



SHODAN-EYE VULNERABILITY SCANNING

OUR COMPANY

Nel corso di questa presentazione esamineremo la progettazione della nostra web app Shodan-Eye Vulnerability Scanning, basata sulla piattaforma Azure Cloud. Esploreremo le sfide, le soluzioni e le best practices adottate nel corso del progetto.



TIMELINE

Creazione del
gruppo e scelta del
progetto

DEFINIZIONE
GRUPPO

Marzo
2024

Aprile
2024

START
Inizio lavori con
metodologia Agile
<<Scrum>>

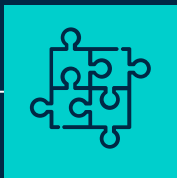
Deploy approvato della
prima build della
webapp
1st build

Aprile
2024

Maggio
2024

Deploy
Build finale e deploy
della versione
definitiva

TABLE OF CONTENTS



01

INTRODUZIONE

Definizione del problema, requisiti di progetto ed analisi delle tecnologie utilizzate



02

LA NOSTRA PROPOSTA

Architettura proposta, scelte progettuali e features implementate



03

CONCLUSIONI

Demo di Shodan-Eye, risultati ottenuti e possibili sviluppi futuri

INTRODUZIONE

01

DEFINIZIONE DEL PROBLEMA

Requisiti di progetto richiesti:

1. Develop a **Shodan-based** security monitoring service to gather information about security vulnerabilities of IoT devices and networks near your target
2. Process and analyze **data** collected by Shodan to identify possible vulnerabilities
3. Give a comprehensive view of **Azure** to process and analyze data collected by Shodan and a platform for viewing this information

Nell'analisi dei requisiti, ci siamo concentrati sulle funzionalità chiave dell'applicazione e sui requisiti di sicurezza. Abbiamo identificato i criteri di sicurezza ed i requisiti di compliance necessari per garantire la protezione delle informazioni sensibili.

TECNOLOGIE UTILIZZATE



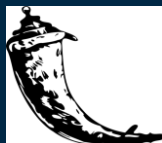
Azure



GitHub



Python



Flask



HTML, CSS e JS



Docker



Prometheus e Grafana

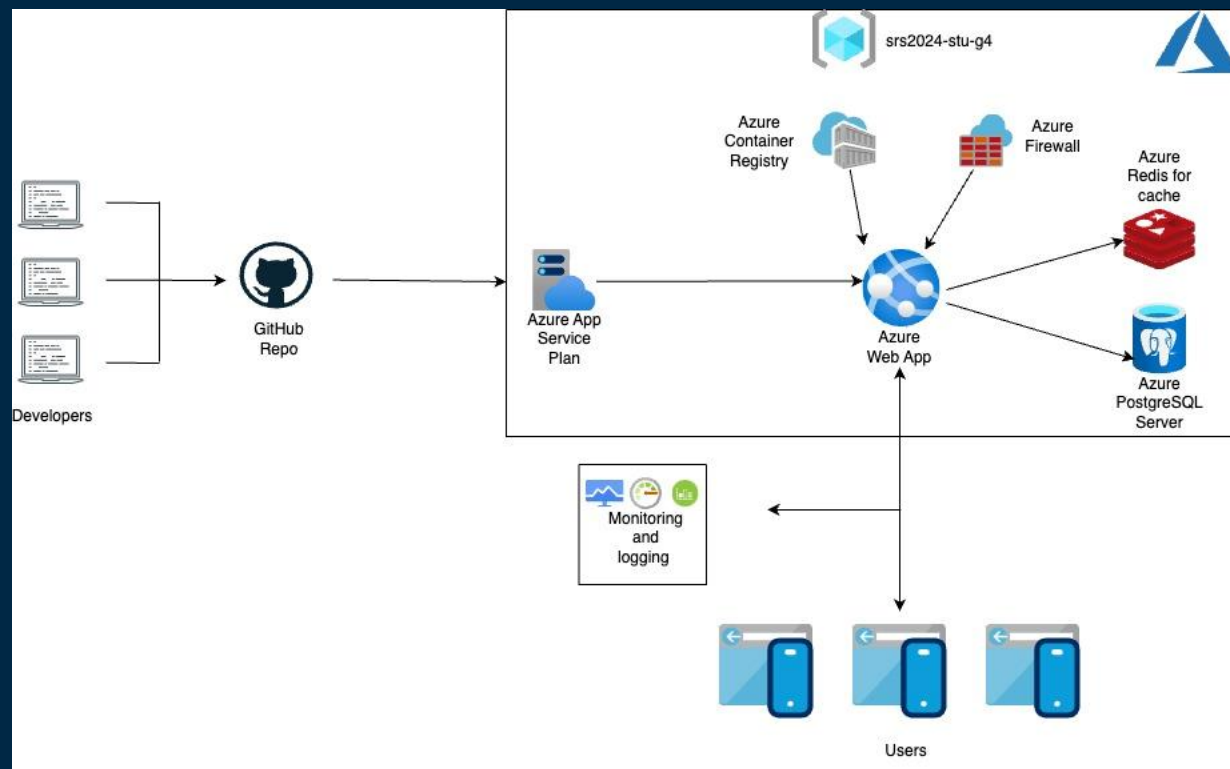


Terraform

La nostra proposta

02

ARCHITETTURA DELLA WEBAPP



L'architettura dell'applicazione è stata progettata per garantire la sicurezza e la scalabilità. Abbiamo adottato un'architettura serverless su Azure per garantire il monitoring delle vulnerabilità in modo efficiente ed affidabile.

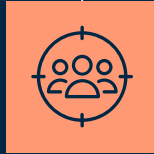
OUR SOLUTIONS

SCALABILITA'



RESILIENZA

SICUREZZA



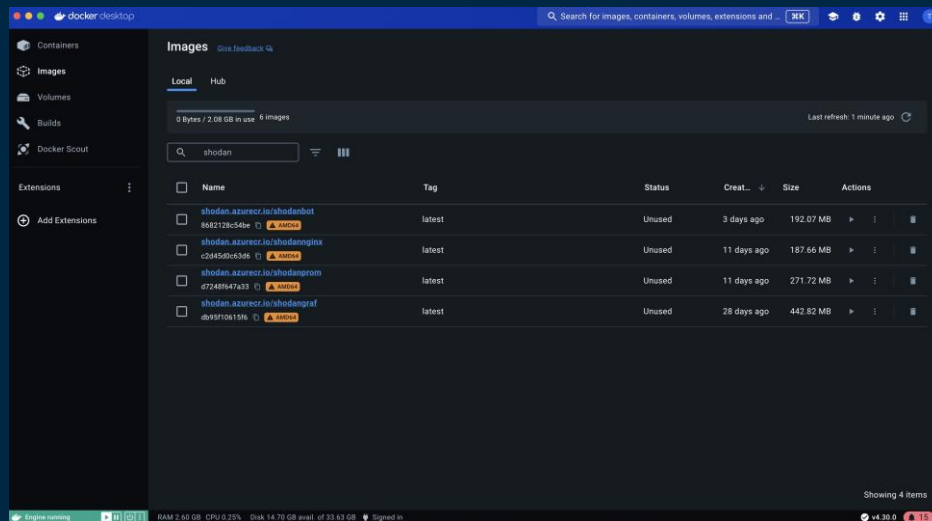
CI/CD

SVILUPPO

– SHODAN-APP




Oltre che la normale immagine Shodan-App sono state buildate anche le seguenti immagini tramite Docker:

- PROMETHEUS
- GRAFANA
- NGINX SERVER



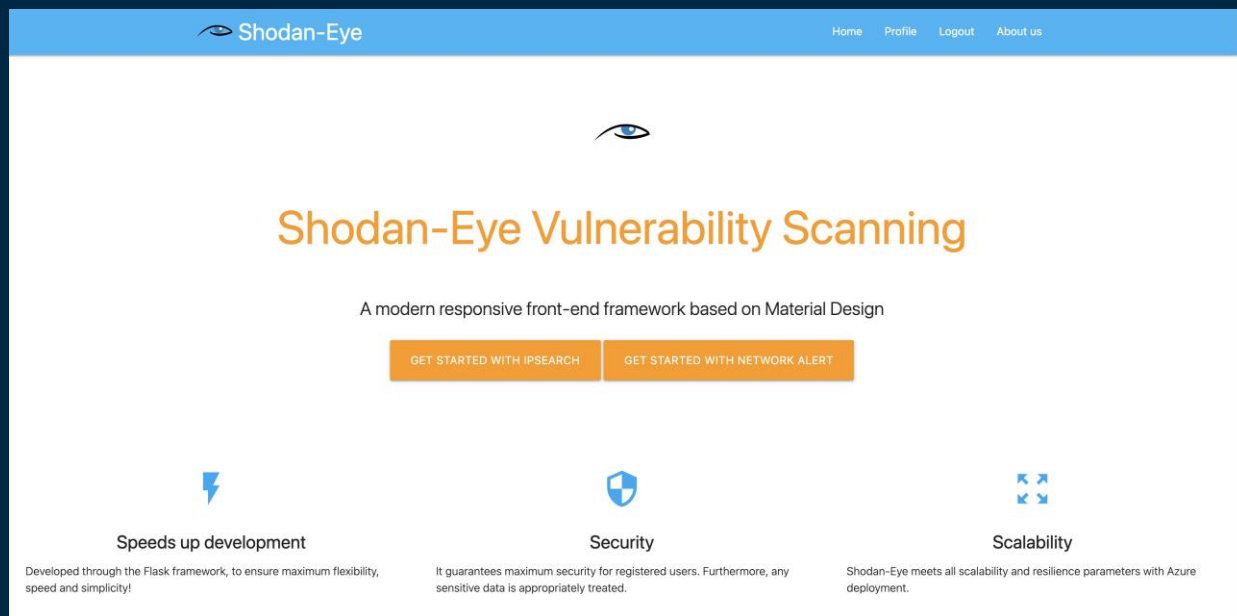
DEPLOYING

- BUILD IMMAGINI TRAMITE DOCKER
- PUSH IMMAGINI SU AZURE CONTAINER REGISTRY
- DEPLOY TRAMITE CUSTOM DOCKER-COMPOSE.YML

 docker-compose.yml
 Dockerfile
≡ Dockerfile_grafana
≡ Dockerfile_nginx
≡ Dockerfile_prometh...
 nginx.conf

```
1 version: '3.8'
2
3 networks:
4   mynetwork:
5     driver: bridge
6
7 services:
8   shodan-app:
9     image: shodan.azurecr.io/shodanbot:latest
10    build:
11      context: .
12      dockerfile: Dockerfile
13    container_name: shodan-app
14    expose:
15      - "8080"
16    network:
17      - mynetwork
18   prometheus:
19     image: shodan.azurecr.io/shodanprom:latest
20    build:
21      context: .
22      dockerfile: Dockerfile_prometheus
23    container_name: prometheus
24    expose:
25      - "9090"
26    network:
27      - mynetwork
28   grafana:
29     image: shodan.azurecr.io/shodangraf:latest
30    build:
31      context: .
32      dockerfile: Dockerfile_grafana
33    container_name: grafana
34    environment:
35      - GF_SERVER_ROOT_URL=http://shodan.scanning.azurewebsites.net/grafana/
36    expose:
37      - "3000"
38    network:
39      - mynetwork
40   nginx:
41     image: shodan.azurecr.io/shodannginx:latest
42    build:
43      context: .
44      dockerfile: Dockerfile_nginx
45    container_name: nginx_proxy
46    ports:
47      - "80:80"
48    depends_on:
49      - shodan-app
50      - prometheus
51      - grafana
52    network:
53      - mynetwork
```

HOMEPAGE



SIGNUP – SIGNIN

Possibilità di registrazione degli utente, in modo da visualizzare le ultime ricerche di ogni utente registrato

IP-SEARCH

Accesso alla pagina di scansione di un ip, o di dispositivi in un range km inserito dall'utente

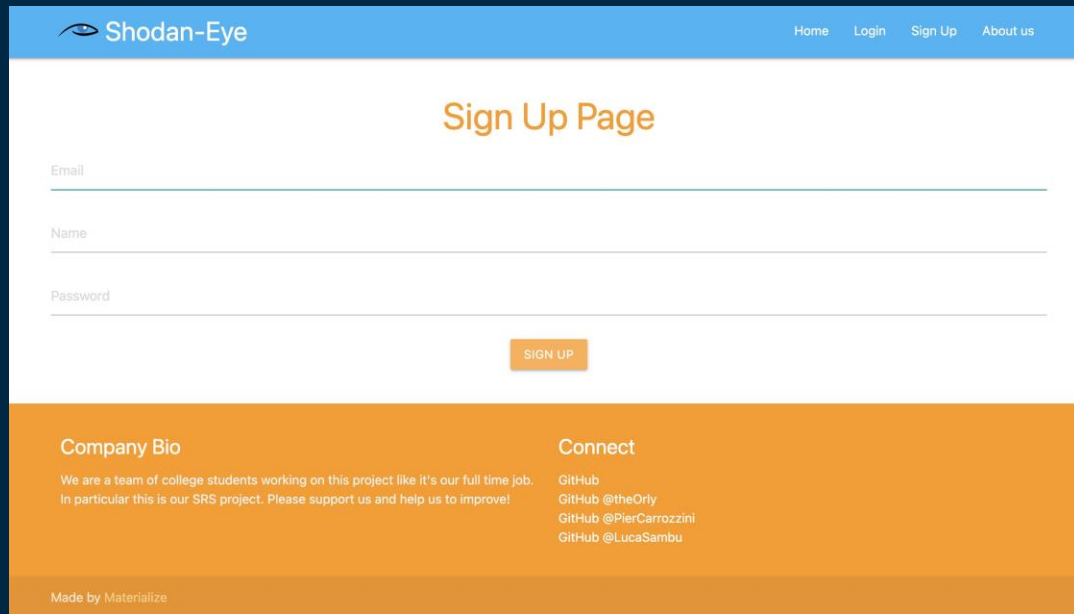
NETWORK ALERTS

Accesso alla pagina di gestione del monitoring di una rete o di un ip

ABOUT US

Accesso alla pagina di informazioni

SIGNUP-SIGNING



The screenshot shows the 'Sign Up Page' of the Shodan-Eye application. The page has a blue header with the 'Shodan-Eye' logo and navigation links for Home, Login, Sign Up, and About us. The main content area is white and features the title 'Sign Up Page' in orange. Below the title are three input fields for Email, Name, and Password, each with a light blue underline. A blue 'SIGN UP' button is positioned below the Password field. The footer is a solid blue bar containing two columns of text: 'Company Bio' and 'Connect'. The 'Company Bio' section describes the project as a team of college students working on the SRS project. The 'Connect' section lists GitHub handles for theOrly, PierCarrozzini, and LucaSambu. At the bottom left of the footer, it says 'Made by Materialize'.

Shodan-Eye

Home Login Sign Up About us

Sign Up Page

Email

Name

Password

SIGN UP

Company Bio

We are a team of college students working on this project like it's our full time job. In particular this is our SRS project. Please support us and help us to improve!

Connect

GitHub
GitHub @theOrly
GitHub @PierCarrozzini
GitHub @LucaSambu

Made by Materialize

SIGNUP

Form per la registrazione a Shodan-Eye Vulnerability Scanning

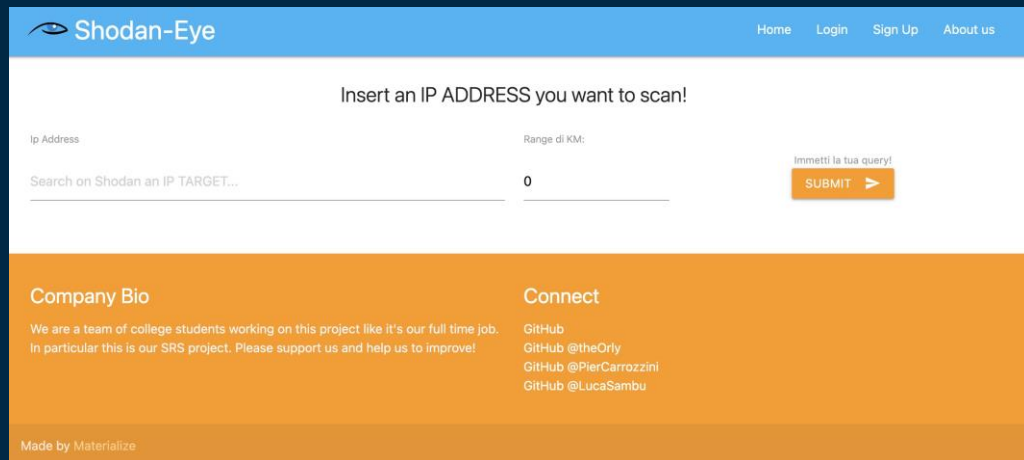
LOGIN

Login page

PROFILE PAGE

Profile page in cui è possibile visionare tutte le scansioni effettuate dall'utente

IP-SEARCH



The screenshot shows the Shodan-Eye web application. At the top is a blue header with the 'Shodan-Eye' logo and navigation links: Home, Login, Sign Up, and About us. Below the header is a white main area with the instruction 'Insert an IP ADDRESS you want to scan!'. There are two input fields: 'Ip Address' with a placeholder 'Search on Shodan an IP TARGET...' and 'Range di KM:' with a placeholder '0'. A small text prompt 'Immetti la tua query!' is above an orange 'SUBMIT >' button. The bottom of the page has an orange footer with 'Company Bio' and 'Connect' sections. 'Company Bio' mentions a team of college students and an SRS project. 'Connect' lists GitHub handles: @theOrly, @PierCarrozzini, and @LucaSambu. A 'Made by Materialize' watermark is in the bottom left corner.

DUE POSSIBILITA' DI SCANNING

IP-ADDRESS ONLY

E' possibile ricercare tutte le informazioni per uno specifico indirizzo ip

IP-ADDRESS AND RANGE

Ricerca di tutte le informazioni di un dispositivo e di tutti i dispositivi presenti nel range km inserito

NETWORK ALERT

The screenshot shows the Shodan-Eye Alert Service web interface. At the top is a blue header with the Shodan-Eye logo and navigation links: Home, Login, Sign Up, and About us. The main content area is white and titled 'Shodan-Eye Alert Service'. It contains three sections: 'Create alert', 'Delete alert', and 'Alert now active!'. The 'Create alert' section has four input fields: 'Alert name', 'Network', 'Triggers' (set to 'any'), and 'Tempo di scadenza (minuti)' (set to '60'). A blue arrow button is to the right. The 'Delete alert' section has an 'Alert name' input field and a blue square button. The 'Alert now active!' section shows a blue button with a bell icon and the text 'ALERT ACTIVE'. The footer is orange and contains 'Company Bio', 'Connect' (with GitHub links for @theOrly, @PierCarrozzini, and @LucaSambu), and 'Made by Materialize'.

Shodan-Eye Alert Service

Home Login Sign Up About us

Create alert

Alert name: Network: any Tempo di scadenza (minuti): 60

Delete alert

Alert name:

Alert now active!

ALERT ACTIVE

Company Bio

We are a team of college students working on this project like it's our full time job. In particular this is our SRS project. Please support us and help us to improve!

Connect

GitHub
GitHub @theOrly
GitHub @PierCarrozzini
GitHub @LucaSambu

Made by Materialize

CREATE ALERT

Creazione di un alert inserendo il nome, l'indirizzo ip e i trigger da abilitare per quel network monitoring oltre che la durata in minuti

DELETE ALERT

Distruzione di un alert attivo inserendo il suo ID, che è possibile leggere nella lista di alert

ALERTS LIST

Lista di tutti gli alert attualmente attivi

SICUREZZA

L'integrazione della sicurezza è stata un aspetto fondamentale del progetto, ed è stata conseguita tramite:

- SECURE SIGNUP/LOGIN
- INFO SENSIBILI IMPOSTATE COME VARIABILI DI AMBIENTE SU AZURE
- MODULI DI CONTROLLO DELL'INPUT DELL'UTENTE TRAMITE JAVASCRIPT

```
<script>
  function validateIPAddress() {
    var ipAddress = document.getElementById('ip_address').value;
    var ipPattern = /^(\d{1,3}\.){3}\d{1,3}$/; // Regex per un indirizzo IP valido

    if (!ipPattern.test(ipAddress)) {
      alert("Inserisci un indirizzo IP valido!");
      return false;
    }
    return true;
  }
</script>
```

```
variables.tf
terraform_configuration > variables.tf
42
43 variable "REDIS_PSW" {
44   type      = string
45   description = "Redis pw"
46   sensitive = true
47 }
48
49 variable "shodan_api_key" {
50   type      = string
51   description = "Shodan API key"
52   sensitive = true
53 }
54
55 variable "telegram_api_key" {
56   type      = string
57   description = "Telegram API key"
58   sensitive = true
59 }
60
61 variable "postgresql_administrator_username" {
62   type      = string
63   description = "Username for the SQL administrator"
64   default   = "psqladmin"
65 }
66
67 variable "postgresql_administrator_password" {
68   type      = string
69   description = "Password for the SQL administrator"
70   sensitive = true
71 }
```

MONITORING & LOGGING

E' stata data particolare importanza alle operazioni di monitoring e logging a partire già dal codice. Shodan-Eye è stato sviluppato con appositi accorgimenti quali:

- Libreria «logging»

Per la stampa su console di tutte le informazioni

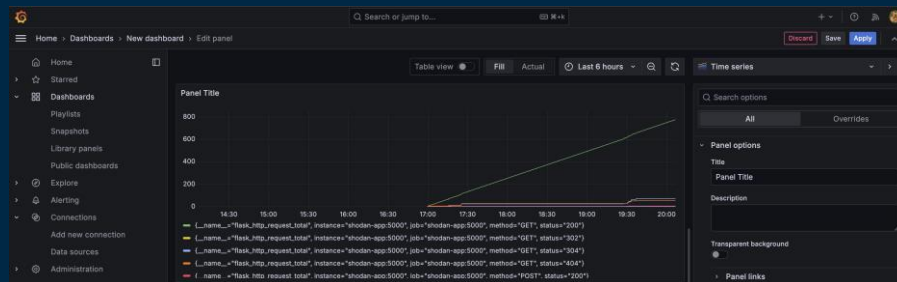
- «prometheus_flask_exporter»

Libreria apposita per esportare le metriche di interesse tramite il client di Prometheus

- Grafana dashboard

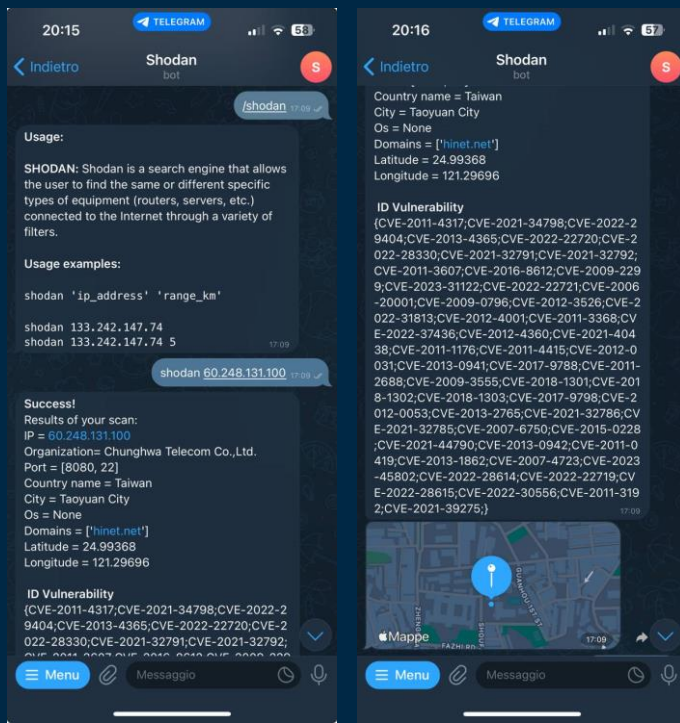
Visualizzazione grafica di tutti i dati

```
2024-06-11T18:05:09.513710Z INFO root:Metrics route only for debug
2024-06-11T18:05:09.525139060Z INFO werkzeug:172.16.51.3 - [11/Jun/2024 18:05:09] "GET /metrics HTTP/1.1" 200 -
2024-06-11T18:05:24.517649834Z INFO root:Metrics route only for debug
2024-06-11T18:05:24.529768906Z INFO werkzeug:172.16.51.3 - [11/Jun/2024 18:05:24] "GET /metrics HTTP/1.1" 200 -
2024-06-11T18:05:39.505268412Z INFO root:Metrics route only for debug
2024-06-11T18:05:39.522199169Z INFO werkzeug:172.16.51.3 - [11/Jun/2024 18:05:39] "GET /metrics HTTP/1.1" 200 - Ending Log Tail of existing log ---Starting Live Log Stream ---
```



SHODAN-EYE TELEGRAM BOT

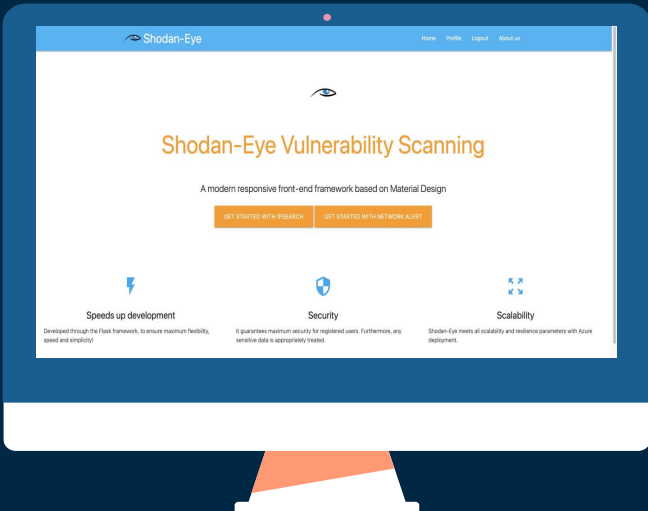
E' stato progettato e sviluppato, inoltre, un apposito bot telegram dedicato che svolge alcune funzioni di Shodan-Eye Vuln. Scanning



E' possibile accedere alle funzionalità di IP-SEARCH (only address e range) direttamente tramite il BOT Telegram, il quale poi stamperà nella chat tutte le informazioni trovate e il collegamento tramite Maps alle coordinate del dispositivo.

CONCLUSIONI

03



Do you have any questions?

GITHUB SHODAN-EYE PROJECT



THANKS