**طريقة إعداد شهادة SSL ذاتية التوقيع لمشروع PHP**

مرحباً! اختيارك لشهادة SSL ذاتية التوقيع هو الخيار الأفضل لتطويرك. لإعدادها في مشروع PHP، سنستخدم **OpenSSL** و **Apache** أو **Nginx**، وهما أشهر خوادم الويب.

**الخطوة الأولى: إنشاء الشهادة**

سنستخدم OpenSSL لإنشاء ملفين رئيسيين:

1. **مفتاح خاص (Private Key):** وهو المفتاح السري الذي يجب ألا يشاركه أحد.
2. **شهادة (Certificate):** وهي الشهادة العامة التي يثق بها المتصفح.

يمكنك تشغيل هذا الأمر في سطر الأوامر (Command Line):

openssl req -x509 -newkey rsa:2048 -keyout server.key -out server.crt -days 365 -nodes

* **req -x509**: هذا يعني أننا نريد إنشاء شهادة X.509 (وهو نوع الشهادة المستخدمة في الويب).
* **-newkey rsa:2048**: نُنشئ مفتاحًا خاصًا جديدًا من نوع RSA بطول 2048 بت، وهو معيار آمن.
* **-keyout server.key**: سيتم حفظ المفتاح الخاص في ملف اسمه server.key.
* **-out server.crt**: سيتم حفظ الشهادة في ملف اسمه server.crt.
* **-days 365**: صلاحية الشهادة ستكون لمدة 365 يومًا.
* **-nodes**: تعني "no des" (أي عدم تشفير المفتاح الخاص بكلمة مرور)، وهذا يسهل استخدامه في بيئة التطوير.

أثناء تنفيذ الأمر، سيُطلب منك إدخال بعض المعلومات. أهم شيء هو Common Name، حيث يجب أن تكتب localhost.

**الخطوة الثانية: إعداد خادم الويب (Apache أو Nginx)**

بعد إنشاء الملفات، ستحتاج لإخبار خادم الويب الخاص بك بمكان هذه الملفات وكيفية استخدامها.

**لخادم Apache:**

1. قم بتفعيل وحدة **SSL** في Apache (إذا لم تكن مفعلة بالفعل).

sudo a2enmod ssl

1. عدّل ملف إعدادات المضيف الافتراضي (Virtual Host) الخاص بمشروعك (عادةً ما يكون في مسار مثل C:\xampp\apache\conf\extra\httpd-vhosts.conf أو /etc/apache2/sites-available/).
2. أضف إعدادات SSL التالية:

Apache

<VirtualHost \*:443>

DocumentRoot "/path/to/your/php/project"

ServerName localhost

SSLEngine on

SSLCertificateFile "/path/to/server.crt"

SSLCertificateKeyFile "/path/to/server.key"

</VirtualHost>

تأكد من استبدال /path/to/your/php/project و /path/to/your/certificate بالمسارات الصحيحة.

1. أعد تشغيل Apache.

**لخادم Nginx:**

1. عدّل ملف إعدادات المضيف الافتراضي (Virtual Host) الخاص بمشروعك (عادةً ما يكون في مسار مثل /etc/nginx/sites-available/default).
2. أضف إعدادات SSL التالية:

Nginx

server {

listen 443 ssl;

server\_name localhost;

ssl\_certificate /path/to/server.crt;

ssl\_certificate\_key /path/to/server.key;

root /path/to/your/php/project;

index index.php index.html index.htm;

location ~ \.php$ {

include snippets/fastcgi-php.conf;

fastcgi\_pass unix:/var/run/php/php7.4-fpm.sock; # (أو حسب إصدار PHP-FPM)

}

}

1. أعد تشغيل Nginx.

**الخطوة الثالثة: تثبيت الشهادة في نظام التشغيل**

رغم أنك أعددت الخادم، سيظل المتصفح يُظهر تحذيرًا لأن الشهادة **ذاتية التوقيع** وليست من جهة موثوقة. لتجاوز هذا التحذير، يجب أن تثبت الشهادة في نظام التشغيل الخاص بك.

* **لنظام Windows:**
  1. اضغط على مفتاح Windows وابحث عن "Manage computer certificates".
  2. في نافذة الشهادات، اذهب إلى "Trusted Root Certification Authorities" > "Certificates".
  3. انقر بزر الماوس الأيمن على "Certificates" واختار "All Tasks" > "Import".
  4. اتبع التعليمات، واختار ملف server.crt الذي أنشأناه.
* **لنظام macOS:**
  1. افتح تطبيق "Keychain Access".
  2. اذهب إلى "File" > "Import Items...".
  3. اختار ملف server.crt، ثم انقر مرتين على الشهادة التي تم إضافتها.
  4. في نافذة الشهادة، قم بتوسيع قسم "Trust" واختار "Always Trust".

الآن، عند فتح https://localhost في متصفحك، لن يظهر أي تحذير، وستعمل كل ميزات الأمان التي تتطلب HTTPS بشكل طبيعي.

إذا واجهت أي مشاكل، فغالبًا ما تكون بسبب مسارات الملفات الخاطئة أو إعدادات الخادم.