Zadanie 7
I-UPB: Úvod do počítačovej bezpečnosti

November 29, 2021

1 Úvod

Cieľom zadania je demonštrovať útok na nezabezpečenú aplikáciu s ktorou používateľ komunikuje cez protokol HTTPS a neskôr aplikáciu zabezpečiť pomocou HTTPS protokolu a SSL certifikátu podpísaného známou autoritou.

V tomto prípade bola vytvorená jednoduchá statická webová stránka ktorá bola poskytovaná používateľovi reverznej proxy nginx pre zjednodušenie konfigurácie SSL zabezpečenia.

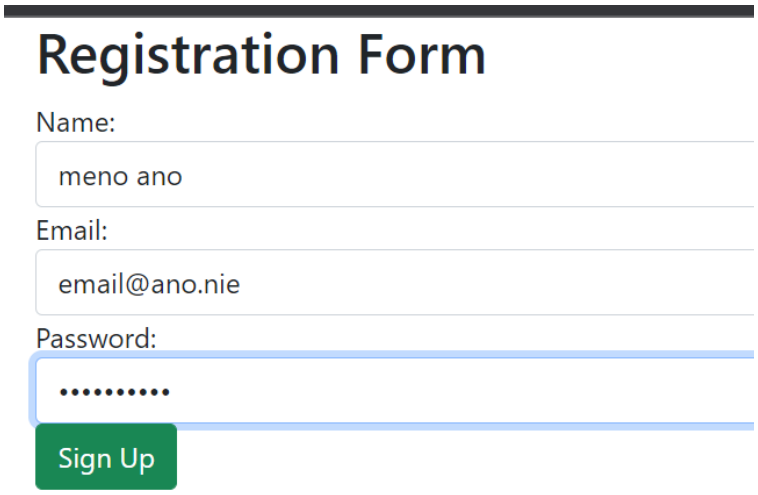

Figure 1: Webová aplikácia

2 Konfigurácia servera

Spomínaný server pre svoje fungovanie pomocou HTTP nepotrebuje žiadnu špeciálnu konfiguráciu iba skopírovať súbory do adresára ktorý je nadstavený ako default pre statické súbory. Zároveň default otvorený port je 80 ktorý sa štandardne používa pre webové aplikácie. Po nahrati html súboru do priečinka *html* môžeme vidieť našu webovú aplikáciu s formulárom.

2.1 HTTP

Keďže náš server je nakonfigurovaný na HTTP protokol tak nástrojom Wireshark dokážeme odchytávať nezašifrovanú komunikáciu.

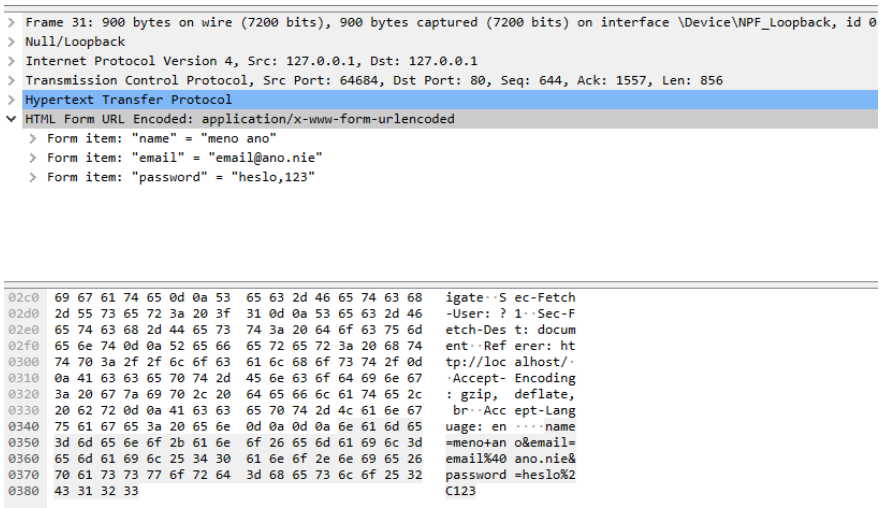

Figure 2: Odchytávanie nešifrovanej komunikácie

Na obrázku vidíme že dochytené dáta obsahujú nami vyplnený formulára.

2.2 HTTPS

Pokiaľ chceme zabezpečiť komunikáciu aby nemohla byť jednoducho odchytávaná tak je nutné nginx nadstaviť aby na všetkú prichádzajúcu komunikáciu na porte 80 presmerovával na port 433 a používal HTTPS protokol.

```
 server {
    listen       80;
    server_name  localhost;
    location / {
        root   html;
        index  index.html index.htm;
    }
 return 301 https://$host$request_uri;
}
```

Uvedená konfigurácia obsahuje defaultné nastavenie adresárov pre statické súbory a hlavne presmerovania každej požiadavky na protokol HTTPS.

Ďalej musíme nakonfigurovať nginx pre HTTPS protokol čo spravíme následujúcim konfigom.

```
server {
    listen       443 ssl;
    server_name  localhost;
    ssl_certificate      cert.pem;
    ssl_certificate_key  key.pem;
    ssl_session_cache    shared:SSL:1m;
    ssl_session_timeout  5m;
    ssl_ciphers  HIGH:!aNULL:!MD5;
    ssl_prefer_server_ciphers  on;
    location / {
        root   html;
        index  index.html index.htm;
    }
}
```

Konfigurácia obsahuje dôležitú časť a to je SSL certifikát. Použitý SSL certifikát je self-signed čo má za následok že návštevník webovej aplikácie bude najskôr upozornený že certifikát nevydávala žiadna registrovaná certifikačná autorita.

Pre vygenerovanie self-signed SSL certifikátu bol použitý nástroj OpenSSL. Príkaz pre vygenerovanie SSL certifikátu platného 1 rok je:

```
openssl req -x509 -newkey rsa:4096 -nodes -out cert.pem -keyout key.pem -days 365
```

Keď naštívime našu webovú aplikáciu tak sme okmžite presmerovaný na HTTPS protokol ktorý je na porte 433.

Po tejto konfigurácií môžeme odchytávať komunikáciu cez HTTPS protokol no neuvidíme žiadne dáta.

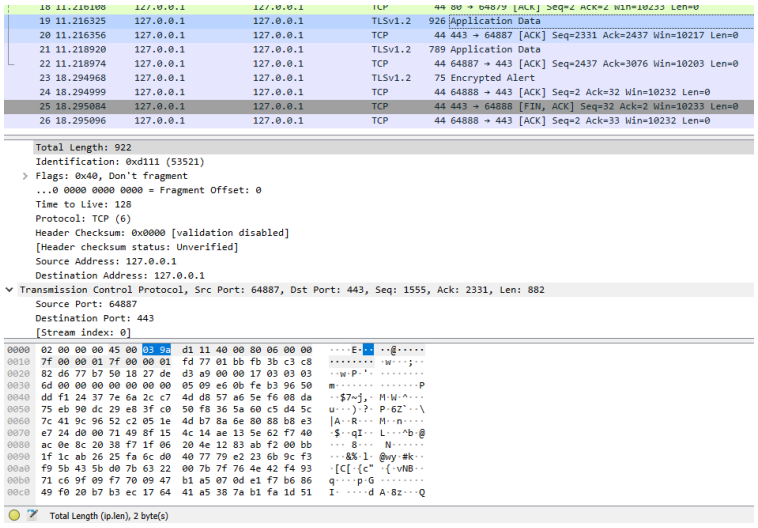

Figure 3: Odchytávanie šifrovanej komunikácie