

DOCUMENTATION

Setup instructions for participants

You'll access an application with a known SQL Injection (SQLi) vulnerability. Your task is to

1. Find the vulnerability
2. Use Seer Box to patch the application and block the attack

1. Set up the environment

You'll need a Ubuntu Linux system with Docker installed and full administration capabilities.

1. Install required system packages: `sudo apt install inotify-tools rsync`
2. Download and unzip the challenge setup package:
http://ctf.pluribus-one.it:8088/downloads/pluribus_cybersuite_hackathon.zip
3. From the terminal, enter the directory containing the challenge files (hackathon_10_2026)
4. Run the following commands to set up the Web Application Firewall:

```
mkdir -p infra/seer_box/sbx_volume/var/feeds
touch infra/seer_box/sbx_volume/var/feeds/modsecurity_ModSecurity
truncate -s 0 infra/firewall/modsecurity/rules.conf
```

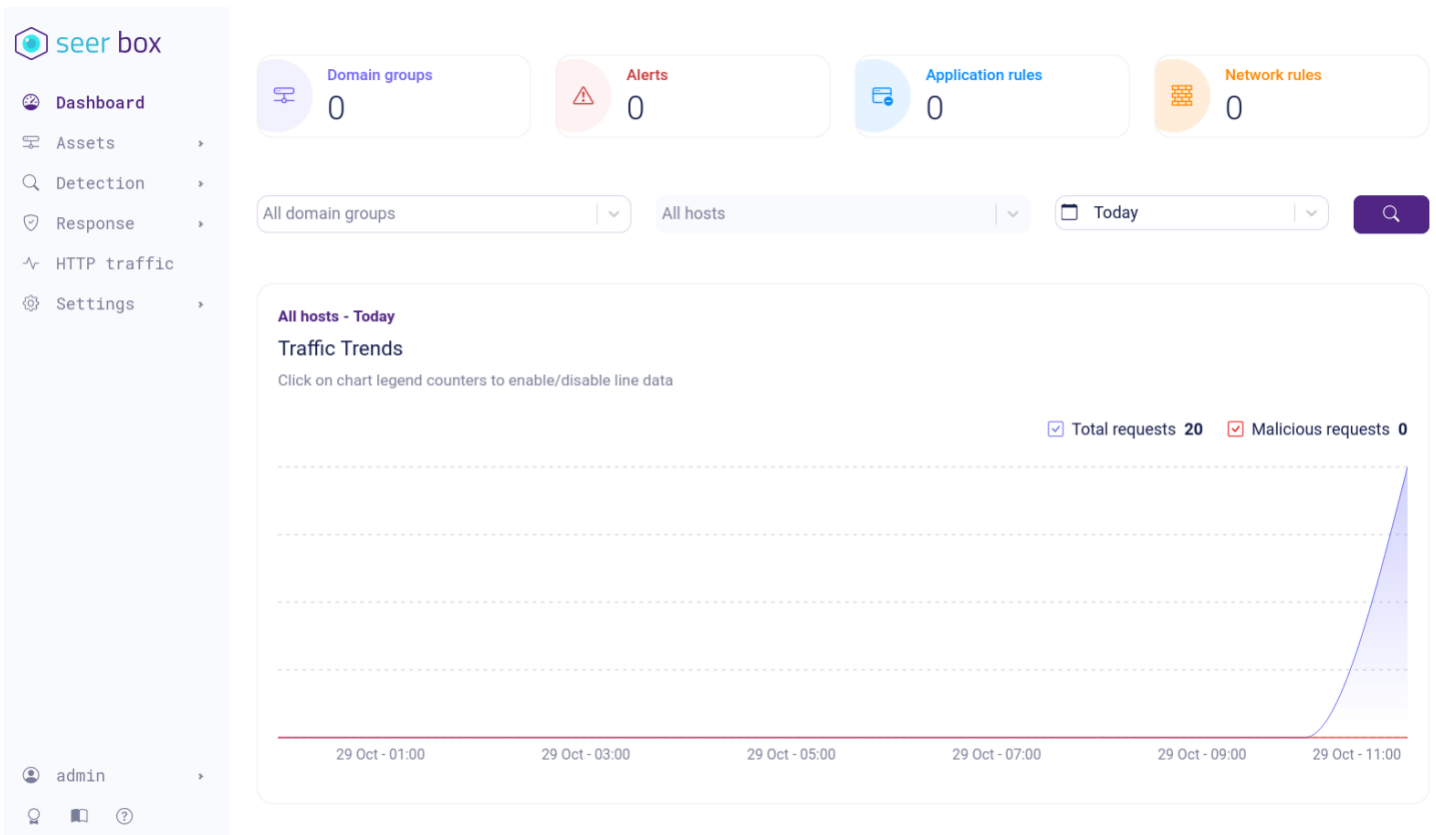
1. Run the challenge's environment: `./start.sh`
2. Once the setup is finished, you can reach the Seer Box web interface at the following URL:
`http://[UBUNTU_IP_ADDRESS]:53380`
3. Login using the default credentials:

Username: admin

Password: SeerBox_4dm1n

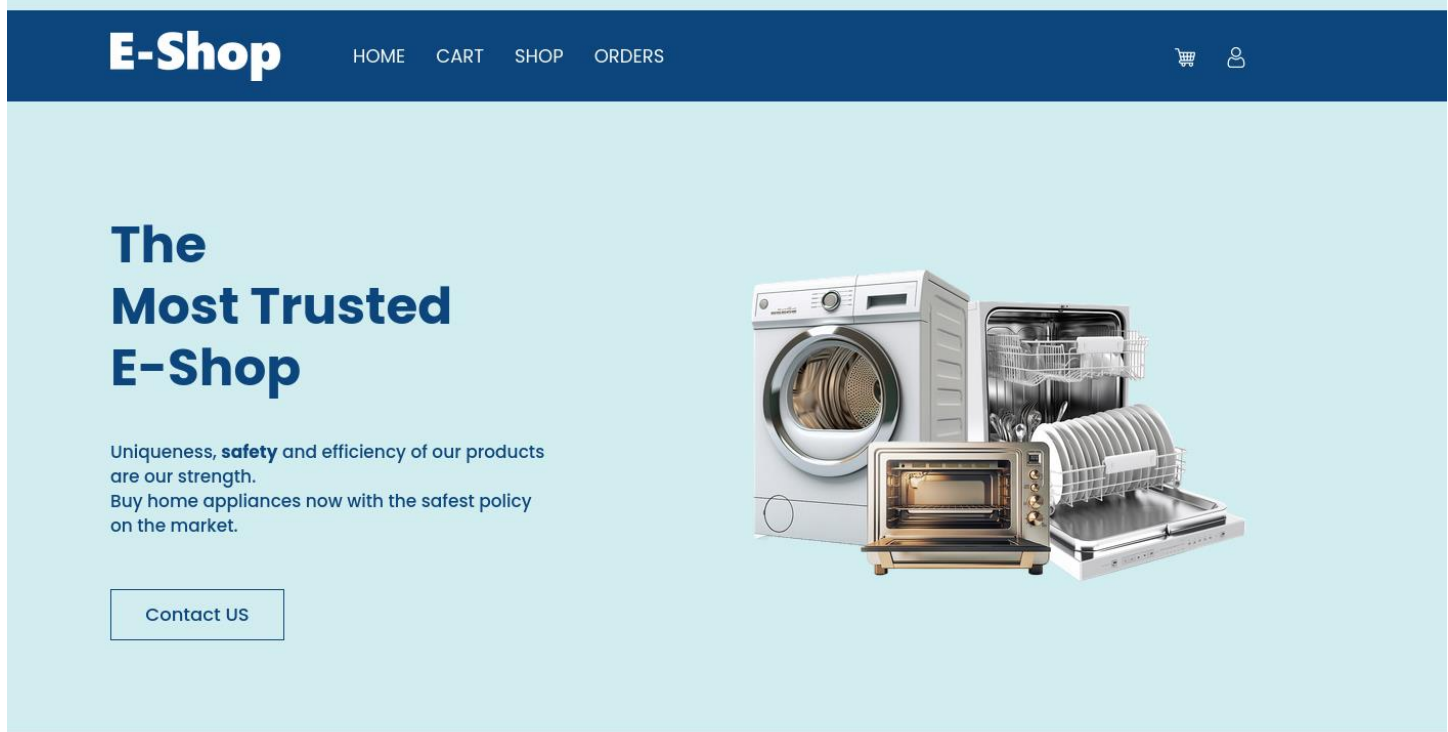
4. Activate Seer Box by obtaining a license key from <https://license.seerbox.it/> . You'll reach Seer Box's dashboard:

CyberSuite Hackathon Challenge: Seer Box



2. Access the vulnerable application

The vulnerable application can be reached at the URL: `http://[UBUNTU_IP_ADDRESS]:8082`



Our Products

There are many variation of our products. Scroll with the arrows below.

You can now find the **SQL Injection** vulnerability, then use Seer Box to **block the attack** and find your flag!