Seguretat de la web

HTTPS:

S'ha implementat https a la web, per a augmentar la seguretat que aquesta aporta als usuaris.

Primer de tot, s'ha generat una clau privada amb CSR utilitzant aquesta comanda:

```
openssl req \
        -newkey rsa:2048 -nodes -keyout domain.key \
        -out domain.csr
```

·El *-newkey rsa:2048* especifica que la clau que es genera, ha de ser de 2048 bits i utilitzant l'algorisme RSA.
·Amb *-nodes* especifiquem que no volem que aquesta clau privada s'encripti amb una contrasenya.

Un com tenim la clau generada, hem de generar un certificat signat per si mateix a partir de la clau privada generada i CSR.

Bàsicament utilitzarem la següent comanda:

```
openssl x509 \
        -signkey domain.key \
        -in domain.csr \
        -req -days 365 -out domain.crt
```

·La opció *-days 365* ens indica que el certificat serà vàlid per 365 dies, podem modificar aquest valor si volem.

Ara ja tenim el certificat generat, així que els incluirem al docker:

Primer de tot, obrirem el ports d'Nginx amb la comanda:

```
nginx:
image : your_nginx_image/nginx:latest
ports :
   - "80:80"
   - "443:443"
```

Després muntem els certificats a la imatge de Nginx:

nginx:
image : your_nginx_image/nginx:latest
ports :

```
    - “80:80”
    - “443:443”
volumes:
    - /data/certs:/etc/nginx/certs
```

Ara modifiquem el fitxer de configuració d’ Nginx, originalment es troba així:

```
 server {
          listen 80:
          server_name  www.yoursite.com;
          location / {
                    proxy_pass http://frontend:500
                   error_log /var/log/front_end_errors.log;
          }
}
```

i el deixarem així:

```
server {
          listen 443 ssl;
          server_name  www.yoursite.com;
          ssl_certificate /etc/nginx/certs/your_site_crt_file.crt;
          ssl_certificate_key /etc/nginx/certs/your_site_crt_file.key;
          location / {
                    proxy_pass http://frontend:5000/;
                    error_log /var/log/front_end_errors.log;
          }
}
```

(en negreta els canvis que s’han realitzat).

Finalment carreguem la nova configuració:

```
          FROM nginx
          COPY nginx.conf /etc/nginx/conf.d/nginx.conf
```

Tot el que ens queda ja es redirigir les peticions de HTTP a HTTPS, bàsicament modifiiarem el fitxer nginx.conf deixant-lo així:

```
server {
          listen     80;
          server_name  localhost;

          return 301 https://$host$request_uri;
}
server {
```

```
        listen      443;
        server_name  localhost;

        ssl                  on;
        ssl_certificate   localhost.pem;
        ssl_certificate_key  localhost.key;

        ssl_session_timeout  5m;

        ssl_protocols  SSLv2 SSLv3 TLSv1;
        ssl_ciphers  HIGH:!aNULL:!MD5;
        ssl_prefer_server_ciphers   on;

        location / {
                root   /usr/share/nginx/html;
                index  index.html index.htm;
        }
}
```

I finalment executem la següent comanda:

docker run --rm --name nginx -p 80:80 -p 443:443 -v `pwd`/nginx.conf:/etc/nginx/conf.d/default.conf:ro -v `pwd`/localhost.key:/etc/nginx/localhost.key:ro -v `pwd`/localhost.pem:/etc/nginx/localhost.pem:ro nginx

ADMINISTRACIÓ:

Per altra banda, es pot accedir a la web com un gestor desde el link:
http://craaxcloud.epsevg.upc.edu:36080/
identifican-te com un administrador. Altrament no es deixarà entrar.

Actualment, l'únic administrador de la base de dades és:

User: alfred.pennyworth@gothamcitymail.com
Pass: mayordomo123