsecops-backend"
}
```


SAST

Static application security testing is a type of software test used for inspecting and analyzing code to identify security vulnerabilities. Software security tools — such as static code analyzers — scan your code as it's being written to identify potential weaknesses, errors and bugs.

TruffleHog

Embed TruffleHog into Gitlab CI/CD:

```
git-secrets:
  stage: build
  script:
    - docker run -v $(pwd):/src --rm hysnsec/trufflehog filesystem --directory=/src --json | tee trufflehog-output.json
  artifacts:
    paths: [trufflehog-output.json]
    when: always
    expire_in: one week
```

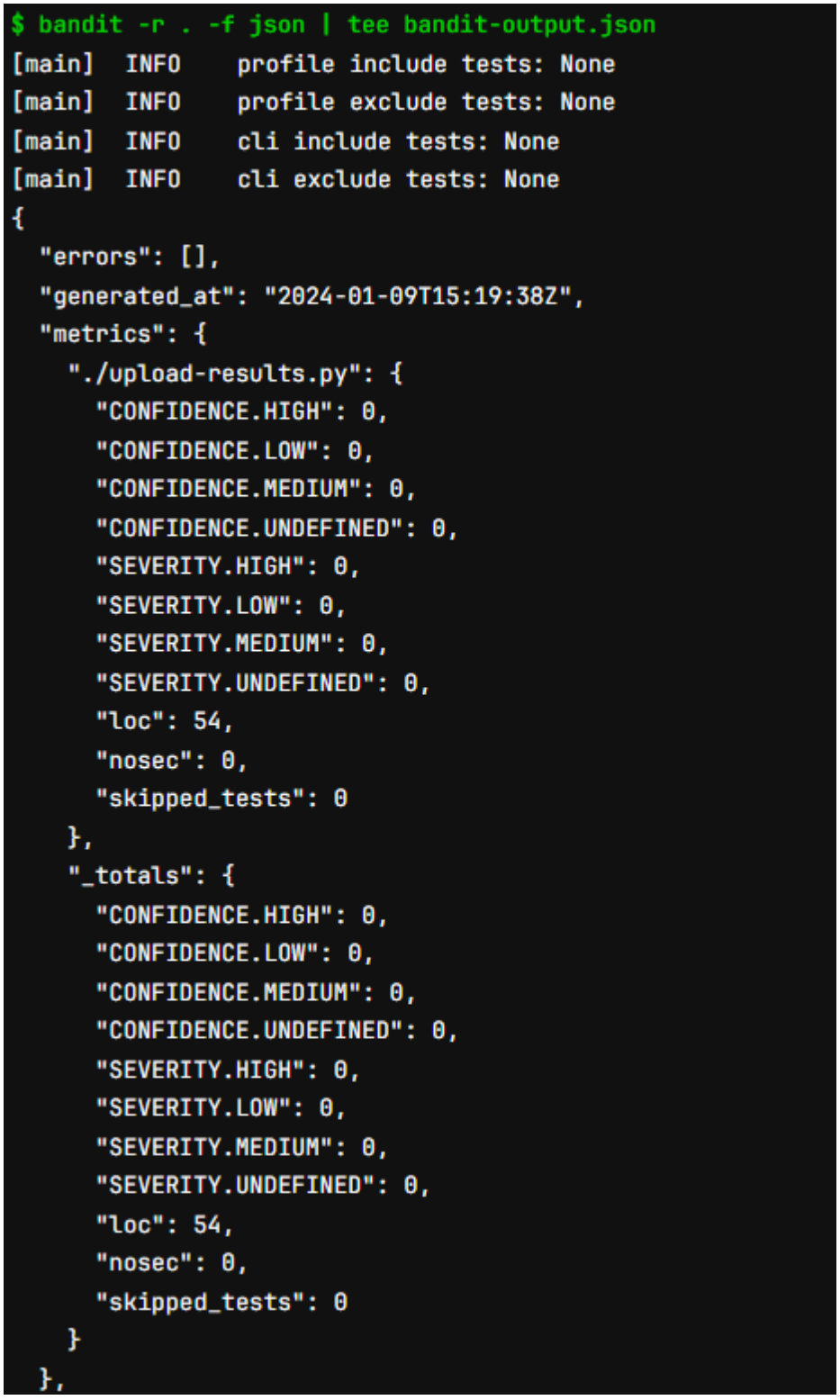
```
$ docker run -v $(pwd):/src --rm hysnsec/trufflehog filesystem --directory=/src --json | tee trufflehog-output.json
{"level":"info-0","ts":"2024-01-09T15:18:39Z","logger":"trufflehog","msg":"--directory flag is deprecated, please pass directories as arguments"}
{"level":"info-0","ts":"2024-01-09T15:18:39Z","logger":"trufflehog","msg":"running source","source_manager_worker_id":"iXgIF","with_units":true}
{"level":"info-0","ts":"2024-01-09T15:18:39Z","logger":"trufflehog","msg":"finished scanning","chunks":14,"bytes":105566,"verified_secrets":0,"unverified_secrets":0,"scan_duration":"417.125512ms"}
```

{"level":"info-0","ts":"2024-01-09T15:18:39Z","logger":"trufflehog","msg":"--directory flag is deprecated, please pass directories as arguments"}
{"level":"info-0","ts":"2024-01-09T15:18:39Z","logger":"trufflehog","msg":"running source","source_manager_worker_id":"iXgIF","with_units":true}
{"level":"info-0","ts":"2024-01-09T15:18:39Z","logger":"trufflehog","msg":"finished scanning","chunks":14,"bytes":105566,"verified_secrets":0,"unverified_secrets":0,"scan_duration":"417.125512ms"}

Bandit

Embed Bandit into Gitlab CI/CD:

```
sast-bandit:
  stage: build
  before_script:
    - apk update
    - apk add --no-cache python3 py3-pip
  script:
    - pip3 install bandit==1.7.4 --break-system-packages
    - pip3 install requests --break-system-packages
    - bandit -r . -f json | tee bandit-output.json
    - cat bandit-output.json
  artifacts:
    paths: [bandit-output.json]
    when: always
```



$ bandit -r . -f json | tee bandit-output.json
[main] INFO profile include tests: None
[main] INFO profile exclude tests: None
[main] INFO cli include tests: None
[main] INFO cli exclude tests: None
{
"errors": [],

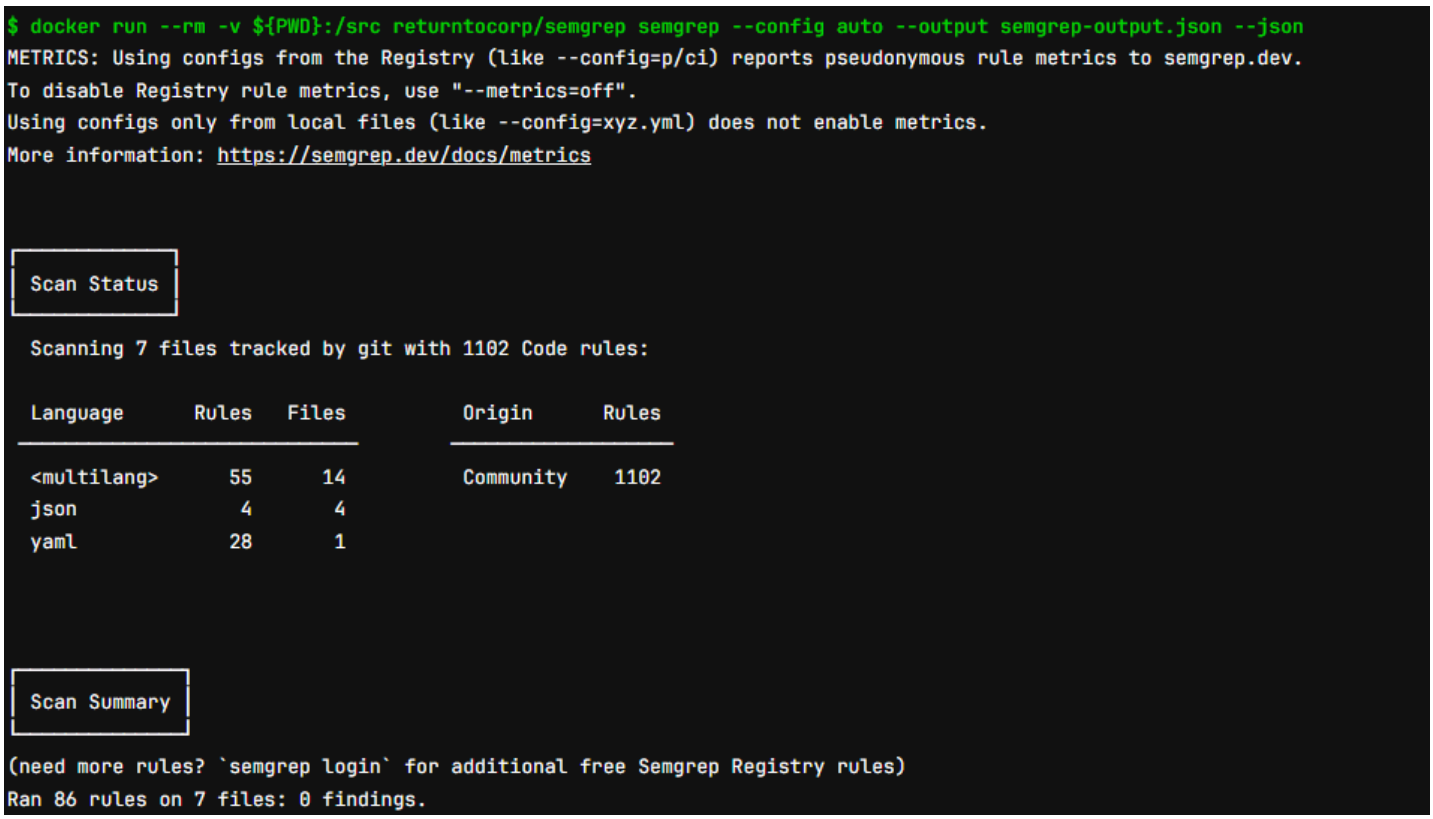
```
 "generated_at": "2024-01-09T15:19:38Z",
 "metrics": {
  "./upload-results.py": {
   "CONFIDENCE.HIGH": 0,
   "CONFIDENCE.LOW": 0,
   "CONFIDENCE.MEDIUM": 0,
   "CONFIDENCE.UNDEFINED": 0,
   "SEVERITY.HIGH": 0,
   "SEVERITY.LOW": 0,
   "SEVERITY.MEDIUM": 0,
   "SEVERITY.UNDEFINED": 0,
   "loc": 54,
   "nosec": 0,
   "skipped_tests": 0
  },
  "_totals": {
   "CONFIDENCE.HIGH": 0,
   "CONFIDENCE.LOW": 0,
   "CONFIDENCE.MEDIUM": 0,
   "CONFIDENCE.UNDEFINED": 0,
   "SEVERITY.HIGH": 0,
   "SEVERITY.LOW": 0,
   "SEVERITY.MEDIUM": 0,
   "SEVERITY.UNDEFINED": 0,
   "loc": 54,
   "nosec": 0,
   "skipped_tests": 0
  }
 },
 "results": []
}
```


Semgrep

Embed Semgrep into Gitlab CI/CD:

```
semgrep:
 stage: build
 script:
```

- docker run --rm -v ${PWD}:/src returntocorp/semgrep semgrep --config auto --output semgrep-output.json --json --metrics=off



METRICS: Using configs from the Registry (like --config=p/ci) reports pseudonymous rule metrics to semgrep.dev.
To disable Registry rule metrics, use "--metrics=off".
Using configs only from local files (like --config=xyz.yml) does not enable metrics.
More information: https://semgrep.dev/docs/metrics

Scan Status

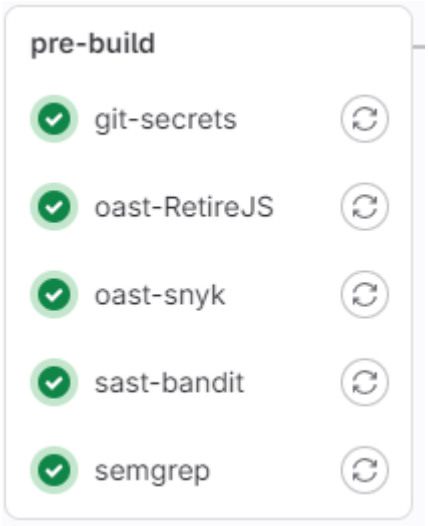
Scanning 7 files tracked by git with 1102 Code rules:

Language Rules Files Origin Rules
<multilang> 55 14 Community 1102
json 4 4
yaml 28 1

Scan Summary

(need more rules? `semgrep login` for additional free Semgrep Registry rules)

Ran 86 rules on 7 files: 0 findings.



DAST

Dynamic Application Security Testing (DAST) is an application security testing methodology in which the application is tested at runtime to discover security vulnerabiltiies. DAST tools don't have access to the application and API's source code, so they detect vulnerabilities by performing actual attacks, similar to a real hacker.

Nikto

Embed Nikto into Gitlab CI/CD:

```
nikto:
  stage: test
```

script:
- docker pull hysnsec/nikto
- docker run --rm -v $(pwd):/tmp hysnsec/nikto -h http://192.168.75.132:8083

```
$ docker run --rm -v $(pwd):/tmp hysnsec/nikto -h http://192.168.75.132:8083
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.75.132
+ Target Hostname:    192.168.75.132
+ Target Port:        8083
+ Start Time:         2024-01-09 16:28:26 (GMT0)
---------------------------------------------------------------------------
+ Server: No banner retrieved
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME typ
e. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /G8qOUp9m.php3: Uncommon header 'content-disposition' found, with contents: inline;filename=f.txt.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ OPTIONS: Allowed HTTP Methods: GET, HEAD, POST, PUT, DELETE, OPTIONS .
+ HTTP method ('Allow' Header): 'PUT' method could allow clients to save files on the web server.
+ HTTP method ('Allow' Header): 'DELETE' may allow clients to remove files on the web server.
+ 8100 requests: 0 error(s) and 6 item(s) reported on remote host
+ End Time:           2024-01-09 16:28:53 (GMT0) (27 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Nmap

Embed Nmap into Gitlab CI/CD:

nmap:
stage: test

script:
- docker pull hysnsec/nmap
- docker run --rm -v $(pwd):/tmp hysnsec/nmap -sSVC -A -p 8083 192.168.75.132

```
$ docker run --rm -v $(pwd):/tmp hysnsec/nmap -sSVC -A -p 8083 192.168.75.132
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-09 16:29 UTC
Nmap scan report for 192.168.75.132
Host is up (0.000062s latency).
PORT     STATE SERVICE VERSION
8083/tcp open  us-srv?
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.1 404
|     Vary: Origin
|     Vary: Access-Control-Request-Method
|     Vary: Access-Control-Request-Headers
|     Content-Disposition: inline;filename=f.txt
|     Content-Type: application/json
|     Date: Tue, 09 Jan 2024 16:29:53 GMT
|     Connection: close
|     {"timestamp":"2024-01-09T16:29:53.520+00:00","status":404,"error":"Not Found","path":"/nice%20ports%2C/Tri%6Eity.txt%2ebak"}
|   GetRequest:
|     HTTP/1.1 404
|     Vary: Origin
|     Vary: Access-Control-Request-Method
|     Vary: Access-Control-Request-Headers
|     Content-Type: application/json
|     Date: Tue, 09 Jan 2024 16:29:53 GMT
|     Connection: close
|     {"timestamp":"2024-01-09T16:29:53.514+00:00","status":404,"error":"Not Found","path":"/"}
|   HTTPOptions:
|     HTTP/1.1 404
|     Vary: Origin
|     Vary: Access-Control-Request-Method
|     Vary: Access-Control-Request-Headers
|     Content-Type: application/json
|     Date: Tue, 09 Jan 2024 16:29:58 GMT
|     Connection: close
|     {"timestamp":"2024-01-09T16:29:58.529+00:00","status":404,"error":"Not Found","path":"/"}
|   RPCCheck, RTSPRequest:
|     HTTP/1.1 400
|     Content-Type: text/html;charset=utf-8
|     Content-Language: en
|     Content-Length: 435
|     Date: Tue, 09 Jan 2024 16:29:58 GMT
|     Connection: close
|     <!doctype html><html lang="en"><head><title>HTTP Status 400
```

Zap

Embed ZAP (Zed Atttack Proxy) into Gitlab CI/CD:

```
zap-baseline:
  stage: test
  image: owasp/zap2docker-stable
  when: always
  script:
    - mkdir -p /zap/wrk/
    - zap-full-scan.py -t http://192.168.75.132:8083 -r report.html
    - cp /zap/wrk/report.html .
  artifacts:
    when: always
    paths: [report.html]
```

```
$ zap-full-scan.py -t http://192.168.75.132:8083 -r report.html
Total of 4 URLs
PASS: Directory Browsing [0]
PASS: Vulnerable JS Library (Powered by Retire.js) [10003]
PASS: In Page Banner Information Leak [10009]
PASS: Cookie No HttpOnly Flag [10010]
PASS: Cookie Without Secure Flag [10011]
PASS: Re-examine Cache-control Directives [10015]
PASS: Cross-Domain JavaScript Source File Inclusion [10017]
PASS: Content-Type Header Missing [10019]
PASS: Anti-clickjacking Header [10020]
PASS: X-Content-Type-Options Header Missing [10021]
PASS: Information Disclosure - Debug Error Messages [10023]
PASS: Information Disclosure - Sensitive Information in URL [10024]
PASS: Information Disclosure - Sensitive Information in HTTP Referrer Header [10025]
PASS: HTTP Parameter Override [10026]
PASS: Information Disclosure - Suspicious Comments [10027]
PASS: Open Redirect [10028]
PASS: Cookie Poisoning [10029]
```

ZAP Scanning Report

Site: http://192.168.75.132:8083

Generated on Tue, 9 Jan 2024 18:15:45

ZAP Version: 2.14.0

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	0
Low	0
Informational	2
False Positives:	0

Alerts

Name	Risk Level	Number of Instances
Storable and Cacheable Content	Informational	4
User Agent Fuzzer	Informational	48

Alert Detail

Informational	Storable and Cacheable Content
Description	The response contents are storable by caching components such as proxy servers, and may be retrieved directly from the cache, rather than from the origin server by the caching servers, in response to sensitive, personal or user-specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending their environment. This is primarily an issue where "shared" caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational er
URL	http://192.168.75.132:8083
Method	GET
Parameter	
Attack	
Evidence	
Other Info	In the absence of an explicitly specified caching lifetime directive in the response, a liberal lifetime heuristic of 1 year was assumed. This is permitted by rfc7234.
URL	http://192.168.75.132:8083/
Method	GET
Parameter	

$ zap-full-scan.py -t http://192.168.75.132:8083 -r report.html
Total of 4 URLs
PASS: Directory Browsing [0]
PASS: Vulnerable JS Library (Powered by Retire.js) [10003]
PASS: In Page Banner Information Leak [10009]
PASS: Cookie No HttpOnly Flag [10010]
PASS: Cookie Without Secure Flag [10011]
PASS: Re-examine Cache-control Directives [10015]
PASS: Cross-Domain JavaScript Source File Inclusion [10017]
PASS: Content-Type Header Missing [10019]
PASS: Anti-clickjacking Header [10020]
PASS: X-Content-Type-Options Header Missing [10021]
PASS: Information Disclosure - Debug Error Messages [10023]
PASS: Information Disclosure - Sensitive Information in URL [10024]
PASS: Information Disclosure - Sensitive Information in HTTP Referrer Header [10025]
PASS: HTTP Parameter Override [10026]
PASS: Information Disclosure - Suspicious Comments [10027]
PASS: Open Redirect [10028]
PASS: Cookie Poisoning [10029]
PASS: User Controllable Charset [10030]
PASS: User Controllable HTML Element Attribute (Potential XSS) [10031]
PASS: Viewstate [10032]
PASS: Directory Browsing [10033]
PASS: Heartbleed OpenSSL Vulnerability (Indicative) [10034]

PASS: Strict-Transport-Security Header [10035]
PASS: HTTP Server Response Header [10036]
PASS: Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) [10037]
PASS: Content Security Policy (CSP) Header Not Set [10038]
PASS: X-Backend-Server Header Information Leak [10039]
PASS: Secure Pages Include Mixed Content [10040]
PASS: HTTP to HTTPS Insecure Transition in Form Post [10041]
PASS: HTTPS to HTTP Insecure Transition in Form Post [10042]
PASS: User Controllable JavaScript Event (XSS) [10043]
PASS: Big Redirect Detected (Potential Sensitive Information Leak) [10044]
PASS: Source Code Disclosure - /WEB-INF folder [10045]
PASS: HTTPS Content Available via HTTP [10047]
PASS: Remote Code Execution - Shell Shock [10048]
PASS: Content Cacheability [10049]
PASS: Retrieved from Cache [10050]
PASS: Relative Path Confusion [10051]
PASS: X-ChromeLogger-Data (XCOLD) Header Information Leak [10052]
PASS: Cookie without SameSite Attribute [10054]
PASS: CSP [10055]
PASS: X-Debug-Token Information Leak [10056]
PASS: Username Hash Found [10057]
PASS: GET for POST [10058]
PASS: X-AspNet-Version Response Header [10061]
PASS: PII Disclosure [10062]
PASS: Permissions Policy Header Not Set [10063]
PASS: Backup File Disclosure [10095]
PASS: Timestamp Disclosure [10096]
PASS: Hash Disclosure [10097]
PASS: Cross-Domain Misconfiguration [10098]
PASS: Source Code Disclosure [10099]
PASS: User Agent Fuzzer [10104]
PASS: Weak Authentication Method [10105]
PASS: HTTP Only Site [10106]
PASS: Httpoxy - Proxy Header Misuse [10107]
PASS: Reverse Tabnabbing [10108]
PASS: Modern Web Application [10109]
PASS: Dangerous JS Functions [10110]
PASS: Authentication Request Identified [10111]
PASS: Session Management Response Identified [10112]
PASS: Verification Request Identified [10113]
PASS: Absence of Anti-CSRF Tokens [10202]
PASS: Private IP Disclosure [2]
PASS: Anti-CSRF Tokens Check [20012]
PASS: HTTP Parameter Pollution [20014]
PASS: Heartbleed OpenSSL Vulnerability [20015]
PASS: Cross-Domain Misconfiguration [20016]
PASS: Source Code Disclosure - CVE-2012-1823 [20017]
PASS: Remote Code Execution - CVE-2012-1823 [20018]
PASS: External Redirect [20019]
PASS: Session ID in URL Rewrite [3]
PASS: Buffer Overflow [30001]

PASS: Format String Error [30002]
PASS: Integer Overflow Error [30003]
PASS: CRLF Injection [40003]
PASS: Parameter Tampering [40008]
PASS: Server Side Include [40009]
PASS: Cross Site Scripting (Reflected) [40012]
PASS: Session Fixation [40013]
PASS: Cross Site Scripting (Persistent) [40014]
PASS: Cross Site Scripting (Persistent) - Prime [40016]
PASS: Cross Site Scripting (Persistent) - Spider [40017]
PASS: SQL Injection [40018]
PASS: SQL Injection - MySQL [40019]
PASS: SQL Injection - Hypersonic SQL [40020]
PASS: SQL Injection - Oracle [40021]
PASS: SQL Injection - PostgreSQL [40022]
PASS: Possible Username Enumeration [40023]
PASS: SQL Injection - SQLite [40024]
PASS: Proxy Disclosure [40025]
PASS: Cross Site Scripting (DOM Based) [40026]
PASS: SQL Injection - MsSQL [40027]
PASS: ELMAH Information Leak [40028]
PASS: Trace.axd Information Leak [40029]
PASS: Out of Band XSS [40031]
PASS: .htaccess Information Leak [40032]
PASS: .env Information Leak [40034]
PASS: Hidden File Finder [40035]
PASS: Bypassing 403 [40038]
PASS: CORS Header [40040]
PASS: Spring Actuator Information Leak [40042]
PASS: Log4Shell [40043]
PASS: Exponential Entity Expansion (Billion Laughs Attack) [40044]
PASS: Spring4Shell [40045]
PASS: Server Side Request Forgery [40046]
PASS: Text4shell (CVE-2022-42889) [40047]
PASS: Source Code Disclosure - Git [41]
PASS: Source Code Disclosure - SVN [42]
PASS: Source Code Disclosure - File Inclusion [43]
PASS: Script Active Scan Rules [50000]
PASS: Script Passive Scan Rules [50001]
PASS: Path Traversal [6]
PASS: Remote File Inclusion [7]
PASS: Insecure JSF ViewState [90001]
PASS: Java Serialization Object [90002]
PASS: Sub Resource Integrity Attribute Missing [90003]
PASS: Insufficient Site Isolation Against Spectre Vulnerability [90004]
PASS: Charset Mismatch [90011]
PASS: XSLT Injection [90017]
PASS: Server Side Code Injection [90019]
PASS: Remote OS Command Injection [90020]
PASS: XPath Injection [90021]
PASS: Application Error Disclosure [90022]

PASS: XML External Entity Attack [90023]
PASS: Generic Padding Oracle [90024]
PASS: Expression Language Injection [90025]
PASS: SOAP Action Spoofing [90026]
PASS: Cookie Slack Detector [90027]
PASS: Insecure HTTP Method [90028]
PASS: SOAP XML Injection [90029]
PASS: WSDL File Detection [90030]
PASS: Loosely Scoped Cookie [90033]
PASS: Cloud Metadata Potentially Exposed [90034]
PASS: Server Side Template Injection [90035]
PASS: Server Side Template Injection (Blind) [90036]
FAIL-NEW: 0 FAIL-INPROG: 0 WARN-NEW: 0 WARN-INPROG: 0 INFO: 0 IGNORE: 0 PASS: 136

Container Security

Container Scanning is often considered part of Software Composition Analysis (SCA). SCA can contain aspects of inspecting the items your code uses. These items typically include application and system dependencies that are almost always imported from external sources, rather than sourced from items you wrote yourself.

```
#Container Scanning

include:
  - template: Security/Container-Scanning.gitlab-ci.yml

container_scanning:
  variables:
    CS_IMAGE: mouadtigmouti/devsecops-backend
```

```
[INFO] [2024-01-09 19:31:20 +0000] [container-scanning]  >  Scanning container from registry mouadtigmouti/devsecops-backend for vulnerabilities with sever
ity level UNKNOWN or higher, with gcs 6.6.2 and Trivy Version: 0.48.1, advisories updated at 2024-01-09T12:13:28+00:00
```

STATUS	CVE SEVERITY	PACKAGE NAME	PACKAGE VERSION	CVE DESCRIPTION
Unapproved	Low	apt	2.2.4	It was found that apt-key in apt, all versions, do not correctly validate gpg keys with the master keyring, leading to a potential man-in-the-middle attack.
Unapproved	High	bash	5.1-2+b3	A flaw was found in the bash package, where a heap-buffer overflow can occur in valid parameter_transform. This issue may lead to memory problems.
Unapproved	Low	bash	5.1-2+b3	TEMP-0841856-B18BAF
Unapproved	Low	bsdutils	1:2.36.1-8+deb11u1	A flaw was found in the util-linux chfn and chsh utilities when compiled with Readline support. The Readline library uses an "INPUTRC" environment variable to get a path to the library config file. When the library cannot parse the specified file, it prints an error message containing data from the file. This flaw allows an unprivileged user to read root-owned files, potentially leading to privilege escalation. This flaw affects util-linux versions prior to 2.37.4.
Unapproved	Low	coreutils	8.32-4+b1	chroot in GNU coreutils, when used with --userspec, allows local users to escape to the parent session via a crafted TIOCSTI ioctl call, which pushes characters to the terminal's input buffer.
Unapproved	Low	coreutils	8.32-4+b1	In GNU Coreutils through 8.29, chown-core.c in chown and chgrp does not prevent replacement of a plain file with a symlink during use of the POSIX "-R -L" options, which allows local users to modify the ownership of arbitrary files by leveraging a race condition.
Unapproved	Critical	dpkg	1.20.9	Dpkg::Source::Archive in dpkg, the Debian package management system, before version 1.21.8, 1.20.10, 1.19.8, 1.18.26 is prone to a directory traversal vulnerability. When extracting untrusted source packages in v2 and v3 source package formats that include a debian.tar, the in-pl