

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 Web JEE et d'une application Mobile Android conformes OWASP

Lieu de stage :

HubSo

Présenté et soutenu par :

Papa Latyr MBODJ

Maîtres de stage :

M. Ahmed Tidiane CISSE

M. OMouhamadou Mansour Sy SAMB

Enseignant encadrant :

Dr. 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

LISTE DES SYMBOLES

CERT	Computer Emergency Response Team
DARPA	Defense Advanced Research Projects Agency
DDOS	Distributed Denial of Service
DOS	Denial Of Service
HTTP	Hypertext Transfer Protocol
OWASP	Open Web Application Security Project
TCP/IP	Transmission Control Protocol/Internet Protocol

TABLE DES MATIÈRES

	Page
Liste des tableaux	xi
Table des figures	xii
Introduction	1
1 Présentation Générale	2
1.1 La Structure d'accueil	3
1.1.1 Présentation de HubSo	3
1.1.2 Domaines d'activités	3
1.1.3 Quelques Solutions de HubSo	3
1.1.4 Organisation	4
1.2 Le Sujet	5
1.2.1 Terminologie	5
1.2.1.1 Sécurité informatique	5
1.2.1.2 Cryptographie	5
1.2.2 Contexte	8
1.2.2.1 Evolution des applications Web et Mobiles	8
1.2.3 Problématique et Objectifs	10
1.2.4 Périmètre	12
2 Etat de l'art	13
2.1 Historique	14
2.1.1 Genèse	14
2.1.2 Seconde Guerre mondiale et guerre froide : grand tournant de l'histoire de la sécurité informatique	14
2.1.3 Vers un usage massif d'Internet	16
2.2 Contexte	18
2.2.1 Contexte juridique	18
2.2.2 Contexte technique	20
2.2.3 Contexte organisationnel	21
2.2.3.1 Mitre Corporation	21
2.2.3.2 Sans Institute	21
2.2.3.3 PCI Standard Council	22

2.2.3.4	Web Application Security Consortium	22
2.3	Owasp	22
2.3.1	Présentation	22
2.3.2	Origines	23
2.3.3	Contexte	23
2.3.4	Projets phares	23
2.3.5	Top 10 Owasp	24
2.3.5.1	Présentation	24
2.3.5.2	Démarches Concurrentes	25
3	Méthodologie de développement	27
3.1	Qu'est ce qu'une méthodologie de développement ?	28
3.2	Intérêt d'une méthodologie	28
3.3	Catégories de méthodologies de développement	28
3.4	Choix d'une méthodologie de développement	29
3.5	Intérêt d'une modélisation	30
3.6	Présentation d'UML	30
3.7	Diagrammes UML	31
4	Analyse et Conception	33
4.1	Spécifications	33
4.1.1	Spécifications fonctionnelles	33
4.1.1.1	Les Acteurs	33
4.1.1.2	Les fonctionnalités générales	33
4.1.2	Spécifications non fonctionnelles	36
4.2	Analyse	36
4.2.1	Package Gestion des injections	37
4.2.1.1	Diagramme de cas d'utilisation	37
4.2.2	Package Gestion des violations de gestion d'authentification	38
4.2.2.1	Diagramme de cas d'utilisation	38
4.2.3	Package Gestion des expositions de données sensibles	39
4.2.3.1	Diagramme de cas d'utilisation	39
4.2.4	Package Gestion des attaques sur les entités XML externes	39
4.2.4.1	Diagramme de cas d'utilisation	39
4.2.5	Package Gestion des violations de contrôle d'accès	40
4.2.5.1	Diagramme de cas d'utilisation	40
4.2.6	Package Gestion des mauvaises configurations de sécurité	41
4.2.6.1	Diagramme de cas d'utilisation	41
4.2.7	Package Gestion des XSS	41
4.2.7.1	Diagramme de cas d'utilisation	41
4.2.8	Package Gestion des désérialisations non sécurisées	42
4.2.8.1	Diagramme de cas d'utilisation	42
4.2.9	Package Gestion des utilisations de composants vulnérables	43

4.2.9.1	Diagramme de cas d'utilisation	43
4.2.10	Package Gestion de la journalisation et de la surveillance insuffisantes . .	43
4.2.10.1	Diagramme de cas d'utilisation	43
4.2.11	Système global	44
4.2.12	Sous-système "Utilisateurs"	47
4.2.12.1	Diagramme de cas d'utilisation	47
4.2.12.2	Cas d'utilisation "Authentification utilisateur"	47
4.2.12.3	Cas d'utilisation "Déconnexion utilisateur"	51
4.2.12.4	Cas d'utilisation "Vérification force mot de passe"	51
4.2.12.5	États d'un utilisateur	54
4.2.13	Sous-système "Cryptographie"	54
4.2.13.1	Diagramme de cas d'utilisation	54
4.2.14	Sous-système "Encodage"	55
4.2.14.1	Diagramme de cas d'utilisation	55
4.2.15	Sous-système "Validation"	55
4.2.15.1	Diagramme de cas d'utilisation	55
4.2.15.2	Cas d'utilisation "Valider donnée"	56
4.2.16	Sous-système "HTTP"	57
4.2.16.1	Diagramme de cas d'utilisation	57
4.2.16.2	Cas d'utilisation "Ajouter cookie"	57
4.2.17	Sous-système "Interpréteurs"	58
4.2.17.1	Diagramme de cas d'utilisation	58
4.2.18	Sous-système "Logging"	58
4.2.18.1	Diagramme de cas d'utilisation	58
4.2.19	Sous-système "Gestion des composants"	59
4.2.19.1	Diagramme de cas d'utilisation	59
4.2.20	Diagramme de classes	59
4.3	Conception	60
4.3.1	Architecture Technique	60
I	Réalisation	61
II	Bilan et Perspectives	63
4.4	Le Protocole SSL	70
	Bibliographie	72

LISTE DES TABLEAUX

TABLE	Page
2.1 Années d'adoption de lois sur les données personnelles dans différents pays en Afrique	19
2.2 Correspondance Top 10 Owasp A1 - CWE/Sans Top 25	26

TABLE DES FIGURES

FIGURE	Page
1.1 Organigramme de HubSo	4
3.1 Schéma d'ensemble des diagrammes UML	32
4.1 Diagramme de packages du système	37
4.2 Diagramme de cas d'utilisation du package "Gestion des injections"	38
4.3 Diagramme de cas d'utilisation du package "Gestion des violations de gestion d'authentification"	38
4.4 Diagramme de cas d'utilisation du package "Gestion des expositions de données sensibles"	39
4.5 Diagramme de cas d'utilisation du package "Gestion des attaques sur les entités XML externes"	40
4.6 Diagramme de cas d'utilisation du package "Gestion des violations de contrôle d'accès"	40
4.7 Diagramme de cas d'utilisation du package "Gestion des mauvaises configurations de sécurité"	41
4.8 Diagramme de cas d'utilisation du package "Gestion des XSS"	42
4.9 Diagramme de cas d'utilisation du package "Gestion des désérialisations non sécurisées"	42
4.10 Diagramme de cas d'utilisation du package "Gestion des utilisations de composants vulnérables"	43
4.11 Diagramme de cas d'utilisation du package "Gestion de la journalisation et de la surveillance insuffisantes"	44
4.12 Diagramme de cas d'utilisation global du système	45
4.13 Diagramme de packages du système (réorganisé)	46
4.14 Diagramme de cas d'utilisation du sous-système "Utilisateurs"	47
4.15 Diagramme d'activités du cas "Authentification utilisateur"	50
4.16 Diagramme d'activités du cas "Authentification utilisateur"	53
4.17 Diagramme d'états-transition d'un utilisateur	54
4.18 Diagramme de cas d'utilisation du sous-système "Cryptographie"	54
4.19 Diagramme de cas d'utilisation du sous-système "Encodage"	55
4.20 Diagramme de cas d'utilisation du sous-système "Validation"	55
4.21 Diagramme de cas d'utilisation du sous-système "HTTP"	57
4.22 Diagramme de cas d'utilisation du sous-système "Interpreteurs"	58
4.23 Diagramme de cas d'utilisation du sous-système "Gestion de la journalisation et de la surveillance insuffisantes"	58

4.24	Diagramme de cas d'utilisation du sous-système "Gestion de la journalisation et de la surveillance insuffisantes"	59
4.25	Diagramme de classes d'analyse dy système	59

INTRODUCTION

....

Ce document s'articule autour de

CHAPITRE **1**

PRÉSENTATION GÉNÉRALE

1.1 La Structure d'accueil

1.1.1 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.

1.1.2 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.

1.1.3 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 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.

1.1.4 Organisation

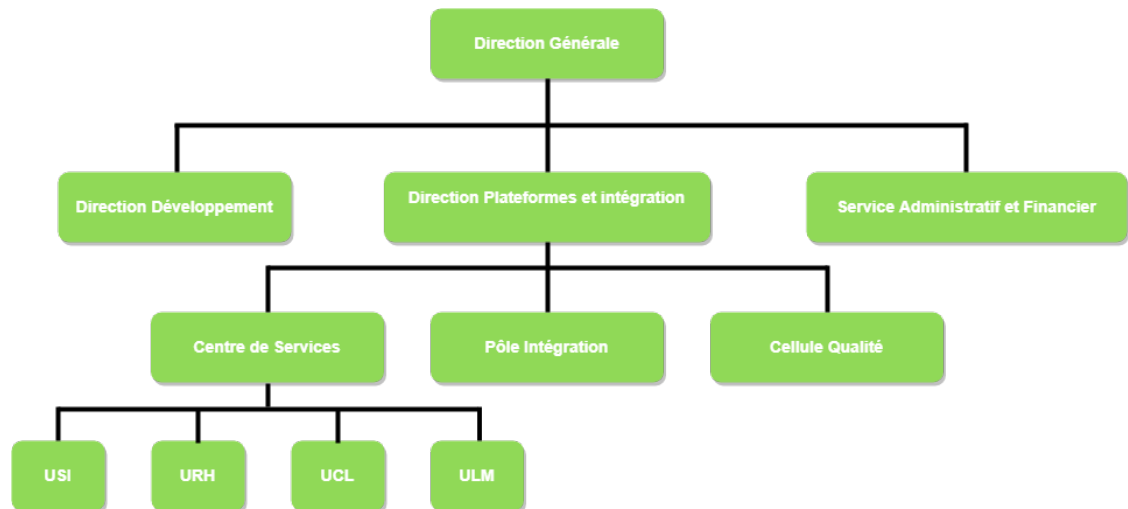


FIGURE 1.1 – Organigramme de HubSo

La figure 1.1 représente l'organigramme 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.

1.2 Le Sujet

1.2.1 Terminologie

1.2.1.1 Sécurité informatique

La sécurité peut être définie comme étant un état, une situation 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.[1]

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, 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.

1.2.1.2 Cryptographie

La sécurité de l'information 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 de l'information 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).

Il existe de nombreuses fonctions de cryptographie. Il y a notamment :

- le cryptage ou chiffrement [2] :

Les données, souvent désignées comme texte en clair, sont chiffrées à l'aide d'un algorithme et d'une clé de chiffrement. Ce processus génère un texte chiffré, ou cryptogramme, qui ne peut être affiché dans sa forme d'origine que s'il est déchiffré à l'aide de la bonne clé.

Le déchiffrement est simplement le contraire du chiffrement, suivant les mêmes étapes mais dans l'ordre inverse de l'application des clés. Les algorithmes de chiffrement actuels relèvent de deux catégories : symétriques et asymétriques.

Les fonctions de chiffrement symétrique utilisent la même clé pour le chiffrement et le déchiffrement d'un message. Le chiffrement à clé symétrique est beaucoup plus rapide que son homologue asymétrique, mais l'expéditeur doit échanger la clé utilisée pour chiffrer les données avec le destinataire pour que ce dernier puisse les déchiffrer.

Les fonctions de chiffrement asymétrique utilisent deux clés différentes mais mathématiquement liées, une publique et l'autre privée. La clé publique peut être partagée avec quiconque, tandis que la clé privée doit rester secrète. Le texte en clair est chiffré avec la clé privée alors que la clé publique est utilisée pour le déchiffrement.

Dans la mesure où il y a obligation de distribuer et de gérer en toute sécurité de grands nombres de clés, les processus cryptographiques utilisent généralement un algorithme symétrique pour chiffrer efficacement les données, mais un algorithme asymétrique pour l'échange des clés.

- le hashage [3] :

Les fonctions de hashage permettent de calculer une empreinte (appelée aussi hash) d'une donnée informatique. Les fonctions de hashage implémentent quelques propriétés que nous allons définir maintenant :

- le grand nombre de hash possibles ;
- la taille de l'empreinte est fixe, quelle que soit la taille de la donnée hachée ;
- L'empreinte d'un mot de passe de huit caractères aura donc la même taille que l'empreinte d'un fichier de plusieurs centaines de méga-octets ;
- un changement infime dans la donnée hachée entraîne un changement important dans l'empreinte correspondante (ce qui rend une recherche inverse par dichotomie impossible) ;
- le calcul d'une empreinte est très rapide ;
- il n'est pas possible, en connaissant l'empreinte et la fonction de hashage utilisée, de

calculer la donnée d'origine.

Le cassage d'une donnée hachée se fait le plus souvent par l'utilisation de Rainbow Tables¹. Le salage du hash est une technique efficace permettant de se prémunir de ces attaques. Elle consiste à ajouter à la donnée à hasher un sel, qui peut être une valeur arbitraire, et qui rendra donc les attaques par Rainbow Table inefficaces :

$$(1.1) \quad \textit{empreinte} = \textit{hashage}(\textit{mot} - \textit{de} - \textit{passe} + \textit{sel})$$

Il n'est pas nécessaire que le sel soit une information secrète, son utilité étant de rendre les dictionnaires inversés inefficaces. Ces fonctions sont généralement utilisées pour les besoins suivants :

- ✓ la vérification de l'intégrité d'une donnée : dans ce cas, le hash (généralement appelée somme de contrôle ou checksum) est utilisé pour s'assurer qu'une donnée informatique n'a pas été corrompue ;
 - ✓ le stockage des mots de passes : le hashage du mot de passe permet d'éviter que ce dernier soit stocké en clair. Nous reviendrons sur ce cas d'utilisation dans la suite de cet article ;
 - ✓ la construction de jetons : comme les jetons « remember me ».
- la signature [4] :

Les fonctions de signature numérique, par analogie avec la signature manuscrite d'un document papier permettent de s'assurer qu'une donnée provient bien d'une entité donnée et qu'elle n'a pas été modifiée.

Les fonctions de signature numérique utilisent surtout des algorithmes à clé publique, pour lesquels deux clés différentes (privée et publique) sont nécessaires. Le signataire utilise sa clé privée pour chiffrer l'empreinte numérique du message à transmettre, préalablement calculée à l'aide d'une fonction de hashage, tandis que le destinataire utilise la clé publique du signataire pour déchiffrer l'empreinte du message qu'il compare avec l'empreinte obtenue après hashage du même message en clair.

La signature numérique correspond ainsi à une marque personnelle apposée à un document électronique par l'utilisation d'un procédé technologique : généralement la cryptographie asymétrique. La signature numérique équivaut à une signature manuscrite, en ce sens qu'elle offre une preuve de l'identité du signataire du message ou du document électronique reçu.

Une signature numérique permet en fait d'attribuer trois qualités à un document électronique : l'authentification, l'intégrité et la non-répudiation des données. En effet, une vérification réussie de la signature numérique permet au destinataire de confirmer l'identité de l'expéditeur (authentification), de s'assurer que le document reçu est identique au document expédié (intégrité des données) et d'empêcher l'expéditeur de répudier le document, c'est-à-dire de nier l'avoir transmis (non-répudiation).

1. Ensemble de hash précalculées en hashant des données courantes avec un algorithme de hashage

1.2.2 Contexte

1.2.2.1 Evolution des applications Web et Mobiles

Aux premiers jours de l'internet, le World Wide Web² consistait en de simples pages web, des pages d'information constituées 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 ;
- 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 (HyperText Transfer Protocol), 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 ;

2. Système reliant des ressources hypertextes sur Internet grâce au protocole Http³

- ✓ Les navigateurs sont devenus aujourd'hui hautement sophistiqués 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 devenues 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.

Les applications mobiles permettent de mettre à la disposition des utilisateurs des services 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 ;
- ✓ le fonctionnement en mode hors ligne est possible.

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'utilisateurs. Il suffit de voir le nombre d'utilisateurs d'une application telle que WhatsApp qui, en 2017, était utilisée par plus d'un milliard de personnes mensuellement, pour s'en convaincre [5]. 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'applications mobiles. Depuis 2017, plus de la moitié de la population mondiale utilise désormais un smartphone et plus de la moitié du trafic internet mondial s'effectue désormais à partir de téléphones mobiles.[6]

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. De même, dans le monde des applications Web et mobiles, les besoins évoluent très rapidement et pour arriver à satisfaire ces besoins nouvelles technologies sont créées. On assiste à la naissance de multiples nouvelles technologies.

1.2.3 Problématique et Objectifs

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 découle du fait qu'elles doivent accepter et traiter des données, lesquelles données pouvant être non fiables ou malveillantes. Cependant, plusieurs autres facteurs [7] 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 patches, 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 « Minimum fonctionnal value » c'est-à-dire vers la production d'un livrable fonctionnel le plus rapidement possible. 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.

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 (Open Web Application Security Project), étude dont la finalité est de fournir à ses développeurs les éléments dont ils ont besoin pour produire du code sécurisé.

En effet, HubSo travaille souvent avec des entreprises de renom comme Total qui est une multinationale présente un peu partout dans le monde. Et de nos jours, ces genres d'entreprises, du fait de ce qu'ils représentent en terme de valeur monétaire, d'intérêts sont souvent la cible d'individus mal intentionnés : cybercriminels, terroristes... C'est pourquoi avant d'accepter les applications qui leurs sont livrées, ces applications sont d'abord sujettes à des audits de sécurité. C'est dans ce sens que HubSo reçoit souvent des équipes d'audit de sécurité dont celles de Mozart qui est très reconnu dans le domaine de l'audit de sécurité des applications web et mobiles. Dès lors, HubSo se doit de leur fournir des applications avec un certain de sécurité pour ne pas compromettre leurs intérêts mais aussi pour des questions de sa propre renommée. Pour y arriver, les objectifs suivants ont été assigné :

- ✓ 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 :

- ✓ Architecture type Owasp (Client Android, Serveur JEE);
- ✓ Intégration d'une application existante;
- ✓ 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
- ✓ 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

1.2.4 Périmètre

La sécurité des applications web implique plusieurs domaines dont 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.

CHAPITRE **2**

ETAT DE L'ART

2.1 Historique

2.1.1 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. [8]

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 essentiellement en un problème de chiffrement de données. On utilisait alors la cryptographie classique avec le chiffrement par substitution d'abord puis plus tard le chiffrement par transposition.

2.1.2 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 la période des deux guerres, 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 sophistiqués furent mis 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 nazies 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 anti-hitlérienne 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. [9]

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.

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 développés¹. 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 [10], un système d'exploitation multi utilisateurs fut créé en 1965. 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 entrant 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 enregistrerait 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 [11].

A cette époque, pour éprouver la sécurité des systèmes en place, il était très courant de faire appel à des Tiger Team [12]. 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'intrusion².

1. Un 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.

2. C'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 » [13]. 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.

2.1.3 Vers un usage massif d'Internet

La première grande menace sur le réseau Internet fut celle du ver³ Morris [14] en 1988. Le ver Morris était initialement un programme conçu afin de mesurer la taille du réseau internet, sans intention néfaste, mais à cause d'un bug de la part de son concepteur, se déplaçait de machine en machine, et une fois sur la machine, ne s'arrêtait pas mais se reproduisait plutôt. Et à partir de là, plusieurs conséquences sont rapidement apparues. La charge processeur qu'il provoquait était susceptible d'altérer les performances de la machine voire d'empêcher son accès. C'est donc devenu par la force des choses une attaque par Déni de Service (DOS - Denial Of Service - ou DDOS - Distributed Denial of Service).

Le nombre de victimes du ver Morris est estimé à 6000 représentant 10% de la population Internet d'alors. Cet événement fut un événement marquant dans l'histoire de la sécurité informatique. En effet, le ver Morris a parfois été appelé le « Grand ver » à cause de l'effet dévastateur qu'il avait

3. En informatique, un ver est un programme malicieux capable de s'auto-reproduire et de se déplacer à travers un réseau sans avoir d'un support physique ou logique

eu sur l'Internet à cette époque, autant pour les pannes causées que pour l'impact psychologique qu'il a eu sur la perception que les professionnels de l'informatique et le grand public avaient de la sécurité et de la fiabilité de l'Internet. L'on réalisa dès lors, que sur le réseau Internet, des événements malencontreux peuvent se produire et qu'il faudrait penser à prévenir de ce genre de choses en mettant en place des mesures de sécurité pour le rendre plus sûr. Après cet incident et Robert Morris, l'auteur du vers fut condamné par la loi américaine sur la répression des fraudes et infractions dans le domaine informatique (Computer Fraud and Abuse Act). Cette loi a été adoptée un peu plus tôt en 1986 afin de protéger les organismes contre les éventuels cybercriminels qui pourraient s'attaquer à leurs systèmes informatiques. De même, la DARPA (Defense Advanced Research Projects Agency), l'agence chargée de la recherche sur les projets de défense avancées aux États-Unis créa le CERT (Computer Emergency Response Team). Il s'agit d'une organisation était composée d'informaticiens d'horizons différents réunis pour régler l'incident et empêcher ce genre de chose de se produire à nouveau.

Le ver Morris ouvra la voie aux virus et vers informatiques. Bientôt, des individus se mirent à créer des virus, parfois dans un but de faire mal et parfois par des amateurs qui le font par passion. Et cela ne laissa pas indifférents les experts en sécurité informatique de l'époque qui se mirent rapidement à créer des entreprises éditrices d'antivirus. L'industrie de l'antivirus commença ainsi. Du fait des dégâts que peuvent occasionner certains virus, les utilisateurs commencèrent à acheter des antivirus pour sécuriser leurs systèmes informatiques. Bien que des avancées en termes de sécurité aient déjà été faites, ce fut la première fois que le grand public investissait pour s'offrir de la sécurité informatique avec l'achat des premiers antivirus.

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 (Transmission Control Protocol/Internet Protocol), tout ordinateur devient instantanément compatible avec tous les autres utilisateurs d'Internet. Internet, à ses débuts reposait exclusivement sur le protocole HTTP, qui reposait à son tour sur le protocole TCP/IP [15]. Mais, il ne garantissait pas la confidentialité et l'intégrité des données transmises. Cependant il n'y avait pas encore d'autres alternatives. 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. L'année 1995 a été une année charnière pour le World Wide Web en général et pour la sécurité en particulier. En effet, Netscape 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.

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 d'apporter de la

sécurité 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 sont 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 (Secure Socket Layer - Plus d'informations sont disponibles sur SSL en annexe).

Avec le protocole SSL, la sécurité a été sensiblement améliorée. SSL elle-même a été améliorée avec sa version SSL/TLS (Secure Socket Layer/Transport Layer Security).

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 certains "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. Bien que, comme tout système de chiffrement, le protocole 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.

2.2 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 protège 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.

2.2.1 Contexte juridique

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. Les premières législations sur la protection des données personnelles 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 2.1 décrit l'ordre d'adoption des lois par différents pays. [16]

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

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.

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.

2.2.2 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.

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. A ce sujet, un accord a été signé entre Suricate, une entreprise luxembourgeoise spécialisée dans la cyber sécurité et l'ADIE (Agence De l'Informa-

tique de l'Etat) pour la mise en place d'un CERT national.

Les CERTs 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 - Forum of Incident Response and Security Teams). 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 régionales 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 qui œuvrent pour une meilleure sécurité de l'information. Parmi celles-ci, les plus connues sont Mitre, Sans Institute et Owasp.

2.2.3 Contexte organisationnel

2.2.3.1 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.

2.2.3.2 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.

2.2.3.3 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.

2.2.3.4 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.

2.3 Owasp

2.3.1 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.

2.3.2 Origines

OWASP a été créé par un certain Mark Curphey le 9 septembre 2001. Son but initial était 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.

2.3.3 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 des 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.

2.3.4 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.

2.3.5 Top 10 Owasp

2.3.5.1 Présentation

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.

2.3.5.2 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 où 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 :

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

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 2.2 – Correspondance Top 10 Owasp A1 - CWE/Sans Top 25

CHAPITRE 3

MÉTHODOLOGIE DE DÉVELOPPEMENT

Sommaire

1.1	La Structure d'accueil	3
1.1.1	Présentation de HubSo	3
1.1.2	Domaines d'activités	3
1.1.3	Quelques Solutions de HubSo	3
1.1.4	Organisation	4
1.2	Le Sujet	5
1.2.1	Terminologie	5
1.2.2	Contexte	8
1.2.3	Problématique et Objectifs	10
1.2.4	Périmètre	12

3.1 Qu'est ce qu'une méthodologie de développement ?

A methodology formally defines the process that you use to gather requirements, analyze them, and design an application that meets them in every way. There are many methodologies, each differing in some way or ways from the others.

Une méthodologie est une démarche, une ligne de conduite qui est suivi par l'ensemble de l'équipe projet du lancement jusqu'à la livraison de celui-ci. Elle permet d'uniformiser le processus de travail et facilite la communication de l'équipe projet via des concepts et termes bien définis et compris par tous. Une méthodologie est un processus, une démarche à suivre pour aboutir à la concrétisation d'un projet. There are many reasons why one methodology may be better than another for your particular project : For example, some are better suited for large enterprise applications while others are built to design small embedded or safety-critical systems. On another axis, some methods better support large numbers of architects and designers working on the same project, while others work better when used by one person or a small group

3.2 Intérêt d'une méthodologie

3.3 Catégories de méthodologies de développement

Les méthodes traditionnelles prônent un enchaînement séquentiel des différentes activités, depuis les spécifications jusqu'à la validation du système, selon un planning préétabli. Elles visent à mieux prédire la façon dont les choses « devraient » se passer. Malheureusement, cette vision rassurante est bien loin de la réalité des projets.

La conséquence est que plus de 80% des projets exécutés selon ces méthodologies connaissent des retards, des dépassements budgétaires, quand ils ne finissent pas en échec total, pour n'avoir pas su satisfaire les attentes des clients [W11Agiles <http://www.blog.erlem.fr/management/46-methodes-agiles-pourquoi-lesadopter>]. Ces problèmes sont liés à plusieurs caractéristiques fondamentales de ces méthodologies :

- Le rôle joué par le client qui intervient principalement au moment du lancement du projet, à quelques jalons majeurs parfois espacés de plusieurs mois, et surtout en fin de projet pour la réception et la recette du système. Cet « effet tunnel » conduit souvent à une solution souvent inadaptée et de piètre qualité ;
- Le mode contractuel forfaitaire qui durcit les relations entre client et fournisseur, rend le passage de témoin long et douloureux à la fin du projet ;
- Une trop grande standardisation des activités d'ingénierie, dont l'enchaînement se révèle souvent inefficace. Formellement, les contrôles d'avancement et de qualité ne peuvent être menés que sur la base de documents dans les premières étapes, et bien des organisations sont devenues des usines à produire de la documentation au lieu de produire de la valeur (fonctions logicielles) pour les clients et les utilisateurs ;
- Le passage de relai entre les phases successives dans lesquelles oeuvrent très souvent des équipes différentes, généralise une relation de type client-fournisseur et n'encourage ni l'empathie ni l'esprit d'équipe, bien au contraire. Chaque transition se traduit par une perte de temps, de savoir, d'informations ou de responsabilité.

À l'opposé des approches traditionnelles, Les méthodes agiles utilisent un principe de développement itératif qui consiste à découper le projet en plusieurs étapes qu'on appelle « itérations ». Ces itérations ne sont rien d'autre que des mini-projets définis avec le client en détaillant les différentes fonctionnalités qui seront développées en fonction de leur priorité. Au lieu de consacrer beaucoup de temps à la planification, en essayant de tout prévoir, il suffit de se fixer un objectif plus modeste, réalisable dans un délai relativement court, et de planifier la suite des choses en fonction des résultats observés. L'agilité peut également dans ce cas améliorer les résultats déjà obtenus et faciliter la résolution de bon nombre des difficultés vécues. Elle va amener les personnes impliquées à :

- Mieux collaborer, prendre du recul sur l'application en priorisant les actions ;
- Donner plus de visibilité aux clients et utilisateurs ;
- Éliminer « l'effet tunnel » en le remplaçant par des itérations courtes et maîtrisées.

Il existe de nombreuses méthodes Agiles. Parmi celles-ci, nous avons entre autres XP (Extreme Programming), Scrum, RAD (Rapid Application Development), PUMA, etc.

3.4 Choix d'une méthodologie de développement

3.5 Intérêt d'une modélisation

Un modèle est une représentation abstraite et simplifiée d'une entité du monde réel en vue de le décrire, de l'expliquer ou de le prévoir. Modéliser, c'est décrire de manière visuelle et graphique les besoins et les solutions fonctionnelles et techniques d'un projet.

Concrètement, un modèle permet de réduire la complexité d'un phénomène ou d'une entité en éliminant les détails qui n'influencent pas son comportement de manière significative. Il reflète ce que le concepteur croit important pour la compréhension et la prédiction du phénomène modélisé. Les limites du phénomène modélisé dépendent des objectifs du modèle.

Modéliser un système avant sa réalisation permet de mieux comprendre le fonctionnement du système. C'est également un bon moyen de maîtriser sa complexité et d'assurer sa cohérence. Un modèle est un langage commun, précis, qui est connu par tous les membres de l'équipe et il est donc, à ce titre, un vecteur privilégié pour communiquer. Cette communication est essentielle pour aboutir à une compréhension commune et précise d'un système par ses différentes parties prenantes.

3.6 Présentation d'UML

UML est l'acronyme de « Unified Modeling Language » qu'on peut traduire par « langage de modélisation unifié ». Il s'agit d'un langage de modélisation graphique et textuel, un outil de modélisation constitué d'un ensemble de schémas, appelés diagrammes UML, qui donnent chacun une vision différente du projet à traiter. En effet, un document texte décrivant de façon précise un système contiendrait plusieurs pages. En général, peu de personnes ont envie de lire ce genre de document. De plus, un long texte de plusieurs pages est source d'interprétations et d'incompréhension. UML nous aide à faire cette description de façon graphique et devient alors un excellent moyen pour « visualiser » le futur système.

UML utilise l'approche objet qui a déjà fait ses preuves. Il permet de faire une abstraction des technologies objet en permettant d'exprimer et d'élaborer des modèles objet, indépendamment de tout langage de programmation. L'aspect formel de sa notation, limite les ambiguïtés et les incompréhensions.

Son indépendance par rapport aux langages de programmation, aux domaines d'application et aux processus, en fait un langage universel. En effet, le processus de collecte et d'analyse des exigences d'une application et de leur intégration dans la conception d'un programme, est complexe et il existe actuellement nombre de méthodologies qui définissent des procédures formelles spécifiant la démarche à suivre. Une des caractéristiques d'UML est qu'il est indépendant de toute méthodologie. Quelle que soit la méthodologie de développement utilisée dans un projet, on peut utiliser UML pour la modélisation du système. Il a été pensé pour servir de support à une analyse des concepts objet. C'est un langage formel, défini par un méta-modèle.

UML est aussi un support de communication performant, qui facilite la compréhension de systèmes aussi complexes qu'ils soient.

UML est le résultat de la fusion de trois méthodes orientées objet Booch, OMT (Object Modeling Technique) et OOSE (Object Oriented Software Engineering) conçues respectivement par Grady Booch, James Rumbaugh et Ivar Jacobson. UML a démarré avec la version 0.8 intégrant les

méthodes BOOCH 93 et O.M.T. Par la suite ce fut l'avènement de la version 0.9 ayant intégré la méthode OOSE. La version 1.0, proposé à l'O.M.G en 1996, fut finalement standardisée en 1997 sous la version 1.1 . Depuis, il y a eu plusieurs révisions du standard. Les dernières améliorations étant conséquentes, UML est passé à une nouvelle version : UML 2.0 (ou UML 2), abrégé souvent en U2. En 2005, l'Organisation internationale de normalisation (ISO) a également publié UML en tant que norme ISO approuvée. Actuellement, UML en est à sa version 2.5.

3.7 Diagrammes UML

UML propose 14 diagrammes qui sont dépendants hiérarchiquement et se complètent, de façon à permettre la modélisation d'un projet tout au long de son cycle de vie. Un diagramme UML est une représentation graphique, qui s'intéresse à un aspect précis du modèle. C'est une perspective du modèle. Ces diagrammes sont répartis en 3 grands groupes :

>Diagrammes structurels ou statiques qui s'intéressent la structure interne du système :

- o Diagramme de classes : il représente les classes intervenant dans le système et les associations, agrégations, généralisation, interfaces, etc ;
- o Diagramme d'objets : il sert à représenter les instances de classes (objets) utilisées dans le système ;
- o Diagramme de composants : il permet de montrer les composants du système d'un point de vue physique ;
- o Diagramme de déploiement : il sert à représenter les éléments matériels et la manière dont les composants du système sont répartis sur ces éléments matériels et interagissent entre eux ;
- o Diagramme de paquetages : il sert à représenter les dépendances entre paquetages, c'est-à-dire les dépendances entre ensembles de définitions ;
- o Diagramme de structure composite : il montre l'organisation interne d'un élément statique complexe ;
- o Diagramme de profils : il permet de spécialiser, de personnaliser pour un domaine particulier un méta-modèle de référence d'UML ;

>Diagrammes comportementaux qui s'intéressent aux interactions du système, avec lui même et avec d'autres entités :

- o Diagramme des cas d'utilisation : il représente la structure des grandes fonctionnalités nécessaires aux utilisateurs du système ;
- o Diagramme d'états-transitions : il représente la façon dont évoluent les objets appartenant à une même classe ;
- o Diagramme d'activités : le diagramme d'activités n'est autre que la représentation du processus tel qu'il a été élaboré lors du travail qui a préparé la modélisation : il montre l'enchaînement des activités qui concourent au processus ;

>Diagrammes d'interaction ou dynamiques :

- o Diagramme de séquence : il permet de décrire séquentiellement les différents scénarios d'utilisation du système ;
- o Diagramme de communication : c'est la représentation simplifiée d'un diagramme de séquence se concentrant sur les échanges de messages entre les objets ;
- o Diagramme global d'interaction : permet de donner une vue d'ensemble des interactions du

système. Il est réalisé avec le même graphisme que le diagramme d'activités. ;

o Diagramme de temps : il permet de décrire les variations d'un objet au cours du temps.

La figure 3.1 une vue globale et hiérarchique des quatorze diagrammes UML.

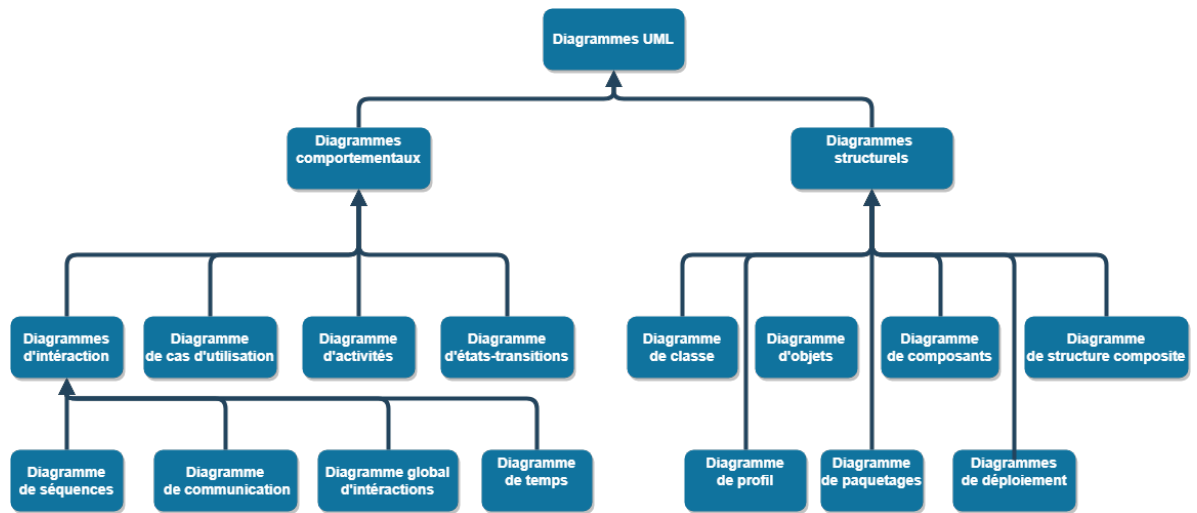


FIGURE 3.1 – Schéma d'ensemble des diagrammes UML

Ces diagrammes, d'une utilité variable selon les cas, ne sont pas nécessairement tous produits à l'occasion d'une modélisation. Nous utiliserons au besoin certains de ces diagrammes pour illustrer les aspects de notre solution.

C H A P I T R E 4

ANALYSE ET CONCEPTION

Nous nous sommes intéressés au Top 10 d'Owasp qui nous a servi de cahiers de charge pour notre recueil de besoins. Les spécifications ont été faites sur la base de ce document. La version originale du document est disponible en annexe.

Le Top 10 Owasp, en recensant les dix risques de sécurité les plus critiques des applications Web, les explique et donne pour chacune de celles-ci, un ensemble de directives de codage à mettre en œuvre pour se protéger de ces risques de sécurité. Cependant, le document original n'est pas assez parlant pour bon nombre de personnes et le fait qu'il soit rédigé en anglais est un obstacle pour d'autres. Nous avons tenté d'expliquer chaque point du Top 10 afin de les faire connaître aux développeurs. Cela a fait l'objet d'un document distribué aux développeurs et affiché dans les locaux de HubSo. De même, nous avons, pour chaque risque, recensé les pratiques à mettre en œuvre pour s'en prémunir. Celles-ci feront l'objet des spécifications et de l'analyse.

4.1 Spécifications

4.1.1 Spécifications fonctionnelles

Les spécifications fonctionnelles décrivent les processus métier dans lesquels notre système devra intervenir, les tâches prises en charge par le système. Dans notre cas, il s'agira des tâches préconisées par le Top 10 pour chacun des risques de sécurité.

4.1.1.1 Les Acteurs

Un acteur représente un rôle joué par une entité externe (utilisateur humain, dispositif matériel ou autre système) qui interagit directement avec le système étudié.

Notre système est principalement en interaction avec les autres applications utilisant les différentes fonctionnalités mises à disposition par celui-ci.

4.1.1.2 Les fonctionnalités générales

Notre système met à la disposition des applications qui l'utilisent un ensemble de fonctionnalités leur permettant de gérer les différentes risques de sécurité énoncées par le Top 10. Il s'agit d'une bibliothèque de sécurité. Ces fonctionnalités, sont dans un premier regroupées en modules avec chaque module correspondant à la gestion d'un risque.

►Gestion des injections

Ce module regroupe les fonctions de sécurité permettant de se protéger des injections. Pour prévenir les injections, les fonctions de sécurités suivantes doivent être mises à disposition par le système :

- ✓ la validation des entrées ;
- ✓ la récupération de données de manière sécurisée ;
- ✓ l'encodage des données ;
- ✓ le paramétrage de requêtes vers les systèmes de gestion de base de données ;
- ✓ le cryptage de données avec un algorithme fort.

►Gestion des violations de Gestion d'Authentification

Ce module regroupe les fonctions de sécurité permettant de se protéger des violations de gestion d'authentification. Pour prévenir la violation de gestion d'authentification, les fonctions de sécurités suivantes doivent être disponibles dans notre système :

- ✓ l'authentification ;
- ✓ la déconnexion ;
- ✓ la vérification de la force d'un mot de passe ;
- ✓ la génération aléatoire de données : il s'agit de générer aléatoirement avec un algorithme non prévisible des données aléatoires numériques et alphanumériques ;
- ✓ la journalisation des événements de connexion (logging) ;
- ✓ le cryptage de données avec un algorithme fort.

►Gestion des expositions de données sensibles

Ce module regroupe les fonctions de sécurité permettant d'éviter l'exposition de données sensibles. Pour ce faire, les fonctions de sécurités suivantes doivent être disponibles dans notre système :

- le hachage fort de mots de passe avec un sel ¹ ;
- l'ajout d'entêtes HTTP (Entête Cache essentiellement) ;
- la vérification de l'utilisation d'un canal sécurisé HTTPS ;
- l'authentification des requêtes HTTP en Digest ² ;
- le cryptage de données avec un algorithme fort.

►Gestion des attaques sur les entités XML externes

Ce module regroupe les fonctions de sécurité permettant de se protéger des attaques sur les entités XML externes. Il contient les fonctions de sécurités :

- l'encodage de données en HTML ;
- la validation des entrées.

►Gestion des violations de contrôle d'accès

Ce module regroupe les fonctions de sécurité permettant de se protéger des violations de contrôle d'accès. Pour prévenir les violations de contrôle d'accès, les fonctions de sécurités suivantes doivent être mises à disposition par le système :

1. donnée ajoutée au mot de passe avant hachage
2. Explication Digest

- la vérification des autorisations sur les ressources (autorisations sur les fichiers, urls, fonctions);
- la vérification des rôles des utilisateurs;
- l'authentification;
- la déconnexion;
- la journalisation des accès aux ressources et événements de connexion.

► Gestion des mauvaises configurations de sécurité

Ce module regroupe les fonctions de sécurité permettant d'éviter les problèmes de sécurité découlant des mauvaises configurations de sécurité. On a principalement :

- le paramétrage des entêtes HTTP : il s'agit de toutes les entêtes HTTP relatives à la sécurité (Entêtes HSTS, X-Frame-Options, X-XSS-Protection, X-Content-Type-Options, CSP, X-Permitted-Cross-Domain-Policies entre autres).

► Gestion des cross-site scripting (XSS)

Ce module regroupe un ensemble de fonctions de sécurité permettant de se protéger des attaques XSS. Il s'agit de :

- la validation des entrées;
- la sanitization des entrées;
- l'encodage des sorties selon le contexte de sortie (HTML, CSS, JavaScript)³;
- l'ajout d'entêtes HTTP (CSP principalement).

► Gestion des désérialisations non sécurisée

Ce module regroupe les fonctions de sécurité permettant d'éviter les problèmes de sécurité découlant des désérialisations non sécurisées. On a principalement :

- la signature d'un message ; - la vérification de signatures.

► Gestion de l'utilisation de composants vulnérables

Ce module regroupe les fonctions de sécurité relatives à l'utilisation de composants vulnérables. Il regroupe les fonctionnalités suivantes :

- la détection de composants vulnérables;
- la notification de nouvelle version d'un composant.

► Gestion de la journalisation et de la surveillance insuffisante

Ce module regroupe les fonctions de sécurité relatives à la journalisation et à la surveillance. Il s'agit de journaliser afin d'avoir une trace de ce qui se passe dans le système mais aussi surveiller afin d'être réactif par rapport aux événements du système. Les fonctionnalités sont les suivantes :

- la journalisation des événements.

3. Toute donnée devant être ajoutée au code source

4.1.2 Spécifications non fonctionnelles

Les besoins non fonctionnelles ou exigences techniques portent sur les différents points suivants : - le pinning de certificats ;

- l'utilisation de protocoles sécurisés ;

- The preferred option is to use a safe API, which avoids the The preferred option is to use a safe API, which avoids use of the interpreter entirely or provides a parameterized interface or migrate to use Object Relational Mapping Tools (ORMs).

- Do not ship or deploy with any default credentials, particularly for admin users.

- Implement weak-password checks, such as testing new or changed passwords against a list of the top 10000 worst passwords.

- établir une politique de mots de passe ;

- A repeatable hardening process that makes it fast and easy to deploy another environment that is properly locked down. Development, QA, and production environments should all be configured identically, with different credentials used in each environment. This process should be automated to minimize the effort required to setup a new secure environment ; - A minimal platform without any unnecessary features, components, documentation, and samples. - Remove or do not install unused features and frameworks. - A task to review and update the configurations appropriate to all security notes, updates and patches as part of the patch management process (see A9 :2017-Using Components with Known Vulnerabilities). In particular, review cloud storage permissions (e.g. S3 bucket permissions).

- A segmented application architecture that provides effective, secure separation between components or tenants, with segmentation, containerization, or cloud security groups (ACLs). - Sending security directives to clients, e.g. Security Headers. - An automated process to verify the effectiveness of the configurations and settings in all environments.

- portabilité

- compatibilité

- formation

- efficacité : efficacité en temps, efficacité en ressources

- facilité d'intégration

- Toute information confidentielle fournie par les clients via l'Internet sera cryptée avec le système XYZ ou par l'algorithme, la méthode....ABC..

- Tous les logiciels du côté client vont être téléchargés et installés à partir du navigateur, sans que le poste du client ne soit redémarré ou configuré manuellement

- Le comportement du programme doit être paramétrable par des fichiers texte de configuration

- autres besoins non fonctionnels spécifiés par les autres points ;

4.2 Analyse

Après avoir défini les acteurs et énuméré les fonctionnalités générales du système, nous passons à la phase d'analyse. Nous utiliserons les diagrammes de cas d'utilisation pour mieux représenter ce qui est attendu du système. Pour certains cas d'utilisation, une description textuelle

sera faite. Nous utiliserons aussi des diagrammes d'activité pour illustrer le séquençement des actions par rapport à certains cas d'utilisation.

Pour des besoins de concision, chaque point du Top 10 sera considéré comme un package et comportera les fonctionnalités définies plus tôt. Ces packages sont les suivants :

- package gestion des injections
- package gestion des violations de Gestion d'Authentification
- package gestion des expositions de données sensibles
- package gestion des attaques sur les entités XML externes
- package gestion des violations de contrôle d'accès
- package gestion des cross-site scripting (XSS)
- package gestion de l'utilisation de composants vulnérables
- package gestion de la journalisation et de la surveillance insuffisante

La figure 4.1 ci-dessous représente ces différents packages.

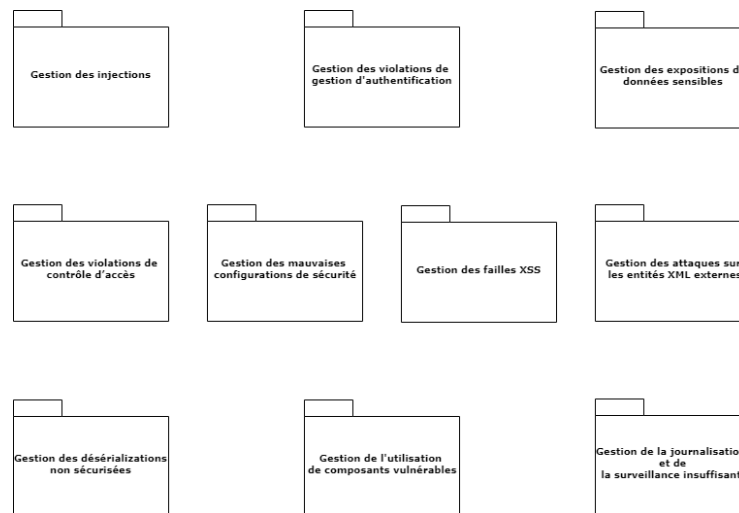


FIGURE 4.1 – Diagramme de packages du système

4.2.1 Package Gestion des injections

4.2.1.1 Diagramme de cas d'utilisation

Le diagramme de cas d'utilisation du package "Gestion des injections" est représenté ci-dessous. Il comprend les cas d'utilisation permettant à une application donnée de mitiger les risques d'injection.

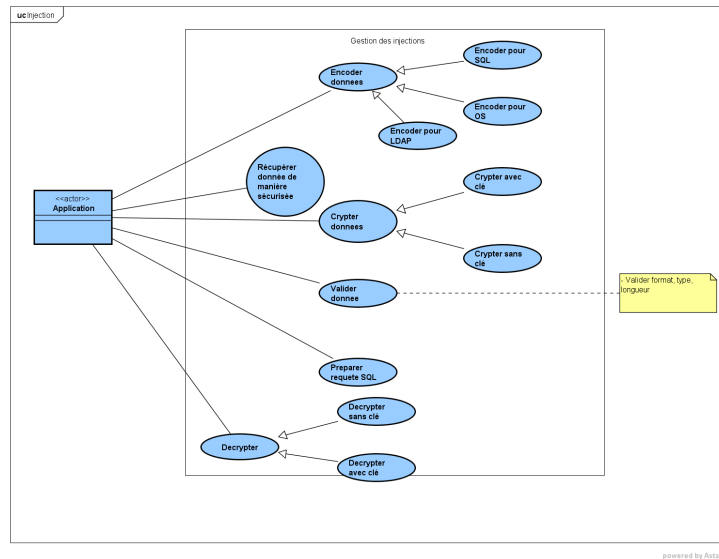


FIGURE 4.2 – Diagramme de cas d'utilisation du package "Gestion des injections"

4.2.2 Package Gestion des violations de gestion d'authentification

4.2.2.1 Diagramme de cas d'utilisation

Le diagramme de cas d'utilisation du package "Gestion des violations de gestion d'authentification" est représenté ci-dessous. Il comprend les cas d'utilisation permettant à une application donnée de mitiger les risques de violations de gestion d'authentification.

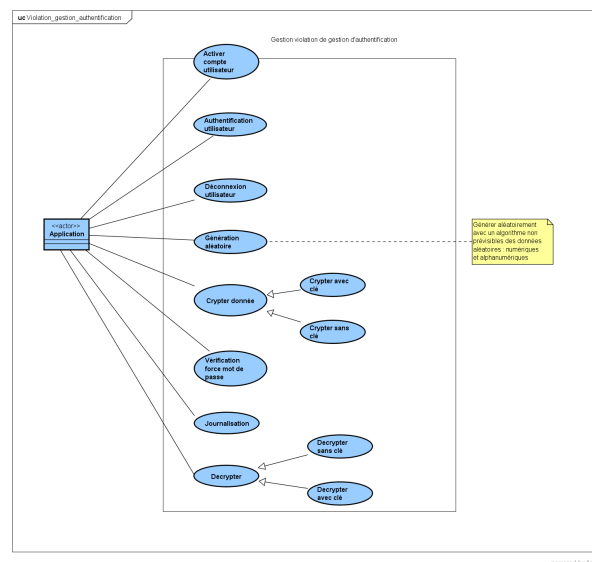


FIGURE 4.3 – Diagramme de cas d'utilisation du package "Gestion des violations de gestion d'authentification"

4.2.3 Package Gestion des expositions de données sensibles

4.2.3.1 Diagramme de cas d'utilisation

Le diagramme de cas d'utilisation du package "Gestion des expositions de données sensibles" est représenté ci-dessous. Il comprend les cas d'utilisation permettant à une application donnée de mitiger les risques d'exposition de données sensibles.

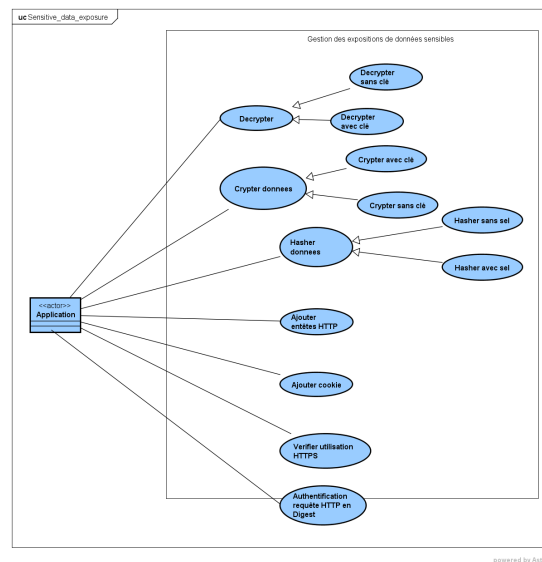


FIGURE 4.4 – Diagramme de cas d'utilisation du package "Gestion des expositions de données sensibles"

4.2.4 Package Gestion des attaques sur les entités XML externes

4.2.4.1 Diagramme de cas d'utilisation

Le diagramme de cas d'utilisation du package "Gestion des attaques sur les entités XML externes" est représenté ci-dessous. Il comprend les cas d'utilisation permettant à une application donnée de mitiger les risques découlant des attaques sur les entités XML externes.

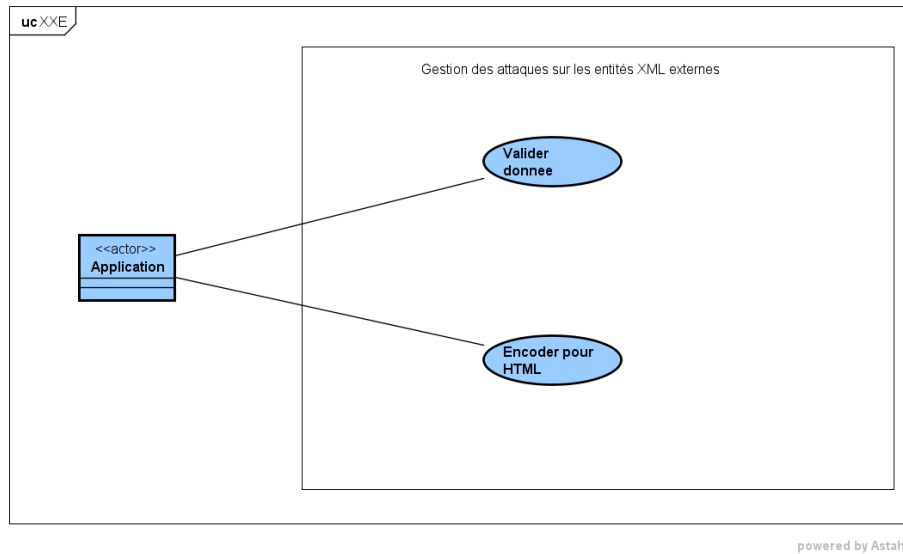


FIGURE 4.5 – Diagramme de cas d'utilisation du package "Gestion des attaques sur les entités XML externes"

4.2.5 Package Gestion des violations de contrôle d'accès

4.2.5.1 Diagramme de cas d'utilisation

Le diagramme de cas d'utilisation du package "Gestion des violations de contrôle d'accès" est représenté ci-dessous. Il comprend les cas d'utilisation permettant à une application donnée de mitiger les risques découlant des violations de contrôle d'accès.

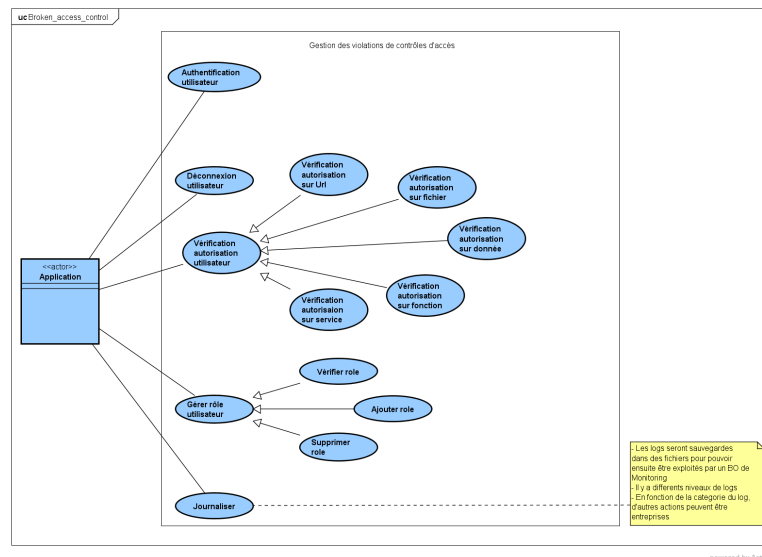


FIGURE 4.6 – Diagramme de cas d'utilisation du package "Gestion des violations de contrôle d'accès"

4.2.6 Package Gestion des mauvaises configurations de sécurité

4.2.6.1 Diagramme de cas d'utilisation

Le diagramme de cas d'utilisation du package "Gestion des mauvaises configurations de sécurité" est représenté ci-dessous. Il comprend les cas d'utilisation permettant à une application donnée de mitiger les risques de mauvaises configurations de sécurité.

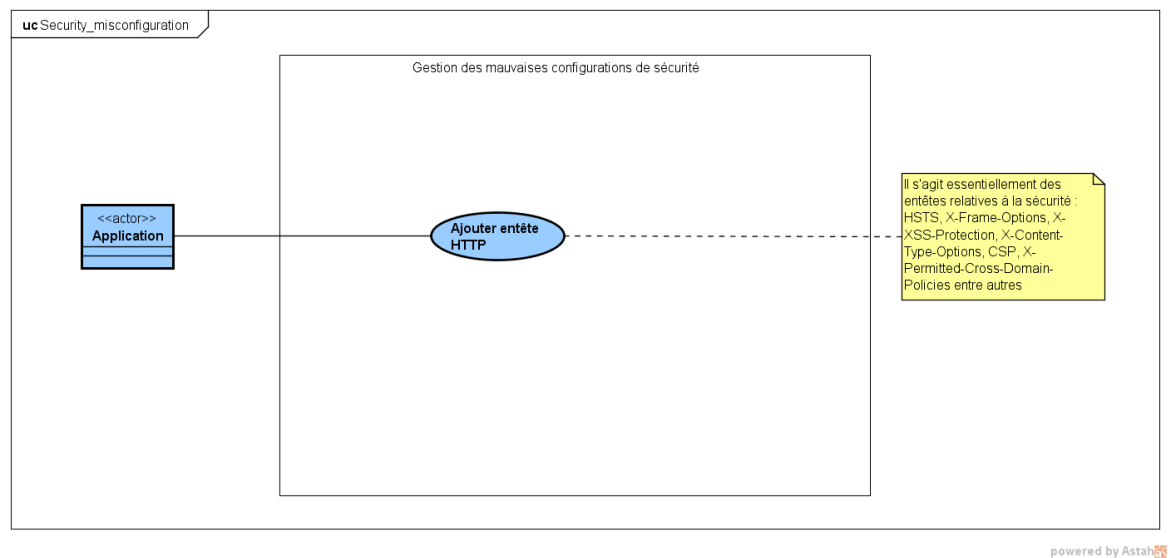


FIGURE 4.7 – Diagramme de cas d'utilisation du package "Gestion des mauvaises configurations de sécurité"

4.2.7 Package Gestion des XSS

4.2.7.1 Diagramme de cas d'utilisation

Le diagramme de cas d'utilisation du package "Gestion des XSS" est représenté ci-dessous. Il comprend les cas d'utilisation permettant à une application donnée de mitiger les attaques XSS.

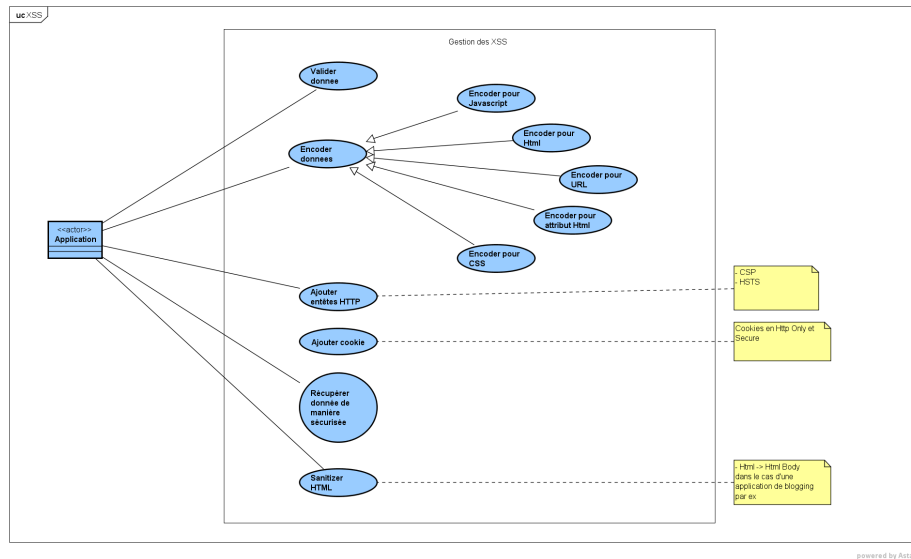


FIGURE 4.8 – Diagramme de cas d'utilisation du package "Gestion des XSS"

4.2.8 Package Gestion des désérialisations non sécurisées

4.2.8.1 Diagramme de cas d'utilisation

Le diagramme de cas d'utilisation du package "Gestion des désérialisations non sécurisées" est représenté ci-dessous. Il comprend les cas d'utilisation permettant à une application donnée de mitiger les risques de désérialisations non sécurisées.

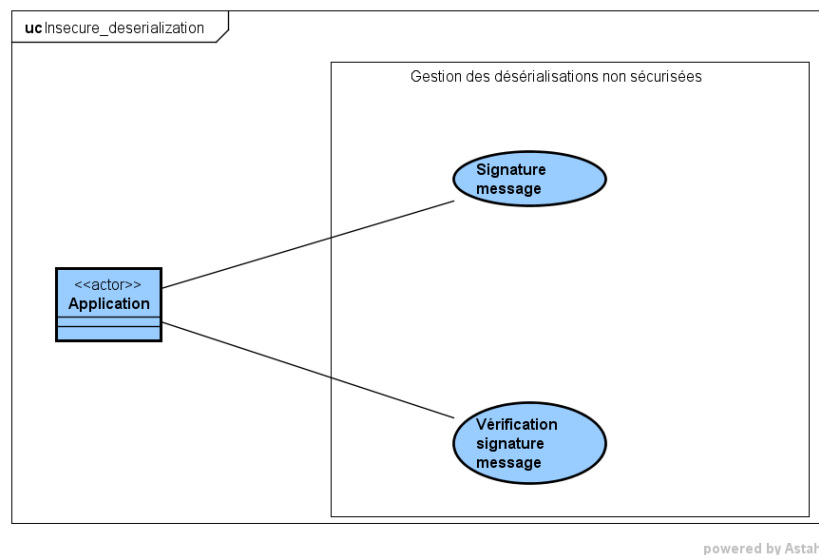


FIGURE 4.9 – Diagramme de cas d'utilisation du package "Gestion des désérialisations non sécurisées"

4.2.9 Package Gestion des utilisations de composants vulnérables

4.2.9.1 Diagramme de cas d'utilisation

Le diagramme de cas d'utilisation du package "Gestion des utilisations de composants vulnérables" est représenté ci-dessous. Il comprend les cas d'utilisation permettant à une application donnée de mitiger les risques découlant de l'utilisation de composants vulnérables.

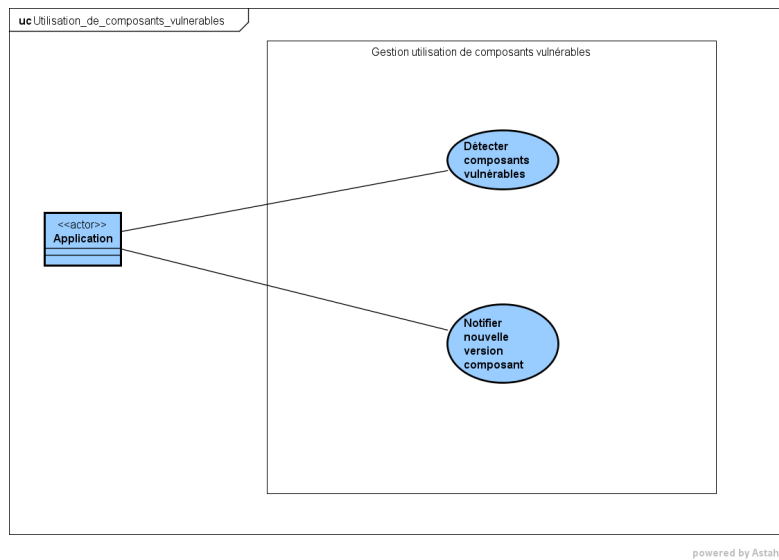


FIGURE 4.10 – Diagramme de cas d'utilisation du package "Gestion des utilisations de composants vulnérables"

4.2.10 Package Gestion de la journalisation et de la surveillance insuffisantes

4.2.10.1 Diagramme de cas d'utilisation

Le diagramme de cas d'utilisation du package "Gestion de la journalisation et de la surveillance insuffisantes" est représenté ci-dessous. Il comprend les cas d'utilisation permettant à une application donnée de mitiger les risques de journalisation et de surveillance insuffisantes.

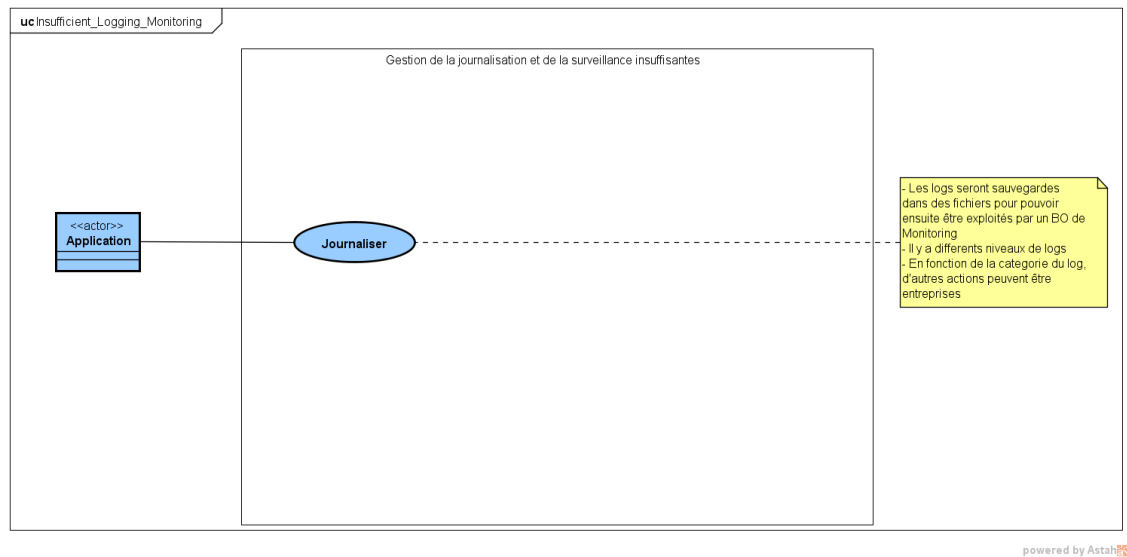


FIGURE 4.11 – Diagramme de cas d'utilisation du package "Gestion de la journalisation et de la surveillance insuffisantes"

4.2.11 Système global

Nous avons organisé les cas d'utilisation en packages, chaque package correspondant à la gestion d'un risque du Top 10, et cela pour des questions de lisibilité mais aussi pour des questions d'identification des fonctions de sécurité à mettre en place en adéquation avec le risque en question. Cependant, le système que nous devons mettre en place tourne autour de ces fonctions de sécurité. Il s'agit de mettre à la disposition des développeurs ces fonctions de sécurités.

En effet, certaines fonctions de sécurité recommandées pour un risque, peuvent aussi l'être pour d'autres. Par exemple, si l'on essaie de mitiger le risque de XSS, la meilleure façon de le faire est de mettre en place des fonctions permettant la validation des entrées ainsi que l'encodage des sorties que les développeurs peuvent facilement utiliser. Mais ces mêmes fonctions peuvent être utilisées pour se protéger de beaucoup d'autres attaques.

Ainsi, nous nous concentrons maintenant sur ces fonctions de sécurité. Nous présenterons à la volée toutes les fonctionnalités attendues par les applications pour se protéger au moins des dix risques de sécurité présentes dans le Top 10.

Ci-dessous, nous avons le diagramme de cas d'utilisation global du système :



45

Toutefois, cette représentation n'est pas non plus le meilleur car ne favorisant pas une bonne lisibilité. Ainsi, nous avons décidé pour des raisons de lisibilité de séparer ces fonctions en modules, chaque module comprenant les fonctions de sécurité de même nature.

Ainsi, nous avons les modules suivants : - Module "Utilisateurs" comprenant les fonctions relatives aux utilisateurs ;

- Module "Cryptographie" comprenant les fonctions se rapportant à la cryptographie ;

- Module "Encodage" comprenant les fonctions d'encodage ;

- Module "Validation" regroupant les fonctions relatives à la validation ;

- Module "HTTP" regroupant les fonctions relatives aux paramètres HTTP ; - Module "Interpréteurs" regroupant les fonctions relatives aux interpréteurs ; - Module "Logging" regroupant les fonctions relatives à la journalisation ;

- Module "Gestion des composants" regroupant les fonctions relatives aux composants utilisés dans l'application.

Chaque module est un sous-système et sera représenté par un package. Cette séparation nous donne le diagramme de packages suivant :

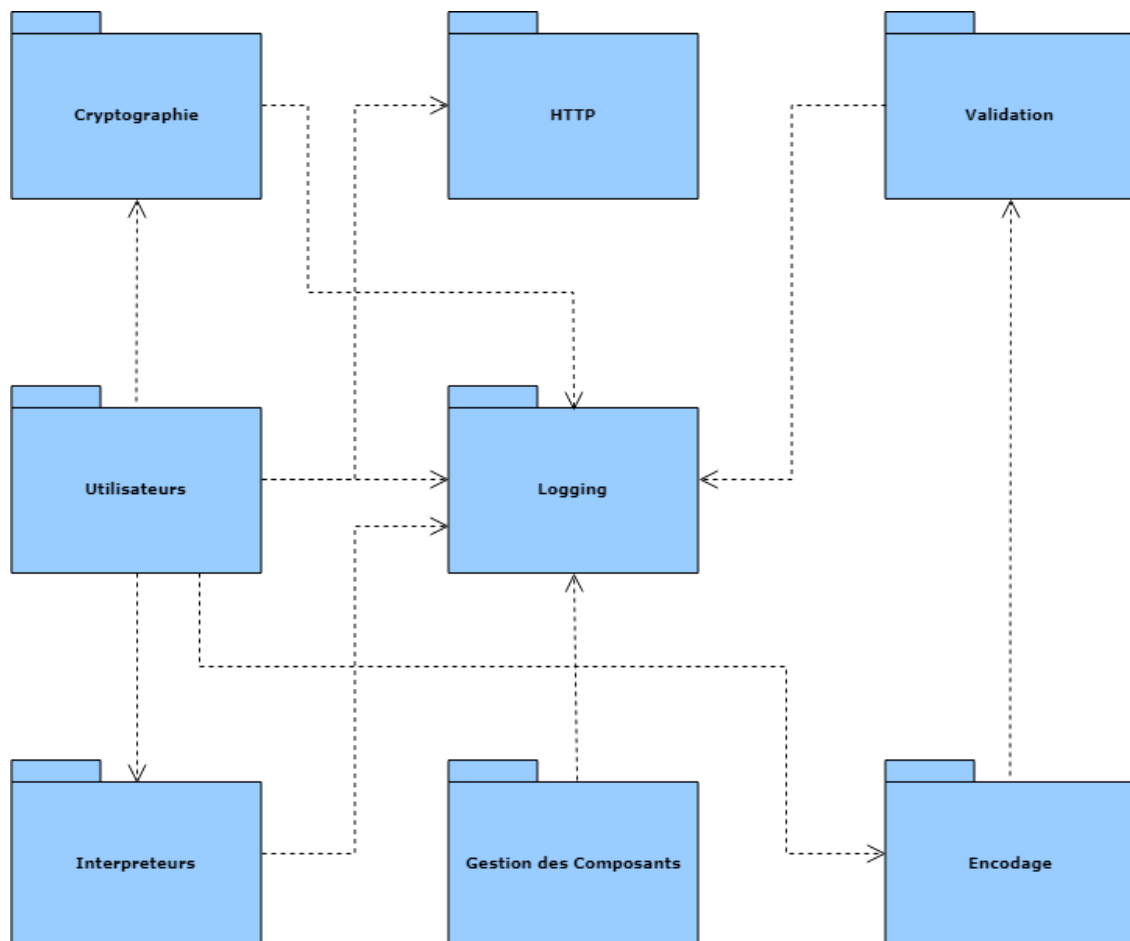


FIGURE 4.13 – Diagramme de packages du système (réorganisé)"

4.2.12 Sous-système "Utilisateurs"

4.2.12.1 Diagramme de cas d'utilisation

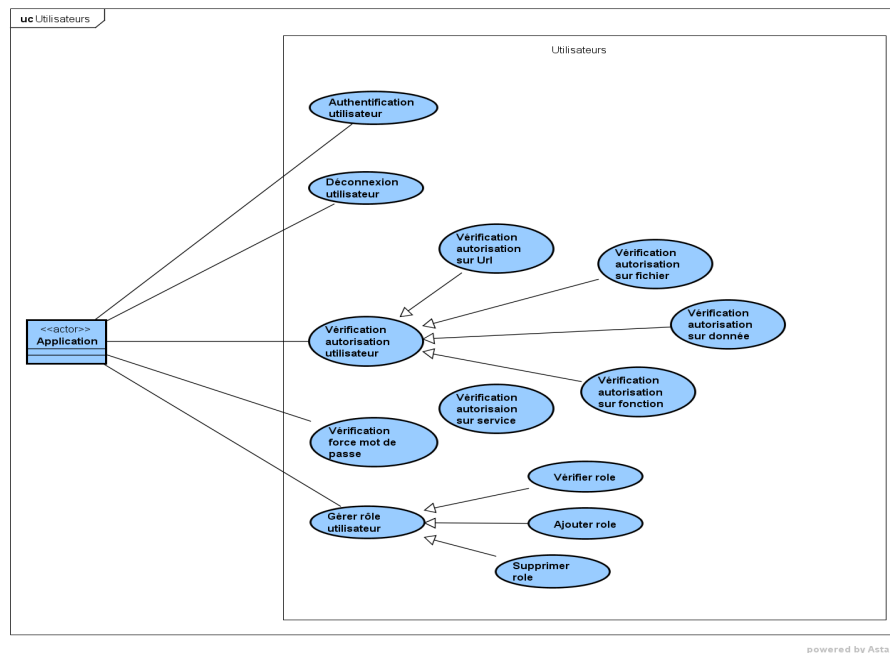


FIGURE 4.14 – Diagramme de cas d'utilisation du sous-système "Utilisateurs"

4.2.12.2 Cas d'utilisation "Authentification utilisateur"

►Description textuelle

Sommaire d'identification

Titre : Authentification utilisateur

Résumé : Ce cas d'utilisation permet à une application d'authentifier un utilisateur.

Acteur : Application

Responsable : Papa Latyr Mbodj

Description des scénarios

Précondition(s)

— Aucune

Scénario nominal

1. L'application donne une requête HTTP POST contenant nom d'utilisateur et mot de passe.
2. Le système récupère l'utilisateur avec le nom d'utilisateur donné.
3. Le système enregistre l'adresse IP de connexion.
4. Le système s'assure que la requête est de type POST et que HTTPS est utilisé.
5. Le système s'assure que l'utilisateur n'est pas expiré.
6. Le système s'assure que l'utilisateur est activé.
7. Le système s'assure que l'utilisateur n'est pas bloqué.
8. Le système déconnecte l'utilisateur.

9. Le système hashé le mot de passe donné et le compare avec celui de l'utilisateur récupéré précédemment.
10. Le système crée une nouvelle session pour l'utilisateur et l'enregistre.
11. Le système enregistre la date et l'heure de connexion
12. Le système enregistre l'adresse IP de l'hôte ayant envoyé la requête. Le système met à jour l'état de connexion de l'utilisateur
13. Le système journalise la connexion de l'utilisateur.
14. Le système retourne l'utilisateur modifié.

Enchaînements d'erreur

E1 : Utilisateur avec nom d'utilisateur donné inexistant

L'enchaînement E1 démarre au point 2 du scénario nominal.

3. Le système journalise l'échec de la connexion avec le message "Login ou mot de passe incorrect".
4. Le système produit une exception avec le même message.
5. Le système refuse la connexion ; le cas d'utilisation se termine en échec.

E2 : Requête pas de type POST ou HTTPS non utilisé

L'enchaînement E2 démarre au point 4 du scénario nominal.

5. Le système met à jour la date et l'heure de la dernière connexion échouée de l'utilisateur.
6. Le système incrémente le nombre de tentatives de connexion échouées pour cet utilisateur.
 - 6.a. Nombre maximal de tentatives de connexions échouées atteint ou dépassé :
 - 6.a.1. Le système bloque l'utilisateur.
 - 6.a.2. Le système journalise le blocage de l'utilisateur avec le message "Utilisateur bloqué" avec le nom de l'utilisateur.
 - 6.a.3. Le système produit une exception avec le même message.
 - 6.b. Nombre maximal de tentatives de connexions échouées non atteint :
 - 6.b.1 Le système journalise l'échec de la connexion avec le message "Tentative de connexion avec une requête non sécurisée".
 - 6.b.2 Le système produit une exception avec le même message.
7. Le système refuse la connexion ; le cas d'utilisation se termine en échec.

E3 : Utilisateur expiré

L'enchaînement E3 démarre au point 5 du scénario nominal.

6. Le système journalise l'échec de la connexion avec le message "Utilisateur expiré" avec le nom de l'utilisateur.
7. Le système produit une exception avec le même message.
8. Le système refuse la connexion ; le cas d'utilisation se termine en échec.

E4 : Utilisateur non activé

L'enchaînement E4 démarre au point 6 du scénario nominal.

7. Le système journalise l'échec de la connexion avec le message "Utilisateur inactif" avec le nom de l'utilisateur.
8. Le système produit une exception avec le même message.
9. Le système refuse la connexion ; le cas d'utilisation se termine en échec.

E5 : Utilisateur bloqué

L'enchaînement E5 démarre au point 7 du scénario nominal.

8. Le système met à jour la date et l'heure de la dernière connexion échouée de l'utilisateur.
9. Le système incrémente le nombre de tentatives de connexion échouées pour cet utilisateur.
- 10.a. Nombre maximal de tentatives de connexions échouées atteint ou dépassé :
 - 10.a.1. Le système bloque l'utilisateur.
 - 10.a.2. Le système journalise le blocage de l'utilisateur avec le message "Utilisateur bloqué" avec le nom de l'utilisateur.
 - 10.a.3. Le système produit une exception avec le même message.
 - 10.a.4. Le système refuse la connexion ; le cas d'utilisation se termine en échec.

E8 : Mot de passe erroné

L'enchaînement E8 démarre au point 9 du scénario nominal.

12. Le système met à jour la date et l'heure de dernière connexion échouée de l'utilisateur.
13. Le système incrémente le nombre de tentatives de connexion échouées pour cet utilisateur.
- 13.a. Nombre maximal de tentatives de connexions échouées atteint :
 - 13.a.1. Le système bloque l'utilisateur.
 - 13.a.2. Le système journalise le blocage de l'utilisateur avec le message "Utilisateur bloqué" avec le nom de l'utilisateur.
 - 13.a.3. Le système produit une exception avec le même message.
 - 13.a.4. Le système refuse la connexion ; le cas d'utilisation se termine en échec.
- 13.b. Nombre maximal de tentatives de connexions échouées non atteint :
 - 13.b.1 Le système journalise l'échec de la connexion avec le message "Login ou mot de passe incorrect".
 - 13.b.2 Le système produit une exception avec le même message. en échec.
14. Le système refuse la connexion ; le cas d'utilisation se termine en échec.

Post-condition(s)

- L'utilisateur en question est authentifié sur l'application.

Exigences non fonctionnelles

- L'application doit être hébergée sur un serveur protégé par un firewall anti DDoS.

►Diagramme d'activités

50

4.2.12.3 Cas d'utilisation "Déconnexion utilisateur"

► Description textuelle

Sommaire d'identification

Titre : Déconnexion utilisateur

Résumé : Ce cas d'utilisation permet à une application de déconnecter un utilisateur.

Acteur : Application

Responsable : Papa Latyr Mbodj

Description des scénarios

Précondition(s)

— Aucune

Scénario nominal

1. Le système supprime le cookie "Se rappeler de moi".
2. Le système invalide la session contenue dans la requête courante.
3. Le système supprime le cookie contenant l'identificateur de session.
4. Le système met à jour l'état de connexion de l'utilisateur.
5. Le système journalise la déconnexion de l'utilisateur.

Post-condition(s)

— L'utilisateur en question est déconnecté de l'application.

4.2.12.4 Cas d'utilisation "Vérification force mot de passe"

► Description textuelle

Sommaire d'identification

Titre : Vérification force mot de passe

Résumé : Ce cas d'utilisation permet à une application de vérifier qu'un nouveau mot de passe est fort.

Acteur : Application

Responsable : Papa Latyr Mbodj

Description des scénarios

Précondition(s)

— Aucune

Scénario nominal

1. L'application donne le login, l'ancien mot de passe et le nouveau mot de passe.
2. Le système s'assure que le nouveau mot de passe n'est pas nul.
3. Le système s'assure que le nouveau mot de passe ne correspond pas au login.
4. Le système s'assure que le nouveau mot de passe ne contient pas une partie de l'ancien mot de passe (3 caractères).
5. Le système compte le nombre de lettres minuscules contenues dans le nouveau mot de passe.
6. Le système compte le nombre de lettres majuscules contenues dans le nouveau mot de passe.

7. Le système compte le nombre de chiffres contenus dans le nouveau mot de passe.
8. Le système compte le nombre de caractères spéciaux contenus dans le nouveau mot de passe.
9. Le système évalue la force du mot de passe.
10. Le mot de passe est accepté.

Enchaînements d'erreur

E1 : Nouveau mot de passe nul

L'enchaînement E1 démarre au point 2 du scénario nominal.

3. Le système journalise l'invalidité du mot de passe avec le message "Le nouveau mot de passe ne peut pas être nul".
4. Le système produit une exception avec le même message.
5. Le système refuse le mot de passe ; le cas d'utilisation se termine en échec.

E2 : Nouveau mot de passe correspondant au login

L'enchaînement E2 démarre au point 3 du scénario nominal.

4. Le système journalise l'invalidité du mot de passe avec le message "Le nouveau mot de passe ne peut pas correspondre au login".
5. Le système produit une exception avec le même message.
6. Le système refuse le mot de passe ; le cas d'utilisation se termine en échec.

E3 : Nouveau mot de passe contenant une partie de l'ancien mot de passe

L'enchaînement E3 démarre au point 4 du scénario nominal.

5. Le système journalise l'invalidité du mot de passe avec le message "Le nouveau mot de passe ne peut pas contenir une partie de l'ancien mot de passe".
6. Le système produit une exception avec le même message.
7. Le système refuse le mot de passe ; le cas d'utilisation se termine en échec.

E4 : Mot de passe faible

L'enchaînement E4 démarre au point 9 du scénario nominal.

10. Le système journalise l'invalidité du mot de passe avec le message "Le nouveau mot de passe n'est pas long ou non complexe".
11. Le système produit une exception avec le même message.
12. Le système refuse le mot de passe ; le cas d'utilisation se termine en échec.

Post-condition(s)

- Le nouveau mot de passe est accepté.

Exigences non fonctionnelles

- L'application doit définir une bonne politique de mots de passe.

► Diagramme d'activités

La force du mot de passe est calculé en considérant que la taille minimale d'un mot de passe est de 4 caractères. Et pour que ce mot de passe soit fort, il faudrait qu'il contienne 1 lettre minuscule, 1 lettre majuscule, 1 chiffre et 1 caractère spécial. Sa force est de $(1+1+1+1) * 4$ (nombre de caractères du mot de passe) ce qui donne 16. La force minimale est ainsi de 16.

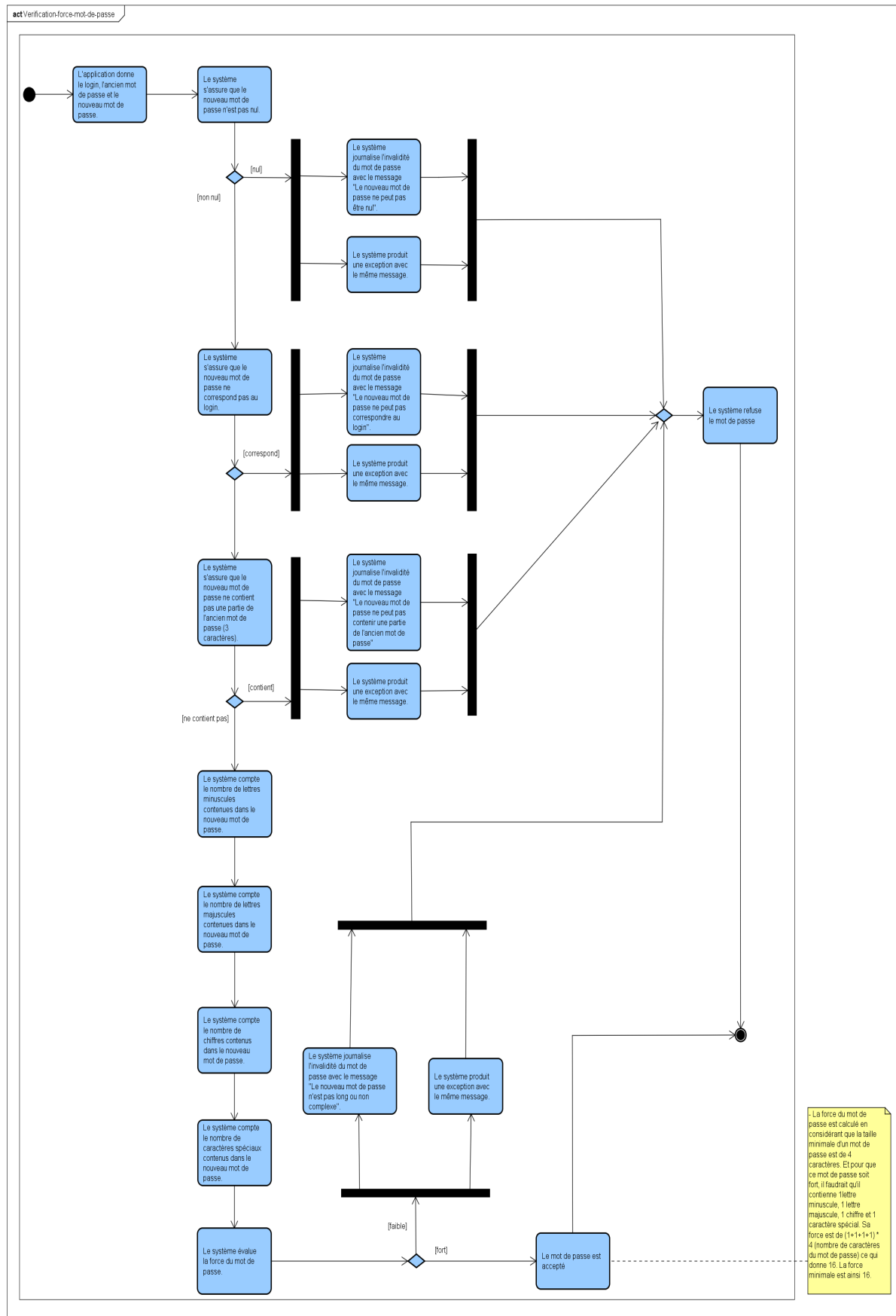


FIGURE 4.16 – Diagramme d'activités du cas "Authentification utilisateur"

4.2.12.5 États d'un utilisateur

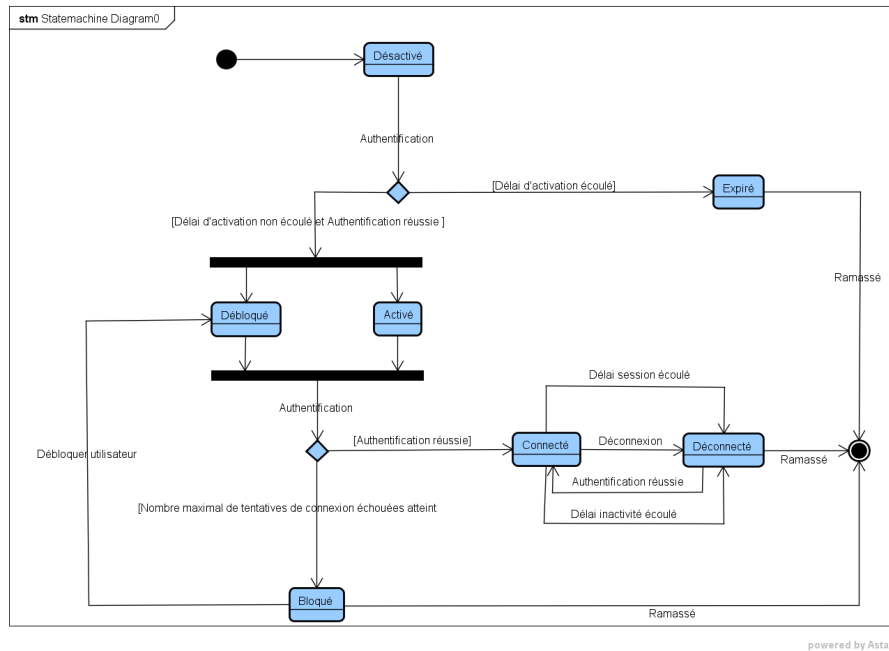


FIGURE 4.17 – Diagramme d'états-transition d'un utilisateur

4.2.13 Sous-système "Cryptographie"

4.2.13.1 Diagramme de cas d'utilisation

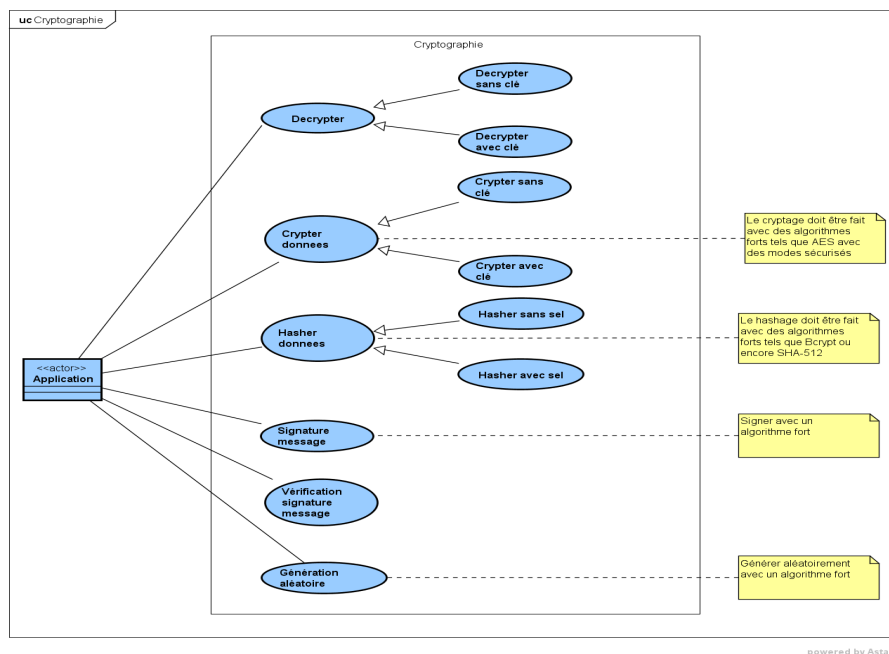


FIGURE 4.18 – Diagramme de cas d'utilisation du sous-système "Cryptographie"

*

4.2.14 Sous-système "Encodage"

4.2.14.1 Diagramme de cas d'utilisation

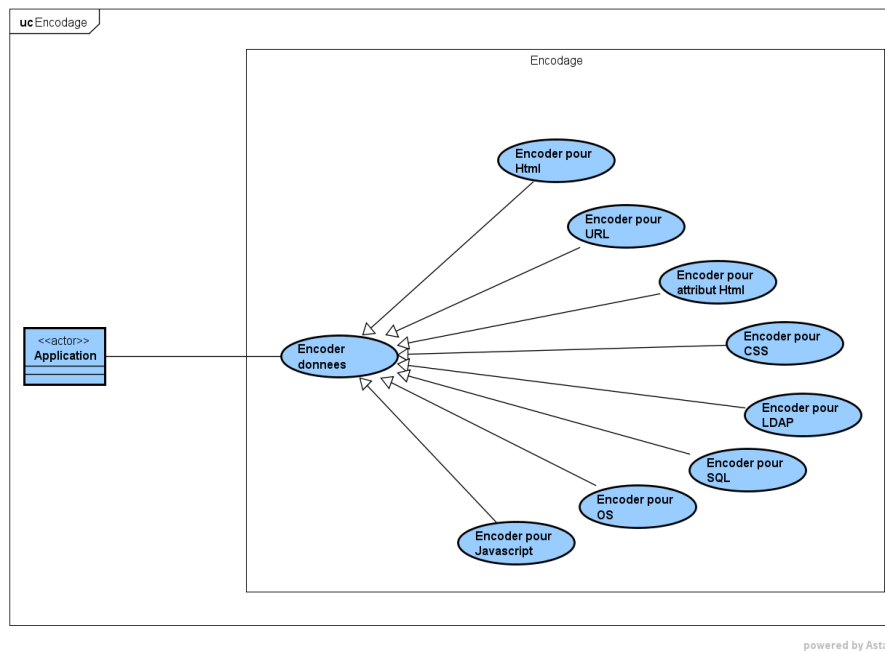


FIGURE 4.19 – Diagramme de cas d'utilisation du sous-système "Encodage"

4.2.15 Sous-système "Validation"

4.2.15.1 Diagramme de cas d'utilisation

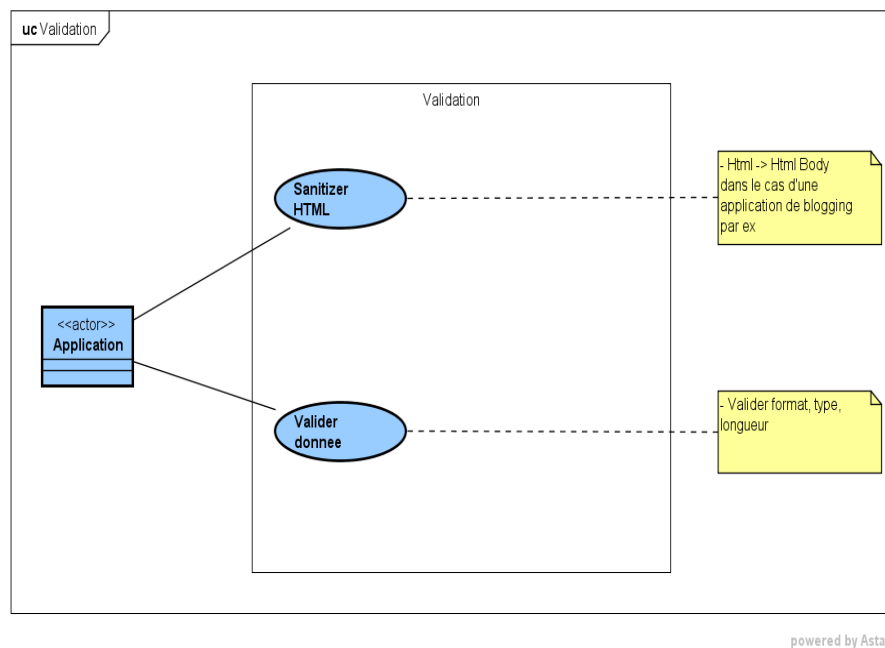


FIGURE 4.20 – Diagramme de cas d'utilisation du sous-système "Validation"

4.2.15.2 Cas d'utilisation "Valider donnée"

► Description textuelle

Sommaire d'identification

Titre : Valider donnée

Résumé : Ce cas d'utilisation permet à une application d'obtenir à partir d'une valeur donnée .

Acteur : Application

Responsable : Papa Latyr Mbodj

Description des scénarios

Précondition(s)

— Aucune

Scénario nominal

1. L'application donne le login, l'ancien mot de passe et le nouveau mot de passe.
2. Le système s'assure que le nouveau mot de passe n'est pas nul.
3. Le système s'assure que le nouveau mot de passe ne correspond pas au login.
4. Le système s'assure que le nouveau mot de passe ne contient pas une partie de l'ancien mot de passe (3 caractères).
5. Le système compte le nombre de lettres minuscules contenues dans le nouveau mot de passe.
6. Le système compte le nombre de lettres majuscules contenues dans le nouveau mot de passe.
7. Le système compte le nombre de chiffres contenus dans le nouveau mot de passe.
8. Le système compte le nombre de caractères spéciaux contenus dans le nouveau mot de passe.
9. Le système évalue la force du mot de passe.
10. Le mot de passe est accepté.

Enchaînements d'erreur

E1 : Nouveau mot de passe nul

L'enchaînement E1 démarre au point 2 du scénario nominal.

3. Le système journalise l'invalidité du mot de passe avec le message "Le nouveau mot de passe ne peut pas être nul".
4. Le système produit une exception avec le même message.
5. Le système refuse le mot de passe ; le cas d'utilisation se termine en échec.

E2 : Nouveau mot de passe correspondant au login

L'enchaînement E2 démarre au point 3 du scénario nominal.

4. Le système journalise l'invalidité du mot de passe avec le message "Le nouveau mot de passe ne peut pas correspondre au login".
5. Le système produit une exception avec le même message.
6. Le système refuse le mot de passe ; le cas d'utilisation se termine en échec.

E3 : Nouveau mot de passe contenant une partie de l'ancien mot de passe

L'enchaînement E3 démarre au point 4 du scénario nominal.

5. Le système journalise l'invalidité du mot de passe avec le message "Le nouveau mot de passe ne peut pas contenir une partie de l'ancien mot de passe".
6. Le système produit une exception avec le même message.
7. Le système refuse le mot de passe ; le cas d'utilisation se termine en échec.

E4 : Mot de passe faible

L'enchaînement E4 démarre au point 9 du scénario nominal.

10. Le système journalise l'invalidité du mot de passe avec le message "Le nouveau mot de passe n'est pas long ou non complexe".
11. Le système produit une exception avec le même message.
12. Le système refuse le mot de passe ; le cas d'utilisation se termine en échec.

Post-condition(s)

- Le nouveau mot de passe est accepté.

Exigences non fonctionnelles

- L'application doit définir une bonne politique de mots de passe.

► Diagramme d'activités

4.2.16 Sous-système "HTTP"

4.2.16.1 Diagramme de cas d'utilisation

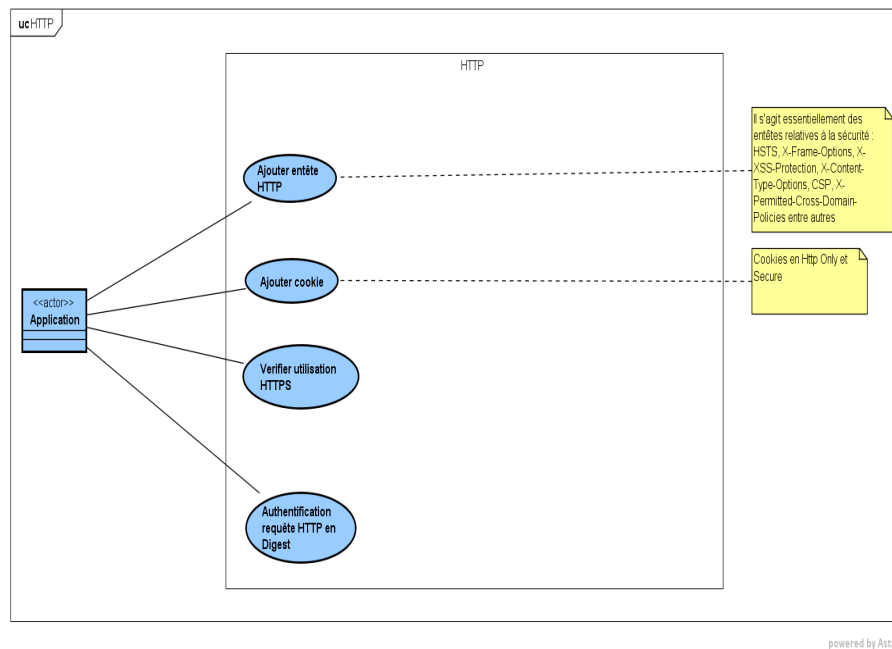


FIGURE 4.21 – Diagramme de cas d'utilisation du sous-système "HTTP"

4.2.16.2 Cas d'utilisation "Ajouter cookie"

► Description textuelle

► Diagramme d'activités

4.2.17 Sous-système "Interpréteurs"

4.2.17.1 Diagramme de cas d'utilisation

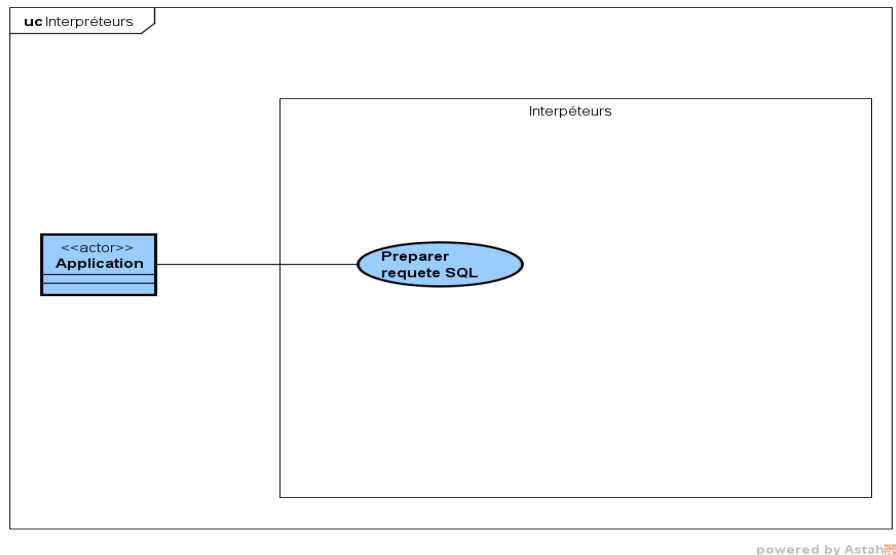


FIGURE 4.22 – Diagramme de cas d'utilisation du sous-système "Interpreteurs"

4.2.18 Sous-système "Logging"

4.2.18.1 Diagramme de cas d'utilisation

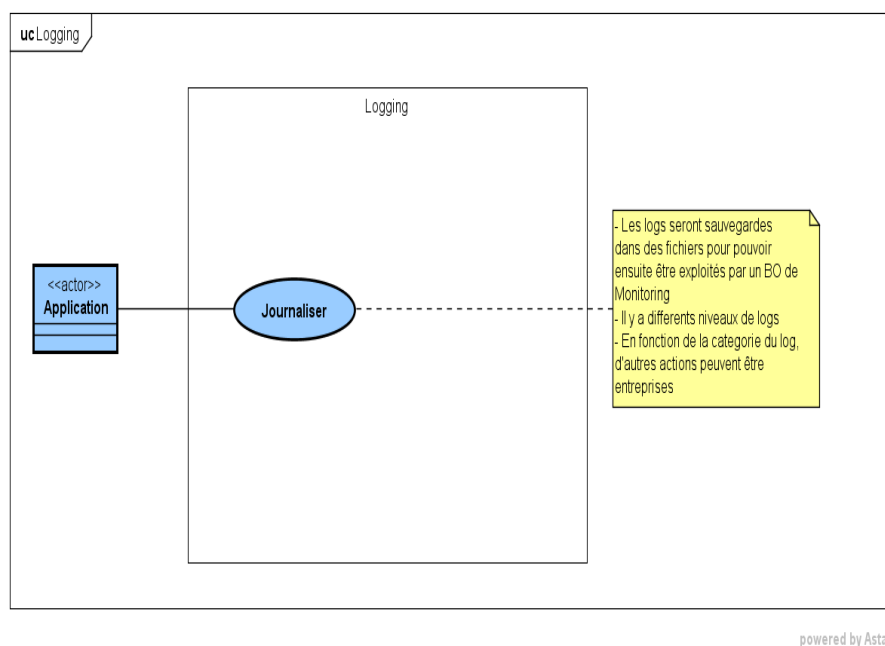


FIGURE 4.23 – Diagramme de cas d'utilisation du sous-système "Gestion de la journalisation et de la surveillance insuffisantes"

4.2.19 Sous-système "Gestion des composants"

4.2.19.1 Diagramme de cas d'utilisation

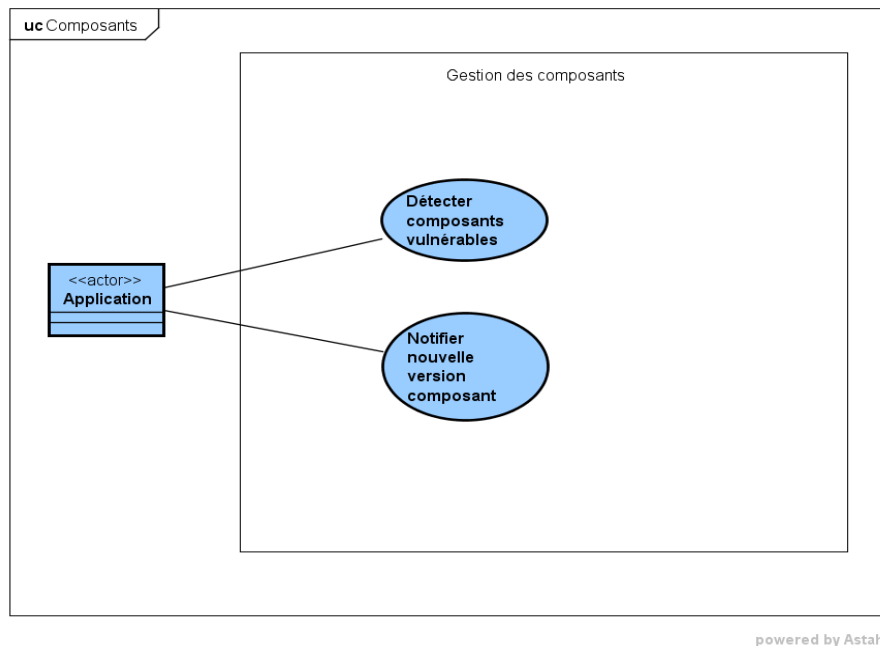


FIGURE 4.24 – Diagramme de cas d'utilisation du sous-système "Gestion de la journalisation et de la surveillance insuffisantes"

4.2.20 Diagramme de classes

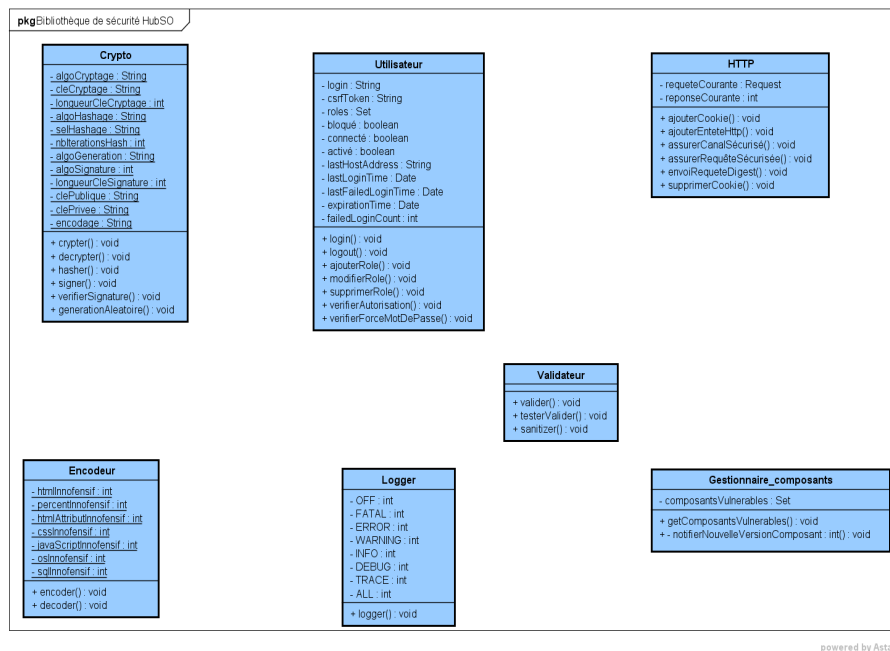


FIGURE 4.25 – Diagramme de classes d'analyse de système

4.3 Conception

4.3.1 Architecture Technique

Première partie

Réalisation

Table des matières

2	Historique	
2.1	Genèse	14
2.2	Seconde Guerre mondiale et guerre froide : grand tournant de l'histoire de la sécurité informatique	14
2.3	Vers un usage massif d'Internet	17
3	Contexte	
3.1	Contexte juridique	18
3.2	Contexte technique	20
4	Owasp	
4.1	Présentation	22
4.2	Origines	22
4.3	Contexte	23
4.4	Organismes concurrents	23
4.4.1	Mitre Corporation	23
4.4.2	Sans Institute	23
4.4.3	PCI Standard Council	24
4.4.4	Web Application Security Consortium	24
4.5	Projets phares	24
4.6	Top 10 Owasp	25
4.6.1	Présentation	25
4.6.2	Démarches Concurrentes	26

Deuxième partie

Bilan et Perspectives

Table des matières

5	Méthodologie de développement	
5.1	Qu'est ce qu'une méthodologie de développement ?	29
5.2	Intérêt d'une méthodologie	29
5.3	Catégories de méthodologies de développement	29
5.4	Choix d'une méthodologie de développement	30
5.5	Intérêt d'une modélisation	31
5.6	Présentation d'UML	31
5.7	Diagrammes UML	32
6	Spécifications et Analyse des besoins	
6.1	Spécifications	34
6.1.1	Spécifications fonctionnelles	34
6.1.2	Spécifications non fonctionnelles	37
6.2	Analyse	37
6.2.1	Package Gestion des injections	38
6.2.2	Package Gestion des violations de gestion d'authentification	39
6.2.3	Package Gestion des expositions de données sensibles	40
6.2.4	Package Gestion des attaques sur les entités XML externes	40
6.2.5	Package Gestion des violations de contrôle d'accès	41
6.2.6	Package Gestion des mauvaises configurations de sécurité	42
6.2.7	Package Gestion des XSS	42
6.2.8	Package Gestion des désérialisations non sécurisées	43
6.2.9	Package Gestion des utilisations de composants vulnérables	44
6.2.10	Package Gestion de la journalisation et de la surveillance insuffisantes	44
6.2.11	Système global	45
6.2.12	Sous-système "Utilisateurs"	48
6.2.13	Sous-système "Cryptographie"	55
6.2.14	Sous-système "Encodage"	56
6.2.15	Sous-système "Validation"	56

6.2.16	Sous-système "HTTP"	58
6.2.17	Sous-système "Interpréteurs"	59
6.2.18	Sous-système "Logging"	59
6.2.19	Sous-système "Gestion des composants"	60
6.2.20	Diagramme de classes	60
6.3	Conception	61
6.3.1	Architecture Technique	61
6.3.2	Diagramme de déploiement	61
6.3.3	La bibliothèque ESAPI	61
6.3.4	Diagramme de classes de conception	62

CONCLUSION

Annexe

Top 10 Owasp : Explicitation

A1 : 2017 – FAILLE D'INJECTION

Les failles d'injection telles que les injections SQL, NoSQL, OS et LDAP sont fréquentes dans les applications Web. L'injection se produit quand des données provenant de l'utilisateur sont envoyées à un interpréteur en tant qu'élément faisant partie d'une commande ou d'une requête. Les données hostiles de l'attaquant dupent l'interpréteur afin de l'amener à exécuter des commandes fortuites, à changer des données, etc.

A2 : 2017 – VIOLATION DE GESTION D'AUTHENTIFICATION

Les fonctions applicatives relatives à l'authentification et la gestion de session ne sont souvent pas mises en œuvre correctement, permettant aux attaquants de compromettre les mots de passe, clés, jetons de session, ou d'exploiter d'autres failles d'implémentation pour s'approprier les identités d'autres utilisateurs.

A3 : 2017 – EXPOSITION DE DONNEES SENSIBLES

L'exposition de données sensibles peut se produire lorsque des fonctions de sécurité adéquates ne sont pas appliquées sur les données ou sont appliquées de façon incorrecte permettant ainsi aux attaquants de dérober des informations sensibles telles que des mots de passe, des informations de paiement, des adresses ou toute autre information pouvant être d'une certaine valeur pour l'attaquant. Les données sensibles doivent être bien protégées à la fois au stockage et durant leur transport et des précautions particulières doivent être prises lorsqu'elles sont échangées avec un navigateur Web.

A4 : 2017 – ATTAQUE XXE

Une attaque XXE est un type d'attaque contre un analyseur syntaxique XML. Cette attaque se produit lorsqu'un fichier XML contenant une référence à une entité externe est traité par un analyseur XML mal configuré. Les attaquants peuvent facilement exploiter les vulnérabilités dans ces analyseurs XML, en leur donnant des fichiers XML malveillants qui peuvent contenir du code indésirable. Cette attaque peut mener à la divulgation de données confidentielles, au déni de service, à la falsification des requêtes côté serveur, à l'analyse des ports du point de vue de la machine où se trouve l'analyseur et à d'autres impacts.

A5 : 2017 – VIOLATION DE CONTRÔLE D'ACCES

Le contrôle d'accès permet de spécifier ce qu'il est permis aux utilisateurs authentifiés de faire sur une application. Pour mettre en place un contrôle d'accès adéquat, il faut s'assurer que de bonnes vérifications d'autorisation et une bonne authentification permettant de dire ce qu'un tel utilisateur peut faire sur l'application soient en place. Les restrictions sur ce que les utilisateurs authentifiés sont autorisés à faire ne sont souvent pas correctement appliquées. Les attaquants peuvent exploiter ces failles pour accéder à des fonctionnalités et/ou données non autorisées, telles

que l'accès aux comptes d'autres utilisateurs, l'affichage de fichiers sensibles, la modification des données d'autres utilisateurs, la modification des droits d'accès, etc.

A6 : 2017 – MAUVAISE CONFIGURATION DE SECURITE

La sécurité d'une application Web ne concerne pas seulement le code. D'après l'Owasp, la mauvaise configuration de sécurité est le problème le plus souvent rencontré. Ceci est généralement le résultat de configurations par défaut non sécurisées, de configurations incomplètes, d'un stockage cloud ouvert, d'en-têtes HTTP mal configurés, de messages d'erreur détaillés contenant des informations sensibles, entre autres. Une sécurité renforcée nécessite un ensemble de configurations correctes et sécurisées déployées pour les applications, les frameworks, les serveurs, les bases de données et le code. De même, toutes ces configurations doivent être maintenues à jour.

A7 : 2017 – CROSS-SITE SCRIPTING (XSS)

Les failles XSS se produisent lorsqu'une application accepte des données non fiables et les envoie à un browser web sans validation appropriée. XSS permet à des attaquants d'exécuter du script dans le navigateur de la victime afin de détourner des sessions utilisateur, défigurer des sites web, insérer du contenu hostile, effectuer des attaques par phishing, et prendre le contrôle du navigateur de l'utilisateur en utilisant un script malicieux. Le script malicieux est habituellement écrit en JavaScript, mais n'importe quel langage de programmation supporté par le navigateur de la victime est un moyen d'exécution de cette attaque.

A8 : 2017 – DESERIALISATION NON SECURISEE

La sérialisation est le processus consistant à transformer un objet en un format pouvant être restauré plus tard. Les objets sont le plus souvent sérialisés afin d'être sauvegardés ou d'être transmis dans le cadre d'une communication. La désérialisation est le processus inverse, c'est-à-dire le fait de prendre des données structurées à partir d'un certain format et de les reconstruire en un objet. Une désérialisation non sécurisée conduit souvent à l'exécution de code distant, et même si les failles de désérialisation n'aboutissent pas à l'exécution de code distant, elles peuvent être utilisées pour effectuer des attaques, y compris des attaques d'injection et d'escalade de privilèges.

A8 : 2017 – DESERIALISATION NON SECURISEE

La sérialisation est le processus consistant à transformer un objet en un format pouvant être restauré plus tard. Les objets sont le plus souvent sérialisés afin d'être sauvegardés ou d'être transmis dans le cadre d'une communication. La désérialisation est le processus inverse, c'est-à-dire le fait de prendre des données structurées à partir d'un certain format et de les reconstruire en un objet. Une désérialisation non sécurisée conduit souvent à l'exécution de code distant, et même si les failles de désérialisation n'aboutissent pas à l'exécution de code distant, elles peuvent être utilisées pour effectuer des attaques, y compris des attaques d'injection et d'escalade de privilèges.

A9 : 2017 – UTILISATION DE COMPOSANTS VULNERABLES

Les composants logiciels, bibliothèques et frameworks utilisés dans les applications Web proviennent le plus souvent de la communauté open source et doivent être utilisés avec prudence au cas où des vulnérabilités s'y cacheraient. En effet certaines versions d'un composant peuvent être sujettes à diverses vulnérabilités qui pourraient avoir été corrigées dans les versions les plus récentes. Une fois qu'une vulnérabilité est révélée, les failles sont rendues publiques. Ces failles peuvent ensuite être utilisées pour compromettre avec succès la version vulnérable d'un composant et par le même biais, les applications l'utilisant.

A10 : 2017 – LOGGING ET MONITORING INSUFFISANTS

Les événements tels que les tentatives de connexion réussies et infructueuses, l'adresse IP des connexions entrantes, les événements importants tels que les transactions de grande valeur doivent être enregistrés et surveillés régulièrement. Ce faisant, l'on peut comprendre tout ce qui se passe sur l'application et être prêt à réagir en cas d'attaque. Autrement, il peut être très difficile de répondre à une attaque ou de connaître l'origine d'une certaine faille.

4.4 Le Protocole SSL

SSL Ce protocole vient en réponse à la préoccupation croissante de la sécurité sur Internet et tire profit des nouveaux algorithmes de chiffrement tels que l'AES venu remplacer le DES et jugé très sécurisé. L'objectif du protocole SSL est de créer un canal de données sécurisé entre le client et le serveur. SSL fournit des améliorations de sécurité au protocole HTTP utilisé jusqu'alors. SSL assure 3 choses : - la confidentialité avec des mécanismes de chiffrements - l'intégrité avec le hachage des données transmises - l'authentification avec l'utilisation de certificats Les certificats Pour être sûr que la clé publique provient bien de celui que l'on croit, on utilise une autorité tierce (appelé le tiers de confiance). Cette autorité est celle qui va générer une clé publique certifiée par exemple pour un serveur Web, puis c'est ensuite elle qui garantira à tout demandeur (par exemple le client web) que la clé publique envoyée appartient bien à celui qui le prétend (au serveur Web). La garantie qu'une clé publique provient bien de l'émetteur qu'il prétend être, s'effectue donc via un certificat d'authenticité émanant d'une autorité de certification (AC), le tiers de confiance. Un certificat est un simple fichier informatique délivré par une autorité de certification qui contient : - la clé publique liée à la clé privée de son détenteur et des informations sur son identité; - le nom distinctif de l'autorité de certification; - la signature électronique (chiffrement de l'empreinte par clé privée) de l'autorité de certification. C'est ce certificat qui permet d'initialiser une connexion SSL. SSL consiste en 2 protocoles : - SSL Handshake protocol : avant de communiquer, les 2 programmes SSL négocient des clés et des protocoles de chiffrement communs. - SSL Record protocol : Une fois négociés, ils chiffrent toutes les informations échangées et effectuent divers contrôles. La négociation SSL (« handshake ») Au début de la communication le client et le serveur s'échangent : - la version SSL avec laquelle ils veulent communiquer, - la liste des méthodes de chiffrement (symétrique et asymétrique) et de signature que chacun connaît (avec longueurs de clés), - les méthodes de compression que chacun connaît, - des nombres aléatoires, - les certificats. Client et serveur essaient d'utiliser le protocole de chiffrement le plus

puissant et diminuent jusqu'à trouver un protocole commun aux deux. Une fois que cela est fait, ils peuvent commencer à échanger des données. La communication SSL (« record ») Avec SSL, l'expéditeur des données : • découpe les données en paquets, • compresse les données, • signe cryptographiquement les données, • chiffre les données, • les envoie. Celui qui réceptionne les données : • déchiffre les données, • vérifie la signature des données, • décompresse les données, • réassemble les paquets de données. SSL utilise : - un système de chiffrement asymétrique (comme RSA ou Diffie-Hellman). Vous pouvez Ce système est utilisé pour générer la clé principale qui permettra de générer des clés de session. - un système de chiffrement symétrique (DES, 3DES, IDEA, RC4...) en utilisant les clés de session pour chiffrer les données. - un système de signature cryptographique des messages (HMAC, utilisant MD5, SHA...) pour s'assurer que les messages ne sont pas corrompus. C'est lors de la négociation SSL que le client et le serveur choisissent les différents systèmes qu'ils utiliseront tout au long de leur communication. 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 infailible, 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.

BIBLIOGRAPHIE

- [1] Alex Corenthin.
Cours de sécurité des systèmes d'information - partie 1.
page 5, 2018.
- [2] Bienvenue dans le monde du cryptage.
<http://wallu.pagesperso-orange.fr/pag-cryptage.htm>.
- [3] Introduction à la sécurisation des applications web.
<https://blog.xebia.fr/2010/12/10/introduction-a-la-securisation-des-applications-web/>.
- [4] Signature numérique.
https://fr.wikipedia.org/wiki/Signature_num%C3%A9rique.
- [5] Nombre d'utilisateurs actifs mensuels de whatsapp dans le monde d'avril 2013 à décembre 2017 (en millions).
<https://fr.statista.com/statistiques/564832/nombre-d-utilisateurs-actifs-mensuels-de-wha>
- [6] Baromètre utilisateurs.
<https://www.consumerbarometer.com/en/trending/?countryCode=US&category=TRN-NOFILTER-ALL>.
- [7] Marcus Pinto Dafydd Stuttard.
The Web Application Hacker's Handbook : Finding and Exploiting Security Flaws, Second Edition.
Wiley Inc., second edition binder edition.
- [8] Gervais Mendy.
Ingénierie de la cryptographie.
page 5, 2018.
- [9] The history of application security testing – part 1.
<https://www.checkmarx.com/2017/02/27/history-application-security-testing/>.
- [10] F. J. Corbató.
Introduction and overview of the multics system.
- [11] Multics b2 security evaluation.
- [12] The history of penetration testing.
<https://resources.infosecinstitute.com/the-history-of-penetration-testing/#gref>.

- [13] Arpanet.
<https://icannwiki.org/ARPANET>.
- [14] By Larry Boettger.
The morris worm : How it affected computer security and lessons learned by it.
2000.
- [15] David D. Clark Robert E. Kahn Leonard Kleinrock Daniel C. Lynch Jon Postel Larry G. Roberts Stephen Wolf Barry M. Leiner, Vinton G. Cerf.
Brief history of the internet.
1997.
- [16] Dr.Mouhamadou LO.
La Protection des données à caractère personnel en Afrique, Réglementation et régulation.
Baol Editions, 9 2017.