I’ve been learning a new tool recently: **DefectDojo**.

“DefectDojo is a DevSecOps, ASPM (application security posture management), and vulnerability management tool. DefectDojo orchestrates end-to-end security testing, vulnerability tracking, deduplication, remediation, and reporting.”

I can’t stress enough the importance of being able to quickly deploy and test tools like this for a career in Cyber Security.

Okay, but what does that mean and how can I learn it?

DefectDojo is basically a command centre for keeping software safe from security threats. It helps teams involved in creating and managing software to:

1. **Run security checks:** It continuously tests software to find any weak spots that hackers could exploit.

1. **Keep track of problems:** When it finds security issues, it keeps all the details in one place so they can be managed easily.

2. **Avoid repeating the same work:** It's smart enough to recognize if the same security issue pops up more than once, so teams don’t waste time dealing with duplicates.

3. **Fix issues:** It helps guide the process of fixing these security weak spots from start to finish.

4. **Report on progress:** It generates reports that let teams see how well they are doing in fixing issues and improving the software’s safety.

Essentially, DefectDojo helps ensure that software is built securely and stays protected as it evolves, making the whole process a lot more streamlined and effective for everyone involved.

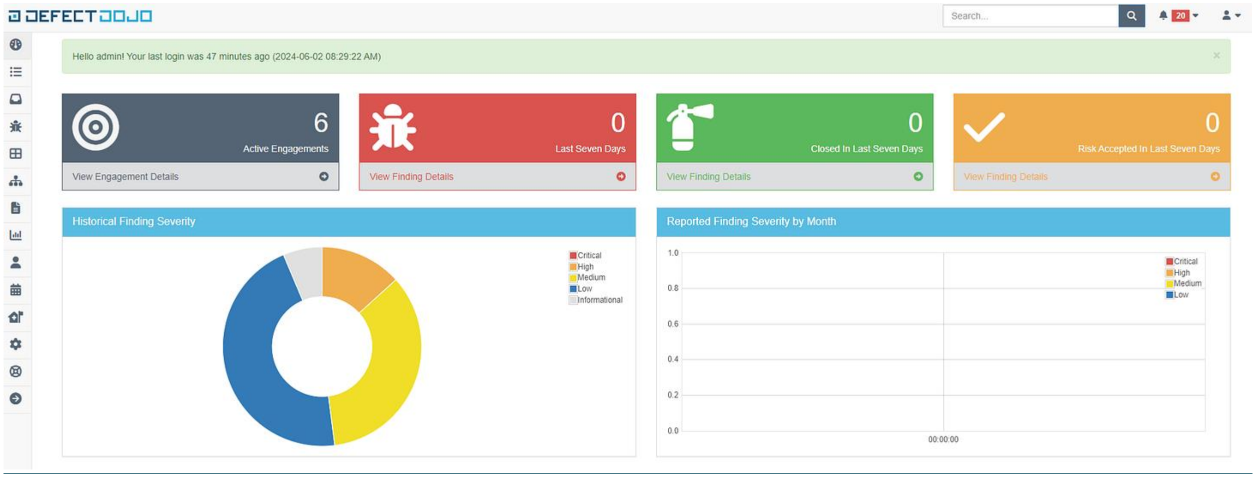
Cool! I know what it is now but I want to get hands-on… Awesome, you’re in the right place. Below are two methods to get started:

Quick and Easy:

If you're curious about DefectDojo and just want a quick look without any setup, there's a demo available:

1. Visit the demo site: DefectDojo Demo.

2. Find the demo login credentials on their GitHub page.
3. Log in and explore the interface to see how it manages and tracks security vulnerabilities.

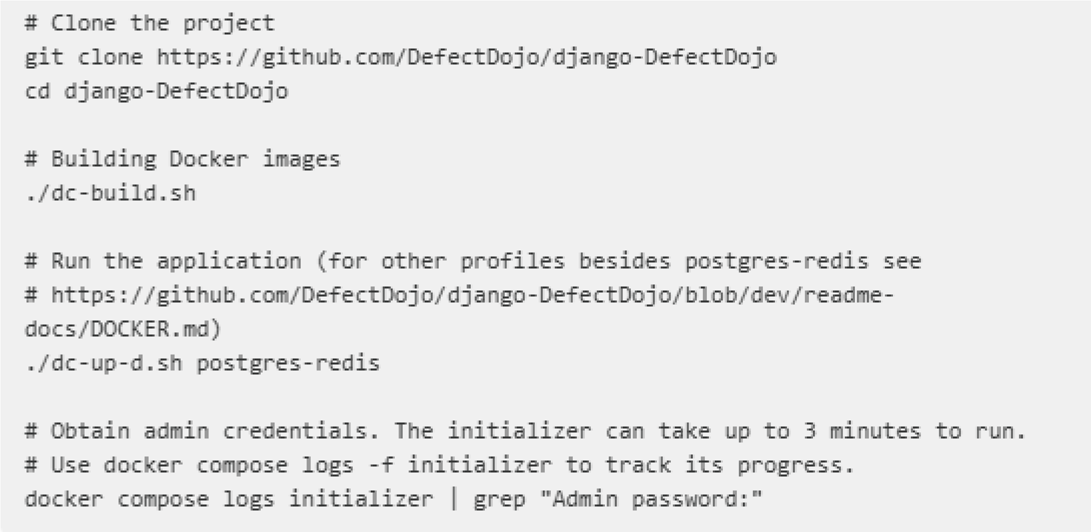


Hello admin! Your last login was 47 minutes ago (2024-06-02 08:29:22 AM)

The Best Way:

For a deeper dive into how DefectDojo works, setting it up on your own is the best approach. Here's how you can do it using AWS and Docker:

1. **Set Up on AWS**:
   - Create an AWS account if you don't have one.
   - Deploy an EC2 instance, which is a virtual server in Amazon's cloud.
2. **Install Docker**:
   - Once your EC2 instance is running, connect to it.
   - Install Docker and Docker Compose on your EC2 instance. These tools help you manage applications in lightweight containers: Docker Cheat Sheet
3. **Run DefectDojo**:



```
# Clone the project
git clone https://github.com/DefectDojo/django-DefectDojo
cd django-DefectDojo

# Building Docker images
./dc-build.sh

# Run the application (for other profiles besides postgres-redis see
# https://github.com/DefectDojo/django-DefectDojo/blob/dev/readme-
docs/DOCKER.md)
./dc-up-d.sh postgres-redis

# Obtain admin credentials. The initializer can take up to 3 minutes to run.
# Use docker compose logs -f initializer to track its progress.
docker compose logs initializer | grep "Admin password:"
```

4. **Set up your first project:**

- In DefectDojo, create a new "Product" (think of this as your software project).
- Start an "Engagement," which is where you'll test your product.
- Import sample scan files from DefectDojo's sample repository to see how DefectDojo handles different types of security scan results.

Level Up Your Learning

To truly understand how DefectDojo can fit into real-world scenarios:

- Set up a code analysis tool like SonarScanner on your code.
- Scan a vulnerable project, like the WebGoat application (a purposely insecure app used for training).
- Export the scan results and import them into DefectDojo to see how it manages and tracks real vulnerabilities.

Again, being able to quickly deploy and test tools like this for a career in Cyber Security is going to serve you extremely well and while this is super high level it's a great starting point for your own research.