REPUBLIQUE DU SENEGAL

UNIVERSITE CHEIKH ANTA DIOP

Ecole Supérieure Polytechnique de Dakar
Département Génie Informatique

MEMOIRE DE FIN DE CYCLE

Pour l'obtention du :

DIPLÔME D'INGENIEUR DE CONCEPTION EN INFORMATIQUE

Etude et mise en oeuvre d'une application conforme OWASP

Lieu de stage :
HubSo

Présenté et soutenu par :
Papa Latyr MBODJ

Maîtres de stage :
Ahmed Tidiane CISSE
Mouhamadou Mansour Sy SAMB

Professeur encadreur :
M. Ibra DIOUM

Année universitaire : 2017-2018

VISA

DÉDICACES

Remerciements

AVANT-PROPOS

Établissement public à caractère administratif doté de la personnalité juridique et de l'autonomie financière, l'École Supérieure Polytechnique (ESP) fait partie intégrante de l'université Cheikh Anta DIOP de Dakar (UCAD). Elle a été créée par la loi n° 94-78 du 24 novembre 1994. Elle a pour vocation de former des techniciens supérieurs, des ingénieurs de conception, des managers dans ses six (06) départements : Génie Chimique, Génie Civil, Génie Electrique, Génie Informatique, Génie Mécanique et Gestion.
Le Département Génie Informatique forme des ingénieurs de conception en informatique de qualité capables de s'adapter aussi bien dans les entreprises que dans le domaine de la recherche. Pour l'obtention du Diplôme d'Ingénieur de Conception (DIC), les élèves-ingénieurs sont tenus d'effectuer un stage dans une structure qui leur permettra :
- De renforcer leur savoir et surtout d'acquérir un savoir-faire, tout en essayant d'adapter leurs connaissances aux cadres de la vie professionnelle avec un dynamisme d'ingénieur ;
- De travailler sur un Projet de Fin de Cycle et de mener à bien l'élaboration de celui-ci depuis l'étude préalable jusqu'à sa mise en exploitation.

C'est dans cette optique que nous avons effectué un stage d'une durée de six mois à HubSo.

RÉSUMÉ

Abstract

TABLE DES MATIÈRES

LISTE DES TABLEAUX

TABLE DES FIGURES

INTRODUCTION

....

Ce document s'articule autour de

Première partie

Présentation Générale

Table des matières

CHAPITRE 1

LA STRUCTURE D'ACCUEIL

1.1 Présentation de HubSo

HubSocial est une entreprise informatique créée en 2011. Le 01er Mai 2018, elle change de nom et devient HubSo.Elle œuvre pour le développement de solutions informatiques à valeurs sociales au Sénégal. Par l'usage des nouvelles technologies de l'information et de la communication, elle tente de matérialiser le concept d'actions sociales, d'aider les personnes et groupes les plus fragiles à mieux appréhender les domaines de la santé, de l'éducation, de la réduction de la pauvreté etc...
HubSo accompagne aussi d'autres entreprises à mettre en place des solutions informatiques qui leur sont adaptées. Sur ce point, HubSo étant un grand adepte du manifeste agile, tient à cœur la collaboration avec ces entités pour bâtir des partenariats solides plus que tout. De même, elle collabore aussi avec d'autres entreprises de services du numérique. Parmi ces collaborateurs de HubSo, nous avons :
- Intouch, le plus proche partenaire ;
- Mazars ;
- Yux ;
- Performances Group ;
- 2SI ;
- entre autres.

1.2 Domaines d'activités

HubSo propose les services suivants :
- Développement de solutions informatiques : HubSo est reconnue pour son expérience et ses références en matière de développement autour des technologies JEE et Android. Une équipe de plus de 15 ingénieurs de conception est à l'écoute de vos besoins ;
- Conseil en architecture d'entreprise : Les équipes de Hubso animent des ateliers avec ses clients pour concevoir leur architecture d'entreprise ;
- Tierce maintenance applicative : aide à la maintenance d'application déjà en production et devant être corrigées ou améliorées ;
- Promotion de solutions innovantes pour la société : Hubso, c'est aussi l'innovation par la promotion de solutions.

1.3 Quelques Solutions de HubSo

Hubso propose entre autres, les solutions suivantes :
- TONGTONG
TongTong est un site de vente en ligne basé sur les concepts d'achat groupé. TongTong, lancé par Hubso en 2014 , est aujourd'hui une référence dans le domaine de l'Ecommerce, notamment en matière de produits alimentaires manufacturés, de légumes, de produits locaux, etc. Il est possible de faire ses commandes sur www.tongtong.sn
- GRANT
GRANT est une solution permettant à une entreprise de subventionner un ou plusieurs services pour ses employés. Elle a été lancée par Hubso en 2017. Les subventions de tickets restaurant ont été intégrées à la plateforme et sont aujourd'hui utilisées par plusieurs entreprises.
- AVISJOURNAUX.COM
AVISJOURNAUX.COM diffuse quotidiennement tous les appels d'offres et autres avis parus au Sénégal à ses milliers d'abonnés. C'est aujourd'hui une solution de référence dans le domaine, plébiscitée par les nombreux messages d'encouragement. Les abonnements "Grand public" sont gratuits. Cependant, une offre dédiée est commercialisée pour les regroupements de professionnels désirant bénéficier d'un service plus adapté.

1.4 Organisation

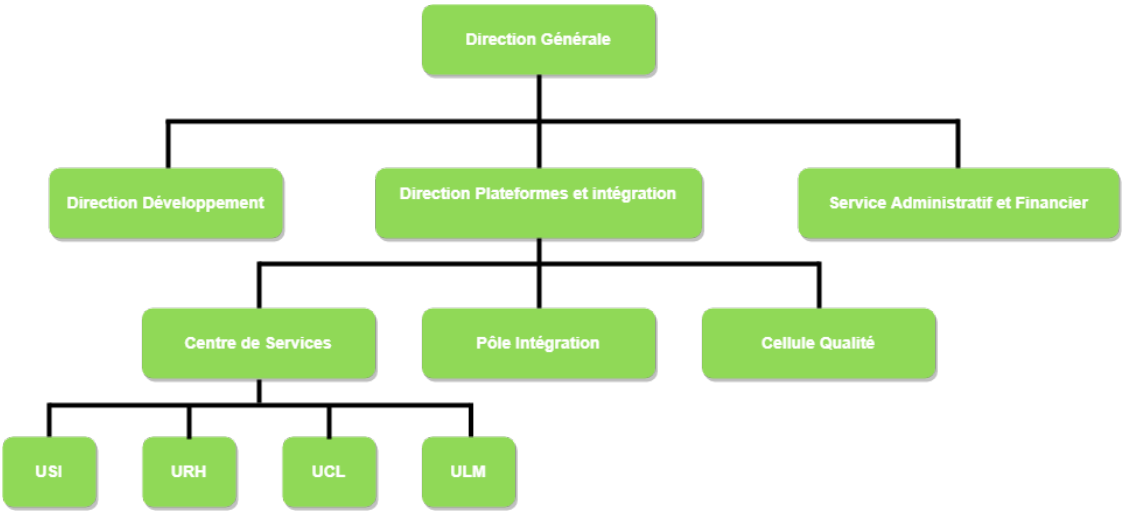

FIGURE 1.1 – Organigramme de HubSo

La figure 1.1 représente l'organnigramme de HubSo. HubSo comprend trois départements reliés à la Direction Générale :
- Direction Développement qui s'occupe du développement des solutions informatiques ;
- Service Administratif et Financier s'occupant des affaires administratives et financières - Direction plateformes et intégration qui comprend en son sein la Cellule Qualité chargée d'assurer la

Qualité des produits développés, le Pôle Intégration qui assure que tout produit développé répond aux exigences en matière de performance, de sécurité et de conformité par rapport aux différentes politiques de l'entreprise et le Centre de Services qui abrite l'Unité de Support Informatique (USI),l'Unité Logistique et Matérielle, l'Unité de Ressources Humaines et l'Unité de CL et dont le rôle est de mettre les employés dans les meilleures conditions et d'assurer un suivi des tâches de ces derniers grâce à un système de tickets.
Le Stage que nous avons réalisé s'est déroulé au niveau du Pôle Intégration.

CHAPITRE 2

LE SUJET

2.1 Terminologie

2.1.1 Sécurité informatique

La sécurité peut être définie comme étant une situation, un état dans laquelle quelqu'un ou quelque chose n'est exposé à aucun danger, à aucun risque d'agression, de détérioration ou encore par le long processus visant à atteindre cet état.
Lorsqu'on parle de sécurité dans le domaine des technologies de l'information et de la communication, on fait très souvent allusion à la sécurité de l'information. La sécurité de l'information ou encore sécurité informatique, en anglais Information Security abrégé Infosec consiste en la mise en place d'un ensemble de stratégies pour gérer les processus, les outils et les politiques nécessaires pour prévenir, détecter, documenter et contrer les menaces à l'information. La sécurité de l'information recouvre donc toutes les techniques permettant d'assurer la protection de l'information. La sécurité de l'information se fonde sur 3 principes fondamentaux :
- la confidentialité : c'est le fait d'assurer que l'information ne puisse être accessible qu'à ceux qui ont l'autorisation de la consulter. Cela sous-entend le fait de rendre inintelligible cette information aux personnes non autorisées ;
- l'intégrité : assurer que l'information n'est pas modifiable par un tiers non autorisé. Elle consiste à certifier que les données n'ont pas été détruites ou altérées tant de façon intentionnelle qu'accidentelle ;
- la disponibilité : assurer que l'information est accessible en temps voulu par ceux qui en ont l'autorisation. Ne pas pouvoir accéder à une information en temps voulu est semblable à la non-possession de celle-ci.

Comme principes supplémentaires, nous notons :
- l'authentification : elle consiste à assurer l'identité d'un tiers et permet de garantir qu'un tiers est bien celui qu'il prétend être ;
- la non-répudiation : le fait de ne pas pouvoir nier une action faite sur le système.

2.1.2 Cryptographie

La sécurité informatique est un domaine pluridisciplinaire. En effet, pour arriver à ses buts, elle a, tout au cours de son évolution, utilisé, entre autres, la cryptographie. La cryptographie peut être définie comme un art et une science permettant de concevoir des techniques pour garder

le secret des messages transmis. Voici les problèmes que doit résoudre la cryptographie :
- la confidentialité ;
- l'intégrité ;
- l'authentification.
On voit ainsi que la sécurité informatique et la cryptographie partagent des objectifs similaires. Et c'est pour cette raison que tout au long de l'histoire, elle a été utilisée dans le domaine de la sécurité informatique. De même, les évolutions dans le domaine de la sécurité informatique ont souvent été rendus possibles grâce aux avancées de la cryptographie. On distingue :
- la cryptographie classique qui décrit la période d'avant les ordinateurs. Elle traite des systèmes reposant sur les lettres et les caractères d'une langue naturelle. Dans cette famille, on retrouve le chiffrement par substitution qui consiste, à remplacer, sans en bouleverser l'ordre les symboles d'un texte clair par d'autres symboles et le chiffrement par transposition qui repose sur le bouleversement de l'ordre des symboles du message clair. Les techniques de chiffrement les plus connues dans cette famille sont le chiffrement de César et le chiffrement de Vigenère ;
- la cryptographie moderne qui utilise la puissance de calcul des ordinateurs pour affiner ces techniques de chiffrement. Dans cette famille, nous avons le chiffrement symétrique qui utilise une même clé pour le chiffrement et le déchiffrement ; DES en est la technique la plus connue et le chiffrement asymétrique qui utilise des clés différentes pour le chiffrement et le déchiffrement ; RSA est l'algorithme de chiffrement asymétrique le plus utilisé.

2.2 Contexte

Aux premiers jours de l'internet, le World Wide Web [1] consistait en de simples pages web, des pages d'information constituée de ressources statistiques. Le flot d'informations était à sens unique, du serveur au navigateur. L'authentification des utilisateurs n'était souvent pas nécessaire car les mêmes informations étaient affichées à tous les utilisateurs. Les risques de sécurité découlaient exclusivement de l'hébergement des sites web, c'est-à-dire au niveau des serveurs web. En cas d'attaque, il n'y avait que peu de risques car l'information au niveau des serveurs était déjà accessible au grand public. Les attaques consistaient donc le plus souvent à des démaquillages des sites web.
De nos jours, le World Wide Web est très différent de ce qu'il était à ses débuts. De nouveaux sites web plus poussés apparaissent : les applications Web. Ils ne se limitent plus à l'affichage de ressources statistiques. La majorité des sites web de nos jours, sont en réalité des applications web. Une application web est un site Web qui permet à ses utilisateurs de réaliser des tâches spécifiques. Le flux d'informations n'est plus à sens unique mais plutôt bidirectionnel entre le serveur et le client (navigateur, téléphone mobile, autre application).
Le contenu présenté aux utilisateurs est spécifique à chaque utilisateur en fonction de préférences préalablement enregistrées par ce dernier ou encore d'autres paramètres de l'application. Les applications web peuvent assurer pratiquement toutes sortes de fonctionnalités. Voici quelques types d'applications que l'on retrouve très souvent :
- Réseaux sociaux : Facebook, Twitter, Google plus entre autres ;

1. Système reliant des ressources hypertextes sur Internet grâce au protocole Http

- Vente en ligne : Amazon, Ebay ;
- Banque en ligne : Cbao, Citibank ;
- Mailing : Yahoo, Gmail

En plus des applications web disponibles publiquement, nous avons les applications web internes aux entreprises qui soutiennent les entreprises dans l'accomplissement de tâches spécifiques :
- applications de gestion de ressources humaines et de la paie ;
- applications de collaborations ;
- applications de messagerie interne ;
- applications sur mesure propres au fonctionnement de l'entreprise.

Cette évolution très rapide des applications Web s'explique par plusieurs facteurs :
- HTTP, le principal protocole de communication utilisé par le Web est assez simple. Il permet également au serveur de communiquer avec tous les clients sans avoir à maintenir une connexion ouverte à chaque utilisateur grâce au paradigme requête/réponse ;
- Chaque utilisateur Web a déjà un navigateur installé sur son ordinateur et appareil mobile. Les applications Web se déploient une seule fois au niveau du serveur évitant ainsi de distribuer et de gérer séparément chaque logiciel client, comme ce fut le cas pour les applications pré-web. La maintenance est simple et changements faits ne nécessitent qu'un seul redéploiement au niveau du serveur et ont effet immédiat sur tous les clients ;
- Les navigateurs sont devenus aujourd'hui hautement sophistiquées permettant ainsi une très bonne expérience utilisateur ;
- Les technologies de base et les langages utilisés pour développer des applications web sont relativement simples. Un large éventail de plates-formes et d'outils de développement sont disponible pour faciliter le développement d'applications puissantes.

Toutes ces raisons ont fait que les applications Web sont devenus des outils incontournables de nos quotidiens aussi bien pour des raisons personnelles que professionnelles.

Parallèlement, avec le développement fulgurant de l'industrie mobile au début des années 2000, les téléphones mobiles ne sont plus de vulgaires appareils dont l'utilité est limitée à la communication. Désormais, ils proposent des fonctionnalités plus poussées grâce à des systèmes d'exploitation embarqués ; nous avons notamment Android de Google et Ios de Apple. Ces systèmes d'exploitation mobiles font des appareils mobiles des mini ordinateurs offrant des fonctionnalités similaires à celles des ordinateurs. A partir de ce moment, ce fut l'explosion des applications mobiles. Une application mobile ou encore de façon plus simple une App, est un type de logiciel conçu pour fonctionner sur un appareil mobile tel un smartphone, une tablette ou encore un assistant personnel.

Il existe principalement trois types d'applications mobiles :
- Native : applications mobiles spécifiques systèmes d'exploitation mobile Ios, Android ou Windows Phone ;
- Hybride : applications mobiles disponibles à la fois pour toutes les plateformes ;
- Web : Version responsive [2] utilisant des navigateurs web embarqués.

Les applications mobiles permettent de mettre à la disposition des utilisateurs des services

2. Le Responsive Web Design (RWD), ou conception web adaptative, regroupe une série de techniques de conception graphique et de développement permettant de créer un site qui pourra s'auto-adapter en fonction de la taille d'un écran.

similaires à ceux accédés à travers un ordinateur personnel. Ainsi,leurs champs d'application sont infinis et similaires à ceux des applications Web et même parfois plus poussés :
- Paiement de transactions ;
- Consultation médicale ;
- Applications de sauvegarde de mots de passe.

En plus, les spécificités techniques d'une application mobile lui confèrent de nombreux avantages par rapport aux applications Web :
- l'utilisation est plus simple et plus intuitive ;
- l'exécution est plus rapide : les éléments d'interface n'ont pas besoin d'être téléchargés depuis un serveur ;
- l'accès aux données de l'utilisateur est plus facile ;
- certaines applications mobiles peuvent même fonctionner hors ligne.

Du fait des nombreux avantages des applications mobiles et surtout de leur simple accessibilité, les applications sont devenues très prisées et sont utilisées quotidiennement par des milliards d'utilisateur. Il suffit de voir le nombre d'utilisateurs d'une application telle que WhatsApp qui, en 2017 [W1], était utilisée par plus d'un milliard de personnes quotidiennement, pour s'en convaincre. Aujourd'hui, il existe plusieurs plateformes proposant des applications mobiles en téléchargement : on peut citer à titre d'exemple le Play Store de Google et l'Apple App Store de Apple. Les entreprises se sont attaquées massivement à ce marché et il existe aujourd'hui des milliards d'application mobiles. Depuis 2017, plus de la moitié de la population mondiale utilise désormais un smartphone. [W1 : https ://www.lauyan.com/fr/responsive-webdesign-faq.html] Ces applications mobiles utilisent soit des navigateurs embarqués, soit des APIS exposées par une application web. Les fonctions et les données manipulées par les applications mobiles sont généralement les mêmes que celles manipulées par les applications Web. De même, presque toutes les applications Web sont disponibles en version mobile.

Les applications Web et mobiles manipulent aujourd'hui des données hautement sensibles et fournissent des informations très confidentielles. Elles prennent en charge des fonctionnalités très délicates telles que les transactions financières ; il y a de cela quelques années, lorsqu'on voulait faire une transaction financière, il fallait aller à la banque et un agent le faisait pour vous alors qu'aujourd'hui, avec ces applications web, il est possible de faire ces transactions soit même en ligne en fournissant certaines informations. Ceci étant, si un attaquant arrivait à compromettre ce genre d'applications par exemple, il lui serait facile de faire des transactions frauduleuses et vider votre compte bancaire. Qu'un individu malintentionné arrive à compromettre ce genre d'applications représenteraient de gros risques à la fois pour les propriétaires de ces applications dont le business repose essentiellement sur ces dernières mais aussi pour les utilisateurs qui auront fourni des informations très sensibles (mots de passe, numéros de carte de crédit entre autres).

La Sécurité de ces applications est devenue très critique. L'augmentation rapide de la connectivité, combinée à l'augmentation spectaculaire de la valeur des données manipulées par ces applications ainsi que l'utilisation croissante de nouveaux protocoles et technologies ont abouti à des applications représentant un risque important à la fois pour les organisations qui les mettent en place et pour les utilisateurs de ces applications.

Le principal problème de sécurité rencontré par la majorité des applications Web et Mobile dé-

coulent du fait qu'elles doivent accepter et traiter des données, lesquelles donnée pouvant être non fiables oi malveillantes. Cependant, plusieurs autres facteurs contribuent à cet état de fait et expliquent pourquoi tant d'applications Web et mobiles sont vulnérables.

• Bien que la prise de conscience quant aux problèmes de sécurité des applications Web ait augmenté ces dernières années grâce aux différentes initiatives dans ce sens, elle reste moins développée que dans des domaines plus anciens tels que les réseaux et les systèmes d'exploitation. De fausses idées existent encore à propos de la plupart des concepts de base de la sécurité des applications Web. De nos jours, le travail d'un développeur Web consiste de plus en plus à intégrer, réutiliser des dizaines, voire des centaines, de composants tiers, conçus pour abstraire la complexité inhérente à ces différents composants et à réduire les temps de développement. Cependant, il est courant de voir des développeurs Web expérimentés faire des hypothèses sur la sécurité de leurs applications basées sur les frameworks qu'ils utilisent et à qui l'explication de simples failles de sécurité vient comme une révélation.

• Pour réduire les temps de développement des applications web, de plus en plus de composants tiers sont réutilisés. Cependant, ces composants ont parfois des failles de sécurité qui ouvrent des brèches aux attaquants. Et très souvent, avant que ces failles de sécurité ne soient découvertes par les éditeurs et ne soient corrigées par des patchs, elles sont déjà exploitées.

• De nos jours, de plus en plus d'outils sont créés afin de permettre à des non professionnels de l'informatique de pouvoir créer de puissantes applications Web en quelques clics. Ces outils fournissent du code prêt à l'emploi et pouvant gérer de nombreux cas de figures : blogs, vente en ligne, entre autres. Ils fournissent de nombreuses fonctionnalités prêtes à l'emploi incluant même des fonctionnalités de sécurité telles que l'authentification, la gestion des utilisateurs entre autres. Ces outils permettent la création d'applications sans nécessiter une compréhension technique de la façon dont les applications fonctionnent ou des risques potentiels qu'elles peuvent contenir et comment ils doivent être pris en compte. Et il y a une énorme différence entre produire un code fonctionnel et un code sécurisé. Or ce genre d'outils est très utilisé et parfois même par des entreprises de renom. Il n'est pas rare que des failles de sécurité soient découvertes dans ces outils. Ainsi, quand une vulnérabilité est découverte, il affecte de nombreuses applications à la fois.

• Les menaces évoluent très rapidement. De même, elles apparaissent plus rapidement qu'elles ne sont résolues. Il est courant que les défenses acceptées pour une certaine menace d'être dépassées par de nouvelles formes d'attaques. Une équipe de développement qui commence un projet avec une connaissance avancée de plusieurs menaces et de leurs contre-mesures peut être complètement dépassée avant la fin du projet du fait de l'évolution rapide des techniques d'attaques.

• Le développement des applications Web est très souvent soumis à des contraintes de temps et de ressources. Pour la plupart des organisations, il est impossible d'engager une équipe d'experts sécurité dédiée à la gestion des besoins de sécurité. De même, dans le cycle de développement logiciel, les considérations de sécurité ne sont pas très souvent prises en compte. En effet, la plupart des méthodologies utilisées de nos jours sont des méthodes agiles. Elles sont orientées rapidité de développement, c'est-à-dire produire plus de fonctionnalités très rapidement. Et dans ces méthodologies agiles, les exigences de sécurité tombent dans le champ des exigences non fonctionnelles. Aussi, les fonctions de sécurité n'ont pas la même visibilité que les fonctions business de l'application. Les équipes de développement dans les méthodologies agiles sont amenées à

produire des fonctionnalités qui sont visibles pour le client.
Tous ces facteurs contribuent à rendre les applications Web et Mobile encore plus vulnérables.

2.3 Problématique et Objectifs

Beaucoup d'entreprises attendent de leurs développeurs des applications avec un certain degré de sécurité sans faire grand-chose pour permettre à ces développeurs d'en construire. C'est la raison pour laquelle HubSo s'est proposée de faire une étude sur la mise en place d'applications Web et Mobiles conformes par rapport à Owasp, étude dont la finalité est de fournir à ses développeurs les éléments dont ils ont besoin pour produire du code sécurisé.
Le premier objectif est de mettre à la disposition des développeurs un ensemble de contrôles de sécurité disponibles dans leur environnement. Chaque organisation par défaut dispose d'un certain nombre de contrôles de sécurité dans son infrastructure, tels que des bibliothèques de chiffrement, des serveurs de logs, des serveurs d'authentification, etc. Les développeurs ont besoin d'un accès facile à ces contrôles et cela permet à la longue d'avoir une manière standard de prendre en compte la sécurité durant le cycle de développement logiciel : il s'agira d'une bibliothèque disponible pour les projets Web et Mobile.
Une fois ces contrôles de sécurité disponibles, il faut élaborer un ensemble de directives de codage sécurisé par rapport à Owasp. C'est un ensemble de règles que les développeurs doivent suivre lors du développement d'applications. Ces directives doivent être spécifiques à l'entreprise et contenir de nombreux extraits de code et des exemples de codage sécurisé. En outre, la directive doit être adaptée à l'environnement, aux règles et aux technologies utilisés car les stratégies théoriques (polices de sécurité, recommandation. . .) ne sont souvent pas très parlant aux développeurs : ce sera un guide de bonnes pratiques Owasp pour développeurs. La dernière chose à faire pour aider les développeurs est de leur donner un peu de formation en codage sécurisé. Cette formation devrait couvrir quand et comment utiliser tous les principaux contrôles de sécurité, en donnant des exemples des failles de sécurité courantes associées à chaque contrôle et comment suivre les directives de codage sécurisé afin d'utiliser les contrôles pour éviter ces vulnérabilités.
Les autres objectifs sont les suivants :
- une architecture type OWASP (Client Android, Serveur JEE) ; - un projet type Web JEE conforme OWASP avec à minima les fonctionnalités suivantes :
- Authentification et gestion de sessions - Gestion des utilisateurs et mots de passe - Gestion des profils et génération des composants graphiques - un projet type Android conforme OWASP avec à minima les fonctionnalités suivantes : - authentification et gestion de sessions (Offline et Online)
- gestion des utilisateurs et mots de passe - gestion des profils et génération des composants graphiques - Intégration BO Total et PDA Total

2.4 Périmètre

La sécurité des applications web implique la sécurité au niveau de ces infrastructures qui communiquent en réseau (Sécurité réseau) mais aussi la sécurité lors de l'utilisation des technologies web et mobiles utilisées (Sécurité applicative). Nous nous intéressons, dans le cadre de ce stage, à la sécurité applicative.

Deuxième partie

Etat de l’art

Table des matières

CHAPITRE 3

HISTORIQUE

3.1 Genèse

Le domaine de la sécurité de l'information est très ancien. Déjà, dès l'antiquité, des techniques de chiffrement de l'information étaient utilisées. Vers 1900 av JC, le scribe de Khnumhotep II retraçait la vie de son maître dans sa tombe en utilisant un certain nombre de symboles inhabituels pour masquer le sens des inscriptions avec les hiéroglyphes qu'il dessinait. Vers 500 av. J.-C., les Spartiates ont développé un dispositif appelé Scytale, qui a été utilisé pour envoyer et recevoir des messages secrets. Plus récemment dans l'histoire, l'empereur romain Jules César utilisa la technique de chiffrement qui porte son nom (Chiffrement de César) afin de crypter ses messages personnels. Ces Expériences, Bien Que Ne Couvrant Que Le Principe De La Confidentialité, Sont Les Ancêtres De La Sécurité De L'information.
A cette époque, assurer la sécurité de l'information se résumait en un problème de cryptage de données. On utilisait alors la cryptographie classique avec le chiffrement par substitution[1] d'abord puis plus tard le chiffrement par transposition[2].

3.2 Seconde Guerre mondiale et guerre froide : grand tournant de l'histoire de la sécurité informatique

Avec le temps, les techniques permettant d'assurer la sécurité de l'information deviennent de plus en plus pointues. La seconde guerre mondiale et la guerre froide ont marqué un tournant dans l'histoire de nombreuses technologies, y compris celles qui ont façonné l'industrie de la sécurité de l'information.
En effet, durant cette période, de nouveaux moyens de communication apparaissent : la radio et le cinéma étaient les principaux vecteurs de l'information. Sur le champ de bataille, les différentes unités devaient coordonner leurs actions et pour ce faire des informations étaient échangées entre elles. Toutes ces communications étaient diffusées par radio et pouvaient être interceptées par l'ennemi. Il était d'une importance cruciale de rendre l'information inintelligible à l'ennemi puisqu'il s'agissait de communiquer sur les stratégies d'actions à mener. Pour protéger ces communications militaires, des systèmes très sophistiquées furent mises en place. Il s'agissait surtout de machines permettant de chiffrer l'information. Enigma était la machine de chiffrement la plus avancée de l'époque : elle sécurisait les communications des flottes et des troupes nazis en

leur permettant de chiffrer leurs messages par un chiffrement par substitution. Elle utilisait des algorithmes de chiffrement par substitution très poussés à l'époque. Elle avait la réputation d'être inviolable. Cependant, des experts en chiffrement polonais et britanniques ont réussi à trouver le moyen de casser Enigma en créant une machine connue sous le nom de « Bombe cryptographique » permettant de déchiffrer ses messages, donnant ainsi à la coalition antihitlérienne un avantage significatif ou « l'avantage définitif » selon Churchill et Eisenhower lors de la seconde guerre mondiale et soulignant du même pied l'importance capitale qu'a revêtu la sécurité de l'information lors de cette époque.

Puis, la seconde guerre mondiale laissa place à la guerre froide, une guerre d'opinion opposant deux blocs : d'un côté les états unis démocrates et de l'autre les russes, communistes. Ce fut la naissance d'une course à l'armement et à l'avancée technologique pour dominer le camp adverse. C'est durant cette période que les premiers ordinateurs sont créés. A cette époque, ils sont beaucoup plus utilisés comme outils de calcul pour des applications scientifiques et n'étaient pas très répandus. C'était des systèmes mono-utilisateurs logés dans de grande salle et il n'y avait pas communication entre ces différentes machines. La sécurité n'était pas une priorité et n'impliquait que le fait de sécuriser les salles où étaient installées ces machines. Du fait de leur puissance et de leurs nombreux avantages, de plus en plus d'ordinateurs et de systèmes d'exploitation furent créés. De même, la cryptographie entre dans une nouvelle ère : des techniques de chiffrement plus avancées sont mises en place grâce à la puissance de calcul des ordinateurs. C'est la naissance de la cryptographie moderne [1]. Avec la prolifération des terminaux distants sur les ordinateurs commerciaux, le contrôle physique de l'accès à la salle informatique n'était plus suffisant. En réponse à cela, des systèmes de contrôle d'accès logique ont été développés/footnoteUn système de contrôle d'accès maintient une table en ligne des utilisateurs autorisés. Un enregistrement d'utilisateur type stocke le nom de l'utilisateur, son numéro de téléphone, son numéro d'employé et des informations sur les données auxquelles l'utilisateur était autorisé à accéder et les programmes qu'il était autorisé à exécuter. Un utilisateur peut être autorisé à afficher, ajouter, modifier et supprimer des enregistrements de données dans différentes combinaisons pour différents programmes. Dans le même temps, les gestionnaires de système ont reconnu l'importance de pouvoir se remettre de catastrophes pouvant détruire le matériel et les données. Les centres de données ont commencé à faire régulièrement des copies sur bande de fichiers pour le stockage hors site. Les gestionnaires de centre de données ont également commencé à élaborer et à mettre en œuvre des plans de reprise après sinistre. Ce sont les premières politiques de sécurité entreprises. Cependant, même avec un tel système en place, de nouvelles vulnérabilités ont été reconnues au cours des années suivantes. Il fallait des systèmes plus fiables. Multics, un système d'exploitation multi utilisateurs fut créé en 1964. Ce fut la première fois que la problématique de la sécurité de l'information fut prise en compte en amont. En effet, dès la conception de Multics, les décisions prises (langages de programmation, architecture du noyau, etc.) prenaient en compte les exigences de sécurité. Les fonctions de sécurité de Multics comprenaient également le chiffrement des mots de passe, des audits de connexion et des procédures de maintenance logicielle. Les mots de passe dans Multics n'étaient jamais stockés en texte clair. Lorsqu'un utilisateur entrait son mot de passe, ce mot de passe était chiffré, puis comparé au mot de passe stocké sur le système. Cela permit de garder les mots de passes des utilisateurs en cas de dump système. De même, un journal d'audit de connexion enregistrait l'heure, la date et le terminal de chaque tentative de connexion,

et notifiait à l'utilisateur le nombre de tentatives de mot de passe incorrectes sur son compte depuis la dernière connexion réussie. Enfin, des procédures de maintenance logicielle, telles que la vérification du nouveau logiciel permettaient de maintenir le système sûr et épargné des régressions de sécurité. Au début des années 1970, alors que l'armée américaine était à la recherche de systèmes informatiques multi utilisateurs capables de protéger les informations classifiées, Multics lui fut recommandé. A cette époque, pour éprouver la sécurité des systèmes en place, il était très courant de faire appel à des Tiger Team. Il s'agissait d'experts rassemblés pour gérer des situations spéciales, régler des problèmes spécifiques le plus rapidement possible. Au début, leur travail consistait surtout en des revues manuelles de code pour détecter la source des bugs. Un peu plus tard, ils ont commencé à utiliser le « pentest » ou test d'intrusion/footnoteC'est une méthode permettant d'évaluer la sécurité d'un système informatique à travers des tentatives d'intrusion à la manière d'un attaquant. Dès 1969, l'ARPA (Advanced Research Project Agency), une agence dédiée aux projets de recherche avancée renommée plus tard en DARPA (Defense Advanced Research Project Agency) arriva à interconnecter les ordinateurs de quatre universités en un réseau afin de leur permettre de partager leurs résultats de recherche : ce réseau fut nommé l'Arpanet. Dans Arpanet, les utilisateurs se connaissaient plus ou moins et étaient pour la majorité des académiciens : la sécurité n'était pas un problème majeur dans ce « réseau d'amis ». C'est ce simple réseau de quatre nœuds sans aucune préoccupation de sécurité qui conduisit plus tard à la naissance d'Internet et du World Wide Web. Vers la fin des années 1970, l'analyse de codes source, qui était faite manuellement, vit une révolution. Lint, le premier outil d'analyse de codes source automatisée apparut. Initialement, il était destiné aux codes sources écrits en langage C. Lint était pratique pour trouver des bugs potentiels, mais était très lent et n'était pas équipé de la vue complète du programme. Il ne pouvait analyser qu'un seul fichier à la fois. Lint a ouvert la voie à la première génération d'outils destinés à la sécurité des applications informatiques qui, bien qu'ils aient été utiles pour trouver des bugs spécifiques, étaient assez maladroits et ne faisaient pas mieux que l'analyse manuelle. La décennie 1970 vit également l'apparition des premiers micro-ordinateurs. Au début, parce qu'ils étaient entièrement autonomes et généralement sous le contrôle d'un seul individu, il y avait peu de problèmes de sécurité. Très rapidement ils passent d'un passe-temps pour les passionnés d'informatique en un sérieux outil de travail. A partir de ce moment, des logiciels commencent à être créés pour les ordinateurs. L'on sait que pour cela, il fallait écrire du code source parfois enclin à des bugs et à des vulnérabilités de sécurité.

Les années 1980 marquèrent de réelles avancées. IBM lança le premier ordinateur personnel et bientôt des millions d'ordinateurs personnels pour des usages commercial, industriel et même gouvernemental furent installés. Désormais, les ordinateurs personnels devinrent incontournables à des milliers d'utilisateurs qui y voyaient un outil de travail. Internet qui était initialement réservé au gouvernement américain, à ses partenaires et à quelques privilégiés commence à avoir de nouveaux nœuds et par conséquent plus d'utilisateurs. A partir des années 1990, Internet devient un réseau mondial à l'aide du World Wide Web qui vit le jour de même que les premiers navigateurs. Internet offre plusieurs avantages importants : le coût est relativement faible, les connexions sont disponibles localement dans la plupart des pays industrialisés et, en adoptant le protocole Internet TCP/IP, tout ordinateur devient instantanément compatible avec tous les autres utilisateurs d'Internet. Internet, à ses débuts reposaient exclusivement sur le protocole http[1],

qui reposait à son tour sur le protocole TCP/IP[1]. Mais, il ne garantissait pas la confidentialité et l'intégrité des données transmises. Cependant il n'y avait pas encore d'autres alternatives.

3.3 Vers un usage massif d'Internet

Les premières pages Web ne tardent pas à voir le jour aidées en cela par la création du langage Html. En outre, les ordinateurs deviennent de plus en plus dépendants d'Internet et par la même voie deviennent de plus en plus vulnérables aux attaques à travers ce réseau.
Avec la création des premiers navigateurs, le potentiel inouï du Web attire les investisseurs qui y voient des applications commerciales. 1995 a été une année charnière pour le World Wide Web en général et pour la sécurité en particulier. En effet, Netscape [1] a lancé un navigateur web, le Netscape Navigator qui révolutionna la navigation sur le Web. Très rapidement, Netscape réalisa que le Web avait besoin d'être plus dynamique d'où la création de JavaScript adopté comme standard en 1997 par l'Ecma International [1].
Au fur et à mesure qu'Internet se développait, des sites web plus évolués apparaissent : les applications Web.De plus en plus de sociétés commerciales se mirent à proposer des achats en ligne pour les particuliers. Parmi celles-ci, EBay et Amazon. L'offre se mit à croître régulièrement, mais le chiffre d'affaires dégagé par le commerce électronique restait modeste tant que les clients n'avaient pas une confiance suffisante dans le réseau internet. Une des façons de sécuriser ce paiement fut d'utiliser des protocoles plus sûrs que HTTP qui a rapidement montré des failles de sécurité.
Jusqu'à maintenant, http était le seul protocole utilisé sur le Web. Cependant, avec les nouvelles avancées que ce dernier a connues, les enjeux de la sécurité y sont devenus plus importants. Avec le protocole http, les données étaient transmises en clair, permettant à un individu malintentionné de les récupérer et de les modifier ou de les utiliser à des fins néfastes. Ainsi, en fournissant son nouveau navigateur, Netscape a conçu le protocole SSL [Annexe].
Avec le protocole SSL, la sécurité a été sensiblement améliorée. Bien que, comme tout système de chiffrement, le SSL/TLS ne pourra jamais être totalement infaillible, le grand nombre de banques et de sites de commerce électronique l'utilisant pour protéger les transactions de leurs clients peut être considéré comme un gage de sa résistance aux attaques malveillantes. Il faut noter cependant que SSL ne garantit que le transport sécurisé des messages.
SSL est un protocole indépendant qui peut être appliqué à plusieurs autres protocoles. Son utilisation la plus connue est son association avec le protocole HTTP connue comme le protocole HTTPS pour dire, chez certain "HTTP over SSL" et pour d'autres "HTTP Secure". Il a en outre d'autres applications telles que le SSH permettant la connexion à une machine distante et le FTPS permettant le transfert de fichiers.

CHAPITRE 4

CONTEXTE

Compte tenu de leur rôle essentiel dans nos sociétés et nos économies modernes, les ordinateurs, les téléphones mobiles et l'internet doivent fonctionner ensemble correctement tout en fournissant un cadre qui protègent tout un chacun.
Il faut donc adopter des mesures drastiques afin d'assurer la sécurité lors de nos interactions avec ces différents outils qui font partie aujourd'hui de notre quotidien. Ces mesures sont prises sur deux aspects :
- l'aspect juridique : de nouvelles lois sont adoptées ;
- l'aspect technique : des services de protection des données sont créés aux échelles nationale, sous régionale et internationale.

4.1 Contexte juridique

Pays	Année
Seychelles	1988
Cap-Vert	2001
Zimbabwe	2002
Burkina Faso ; Tunisie ; Iles Maurice	2004
Sénégal	2008
Bénin ; Maroc	2009
Ghana	2010
Gabon ; Angola	2011
Mali ; Côte d'Ivoire ; Afrique du Sud ; Lesotho	2013
Madagascar ; Comores	2014
Tchad	2015
Guinée Equatoriale	2016
Niger	2017

TABLE 4.1 – Années d'adoption de lois sur les données personnelles dans différents pays en Afrique

Dans le cadre juridique, on parle le plus souvent de données à caractère personnel ou données personnelles. La notion de données à caractère personnel est définie comme étant toute information relative à une personne physique identifiée, génétique, psychique ou identifiable directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs

éléments propres à son identité physique, physiologique, génétique, psychique, culturelle, sociale ou économique [1]. Les premières législations sur la protection des données personnelles [1] ont été adoptées en Allemagne (1971), en Suède (1973), en France (1978), au Luxembourg (1979) et au Canada (1979).

En Afrique, la protection des données à caractère personnel est promue par plusieurs organismes communautaires même si les lois sur la protection des données sont relativement récentes. Le tableau 4.1 décrit l'ordre d'adoption des lois par différents pays.

En Afrique de l'Ouest, la CEDEAO et l'UEMOA sont intervenus en tant qu'acteur régional dans la réglementation des données personnelles en adoptant des mesures juridiques tout comme l'Union Africaine au niveau continental.

Au Sénégal, nous avons la loi n° 2008-11 du 25 Janvier 2008 portant loi d'orientation relative à la société de l'information qui définit un cadre général pour adapter le droit sénégalais aux besoins de la société de l'information.

Nous avons aussi la loi n° 2008-11 du 25 Janvier 2008 portant sur la cybercriminalité .La cybercriminalité ou criminalité informatique concerne toute infraction qui implique l'utilisation des technologies de l'information et de la communication.

Il y a aussi la loi sur les transactions électroniques qui vise, de façon globale, à favoriser le développement du commerce par les Technologies de l'Information et de la Communication (TIC) en posant des règles précises [1].

Il y a surtout la loi n° 2008-12 du 25 Janvier 2008 sur la protection des données à caractère personnel qui est le principal corpus protecteur des dites données.

Ce cadre juridique définit des exigences de sécurité que doivent respecter les responsables des traitements des données à caractère personnel. Elles imposent à ces derniers des obligations de confidentialité, de sécurité, de conservation et de pérennité des données. En effet, tout responsable de traitement de données personnelles se doit de mettre en œuvre les mesures techniques et organisationnelles adéquates pour protéger les données collectées contre la destruction accidentelle ou illicite, la perte, l'altération, la diffusion ou l'accès non autorisé notamment lorsque le traitement comporte des transmissions des données dans un réseau, ce qui est presque toujours le cas, ainsi que contre toute autre forme de traitement illicite. Ces mesures doivent assurer un niveau de sécurité approprié au regard des risques présentés par le traitement et la nature des données manipulées, empêchant le tiers de procéder à leur modification, à leur altération ou à leur consultation sans autorisation.

Cette obligation se traduit donc par la nécessité de mettre en œuvre des mesures de sécurité physique (verrous des salles serveur, coffres forts, etc.) et des mesures de sécurité logique (contrôles d'accès, cryptage des données, etc.).

Au Sénégal, le fait de procéder à des traitements automatisés de données personnelles sans prendre toutes les précautions utiles pour préserver leur sécurité est passible d'une peine d'emprisonnement de 1 à 7 ans et d'une amende allant de 500 000 à 10 000 000 de francs CFA. Pour assurer le respect des règles juridiques quant à la protection des données personnelles, il est institué par les différentes lois, un organisme responsable. Au Sénégal, c'est la CDP (Commission des Données Personnelles) qui joue ce rôle.

4.2 Contexte technique

De partout dans le monde, des CERT sont mis en place pour prendre en compte les incidents susceptibles de se produire sur Internet. Un CERT est un Centre d'alerte et de réaction aux attaques informatiques ciblant les entreprises ou administrations mais dont les informations sont généralement accessibles à tous. Le premier CERT (CERT-CC) a été créé aux Etats-Unis à l'Université Carnegie-Mellon en réponse à l'attaque du ver Morris [1].
Le but des CERT est de répondre aux incidents de sécurité informatique, de coordonner la communication entre experts lors de ces incidents de sécurité, de signaler les vulnérabilités et promouvoir des pratiques de sécurité efficaces dans toute la communauté internet afin de prévenir les incidents futurs.
Dans presque tous les pays développés, nous avons au moins un CERT national :
- CERT-FR en France ;
- CERTBund en Allemagne ;
- JPCERT au Japon ;
- UKCERT au Royaume-Uni.
Cette liste est loin d'être exhaustive. En Afrique, des efforts ont été récemment faits dans ce domaine même s'il faudrait que plus de pays africains mettent en place des CERT. Nous avons notamment : - le CSIRT du Kenya ;
- le CERT des îles Maurice ;
- l'ECS-CSIRT de l'Afrique du Sud ;
- le TunCERT de la Tunisie ;
- le CI-CERT de la Cote d'Ivoire ;
- le CERT-GH du Ghana ;
- le DZ-CERT de l'Algérie ; - ou encore le maCERT du Maroc.
Nous avons aussi le Forum africain des équipes de réponse aux incidents informatiques (AfricaCERT) qui veut asseoir les bases d'une coopération dynamique entre les équipes nationales africaines de CERT pour lutter contre le phénomène de la cybercriminalité qui menace l'économie, l'image et la jeunesse africaines.
Au Sénégal, il urge de mettre en place un CERT Les CERT à travers le monde sont des entités indépendantes, bien qu'il puisse y avoir des activités coordonnées entre les groupes. Ces dernières années, de nombreux CERT ont vu le jour et font partie du Forum des équipes de réaction aux incidents de sécurité informatique (FIRST).
FIRST est une organisation de premier plan et un leader mondial reconnu dans la réponse aux incidents de sécurité informatique. L'appartenance à FIRST permet aux CERTs d'intervenir plus efficacement face aux incidents de sécurité en fournissant un accès aux meilleures pratiques de sécurité, à des outils de gestion de la sécurité et à une communication de confiance entre les équipes membres. Il s'agit d'une confédération internationale de CERTs de confiance qui gèrent de manière coopérative les incidents de sécurité informatique et favorisent les programmes de prévention des incidents. Ils travaillent tous pour un objectif commun de sécurité informatique. En outre, de nombreuses sociétés privées de d'édition de logiciels anti-virus ont des divisions qui jouent le rôle de CERT.
Il existe aussi en plus des CERTS, des autorités techniques nationales, sous-régionales et régio-

nales chargées de préserver la sécurité de l'information aux niveaux nationales, sous-régionales et régionales. L'enjeu de ces autorités nationales est de préserver la souveraineté et l'autonomie de décision et d'action dans le domaine informatique et protéger l'ensemble des infrastructures critiques.
En parallèle à ces initiatives étatiques, il existe des organisations indépendantes sans but lucratif qui œuvrent pour une meilleure sécurité de l'information. Parmi celles-ci, les plus connues sont Mitre, Sans Institute et Owasp.

CHAPITRE 5

OWASP

5.1 Présentation

OWASP (Open Web Application Security Project) est une communauté en ligne ouverte et libre travaillant sur la sécurité des applications Web. OWASP se propose de permettre aux organisations de concevoir, développer, acquérir, exploiter et maintenir des applications logicielles fiables.
OWASP est aujourd'hui reconnue dans le monde de la sécurité des systèmes d'information pour ses travaux et recommandations liées aux applications Web. Ces recommandations vont dans le sens de bonnes/mauvaises pratiques de développement, d'une base sérieuse en termes de statistiques, et d'un ensemble de ressources amenant à une base de réflexion sur la sécurité. Des outils sont aussi proposés pour effectuer des audits de sécurité. La Fondation OWASP, un organisme de bienfaisance à but non lucratif soutient les efforts de l'OWASP à travers le monde. Tous les outils, documents, forums et chapitres d'OWASP sont gratuits et ouverts à toute personne intéressée par l'amélioration de la sécurité des applications.
OWASP est libre de toute pression commerciale et n'est affilié à aucune entreprise de technologie. Cela lui permet de fournir des informations objectives, pratiques et effectives sur la sécurité des applications. Les professionnels de la sécurité peuvent intégrer les recommandations d'OWASP dans leurs travaux. Les fournisseurs de service sécurité peuvent baser leurs produits et services sur les standards OWASP. Les consommateurs peuvent utiliser les normes comme documents de référence pour tester les applications ou les services qu'ils utilisent.

5.2 Origines

OWASP a été créé par un certain Mark Curphey le 9 septembre 2001. Son but initial étatit de lancer un projet pour définir une méthodologie de test standard pour la sécurité des applications Web. Il continue de définir des recommandations de sécurité, des spécifications et des explications dans des domaines clés de la sécurité des applications Web. Sa philosophie est d'être à la fois libre et ouverte à tous. Elle a pour vocation de publier des recommandations de sécurisation Web et de proposer aux internautes, administrateurs et entreprises des méthodes et outils de référence permettant de contrôler le niveau de sécurisation de ses applications Web.

5.3 Contexte

De nos jours, le développement de produits informatiques est fermement axé sur la vitesse. La course du Time-To-Market est extrêmement compétitive. Pour innover, les entreprises développent à un rythme effréné, en établissant des méthodologies qui permettent de perfectionner leur logiciel tout en réduisant le temps de développement. La sécurité, cependant, est souvent une réflexion secondaire pour les développeurs et les clients poussent toujours à livrer plus rapidement. Cela ouvre la porte à des failles de sécurité, de plus en plus présentes dans les logiciels. Et le Web n'échappe pas à cet état de fait.
De même, il est souvent difficile de trouver des conseils impartiaux, objectifs et des informations pratiques aidant à la prise en compte de la sécurité dans le développement. Le marché concurrentiel de la technologie et des services a beaucoup à dire sur ce point, mais une grande partie les conseils et recommandations sont donnés pour vous orienter vers un outil ou un fournisseur de services particulier.
L'OWASP a été créé pour lutter contre ce problème, en offrant des conseils impartiaux et objectifs sur les meilleures pratiques et en encourageant la création de normes ouvertes.

5.4 Organismes concurrents

5.4.1 Mitre Corporation

Mitre Corporation est une organisation à but non lucratif travaillant dans l'intérêt public fondé en 1958. Elle gère les centres de recherche et de développement financés par l'état fédéral (FFRDCS) notamment celui du Département de la Défense chargé de la sécurité nationale aux Etats Unis. Les FFRDCS fournissent des services dans les domaines de l'acquisition et de l'analyse de systèmes notamment sur la cyber-sécurité et la mise en réseau mondiale. Ils s'engagent également dans la recherche et le développement de technologies telles que la biosécurité et l'informatique quantique.
Mitre Corporation entretient une Cyber académie avec des cours en ligne. Elle maintient aussi la liste des CVE avec le sponsoring du Département de la Sécurité Intérieure, la liste CCE, la liste CAPEC et la liste CWE. Mitre Corporation est un partenaire très proche du gouvernement fédéral des Etats-Unis.

5.4.2 Sans Institute

Sans Institute est une organisation privée à but lucratif qui offre des formations et des certifications en sécurité de l'information et en cyber sécurité à travers le monde fondée en 1989. Elle maintient le plus grand référentiel d'informations sur la sécurité dans le monde et est également le plus grand organisme de certification. Sans Institute fournit une vaste collection de documents de recherche sur la sécurité et supervise un système d'alerte d'attaques : Internet Storm Center. Son programme GIAC (Global Information Assurance Certification) fournit un moyen normalisé de garantir les connaissances et les compétences d'un professionnel de la sécurité. La majorité

des ressources de Sans Institute sont libres.

5.4.3 PCI Standard Council

Le PCI Standard Council est une organisation fondée en 2006 par American Express, Discover, JCB International, MasterCard et Visa Inc. Elle recommande, maintient et évolue des normes pour la sécurité des données des titulaires de cartes dans l'industrie des cartes de paiement à travers le monde. Les normes PCI Data Security aident à protéger la sécurité des données de carte de paiement bancaires. Ils définissent les exigences opérationnelles et techniques pour les organisations acceptant ou traitant des transactions de paiement, et pour les développeurs de logiciels et les fabricants d'applications et de dispositifs utilisés dans ces transactions.

5.4.4 Web Application Security Consortium

Le WASC (Web Application Security Consortium) est une organisation mondiale consacrée à l'établissement, au perfectionnement et à la promotion des normes de sécurité sur Internet. Le consortium, créé en janvier 2004, est composé de membres indépendants ainsi que de membres associés à des entreprises, des organismes gouvernementaux et des établissements universitaires. Le champ d'actions du WASC comprend la recherche et la publication d'informations sur les problèmes de sécurité des applications Web. L'organisation informe les particuliers et les entreprises sur ces problèmes et sur les mesures à prendre pour lutter contre des menaces spécifiques. Elle accompagne également les utilisateurs d'Internet et les organisations dévouées à la sécurité des applications Web. Le WASC est une organisation indépendante, bien que les membres puissent appartenir à des sociétés impliquées dans la recherche, le développement, la conception et la distribution de produits liés à la sécurité Web.

5.5 Projets phares

Tous les projets OWASP d'outils, de documents et de bibliothèques de codes sont organisés dans les catégories suivantes :
- Projets phares :
La désignation OWASP Flagship est attribuée aux projets qui ont démontré leur valeur stratégique pour l'OWASP et la sécurité des applications dans son ensemble.
- Projets de laboratoire :
Les projets OWASP Labs représentent des projets qui ont produit un livrable de valeur révisé par l'OWASP.
- Projets d'incubation :
Les projets OWASP Incubators représentent les projets qui sont encore en cours d'élaboration, avec des idées et dont le développement sont toujours en cours.
Les projets d'OWASP couvrent de nombreux aspects de la sécurité des applications. Elles concernent des documents, des outils, des environnements d'enseignement, des lignes directrices, des listes de vérification et d'autres documents pour aider les organisations à améliorer

leur capacité à produire du code sécurisé. Les projets sont l'une des principales méthodes par lesquelles OWASP s'efforce de réaliser sa mission, qui est de rendre la sécurité plus « visible ».
Les projets OWASP sont animés par des bénévoles et sont ouverts à tous. Cela signifie que n'importe qui peut diriger un projet, que n'importe qui peut contribuer à un projet et que n'importe qui peut utiliser un projet.
Voici une liste (non exhaustive) de projets populaires, ainsi qu'une description succincte de chacun d'eux :
- Owasp Testing Guide :
Il s'agit d'un document de plusieurs centaines de pages destiné à aider une personne à évaluer le niveau de sécurité d'une application Web.
- Owasp code Review Guide :
Il s'agit d'un document de plusieurs centaines de pages présentant une méthode de revue de code sécurité.
- Owasp Application Security Verification Standard :
Le projet ASVS vise à créer un ensemble de normes commerciales permettant d'effectuer une vérification de sécurité rigoureuse d'une application au niveau applicatif.
- Top 10 Owasp :
Il s'agit d'une liste des dix failles de sécurité les plus critiques pour les applications Web.

5.6 Top 10 Owasp

Il s'agit d'un document de sensibilisation à la sécurité des applications Web. La liste résulte d'un consensus entre les experts en sécurité leaders dans le domaine, concernant les dix failles de sécurité les plus critiques pour les applications Web. Le classement de ces failles de sécurité est basé sur leur fréquence, la gravité des vulnérabilités et l'ampleur de leur impact commercial potentiel. Le Top 10 de l'OWASP a pour but d'informer sur l'existence de ces risques et de fournir des guides simplifiés sur les bonnes pratiques pour s'en prémunir. L'OWASP maintient le Top 10 depuis 2003. Il a été créé à l'origine pour aider les organisations à établir une base, un point de départ leur permettant de déterminer si leur infrastructure de sécurité est prête à résister aux principales menaces. La liste continue de servir de liste de contrôle et de standard de développement d'applications Web pour plusieurs des plus grandes organisations du monde.
La liste est mise à jour tous les trois ou quatre ans pour suivre le rythme des changements qui se produisent sur le marché de la sécurité des applications Web. La version la plus récente a été publiée en 2017. Celle-ci, contrairement à celles précédentes, n'est plus uniquement basé sur la « vision » de l'OWASP sur le sujet. Le processus méthodologique a été entièrement revu. Il repose ainsi sur les remontées de 500 utilisateurs et de 40 sociétés spécialisées dans le domaine de la sécurité des applications. La liste des contributeurs et les données techniques issues de leurs remontées sont disponibles en Open Source sur Github. En outre, les statistiques concernent un panel de plus de 100 000 applications et services Web.
Cet ensemble de vulnérabilités d'application Web largement accepté est complété par un ensemble de directives de codage et de test sécurisés. Ces guides sont disponibles sur le site de l'OWASP et s'adressent aux développeurs, architectes, chefs de projets, managers ...

Evaluer la sécurité d'une application Web en se basant sur le Top 10 de l'OWASP est une pratiquement largement acceptée. De nombreuses organisations, notamment le Conseil des normes de sécurité PCI, l'Institut national des normes et technologies (NIST) et la Commission Fédérale du Commerce (FTC), citent régulièrement le Top 10 d'OWASP comme un guide de référence intégral pour atténuer les vulnérabilités des applications Web et respecter les principales normes de sécurité.

5.6.1 Démarches Concurrentes

Le Top 10 Owasp n'est pas la seule liste de vulnérabilités existante en matière de sécurité, il y a aussi, parmi les plus populaires :

- la liste CWE :

Le Common Weakness Enumeration (CWE), maintenu par Mitre Corporation, est une liste de vulnérabilités que l'on retrouve lors du développement d'applications. C'est un projet géré par MITRE. Pour chaque entrée, le CWE fournit une description de la vulnérabilité ainsi que les étapes pour y remédier. Cependant, contrairement aux Top 10 d'OWASP qui recense les 10 vulnérabilités les plus critiques, le CWE se veut être une démarche plus globale. Au moment ou nous écrivons ces lignes, 714 vulnérabilités sont recensées sur la liste CWE. Elle peut constituer une suite à la gestion de la sécurité pour une organisation après que celle-ci ait pris en compte le Top 10.

- le CWE/Sans Top 25 :

MITRE s'est associé à Sans Institute pour développer le CWE/Sans Top 25, une liste des 25 vulnérabilités logicielles les plus critiques. Bien que le Top 10 Owasp et le CWE / 25 e OWASP soient différents, ils partagent la plupart des mêmes vulnérabilités. En effet, là où le Top 10 adresse les failles en faisant une approche groupée, le CWE/Sans Top 25 utilise une approche plus granulaire. Par exemple, la correspondance Owasp Top 10 – CWE/Sans Top 25 peut être faite sur le point A1 : Injection comme suit :

Owasp Top 10	CWE/Sans Top 25
A1 :Injection	CWE-78 : Improper Neutralization of Special Elements Used in an OS Command CWE-89 : SQL Injection CWE-94 : Code Injection CWE-434 : Unrestricted Upload of File with Dangerous Type CWE-494 : Download of Code Without Integrity Check CWE-829 : Inclusion of Functionality from Untrusted Control Sphere

TABLE 5.1 – Correspondance Top 10 Owasp A1 - CWE/Sans Top 25

Cette correspondance peut être faite pour toutes les entrées du Top 10 d'Owasp.

Troisième partie

Analyse et Conception

Quatrième partie

Réalisation

Cinquième partie

Bilan et Perspectives

Conclusion