Computer Networks (LINGI1341) : Projet Individuel

FSA2BA

Nom : Chauvaux Nicolas, Noma : 1995-1600

***Introduction*—Ce document rentre dans le travail individuel réalisé dans la cadre du cours LINGI1341 donné par le professeur Olivier Bonaventure à l'Université Catholique de Louvain-la-Neuve.**

I. Introduction

Dans ce document, nous allons analyser le site web *openclassrooms.com* . Il s'agit d'un site français ayant pour but de proposer des cours divers sur les différents sujets liés à l'informatique ou encore le marketing, les sciences et l'entreprenariat. Ce site a reçu plusieurs prix pour son innovation. Il possédait en 2015 plus de 1 millions de comptes utilisateurs

Pour analyser ce site web, nous avons utilisé plusieurs outils comme NStools qui permet une analyse détaillée des entêtes. Celui-ci effectue aussi une série de tests vérifiant la bonne configuration des serveurs.

II. Analyse DNS

Nous pouvons remarqué que *Openclassrooms* utilise deux noms de domaine :

- openclassrooms.com (principale)
- openclassroom.com

Le deuxième noms de domaine est re-dirigé vers le premier lors de la requête HTTP comme nous le verrons par la suite. Non pouvons en effet vérifier cette information puisque *openclassroom.com* possède le CNAME "webredir.vip.gandi.net". Celui-ci permet d'établir une connexion avec les utilisateurs oubliant le "s". Seul *openclassrooms.com* est accessible en IPV6.

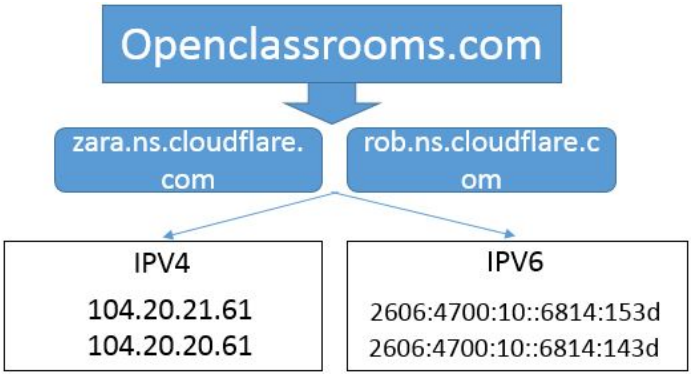

Fig. 1. Analyse DNS

Le second serveur est le serveur maître d'après les informations fournie dans SOA ("Start of Authority") (RFC 2136). En effet, chaque nom de domaine doit au minimum avoir deux DNS, l'un primaire et l'autre secondaire). Le serveur Zaza, permettant le transfert de zone DNS et une augmentation de la sécurité des DNS. L'analyse des champs présents peut se faire via ce site web.

```
Authoritative answers can be found from:
openclassrooms.com
        origin = rob.ns.cloudflare.com
        mail addr = dns.cloudflare.com
        serial = 2029394315
        refresh = 10000
        retry = 2400
        expire = 604800
        minimum = 3600
```

Fig. 2. Analyse entête SOA

Voici la définition de chaque champ :

- origin : Il s'agit du serveur maître
- mail addr : mail du responsable de la zone DNS
- serial : Ce champ est modifié à chaque changement et indique la date de mise à jour). Ce champ est donné sous la forme YYYYMMDDVV avec
  - YYYY pour l'année
  - MM pour le mois
  - DD pour le jour
  - VV pour la version commençant à 00
- refresh : Indique le temps après lequel un serveur secondaire doit vérifier auprès du serveur primaire si le numéro de série à changé.
- retry : Temps avant de re-questionner le serveur en cas d'échec (15min-1h)
- expire : Temps durant lequel les serveurs secondaires doivent continuer à répondre aux requêtes sans avoir eu de signe de vie du serveur primaire.
- minimum : Il s'agit du TTL (time to live) par défaut dans le cas ou aucun TTL n'a été fourni.

Le nom de domaine possède 5 serveurs de mail, tous provenant de Google :

alt1.aspmx.l.google.com	aspmx.l.google.com	aspmx2.googlemail.com
aspmx3.googlemail.com	alt2.aspmx.l.google.com	

Fig. 3. Serveur Mail

Openclassrooms utilise des serveurs virtuels dédiés (VPS qui

ont l'avantage d'héberger plusieurs sites web sur un même serveur physique tout en gardant des environnements totalement indépendants. Les serveurs appartiennent à Amazon Web Services (AWS).
Aucun CDN n'est utilisé pour ce nom de domaine ce qui peut avoir un impact très négatif pour certains endroit du monde, comme le montre RIPE Atlas avec un délai atteignant 1130ms dans le sud de l'Afrique ou encore 800ms à Cuba. Le site souhaitant se tourner vers l'international depuis 2013 au lancement de la version 4 de leur plate-forme, il faudra résoudre ce problème si ils souhaitent atteindre des endroits ou le délai est élevé. Nous verrons cependant qu'un CDN est utilisé pour certains types de ressources.

III. Analyse HTTP(S)

A. HTTP

Si nous tentons d'accéder au site via une connexion non sécurisé, une re-direction permanente (code 301) ou temporaire (code 302) sera envoyé au client. On constate que celle-ci cause un délai de 300ms. Cela aurait pu être optimisé en re-dirigant directement vers "https://openclassrooms.com/fr". De plus aucun cookie n'est transféré durant ces re-directions. Pour permettre la re-direction $HTTP \rightarrow HTTPS$, le client place dans l'entête HTTP l'option Upgrade-Insecure-Requests:1 pour indiquer au serveur qu'il préfère une réponse cryptée et authentifiée. Il est aussi utilisé par un serveur pour indiquer au client qu'il devrait accéder au ressources via HTTPS. L'option strict-transport-security joue un rôle important dans les re-directions. En effet, cela permet au navigateur de ne jamais faire de requête HTTP à un serveur si durant une communication précédente l'option était présente. Cela réduit les attaques (man-in-the-middle) lors des re-directions. On peut cependant constater que cela n'est pas possible pour la re-direction *openclassroom.com* (sans s) puisque celui-ci ne supporte pas HTTPS.

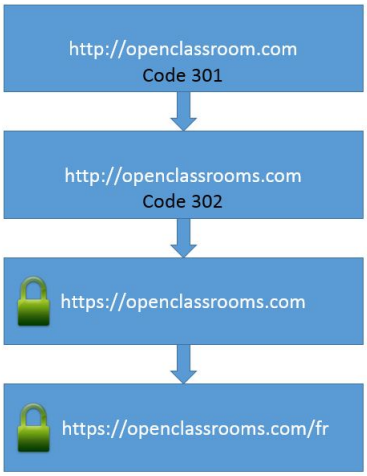

Fig. 4. Analyse entête SOA

B. HTTPS

Ce sites fait appel à de nombreux autres domaines (tous sécurisés) aussi divers les uns que les autres. 1) Les traqueurs :

- Crazy Egg permettant notamment de savoir exactement l'endroit de chaque clique utilisateur.
- Analytics.js
- Goole analytics
- ...

Certains d'entre eux, comme Facebook, Twitter, Google, envois des 1x1 pickel dans le but de récupérer des informations sur les utilisateurs (type d'OS, navigateur, adresse ip, activités). 2) Les polices, images et autres Ils utilisent d'autres domaines pour fournir une parties des éléments dont ils ont besoin. C'est le cas par exemple de plusieurs images, provenant de Imgix ou encore pour les fichiers .css fournit par le CDNJS de Cloudflare

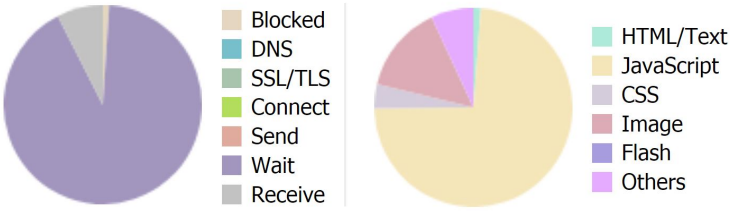

Fig. 5. Répartition des ressources

On voit nettement le grand nombre de fichier javascript transféré (39), dû en partie à tous les traqueurs.

C. Utilisation des cookies

Nous n'analyserons ici uniquement les cookies utilisé par openclassrooms.com directement. Les ressources partagées émettent aussi un grand nombre de cookie provenant de divers domaines, mais ceux-ci ne nous intéressent pas.

- AWSELB : Il s'agit d'un cookie assez particulier, directement lié aux modes de fonctionnements des serveurs d'Amazon. Amazon Web Services (AWS) fournit ce qu'on appel un *Equilibreur de charge*. Comme expliqué précédemment, Openclassrooms utilise une série de serveurs virtuel. *L'équilibreur de charge* va permettre de re-diriger les requêtes vers le serveur virtuel le moins chargé. Ce cookie va permettre de lié une connexion à une instance. Si le cookie est présent, alors *l'équilibreur de charge* va re-diriger la requête vers l'instance qui y es spécifié, sinon il fait tourner son algorithme de charge.
- __CFDUID: est un cookie utilisé par CloudFlare pour identifié les clients individuellement. Il est essentiel de l'utilisé pour pouvoir bénéficier de la sécurité proposé par CloudFlare (pour ses clients). Celui-ci permet de vérifier la fiabilité des clients.
- AMPLITUDE_IDUNDEFINEDOPENCLASSROOMS.COM : Il s'agit d'un cookie traqueur. Celui-ci peut être utilisé de multiple facon comme pour l'analyse de la fréquence de "click" sur un bouton.
- _FBP : est un cookie appartenant à Facebook.
- AJS_ANONYMOUS_ID / AJS_GROUP_ID / AJS_USER_ID : ce sont des cookies provenant du module Analytics.js qui permet aussi de voir ce que le client à visité avant.

- _GA / _GID: Cookie de Google Analytics pour identifier les utilisateurs.
- _GAT : Ce cookie permet de diminuer le taux de requêtes en cas de fort trafic. Notamment en limitant le nombre de requête vers *doubleclick.net*.

Lors de la connexion à un compte utilisateur sur *openclassrooms.com*, tous les cookies précédents sont envoyés par le client. Nous pouvons observer de nouveaux cookies, dans la réponse du serveur, permettant à l'utilisateur d'accéder aux contenus réservés aux utilisateurs. Il est important de constater que tout ces cookies ont l'attribut "secure: true". Cet attribut permet d'informer le client qu'il ne doit jamais transférer ces cookies sur un canal non sécurisé. En effet, l'usurpation de ces cookies peut entraîner un vol de compte utilisateur. L'attribut "HTTPOnly" est aussi présent. Celui-ci permet d'empêcher tout fichier javascript d'accéder aux cookies. Étrangement un cookie avec la date d'expiration du 1^{er} *janvier 1970* est envoyé avec la valeur mis à *deleted.*

En plus des cookies, ce site envoi aussi des sessions PHP. Celles-ci permettent au serveur de stocker des informations à propos d'un utilisateur (comme un identifiant d'utilisateur). Ceux-ci on été créé pour pallier à la non-connexion du protocole HTTP. Les variables de sessions ne sont pas stocké sur l'ordinateur client et sont supprimé à la fin de la navigation.

D. Entête HTTP

- CF-RAY : Cette entête est uniquement utilisé par les serveur de CloudFlare pour signaler que la requête à été fournie par leurs serveur. Cela peut être très utile pour régler les problèmes de connectivité. Elle est constitué d'un
- CF-CACHE-STATUS : Cette entête peut prend plusieurs valeur dont MISS (signifie que aucun cache n'est présent pour la donnée demandé) et HIT (la ressources fournie provient du cache et non du serveur d'origine). On peut constater que Openclassrooms utilise le cache des serveurs de CloudFlare pour les fichiers images, css et javascript. C'est à dire que Openclassrooms utilisent le cache CDN de CloudFlare pour ces ressources lorsque "cache-control: public". Cependant, pour le fichier HTML, Openclassrooms empêche explicitement les serveurs de CloudFlare d'utiliser le cache. Ceci est fait grâce à l'entête "cache-control: no-cache="set-cookie"". Les informations doivent dés lors être prise du serveur source. On constate aussi ici l'utilisation d'un entête obsolète "pragma" qui est remplacé par "cache-control".
- EXPECT-CT: Il s'agit d'une entête informant le navigateur du client qu'il doit vérifier si le certificat fourni se trouve dans la liste de transparence des certificats SSL. Suite à des failles dans le système de certifications HTTPS, cette méthode, émise par Google, permet d'avoir un suivit sur l'ensemble des certificats attribut. Les faux certificats peuvent ainsi être détecté rapidement.
- REFERRER-POLICY: SAME-ORIGINE : Cet option est utilisé lorsqu'on navigue dans un site web. Lors du chargement d'une page, le client va envoyer dans sa requête une option "referer" avec comme valeur l'URL de la page précédente. La valeur same-origine informe qu'il ne faut pas fournir cet URL à un autre site.
- X-CONTENT-TYPE-OPTIONS:NOSNIFF : Lorsqu'un serveur envois des données et qu'il spécifie un type de données (par exemple text/css), cet entête empêche les navigateurs de modifié le type.

IV. Analyse TLS

Openclassrooms supporte les 4 versions de TLS, c'est à dire les versions :1.0-1.1-1.2-1.3. Nous constatons dés lors que ce site n'est pas en conformité avec la norme PCI DSS (Payment Card Industry Data Security Standard) qui informe que SSL et TLS1.0 doivent être supprimé depuis le 30 juin 2018. En effet, ceux-ci ont été révélé vulnérable aux attaques du type "homme du milieu" ou un pirate serait capable de récupérer les cookies de sessions normalement cryptée. Ce nom de domaines possède un certificat EV (validation étendue) SSL. Il s'agit du type de certificat ayant le niveau de chiffrement le plus élevé. En outre, il permet aux utilisateurs de facilement vérifier l'identité du site web en regardant simplement la barre de recherche de leur navigateur. Comme dit précédemment

Fig. 6. Certificat EV SSL

dans l'analyse HTTP, ce site supporte la transparence des certificat ce que rend sa sécurité encore plus accrue.

Enfin, il semblerai que le serveur ne supporte pas OCSP

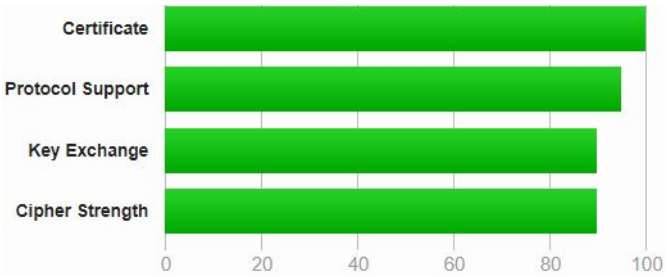

Fig. 7. Certificat EV SSL

Must Staple (RFC7633). OCSP est une requête permettant de vérifier si un certificat reçu est révoqué ou non par la CA (autorité de certification). Le problème initiale de OSCP était que chaque client devait interroger la CA, ce qui surcharge ceux-ci. OCSP Must Staple (ou OCSP agraphé) permet au serveur d'un site web de lui même interroger la CA de temps en temps et d'inscrire la réponse dans le "Serveur Hello". Cela permet au client d'avoir un chargement plus rapide. De plus, le "must" signifie qu'il y aura toujours une réponse OCSP attaché. Si elle n'y est pas, alors la connexion est refusé. Openclassrooms supporte par contre PCSP Staple, qui possède une faille de sécurité. En effet, il n'impose pas que la réponse OCSP soit agrafé dans la réponse TCP et dans les cas ou les serveurs OCSP sont en pannes, le client n'arrivant

pas à les joindre, va tout de même accepté le certificat alors qu'il peut être incorrecte. Un autre problème est que aucun CAA (DNS Certification Authority Authorization) défini dans RFC6844 n'est spécifié. Celui-ci permet au détenteur d'un nom de domaine de spécifier quel CA est autorisé à fournir un certificat pour ce nom de domaine. Ça présence permet de renforcer la sécurité en empêchant l'émission de certificat erroné.
Les serveurs de Openclassrooms supportent deux options TLS intéressantes :

- Session resumption (caching) : Lors de la connexion sécurisé à un serveur, celui-ci conserve un identifiant de session. Si le client veux se reconnecté, celui-ci peut envoyé l'ID de session précédent pour ne pas devoir renégocier toutes les options.
- Session resumption (tickets) : Le procéder ici à pour but comme pour l'option précédente de reprendre une connexion précédemment effectué. Cependant, le procédé est totalement différent. Dans ce cas-ci, le serveur ne sauvegarde aucune information sur les connexion précédente mais envois un ticket de session, que lui seul peut décrypter, à la fin de la connexion TLS et qui contient la clé de session et autres informations utiles. Le client va stocker ce "ticket" dans son cache et la renvoyer au serveur lors de la prochaine connexion.

A. *Clés cryptographique*

Les 4 versions TLS utilisé par les serveurs d'Openclasrooms supportent l'utilisation de suites de chiffrements dites PFS (secret de transmission parfait). Ce type de protocole d'accord de clé cryptographie garanti, en cas d'attaque visant le serveur, que vos clés de sessions ne seront pas compromise et cela même si l'attaquant a réussi à obtenir la clé privé du serveur. Ainsi, toutes les communications précédente avec ce serveurs ne pourrons pas être décrypté par l'attaquant. Attention cependant, ceci n'est pas le cas pour les communication future puisque la personne malveillante peut se faire passer pour le serveur compromis.
Nous pouvons observer, suite à l'analyse de SSLLab, l'ordre de préférence du serveur pour les SC (suites de chiffrements). Notons que pour TLSv1.3, le serveur n'a aucune préférence pour les suites de chiffrements et n'accepte que les trois SC par défaut dans TLSv1.3. L'analyse pour les versions précédente est plus intéressant puisqu'on peut observé que le serveur d'Openclassrooms ne place pas les SC les plus faibles (n'étant pas PFS) en dernière position.

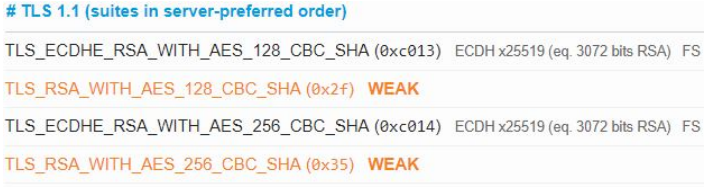

Fig. 8. Ordre de préférences : suite de chiffrements TLSv1.1

Openclassrooms obtiendrait probablement la note A+ pour les test "SSLLabs" en fixant la valeur de "max-age" pour l'attribut HSTS (RFC6797) a une valeur supérieur à 180 jours (actuellement fixé à "max-age=2592000", c'est à dire 30 jours).

V. Analyse TCP

Pour cette partie, nous allons utiliser le programme de capture de paquet réseau WireShark.

A. *Three-way handshake*

Les serveurs d'Openclassrooms supporte TCP Sack (TCP Selective Acknowledgements) comme nous pouvons le voir lors de l'échange des options "Fig. 9".

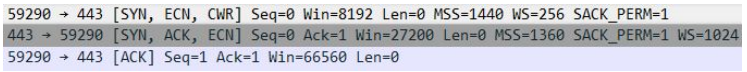

Fig. 9. Tcp handshake

Les drapeaux ECN (notification explicite de congestion) et CWR (Congestion Window Reduced) ne sont indiqué dans le SYN par le client uniquement pour indiquer le serveur qu'il supporte ces options. Les options TCP MSS = 1440 (maximum size segment), WS = 8 (window scale) y sont négociées. De plus, plusieurs connexion TCP sont possible simultanément.

B. *Fermeture de connexion*

En ce qui concerne la fermeture de connexion, le client et le serveur utilise le drapeau FIN. Cependant, on constate que le client utilise ensuite le drapeau RST (réinitialiser la connexion) alors que la connexion est fermée.

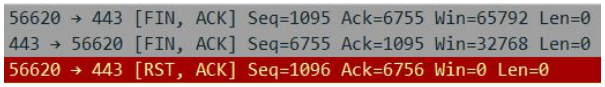

Fig. 10. TCP Fin flag

C. *Re-connexion*

Nous avons vu dans la section concernant l'analyse TLS qu'il était possible de récupérer une connexion précédente à l'aide de "Session resumption (tickets)". La "Fig. 11" nous montre les premiers paquets envoyer entre client serveur lors de l'accès au site précédemment visité. Nous pouvons constater que le client envois directement un paquet TLS sans même passer par une connexion TCP. Étrangement la reconnexion se fait via TLSv1.2 et non TLSv1.3 comme pour la première connexion.

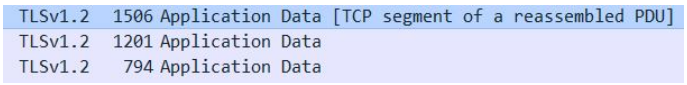

Fig. 11. Re-connexion

VI. Conclusion

L'analyse d'un site web connu,durant ce projet, m'a permis de comprendre plus en profondeur les mécanismes utilisé par ces sociétés pour optimiser la sécurité et l'accès à leur site. Cela m'a permit fait prendre conscience de la complexité de toute l'infrastructure mise en oeuvre.

REFERENCES

[1] WIKIPEDIA, *SOA Resource Record* [En ligne], https://fr.wikipedia.org/wiki/SOA_Resource_Record, consulté le 11 décembre 2018.

[2] WIKIPEDIA, *OpenClassrooms* [En ligne], https://fr.wikipedia.org/wiki/OpenClassrooms, consulté le 24 novembre 2018.

[3] WIKIPEDIA, *Amazon Web Services* [En ligne], https://fr.wikipedia.org/wiki/Amazon_Web_Services, consulté le 15 décembre 2018.

[4] AMAZON, *Etude de cas AWS : OpenClassrooms* [En ligne], https://aws.amazon.com/fr/solutions/case-studies/openclassrooms/, consulté le 15 décembre 2018.

[5] WIKIPEDIA, *Transfert de zone DNS* [En ligne], https://fr.wikipedia.org/wiki/Transfert_de_zone_DNS, consulté le 1 décembre 2018.

[6] ACEI, *Comprendre le transfert de fichier de zone et les TSIG* [En ligne], https://acei.ca/l%E2%80%99utilisation-de-tsig-pour-des-communications-s%C3%A9curis%C3%A9es-entre-les-serveurs-dns/comprendre-le, consulté le 1 décembre 2018.

[7] NS, *UNDERSTANDING TTL VALUES IN DNS RECORDS* [En ligne], https://ns1.com/resources/understanding-ttl-values-in-dns-records, consulté le 1 décembre 2018.

[8] De Cricket Liu, "DNS BIND Cookbook" [Livre en ligne], https://books.google.be/books?id=mjabAgAAQBAJ&pg=PT39&lpg=PT39&dq=YYYYMMDDVV+SOA&source=bl&ots=V6Q6i84Cnx&sig=41XGjGiOmxPBNQcstS4VTWxaWAk&hl=fr&sa=X&ved=2ahUKEwjIqIXGmJ3fAhVQbFAKHd1nBH4Q6AEwCHoECAUQAQ#v=onepage&q=YYYYMMDDVV%20SOA&f=false, consulté le 1 décembre 2018.

[9] RYTE WIKI, *Pixel espion* [En ligne], https://fr.ryte.com/wiki/Pixel_espion, consulté le 8 décembre 2018.

[10] CloudFlare, *Support CloudFlare* [En ligne], https://support.cloudflare.com/hc/en-us/articles/200170156-What-does-the-Cloudflare-cfduid-cookie-do-, consulté le 1 décembre 2017.

[11] MDN web docs, *Strict-Transport-Security* [En ligne], https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security, consulté le 13 décembre 2018.

[12] Doug Beattie, *Pensez à désactiver le TLS 1.0 (et toutes les versions de SSL) si ce n'est déjà fait* [En ligne], https://www.globalsign.fr/fr/blog/desactiver-tls-10-et-toutes-les-versions-ssl/, consulté le 8 décembre 2018.

[13] LAURA K. GRAY, *Are You Ready for 30 June 2018? Saying Goodbye to SSL/early TLS* [En ligne], https://blog.pcisecuritystandards.org/are-you-ready-for-30-june-2018-sayin-goodbye-to-ssl-early-tls, consulté le 8 décembre 2018.

[14] COMODO, *Deprecation of TLS 1.0* [EN ligne], https://www.comodo.com/e-commerce/ssl-certificates/tls-1-deprecation.php, consulté le 8 décembre 2018.

[15] GLOBALSIGN, *Certificat EV SSL à validation étendue* [En ligne], https://www.globalsign.fr/fr/centre-information-ssl/definition-certificat-ev-ssl/, consulté le 9 décembre 2018.

[16] Hanno Böck, *The Problem with OCSP Stapling and Must Staple and why Certificate Revocation is still broken* [En ligne], https://blog.hboeck.de/archives/886-The-Problem-with-OCSP-Stapling-and-Must-Staple-and-why-Certificate-Revocation-is-still-broken.html, consulté le 9 décembre 2018.

[17] P. Hallam-Baker, *X.509v3 Transport Layer Security (TLS) Feature Extension* [En ligne], https://tools.ietf.org/html/rfc7633, consulté le 8 décembre 2018.

[18] WIKIPEDIA, *Forward secrecy* [En ligne], https://en.wikipedia.org/wiki/Forward_secrecy, consulté le 8 décembre 2018.

[19] OPENSSL, *TLSv1.3* [En ligne], https://wiki.openssl.org/index.php/TLS1.3, consulté le 8 décembre 2018.

[20] IETF, *DNS Certification Authority Authorization (CAA) Resource Record* [En ligne], https://tools.ietf.org/html/rfc6844, consulté le 2 décembre 2018.

[21] IETF, *Sécurité du transport strict HTTP (HSTS)* [En ligne], https://tools.ietf.org/html/rfc6797, consulté le 7 décembre 2018.

[22] TBS CERTIFICATS, *Facilitez votre migration à HTTPS avec la directive CSP Upgrade Insecure Requests* [En ligne], https://www.tbs-certificats.com/FAQ/fr/upgrade-insecure-requests.html, consulté le 7 décembre 2018.

[23] AMAZON, *Configurer des sessions permanentes pour votre Classic Load Balancer* [En ligne], https://docs.aws.amazon.com/fr_fr/elasticloadbalancing/latest/classic/elb-sticky-sessions.html, consulté le 13 décembre 2018.

[24] GOOGLE, *Google Analytics Cookie Usage on Websites* [En ligne], https://developers.google.com/analytics/devguides/collection/analyticsjs/cookie-usage, consulté le 13 décembre 2018.

[25] WIKIPEDIA, *Secure cookie* [En ligne], https://en.wikipedia.org/wiki/Secure_cookie, consulté le 13 décembre 2018.

[26] CloudFlare, *What do the various Cloudflare cache responses (HIT, Expired, etc.) mean?* [En ligne], https://support.cloudflare.com/hc/en-us/articles/200168266-What-do-the-various-Cloudflare-cache-responses-HIT-Expired-etc-mean-, consulté le 13 décembre 2018.

[27] CERTIFICATE TRANSPARENCY, *What is Certificate Transparency?* [En ligne], https://www.certificate-transparency.org/what-is-ct, consulté le 13 décembre 2018.

Programmes en ligne :

[28] DNSLytics, [Application en ligne], https://dnslytics.com/ip/173.245.59.140, dernière consultation le 15 décembre 2018.

[29] Ripe NCC, [Application en ligne], https://atlas.ripe.net/measurements/17177681/#!general, consulté le 13 décembre 2018.

[30] NS TOOLS, [Application en ligne], https://nstools.fr/openclassrooms.com, dernière consultation le 15 décembre 2018.

[31] , SOFTWAREISHARD, *Visualisé des fichiers HAR* [Application en ligne], http://www.softwareishard.com/har/viewer/, dernière consultation le 13 décembre 2018.

[32] SSL LABS, [Application en ligne], https://www.ssllabs.com/ssltest/analyze.html?d=openclassrooms.com, dernière consultation le 15 décembre 2018.