Trabajo Práctico Integrador: Introducción a la Ciberseguridad

Capturas/ Respuestas PARTE-2

En este apartado se van a encontrar todas las salidas de escaneo que fueron realizadas en la parte-2.

Índice

Escaneo carpeta actual con Trivy **1**

```
┌──(kali㉿kali)-[~/Downloads/webapp]
└─$ sudo docker run --rm -v $(pwd):/scan aquasec/trivy:latest fs /scan --scanners secret
2025-11-04T01:10:36Z    INFO    [secret] Secret scanning is enabled
2025-11-04T01:10:36Z    INFO    [secret] Please see
https://trivy.dev/v0.67/docs/scanner/secret#recommendation for faster secret detection
2025-11-04T01:10:36Z    WARN    [pip] Unable to find python `site-packages` directory.
License detection is skipped.      err="unable to find path to Python executable"
2025-11-04T01:10:36Z    INFO    Number of language-specific files       num=1

Report Summary

┌──────────────────────┬──────┬─────────┐
│        Target        │ Type │ Secrets │
├──────────────────────┼──────┼─────────┤
│ requirements.txt     │ pip  │    -    │
├──────────────────────┼──────┼─────────┤
│ .env                 │ text │    5    │
├──────────────────────┼──────┼─────────┤
│ .env.production      │ text │    3    │
├──────────────────────┼──────┼─────────┤
│ config.json          │ text │    6    │
├──────────────────────┼──────┼─────────┤
│ secrets/api_key.txt  │ text │    2    │
└──────────────────────┴──────┴─────────┘
Legend:
- '-': Not scanned
- '0': Clean (no security findings detected)


.env (secrets)
==============
Total: 5 (UNKNOWN: 0, LOW: 0, MEDIUM: 0, HIGH: 1, CRITICAL: 4)
```

CRITICAL: GitHub (github-pat)
═══
GitHub Personal Access Token
───
 .env:22 (offset: 960 bytes)
───
  20   STRIPE_LIVE_KEY=**utsrqponmlkjihgf
  21
PAYPAL_CLIENT_SECRET=EBWWkK4Jk2Pm9uN8qL7r3Vx6bZ8cA5sDhGjKlMnPqRsTu
VwX
  22 [GITHUB_TOKEN=**1234
  23   GITHUB_CLIENT_SECRET=1234567890abcdef1234567890abcdef12345678
───

CRITICAL: GitLab (gitlab-pat)
═══
GitLab Personal Access Token
───
 .env:84 (offset: 3762 bytes)
───
  82   # Tokens de CI/CD
  83   JENKINS_API_TOKEN=1234567890abcdefghijklmnopqrstuvwxyz
  84 [GITLAB_ACCESS_TOKEN=**************************
  85
CIRCLECI_API_TOKEN=1234567890abcdefghijklmnopqrstuvwxyz1234567890abcdef
───

HIGH: Slack (slack-access-token)
═══
Slack token
───
 .env:31 (offset: 1423 bytes)
───
  29   # Servicios de terceros
  30   TWILIO_AUTH_TOKEN=1234567890abcdef1234567890abcdef
  31 [SLACK_BOT_TOKEN=***************-1234567890-1234567890abcdefghijklmn
  32
DISCORD_BOT_TOKEN=ODY2NzE2MDMwMjIyODQ4MDMy.YPW2Fg.abcdefghijklmnop
qrstuvwxyz123456
───

CRITICAL: Stripe (stripe-secret-token)
═══
Stripe Secret Key
───
 .env:19 (offset: 746 bytes)
───
  17
  18   # APIs externas
  19 [STRIPE_SECRET_KEY**fghijklmnopqrstuv

```
  20   STRIPE_LIVE_KEY=****************************************utsrqponmlkjihgf
──────────────────────────────────────────────────────────────────────────────


CRITICAL: Stripe (stripe-secret-token)
══════════════════════════════════════════════════════════════════════════════
Stripe Secret Key
──────────────────────────────────────────────────────────────────────────────
 .env:20 (offset: 820 bytes)
──────────────────────────────────────────────────────────────────────────────
  18   # APIs externas
  19   STRIPE_SECRET_KEY=****************************************fghijklmnopqrstuv
  20 [ STRIPE_LIVE_KEY=****************************************utsrqponmlkjihgf
  21
PAYPAL_CLIENT_SECRET=EBWWkK4Jk2Pm9uN8qL7r3Vx6bZ8cA5sDhGjKlMnPqRsTu
VwX
──────────────────────────────────────────────────────────────────────────────



.env.production (secrets)
==========================
Total: 3 (UNKNOWN: 0, LOW: 0, MEDIUM: 1, HIGH: 0, CRITICAL: 2)

CRITICAL: GitLab (gitlab-pat)
══════════════════════════════════════════════════════════════════════════════
GitLab Personal Access Token
──────────────────────────────────────────────────────────────────────────────
 .env.production:66 (offset: 2858 bytes)
──────────────────────────────────────────────────────────────────────────────
  64   # CI/CD Production
  65
JENKINS_API_TOKEN=production_jenkins_api_token_1234567890abcdefghijklmnopqrst
uvwxyz
  66 [ GITLAB_ACCESS_TOKEN=**************************0abcdefghijklmnopqrstuvwxyz
  67
GITHUB_ACTIONS_TOKEN=ghs_production_1234567890abcdefghijklmnopqrstuvwxyz
──────────────────────────────────────────────────────────────────────────────


MEDIUM: SendGrid (sendgrid-api-token)
══════════════════════════════════════════════════════════════════════════════
SendGrid API token
──────────────────────────────────────────────────────────────────────────────
 .env.production:33 (offset: 1237 bytes)
──────────────────────────────────────────────────────────────────────────────
  31
  32   # Email Services Production
  33 [
SENDGRID_API_KEY=**********************************************************************abcd
ef
  34   MAILGUN_API_KEY=key-production-1234567890abcdefghijklmnopqrstuvwxyz
──────────────────────────────────────────────────────────────────────────────
```

CRITICAL: Stripe (stripe-secret-token)
═══
Stripe Secret Key
───
 .env.production:14 (offset: 334 bytes)
───
  12
  13   # Production API Keys
  14 [STRIPE_LIVE_SECRET_KEY=**utsrqponmlkjihgf
  15
PAYPAL_LIVE_CLIENT_SECRET=EBWWkK4Jk2Pm9uN8qL7r3Vx6bZ8cA5sDhGjKlMnP
qRsTuVwXyZ123
───

config.json (secrets)
=====================
Total: 6 (UNKNOWN: 0, LOW: 0, MEDIUM: 0, HIGH: 2, CRITICAL: 4)

CRITICAL: GitHub (github-pat)
═══
GitHub Personal Access Token
───
 config.json:31 (offset: 1019 bytes)
───
  29   "stripe_secret": "**fghijklmnopqrstuv",
  30   "stripe_live": "**utsrqponmlkjihgf",
  31 ["github_token": "**1234",
  32   "github_client_secret": "1234567890abcdef1234567890abcdef12345678",
───

CRITICAL: GitLab (gitlab-pat)
═══
GitLab Personal Access Token
───
 config.json:58 (offset: 2645 bytes)
───
  56   "ci_cd": {
  57   "jenkins_api_token": "1234567890abcdefghijklmnopqrstuvwxyz",
  58 ["gitlab_access_token": "**************************",
  59   "circleci_api_token":
"1234567890abcdefghijklmnopqrstuvwxyz1234567890abcdef"
───

HIGH: AsymmetricPrivateKey (private-key)
═══
Asymmetric Private Key
───
 config.json:66 (offset: 2988 bytes)
───

```
  64        "email": "admin@vulnerable.com",
  65        "api_token": "admin_api_token_123456789",
  66 [ ----BEGIN RSA PRIVATE
KEY-----**********************************************************************-----END RSA
PRIVATE
  67      },
```

HIGH: Slack (slack-access-token)

Slack token

```
 config.json:43 (offset: 1759 bytes)
```

```
  41      "third_party_services": {
  42        "twilio_auth_token": "1234567890abcdef1234567890abcdef",
  43 [      "slack_bot_token": "***************-1234567890-1234567890abcdefghijklmn",
  44        "discord_bot_token":
"ODY2NzE2MDMwMjIyODQ4MDMy.YPW2Fg.abcdefghijklmnopqrstuvwxyz123456",
```

CRITICAL: Stripe (stripe-secret-token)

Stripe Secret Key

```
 config.json:29 (offset: 855 bytes)
```

```
  27      },
  28      "external_apis": {
  29 [      "stripe_secret": "****************************************fghijklmnopqrstuv",
  30        "stripe_live": "****************************************utsrqponmlkjihgf",
```

CRITICAL: Stripe (stripe-secret-token)

Stripe Secret Key

```
 config.json:30 (offset: 937 bytes)
```

```
  28      "external_apis": {
  29        "stripe_secret": "****************************************fghijklmnopqrstuv",
  30 [      "stripe_live": "****************************************utsrqponmlkjihgf",
  31        "github_token": "****************************************1234",
```

secrets/api_key.txt (secrets)

```
==============================
Total: 2 (UNKNOWN: 0, LOW: 0, MEDIUM: 0, HIGH: 0, CRITICAL: 2)
```

```
CRITICAL: Stripe (stripe-secret-token)
═══════════════════════════════════════════════════════
Stripe Secret Key
─────────────────────────────────────────────────────
 secrets/api_key.txt:2 (offset: 50 bytes)
─────────────────────────────────────────────────────
   1   sk-1234567890abcdefghijklmnopqrstuvwxyz0987654321
   2 [ ****************************************fghijklmnopqrstuv
   3   ****************************************utsrqponmlkjihgf
─────────────────────────────────────────────────────


CRITICAL: Stripe (stripe-secret-token)
═══════════════════════════════════════════════════════
Stripe Secret Key
─────────────────────────────────────────────────────
 secrets/api_key.txt:3 (offset: 108 bytes)
─────────────────────────────────────────────────────
   1   sk-1234567890abcdefghijklmnopqrstuvwxyz0987654321
   2   ****************************************fghijklmnopqrstuv
   3 [ ****************************************utsrqponmlkjihgf
─────────────────────────────────────────────────────
```

Escaneo carpeta actual con Trufflehog: **2** [volver al indice]

```
┌──(kali㉿kali)-[~/Downloads/webapp]
└─$ sudo docker run --rm -v $(pwd):/scan trufflesecurity/trufflehog:latest filesystem /scan
🐷🔑🐷  TruffleHog. Unearth your secrets. 🐷🔑🐷

2025-11-04T01:21:42Z    info-0  trufflehog      running source
{"source_manager_worker_id": "pr0Eh", "with_units": true}
Found unverified result 🐷🔑❓
Verification issue: lookup backup-server.internal on 181.30.140.195:53: no such host
Detector Type: Postgres
Decoder Type: BASE64
Raw result:
postgresql://backup_user:SuperSecretBackupPass2024!@backup-server.internal:5432
Sslmode: <unset>
File: /scan/.env
Line: 16

Found unverified result 🐷🔑❓
Detector Type: Stripe
Decoder Type: PLAIN
Raw result: sk_live_51H1vSILkdIwHu0bS9876543210zyxwvutsrqponmlkjihgf
Rotation_guide: https://howtorotate.com/docs/tutorials/stripe/
File: /scan/.env
Line: 20

Found unverified result 🐷🔑❓
Detector Type: Stripe
Decoder Type: PLAIN
```

Raw result: sk_live_51H1vSILkdIwHu0bS9876543210zyxwvutsrqponmlkjihgf
Rotation_guide: https://howtorotate.com/docs/tutorials/stripe/
File: /scan/.env.production
Line: 14

Found unverified result 🐷🔑❓
(Verification info cached)
Detector Type: Stripe
Decoder Type: PLAIN
Raw result: sk_live_51H1vSILkdIwHu0bS9876543210zyxwvutsrqponmlkjihgf
Rotation_guide: https://howtorotate.com/docs/tutorials/stripe/
File: /scan/.git/objects/1d/6cdd4bcf9bea2d47c452e171eed8316ed80afd
Line: 14

Found unverified result 🐷🔑❓
(Verification info cached)
Detector Type: Stripe
Decoder Type: PLAIN
Raw result: sk_live_51H1vSILkdIwHu0bS9876543210zyxwvutsrqponmlkjihgf
Rotation_guide: https://howtorotate.com/docs/tutorials/stripe/
File: /scan/.git/objects/94/c944e5777631f2c6d03a096dde61a022f952ef
Line: 30

Found unverified result 🐷🔑❓
(Verification info cached)
Detector Type: Stripe
Decoder Type: PLAIN
Raw result: sk_live_51H1vSILkdIwHu0bS9876543210zyxwvutsrqponmlkjihgf
Rotation_guide: https://howtorotate.com/docs/tutorials/stripe/
File: /scan/.git/objects/b2/4059185c029ad98aa66c475c9c647c2be531d5
Line: 3

Found unverified result 🐷🔑❓
Verification issue: lookup db on 181.30.140.195:53: no such host
Detector Type: Postgres
Decoder Type: PLAIN
Raw result: postgresql://admin:password123@db:5432
Sslmode: <unset>
File: /scan/.git/objects/b9/9b36032846b9794a14827764c596959dc67950
Line: 14

Found unverified result 🐷🔑❓
Verification issue: lookup stage-db on 181.30.140.195:53: no such host
Detector Type: Postgres
Decoder Type: PLAIN
Raw result: postgresql://admin:StagePass456@stage-db:5432
Sslmode: <unset>
File: /scan/.git/objects/b9/9b36032846b9794a14827764c596959dc67950
Line: 120

Found unverified result 🐷🔑❓
(Verification info cached)
Detector Type: Stripe
Decoder Type: PLAIN

Raw result: sk_live_51H1vSILkdIwHu0bS9876543210zyxwvutsrqponmlkjihgf
Rotation_guide: https://howtorotate.com/docs/tutorials/stripe/
File: /scan/.git/objects/c0/958773ade15adbf28ddcd3164a7517eeb6ddd4
Line: 20

Found unverified result 🐷🔑❓
Verification issue: lookup prod-db on 181.30.140.195:53: no such host
Detector Type: Postgres
Decoder Type: PLAIN
Raw result: postgresql://admin:SecretPass123@prod-db:5432
Sslmode: <unset>
File: /scan/.git/objects/b9/9b36032846b9794a14827764c596959dc67950
Line: 119

Found unverified result 🐷🔑❓
Verification issue: lookup backup-server.internal on 181.30.140.195:53: no such host (Verification info cached)
Detector Type: Postgres
Decoder Type: PLAIN
Raw result: postgresql://backup_user:SuperSecretBackupPass2024!@backup-server.internal:5432
Sslmode: <unset>
File: /scan/.git/objects/c0/958773ade15adbf28ddcd3164a7517eeb6ddd4
Line: 16

Found unverified result 🐷🔑❓
Verification issue: lookup db on 181.30.140.195:53: no such host
Detector Type: Postgres
Decoder Type: PLAIN
Raw result: postgresql://admin:password123@db:5432
Sslmode: <unset>
File: /scan/.git/objects/5b/7b096a33d0257b0e573e8b9b7b87ec7c285e30
Line: 36

Found unverified result 🐷🔑❓
Verification issue: lookup prod-db on 181.30.140.195:53: no such host
Detector Type: Postgres
Decoder Type: PLAIN
Raw result: postgresql://admin:SecretPass123@prod-db:5432
Sslmode: <unset>
File: /scan/.git/objects/5b/7b096a33d0257b0e573e8b9b7b87ec7c285e30
Line: 52

Found unverified result 🐷🔑❓
Verification issue: lookup db on 181.30.140.195:53: no such host
Detector Type: Postgres
Decoder Type: PLAIN
Raw result: postgresql://prod_user:prod_password_secret_123456@db:5432
Sslmode: <unset>
File: /scan/.git/objects/ce/a137d3c5ccdada3eaf21405fb2c590122b674e
Line: 7

Found unverified result 🐷🔑❓
Verification issue: lookup prod-db on 181.30.140.195:53: no such host

(Verification info cached)
Detector Type: Postgres
Decoder Type: PLAIN
Raw result: postgresql://admin:SecretPass123@prod-db:5432
Sslmode: <unset>
File: /scan/Dockerfile
Line: 52

Found unverified result 🐷🔑❓
Verification issue: lookup db on 181.30.140.195:53: no such host
(Verification info cached)
Detector Type: Postgres
Decoder Type: PLAIN
Raw result: postgresql://admin:password123@db:5432
Sslmode: <unset>
File: /scan/Dockerfile
Line: 36

Found unverified result 🐷🔑❓
(Verification info cached)
Detector Type: Stripe
Decoder Type: PLAIN
Raw result: sk_live_51H1vSILkdIwHu0bS9876543210zyxwvutsrqponmlkjihgf
Rotation_guide: https://howtorotate.com/docs/tutorials/stripe/
File: /scan/config.json
Line: 30

Found unverified result 🐷🔑❓
Verification issue: lookup db on 181.30.140.195:53: no such host
(Verification info cached)
Detector Type: Postgres
Decoder Type: PLAIN
Raw result: postgresql://prod_user:prod_password_secret_123456@db:5432
Sslmode: <unset>
File: /scan/docker-compose.prod.yml
Line: 7

Found unverified result 🐷🔑❓
Verification issue: lookup db on 181.30.140.195:53: no such host
(Verification info cached)
Detector Type: Postgres
Decoder Type: PLAIN
Raw result: postgresql://admin:password123@db:5432
Sslmode: <unset>
File: /scan/docker-compose.yml
Line: 14

Found unverified result 🐷🔑❓
Verification issue: lookup prod-db on 181.30.140.195:53: no such host
(Verification info cached)
Detector Type: Postgres
Decoder Type: PLAIN
Raw result: postgresql://admin:SecretPass123@prod-db:5432
Sslmode: <unset>

```
File: /scan/docker-compose.yml
Line: 119

Found unverified result 🐷🔑❓
Verification issue: lookup stage-db on 181.30.140.195:53: no such host
(Verification info cached)
Detector Type: Postgres
Decoder Type: PLAIN
Raw result: postgresql://admin:StagePass456@stage-db:5432
Sslmode: <unset>
File: /scan/docker-compose.yml
Line: 120

Found unverified result 🐷🔑❓
(Verification info cached)
Detector Type: Stripe
Decoder Type: PLAIN
Raw result: sk_live_51H1vSILkdIwHu0bS9876543210zyxwvutsrqponmlkjihgf
Rotation_guide: https://howtorotate.com/docs/tutorials/stripe/
File: /scan/secrets/api_key.txt
Line: 3

Found unverified result 🐷🔑❓
Verification issue: context deadline exceeded
Detector Type: MongoDB
Decoder Type: PLAIN
Raw result: mongodb://admin:password123@localhost:27017/vulnerable
Rotation_guide: https://howtorotate.com/docs/tutorials/mongo/
File: /scan/.env
Line: 14

Found unverified result 🐷🔑❓
Verification issue: context deadline exceeded
Detector Type: MongoDB
Decoder Type: PLAIN
Raw result: mongodb://admin:password123@localhost:27017/vulnerable
Rotation_guide: https://howtorotate.com/docs/tutorials/mongo/
File: /scan/.git/objects/c0/958773ade15adbf28ddcd3164a7517eeb6ddd4
Line: 14

2025-11-04T01:21:51Z    info-0  trufflehog      finished scanning       {"chunks": 75, "bytes":
113247, "verified_secrets": 0, "unverified_secrets": 24, "scan_duration": "8.470567435s",
"trufflehog_version": "3.90.12", "verification_caching":
{"Hits":58,"Misses":44,"HitsWasted":3,"AttemptsSaved":55,"VerificationTimeSpentMS":771
74}}
```

Vulnerabilidades en Dependencias **3** subir al indice

```
┌──(kali㉿kali)-[~/Downloads/webapp]
└─$ sudo docker run --rm -v $(pwd):/scan aquasec/trivy:latest fs /scan --scanners vuln
2025-11-04T01:29:29Z    INFO    [vulndb] Need to update DB
2025-11-04T01:29:29Z    INFO    [vulndb] Downloading vulnerability DB...
```

```
2025-11-04T01:29:29Z    INFO    [vulndb] Downloading artifact...
repo="mirror.gcr.io/aquasec/trivy-db:2"
847.18 KiB / 74.14 MiB
[>_____________________________________________________________] 1.12% ?
p/s ?2.12 MiB / 74.14 MiB
[->____________________________________________________________] 2.87% ?
p/s ?4.19 MiB / 74.14 MiB
[--->__________________________________________________________] 5.65% ?
p/s ?7.80 MiB / 74.14 MiB [----->_______________________________________]
10.52% 11.63 MiB p/s ETA 5s9.73 MiB / 74.14 MiB
[------>_______________________________________] 13.13% 11.63 MiB p/s ETA
5s14.34 MiB / 74.14 MiB [--------->_____________________________________]
19.35% 11.63 MiB p/s ETA 5s14.34 MiB / 74.14 MiB
[--------->_____________________________________] 19.35% 11.58 MiB p/s ETA
5s14.34 MiB / 74.14 MiB [--------->_____________________________________]
19.35% 11.58 MiB p/s ETA 5s14.34 MiB / 74.14 MiB
[--------->_____________________________________] 19.35% 11.58 MiB p/s ETA
5s14.84 MiB / 74.14 MiB [--------->_____________________________________]
20.02% 10.89 MiB p/s ETA 5s17.62 MiB / 74.14 MiB
[---------->____________________________________] 23.77% 10.89 MiB p/s ETA
5s18.75 MiB / 74.14 MiB [---------->____________________________________] 25.29%
10.89 MiB p/s ETA 5s20.56 MiB / 74.14 MiB
[---------->____________________________________] 27.73% 10.80 MiB p/s ETA
4s24.94 MiB / 74.14 MiB [---------->____________________________________] 33.64%
10.80 MiB p/s ETA 4s28.64 MiB / 74.14 MiB
[----------->___________________________________] 38.63% 10.80 MiB p/s ETA 4s30.64
MiB / 74.14 MiB [----------->___________________________________] 41.33% 11.18 MiB
p/s ETA 3s34.96 MiB / 74.14 MiB [------------------->___________________________]
47.15% 11.18 MiB p/s ETA 3s35.71 MiB / 74.14 MiB
[------------------->___________________________] 48.16% 11.18 MiB p/s ETA 3s37.96
MiB / 74.14 MiB [------------------->___________________________] 51.20% 11.25 MiB p/s
ETA 3s40.21 MiB / 74.14 MiB [-------------------->__________________________] 54.23%
11.25 MiB p/s ETA 3s44.52 MiB / 74.14 MiB
[---------------------->_________________________] 60.05% 11.25 MiB p/s ETA 2s46.86 MiB /
74.14 MiB [---------------------->_________________________] 63.21% 11.48 MiB p/s ETA
2s49.02 MiB / 74.14 MiB [----------------------->________________________] 66.12% 11.48 MiB
p/s ETA 2s50.89 MiB / 74.14 MiB [----------------------->________________________] 68.65%
11.48 MiB p/s ETA 2s53.80 MiB / 74.14 MiB [------------------------->______________]
72.57% 11.49 MiB p/s ETA 1s56.39 MiB / 74.14 MiB
[------------------------->______________] 76.07% 11.49 MiB p/s ETA 1s59.24 MiB /
74.14 MiB [-------------------------->_____________] 79.90% 11.49 MiB p/s ETA 1s61.74
MiB / 74.14 MiB [-------------------------->_____________] 83.27% 11.60 MiB p/s ETA
1s63.99 MiB / 74.14 MiB [--------------------------->____________] 86.31% 11.60 MiB p/s
ETA 0s66.11 MiB / 74.14 MiB [---------------------------->___________] 89.17% 11.60 MiB
p/s ETA 0s68.58 MiB / 74.14 MiB [----------------------------->__________] 92.50% 11.59
MiB p/s ETA 0s70.21 MiB / 74.14 MiB [------------------------------>_____] 94.70%
11.59 MiB p/s ETA 0s74.14 MiB / 74.14 MiB [------------------------------->]
100.00% 11.31 MiB p/s ETA 0s74.14 MiB / 74.14 MiB
[------------------------------->] 100.00% 11.31 MiB p/s ETA 0s74.14 MiB / 74.14
MiB [------------------------------->] 100.00% 11.31 MiB p/s ETA 0s74.14 MiB /
74.14 MiB [------------------------------->] 100.00% 10.58 MiB p/s ETA 0s74.14 MiB
/ 74.14 MiB [------------------------------->] 100.00% 10.58 MiB p/s ETA 0s74.14
MiB / 74.14 MiB [------------------------------->] 100.00% 10.58 MiB p/s ETA
0s74.14 MiB / 74.14 MiB [------------------------------->] 100.00% 9.90 MiB p/s
```

```
ETA 0s74.14 MiB / 74.14 MiB [---------------------------------------------->] 100.00% 9.90 MiB
p/s ETA 0s74.14 MiB / 74.14 MiB [---------------------------------------------->] 100.00% 9.26
MiB p/s ETA 0s74.14 MiB / 74.14 MiB [---------------------------------------------->] 100.00%
9.26 MiB p/s ETA 0s74.14 MiB / 74.14 MiB [---------------------------------------------->]
100.00% 9.26 MiB p/s ETA 0s74.14 MiB / 74.14 MiB
[---------------------------------------------->] 100.00% 8.66 MiB p/s ETA 0s74.14 MiB / 74.14
MiB [---------------------------------------------->] 100.00% 8.66 MiB p/s ETA 0s74.14 MiB /
74.14 MiB [---------------------------------------------->] 100.00% 8.66 MiB p/s ETA 0s74.14 MiB
/ 74.14 MiB [---------------------------------------------->] 100.00% 8.10 MiB p/s ETA 0s74.14
MiB / 74.14 MiB [---------------------------------------------->] 100.00% 8.10 MiB p/s ETA
0s74.14 MiB / 74.14 MiB [---------------------------------------------->] 100.00% 8.10 MiB p/s
ETA 0s74.14 MiB / 74.14 MiB [---------------------------------------------->] 100.00% 7.58 MiB
p/s ETA 0s74.14 MiB / 74.14 MiB [---------------------------------------------->] 100.00% 7.58
MiB p/s ETA 0s74.14 MiB / 74.14 MiB [---------------------------------------------->] 100.00%
7.58 MiB p/s ETA 0s74.14 MiB / 74.14 MiB [---------------------------------------------->]
100.00% 7.09 MiB p/s ETA 0s74.14 MiB / 74.14 MiB
[---------------------------------------------->] 100.00% 7.09 MiB p/s ETA 0s74.14 MiB / 74.14
MiB [---------------------------------------------->] 100.00% 7.09 MiB p/s ETA 0s74.14 MiB /
74.14 MiB [---------------------------------------------->] 100.00% 6.63 MiB p/s ETA 0s74.14 MiB
/ 74.14 MiB [---------------------------------------------->] 100.00% 6.63 MiB p/s ETA 0s74.14
MiB / 74.14 MiB [---------------------------------------------->] 100.00% 6.63 MiB p/s ETA
0s74.14 MiB / 74.14 MiB [---------------------------------------------->] 100.00% 6.21 MiB p/s
ETA 0s74.14 MiB / 74.14 MiB [---------------------------------------------->] 100.00% 6.21 MiB
p/s ETA 0s74.14 MiB / 74.14 MiB [---------------------------------------------->] 100.00% 6.21
MiB p/s ETA 0s74.14 MiB / 74.14 MiB [---------------------------------------------->] 100.00%
5.81 MiB p/s ETA 0s74.14 MiB / 74.14 MiB [---------------------------------------------->]
100.00% 5.81 MiB p/s ETA 0s74.14 MiB / 74.14 MiB
[---------------------------------------------->] 100.00% 5.81 MiB p/s ETA 0s74.14 MiB / 74.14
MiB [---------------------------------------------->] 100.00% 5.43 MiB p/s ETA 0s74.14 MiB /
74.14 MiB [---------------------------------------------->] 100.00% 5.43 MiB p/s ETA 0s74.14 MiB
/ 74.14 MiB [---------------------------------------------->] 100.00% 5.43 MiB p/s ETA 0s74.14
MiB / 74.14 MiB [---------------------------------------------->] 100.00% 5.08 MiB p/s ETA
0s74.14 MiB / 74.14 MiB [---------------------------------------------->] 100.00% 5.08 MiB p/s
ETA 0s74.14 MiB / 74.14 MiB [---------------------------------------------->] 100.00% 5.08 MiB
p/s ETA 0s74.14 MiB / 74.14 MiB [---------------------------------------------->] 100.00% 4.75
MiB p/s ETA 0s74.14 MiB / 74.14 MiB [---------------------------------------------->] 100.00%
4.75 MiB p/s ETA 0s74.14 MiB / 74.14 MiB [---------------------------------------------->]
100.00% 4.75 MiB p/s ETA 0s74.14 MiB / 74.14 MiB
[---------------------------------------------->] 100.00% 4.45 MiB p/s ETA 0s74.14 MiB / 74.14
MiB [---------------------------------------------->] 100.00% 4.45 MiB p/s ETA 0s74.14 MiB /
74.14 MiB [---------------------------------------------->] 100.00% 4.45 MiB p/s ETA 0s74.14 MiB
/ 74.14 MiB [---------------------------------------------->] 100.00% 4.16 MiB p/s ETA 0s74.14
MiB / 74.14 MiB [---------------------------------------------->] 100.00% 4.16 MiB p/s ETA
0s74.14 MiB / 74.14 MiB [---------------------------------------------->] 100.00% 4.16 MiB p/s
ETA 0s74.14 MiB / 74.14 MiB [---------------------------------------------->] 100.00% 3.89 MiB
p/s ETA 0s74.14 MiB / 74.14 MiB [---------------------------------------------->] 100.00% 3.89
MiB p/s ETA 0s74.14 MiB / 74.14 MiB [---------------------------------------------->] 100.00%
3.89 MiB p/s ETA 0s74.14 MiB / 74.14 MiB [---------------------------------------------->]
100.00% 3.64 MiB p/s ETA 0s74.14 MiB / 74.14 MiB
[---------------------------------------------->] 100.00% 3.64 MiB p/s ETA 0s74.14 MiB / 74.14
MiB [---------------------------------------------->] 100.00% 3.64 MiB p/s ETA 0s74.14 MiB /
74.14 MiB [---------------------------------------------->] 100.00% 3.41 MiB p/s ETA 0s74.14 MiB
/ 74.14 MiB [----------------------------------------------] 100.00% 4.15 MiB p/s
18s2025-11-04T01:29:55Z    INFO    [vulndb] Artifact successfully
```

```
downloadedrepo="mirror.gcr.io/aquasec/trivy-db:2"
2025-11-04T01:29:55Z    INFO    [vuln] Vulnerability scanning is enabled
2025-11-04T01:29:55Z    WARN    [pip] Unable to find python `site-packages` directory. License detection is skipped.    err="unable to find path to Python executable"
2025-11-04T01:29:55Z    INFO    Number of language-specific files    num=1
2025-11-04T01:29:55Z    INFO    [pip] Detecting vulnerabilities...
```

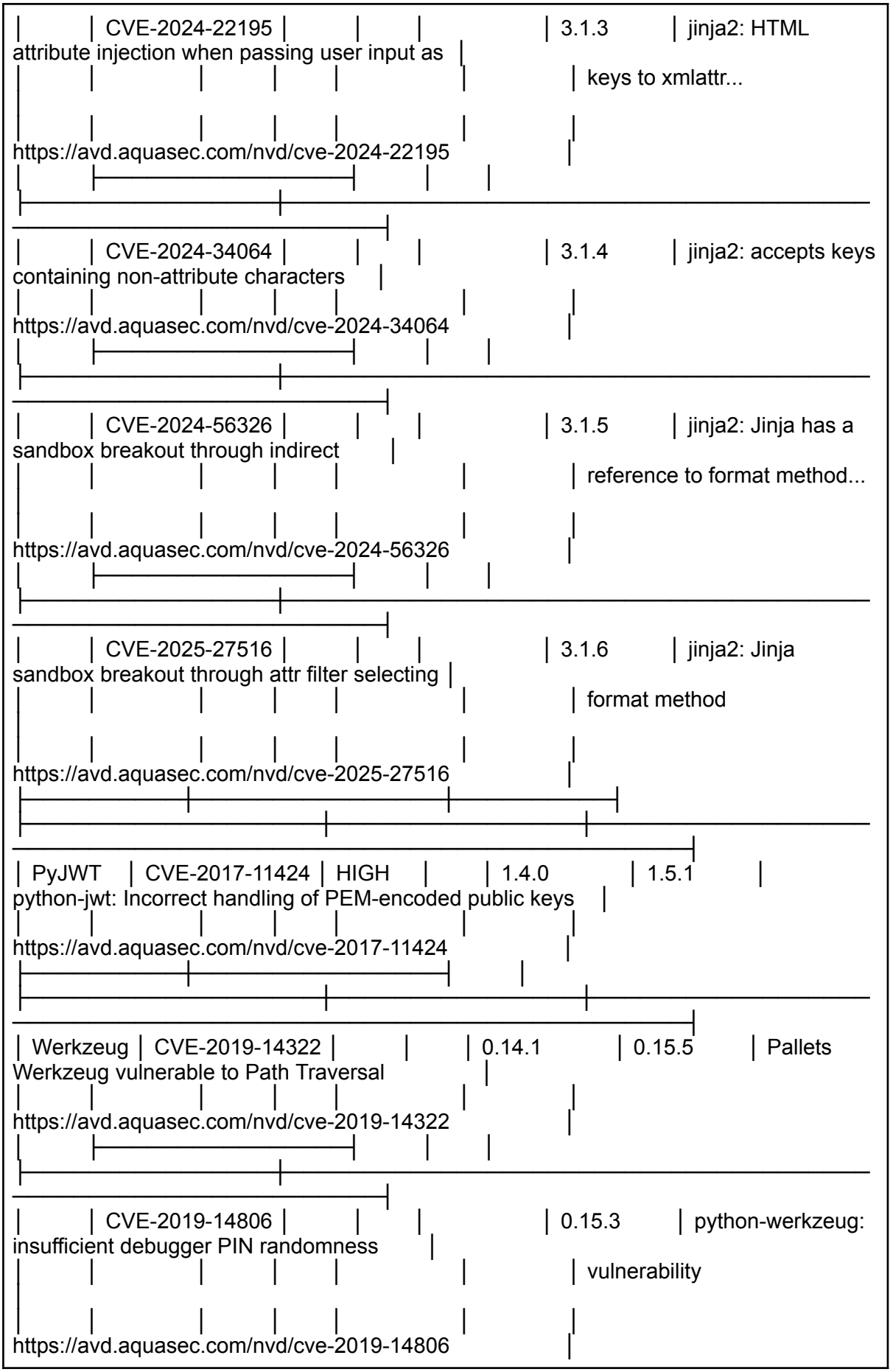
Report Summary

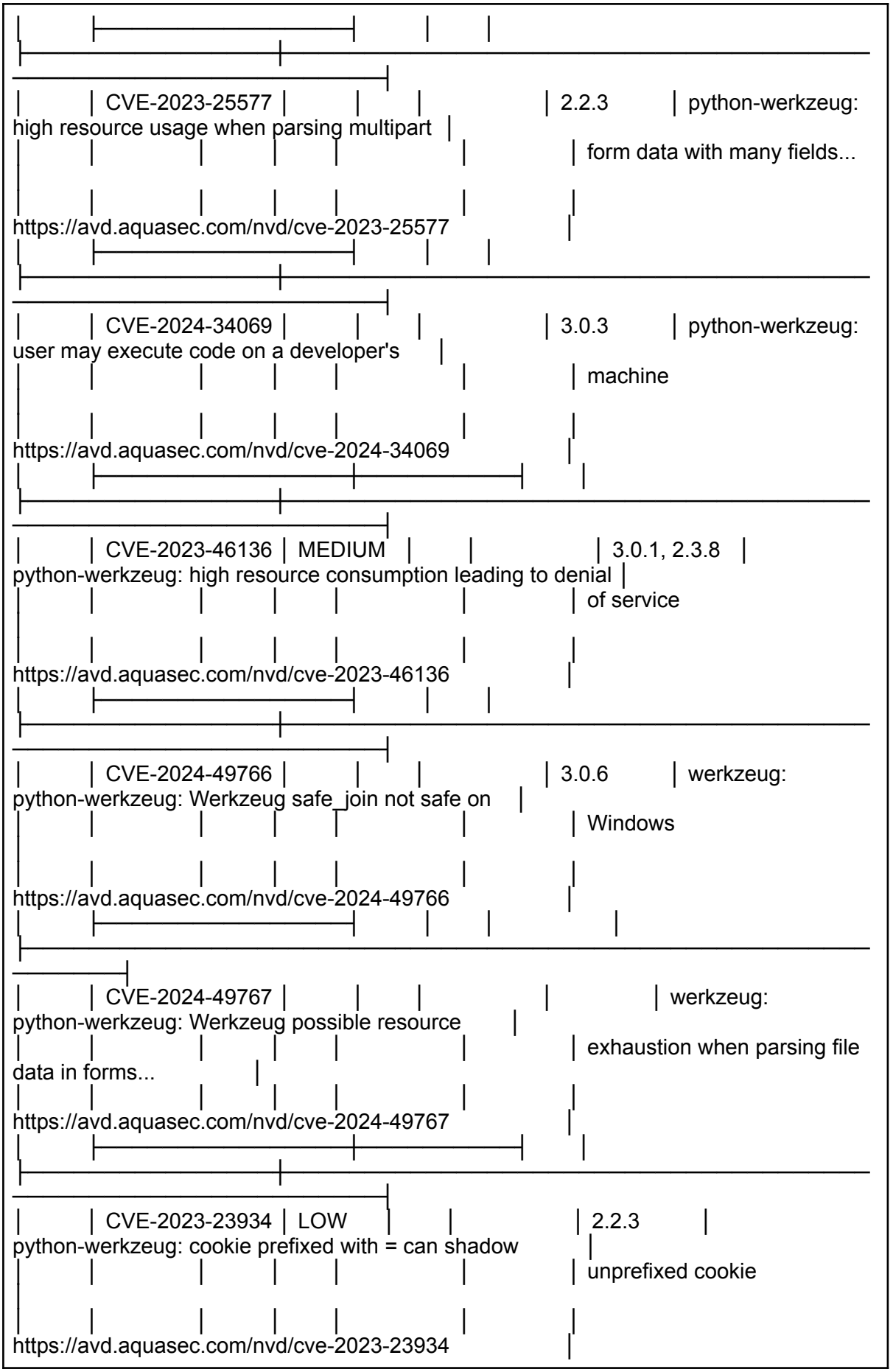
Target	Type	Vulnerabilities
requirements.txt	pip	29

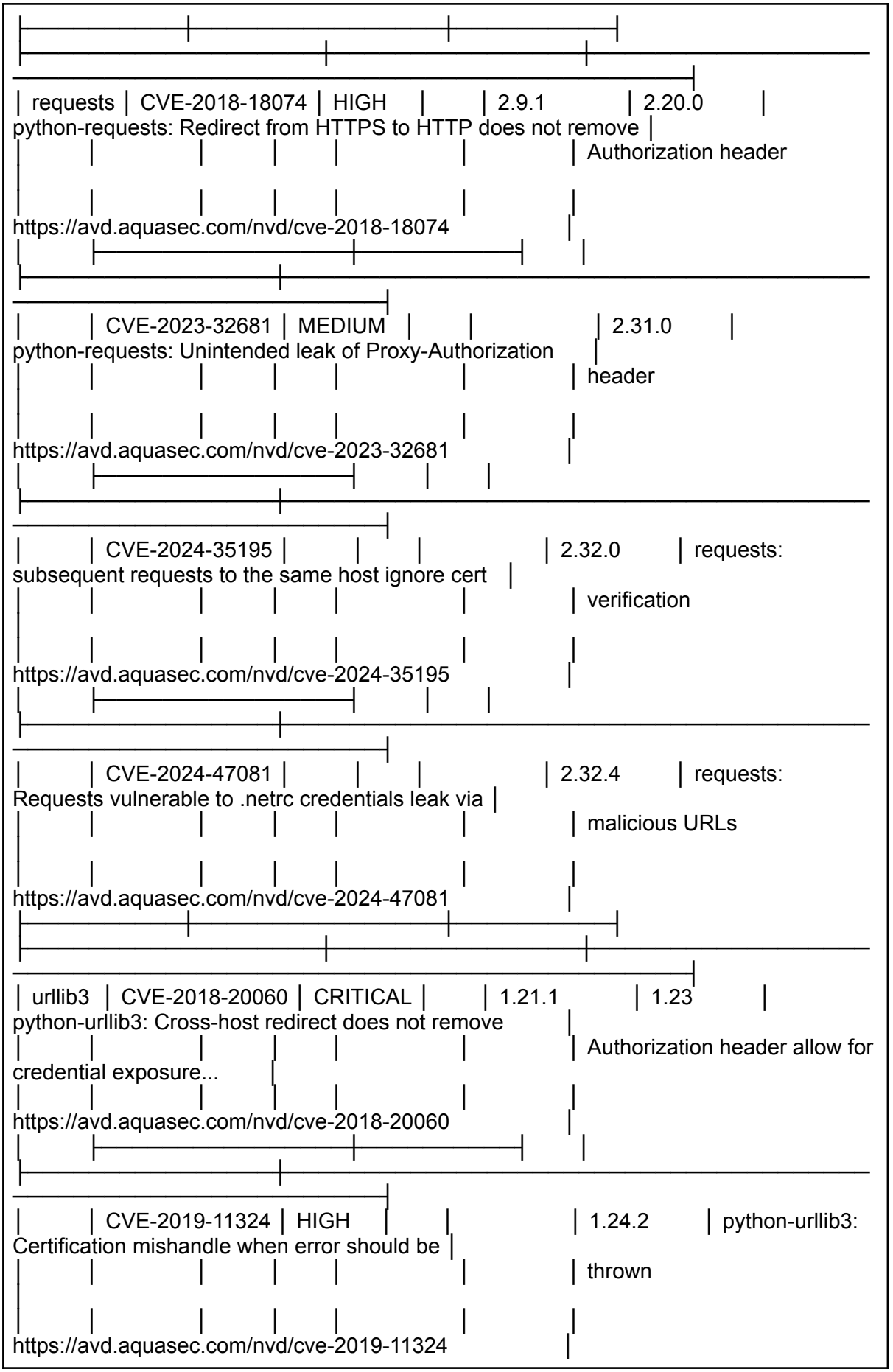
Legend:
- '-': Not scanned
- '0': Clean (no security findings detected)

requirements.txt (pip)
=====================
Total: 29 (UNKNOWN: 0, LOW: 1, MEDIUM: 17, HIGH: 10, CRITICAL: 1)

Library	Vulnerability	Severity	Status	Installed Version	Fixed Version	Title
Flask	CVE-2023-30861	HIGH	fixed	1.0.2	2.3.2, 2.2.5	flask: Possible disclosure of permanent session cookie due to missing Vary: Cookie... https://avd.aquasec.com/nvd/cve-2023-30861
Jinja2	CVE-2019-10906			2.10	2.10.1	python-jinja2: str.format_map allows sandbox escape https://avd.aquasec.com/nvd/cve-2019-10906
	CVE-2020-28493	MEDIUM			2.11.3	python-jinja2: ReDoS vulnerability in the urlize filter https://avd.aquasec.com/nvd/cve-2020-28493


CVE-2024-22195
3.1.3
jinja2: HTML attribute injection when passing user input as keys to xmlattr...
https://avd.aquasec.com/nvd/cve-2024-22195
CVE-2024-34064
3.1.4
jinja2: accepts keys containing non-attribute characters
https://avd.aquasec.com/nvd/cve-2024-34064
CVE-2024-56326
3.1.5
jinja2: Jinja has a sandbox breakout through indirect reference to format method...
https://avd.aquasec.com/nvd/cve-2024-56326
CVE-2025-27516
3.1.6
jinja2: Jinja sandbox breakout through attr filter selecting format method
https://avd.aquasec.com/nvd/cve-2025-27516
PyJWT
CVE-2017-11424
HIGH
1.4.0
1.5.1
python-jwt: Incorrect handling of PEM-encoded public keys
https://avd.aquasec.com/nvd/cve-2017-11424
Werkzeug
CVE-2019-14322
0.14.1
0.15.5
Pallets Werkzeug vulnerable to Path Traversal
https://avd.aquasec.com/nvd/cve-2019-14322
CVE-2019-14806
0.15.3
python-werkzeug: insufficient debugger PIN randomness vulnerability
https://avd.aquasec.com/nvd/cve-2019-14806


CVE-2023-25577
2.2.3
python-werkzeug: high resource usage when parsing multipart form data with many fields...
https://avd.aquasec.com/nvd/cve-2023-25577
CVE-2024-34069
3.0.3
python-werkzeug: user may execute code on a developer's machine
https://avd.aquasec.com/nvd/cve-2024-34069
CVE-2023-46136
MEDIUM
3.0.1, 2.3.8
python-werkzeug: high resource consumption leading to denial of service
https://avd.aquasec.com/nvd/cve-2023-46136
CVE-2024-49766
3.0.6
werkzeug: python-werkzeug: Werkzeug safe_join not safe on Windows
https://avd.aquasec.com/nvd/cve-2024-49766
CVE-2024-49767
werkzeug: python-werkzeug: Werkzeug possible resource exhaustion when parsing file data in forms...
https://avd.aquasec.com/nvd/cve-2024-49767
CVE-2023-23934
LOW
2.2.3
python-werkzeug: cookie prefixed with = can shadow unprefixed cookie
https://avd.aquasec.com/nvd/cve-2023-23934



```
│        ├──────────────────────────┤       │      │
├──────────────────────────┼────────────────────────────────────────────────────────────────────────────────
──────────────────────────────────────┤
│        │ CVE-2023-43804 │        │      │             │ 2.0.6, 1.26.17 │ python-urllib3:
Cookie request header isn't stripped during  │
│        │            │       │      │             │            │ cross-origin redirects
│
│        │            │       │      │             │            │
https://avd.aquasec.com/nvd/cve-2023-43804                    │
│        ├──────────────────────────┼─────────────────┤      │
├──────────────────────────┼────────────────────────────────────────────────────────────────────────────────
──────────────────────────────────────┤
│        │ CVE-2018-25091 │ MEDIUM  │      │             │ 1.24.2       │ urllib3: urllib3
does not remove the authorization HTTP       │
│        │            │       │      │             │            │ header when following a...
│
│        │            │       │      │             │            │
https://avd.aquasec.com/nvd/cve-2018-25091                    │
│        ├──────────────────────────┤       │      │
├──────────────────────────┼────────────────────────────────────────────────────────────────────────────────
──────────────────────────────────────┤
│        │ CVE-2019-11236 │        │      │             │ 1.24.3       │ python-urllib3:
CRLF injection due to not encoding the       │
│        │            │       │      │             │            │ '\r\n' sequence leading to...
│
│        │            │       │      │             │            │
https://avd.aquasec.com/nvd/cve-2019-11236                    │
│        ├──────────────────────────┤       │      │
├──────────────────────────┼────────────────────────────────────────────────────────────────────────────────
──────────────────────────────────────┤
│        │ CVE-2020-26137 │        │      │             │ 1.25.9       │ python-urllib3:
CRLF injection via HTTP request method       │
│        │            │       │      │             │            │
https://avd.aquasec.com/nvd/cve-2020-26137                    │
│        ├──────────────────────────┤       │      │
├──────────────────────────┼────────────────────────────────────────────────────────────────────────────────
──────────────────────────────────────┤
│        │ CVE-2023-45803 │        │      │             │ 2.0.7, 1.26.18 │ urllib3: Request
body not stripped after redirect from 303   │
│        │            │       │      │             │            │ status changes request...
│
│        │            │       │      │             │            │
https://avd.aquasec.com/nvd/cve-2023-45803                    │
│        ├──────────────────────────┤       │      │
├──────────────────────────┼────────────────────────────────────────────────────────────────────────────────
──────────────────────────────────────┤
│        │ CVE-2024-37891 │        │      │             │ 1.26.19, 2.2.2 │ urllib3:
proxy-authorization request header is not stripped  │
│        │            │       │      │             │            │ during cross-origin redirects
│
│        │            │       │      │             │            │
https://avd.aquasec.com/nvd/cve-2024-37891                    │
│        ├──────────────────────────┤       │      │
├──────────────────────────┼────────────────────────────────────────────────────────────────────────────────
```

```
──────────────────────────────────────┤
│         │ CVE-2025-50181 │         │       │                │ 2.5.0          │ urllib3: urllib3
redirects are not disabled when retries are │
│         │                │         │       │                │                │ disabled on PoolManager...
│
│         │                │         │       │                │                │
https://avd.aquasec.com/nvd/cve-2025-50181                    │
└─────────────────┴──────────────────────────┴──────────────┴──────────────┴──────────
──────────────────┴──────────────────────────┴──────────────────────────────────────
──────────────────────────────────────────────┘
```

Escaneo para ver si las vulnerabilidades se fueron (Trivy) **4** [subir al inice]

```
┌──(kali㉿kali)-[~/Downloads/webapp]
└─$ sudo docker run --rm -v $(pwd):/scan aquasec/trivy:latest fs /scan --scanners vuln
[sudo] password for kali:
2025-11-04T01:47:03Z    INFO    [vulndb] Need to update DB
2025-11-04T01:47:03Z    INFO    [vulndb] Downloading vulnerability DB...
2025-11-04T01:47:03Z    INFO    [vulndb] Downloading artifact...
repo="mirror.gcr.io/aquasec/trivy-db:2"
703.17 KiB / 74.14 MiB
[>_____________________________________________________] 0.93% ?
p/s ?2.78 MiB / 74.14 MiB
[-->____________________________________________________] 3.75% ?
p/s ?3.94 MiB / 74.14 MiB
[--->___________________________________________________] 5.31% ?
p/s ?5.31 MiB / 74.14 MiB [--->_____________________________________________________]
7.16% 7.70 MiB p/s ETA 8s6.44 MiB / 74.14 MiB
[---->__________________________________________________] 8.68% 7.70 MiB p/s ETA
8s7.25 MiB / 74.14 MiB [---->_______________________________________________________]
9.78% 7.70 MiB p/s ETA 8s8.81 MiB / 74.14 MiB
[----->_________________________________________________] 11.89% 7.58 MiB p/s ETA
8s9.97 MiB / 74.14 MiB [------>_____________________________________________________]
13.45% 7.58 MiB p/s ETA 8s12.00 MiB / 74.14 MiB
[------->_______________________________________________] 16.18% 7.58 MiB p/s ETA
8s14.12 MiB / 74.14 MiB [--------->_________________________________________________]
19.05% 7.67 MiB p/s ETA 7s15.62 MiB / 74.14 MiB
[---------->____________________________________________] 21.07% 7.67 MiB p/s ETA
7s16.66 MiB / 74.14 MiB [---------->_____________________________________________]
22.47% 7.67 MiB p/s ETA 7s17.72 MiB / 74.14 MiB
[----------->___________________________________________] 23.90% 7.56 MiB p/s ETA
7s18.97 MiB / 74.14 MiB [----------->_____________________________________________] 25.58%
7.56 MiB p/s ETA 7s20.16 MiB / 74.14 MiB
[------------>__________________________________________] 27.19% 7.56 MiB p/s ETA
7s21.09 MiB / 74.14 MiB [------------>_____________________________________________] 28.45%
7.43 MiB p/s ETA 7s22.22 MiB / 74.14 MiB
[------------->_________________________________________] 29.97% 7.43 MiB p/s ETA
6s23.56 MiB / 74.14 MiB [-------------->___________________________________________] 31.78%
7.43 MiB p/s ETA 6s24.72 MiB / 74.14 MiB
[--------------->________________________________________] 33.34% 7.34 MiB p/s ETA 6s28.16
MiB / 74.14 MiB [------------------>_____________________________________] 37.98% 7.34 MiB
p/s ETA 6s28.84 MiB / 74.14 MiB [------------------->____________________________________]
```

38.90% 7.34 MiB p/s ETA 6s30.09 MiB / 74.14 MiB [----------->_____] 40.59% 7.45 MiB p/s ETA 5s31.09 MiB / 74.14 MiB [----------->_____] 41.94% 7.45 MiB p/s ETA 5s32.34 MiB / 74.14 MiB [----------->_____] 43.63% 7.45 MiB p/s ETA 5s33.41 MiB / 74.14 MiB [----------->_____] 45.06% 7.31 MiB p/s ETA 5s34.50 MiB / 74.14 MiB [----------->_____] 46.53% 7.31 MiB p/s ETA 5s36.37 MiB / 74.14 MiB [----------->_____] 49.06% 7.31 MiB p/s ETA 5s37.66 MiB / 74.14 MiB [----------->_____] 50.79% 7.31 MiB p/s ETA 4s38.72 MiB / 74.14 MiB [----------->_____] 52.22% 7.31 MiB p/s ETA 4s39.69 MiB / 74.14 MiB [----------->_____] 53.53% 7.31 MiB p/s ETA 4s41.53 MiB / 74.14 MiB [----------->_____] 56.02% 7.25 MiB p/s ETA 4s44.25 MiB / 74.14 MiB [----------->_____] 59.68% 7.25 MiB p/s ETA 4s46.47 MiB / 74.14 MiB [----------->_____] 62.68% 7.25 MiB p/s ETA 3s48.53 MiB / 74.14 MiB [----------->_____] 65.46% 7.55 MiB p/s ETA 3s50.16 MiB / 74.14 MiB [----------->_____] 67.65% 7.55 MiB p/s ETA 3s51.84 MiB / 74.14 MiB [----------->_____] 69.93% 7.55 MiB p/s ETA 2s52.84 MiB / 74.14 MiB [----------->_____] 71.28% 7.52 MiB p/s ETA 2s54.84 MiB / 74.14 MiB [----------->_____] 73.97% 7.52 MiB p/s ETA 2s56.22 MiB / 74.14 MiB [----------->_____] 75.83% 7.52 MiB p/s ETA 2s57.50 MiB / 74.14 MiB [----------->_____] 77.56% 7.54 MiB p/s ETA 2s58.59 MiB / 74.14 MiB [----------->_____] 79.03% 7.54 MiB p/s ETA 2s59.25 MiB / 74.14 MiB [----------->_____] 79.92% 7.54 MiB p/s ETA 1s60.12 MiB / 74.14 MiB [----------->_____] 81.10% 7.33 MiB p/s ETA 1s60.81 MiB / 74.14 MiB [----------->_____] 82.02% 7.33 MiB p/s ETA 1s62.16 MiB / 74.14 MiB [----------->_____] 83.84% 7.33 MiB p/s ETA 1s63.37 MiB / 74.14 MiB [----------->_____] 85.48% 7.21 MiB p/s ETA 1s64.56 MiB / 74.14 MiB [----------->_____] 87.08% 7.21 MiB p/s ETA 1s66.66 MiB / 74.14 MiB [----------->____] 89.91% 7.21 MiB p/s ETA 1s68.12 MiB / 74.14 MiB [----------->___] 91.89% 7.26 MiB p/s ETA 0s68.97 MiB / 74.14 MiB [----------->___] 93.03% 7.26 MiB p/s ETA 0s70.28 MiB / 74.14 MiB [----------->__] 94.80% 7.26 MiB p/s ETA 0s72.62 MiB / 74.14 MiB [----------->_] 97.96% 7.28 MiB p/s ETA 0s74.14 MiB / 74.14 MiB [----------->] 100.00% 6.99 MiB p/s ETA 0s74.14 MiB / 74.14 MiB [----------->] 100.00% 6.99 MiB p/s ETA 0s74.14 MiB / 74.14 MiB [----------->] 100.00% 6.99 MiB p/s ETA 0s74.14 MiB / 74.14 MiB [----------->] 100.00% 6.54 MiB p/s ETA 0s74.14 MiB / 74.14 MiB [----------->] 100.00% 6.54 MiB p/s ETA 0s74.14 MiB / 74.14 MiB [----------->] 100.00% 6.12 MiB p/s ETA 0s74.14 MiB / 74.14 MiB [----------->] 100.00% 6.12 MiB p/s ETA 0s74.14 MiB / 74.14 MiB [----------->] 100.00% 6.12 MiB p/s ETA 0s74.14 MiB / 74.14 MiB [----------->] 100.00% 6.12 MiB p/s ETA 0s74.14 MiB / 74.14 MiB [----------->] 100.00% 5.72 MiB p/s ETA 0s74.14 MiB / 74.14 MiB [----------->] 100.00% 5.72 MiB p/s ETA 0s74.14 MiB / 74.14 MiB [----------->] 100.00% 5.72 MiB p/s ETA 0s74.14 MiB / 74.14 MiB [----------->] 100.00% 5.36 MiB p/s ETA 0s74.14 MiB / 74.14 MiB [----------->] 100.00% 5.36 MiB p/s ETA 0s74.14 MiB / 74.14 MiB [----------->] 100.00% 5.36 MiB

```
p/s ETA 0s74.14 MiB / 74.14 MiB [-------------------------------------------->] 100.00% 5.01
MiB p/s ETA 0s74.14 MiB / 74.14 MiB [-------------------------------------------->] 100.00%
5.01 MiB p/s ETA 0s74.14 MiB / 74.14 MiB [-------------------------------------------->]
100.00% 5.01 MiB p/s ETA 0s74.14 MiB / 74.14 MiB
[-------------------------------------------->] 100.00% 4.69 MiB p/s ETA 0s74.14 MiB / 74.14
MiB [-------------------------------------------->] 100.00% 4.69 MiB p/s ETA 0s74.14 MiB /
74.14 MiB [-------------------------------------------->] 100.00% 4.69 MiB p/s ETA 0s74.14 MiB
/ 74.14 MiB [-------------------------------------------->] 100.00% 4.38 MiB p/s ETA 0s74.14
MiB / 74.14 MiB [-------------------------------------------->] 100.00% 4.38 MiB p/s ETA
0s74.14 MiB / 74.14 MiB [-------------------------------------------->] 100.00% 4.38 MiB p/s
ETA 0s74.14 MiB / 74.14 MiB [-------------------------------------------->] 100.00% 4.10 MiB
p/s ETA 0s74.14 MiB / 74.14 MiB [-------------------------------------------->] 100.00% 4.10
MiB p/s ETA 0s74.14 MiB / 74.14 MiB [-------------------------------------------->] 100.00%
4.10 MiB p/s ETA 0s74.14 MiB / 74.14 MiB [-------------------------------------------->]
100.00% 3.84 MiB p/s ETA 0s74.14 MiB / 74.14 MiB
[-------------------------------------------->] 100.00% 3.84 MiB p/s ETA 0s74.14 MiB / 74.14
MiB [-------------------------------------------->] 100.00% 3.84 MiB p/s ETA 0s74.14 MiB /
74.14 MiB [-------------------------------------------->] 100.00% 3.59 MiB p/s ETA 0s74.14 MiB
/ 74.14 MiB [-------------------------------------------->] 100.00% 3.59 MiB p/s ETA 0s74.14
MiB / 74.14 MiB [-------------------------------------------->] 100.00% 3.59 MiB p/s ETA
0s74.14 MiB / 74.14 MiB [-------------------------------------------->] 100.00% 3.36 MiB p/s
ETA 0s74.14 MiB / 74.14 MiB [-------------------------------------------->] 100.00% 3.36 MiB
p/s ETA 0s74.14 MiB / 74.14 MiB [-------------------------------------------->] 100.00% 3.36
MiB p/s ETA 0s74.14 MiB / 74.14 MiB [-------------------------------------------->] 100.00%
3.14 MiB p/s ETA 0s74.14 MiB / 74.14 MiB [-------------------------------------------->]
100.00% 3.14 MiB p/s ETA 0s74.14 MiB / 74.14 MiB
[-------------------------------------------->] 100.00% 3.14 MiB p/s ETA 0s74.14 MiB / 74.14
MiB [-------------------------------------------->] 100.00% 2.94 MiB p/s ETA 0s74.14 MiB /
74.14 MiB [-------------------------------------------->] 100.00% 2.94 MiB p/s ETA 0s74.14 MiB
/ 74.14 MiB [-------------------------------------------->] 100.00% 2.94 MiB p/s ETA 0s74.14
MiB / 74.14 MiB [-------------------------------------------->] 100.00% 2.75 MiB p/s ETA
0s74.14 MiB / 74.14 MiB [-------------------------------------------->] 100.00% 2.75 MiB p/s
ETA 0s74.14 MiB / 74.14 MiB [-------------------------------------------->] 100.00% 2.75 MiB
p/s ETA 0s74.14 MiB / 74.14 MiB [-------------------------------------------->] 100.00% 2.75
MiB p/s ETA 0s74.14 MiB / 74.14 MiB [-------------------------------------------->] 100.00%
2.57 MiB p/s ETA 0s74.14 MiB / 74.14 MiB [-------------------------------------------->]
100.00% 2.57 MiB p/s ETA 0s74.14 MiB / 74.14 MiB
[-------------------------------------------->] 100.00% 2.57 MiB p/s ETA 0s74.14 MiB / 74.14
MiB [-------------------------------------------->] 100.00% 2.41 MiB p/s ETA 0s74.14 MiB /
74.14 MiB [-------------------------------------------->] 100.00% 2.41 MiB p/s ETA 0s74.14 MiB
/ 74.14 MiB [-------------------------------------------->] 100.00% 2.41 MiB p/s ETA 0s74.14
MiB / 74.14 MiB [-------------------------------------------->] 100.00% 2.25 MiB p/s ETA
0s74.14 MiB / 74.14 MiB [-------------------------------------------->] 100.00% 2.25 MiB p/s
ETA 0s74.14 MiB / 74.14 MiB [-------------------------------------------->] 100.00% 2.25 MiB
p/s ETA 0s74.14 MiB / 74.14 MiB [-------------------------------------------->] 100.00% 2.11
MiB p/s ETA 0s74.14 MiB / 74.14 MiB [-------------------------------------------->] 100.00%
2.11 MiB p/s ETA 0s74.14 MiB / 74.14 MiB [-------------------------------------------->]
100.00% 2.11 MiB p/s ETA 0s74.14 MiB / 74.14 MiB
[-------------------------------------------->] 100.00% 1.97 MiB p/s ETA 0s74.14 MiB / 74.14
MiB [-------------------------------------------->] 100.00% 1.97 MiB p/s ETA 0s74.14 MiB /
74.14 MiB [-------------------------------------------->] 100.00% 1.97 MiB p/s ETA 0s74.14 MiB
/ 74.14 MiB [----------------------------------------------] 100.00% 3.18 MiB p/s
23s2025-11-04T01:47:31Z  INFO    [vulndb] Artifact successfully downloaded
repo="mirror.gcr.io/aquasec/trivy-db:2"
```

```
2025-11-04T01:47:31Z    INFO    [vuln] Vulnerability scanning is enabled
2025-11-04T01:47:31Z    WARN    [pip] Unable to find python `site-packages` directory.
License detection is skipped.      err="unable to find path to Python executable"
2025-11-04T01:47:31Z    INFO    Number of language-specific files       num=1
2025-11-04T01:47:31Z    INFO    [pip] Detecting vulnerabilities...

Report Summary

┌──────────────────┬──────┬─────────────────┐
│      Target      │ Type │ Vulnerabilities │
├──────────────────┼──────┼─────────────────┤
│ requirements.txt │ pip  │        1        │
└──────────────────┴──────┴─────────────────┘

Legend:
- '-': Not scanned
- '0': Clean (no security findings detected)


requirements.txt (pip)
======================
Total: 1 (UNKNOWN: 0, LOW: 0, MEDIUM: 0, HIGH: 1, CRITICAL: 0)

┌─────────┬────────────────┬──────────┬────────┬───────────────────┬───────────────┬──────────────────────────────────────────────────────────────┐
│ Library │ Vulnerability  │ Severity │ Status │ Installed Version │ Fixed Version │                            Title                             │
├─────────┼────────────────┼──────────┼────────┼───────────────────┼───────────────┼──────────────────────────────────────────────────────────────┤
│ PyJWT   │ CVE-2022-29217 │ HIGH     │ fixed  │ 1.5.1             │ 2.4.0         │ python-jwt: Key confusion through non-blocklisted public key │
│         │                │          │        │                   │               │ formats                                                      │
│         │                │          │        │                   │               │                                                              │
│         │                │          │        │                   │               │ https://avd.aquasec.com/nvd/cve-2022-29217                   │
└─────────┴────────────────┴──────────┴────────┴───────────────────┴───────────────┴──────────────────────────────────────────────────────────────┘
```

Escaneo con Trivy para ver si esa vulnerabilidad HIGH de PyJWT se fue **5** **volver al indice**

```
┌──(kali㉿kali)-[~/Downloads/webapp]
└─$ sudo docker run --rm -v $(pwd):/scan aquasec/trivy:latest fs /scan --scanners vuln
[sudo] password for kali:
2025-11-04T02:07:01Z    INFO    [vulndb] Need to update DB
2025-11-04T02:07:01Z    INFO    [vulndb] Downloading vulnerability DB...
2025-11-04T02:07:01Z    INFO    [vulndb] Downloading artifact...
repo="mirror.gcr.io/aquasec/trivy-db:2"
991.17 KiB / 74.14 MiB
[>_____________________________________________________] 1.31% ? p/s ?3.09 MiB / 74.14 MiB
```

[-->_____] 4.17% ? p/s ?5.31 MiB / 74.14 MiB
[---->_____] 7.16% ? p/s ?8.09 MiB / 74.14 MiB [----->_____] 10.92% 11.89 MiB p/s ETA 5s10.22 MiB / 74.14 MiB
[------>_____] 13.78% 11.89 MiB p/s ETA 5s13.84 MiB / 74.14 MiB [-------->_____] 18.67% 11.89 MiB p/s ETA 5s15.56 MiB / 74.14 MiB
[---------->_____] 20.99% 11.92 MiB p/s ETA 4s17.87 MiB / 74.14 MiB [---------->_____] 24.11% 11.92 MiB p/s ETA 4s22.22 MiB / 74.14 MiB
[---------->_____] 29.97% 11.92 MiB p/s ETA 4s24.09 MiB / 74.14 MiB [---------->_____] 32.50% 12.07 MiB p/s ETA 4s25.53 MiB / 74.14 MiB
[---------->_____] 34.44% 12.07 MiB p/s ETA 4s27.00 MiB / 74.14 MiB [---------->_____] 36.42% 12.07 MiB p/s ETA 3s28.19 MiB / 74.14 MiB [---------->_____] 38.02% 11.73 MiB p/s ETA 3s29.31 MiB / 74.14 MiB
[---------->_____] 39.54% 11.73 MiB p/s ETA 3s31.22 MiB / 74.14 MiB [---------->_____] 42.11% 11.73 MiB p/s ETA 3s32.91 MiB / 74.14 MiB [---------->_____] 44.38% 11.48 MiB p/s ETA 3s34.41 MiB / 74.14 MiB
[---------->_____] 46.41% 11.48 MiB p/s ETA 3s36.53 MiB / 74.14 MiB [---------->_____] 49.27% 11.48 MiB p/s ETA 3s38.00 MiB / 74.14 MiB [---------->_____] 51.25% 11.29 MiB p/s ETA 3s40.12 MiB / 74.14 MiB
[---------->_____] 54.12% 11.29 MiB p/s ETA 3s41.66 MiB / 74.14 MiB [---------->_____] 56.19% 11.29 MiB p/s ETA 2s43.81 MiB / 74.14 MiB [---------->_____] 59.09% 11.18 MiB p/s ETA 2s45.16 MiB / 74.14 MiB [---------->_____] 60.91% 11.18 MiB p/s ETA 2s46.69 MiB / 74.14 MiB
[---------->_____] 62.97% 11.18 MiB p/s ETA 2s47.59 MiB / 74.14 MiB [---------->_____] 64.20% 10.87 MiB p/s ETA 2s48.03 MiB / 74.14 MiB [---------->_____] 64.79% 10.87 MiB p/s ETA 2s49.22 MiB / 74.14 MiB [---------->_____] 66.39% 10.87 MiB p/s ETA 2s50.59 MiB / 74.14 MiB [---------->_____] 68.24% 10.49 MiB p/s ETA 2s52.37 MiB / 74.14 MiB
[---------->_____] 70.64% 10.49 MiB p/s ETA 2s54.06 MiB / 74.14 MiB [---------->_____] 72.92% 10.49 MiB p/s ETA 1s56.62 MiB / 74.14 MiB [---------->_____] 76.38% 10.46 MiB p/s ETA 1s57.94 MiB / 74.14 MiB [---------->_____] 78.15% 10.46 MiB p/s ETA 1s59.16 MiB / 74.14 MiB [---------->_____] 79.79% 10.46 MiB p/s ETA 1s60.75 MiB / 74.14 MiB
[---------->_____] 81.94% 10.23 MiB p/s ETA 1s61.94 MiB / 74.14 MiB [---------->_____] 83.54% 10.23 MiB p/s ETA 1s63.25 MiB / 74.14 MiB [---------->_____] 85.31% 10.23 MiB p/s ETA 1s64.47 MiB / 74.14 MiB [---------->_____] 86.96% 9.97 MiB p/s ETA 0s65.59 MiB / 74.14 MiB [---------->_____] 88.47% 9.97 MiB p/s ETA 0s66.91 MiB / 74.14 MiB [---------->_____] 90.24% 9.97 MiB p/s ETA 0s68.34 MiB / 74.14 MiB [---------->_____] 92.18% 9.75 MiB p/s ETA 0s69.66 MiB / 74.14 MiB [---------->_____] 93.95% 9.75 MiB p/s ETA 0s71.87 MiB / 74.14 MiB [---------->_____] 96.95% 9.75 MiB p/s ETA 0s74.14 MiB / 74.14 MiB [----------] 100.00% 9.48 MiB p/s ETA 0s74.14 MiB / 74.14 MiB

[--->] 100.00% 8.87 MiB p/s ETA 0s74.14 MiB / 74.14 MiB [--->] 100.00% 8.87 MiB p/s ETA 0s74.14 MiB / 74.14 MiB [--->] 100.00% 8.30 MiB p/s ETA 0s74.14 MiB / 74.14 MiB [--->] 100.00% 8.30 MiB p/s ETA 0s74.14 MiB / 74.14 MiB [--->] 100.00% 8.30 MiB p/s ETA 0s74.14 MiB / 74.14 MiB [--->] 100.00% 7.76 MiB p/s ETA 0s74.14 MiB / 74.14 MiB [--->] 100.00% 7.76 MiB p/s ETA 0s74.14 MiB / 74.14 MiB [--->] 100.00% 7.76 MiB p/s ETA 0s74.14 MiB / 74.14 MiB [--->] 100.00% 7.26 MiB p/s ETA 0s74.14 MiB / 74.14 MiB [--->] 100.00% 7.26 MiB p/s ETA 0s74.14 MiB / 74.14 MiB [--->] 100.00% 7.26 MiB p/s ETA 0s74.14 MiB / 74.14 MiB [--->] 100.00% 6.79 MiB p/s ETA 0s74.14 MiB / 74.14 MiB [--->] 100.00% 6.79 MiB p/s ETA 0s74.14 MiB / 74.14 MiB [--->] 100.00% 6.79 MiB p/s ETA 0s74.14 MiB / 74.14 MiB [--->] 100.00% 6.35 MiB p/s ETA 0s74.14 MiB / 74.14 MiB [--->] 100.00% 6.35 MiB p/s ETA 0s74.14 MiB / 74.14 MiB [--->] 100.00% 6.35 MiB p/s ETA 0s74.14 MiB / 74.14 MiB [--->] 100.00% 5.94 MiB p/s ETA 0s74.14 MiB / 74.14 MiB [--->] 100.00% 5.94 MiB p/s ETA 0s74.14 MiB / 74.14 MiB [--->] 100.00% 5.94 MiB p/s ETA 0s74.14 MiB / 74.14 MiB [--->] 100.00% 5.56 MiB p/s ETA 0s74.14 MiB / 74.14 MiB [--->] 100.00% 5.56 MiB p/s ETA 0s74.14 MiB / 74.14 MiB [--->] 100.00% 5.56 MiB p/s ETA 0s74.14 MiB / 74.14 MiB [--->] 100.00% 5.20 MiB p/s ETA 0s74.14 MiB / 74.14 MiB [--->] 100.00% 5.20 MiB p/s ETA 0s74.14 MiB / 74.14 MiB [--->] 100.00% 5.20 MiB p/s ETA 0s74.14 MiB / 74.14 MiB [--->] 100.00% 4.87 MiB p/s ETA 0s74.14 MiB / 74.14 MiB [--->] 100.00% 4.87 MiB p/s ETA 0s74.14 MiB / 74.14 MiB [--->] 100.00% 4.87 MiB p/s ETA 0s74.14 MiB / 74.14 MiB [--->] 100.00% 4.55 MiB p/s ETA 0s74.14 MiB / 74.14 MiB [--->] 100.00% 4.55 MiB p/s ETA 0s74.14 MiB / 74.14 MiB [--->] 100.00% 4.55 MiB p/s ETA 0s74.14 MiB / 74.14 MiB [--->] 100.00% 4.26 MiB p/s ETA 0s74.14 MiB / 74.14 MiB [--->] 100.00% 4.26 MiB p/s ETA 0s74.14 MiB / 74.14 MiB [--->] 100.00% 4.26 MiB p/s ETA 0s74.14 MiB / 74.14 MiB [--->] 100.00% 3.98 MiB p/s ETA 0s74.14 MiB / 74.14 MiB [--->] 100.00% 3.98 MiB p/s ETA 0s74.14 MiB / 74.14 MiB [--->] 100.00% 3.98 MiB p/s ETA 0s74.14 MiB / 74.14 MiB [--->] 100.00% 3.73 MiB p/s ETA 0s74.14 MiB / 74.14 MiB [--->] 100.00% 3.73 MiB p/s ETA 0s74.14 MiB / 74.14 MiB [--->] 100.00% 3.73 MiB p/s ETA 0s74.14 MiB / 74.14 MiB [--->] 100.00% 3.73 MiB p/s ETA 0s74.14 MiB / 74.14 MiB [--->] 100.00% 3.49 MiB p/s ETA 0s74.14 MiB / 74.14 MiB [--->] 100.00% 3.49 MiB p/s ETA 0s74.14 MiB / 74.14 MiB [--->] 100.00% 3.49 MiB p/s ETA 0s74.14 MiB / 74.14 MiB [--->] 100.00% 3.26 MiB p/s ETA 0s74.14 MiB / 74.14 MiB [--->] 100.00% 3.26 MiB p/s ETA 0s74.14 MiB / 74.14 MiB [--->] 100.00% 3.26 MiB p/s ETA 0s74.14 MiB / 74.14 MiB [--->] 100.00% 3.05 MiB p/s ETA 0s74.14 MiB / 74.14 MiB [--->]

```
100.00% 3.05 MiB p/s ETA 0s74.14 MiB / 74.14 MiB
[---------------------------------------->] 100.00% 3.05 MiB p/s ETA 0s74.14 MiB / 74.14
MiB [---------------------------------------->] 100.00% 2.85 MiB p/s ETA 0s74.14 MiB /
74.14 MiB [---------------------------------------->] 100.00% 2.85 MiB p/s ETA 0s74.14 MiB
/ 74.14 MiB [---------------------------------------->] 100.00% 2.85 MiB p/s ETA 0s74.14
MiB / 74.14 MiB [---------------------------------------->] 100.00% 2.67 MiB p/s ETA
0s74.14 MiB / 74.14 MiB [---------------------------------------->] 100.00% 2.67 MiB p/s
ETA 0s74.14 MiB / 74.14 MiB [----------------------------------------------] 100.00% 3.40 MiB
p/s 22s2025-11-04T02:07:27Z        INFO    [vulndb] Artifact successfully downloaded
repo="mirror.gcr.io/aquasec/trivy-db:2"
2025-11-04T02:07:27Z    INFO    [vuln] Vulnerability scanning is enabled
2025-11-04T02:07:27Z    WARN    [pip] Unable to find python `site-packages` directory.
License detection is skipped.      err="unable to find path to Python executable"
2025-11-04T02:07:27Z    INFO    Number of language-specific files       num=1
2025-11-04T02:07:27Z    INFO    [pip] Detecting vulnerabilities...

Report Summary

┌──────────────────┬──────┬─────────────────┐
│      Target      │ Type │ Vulnerabilities │
├──────────────────┼──────┼─────────────────┤
│ requirements.txt │ pip  │        0        │
└──────────────────┴──────┴─────────────────┘

Legend:
- '-': Not scanned
- '0': Clean (no security findings detected)
```

Escaneo con Trivy el Dockerfile para buscar las malas configuraciones. **6** **subir al indice**

```
┌──(kali㉿kali)-[~/Downloads/webapp]
└─$ sudo docker run --rm -v $(pwd):/scan aquasec/trivy:latest config /scan
[sudo] password for kali:
2025-11-04T02:34:13Z    INFO    [misconfig] Misconfiguration scanning is enabled
2025-11-04T02:34:13Z    INFO    [misconfig] Need to update the checks bundle
2025-11-04T02:34:13Z    INFO    [misconfig] Downloading the checks bundle...
165.46 KiB / 165.46 KiB [---------------------------------------------------------->] 100.00% ? p/s
?165.46 KiB / 165.46 KiB [----------------------------------------] 100.00% 1006.94 KiB p/s
500ms2025-11-04T02:34:20Z        INFO    Detected config files     num=1

Report Summary

┌────────────┬────────────┬──────────────────┐
│   Target   │    Type    │ Misconfigurations │
├────────────┼────────────┼──────────────────┤
│ Dockerfile │ dockerfile │        11        │
└────────────┴────────────┴──────────────────┘

Legend:
- '-': Not scanned
- '0': Clean (no security findings detected)


Dockerfile (dockerfile)
=======================
```

Tests: 33 (SUCCESSES: 22, FAILURES: 11)
Failures: 11 (UNKNOWN: 0, LOW: 1, MEDIUM: 1, HIGH: 2, CRITICAL: 7)

AVD-DS-0002 (HIGH): Last USER command in Dockerfile should not be 'root'

Running containers with 'root' user can lead to a container escape situation. It is a best practice to run containers as non-root users, which can be done by adding a 'USER' statement to the Dockerfile.

See https://avd.aquasec.com/misconfig/ds002

Dockerfile:3

```
3 [ USER root
```

AVD-DS-0004 (MEDIUM): Port 22 should not be exposed in Dockerfile

Exposing port 22 might allow users to SSH into the container.

See https://avd.aquasec.com/misconfig/ds004

Dockerfile:46

```
46 [ EXPOSE 22 3306 5432 6379
```

AVD-DS-0026 (LOW): Add HEALTHCHECK instruction in your Dockerfile

You should add HEALTHCHECK instruction in your docker container images to perform the health check on running containers.

See https://avd.aquasec.com/misconfig/ds026

AVD-DS-0029 (HIGH): '--no-install-recommends' flag is missed: 'apt-get update && apt-get install -y curl wget openssl sqlite3 sudo && rm -rf /var/lib/apt/lists/*'

'apt-get' install should use '--no-install-recommends' to minimize image size.

See https://avd.aquasec.com/misconfig/ds029

Dockerfile:17-23

```
17 ┌ RUN apt-get update && apt-get install -y \
18 │     curl \
19 │     wget \
20 │     openssl \
21 │     sqlite3 \
22 │     sudo \
23 └     && rm -rf /var/lib/apt/lists/*
```

AVD-DS-0031 (CRITICAL): Possible exposure of secret env "ADMIN_PASSWORD" in ENV

Passing secrets via `build-args` or envs or copying secret files can leak them out

See https://avd.aquasec.com/misconfig/ds031

Dockerfile:8

8 [ENV ADMIN_PASSWORD="admin123"

AVD-DS-0031 (CRITICAL): Possible exposure of secret env "API_TOKEN" in ENV

Passing secrets via `build-args` or envs or copying secret files can leak them out

See https://avd.aquasec.com/misconfig/ds031

Dockerfile:7

7 [ENV API_TOKEN="sk-1234567890abcdef"

AVD-DS-0031 (CRITICAL): Possible exposure of secret env "AWS_SECRET_KEY" in ENV

Passing secrets via `build-args` or envs or copying secret files can leak them out

See https://avd.aquasec.com/misconfig/ds031

Dockerfile:11

11 [ENV AWS_SECRET_KEY="AKIAJ38KSL4DJEKJ34EKLJDFJ3498844X"

AVD-DS-0031 (CRITICAL): Possible exposure of secret env "DATABASE_PASSWORD" in ENV

Passing secrets via `build-args` or envs or copying secret files can leak them out

See https://avd.aquasec.com/misconfig/ds031

Dockerfile:6

6 [ENV DATABASE_PASSWORD="password123"

AVD-DS-0031 (CRITICAL): Possible exposure of secret env "ENCRYPTION_KEY" in ENV

Passing secrets via `build-args` or envs or copying secret files can leak them out

See https://avd.aquasec.com/misconfig/ds031

Dockerfile:10

10 [ENV ENCRYPTION_KEY="encryption_key_12345"

AVD-DS-0031 (CRITICAL): Possible exposure of secret env "JWT_SECRET" in ENV

Passing secrets via `build-args` or envs or copying secret files can leak them out

See https://avd.aquasec.com/misconfig/ds031

Dockerfile:9

9 [ENV JWT_SECRET="jwt_secret_key"

AVD-DS-0031 (CRITICAL): Possible exposure of secret env "SECRET_KEY" in ENV

Passing secrets via `build-args` or envs or copying secret files can leak them out

See https://avd.aquasec.com/misconfig/ds031

Dockerfile:5

5 [ENV SECRET_KEY="super_secret_key_123456"