1. Odpalenie ssl

```
teczap@Paw-PC:~/lab$ sudo a2enmod ssl
Considering dependency setenvif for ssl:
Module setenvif already enabled
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Enabling module socache_shmcb.
Enabling module ssl.
See /usr/share/doc/apache2/README.Debian.gz on how to configure SSL and create self-signed certificates.
To activate the new configuration, you need to run:
  service apache2 restart
teczap@Paw-PC:~/lab$ sudo a2enmod headers
Enabling module headers.
To activate the new configuration, you need to run:
  service apache2 restart
```

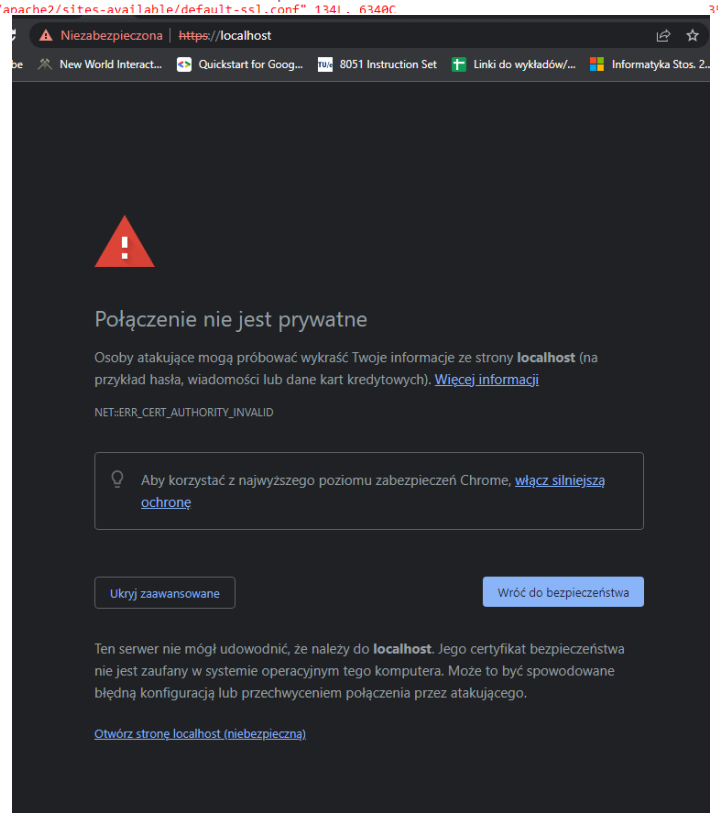
```
teczap@Paw-PC:~/lab$ ls /etc/certificate/
testowy.crt  testowy.key
```

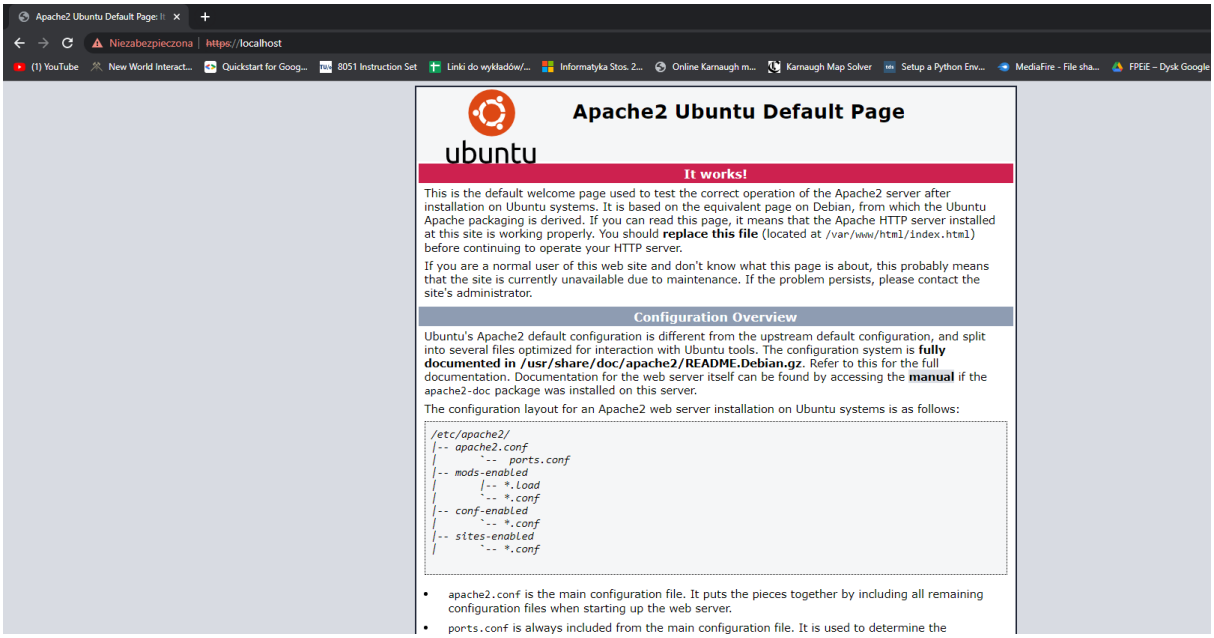
```
teczap@Paw-PC:~/lab$ sudo a2enconf ssl-params
Enabling conf ssl-params.
To activate the new configuration, you need to run:
  service apache2 reload
teczap@Paw-PC:~/lab$ sudo a2ensite default-ssl
Enabling site default-ssl.
To activate the new configuration, you need to run:
  service apache2 reload
teczap@Paw-PC:~/lab$ sudo apache2ctl configtest
Syntax OK
```

teczap@Paw-PC: ~/lab

```
SSLCipherSuite EECDH+AESGCM:EDH+AESGCM:AES256+EECDH:AES256+EDH

    SSLProtocol All -SSLv2 -SSLv3 -TLSv1 -TLSv1.1

    SSLHonorCipherOrder On


    Header always set X-Frame-Options DENY

    Header always set X-Content-Type-Options nosniff

    # Requires Apache >= 2.4

    SSLCompression off

    SSLUseStapling on

    SSLStaplingCache "shmcb:logs/stapling-cache(150000)"


    # Requires Apache >= 2.4.11

    SSLSessionTickets Off
~
~
~
```

```
<IfModule mod_ssl.c>
        <VirtualHost _default_:443>
                ServerAdmin webmaster@localhost

                DocumentRoot /var/www/html

                # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
                # error, crit, alert, emerg.
                # It is also possible to configure the loglevel for particular
                # modules, e.g.
                #LogLevel info ssl:warn

                ErrorLog ${APACHE_LOG_DIR}/error.log
                CustomLog ${APACHE_LOG_DIR}/access.log combined

                # For most configuration files from conf-available/, which are
                # enabled or disabled at a global level, it is possible to
                # include a line for only one particular virtual host. For example the
                # following line enables the CGI configuration for this host only
                # after it has been globally disabled with "a2disconf".
                #Include conf-available/serve-cgi-bin.conf

                #   SSL Engine Switch:
                #   Enable/Disable SSL for this virtual host.
                SSLEngine on

                #   A self-signed (snakeoil) certificate can be created by installing
                #   the ssl-cert package. See
                #   /usr/share/doc/apache2/README.Debian.gz for more info.
                #   If both key and certificate are stored in the same file, only the
                #   SSLCertificateFile directive is needed.
                SSLCertificateFile      /etc/test/localhost/localhost.crt
                SSLCertificateKeyFile /etc/test/localhost/localhost.decrypted.key

                #   Server Certificate Chain:
                #   Point SSLCertificateChainFile at a file containing the
                #   concatenation of PEM encoded CA certificates which form the
                #   certificate chain for the server certificate. Alternatively
                #   the referenced file can be the same as SSLCertificateFile
                #   when the CA certificates are directly appended to the server
                #   certificate for convinience.
                #SSLCertificateChainFile /etc/apache2/ssl.crt/server-ca.crt

                #   Certificate Authority (CA):
                #   Set the CA certificate verification path where to find CA
                #   certificates for client authentication or alternatively one
                #   huge file containing all of them (file must be PEM encoded)
                #   Note: Inside SSLCACertificatePath you need hash symlinks
                #               to point to the certificate files. Use the provided
                #               Makefile to update the hash symlinks after changes.
                #SSLCACertificatePath /etc/ssl/certs/
                #SSLCACertificateFile /etc/apache2/ssl.crt/ca-bundle.crt

                #   Certificate Revocation Lists (CRL):
                #   Set the CA revocation path where to find CA CRLs for client
                #   authentication or alternatively one huge file containing all
                #   of them (file must be PEM encoded)
                #   Note: Inside SSLCARevocationPath you need hash symlinks
                #               to point to the certificate files. Use the provided
                #               Makefile to update the hash symlinks after changes.
                #SSLCARevocationPath /etc/apache2/ssl.crl/
                #SSLCARevocationFile /etc/apache2/ssl.crl/ca-bundle.crl
"/etc/apache2/sites-available/default-ssl.conf" 134L, 6340C                                                    35,31-4
```

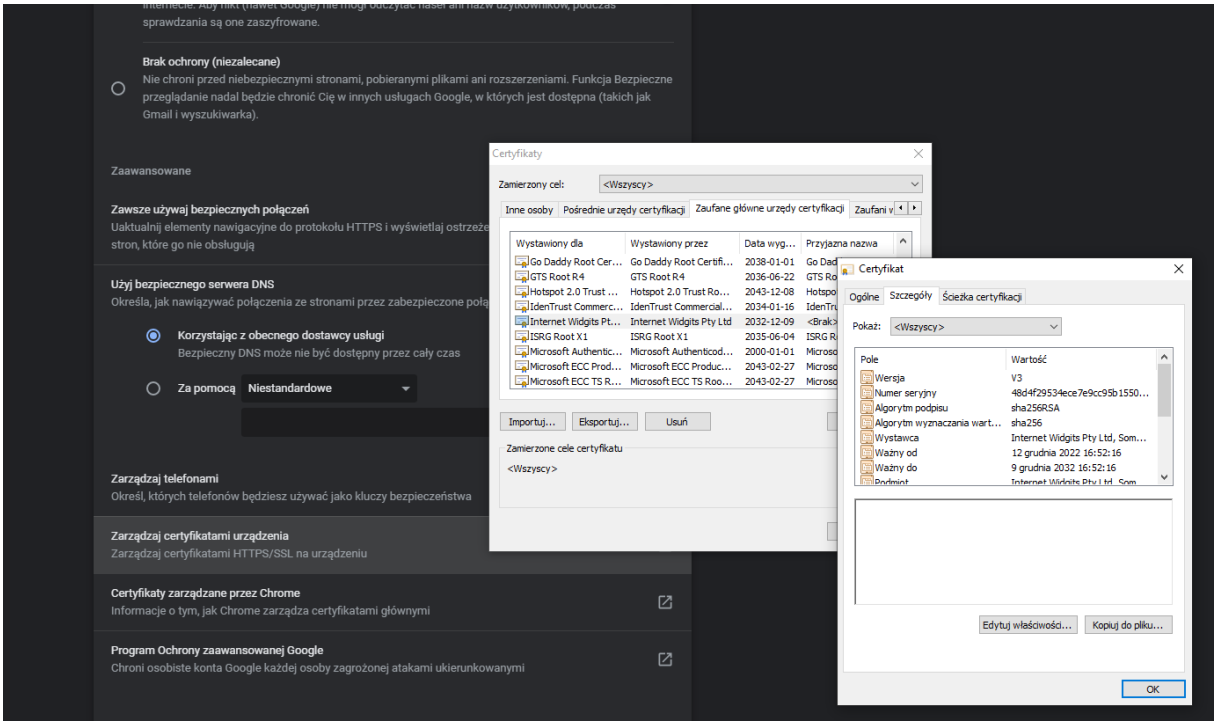


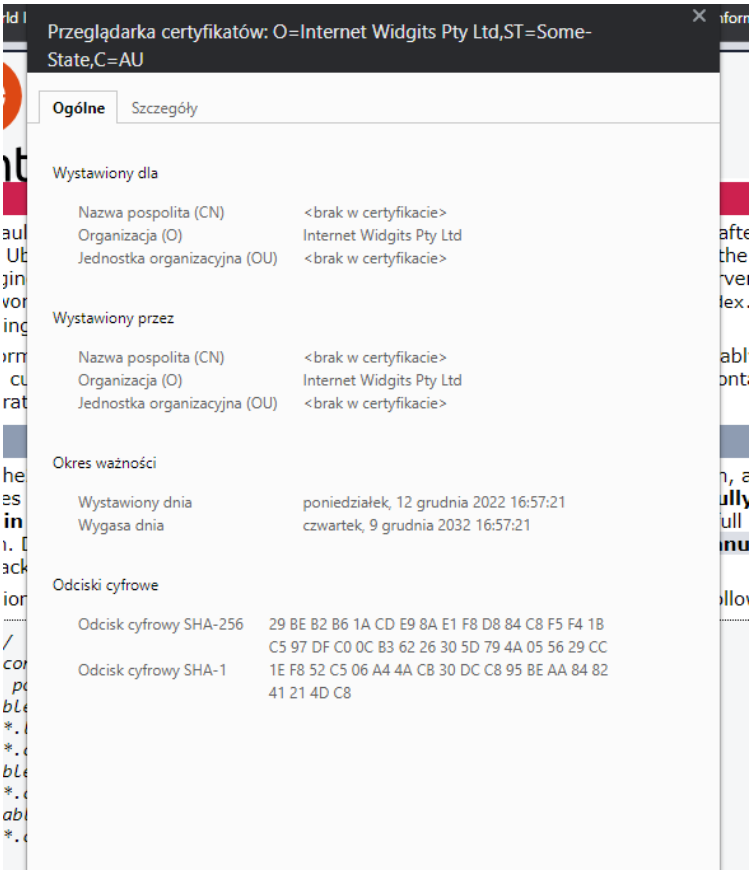


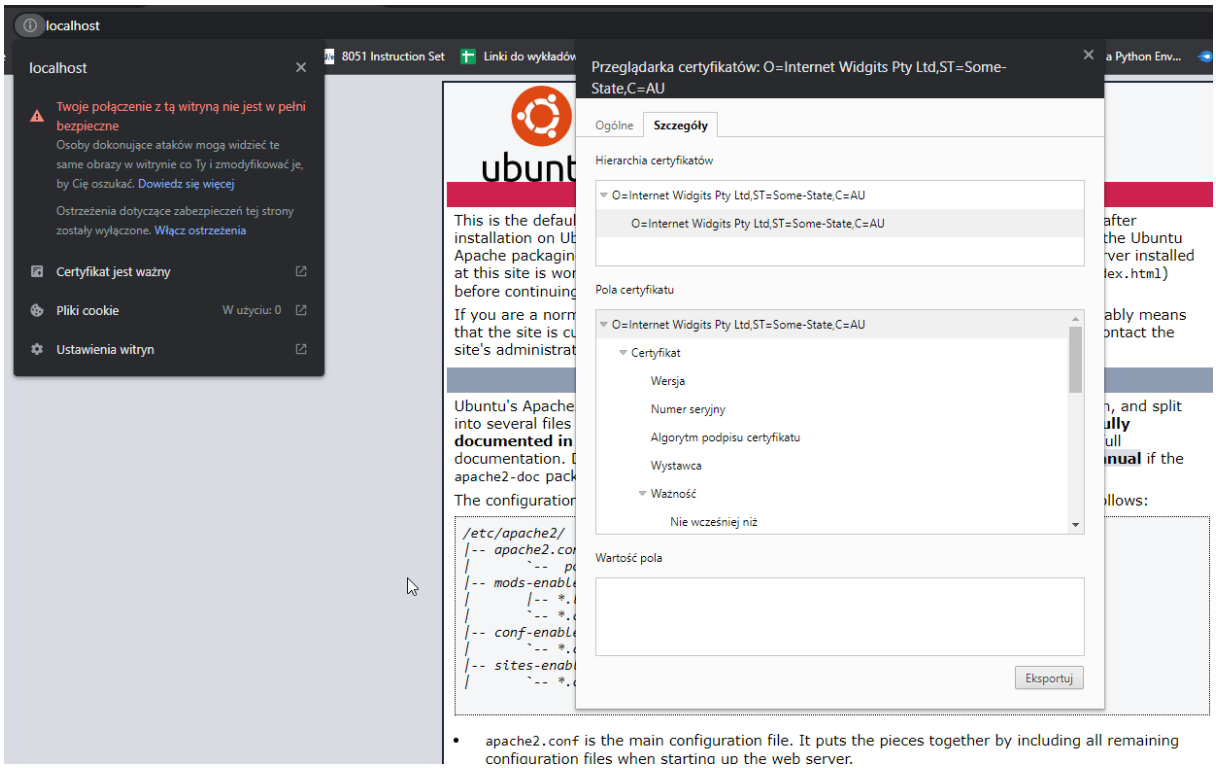
2. Ogarnięcie certyfikatu

```
teczap@Paw-PC:/etc/test/localhost$ ls
localhost.crt  localhost.csr  localhost.decrypted.key  localhost.ext  localhost.key
```

```
teczap@Paw-PC:/etc/test$ ls
CA.key  CA.pem  CA.srl  localhost
```




Przeglądarka certyfikatów: O=Internet Widgits Pty Ltd,ST=Some-State,C=AU
Ogólne
Szczegóły
Wystawiony dla
Nazwa pospolita (CN) <brak w certyfikacie>
Organizacja (O) Internet Widgits Pty Ltd
Jednostka organizacyjna (OU) <brak w certyfikacie>
Wystawiony przez
Nazwa pospolita (CN) <brak w certyfikacie>
Organizacja (O) Internet Widgits Pty Ltd
Jednostka organizacyjna (OU) <brak w certyfikacie>
Okres ważności
Wystawiony dnia poniedziałek, 12 grudnia 2022 16:57:21
Wygasa dnia czwartek, 9 grudnia 2032 16:57:21
Odciski cyfrowe
Odcisk cyfrowy SHA-256 29 BE B2 B6 1A CD E9 8A E1 F8 D8 84 C8 F5 F4 1B C5 97 DF C0 0C B3 62 26 30 5D 79 4A 05 56 29 CC
Odcisk cyfrowy SHA-1 1E F8 52 C5 06 A4 4A C8 30 DC C8 95 BE AA 84 82 41 21 4D C8


localhost
Twoje połączenie z tą witryną nie jest w pełni bezpieczne
Osoby dokonujące ataków mogą widzieć te same obrazy w witrynie co Ty i zmodyfikować je, by Cię oszukać. Dowiedz się więcej
Ostrzeżenia dotyczące zabezpieczeń tej strony zostały wyłączone. Włącz ostrzeżenia
Certyfikat jest ważny
Pliki cookie W użyciu: 0
Ustawienia witryn
Przeglądarka certyfikatów: O=Internet Widgits Pty Ltd,ST=Some-State,C=AU
Ogólne
Szczegóły
Hierarchia certyfikatów
O=Internet Widgits Pty Ltd,ST=Some-State,C=AU
O=Internet Widgits Pty Ltd,ST=Some-State,C=AU
Pola certyfikatu
O=Internet Widgits Pty Ltd,ST=Some-State,C=AU
Certyfikat
Wersja
Numer seryjny
Algorytm podpisu certyfikatu
Wystawca
Ważność
Nie wcześniej niż
Wartość pola
Eksportuj
apache2.conf is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.