|  |  |
| --- | --- |
| Name: | Muskan Shukla |
| Lab User ID: | 23SEK3324\_U14 |
| Date: | 10-01-2024 |
| Application Name: | OWASP Wrong Secrets |

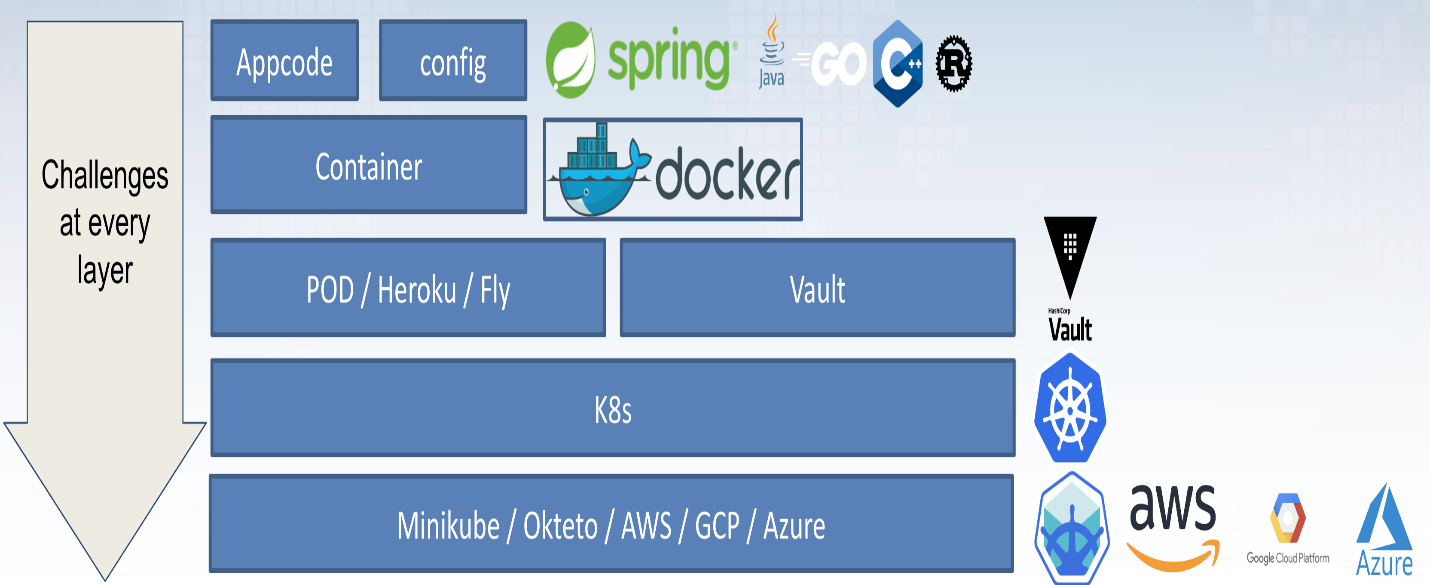
**Follow the below guidelines:**





System Architecture:

(Understand the system and document the physical and logical architecture of the system, use the shapes and icons to capture the system architecture)



OWASP Wrong Secrets System Architecture





Define system’s normal behavior:

(Define the steady state of the system is defined, thereby defining some measurable outputs which can indicate the system’s normal behavior)

Open Web Application Security Project (OWASP) known as "WrongSecrets". The OWASP WrongSecrets project is an exploitable. It primarily serves as a learning tool that allows for exploration and exploitation of various secrets-related vulnerabilities.

Some behavior of using OWASP Wrong Secrets -

1.Getting Started: After installation, the user is presented with challenges related to different types of secret leaks within a cloud environment or a codebase and it aims to teach users about the dangers of incorrect handling of secrets.

2.Exploration: The developed cloud services allow users to get hands-on experience in identifying the wrong implementation and misconfigurations which are causing the secret leaks.

3.Resolution: With each challenge, users are traditionally expected to find and fix the leak and in doing so, they learn the correct ways of handling and implementing secrets.

Hypothesis:

(During an experiment, we need a hypothesis for comparing to a stable control group, and the same applies here too. If there is a reasonable expectation for a particular action according to which we will change the steady state of a system, then the first thing to do is to fix the system so that we accommodate for the action that will potentially have that effect on the system. For eg: "If one of our database servers fails, our service will automatically switch to a backup server, and users will not experience any downtime or data loss.")



**Known**

Ideally if a malicious user gains access to our system or application, our system will securely guard sensitive information and prevent unauthorized access or data breaches.

Assuming OWASP Wrong Secret application already contains vulnerabilities due to exposure of sensitive information like API keys and passwords, if a user gains internal or external access to our system, they could exploit these secrets leading to unauthorized access or data breaches.

**Unknown**

Given that OWASP Wrong Secret application is designed with certain security flaws, we hypothesize that in a chaotic system with unpredictable failures (service outages, network issues, abrupt shutdowns), these failures could lead to additional unforeseen exploits or security loopholes being exposed.

**Unknown**

**Known**

If a user gains access, they can exploit API keys and other secrets. Ideally in an application user should not be able to view or extract secrets.

Experiment:

(Document your Preparation, Implementation, Observation and Analysis )

**Preparation :-**

1. An AWS account was set up with the necessary permissions to create and manage EC2 instances.

2. A t2.medium instance was selected due to its balance of computing power and cost, adequate for the task.

3. An AMI (Amazon Machine Image) with a popular Linux distribution was chosen as the operating system for the EC2 instance.

**Repository :- https://github.com/OWASP/wrongsecrets.git**

**Implementation :-**

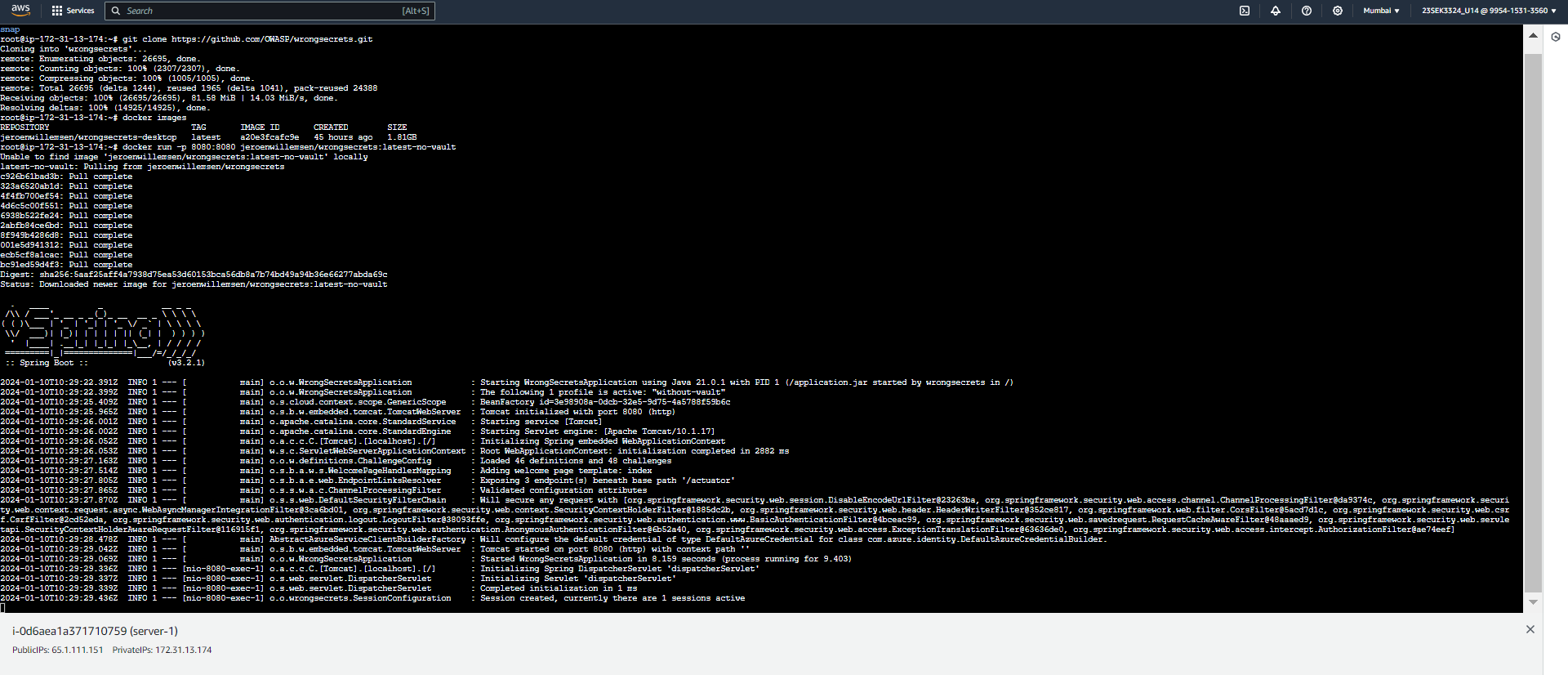
1. A server was developed and deployed using Docker. This could involve setting up a Docker file, building the Docker image, and then running a container from that image.

2. OWASP ZAP is one of the world’s most popular free security tools and is actively maintained by a dedicated international team of volunteers. It can be used for both automated and manual security testing.

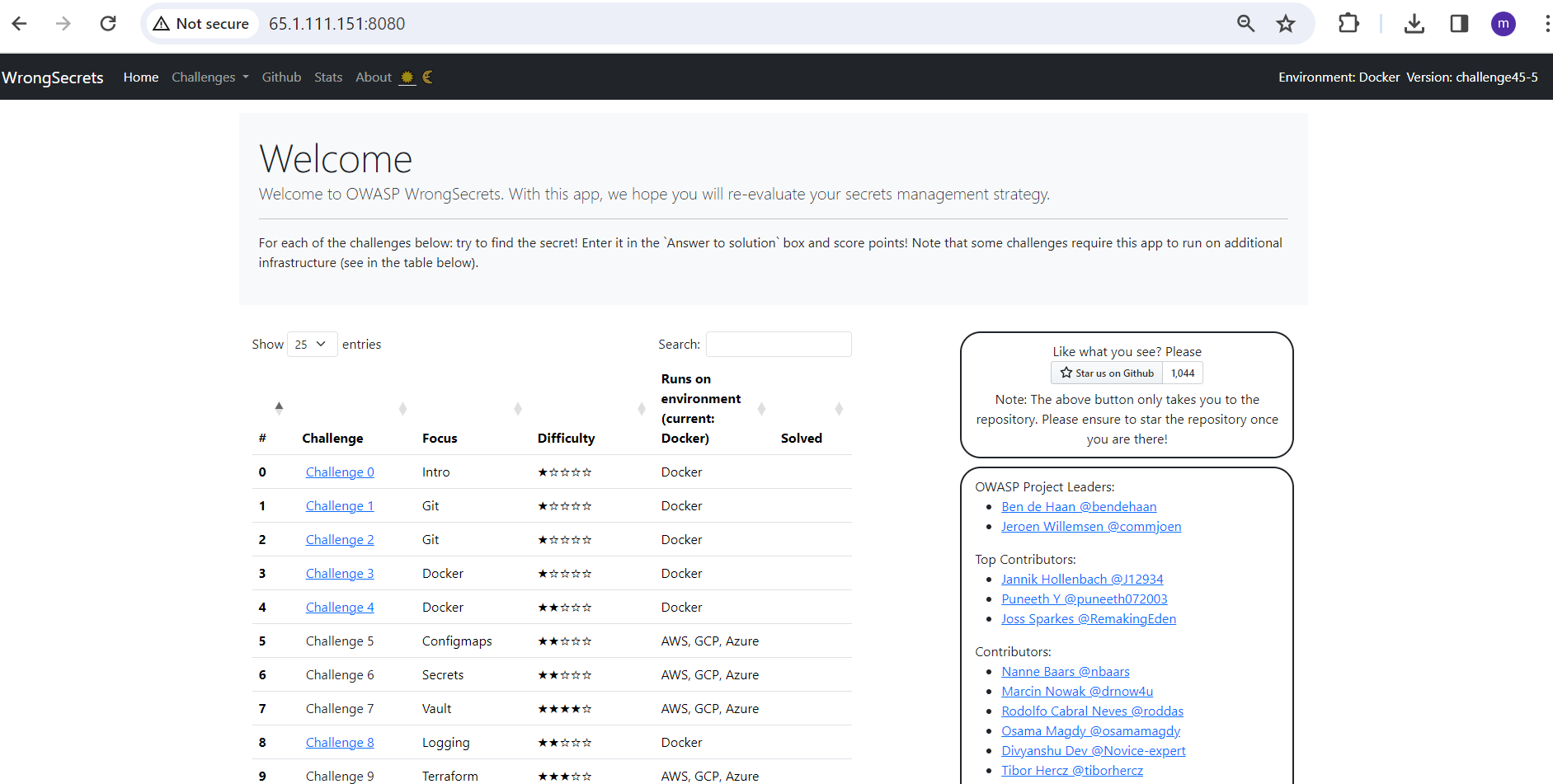
***Command -***

*docker run -p 8080:8080 jeroenwillemsen/wrongsecrets:latest-no-vault*

Live Webserver of Wrong Secret in Amazon EC2 instance



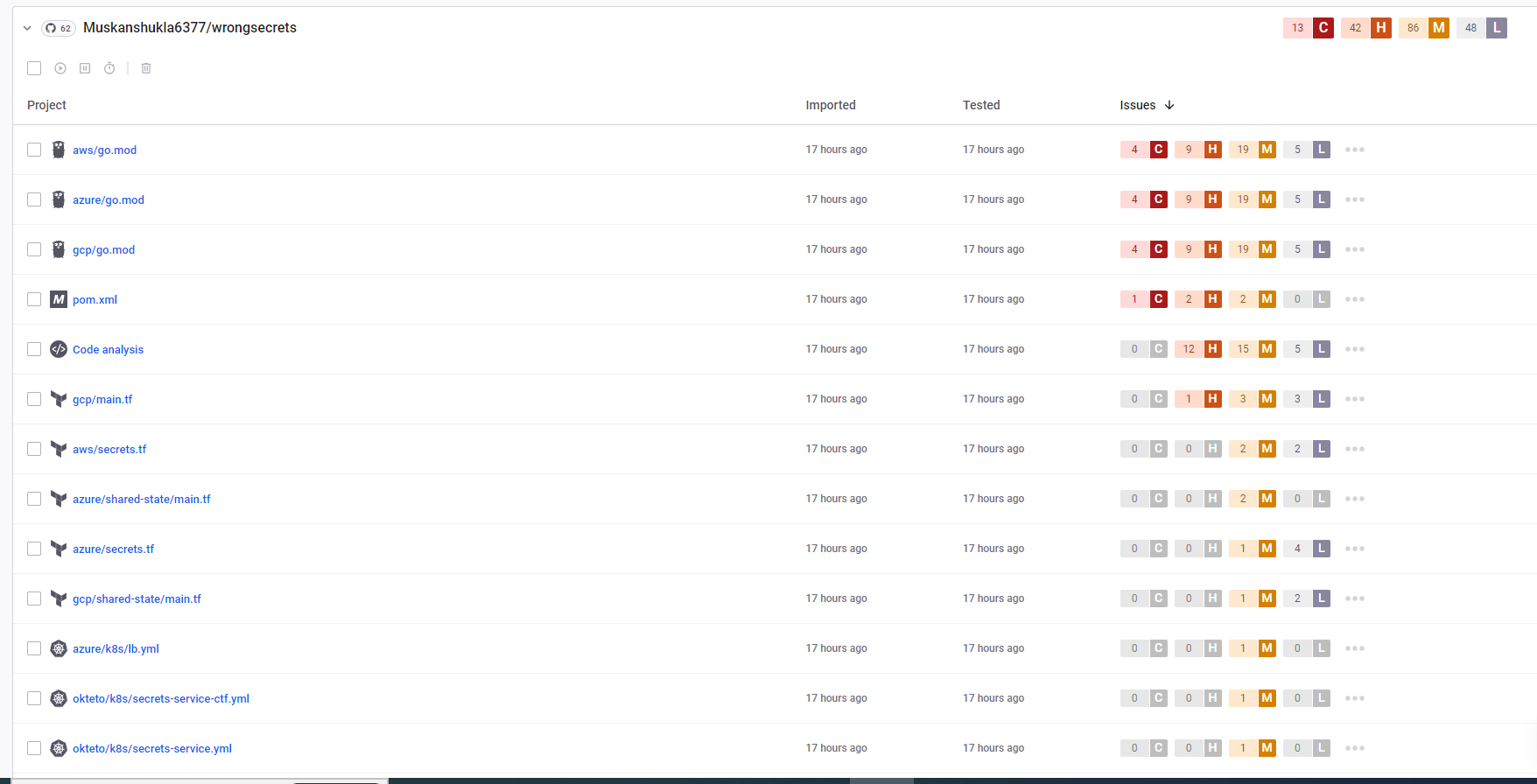
Live Web page of Wrong Secrets on Browser



**Observation and Analysis :-**

After the server was live, a scan was performed by using the Snyk tool Snyk is a platform that allows you to scan, prioritize, and fix security vulnerabilities in your code, open-source dependencies, container images, and infrastructure as code configurations.

After performing SNYK tool, there has 13 critical, 86 medium, 42 high and 48 low vulnerability. Describing some severity issues -



-->***CVE-2018-1098 –***

Impact--> The exploitation of this vulnerability can potentially lead to unauthorized information disclosure, tampering of information, and crucially, escalation of privileges. An attacker could exploit this flaw to execute arbitrary code in the system with administrative privileges.

Mitigation--> To deal with this issue, an update to the new Linux kernel version is highly recommended. Users should upgrade their systems to Linux Kernel version 4.16.6 or later.

-->***CVE-2021-3538 -***

Impact--> It is a vulnerability that was identified in the Polkit’s pkexec component, utilized in UNIX-like operating systems. It could allow attackers to gain unauthorized access and elevated privileges on a system, potentially leading to information extraction, theft, or even destroying data directly.

Mitigation--> At the time of this report, a patch has been released to address the vulnerability. System administrators are strongly urged to apply the patch or update as soon as possible. Until such time, limiting access to vulnerable systems and ensuring strict privilege management protocols can provide a temporary solution. Long-term preventive measures include regular updates, penetration testing, and vulnerability scanning.

-->***CVE-2020-15114 -***

Impact --> This vulnerability has a medium-severity rating from the National Vulnerability Database. This security vulnerability could allow a remote authenticated attacker to inject SQL commands into Python files, leading to arbitrary code execution by the attacker.

Mitigation--> Users are recommended to update their software to version 1.6.0p13 as soon as possible. Meanwhile, users should be wary of any suspicious activity and limit the access of their software to authorized personnel only.