**CLOUD SECURITY TOOLS REPORT**

**GROUP SIX (6)**

Cloud security tools are technologies and solutions intended to safeguard cloud environments, encompassing infrastructure, platforms, or applications; by assuring the security of data, workloads, and services against attacks, misconfigurations, and illegal access. These technologies assist enterprises in mitigating risks such as data breaches, insider threats, compliance violations, and insecure APIs, while offering visibility and control over resources across public, private, or hybrid cloud environments.

Fundamentally, cloud security tools adhere to the **CIA triad**: **Confidentiality**, which ensures that sensitive information is accessible solely to authorized individuals. **Integrity**, which preserves the accuracy and reliability of data and configurations and finally, **Availability**, which ensures that cloud resources and services are consistently accessible as required.

Furthermore, by adhering to the CIA trinity, cloud security products offer a comprehensive framework for protecting cloud-based assets while facilitating business continuity and ensuring regulatory compliance. In order to achieve the principles of the CIA triad in a cloud-based environment, we will examine some fundamental operations namely Cloud Security Posture Management (CSPM), Cloud Access Security Brokers (CASB), and Container Security Tools, along with the specific tools used to implement them. (Hougen, 2025)

***PRERIQUISTS TO PERFORM CLOUD SECURITY OPERATION***

Cloud security operations may include some important prerequisites before doing them. Usually, such prerequisites fall under mainly four different categories.

1. **Access and permissions** – A person need access and permissions on some cloud platform like AWS, Azure, or Google Cloud Platform, at least with a degree of administrative permission or security permission to really configure the security settings, deploy the tools, and see the logs of security. Like ion this report we will solely use AWS cloud provider.
2. **Create cloud account and set up environments** – Active services are part of a well-organized configured cloud account with virtualization, storage, or container resources that enable a proper environment for actual securing and monitoring.
3. **Tools and Integrations for Security** – The necessary tools, e.g., CSPM platforms, CASBs, or container security solutions, that generally make up a security operation must be there or installed for scanning, monitoring, or enforcement.
4. **Basic Knowledge and Skills** – The understanding of cloud architecture at the most rudimentary level, fundamentals of IAM, networking, and security, including the CIA Triad, would be an advantage to explain the results fetched properly and best practices.

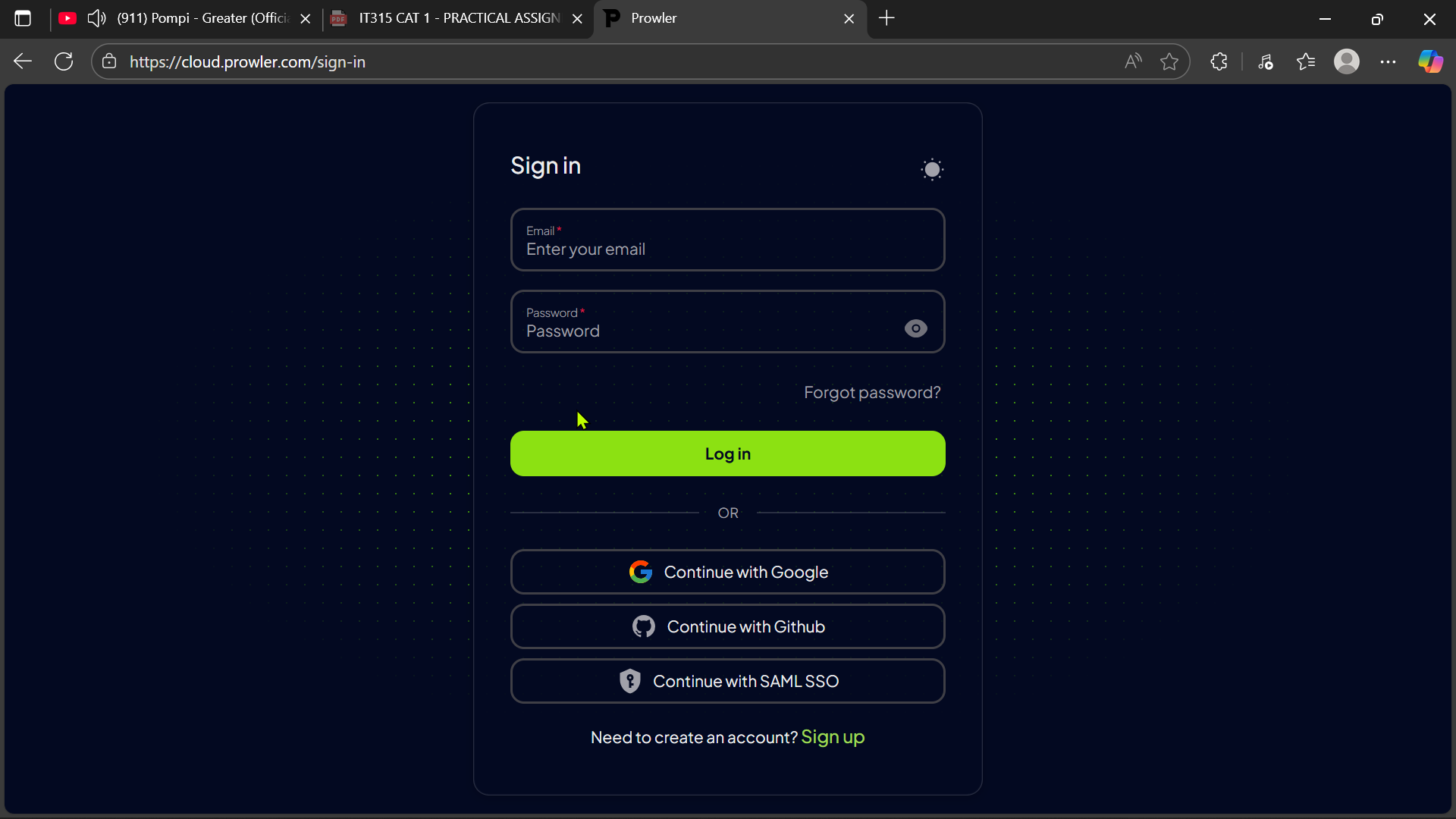
**CLOUD SECURITY POSTURE MANAGEMENT (CSPM) - PROWLER**

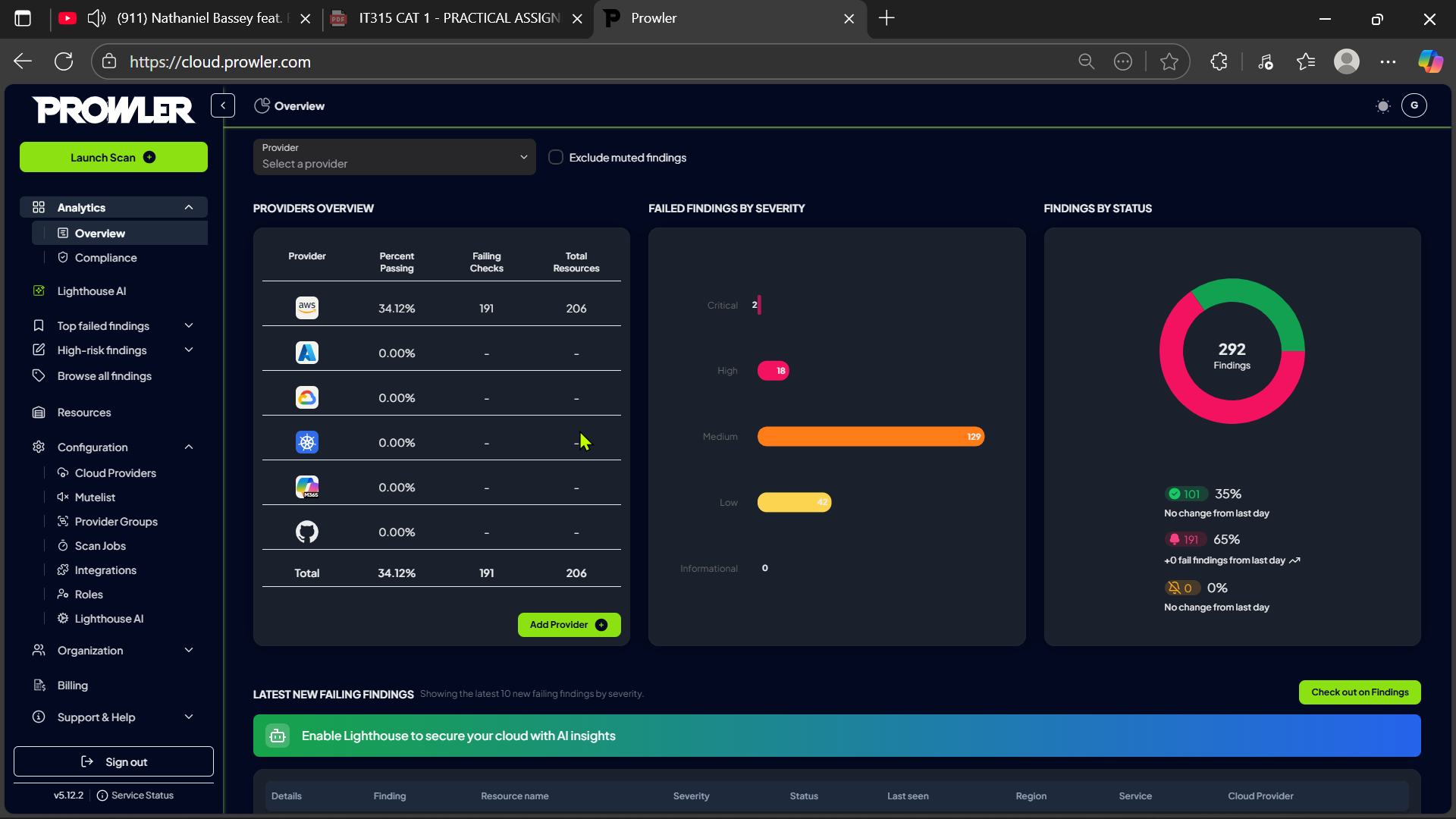
**Cloud Security Posture Management (CSPM)** is a set of tools and practices that continuously monitor and assess cloud environments to identify misconfigurations, security risks, and compliance violations, helping organizations maintain a secure and compliant cloud infrastructure. In this section, we will look at a tool called **Prowler,** which will help us achieve the main objectives of CSPM.

**Prowler** is an open-source CSPM tool for AWS, Azure, GCP, and Kubernetes that performs automated security assessments. It checks for compliance with standards like CIS, GDPR, HIPAA, and PCI-DSS, while also identifying misconfigurations in areas such as IAM, networking, and logging. Prowler is lightweight, command-line based, and widely used in both audits and continuous monitoring, making it a practical tool to demonstrate CSPM in action. The following are some of the screenshots that depicts how you can perform CSPM on AWS cloud environment using Prowler.

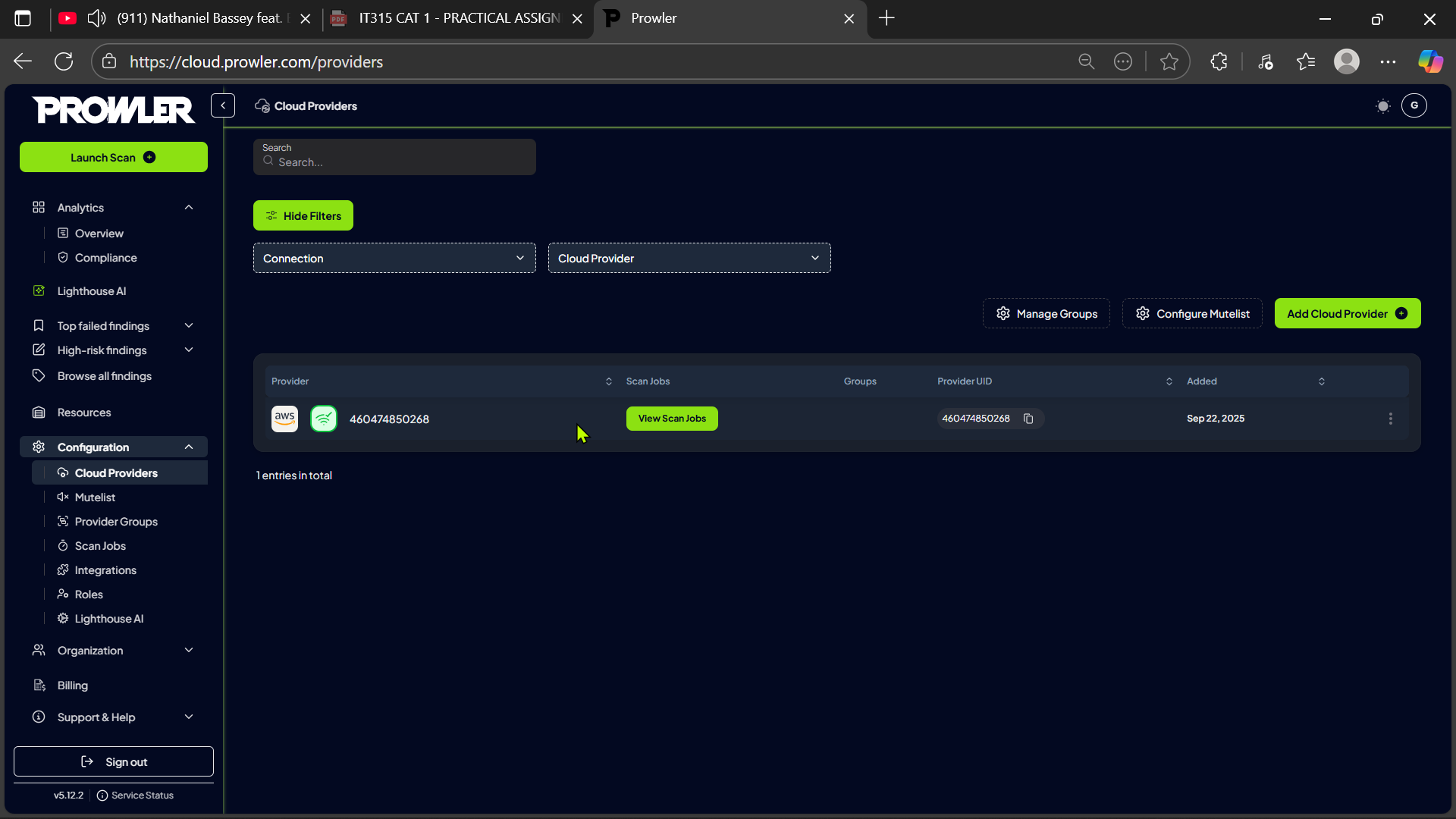
**Method 1:**

Below is a sign-up/in page all you need to do is sign in or sign up if you don’t have an account

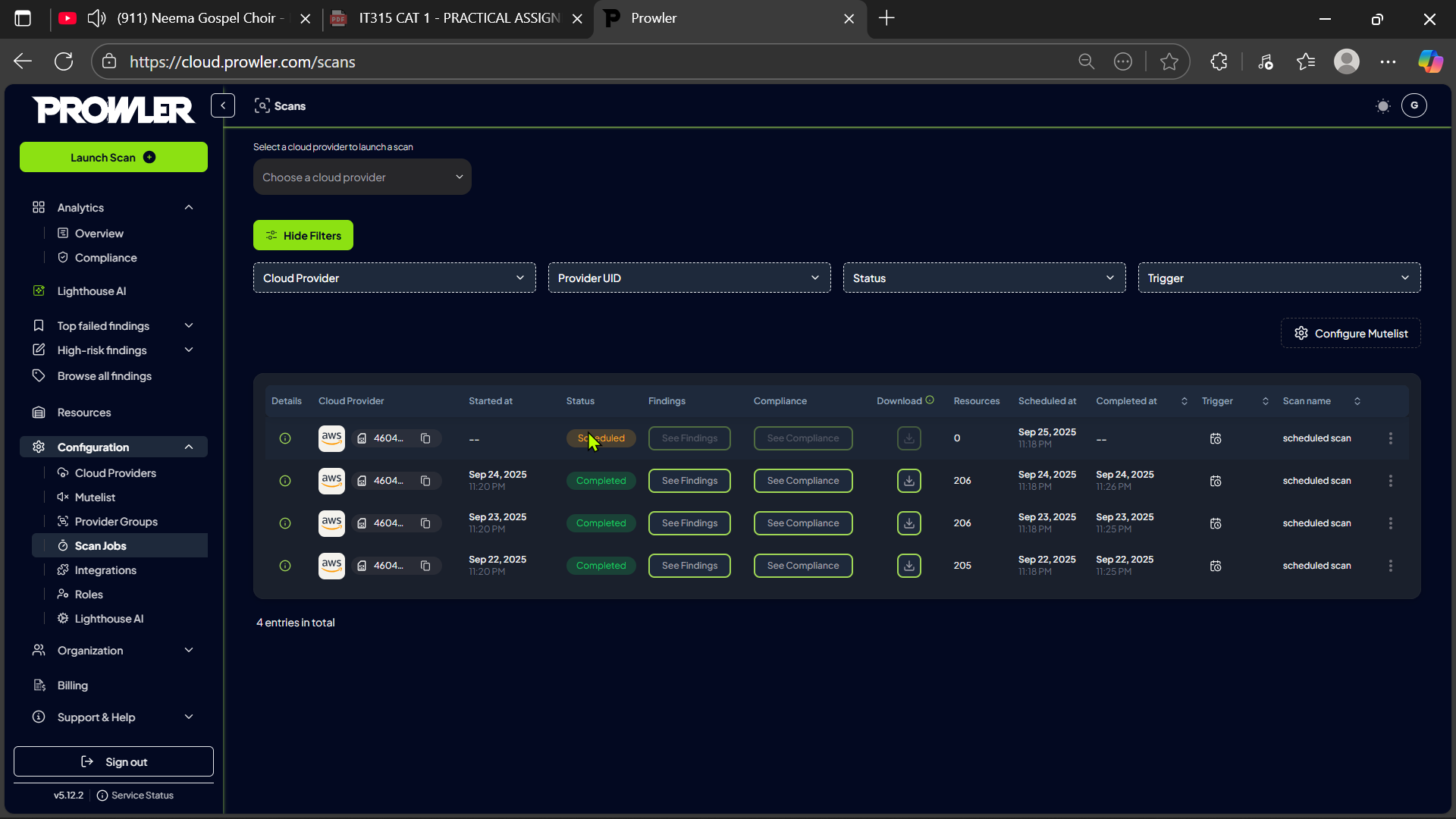


Below is the dashboard, which is the first appearance upon signing-in. However, under the configuration section is an option called cloud providers [click on it]

Below is the tab you’ll find, and the main interest is to add the cloud provider to this tool for operations. There is a button name “add cloud provider” [click on it]



After clicking on the add cloud provider button, you find options of cloud provider, click on your desired cloud provider and finish-up the authentication process and start scan. After the scan is done you go on scan jobs under the configuration option left section and click on it. From this page you can actually manage to download a full audit or see all the findings from misconfigurations to compliance violations.



**Method 2:**

This is the cloudshell or CLI method based that using different commands to perform these operation inside the cloud providers console shell or CLI. How ever the following are some of the commands that can be used under the AWS cloud provider console.

General commands

1. **Install**: *pip install prowler*
2. **List available checks**: *prowler aws --list-checks*
3. **Run specific checks**: *prowler aws -c <check\_name*>
4. **Output formats**: *prowler aws -f json/html/csv (choose output format)*
5. **Help**: *prowler –help*

Focus Areas

1. Identity and Access Management (IAM)

*prowler aws -c check\_iam (checks IAM configurations)*

*prowler aws -c check\_iam\_password\_policy (checks password policy)*

1. Network Security

*prowler aws -c check\_security\_groups (checks security group rules)*

*prowler aws -c check\_vpc\_flow\_logs (checks VPC flow logs)*

1. Data Protection

*prowler aws -c check\_s3\_bucket\_public\_access (checks S3 bucket public access)*

*prowler aws -c check\_s3\_bucket\_encryption (checks S3 bucket encryption)*

1. *Compliance and security posture*

*prowler aws -c compliance (runs compliance checks)*

*prowler aws -f html (generates HTML report for findings)*

**4.0 Trivy – Open Source Vulnerability and Security Scanner**

Trivy is an open-source, comprehensive security scanner developed by Aqua Security. It is designed to detect:

* **Vulnerabilities** in operating system packages and application dependencies.
* **Misconfigurations** in Dockerfiles, Kubernetes manifests, and Infrastructure-as-Code (IaC) files.
* **Secrets** such as API keys, passwords, and tokens accidentally left in source code.
* **License compliance issues** for open-source dependencies.

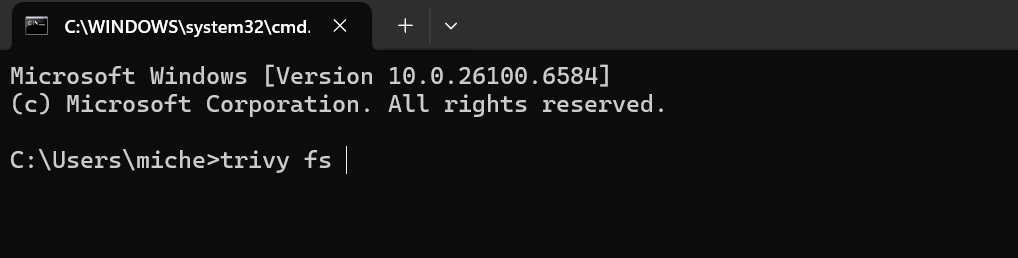
Trivy plays a key role in **shift-left security** by helping developers and DevOps teams find and fix problems early in the development lifecycle.

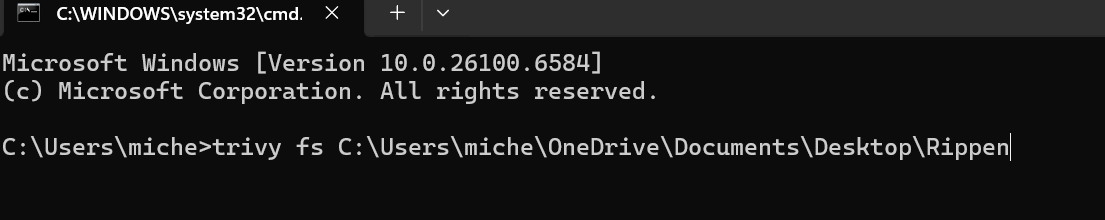
**Why Trivy is Important**

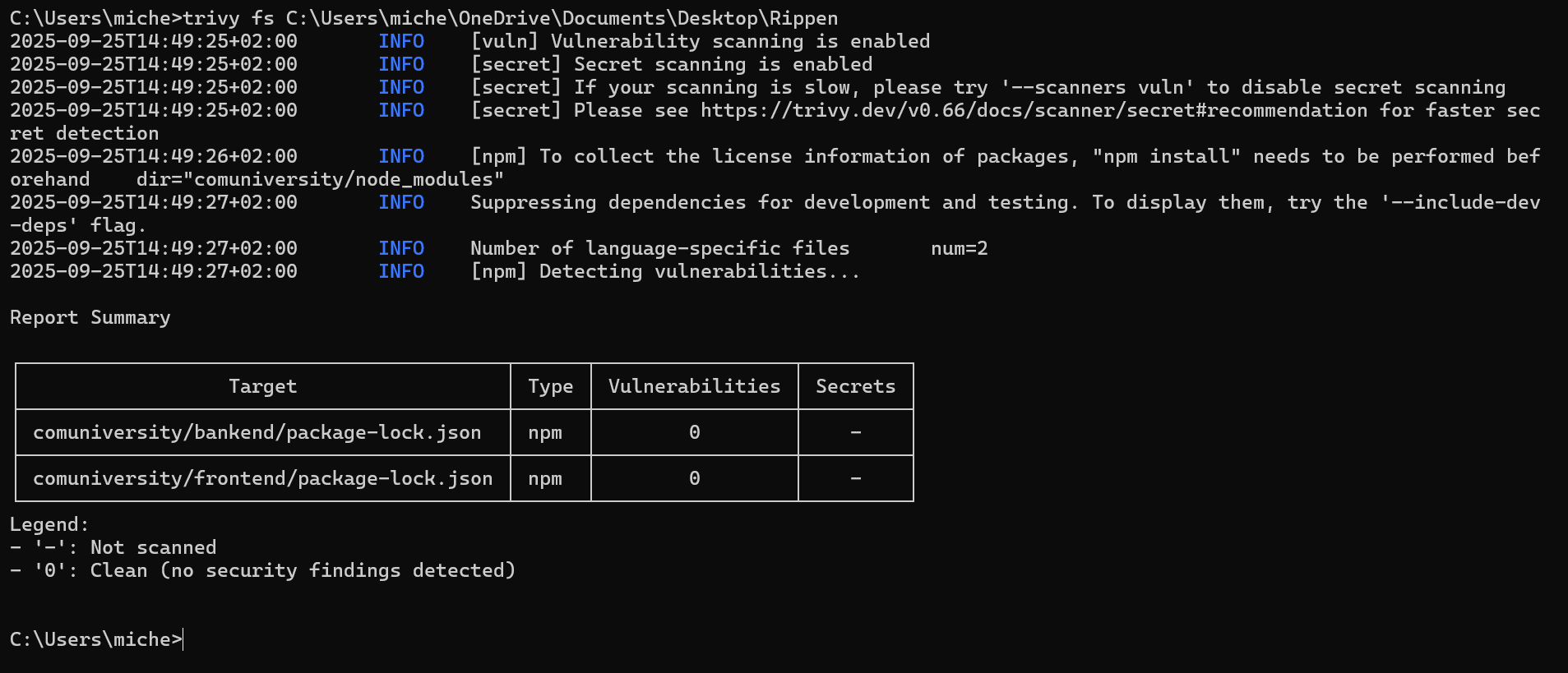
* **Early Detection:** Prevents vulnerabilities from reaching production.
* **DevSecOps Friendly:** Works in local environments and CI/CD pipelines.
* **Broad Coverage:** Supports container images, local file systems, and remote Git repositories.
* **Free & Open Source:** No licensing cost, easy to adopt.

**How Trivy Works**

1. **Scan Request:** The user runs a scan (e.g., image, repo, or folder).
2. **Database Sync:** Trivy downloads or updates its vulnerability database.
3. **Analysis:** It analyzes the target for packages, dependencies, secrets, and configurations.
4. **Matching:** Compares findings against known CVEs and security advisories.
5. **Report Generation:** Produces a clear, human-readable or machine-readable report (table, JSON, SARIF).







**4.4 Example Usage**

You can use Trivy through a simple CLI command:

* **Scan a container image:**

trivy image nginx:latest

* **Scan a local project folder:**

trivy fs C:\Users\miche\OneDrive\Documents\Desktop\Rippen\comuniversity

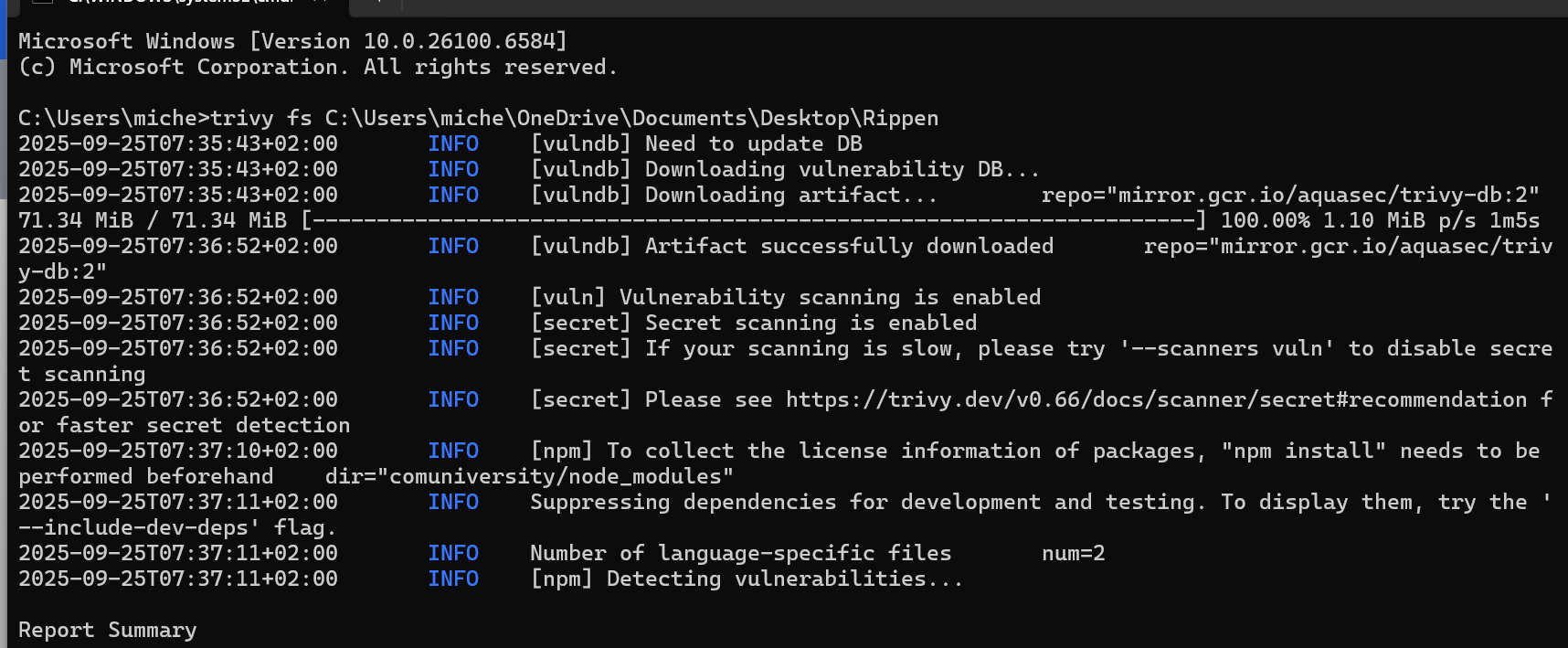
* **Scan a Git repository:**

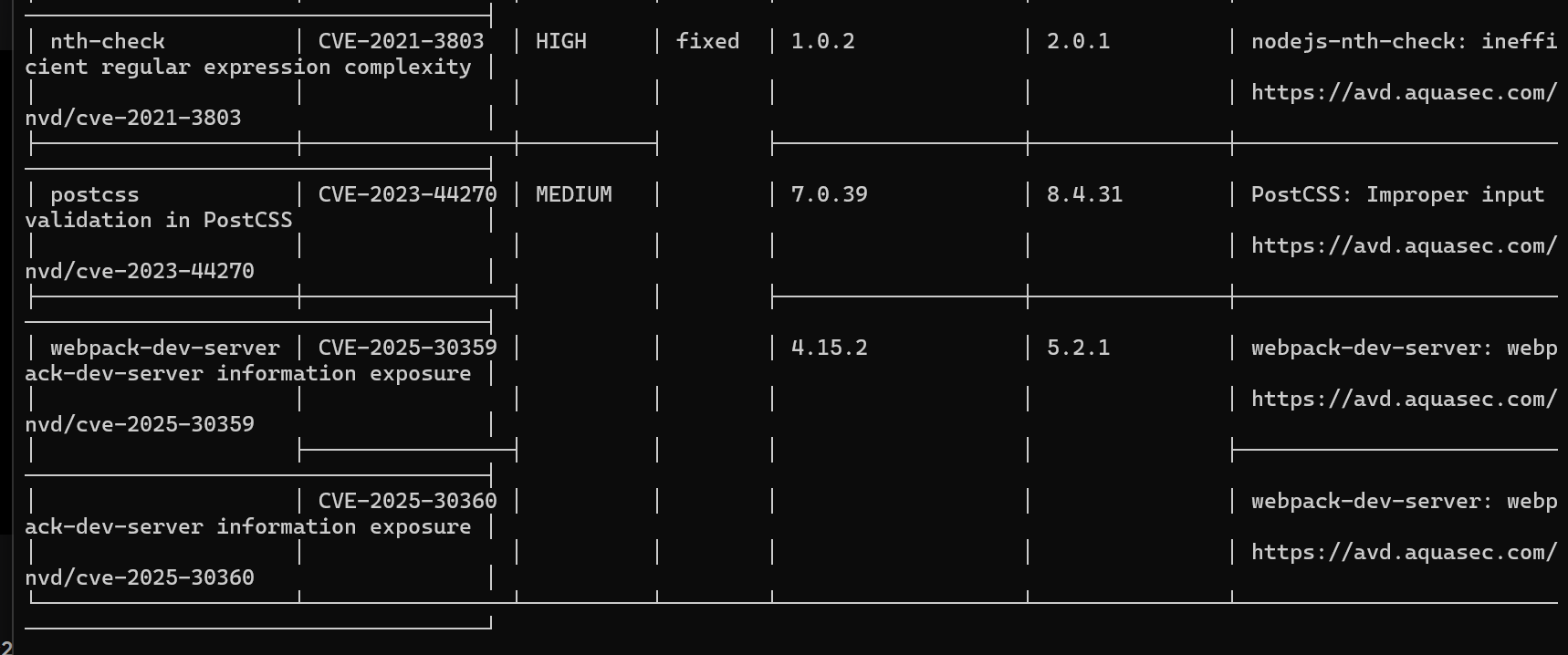
trivy repo <https://github.com/aquasecurity/trivy>

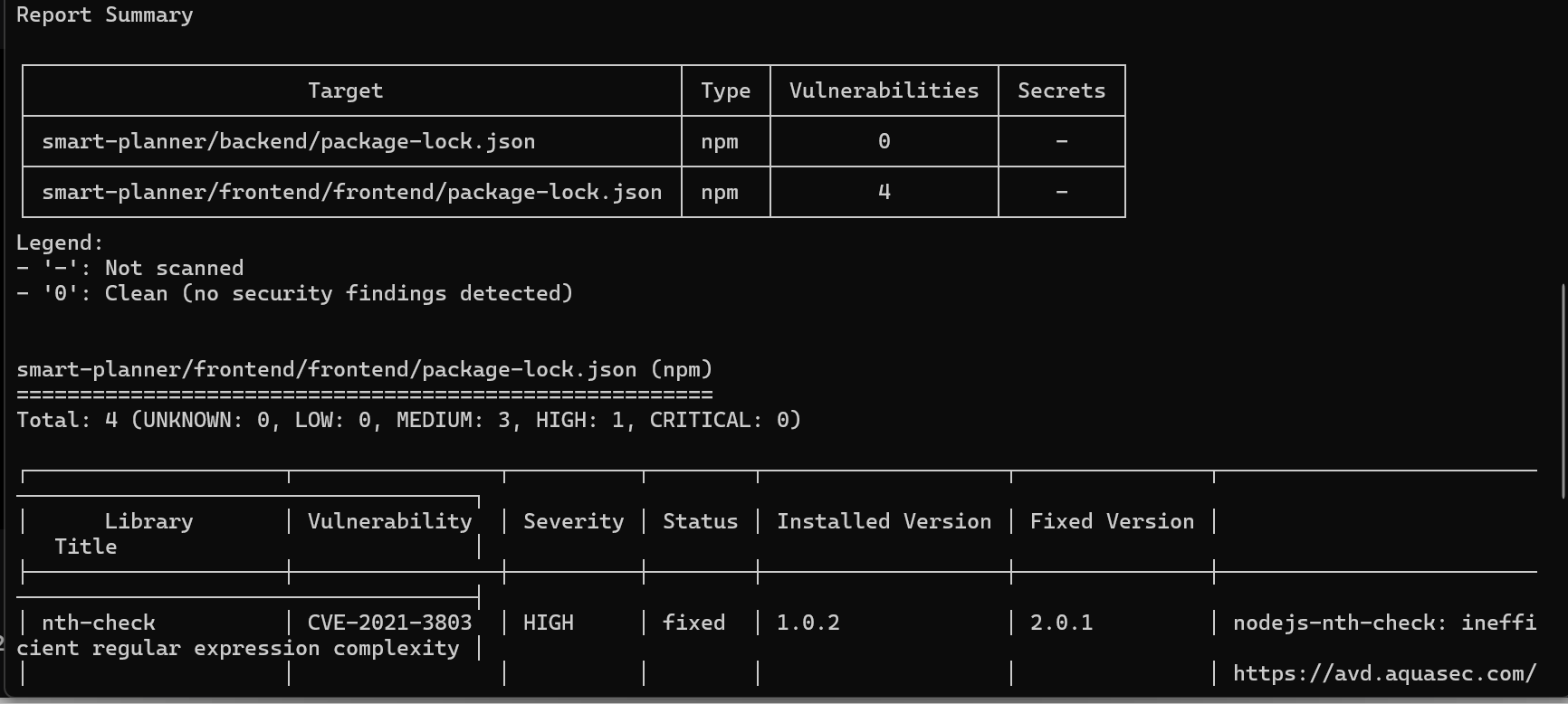
**4.5 Interpreting Results**

Trivy outputs severity levels for each finding:

* **LOW** – Minor issue, monitor but not urgent.
* **MEDIUM** – May pose a risk, consider fixing.
* **HIGH** – Significant risk, fix as soon as possible.
* **CRITICAL** – Must be fixed immediately to avoid exploitation.







**Integration with CI/CD**

Trivy integrates with popular CI/CD tools like GitHub Actions, GitLab CI, Jenkins, and Azure DevOps, enabling automated security checks before deploying applications.

**Advantages of Trivy**

* Free and open source.
* Supports multiple artifact types (images, repos, file systems, Kubernetes).
* Easy to set up (single binary installation).
* Fast and lightweight with offline scanning support.

**Limitations**

* Requires internet access for vulnerability database updates.
* May produce false positives that require manual review.
* Large container images can take longer to analyze.

**Conclusion**

Trivy is a powerful and user-friendly security scanner that helps developers, DevOps, and security teams secure their software early in the lifecycle. Its ability to detect vulnerabilities, misconfigurations, and secrets makes it an essential tool for cloud-native security.

**“Scan Today, Secure Tomorrow!”**