

MOUGAMADOU Marzana 17800563  
VIGNESWARAN Thoussa 20014176

# Compte rendu du projet

Sécurité des réseaux  
Certification SSL d'un site WEB

# Présentation du projet

Le réseau internet est réseau mondial associant des ressources de télécommunication et des ordinateurs serveurs et clients, destiné à l'échange de messages électroniques, d'informations multimédias et de fichiers. En cette période de fermeture des centres commerciaux, de plus en plus de personnes utilisent internet pour faire leur achat. Mais est-ce que cette liaison est-elle sécurisée ? En faisant des recherches, nous avons choisi le sujet sur la certification SSL d'un site internet dans un réseau. Notre choix se base aussi d'un livre en anglais que vous pouvez trouver sur internet qui est Network Security with OpenSSL by John Viega, Matt Messier, Pravir Chandra. Un extrait du livre est : "The SSL (Secure Socket Layer) protocol and its successor TLS (Transport Layer Security) can be used to secure applications that need to communicate over a network."

## Déroulement du projet

- **CREATION DU SERVEUR ET DU SITE**

Au début du projet, nous avons décidé de faire sur Linux mais à chaque fois qu'on essayait on rencontrait des difficultés. En effet, nous avons téléchargé une machine virtuelle puis nous avons installé d'abord Debian comme c'est un système qu'on utilise à l'Université. Mais on n'arrivait pas à créer notre serveur et on avait un message d'erreur de packages. Puis, après recherche nous avons essayé de faire sur Ubuntu, celui-ci avait un problème avec la création du certificat et la génération des clés. Après multiples recherches, nous avons trouvé un forum nous parlant de WampServer qui est utilisé sous Windows. Comme nous nous sommes familiarisés avec Windows nous avons décidé de changer de système d'exploitation.

Pour indication WAMP SERVER 64 (Annexe 1) est une plate-forme de développement Web sous Windows pour des applications Web dynamiques à l'aide du serveur Apache2 et du langage de scripts PHP. Nous avons créé notre serveur grâce à Apache2 qui est un serveur http, et nous avons juste créé un serveur local (Annexe 2).

Pour la création du site, nous avons utilisé WordPress qui est un système de gestion de contenu (content management system (CMS) en anglais) gratuit, libre et open-source.

Ainsi, notre site a bien été créé (Annexe 3) et on remarque notre site est en http. HTTP est l'acronyme de Hypertext Transfer Protocol qui est un protocole de transmission permettant à l'utilisateur d'accéder à des pages web par l'intermédiaire d'un navigateur, c'est-à-dire c'est un protocole de communication entre un client et un serveur.

Notre site est en HTTP et on voit que il y un message disant que « Votre connexion à ce site n'est pas sécurisée : Vous ne devriez pas saisir d'informations sensibles sur ce site (par exemple, vos mots de passe ou les informations de votre carte de paiement), car elles risquent d'être dérobées par des pirates informatiques. »

L'internaute va envoyer une requête en http sur un réseau internet, et le serveur lui répond en http (Annexe 4). Mais une troisième personne entre l'internaute et le serveur peut intervenir pendant la transmission d'informations sur le réseau, d'où le fait qu'il ne faut jamais envoyer nos coordonnées lorsque le site est en http.

Des arnaques peuvent vite arriver lorsque l'on navigue en http, comme par exemple récemment sur l'application Signal, il y a eu un message (Annexe 5) de soi-disant 'Amazon' pour gagner un Iphone 12 Pro et le lien donné était sur http. Plusieurs personnes continuent de se faire arnaquer malheureusement par manque de connaissance en informatique et/ou manque de vigilance.

- **CREATION DU CERTIFICAT**

Dans un certificat SSL, il y a « SSL » qui est l'abréviation de Secure Socket Layer. Il s'agit d'un protocole permettant de sécuriser les échanges entre un internaute et une plateforme (site web, serveur, application mobile) via le chiffrement des données. Le protocole SSL a contribué à la sécurisation du web et au développement du commerce en ligne. Le certificat SSL est un certificat électronique qui intègre le protocole SSL. Il atteste le lien entre l'identité numérique et l'identité physique d'une personne ou d'une entreprise. Et garantit ainsi la confidentialité des données échangées entre le serveur et les internautes, par le biais d'une clé cryptographique.

Tout d'abord, on souhaiterait informer que notre certificat sera auto-signé. En effet, de nombreuses entreprises sont tentées d'utiliser des certificats SSL auto-signés plutôt que des certificats émis et vérifiés par une Autorité de Certification, et ce essentiellement pour des raisons financières. En effet, les prix du certificat SSL (Annexe 6) sont par exemple de deux sociétés connues dans le domaine :

- Gandi, les prix vont de 14 euros 40 à 336 euros annuellement,
- OVH, les prix vont de 3 euros 59 à 11 euros 99 mensuellement.

En cryptographie, une **Autorité de Certification** (AC ou CA pour Certificate Authority en anglais) est un tiers de confiance permettant d'authentifier l'identité des correspondants. Une autorité de certification délivre des certificats décrivant des identités numériques et met à disposition les moyens de vérifier la validité des certificats qu'elle a fournis. A l'inverse des certificats émis par une AC, les certificats auto-signés sont gratuits. L'utilisation d'un certificat auto-signé sur des sites utilisés en interne, tels qu'un portail pour les employés, déclenche également des messages d'alerte dans les navigateurs. De nombreuses organisations conseillent à leurs employés de simplement ignorer ces messages de sécurité car elles savent que leurs sites sont sans danger. Cependant, un tel comportement peut pousser certaines personnes à également ignorer ces messages lorsqu'elles visitent des sites publics, ce qui les rend vulnérables aux menaces.

Pour la création de notre certificat, on va utiliser la plateforme OpenSSL qui est une boîte à outils de chiffrement comportant deux bibliothèques, libcrypto et libssl, fournissant respectivement une implémentation des algorithmes cryptographiques et du protocole de communication SSL/TLS, ainsi qu'une interface en ligne de commande, openssl. On commence par la génération des clés RSA, il est conseillé de générer des clés d'une longueur de 2048 bits pour une meilleure sécurité. Pour un serveur Apache, il est conseillé

de générer des clés sans phrase de passe. Pour notre part, OpenSSL étant déjà sur WampSERVER64 mais malgré cela, je l'ai faite sur Windows pour générer une clé. Avec OpenSSL, la clé privée contient également les informations de la clé publique. Il n'est donc pas nécessaire de générer la clé publique séparément. La création du certificat s'est fait en deux commandes après la création des clés. (Annexe 7)

- **INSTALLATION DU CERTIFICAT SSL**

Pour l'installation du certificat, elle s'effectue en 3 étapes :


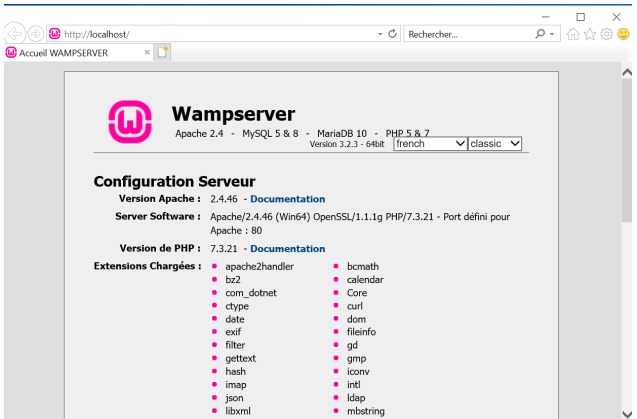
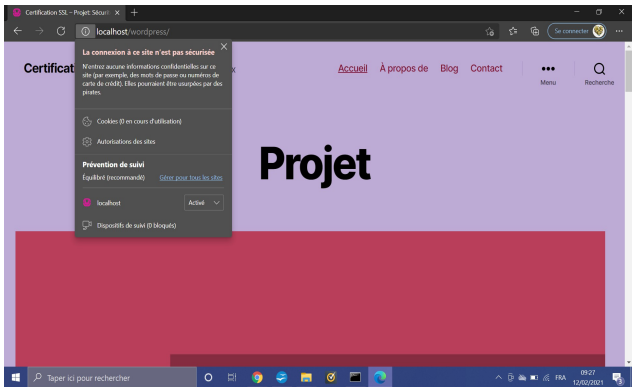
- Configuration d'un répertoire pour stocker les logs de SSL
- Configuration du fichier httpd-ssl.conf du journal des requêtes faites au serveur
- Configuration du fichier httpd.conf

## **Conclusion**

En conclusion, l'intérêt de mettre notre site en connexion https est la sécurité. La connexion en https (Annexe 8) est un navigateur qui envoie une requête en https et au lieu d'avoir une réponse directe, le serveur lui enverra le certificat SSL et celui-ci après être déchiffré et validé par l'autorité de certification permettra de communiquer entre le client et le serveur. On voit que notre site (Annexe 9) nous envoie quand même une alerte car notre certificat est auto-signé (Annexe 10) et n'a pas été validé par l'autorité de certification.

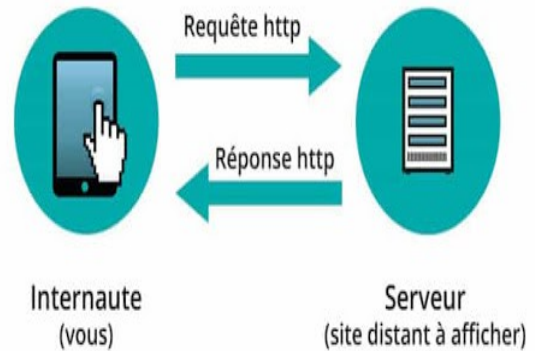
Les risques d'un certificat auto-signé : Si les dangers que représente l'utilisation d'un certificat auto-signé sur un site public paraissent évidents, il est important de comprendre qu'ils existent également pour les sites privés. L'utilisation d'un certificat auto-signé sur des sites utilisés en interne, tels qu'un portail pour les employés, déclenche également des messages d'alerte dans les navigateurs. De nombreuses employeurs conseillent à leurs employés de simplement ignorer ces messages de sécurité car elles savent que leurs sites sont sans danger. Cependant, un tel comportement peut pousser certaines personnes à également ignorer ces messages lorsqu'elles visitent des sites publics, ce qui les rend vulnérables au malware et aux autres menaces.

# Annexe

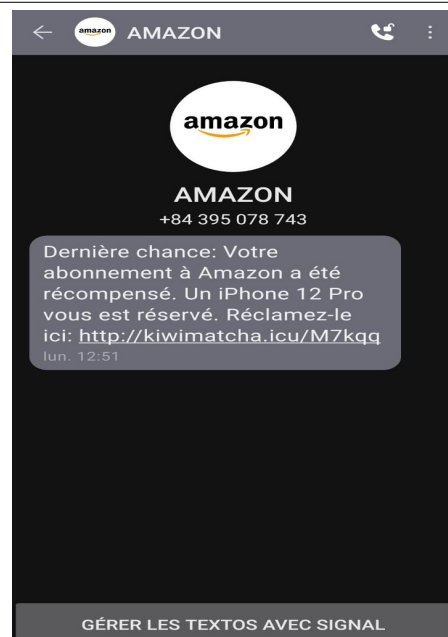
Numéro	Image
1	 The logo for Wampserver64, featuring a stylized 'W' in pink and blue, with a small shield icon to its left. Below the logo, the text 'Wampserver64' is written in a white, sans-serif font. The entire logo is set against a solid blue background.
2	 A screenshot of the Wampserver configuration page in a web browser. The page has a light gray background and a pink 'W' logo. It displays the following information: 'Wampserver', 'Apache 2.4 - MySQL 5 & 8 - MariaDB 10 - PHP 5.6 & 7', 'Version 3.2.3 - 64bit', 'french', and 'classic'. Under 'Configuration Serveur', it lists 'Version Apache : 2.4.46 - Documentation', 'Server Software : Apache/2.4.46 (Win64) OpenSSL/1.1.1g PHP/7.3.21 - Port défini pour Apache : 80', and 'Version de PHP : 7.3.21 - Documentation'. A section titled 'Extensions Chargées :' lists various PHP extensions like apache2handler, bz2, com_dotnet, ctype, date, exif, filter, gettext, hash, imap, json, libxml, bcmath, calendar, Core, curl, dom, fileinfo, gd, gmp, iconv, intl, ldap, and mbstring.
3	 A screenshot of the WordPress installation page in a web browser. The page has a purple background with the word 'Projet' in large white letters. A 'Certificat' (Certificate) dialog box is open in the foreground, displaying security warnings. The browser's address bar shows 'localhost/wordpress/'. The page also includes a navigation menu with links like 'Accueil', 'À propos de', 'Blog', 'Contact', and a search bar.

4

## Connexion en http



5



6

## Prix d'un certificat SSL : Gandi et OVH

Pack	Gratuit (auto-signé) valable sur simple hosting	Standard valable partout	Pro valable partout	Bussiness valable partout
Prix (Annuel)	Gratuit	14,40 euros	40,80 euros	336,00 euros

Pack	Perso	Pro	Perfomance (Boutique en ligne)	Cloud Web (Développeur Web)
Prix (Mensuel)	3,59 euros	7,19 euros	11,99 euros	11,99 euros

7

private - Bloc-notes

Fichier Edition Format Affichage Aide

-----BEGIN RSA PRIVATE KEY-----

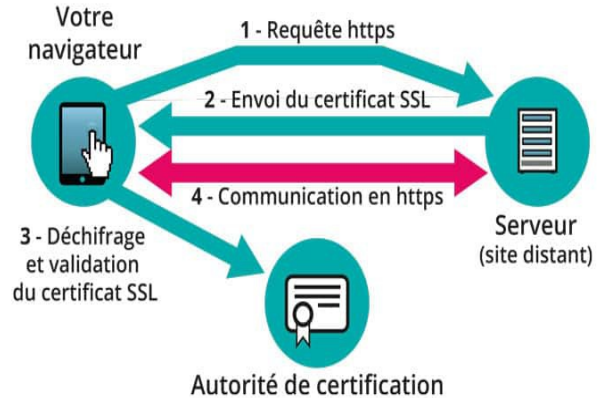
```

MIIEowIBAAKCAQEAwpjSYIjY6w+qbx0X1t32h88emkS36KBk8NEkrEAXIrjRTJhX
GrrJ8skg+A5F0jBgZG1YJD104VtJ2f0M7d2+V0M9vaMQajzR6Kukt/t8YI+QxMb
zXugwmF9Mj8QIAGAF0oLm75Pf/pcg60XS7vVcXRYeREFzI+kQ4KcFL3/1jMvdH7
jIVvPFv2U00B4K6biPcJhZSNpL+0N38Re9how8Kymfnqbu7fe/71pmzR+Jb/wYca
tx3r5aQd70ewLFTWAnjZ0o152dW59muYyU9sqz1TevXK5F5UH7HCUlMGXf+ZKPI+H
ZKK1Y8vdy4T5AeeE8+qm7aFF1GyD4X1QFrQ10wIDAQABAoIBACb4viExJugkkgiA
thaFC2t1cnaIXWm+PZjw+bw5daixhNENLUKgJ/OkjiK/kPiDYc9vEpjmbS75Hig2
0pEMuKLR3UKJBSIU3iEPxwRfEowVnLiOT1HnPxvEhk0tDmHAYOAtcmrPs/Y6nF
aHZ1XrDDEtJlznID5+zRRVrkXIBZqc8Y9jEjP6vNio7rWkyuUf3Y9Q+1zQL9QRx
fYkcWEhqTMBtAWny/s12u/vwbcwBeu3UZ7ZvR72FH4NAfXCnMkuzF0KjIGy7CjaC
8mDvsVdTTUjJ2F0siVYdyfyNua1P255WrJC1V1yy/A5m0S8SDnsW9Fgmf7bQbLZ+
gm3xZAEcGYEA7Ru1/Xy6hA8KwzZrkW9MeVvnUo15AD2w0KJICrfbXfVYS3wQJCv6
1gfQMB/4878vyOMkd6NYI84kEByXdXNn+f5UNpTz2k1A+1yVRFWPhu/QjN4J+wRz
FjuJGGNV+2/CrUia/mR9wtBV8tazdfQWbB4UBzPYRtzzekqH2MFDkgECgYEA0hoC
dH4dVH1ttV6AigXZdwC09UGxCKYe6IXkaCM9c3qqZEw5PIYajokQqEHKDJbR1gb
pguKrcOm4y1lVQ6ubZoMoqxJys1S6ENBfyc9X3W7yRY9Srbr79P2TJQ0GSak11z
8TBSr6KM8C0VjXu4r5C0e2zhbB6dvDJFW/CzfzsCgYEAjg3sGtJ/bf8Ws6HcbKWh
y50Ki3Fe7SYITeXsQc61PswfAjpzgLtyjLBxPiPpox8IIfL0Bj12tPzr3jtdArsB
sGUPtYQuDLuUEwSE6UvZkZ5b9AmTMTcZQtioalQZT2rF18uIEKfKnZaSwMwWbRb
OqtKLIYbLV1zBfFhMhuXwAECGYBd3FzIaib0PCM06XKHMEHMLiVHj9fre4EfioAw
j0ESvsfE5SYWwa8C1eLpGUNluf1pUAVaEsHriwKdbOUfsKVgNXfmxZoZzAML3DA
AfC1A4jn4RcUwAbQ5ujnIuyU0NL1jPrs/yeRa08HZTzBrkn9tOmMUGivog/ZqaOu
xUOLTQKBgEud+fC9wfZKCJuwYmVbqk70qVq1dCznHxZW5zaHBI2gbx/FIMIKfA9g
kprYy1bH1ATwcn1m/XjFZ8KYhSGc+IERBzBMtuRsT/jvkcdmj8jf+qrjjc8m9qq1
7iFJ1JNX2fE1ukaI2uV8RP6rwu9TkXRRPzS2qm7nniMgq4Iwbkrn
-----END RSA PRIVATE KEY-----

```

8

## Connexion en https



9

