

Manuel Utilisateur 3PROJ

Réalisé par :
BERRADA Yahia

SOMMAIRE

1) Introduction

2) Utilisation du serveur

3) Utilisation du client

4) Utilisation du monitoring

5) Utilisation du backup

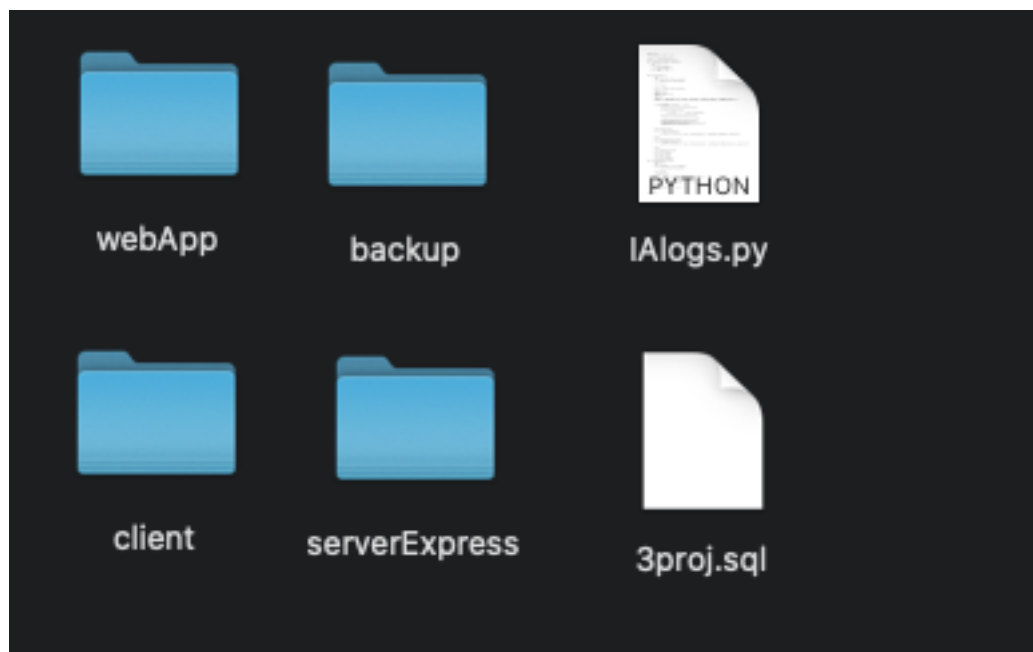
6) Utilisation du script intelligent

1) Introduction

Dans ce manuel utilisateur nous allons voir comment utiliser ce projet ainsi que les différentes applications de ce projet qui peuvent être lancées.

Nous verrons aussi les différentes fonctionnalités de chaque application de ce projet.

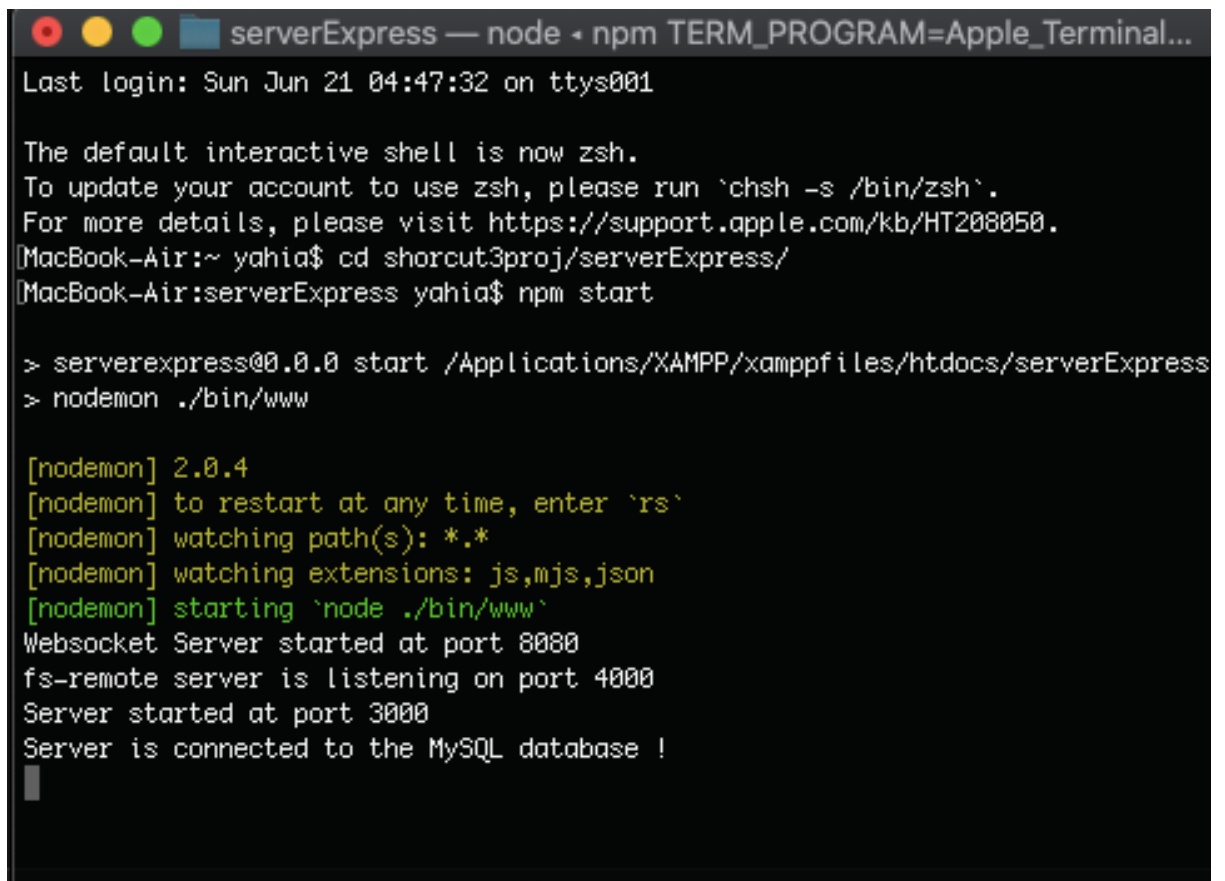
Le projet entier est composé des dossiers suivants :



2) Utilisation du serveur

Étant donné que le serveur est réalisé avec NodeJS, il faudra installer NodeJS sur votre machine pour pouvoir exploiter le serveur de ce projet.

Pour utiliser le serveur, il faut se rendre dans le dossier serverExpress avec un terminal ou un cmd et taper la commande npm start.



```
serverExpress — node • npm TERM_PROGRAM=Apple_Terminal...
Last login: Sun Jun 21 04:47:32 on ttys001


The default interactive shell is now zsh.
To update your account to use zsh, please run `chsh -s /bin/zsh`.
For more details, please visit https://support.apple.com/kb/HT208050.
MacBook-Air:~ yahia$ cd shorcut3proj/serverExpress/
MacBook-Air:serverExpress yahia$ npm start

> serverexpress@0.0.0 start /Applications/XAMPP/xamppfiles/htdocs/serverExpress
> nodemon ./bin/www

[nodemon] 2.0.4
[nodemon] to restart at any time, enter `rs`
[nodemon] watching path(s): *.*
[nodemon] watching extensions: js,mjs,json
[nodemon] starting `node ./bin/www`
Websocket Server started at port 8080
fs-remote server is listening on port 4000
Server started at port 3000
Server is connected to the MySQL database !
```

Comme nous pouvons l'apercevoir, cette commande va permettre de lancer les différents éléments de ce serveur qui sont expliqués dans la documentation technique.

Une fois que le serveur est lancé, nous avons accès au monitoring du serveur que nous verrons plus tard et aussi à l'application web du serveur de l'entreprise qui est démontré avec quelques images ci-dessous.


Health

Home Login Register Users

Lorem ipsum dolor sit amet, consectetur adipisicing elit. Architecto culpa ab, autem facilis incidunt inventore ratione vero debitis animi repellendus consequatur dolor maxime dolorem optio maiores aut, molestiae officiis facere. Lorem ipsum dolor sit amet, consectetur adipisicing elit. Architecto culpa ab, autem facilis incidunt inventore ratione vero debitis animi repellendus consequatur dolor maxime dolorem optio maiores aut, molestiae officiis facere. Lorem ipsum dolor sit amet, consectetur adipisicing elit. Architecto culpa ab, autem facilis incidunt inventore ratione vero debitis animi repellendus consequatur dolor maxime dolorem optio maiores aut, molestiae officiis facere. Lorem ipsum dolor sit amet, consectetur adipisicing elit. Architecto culpa ab, autem facilis incidunt inventore ratione vero debitis animi repellendus consequatur dolor maxime dolorem optio maiores aut, molestiae officiis facere. Lorem ipsum dolor sit amet, consectetur adipisicing elit. Architecto culpa ab, autem facilis incidunt inventore ratione vero debitis animi repellendus consequatur dolor maxime dolorem optio maiores aut, molestiae officiis facere. Lorem ipsum dolor sit amet, consectetur adipisicing elit. Architecto culpa ab, autem facilis incidunt inventore ratione vero debitis animi repellendus consequatur dolor maxime dolorem optio maiores aut, molestiae officiis facere. Lorem ipsum dolor sit amet, consectetur adipisicing elit. Architecto culpa ab, autem facilis incidunt inventore ratione vero debitis animi repellendus consequatur dolor maxime dolorem optio maiores aut, molestiae officiis facere.

© Health Company - 3PROJ SERVER


Health

Home Login Register Users

Login

Enter First Name

Password

Login

© Health Company - 3PROJ SERVER


Health

Home Profile Documents Users Logout

Select your document

Parcourir...

Add document

L'application web de ce serveur dispose de différentes pages tels que :

- Home
- Login
- Register
- Profile
- Users
- Documents

Ces différentes pages seront utilisés pour démontrer certaines vulnérabilités exploitées par le client.

3) Client

Le client étant aussi programmé en Nodejs, il faudra se rendre dans le dossier client et taper la commande npm start.

Si le serveur est correctement lancé, le client pourra donc se connecter et afficher le menu d'attaque ci-dessous :

```
client — node • npm TERM_PROGRAM=Apple_Terminal SHELL=/...
The default interactive shell is now zsh.
To update your account to use zsh, please run `chsh -s /bin/zsh`.
For more details, please visit https://support.apple.com/kb/HT208050.
MacBook-Air:~ yahia$ cd shortcut3proj
MacBook-Air:shortcut3proj yahia$ cd client/
MacBook-Air:client yahia$ npm start

> client@1.0.0 start /Applications/XAMPP/xamppfiles/htdocs/client
> nodemon client.js

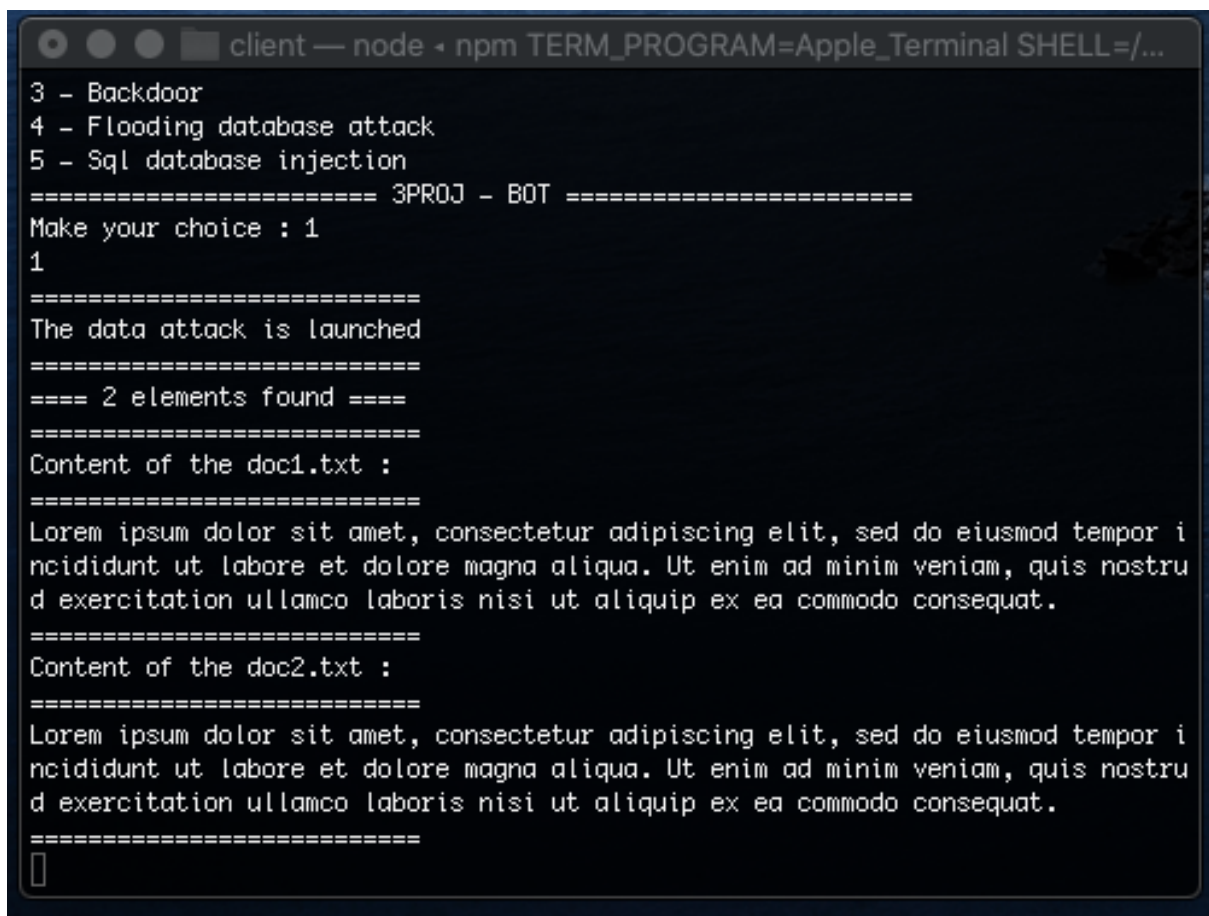
[nodemon] 2.0.4
[nodemon] to restart at any time, enter `rs`
[nodemon] watching path(s): *.*
[nodemon] watching extensions: js,mjs,json
[nodemon] starting `node client.js`
WebSocket Client Connected
===== 3PROJ - BOT =====
1 - Data attack
2 - DoS attack
3 - Backdoor
4 - Flooding database attack
5 - Sql database injection
===== 3PROJ - BOT =====
Make your choice : █
```

Comme nous pouvons le constater ce client propose de réaliser différentes attaques tels que :

- Data attack : consiste à voler des informations contenues dans des documents hébergés par les utilisateurs.
- DoS attack : consiste à mettre hors service le serveur en le surchargeant de connexion.
- Backdoor : consiste à injecter un fichier malicieux qui sera ensuite directement accessible par la plateforme web du serveur pour pouvoir l'exploiter.
- Flooding database : consiste à remplir la base de données à l'aide du formulaire d'inscription avec des fausses informations utilisateurs.
- Sql injection : consiste à injecter un code sql malicieux à la place des valeurs de connexion de la page login.

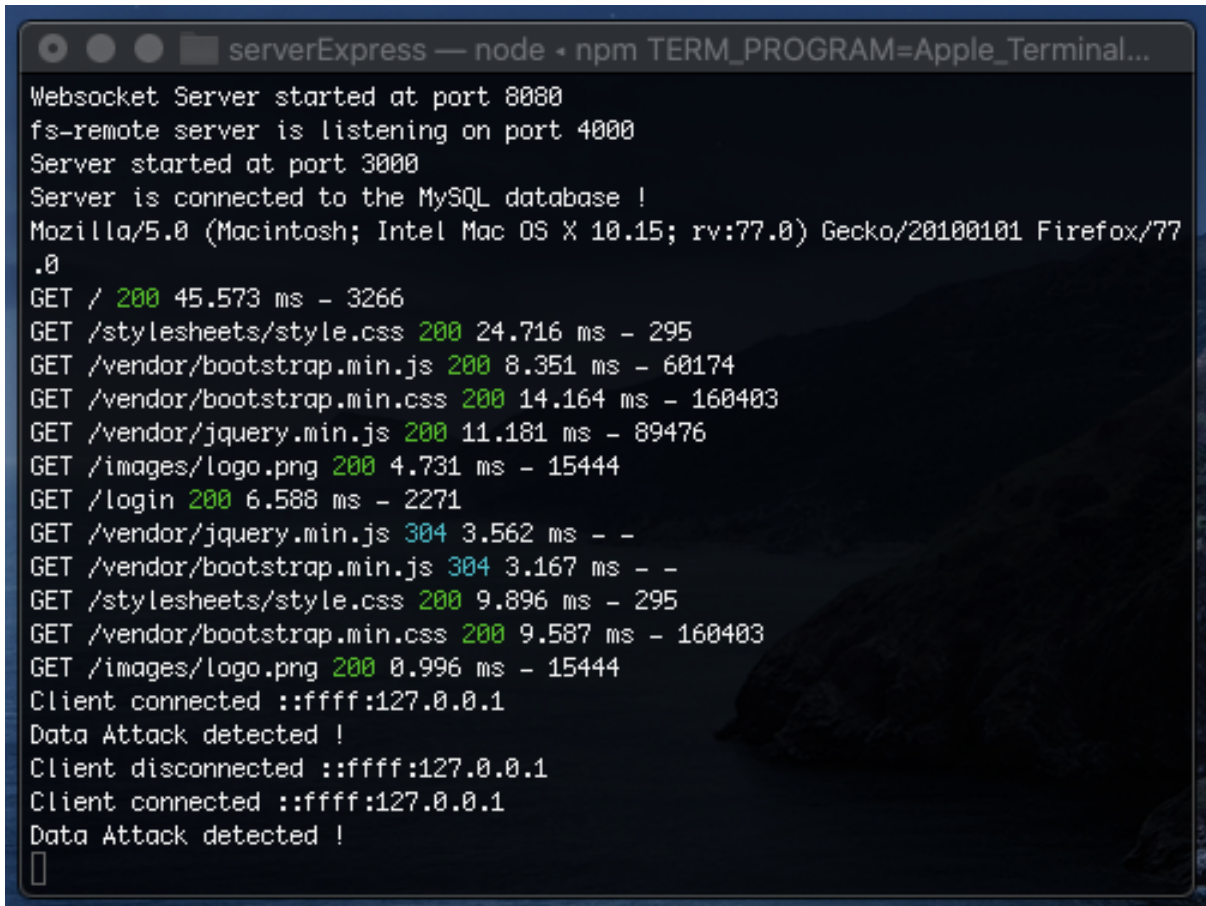
Prenons un exemple avec la première attaque proposée par le menu : data attack.

Cette attaque comme l'illustre l'image ci-dessous à permis de récupérer 2 éléments trouvés qui sont doc1.txt et doc2.txt afin de récupérer les données de ces fichiers.



```
client — node • npm TERM_PROGRAM=Apple_Terminal SHELL=/...
3 - Backdoor
4 - Flooding database attack
5 - Sql database injection
===== 3PROJ - BOT =====
Make your choice : 1
1
=====
The data attack is launched
=====
==== 2 elements found ====
=====
Content of the doc1.txt :
=====
Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor i
ncidunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostru
d exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat.
=====
Content of the doc2.txt :
=====
Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor i
ncidunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostru
d exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat.
=====
█
```


Suite à cette attaque, on peut apercevoir sur la partie du serveur, l'IP de la connexion de l'attaquant ainsi que la détection de l'attaque.



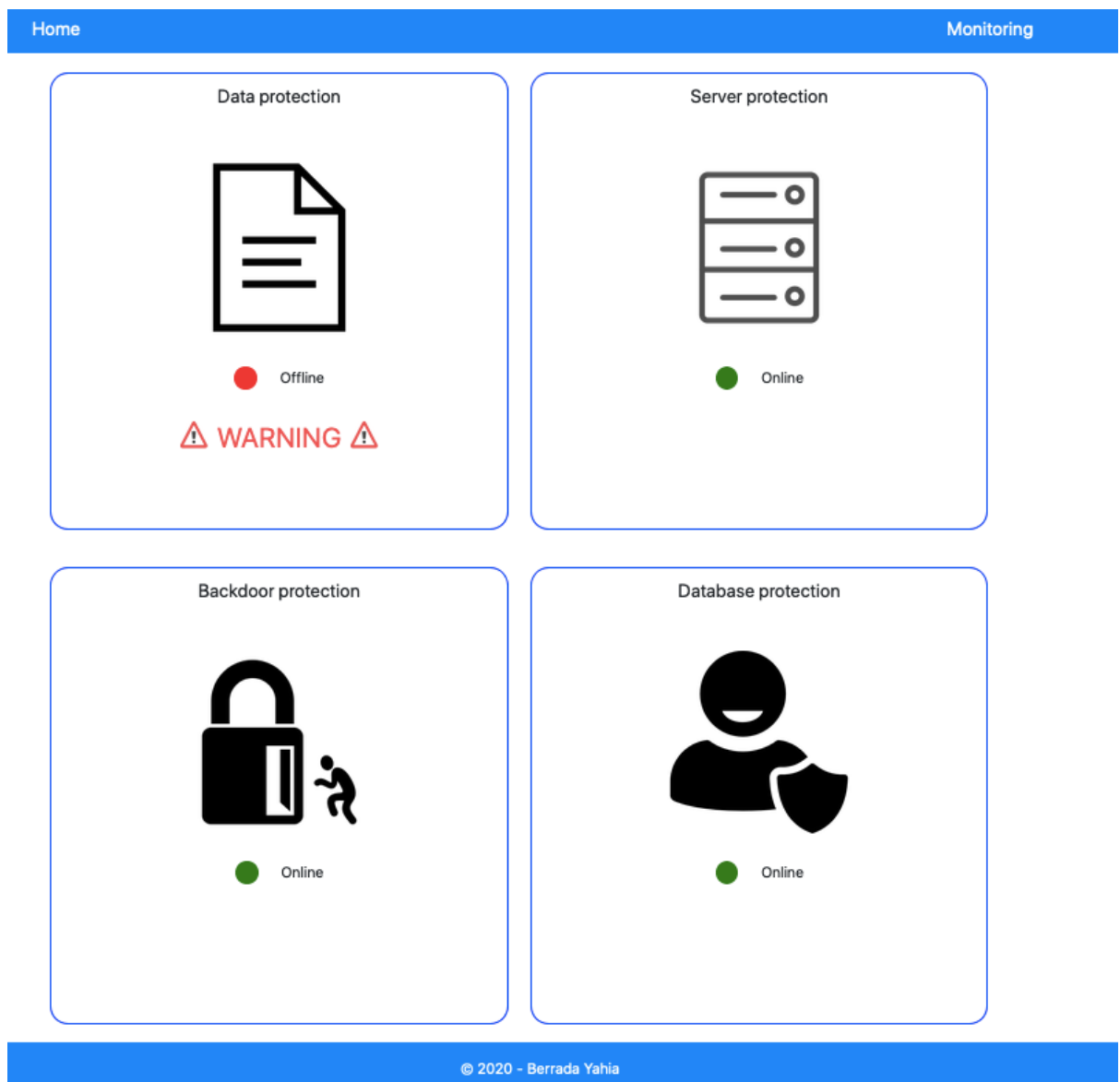
```
serverExpress — node • npm TERM_PROGRAM=Apple_Terminal...
Websocket Server started at port 8080
fs-remote server is listening on port 4000
Server started at port 3000
Server is connected to the MySQL database !
Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:77.0) Gecko/20100101 Firefox/77.0
GET / 200 45.573 ms - 3266
GET /stylesheets/style.css 200 24.716 ms - 295
GET /vendor/bootstrap.min.js 200 8.351 ms - 60174
GET /vendor/bootstrap.min.css 200 14.164 ms - 160403
GET /vendor/jquery.min.js 200 11.181 ms - 89476
GET /images/logo.png 200 4.731 ms - 15444
GET /login 200 6.588 ms - 2271
GET /vendor/jquery.min.js 304 3.562 ms - -
GET /vendor/bootstrap.min.js 304 3.167 ms - -
GET /stylesheets/style.css 200 9.896 ms - 295
GET /vendor/bootstrap.min.css 200 9.587 ms - 160403
GET /images/logo.png 200 0.996 ms - 15444
Client connected ::ffff:127.0.0.1
Data Attack detected !
Client disconnected ::ffff:127.0.0.1
Client connected ::ffff:127.0.0.1
Data Attack detected !
█
```

4) Utilisation du monitoring

Pour utiliser le monitoring il faudra installer php ainsi que mysql sur votre machine.

Le code source de ce monitoring est dans le dossier webApp.

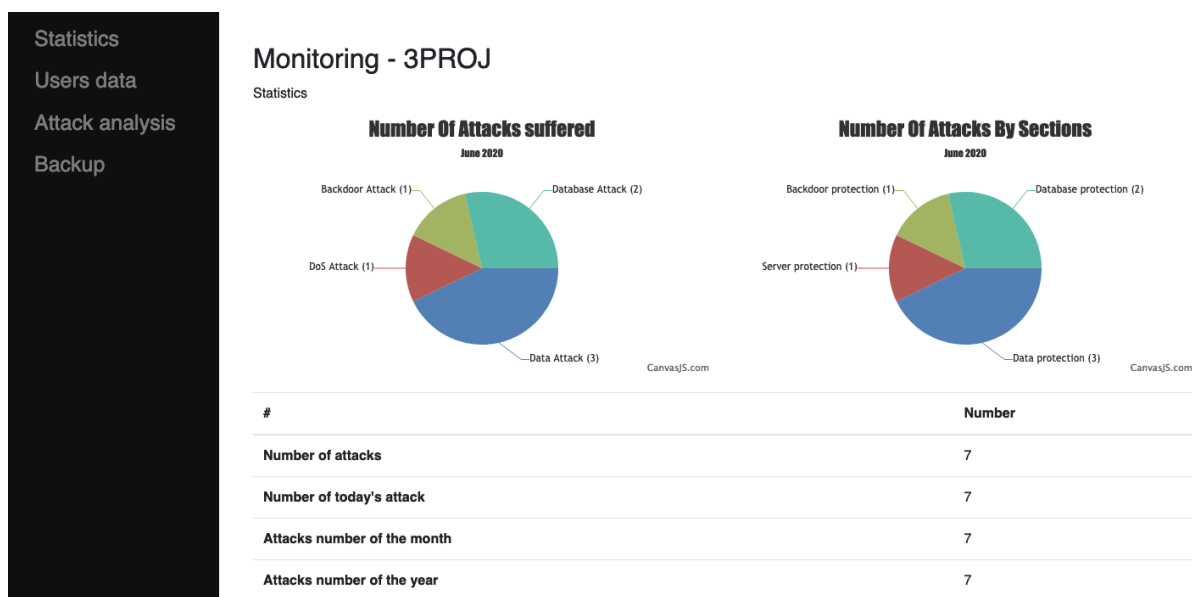
Suite aux différentes attaques que peut subir le serveur, on peut utiliser le monitoring pour voir les parties des sections affectées comme le montre l'image ci-dessous :



Comme nous pouvons l'observer, la page d'accueil du monitoring permet de lister les différents services du serveur et leur état actuel de protection. Par exemple dans cette illustration on peut voir que la section Data protection est en warning car elle a subi une récente attaque de vol d'informations.

Maintenant, nous allons voir la partie administration du monitoring qui contient plusieurs pages, à savoir :

- Une page de statistiques : liste et nombres d'attaques, liste et nombres d'attaques par sections, nombres d'attaques par jour, mois et année.



- Une page données utilisateurs : qui contient l'ensemble des utilisateurs et de leurs documents associés.

Statistics	Monitoring - 3PROJ			
Users data	Users Data (4 total)			
Attack analysis				
Backup				
#	Firstname	Lastname	Nb documents	Documents
1	Yahia	Berrada	2	resume.pdf yahia.png
2	ouxNv	uYdRi	0	
3	UT2i	JdSP	0	
4	I	x	0	

- Une page analyse des attaques : liste les différentes attaques subies et peut filtrer les attaques par l'ip de l'attaquant.

Statistics	Monitoring - 3PROJ			
Users data	Analysis (7 total)			
Attack analysis				
Backup				
	<input type="text" value="Filter IP"/>	<input type="button" value="Filter"/>		
#	Attack name	Attack date	Section ID	Ip attacker
4	Database Attack	2020-06-21	Database protection	::ffff:127.0.0.1
5	Database Attack	2020-06-21	Database protection	::ffff:127.0.0.1
3	Backdoor Attack	2020-06-21	Backdoor protection	::ffff:127.0.0.1
2	DoS Attack	2020-06-21	Server protection	::ffff:127.0.0.1
1	Data Attack	2020-06-21	Data protection	::ffff:127.0.0.1
6	Data Attack	2020-06-21	Data protection	::ffff:127.0.0.1
7	Data Attack	2020-06-21	Data protection	::ffff:127.0.0.1

- Une page backup : répertoriant les historiques de sauvegardes.

Statistics	Monitoring - 3PROJ	
Users data	Backup History (3 total)	
Attack analysis	#	Comment
Backup	1	2020-06-21 simple backup
	2	2020-06-21 simple backup
	3	2020-06-21 simple backup

5) Utilisation du backup

Le script du backup se trouve dans le dossier backup, pour. Ce script nécessite Nodejs pour être utilisé.

Il faudra donc dans un terminal ou un cmd utiliser la commande `node backup.js` pour utiliser ce programme qui permettra de générer un fichier sql de sauvegarde.

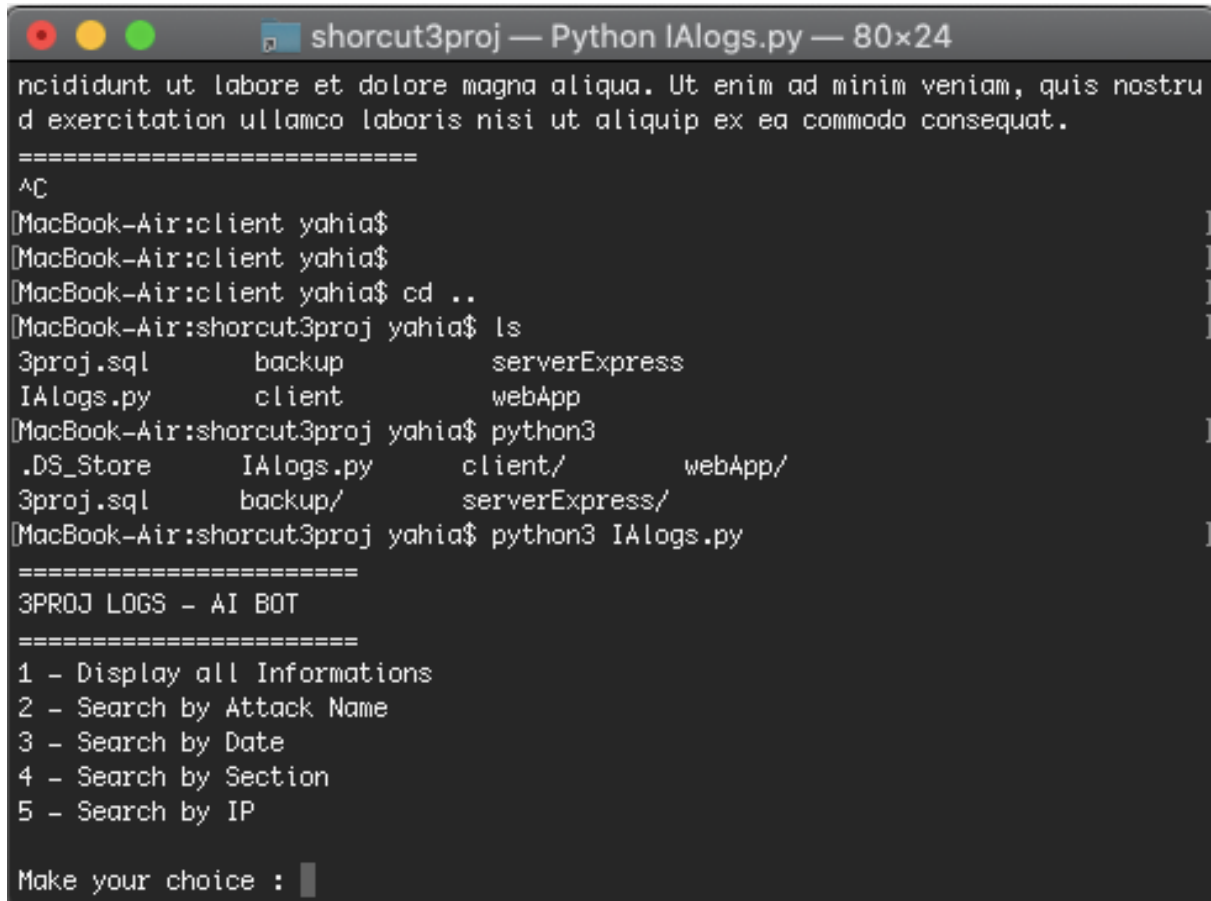
6) Utilisation du script intelligent

Ce script est réalisé en Python, il faudra donc avoir python sur sa machine pour pouvoir exploiter ce programme.

Pour le lancer il faudra donc faire la commande suivante dans un terminal ou un cmd : `python3 IAlogs.py` .

Ce script va permettre d'étudier les logs d'attaques et de pouvoir en tirer des informations concrètes.

Lors du lancement de ce script, le menu suivant apparaît :



```
ncididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostru
d exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat.
=====
^C
[MacBook-Air:client yahia$
[MacBook-Air:client yahia$
[MacBook-Air:client yahia$ cd ..
[MacBook-Air:shortcut3proj yahia$ ls
3proj.sql      backup      serverExpress
IAlogs.py      client      webApp
[MacBook-Air:shortcut3proj yahia$ python3
.DS_Store      IAlogs.py  client/    webApp/
3proj.sql      backup/    serverExpress/
[MacBook-Air:shortcut3proj yahia$ python3 IAlogs.py
=====
3PROJ LOGS - AI BOT
=====
1 - Display all Informations
2 - Search by Attack Name
3 - Search by Date
4 - Search by Section
5 - Search by IP

Make your choice : █
```

Ce script intelligent comme l'illustre l'image, dispose d'un menu qui permet de :

- Afficher toutes les informations des logs
- Chercher une information par nom d'attaque
- Chercher une information par date
- Chercher une information par section
- Chercher une information par ip

Voici une illustration montrant le choix d'afficher toutes les informations de logs :

```

shorcut3proj — Python lAlogs.py — 80x54
=====
attackName : Backdoor Attack
Date : 2020-6-21 at 4:56:22
section : backdoor protection
ip : ::ffff:127.0.0.1
=====
Attaque number : 4
=====
attackName : Database Attack
Date : 2020-6-21 at 4:56:22
section : database protection
ip : ::ffff:127.0.0.1
=====
Attaque number : 5
=====
attackName : Database Attack
Date : 2020-6-21 at 4:56:22
section : database protection
ip : ::ffff:127.0.0.1
=====
Attaque number : 6
=====
attackName : Data Attack
Date : 2020-6-21 at 12:35:14
section : data protection
ip : ::ffff:127.0.0.1
=====
Attaque number : 7
=====
attackName : Data Attack
Date : 2020-6-21 at 12:35:14
section : data protection
ip : ::ffff:127.0.0.1
=====
Attacks infos
attackName has occurred 0 times
Data Attack has occurred 3 times
DoS Attack has occurred 1 times
Backdoor Attack has occurred 1 times
Database Attack has occurred 2 times

Attacked Sections infos
data protection has occurred 3 times
server protection has occurred 1 times
backdoor protection has occurred 1 times
database protection has occurred 2 times

Attacker IP infos
Counter({'::ffff:127.0.0.1': 7})
Dates infos
Counter({'2020-6-21 at 4:56:22': 3, '2020-6-21 at 4:50:56': 2, '2020-6-21 at 12:35:14': 2})

Would you like to continue ? y/n : █

```

On peut observer que tout d'abord il y a un listing précis de toutes les attaques, puis des statistiques d'occurrences des différentes informations tels que les attaques, les sections, les ip et les dates.