



Práctica 1: Autenticación y TLS/SSL

12/12/2018

Freddy Alex Tandazo Yáñez
Universidad Politécnica de Madrid
freddy.tandazo.tandazo@alumnos.upm.es
Madrid - España

Servidor virtual

Para poder crear nuestro nuevo servidor virtual con dominio www.miw.com primero debemos de ir al archivo de httpd.conf y verificar que la ruta del archivo no esté comentada.

```
# Virtual hosts
Include "conf/extra/httpd-vhosts.conf"
```

ahora agregamos nuestro servidor virtual en al final del documento httpd-vhosts.conf

```
86
87 <VirtualHost *:8080>
88     ServerName www.miw.com
89     DocumentRoot C:/xampp/htdocsSAW
90     <Directory "C:/xampp/htdocsSAW">
91         AllowOverride All
92         Require all granted
93     </Directory>
94     <Directory "C:/xampp/htdocsSAW/practical">
95         Options -Indexes
96         DirectoryIndex login.php
97     </Directory>
98 </VirtualHost>
```

En donde la línea 87 definimos las etiquetas de **VirtualHost** agregando el símbolo de asterisco (*) el cual me indica la dirección a la cual voy hacer la petición http, en nuestro caso será 127.0.0.1

Los valores de **8080** me indican el puerto por cual voy hacer mi petición http (el valor 8080 fueron configurados en el archivo http.conf).

ServerName me indica el nombre que el servidor tiene para identificarse.

DocumentRoot me indica la ruta raíz en la cual va a estar mi proyecto.

<Directory "C:/xampp/htdocsSAW">: Hace una especificación al directorio al cual deseamos hacer los cambios. Para la ruta especificada vamos hacer un **AllowOverride All** me indica si puedo hacer cambios desde el archivo .htaccess ubicado desde mi aplicación.

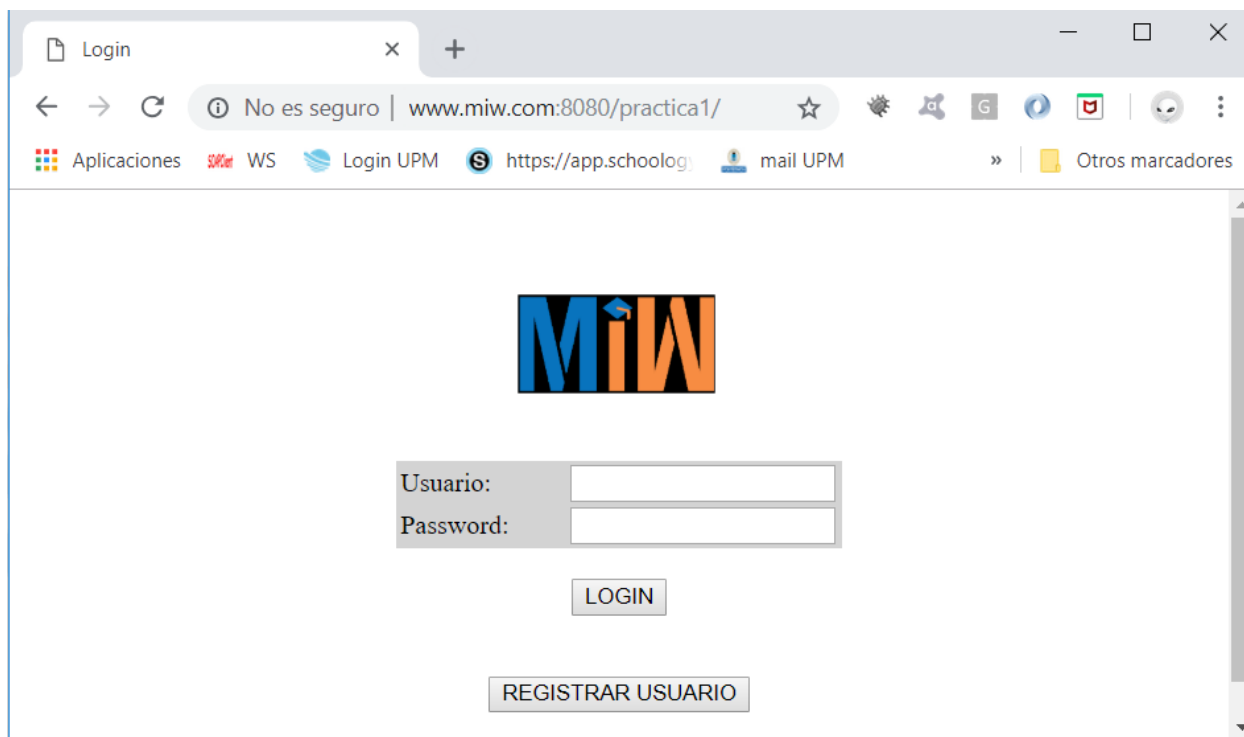
Require All grante me da permisos para acceder a los documentos de mi directorio.

Options -Indexes me ayuda a bloquear el web browsing que puedan hacer a mi aplicación.

DirectoryIndex login.php hace un redireccionamiento a la página principal de la aplicación en caso no se haya definido en la aplicación.

Finalizamos la configuración del **VirtualHost** con su etiqueta de cierre.

Luego probamos desde el navegador.



Autenticación http básica.

Para el fichero .htaccess de la carpeta admin se ha ingresado las siguientes instrucciones:

```
AuthType Basic
AuthName "Restritec Files"
AuthBasicProvider file
AuthUserFile C:/xampp/apache/conf/passw/.htpasswd
#Require valid-user
Require user freddy
Require user fatandaz
```

En donde como resultado obtenemos la imagen a continuación.



***Nota: el usuario es freddy y la contraseña es freddy**

Freddy Alex Tandazo Yáñez

Para no poder permitir el acceso a la ruta

<http://www.miw.com:8080/practica1/includes/abrirbd.php> hemos declarado la siguiente instrucción en el fichero .htaccess el cual se encuentra dentro de la carpeta includes.

```
require all denied
```

Autenticación y autorización web.

Obtengo la variable `_SESSION['permisos']` la cual fue declarada en la pagina de login.php, despues de eso obtengo el quinto elemento del array `_SESSION['permisos']` y compruebo que el carácter sea una 'S' el cual me indica que el usuario tiene permisos para poder acceder a la pagina web de seguridad.php. En caso de no tener asignado la letra 'S' sera redirigido a la pagina de NoAuth.php

```
<?php
    include "../includes/autenticado.php";
    $permisos= $_SESSION['permisos'][5];
    if($permisos != 'S'){
        header("location: ./NoAuth.php");
    }
?>
```

Configuración SSL

```
<VirtualHost *:443>
    ServerName www.miw.com:443
    DocumentRoot C:/xampp/htdocsSAW

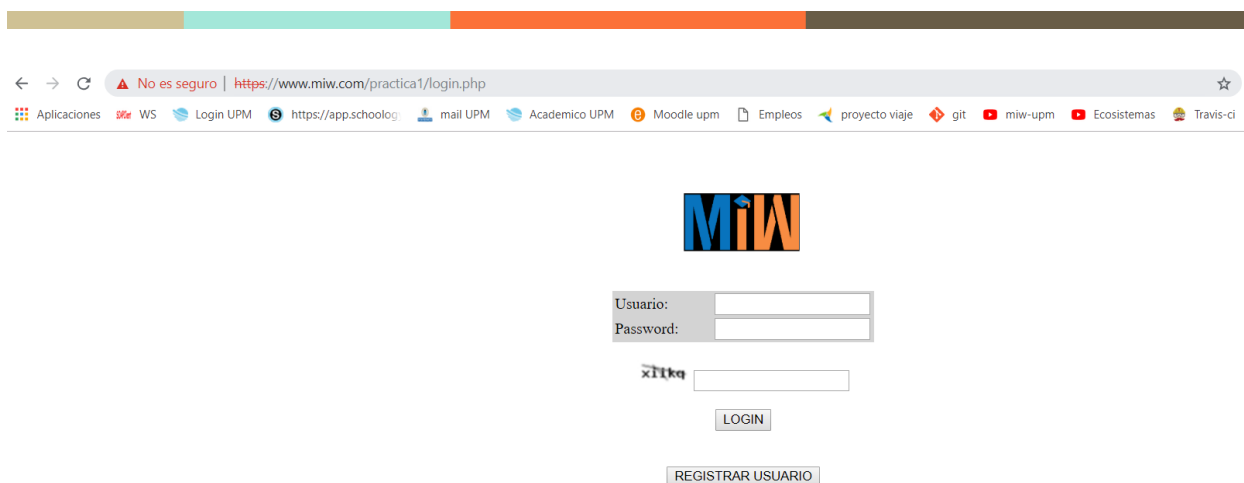
    #   SSL Engine Switch:
    #   Enable/Disable SSL for this virtual host.
    SSLEngine on

    #   SSL Cipher Suite:
    #   List the ciphers that the client is permitted to negotiate.
    #   See the mod_ssl documentation for a complete list.
    SSLCipherSuite ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP:+eNULL

    #   Server Certificate:
    #   Point SSLCertificateFile at a PEM encoded certificate.  If
    #   the certificate is encrypted, then you will be prompted for a
    #   pass phrase.  Note that a kill -HUP will prompt again.  Keep
    #   in mind that if you have both an RSA and a DSA certificate you
    #   can configure both in parallel (to also allow the use of DSA
    #   ciphers, etc.)
    #SSLCertificateFile "conf/ssl.crt/server-dsa.crt"
    #SSLCertificateFile "conf/ssl.crt/server.crt"
    SSLCertificateFile "conf/ssl.crt/miw.crt"

    #   Server Private Key:
    #   If the key is not combined with the certificate, use this
    #   directive to point at the key file.  Keep in mind that if
    #   you've both a RSA and a DSA private key you can configure
    #   both in parallel (to also allow the use of DSA ciphers, etc.)
    #SSLCertificateKeyFile "conf/ssl.key/server-dsa.key"
    #SSLCertificateKeyFile "conf/ssl.key/server.key"
    SSLCertificateKeyFile "conf/ssl.key/miw.key"

    <Directory "C:/xampp/htdocsSAW">
        AllowOverride All
        Require all granted
    </Directory>
    <Directory "C:/xampp/htdocsSAW/practical">
        Options -Indexes
        DirectoryIndex login.php
    </Directory>
</VirtualHost>
```



Explica cómo has utilizado la directiva SSLRequireSSL. ¿Qué diferencia habría si en lugar de utilizar SSLRequireSSL se eliminara la directiva Listen 80 del fichero httpd.conf?

Con la directiva SSLRequireSSL negamos el acceso a clientes que no utilizan SSL y la agregamos en el VirtualHost 443.

Sí, eliminamos la directiva listen 80 no afectaría en nada a SSLRequireSSL debido a que este funciona en el puerto 443 quedando totalmente independiente del listen 80.

¿Por qué ha tenido que aceptar una excepción de seguridad para permitir el certificado?

Debido a que el certificado no es un certificado seguro el navegador lanza un mensaje de problemas con el certificado, indicando que especifique si desea continuar con el uso del certificado en la página web.

¿Qué certificado digital está utilizando ahora la aplicación web?

Estamos usando el certificado miw.crt

¿Por qué motivo se está utilizando este certificado?

Para realizar las pruebas en local, en un ambiente de producción habrá que contratar una entidad que nos genere el certificado de manera que el navegador ya no lance excepciones para nuestra pagina web.

Explique qué directivas ha definido en este apartado y cómo.

```
<VirtualHost *:443>
    ServerName www.miw.com:443
    DocumentRoot C:/xampp/htdocsSAW

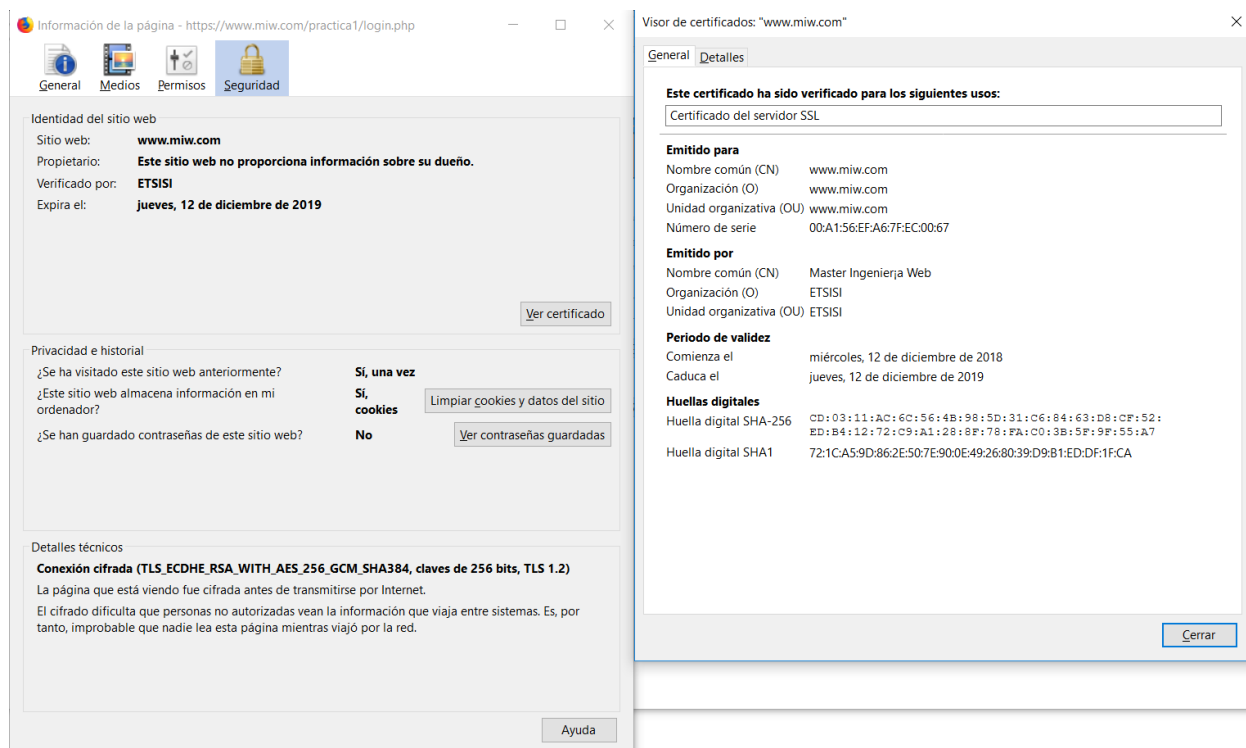
    # SSL Engine Switch:
    # Enable/Disable SSL for this virtual host.
    SSLEngine on

    # SSL Cipher Suite:
    # List the ciphers that the client is permitted to negotiate.
    # See the mod_ssl documentation for a complete list.
    SSLCipherSuite ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP:+eNULL
    SSLHonorCipherOrder on
    SSLProtocol -all +TLSv1.2
```

¿Qué algoritmos se obtienen cuando se realiza una petición a <https://www.miw.com> con el navegador?

El algoritmo que se obtiene es PKCS #1 SHA-256 con cifrado RSA

Añada un pantallazo de la ventana del navegador donde aparecen dichos algoritmos.



Autenticación de clientes con SSL.

Explicar las modificaciones realizadas en `httpd-ssl.conf` y/o en ficheros `.htaccess` para solicitar certificado al cliente cuando accede a `loginert.php`.

```

#   SSL Cipher Suite:
#   List the ciphers that the client is permitted to negotiate.
#   See the mod_ssl documentation for a complete list.
SSLCipherSuite ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP:+eNULL
SSLHonorCipherOrder on
SSLProtocol -all +TLSv1.2

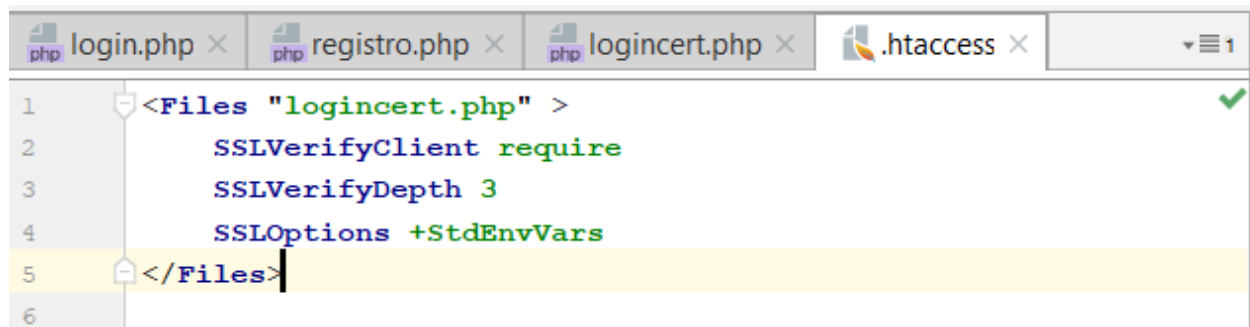
#   Server Certificate:
#   Point SSLCertificateFile at a PEM encoded certificate.  If
#   the certificate is encrypted, then you will be prompted for a
#   pass phrase.  Note that a kill -HUP will prompt again.  Keep
#   in mind that if you have both an RSA and a DSA certificate you
#   can configure both in parallel (to also allow the use of DSA
#   ciphers, etc.)
#SSLCertificateFile "conf/ssl.crt/server-dsa.crt"
#SSLCertificateFile "conf/ssl.crt/server.crt"
#SSLCertificateFile "conf/ssl.crt/miw.crt"

#   Server Private Key:
#   If the key is not combined with the certificate, use this
#   directive to point at the key file.  Keep in mind that if
#   you've both a RSA and a DSA private key you can configure
#   both in parallel (to also allow the use of DSA ciphers, etc.)
#SSLCertificateKeyFile "conf/ssl.key/server-dsa.key"
#SSLCertificateKeyFile "conf/ssl.key/server.key"
#SSLCertificateKeyFile "conf/ssl.key/miw.key"

<Directory "C:/xampp/htdocsSAW">
    AllowOverride All
    Require all granted
</Directory>
<Directory "C:/xampp/htdocsSAW/practical">
    SSLRequireSSL
    Options -Indexes
    DirectoryIndex login.php
</Directory>

SSLVerifyClient require
SSLVerifyDepth 3
SSLCACertificateFile "conf/ssl.crt/CAMIW.crt"
</VirtualHost>


```



```

login.php x registro.php x logincert.php x .htaccess x 1
1 <Files "logincert.php" >
2     SSLVerifyClient require
3     SSLVerifyDepth 3
4     SSLOptions +StdEnvVars
5 </Files>
6

```

Explicar por qué la página logincert.php consigue acceder a las variables de entorno que contienen la información del certificado del cliente. Concretamente, a `SSL_CLIENT_S_DN_CN`.

Cuando esta opción está habilitada, se generan las variables de entorno estándar de SS

Justifique el motivo por el que no es posible dicha autenticación

Porque Burp suit no tiene el registro de llaves.

Explique la configuración realizada en Burp Suite.

Debemos agregar Cliente.p12 con la clave mica.