

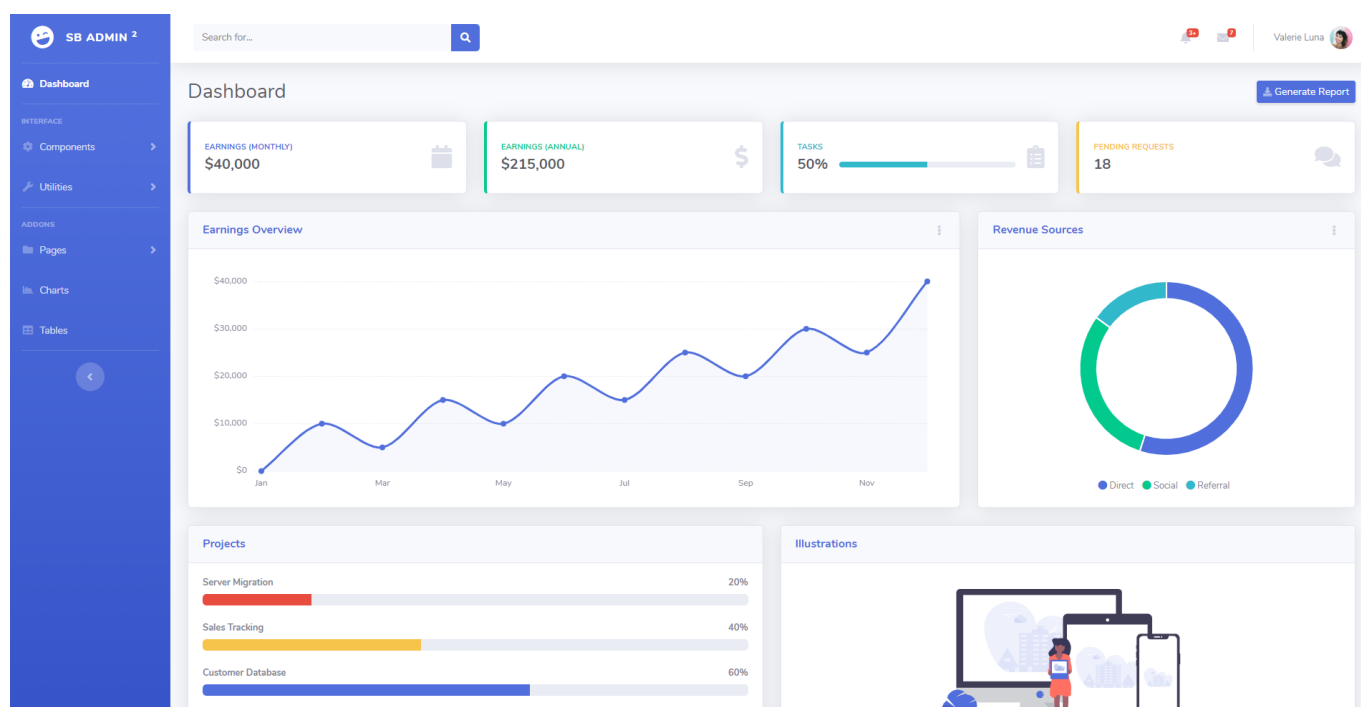
Documentation du site web

Configuration

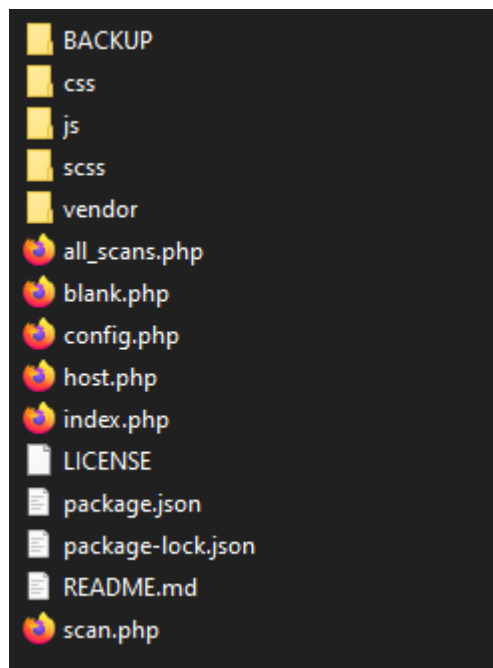
Le dossier du dashboard est à placer dans le répertoire `/var/www/html/` sur la RPI serveur ou sur un serveur externe.
Le site fonctionne sur base de l'API bootstrap, de codes écrits en PHP ainsi que quelques scripts en javascript.

Template utilisé : SB Admin 2

Template - Website



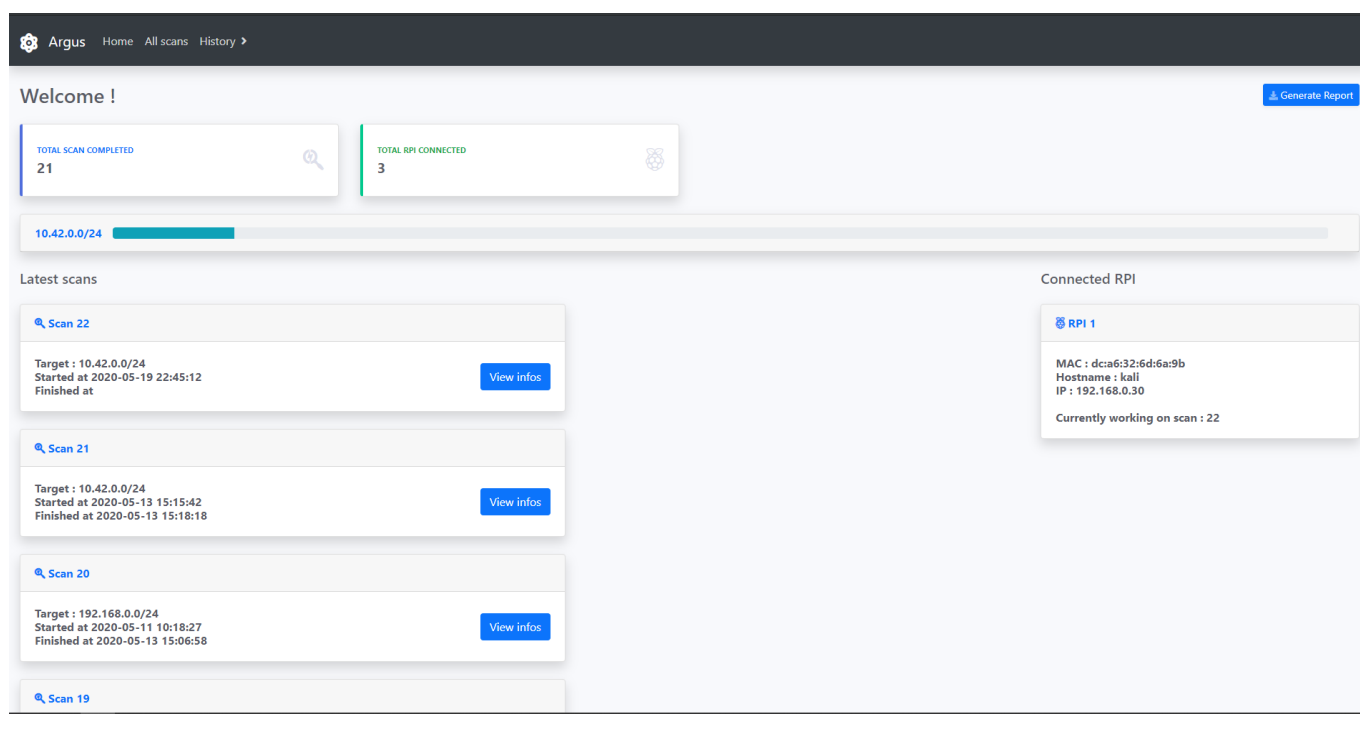
Structure du répertoire



index.php

Présente les informations suivantes :

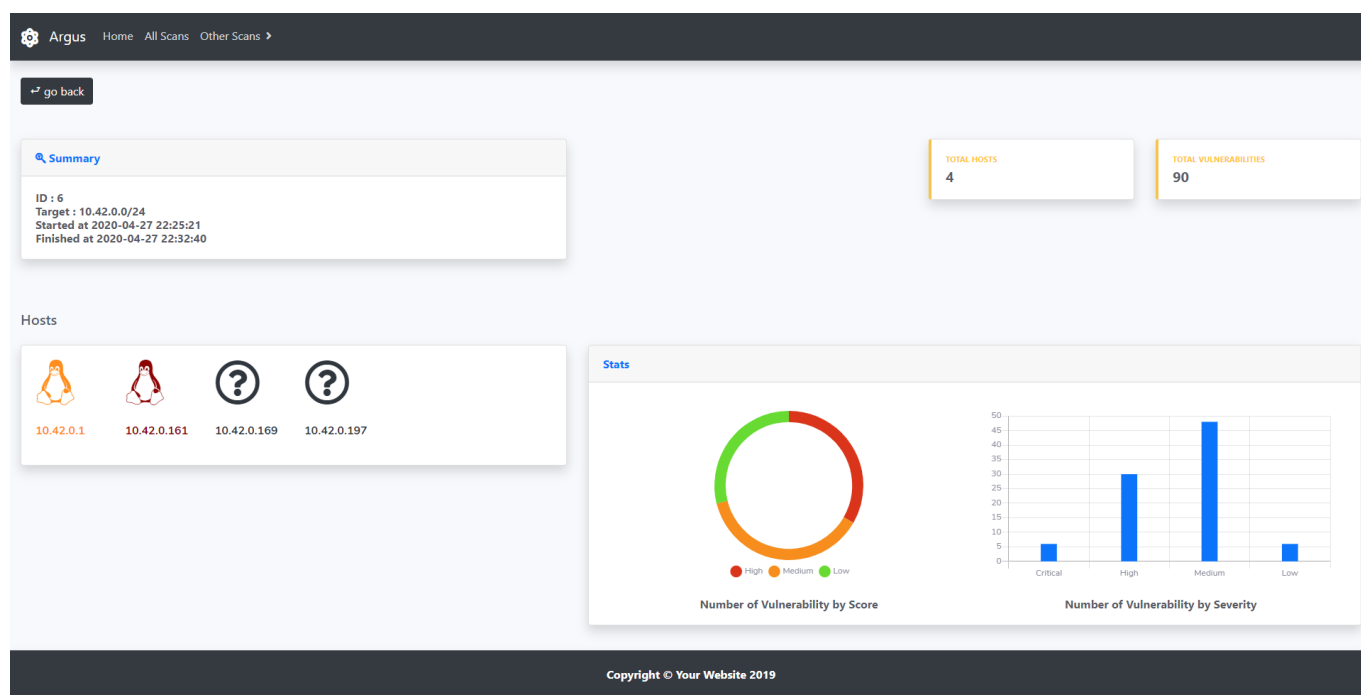
- nombre total de scans terminés
- nombre total de clients connectés
- les 5 derniers scans effectués
- les informations des clients actuellement connectés et actifs sur un scan
- une barre de progression qui s'affiche lorsqu'un scan est effectué



scan.php

Présente les informations suivantes :

- résumé des informations relatives au scan (cible et timestamp)
- les hôtes ayant été découverts sur le réseau ciblé (représentés par un logo du type d'équipement et par la couleur de la plus haute CVE découverte)
- statistiques (nombre total d'hôtes et de vulnérabilités)
- graphiques représentant les CVE découvertes par score et par sévérité



host.php

Présente les informations suivantes :

- résumé des informations relatives à l'hôte (IP, OS, Vendeur, dernier redémarrage)
- graphiques représentant les CVE découvertes par score et par sévérité ainsi que le total d'informations récoltées selon leurs types.
- tableau des services découverts ainsi que leur protocole, port et version
- tableau des cve découvertes triées par score
- liste des utilisateurs découverts sur l'hôte
- liste des outils utilisés et leur résultat

Argus

Home

All Scans

Other Scans

go back

11 - 10.42.0.1

12 - 10.42.0.161

13 - 10.42.0.169

14 - 10.42.0.197

Summary

ID : 12
SCAN ID : 6
IP : 10.42.0.161
OS : Linux 2.6.9 - 2.6.33
Vendor : Apple
Last Boot : Mon Apr 27 22:18:55 2020

Stats

High

Medium

Low

Number of Vulnerability by Score

Critical

High

Medium

Low

Number of Vulnerability by Severity

Service

User

Tool

Number of Information gathered

CVE Detected

Click to Hide

| score | name | severity | complexity | service | info |
|-------|----------------|----------|------------|---------|-----------------|
| 10.0 | CVE-2010-0425 | HIGH | LOW | http | <div>View</div> |
| 9.8 | CVE-2019-10211 | CRITICAL | LOW | mysql | <div>View</div> |
| 9.8 | CVE-2015-3166 | CRITICAL | LOW | mysql | <div>View</div> |
| 9.8 | CVE-2015-0244 | CRITICAL | LOW | mysql | <div>View</div> |
| 9.8 | CVE-2018-1312 | CRITICAL | LOW | http | <div>View</div> |
| 9.8 | CVE-2017-7679 | CRITICAL | LOW | http | <div>View</div> |
| 9.1 | CVE-2018-1115 | CRITICAL | LOW | mysql | <div>View</div> |
| 8.8 | CVE-2015-0243 | HIGH | LOW | mysql | <div>View</div> |

modules/arch/win32/mod_isapi in mod_isapi in the Apache HTTP Server 2.0.37 through 2.0.63, 2.2.0 through 2.2.14, and 2.3.x before 2.3.7, when running on Windows, does not ensure that request processing is complete before calling isapi_unload for an ISAPI .dll module, which allows remote attackers to execute arbitrary code via unspecified vectors related to a crafted request, a reset packet, and

Services

3.5

CVE-2010-0733

LOW

MEDIUM

mysql

View

2.6

CVE-2012-2687

LOW

HIGH

http

View

2.6

CVE-2008-5161

LOW

HIGH

ssh

View

2.6

CVE-2009-4022

LOW

HIGH

domain

View

1.2

CVE-2011-4415

LOW

HIGH

http

View

Tools

nmap

nbtsan

CMD : [nbtsan, 10.42.0.0/24]
Started at 2020-04-27 22:32:06
Doing NBT name scan for addresses from 10.42.0.0/24
IP address NetBIOS Name Server User MAC address
10.42.0.197 STRRR acibc32:88:42:3f
10.42.0.161 METASPLOITABLE METASPLOITABLE 00:00:00:00:00:00

enum4Linux

smtp-user-enum

dig

192.168.0.20/24 [daily-host.php?id=1739map5]

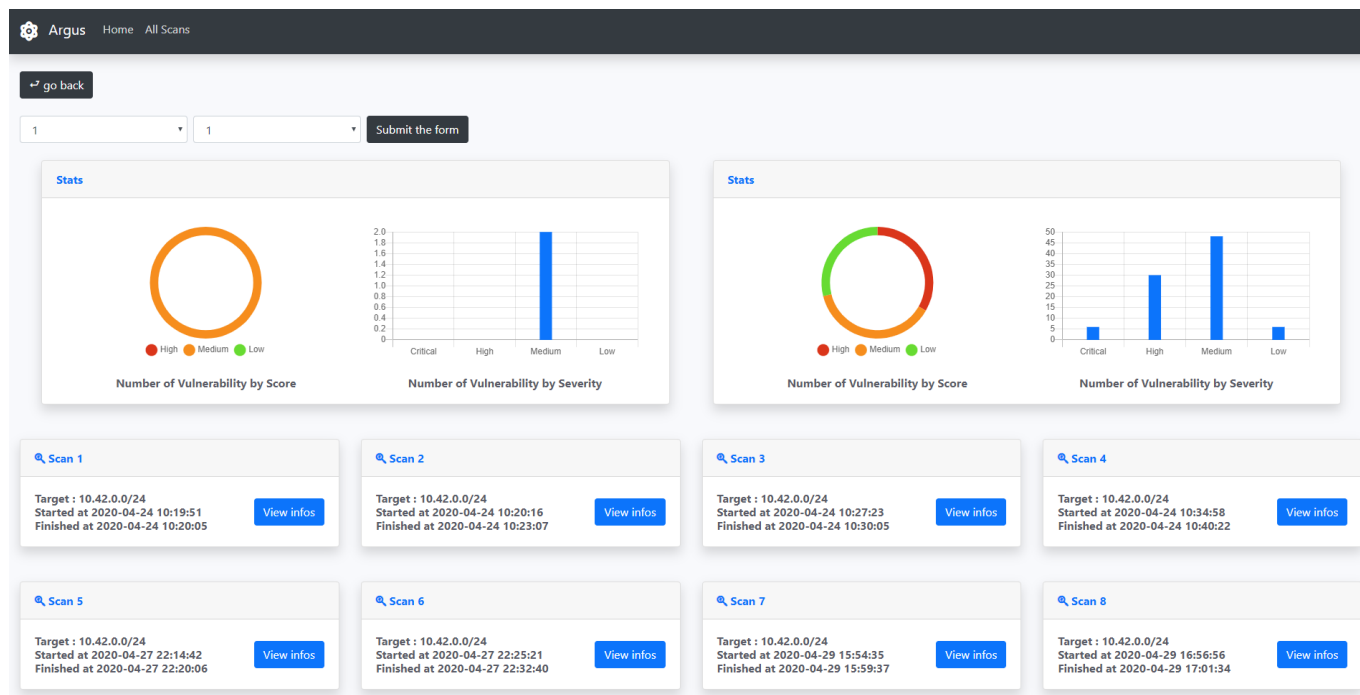
Users

BACKUP
MAIL
NEWS
POSTMASTER
ROOT
SYS
Service
USER
User
bin
daemon
ftp
games
lp
mail
man
news
nobody
postgres
postmaster
root
root
root@localhost
service
sync
sys
user
uucp

all_scans.php

Présente les informations suivantes :

- liste complète des scans effectués et liés à ce serveur
- deux cadres permettant la comparaison entre deux scans sélectionnés



config.php

Permet de définir les informations de connexion à la base de données

```
<?php
```

```
define('DB_SERVER', 'localhost');
define('DB_USERNAME', 'bob');
define('DB_PASSWORD', 'bob');
define('DB_DATABASE', 'STAGE');
$db = mysqli_connect(DB_SERVER,DB_USERNAME,DB_PASSWORD,DB_DATABASE);
```

```
?>
```