

Tarea #2

Seguridad Informática

BITÁCORA

Pasarela de pago electrónico

Eliseo Loría Solís
Cristina Elizondo Meza

II ciclo 2018



Índice

Índice	2
Tecnologías	3
Herramientas	3
Lenguajes	3
Bibliotecas	3
Configuración del Servidor	3
Activar el módulo SSL en el servidor Apache	4
Generar un certificado de seguridad firmarlo e instalarlo en el servidor Apache	6
Configurar un virtualhosts para la aplicación que va a utilizar el certificado con https.	8
Desarrollo	11
Front-End	11
Back-End	13
Referencias	15

Tecnologías

Para el desarrollo del módulo de ejemplo se hizo uso de un conjunto de tecnologías y herramientas, para simular el ambiente, de los servidores web, que interactúan para el pago; a continuación se detalla un listado de las mismas:

Herramientas

- XAMPP, para los servicios de Apache
- Google Chrome y Firefox, como navegadores de prueba y de análisis
- Atom, IDE de desarrollo
- Github, como plataforma de versionamiento
- OpenSSL

Lenguajes

- HTML y CSS
- JavaScript
- PHP

Bibliotecas

- Slim, micro-framework
- Bootstrap 4

Configuración del Servidor

El proceso de configuración del servidor se llevó a cabo en tres pasos.

Activar el módulo SSL en el servidor Apache

Este equipo ▸ Disco local (C:) ▸ xampp ▸ apache ▸ conf

Nombre	Fecha de modifica...	Tipo	Tamaño
ssl.crt	28/08/2018 3:57	Carpeta de archivos	
ssl.csr	28/08/2018 3:57	Carpeta de archivos	
ssl.key	28/08/2018 3:57	Carpeta de archivos	
.rnd	28/08/2018 5:17	Archivo RND	1 KB
ca_client	28/08/2018 5:17	Certificado de seg...	1 KB
ca_client.csr	28/08/2018 5:17	Archivo CSR	1 KB
ca_client.key	28/08/2018 5:17	Archivo KEY	1 KB
ca_client.srl	28/08/2018 5:17	Archivo SRL	1 KB
ca_server	28/08/2018 5:17	Certificado de seg...	1 KB
ca_server.csr	28/08/2018 5:17	Archivo CSR	1 KB
ca_server.key	28/08/2018 5:17	Archivo KEY	1 KB
ca_server.srl	28/08/2018 5:17	Archivo SRL	1 KB
charset.conv	15/07/2018 12:57	Archivo CONV	2 KB
client.csr	28/08/2018 5:17	Archivo CSR	1 KB
client.key	28/08/2018 5:17	Archivo KEY	1 KB
client_signedby_ca_client	28/08/2018 5:17	Certificado de seg...	1 KB
httpd.conf	28/08/2018 4:02	Archivo CONF	22 KB
magic	15/07/2018 12:57	Archivo	14 KB
mime.types	01/08/2018 16:57	Archivo TYPES	60 KB
openssl.cnf	27/03/2018 17:54	Archivo CNF	11 KB
server	28/08/2018 5:17	Certificado de seg...	1 KB
server.csr	28/08/2018 5:17	Archivo CSR	1 KB
server.key	28/08/2018 5:17	Archivo KEY	1 KB

Buscar el archivo httpd.conf en la dirección C:/xampp/apache/conf

```
httpd.conf x
162 #LoadModule reqtimeout_module modules/mod_reqtimeout.so
163 LoadModule rewrite_module modules/mod_rewrite.so
164 #LoadModule sed_module modules/mod_sed.so
165 #LoadModule session_module modules/mod_session.so
166 #LoadModule session_cookie_module modules/mod_session_cookie.so
167 #LoadModule session_crypto_module modules/mod_session_crypto.so
168 #LoadModule session_dbd_module modules/mod_session_dbd.so
169 LoadModule setenvif_module modules/mod_setenvif.so
170 #LoadModule slotmem_plain_module modules/mod_slotmem_plain.so
171 #LoadModule slotmem_shm_module modules/mod_slotmem_shm.so
172 #LoadModule socache_dbm_module modules/mod_socache_dbm.so
173 #LoadModule socache_memcache_module modules/mod_socache_memcache.so
174 LoadModule socache_shmcb_module modules/mod_socache_shmcb.so
175 #LoadModule spelling_module modules/mod_spelling.so
176 LoadModule ssl_module modules/mod_ssl.so
177 LoadModule status module modules/mod_status.so
```

Descomento la línea 176 LoadModule ssl_module modules/mod_ssl.so

Este equipo ► Disco local (C:) ► xampp ► php

Nombre	Fecha de modifica...	Tipo	Tamaño
recnsc	19/07/2018 4:14	Documento de tex...	4 KB
msvcvp110.dll	19/08/2016 17:09	Extensión de la apl...	523 KB
msvcr110.dll	19/08/2016 17:09	Extensión de la apl...	855 KB
news	19/07/2018 4:14	Documento de tex...	112 KB
nghttp2.dll	19/07/2018 4:14	Extensión de la apl...	151 KB
pci	28/08/2018 4:02	Archivo	1 KB
pci	28/08/2018 4:02	Archivo por lotes ...	1 KB
pci	27/01/2016 13:02	Documento de ho...	2 KB
pciconf	28/08/2018 4:02	Archivo	18 KB
pciconf	28/08/2018 4:02	Archivo por lotes ...	1 KB
pear	28/08/2018 4:02	Archivo por lotes ...	5 KB
peardev	28/08/2018 4:02	Archivo por lotes ...	5 KB
pecl	28/08/2018 4:02	Archivo por lotes ...	5 KB
phar.phar	19/07/2018 4:15	Archivo por lotes ...	1 KB
pharcommand.phar	19/07/2018 4:15	Archivo PHAR	52 KB
php	19/07/2018 4:14	Aplicación	98 KB
php	19/07/2018 4:14	Imagen GIF	3 KB
php	28/08/2018 4:29	Opciones de confi...	72 KB

Buscar el archivo php.ini en la dirección C:/xampp/php

```

php.ini
877 extension=php_bz2.dll
878 extension=php_curl.dll
879 extension=php_fileinfo.dll
880 ;extension=php_ftp.dll
881 extension=php_gd2.dll
882 extension=php_gettext.dll
883 ;extension=php_gmp.dll
884 ;extension=php_intl.dll
885 ;extension=php_imap.dll
886 ;extension=php_interbase.dll
887 ;extension=php_ldap.dll
888 extension=php_mbstring.dll
889 extension=php_exif.dll      ; Must be after mbstring as it depends on it
890 extension=php_mysql.dll
891 ;extension=php_oci8_12c.dll ; Use with Oracle Database 12c Instant Client
892 extension=php_openssl.dll

```

Descomentar la línea 892 extension=php_openssl.dll

Generar un certificado de seguridad firmarlo e instalarlo en el servidor Apache

https://wiki.openssl.org/index.php/Binaries

illias Universidad Nacional SISTEMA DE BECAS Acceso a Usuario DescargateloCorp - E Aula Virtual Institucio DescargateloCorp - E Force Download - De Sisar

page discussion edit history

Binaries

Some people have offered to provide OpenSSL binary distributions for selected operating systems. The condition to get a link here is that the link is stable and can provide continued support for OpenSSL for a while.

Note: many Linux distributions come with pre-compiled OpenSSL packages. Those are already well-known among the users of said distributions, and will therefore not be mentioned here. If you are such a user, we ask you to get in touch with your distributor first. This service is primarily for operating systems where there are no pre-compiled OpenSSL packages.

Important Disclaimer: *The listing of these third party products does not imply any endorsement by the OpenSSL project, and these organizations are not affiliated in any way with OpenSSL other than by the reference to their independent web sites here. In particular any donations or payments to any of these organizations will not be known to, seen by, or in any way benefit the OpenSSL project.*

Use these OpenSSL derived products at your own risk; these products have not been evaluated or tested by the OpenSSL project.

Product	Description	URL
OpenSSL for Windows	Works with MSVC++, Builder 3/4/5, and MinGW. Comes in form of self-install executables.	https://slproweb.com/products/Win32OpenSSL.html
OpenSSL for Windows	Pre-compiled Win32/64 libraries without external dependencies to the Microsoft Visual Studio Runtime DLLs, except for the system provided msvcrt.dll.	https://indy.fulgan.com/SSL/
OpenSSL for Windows	Reproducible 1.1.x builds with latest MinGW-w64/GCC, 32/64-bit, static/dynamic libs and executable.	https://bintray.com/vszakats/generic/openssl
OpenSSL for Solaris	Versions for Solaris 2.5 - 11 SPARC and X86	http://www.unixpackages.com/
OpenSSL for Windows, Linux, OSX, Android	Pre-compiled packages at conan.io package manager: Windows x86/x86_64 (Visual Studio 10, 12, 14, 15) Linux x86/x86_64 (gcc 4.6, 4.8, 4.9, 5, 6, 7) OSX (Apple clang).	https://www.conan.io https://bintray.com/conan-community/conan/OpenSSL%3Aconan

Download Win32 OpenSSL

Download Win32 OpenSSL today using the links below!

File	Type	Description
Win32 OpenSSL v1.1.0i Light	3MB Installer	Installs the most commonly used essentials of Win32 OpenSSL v1.1.0i (Recommended for users by the creators of OpenSSL). Note that this is a default build of OpenSSL and is subject to local and state laws. More information can be found in the legal agreement of the installation.
Win32 OpenSSL v1.1.0i	30MB Installer	Installs Win32 OpenSSL v1.1.0i (Recommended for software developers by the creators of OpenSSL). Note that this is a default build of OpenSSL and is subject to local and state laws. More information can be found in the legal agreement of the installation.
Win64 OpenSSL v1.1.0i Light	3MB Installer	Installs the most commonly used essentials of Win64 OpenSSL v1.1.0i (Only install this if you need 64-bit OpenSSL for Windows. Only installs on 64-bit versions of Windows. Note that this is a default build of OpenSSL and is subject to local and state laws. More information can be found in the legal agreement of the installation.
Win64 OpenSSL v1.1.0i	33MB Installer	Installs Win64 OpenSSL v1.1.0i (Only install this if you are a software developer needing 64-bit OpenSSL for Windows. Only installs on 64-bit versions of Windows. Note that this is a default build of OpenSSL and is subject to local and state laws. More information can be found in the legal agreement of the installation.
Win32 OpenSSL v1.0.2p Light	2MB Installer	Installs the most commonly used essentials of Win32 OpenSSL v1.0.2p (Recommended for users by the creators of OpenSSL). Note that this is a default build of OpenSSL and is subject to local and state laws. More information can be found in the legal agreement of the installation.
Win32 OpenSSL v1.0.2p	20MB Installer	Installs Win32 OpenSSL v1.0.2p (Recommended for software developers by the creators of OpenSSL). Note that this is a default build of OpenSSL and is subject to local and state laws. More information can be found in the legal agreement of the installation.
Win64 OpenSSL v1.0.2p Light	3MB Installer	Installs the most commonly used essentials of Win64 OpenSSL v1.0.2p (Only install this if you need 64-bit OpenSSL for Windows. Only installs on 64-bit versions of Windows. Note that this is a default build of OpenSSL and is subject to local and state laws. More information can be found in the legal agreement of the installation.

El primer paso es descargar el OpenSSL <https://wiki.openssl.org/index.php/Binaries>

► Este equipo ► Disco local (C:) ► OpenSSL-Win32 ►

Descomprimir y instalar el ejecutable al finalizar se instalará en la dirección por defecto que vemos en la imagen.


```

1 REM Definimos las variables de entorno
2 SET OPENSSL_HOME = C:\OpenSSL-Win32
3 SET OPENSSL_CONF=C:\OpenSSL-Win32\bin\openssl.cfg
4 SET PATH=%PATH%;C:\OpenSSL-Win32\bin
5
6 REM Creamos un CA, clave de servidor y lo firmamos:
7 openssl genrsa -out ca_server.key 1024
8 openssl req -new -newkey rsa:1024 -nodes -out ca_server.csr -keyout ca_server.key -subj "/C=US/ST=NY/L
9 openssl x509 -req -days 365 -in ca_server.csr -signkey ca_server.key -out ca_server.crt
10 openssl req -new -newkey rsa:1024 -nodes -out server.csr -keyout server.key -subj "/C=US/ST=Texas/L=Au
11 openssl x509 -req -days 365 -CA ca_server.crt -CAkey ca_server.key -CAcreateserial -in server.csr -out
12
13 REM creamos otro CA, clave de cliente y lo firmamos:
14 openssl genrsa -out ca_client.key 1024
15 openssl req -new -newkey rsa:1024 -nodes -out ca_client.csr -keyout ca_client.key -subj "/C=US/ST=TX/L
16 openssl x509 -req -days 365 -in ca_client.csr -signkey ca_client.key -out ca_client.crt
17 openssl genrsa -out client.key 1024
18 openssl req -new -key client.key -out client.csr -subj "/C=US/ST=Texas/L=Austin/O=Client Iqbal/OU=IT/C
19 openssl x509 -req -days 365 -CA ca_client.crt -CAkey ca_client.key -CAcreateserial -in client.csr -out
20 openssl pkcs12 -export -clcerts -in client_signedby_ca_client.crt -inkey client.key -out client_signed

```

Seguidamente ejecutamos las líneas anteriores en la ventana de comandos, ubicados en la carpeta “apache/conf” con el siguiente comando “cd \xampp\apache\conf”.

```

C:\Users\Administrador>openssl req -new -newkey rsa:1024 -nodes -out ca_client.c
sr -keyout ca_client.key -subj "/C=US/ST=TX/L=Austin/O=CA for Client Cert/OU=IT/
CN=www.CAforClient.org"
Generating a 1024 bit RSA private key
.....+++++
.....+++++
writing new private key to 'ca_client.key'
-----

C:\Users\Administrador>openssl x509 -req -days 365 -in ca_client.csr -signkey ca
_client.key -out ca_client.crt
Signature ok
subject=C = US, ST = TX, L = Austin, O = CA for Client Cert, OU = IT, CN = www.C
AforClient.org
Getting Private key

C:\Users\Administrador>openssl genrsa -out client.key 1024
Generating RSA private key, 1024 bit long modulus
.....+++++
.....+++++
e is 65537 (0x010001)

C:\Users\Administrador>openssl req -new -key client.key -out client.csr -subj "/
C=US/ST=Texas/L=Austin/O=Client Iqbal/OU=IT/CN=ClientIqbal"

C:\Users\Administrador>openssl x509 -req -days 365 -CA ca_client.crt -CAkey ca_c
lient.key -CAcreateserial -in client.csr -out client_signedby_ca_client.crt
Signature ok
subject=C = US, ST = Texas, L = Austin, O = Client Iqbal, OU = IT, CN = ClientIq
bal
Getting CA Private Key

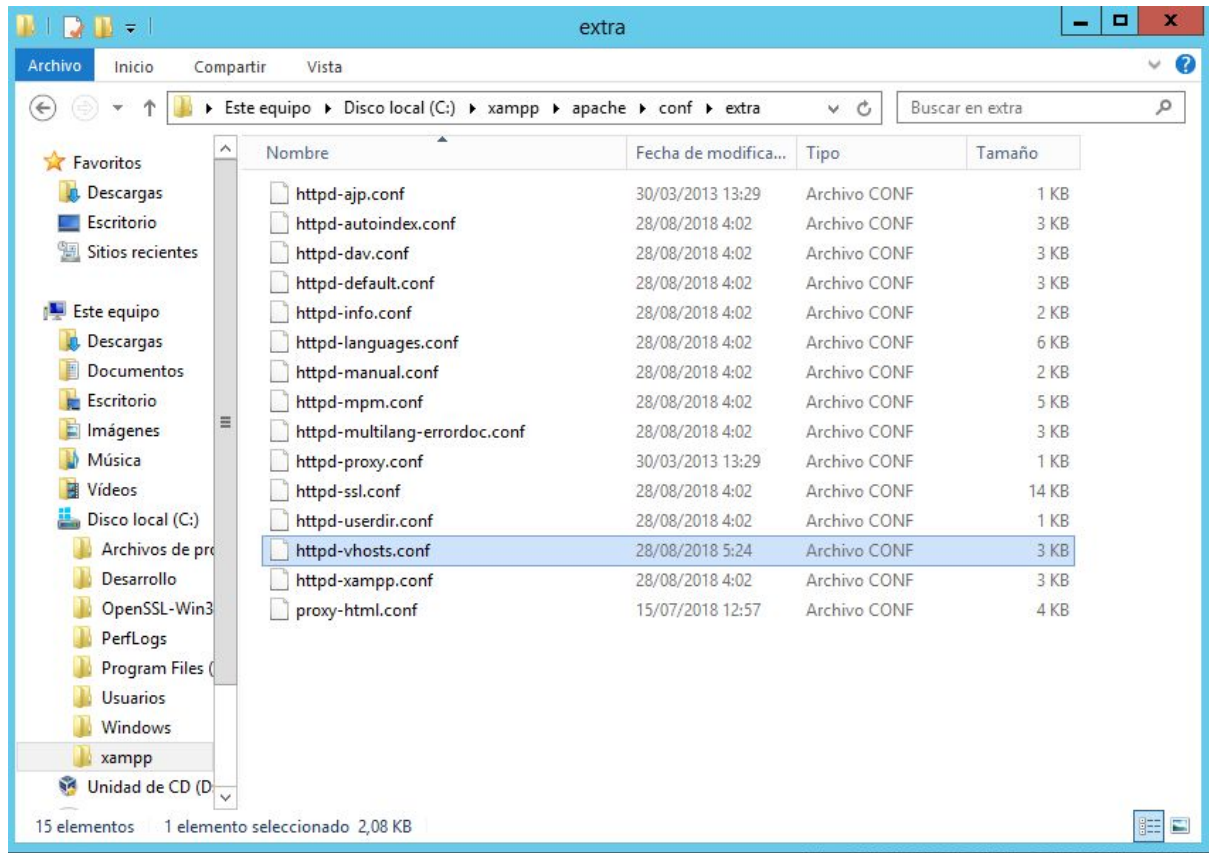
C:\Users\Administrador>openssl pkcs12 -export -clcerts -in client_signedby_ca_cl
ient.crt -inkey client.key -out client_signedby_ca_client.p12
Enter Export Password:
Verifying - Enter Export Password:

C:\Users\Administrador>

```

Al finalizar le proporcionamos un a clave.

Configurar un virtualhosts para la aplicación que va a utilizar el certificado con https.



Se ubica el archivo httpd_vhosts.conf en la dirección C://xampp/apache/conf/extra.


```

##ServerAdmin webmaster@dummy-host.example.com
##DocumentRoot "C:/xampp/htdocs/dummy-host.example.com"
##ServerName dummy-host.example.com
##ServerAlias www.dummy-host.example.com
##ErrorLog "logs/dummy-host.example.com-error.log"
##CustomLog "logs/dummy-host.example.com-access.log" common
##</VirtualHost>

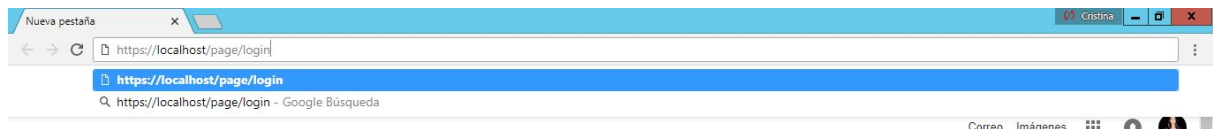
##<VirtualHost *:80>
##ServerAdmin webmaster@dummy-host2.example.com
##DocumentRoot "C:/xampp/htdocs/dummy-host2.example.com"
##ServerName dummy-host2.example.com
##ErrorLog "logs/dummy-host2.example.com-error.log"
##CustomLog "logs/dummy-host2.example.com-access.log" common
##</VirtualHost>
<VirtualHost *:443>
    DocumentRoot "C:/Desarrollo/Pasarela_Pago"
    ServerName www.pasarela_pago.com
    ErrorLog "logs/miapp-error.log"
    CustomLog "logs/miapp-access.log" common
    SSLEngine On
    SSLCertificateFile "C:/xampp/apache/conf/ssl.crt/server.crt"
    SSLCertificateKeyFile "C:/xampp/apache/conf/ssl.key/server.key"
    SSLCipherSuite ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP:+eNULL
    <Directory "C:/Desarrollo/Pasarela_Pago">
        Options All
        AllowOverride All
        Require all granted
    </Directory>
</VirtualHost>

```

Se agregan las últimas 15 líneas que se observan al final del documento.

La ubicación (C:/Desarrollo/Pasarela_Pago) de la aplicación es la que se observa en la línea 2 y la 10 de las 15 agregadas.

Ya estaría listo ahora lo vamos a probar:



Colocamos la dirección <https://localhost/page/login>



La conexión no es privada

Es posible que algunos atacantes intenten robar tu información de **localhost** (p. ej., contraseñas, mensajes o tarjetas de crédito). [Más información](#)

NET::ERR_CERT_AUTHORITY_INVALID

☐ Enviar automáticamente [determinado contenido de la página e información del sistema](#) a Google para detectar apps y sitios peligrosos [Política de privacidad](#)

AVANZADA

VOLVER A SEGURIDAD

Acudimos al sitio seguro

Iniciar sesión

Usuario

Contraseña

Ingresar

Y tenemos la aplicación.

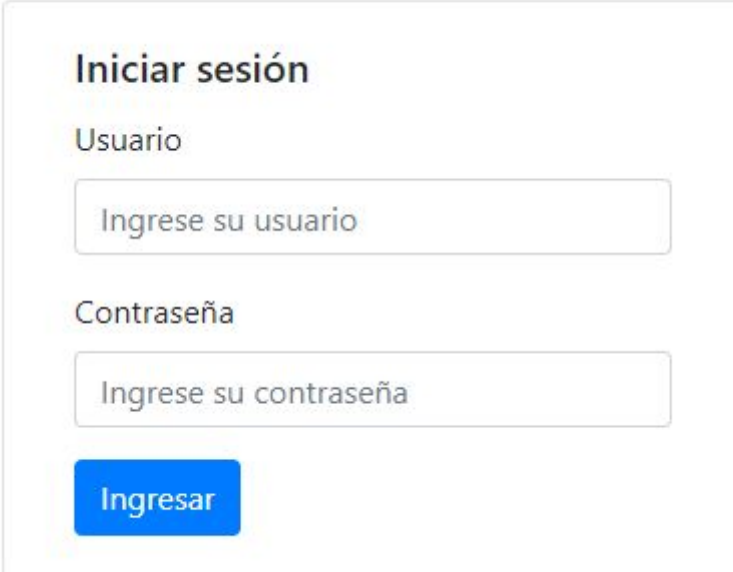
Desarrollo

El desarrollo del módulo de ejemplo se llevó a cabo en dos partes o secciones, las cuales se describen a continuación.

Front-End

Se crearon cuatro plantillas HTML5.

Login: pantalla de inicio de sesión, no funcional, con los campos usuario y contraseña.

A mockup of a login form. It features a title 'Iniciar sesión' in bold. Below it are two input fields: one for 'Usuario' with the placeholder text 'Ingrese su usuario', and another for 'Contraseña' with the placeholder text 'Ingrese su contraseña'. At the bottom is a blue button with the text 'Ingresar' in white.

Iniciar sesión

Usuario

Ingrese su usuario

Contraseña

Ingrese su contraseña

Ingresar

Pago: pantalla que muestra información de la compra, en este caso simula la compra de una unidad de almacenamiento X, de un tamaño a seleccionar, con campos no editables de manera tradicional

Pago del producto

Usuario

eloria@una.cr

☒ 500 GB ☐ 1 TB ☐ 2 TB

Monto del pago

CRC 10000

Salir

Pagar

Pasarela: esta pantalla, se encuentra en el servidor externo y se encarga de procesar el pago con la tarjeta.

Sistema de pago con tarjetas

Monto a debitar: CRC 10000

Tipo de tarjeta a debitar

Tipo de tarjeta... ▾

Número de tarjeta

Código de seguridad

Vencimiento

Número de tarjeta

Código

dd/mm/aa.

Cancelar

Procesar

Respuesta: pantalla que muestra el resultado de realizar la transacción, es dinámica y pueden ser reemplazados en título y el contenido.

Pago realizado

La transacción fue procesada con éxito.

Aceptar

Pago no realizado

No se procesó la transacción, verifique los datos e intentelo de nuevo.

Aceptar

Además se creó un archivo de script, en lenguaje JavaScript que realiza las funciones básica de llamado por medio de ajax a los servicios de la plataforma tanto del servidor principal como del externos.

Back-End

El desarrollo interno de ambos servidores se realizó sobre un mismo archivo dado que es un ejemplo de la funcionalidad.

Se adjuntará el código debidamente documentado por lo que se mostrarán las funcionalidades más importantes en la siguiente sección.

Servicio para creación de un hash de verificación (/service/hash/)

```
$app->post('/hash', function ($request, $response) {  
    $clave_hash = 'EstaEsLaClaveHash';  
    $parsedBody = $request->getParsedBody();  
    $data = ['hash' => hash('md5',  
        $_SESSION['usuario'].'-'  
        .$parsedBody['moneda'].'-'  
        .$parsedBody['timestamp'].'-'  
        .$parsedBody['monto'].'-'  
        .$parsedBody['transaccion'].'-'  
        .$parsedBody['comercio'].'-'  
        .$clave_hash)];  
    return $response->withJson($data, 201);  
});
```


Mediante el uso de una función “hash” se crea una clave única, dicha clave es generada con los valores usuario, moneda, fecha y hora (timestamp), monto, transacción (identificador único de transacción), comercio (identificador único del comercio) y finalmente una clave secreta, sólo conocida por los extremos. Todos estos datos se unen por un guión y generan el hash de la transacción.

El servicio responde con el hash, que luego será enviado a la pasarela de pago para verificar su validez.

Servicio de recepción de datos (/service/cargar/)

```
$app->post('/cargar', function ($request, $response) {  
    //PROCESO  
    $parsedBody = $request->getParsedBody();  
    $_SESSION['usuario'] = $parsedBody['usuario'];  
    $_SESSION['monto'] = $parsedBody['monto'];  
    $_SESSION['moneda'] = $parsedBody['moneda'];  
    $_SESSION['timestamp'] = $parsedBody['timestamp'];  
    $_SESSION['transaccion'] = $parsedBody['transaccion'];  
    $_SESSION['comercio'] = $parsedBody['comercio'];  
    $_SESSION['hash'] = $parsedBody['hash'];  
    $_SESSION['url'] = $parsedBody['url'];  
    $data = ['estado' => 1, 'url' => '/page/pasarela'];  
    return $response->withJson($data, 201);  
});
```

Los datos son enviados mediante post a un servicio de recepción de datos, donde los datos mencionados en el servicio anterior, la clave hash y una URL de respuesta son procesados y guardados por el servidor de la pasarela a la espera de una transacción.

El servidor pasarela responde con un JSON que indica el estado de la transacción y una URL donde debe ser redirigido el sistema para el pago.

Servicio de procesamiento y respuesta (/service/procesar/)

```

$app->post('/procesar', function ($request, $response) {
    $clave_hash = 'EstaEsLaClaveHash';
    $hash = hash('md5',
        $_SESSION['usuario'].'-'
        .$_SESSION['moneda'].'-'
        .$_SESSION['timestamp'].'-'
        .$_SESSION['monto'].'-'
        .$_SESSION['transaccion'].'-'
        .$_SESSION['comercio'].'-'
        . $clave_hash);
    if($hash == $_SESSION['hash']){
        $data = ['estado' => 1, 'url' => $_SESSION['url'].'/1'];
    } else {
        $data = ['estado' => 0, 'url' => $_SESSION['url'].'/0'];
    }
    return $response->withJson($data, 201);
});

```

Finalmente el servidor pasarela de pago procesa los datos de la tarjeta y los enviados por el cliente, regenera el hash, usando los mismos datos y la clave oculta, que en este caso se muestra en pantalla y para el ejemplo es “EstaEsLaClaveHash”.

Con fines de ejemplo no se realiza mayor verificación de los datos de tarjeta y solo se analiza el hash, el cual si coincide con el proporcionado valida el trámite y de lo contrario lo invalida, finalmente realiza una respuesta JSON, con el estado y la URL de respuesta o de origen de la transacción; completando el trámite.

Referencias

pabloclia. (septiembre 21, 2017). Configurar SSL en XAMPP con certificados autofirmados. Agosto 27, 2018, de <http://www.visualxstudio.com> Sitio web: <http://www.visualxstudio.com/blog/configurar-ssl-xampp-certificados-autofirmados/>