

# UPB – Zadanie 7

## TLS (HTTPS) KOMUNIKÁCIA S WEB SERVEROM


Hosting: freeinfinity.net

SSL: GoGetSSL od freeinfinity.net

Sniffing tool: WireShark

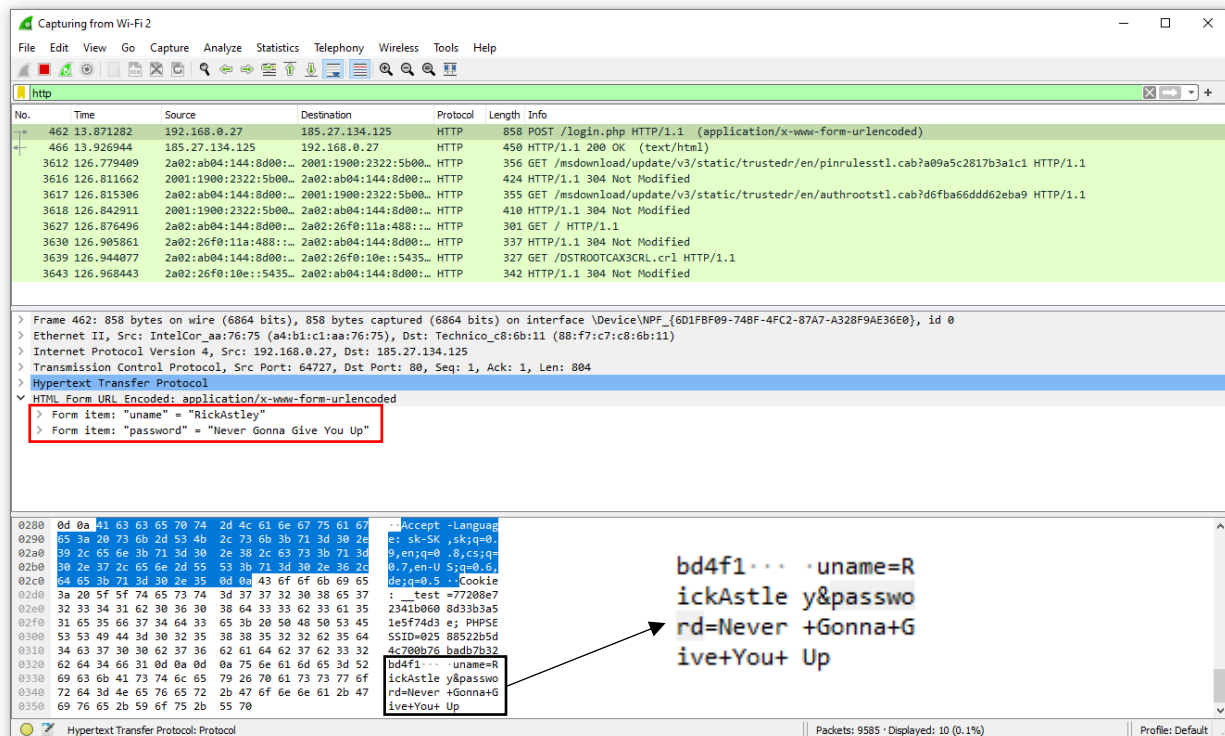
Založil som si účet na infinityfree.net a vytvoril stránku, kde je jednoduchý formulár na prihlásenie. Následne nás presmeruje na stránku kde nám vypíše meno a heslo.

<http://upb7.lovestoblog.com/>



Web, ktorý nám bol poskytnutý bohužiaľ nemá SSL certifikát a teda je aplikácia zraniteľná a použité údaje môžu byť odchytené pomocou sniffingu. Na sniffing sme použili **WireShark**.





Na obrázku si môžeme všimnúť ako boli odchytené údaje meno a heslo.

## SSL

<https://upb7.lovestoblog.com/>

Na inštaláciu SSL som použil verziu, ktorú zdarma infinityfree poskytuje. Zvolený bol konkrétne GoGetSSL, ktorý poskytuje verziu na 90 dní zdarma.

Šifrovanie : 2048 BIT RSA kľúč, SHA256withRSA, podporuje TLS 1.2. Čo je dostatočné na ochranu stránky.

Common name: upb7.lovestoblog.com  
 SANs: upb7.lovestoblog.com, www.upb7.lovestoblog.com  
 Valid from November 24, 2021 to February 23, 2022  
 Serial Number: 34ab9e55843eae4646f39e6de92b9f83  
 Signature Algorithm: sha256WithRSAEncryption  
 Issuer: GoGetSSL RSA DV CA

### Certificate #1: RSA 2048 bits (SHA256withRSA)

**Server Key and Certificate #1**

<b>Subject</b>	upb7.lovestoblog.com Fingerprint SHA256: 2a54e3ede08297d31b17891bd74d08196a2bf10a2978774148a178e711851 Pin SHA256: ar0PKJVVU4Xcy0y8yHVNMOHF5RPTTKppDOeamuLcWUj
<b>Common names</b>	upb7.lovestoblog.com
<b>Alternative names</b>	upb7.lovestoblog.com www.upb7.lovestoblog.com
<b>Serial Number</b>	34ab9e55843eae4646f39e6de02b983
<b>Valid from</b>	Thu, 25 Nov 2021 00:00:00 UTC
<b>Valid until</b>	Wed, 23 Feb 2022 23:59:59 UTC (expires in 2 months and 29 days)
<b>Key</b>	RSA 2048 bits (e 65537)
<b>Weak key (Debian)</b>	No
<b>Issuer</b>	GoGetSSL RSA DV CA AIA: http://ort.usertrust.com/GoGetSSLRSADVCA.crt
<b>Signature algorithm</b>	SHA256withRSA
<b>Extended Validation</b>	No
<b>Revocation information</b>	CRL, OCSP CRL: http://ort.usertrust.com/GoGetSSLRSADVCA.crl OCSP: http://ocsp.usertrust.com
<b>Revocation status</b>	Good (not revoked) OCSP ERROR: Request failed with OCSP status: 6 [http://ocsp.usertrust.com]
<b>DNS CAA</b>	No ( <a href="#">more info</a> )
<b>Trusted</b>	Yes Mozilla Apple Android Java Windows

**Additional Certificates (if supplied)**

<b>Certificates provided</b>	1 (1468 bytes)
<b>Chain issues</b>	Incomplete

**Certification Paths**

[Click here to expand](#)

Capturing from Wi-Fi 2

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ssl

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	162.159.134.234	192.168.0.27	TLSv1.2	215	Application Data
3	0.124863	192.168.0.27	185.27.134.125	TCP	55	52557 → 443 [ACK] Seq=1 Ack=1 Win=515 Len=1 [TCP segment of a reassembled PDU]
6	0.187941	162.159.134.234	192.168.0.27	TLSv1.2	133	Application Data
9	0.492759	192.168.0.27	31.13.84.23	TLSv1.2	83	Application Data
14	0.553682	31.13.84.23	192.168.0.27	TLSv1.2	79	Application Data
18	0.651856	192.168.0.27	104.26.8.174	TCP	55	52558 → 443 [ACK] Seq=1 Ack=1 Win=510 Len=1 [TCP segment of a reassembled PDU]
29	1.497390	2a02:ab04:144:8d00::2a03:2800:f007:18:f	2a03:2800:f007:18:f	TLSv1.2	183	Application Data
30	1.497391	2a02:ab04:144:8d00::2a03:2800:f007:18:f	2a03:2800:f007:18:f	TLSv1.2	183	Application Data

> Frame 9: 83 bytes on wire (664 bits), 83 bytes captured (664 bits) on interface \Device\NPF\_{601FBF09-74BF-4FC2-87A7-A328F9AE36E0}, id 0

> Ethernet II, Src: IntelCor\_aa:76:75 (a4:b1:c1:aa:76:75), Dst: Technico\_c8:6b:11 (88:f7:c7:c8:6b:11)

> Internet Protocol Version 4, Src: 192.168.0.27, Dst: 31.13.84.23

> Transmission Control Protocol, Src Port: 52635, Dst Port: 443, Seq: 1, Ack: 1, Len: 29

▼ Transport Layer Security

▼ TLSv1.2 Record Layer: Application Data Protocol: http-over-tls

Content Type: Application Data (23)

Version: TLS 1.2 (0x0303)

Length: 24

Encrypted Application Data: dcab86bb4284a968a7ef1ccbd212a7c05c97b56f30266599

[Application Data Protocol: http-over-tls]

```

0000  88 f7 c7 c8 6b 11 a4 b1 c1 aa 76 75 08 00 45 00  ....k...vu..E.
0010  00 45 bd b6 40 00 00 06 00 00 c0 a8 00 1b 1f 0d  .E..@:.....
0020  54 17 cd 9b 01 bb 12 08 75 92 68 3c 66 4f 50 1e  T.....u.h<FOP
0030  02 03 34 1f 00 00 17 03 03 00 18 dc ab 86 bb 42  .4.....B
0040  84 a9 68 a7 ef 1c cb d2 12 a7 c0 5c 97 b5 6f 30  .h.....\...o
0050  26 65 99                                     &e.
  
```

Transmission Control Protocol (tcp), 20 bytes

Packets: 4521 · Displayed: 1564 (34.6%)

Profile: Default

Môžeme si všimnúť že dáta sú zašifrované a teda je aplikácia ochránená oproti tomuto typu útoku, keďže útok pomocou WireShark sa nepodaril.