**USTH-BS3 – Web Security-Lab 03: Create and deploy SSL/TLS certificates for websites (1,75 hour)**SSL/TLS certificates have been widely used to enable secure communication using SSL/TLS protocol between clients and servers, especially for websites and web applications.

1. Steps to create and deploy SSL/TLS certificates for websites

* Create a certificate request that contains all ID and website domain name information. Then save the request into a .csr file
  + Most OS/service platforms support tools to create certificate requests
* Send the certificate request file to a certificate authority (CA), such as Verisign, Thawte,… to place an order and make a payment.
* The request will be processed and if approved, a SSL certificate is issued
* When receiving the certificate file 🡪 install into the system
* Assign the certificate to the website.

2. Create a self-signed SSL certificate using Server Certificates function in Microsoft IIS

* Start Windows server / Windows 8, Windows 10
* Open Internet Information Services (IIS) Manager
* Select item Server Certificates
* Click at the Create Self-Signed Certificate on the right-side menu
* Enter the Friendly name (domain name) for the certificate.

We can only create the certificate for the current machine using this tool.

3. Create a SSL certificate using Openssl

* Openssl is an open source tool that allows users to generate key-pair, create certificate request and self-signed certificate.
* Get openssl from: <https://www.openssl.org/source/>
* Install openssl using its user guide
* Generate key-pair: **openssl genrsa -des3 -out server.key 1024**
* Create a certificate request: **openssl req -new -key server.key -out server.csr**
* Create a self-signed SSL certificate:

**openssl x509 -req -days 365 -in server.csr -signkey server.key -out server.crt**

4. Install and assign SSL certificates

* For websites running on MS Windows 🡪 using Microsoft IIS manager
* For websites running on Apache/nginx 🡪 using the server guide.

5. Requested tasks to be completed for students:

5.1. Create a certificate request, save to a file and review the content 🡪 save screenshot to a word file

5.2 Create a self-signed certificate, save to a file and review the content 🡪 save screenshot to a word file

5.3 Create a website on the web server and assign the self-signed certificate to the website

5.4 View the https website on the browser 🡪 save screenshot to a word file

5.5 View the self-signed certificate on the browser 🡪 save screenshot to a word file.

**USTH-BS3 – Web Security -Lab 04: Hijack web sessions (1,25 hour)  
  
A. Review of web sessions**

Review lecture notes, chapter 3, “Securing web sessions” section:

- What is a web session

- How a session is created and how the web server and web client communicate using session token

- Weaknesses in session management

- Measures for securing web sessions.

**B. Labs**

*1. Capture Session ID / token*

- Use Google Chrome, open web page http://attt.ptit.edu.vn:81/code/login.asp

- Start Wireshark snipping tool, select to capture traffic on the interface to capture internet traffic (if you do not have Wireshark, download and install it from https://www.wireshark.org/download.html)

- In Google Chrome, enter username and password to log in (account information will be provided by the lecturer) 🡺 capture the screen and paste into word file

- Go back to Wireshark, enter http in the top filter box to view http traffic only. Open or search for ASPSESSION in the http response. 🡺 capture the screen and paste into word file

- Right click your mouse at the item and select Copy/Value, and then paste into a text editor, such as Notepad.

*2. Insert Cookie/Session ID into web browser*

- Install Firefox web browser if you do not have it on your machine

- Start Firefox. Then open the URL <https://addons.mozilla.org/vi/firefox/addon/a-cookie-manager/> to add the add-on **Cookie Manager** into your Firefox. Cookie Manager allows users to manage cookies.

- Open **Cookie Manager** (new cookie) to insert a new cookie for http://attt.ptit.edu.vn:81 with the ASPSESSION information of session ID captured from step 1. 🡺 capture the screen and paste into word file

- In Firefox, open the URL <http://attt.ptit.edu.vn:81/code/login_success.asp> and see the results 🡺 capture the screen and paste into word file

*3. Find real http websites on the internet and try to hijack their sessions using same techniques.*

*4. How to defend*

- Use https to replace http for sessions with personal data.

*5. Using a simillar technique, hijack a facebook session*

- Log in into your FB account using Google Chrome

- Open Firefox. Check Google Chrome’s FB cookies to see what are the cookies to be imported to Firefox to get into your FB account without username and password.