



Mémoire de fin d'étude pour l'obtention du diplôme
de Post-Graduation Spécialisée en Sécurité Informatique

Promo 2014/2015

Thème

Authentification et Gestion des Droits d'Accès dans une Application Java. Cas d'étude : Gestion des Laissez-Passer

Elaboré par :

- Mr. BENSLIMANE Ali

Encadré par :

- Dr. NOUALI Omar, DSI, CERIST
- CA. KRINAH Abdelghani, DSI, CERIST

Soutenu devant le jury :

- M^{elle} ZEGHACHE Lynda, Présidente
- M^r BOUCENNA Fateh, Examineur
- M^r AMIRA Abdelouahab, Examineur

Remerciements

Nous tenons tout d'abord à remercier Dieu le tout puissant de nous avoir permis de réaliser ce travail et de nous avoir donné la force et la patience d'accomplir ce modeste travail.

En seconde lieu, nous tenons à remercier notre promoteur Dr :MOUALL Omar pour son aide, nous tenons à remercier particulièrement notre Co-promoteur Mr : KRINATH AbdElGhani, pour sa grande patience, ses encouragements, ses orientations et ses conseils précieux durant toute la période du travail.

Non vifs remerciements vont également aux membres du jury pour l'intérêt qu'ils ont porté à notre recherche en acceptant d'examiner notre travail et l'enrichir par leurs propositions.

Et je remercie spécialement le directeur du Cérist monsieur BADACHE, le responsable du département de la formation Monsieur BOUDIN et la responsable de la formation PGS Melle CHAOUL Hind et en particulier tout le personnel du service de la formation du Cérist.

Enfin, nous tenons également à remercier toutes les personnes qui ont participé de près ou de loin à la réalisation de ce travail.

Dédicace

C'est grâce à dieu le tout puissant et par sa grâce que je dédie ce modeste travail à :

Monsieur le DGSN et Monsieur le DPF. En leurs souhaitant la santé, le succès et tout le bonheur.

A mon cher père M, source de sacrifice. Pour ta Tendresse, ton soutien, tes conseils et tes encouragements. Veuillez trouver dans ce travail l'expression et le témoignage de mon attachement, ma reconnaissance et mon respect. Qu'ALLAH t'accorde la santé et la longue vie.

A ma très chère maman F, raison de mon existence. Pour tes Sacrifices, ton soutien, ta générosité et ta tendresse. Tu étais toujours là près de moi pour me soutenir, m'encourager et me guider avec tes précieux conseils. Aucun mot ne saurait exprimer ma grande reconnaissance, ma gratitude et mon profond amour. Qu'ALLAH te garde et te procure une bonne santé et une longue vie.

A mes chères sœurs F et son marie R et ses enfants, et K et son marie M et ses enfants, pour leur patience, soutien et leurs sentiments d'amour aux moments les plus difficiles. Je vous souhaite plein de succès, de joie et de bonheur. Que dieu vous garde et illumine vos chemins.

A mes frères et ses femmes et ses enfants, pour le respect qu'ils m'ont toujours accordé.

A tous les membres de ma grande famille du A à Z sans oublier aucune personne,

A tous mes collègues de travail du proche et du loin. En leurs souhaitant la santé, le succès et tout le bonheur.

A ma femme et mes petits enfants : AM, M, J, L et H qui sont toujours étant à mes cotés même dans tous les moments.

Et à tous ceux qui m'aiment.

BENSLIMANE Ali.

Sommaire

Liste des Figures	v
Liste des Tableaux	vii
Introduction Générale	1
Partie I : Etude de la sécurité des applications et du contrôle des droits d'accès	3
Introduction	3
Chapitre 1 : La sécurité des application	4
Introduction	4
1. Notions de base.....	4
1.1. C'est quoi une application	4
1.2. C'est quoi la sécurité	5
1.3. C'est quoi la sécurité informatique	5
1.4. C'est quoi la sécurité de l'information	5
1.5. Qu'est ce que l'information.....	5
1.6. Confidentialité.....	5
1.7. Intégrité.....	5
1.8. Disponibilité	5
1.9. Actif	5
1.10. Menace	5
1.11. Agent de Menace.....	5
1.12. Vulnérabilité	5
1.13. Risque	5
1.14. Impact.....	6
1.15. Exposition	6
1.16. Attaque	6
1.17. Contre-mesure.....	6
2. Les principaux concepts de l'OWASP	7
2.1. Définition de l'OWASP	7
2.2. Qu'est-ce qu'un risque de sécurité applicatif	8
2.3. Analyse des besoins sécurité	8
2.4. La Méthodologie d'évaluation des risques OWASP.....	9
3. Les principaux risques de sécurité touchant les applications.....	9
3.1. Injection	10
3.2. Violation de Gestion d'Authentification et de Session	10
3.3. Cross-Site Scripting(XSS).....	10
3.4. Références directes non sécurisées à un objet.....	10
3.5. Mauvaise configuration sécurité.....	10
3.6. Exposition de données sensibles	10
3.7. Manque de contrôle d'accès au niveau fonctionnel.....	11
3.8. Falsification de requête intersite(CSRF).....	11
3.9. Utilisation de composants avec des vulnérabilités connues	11
3.10. Redirections et renvois non validés.....	11
4. Analyse du risque de la Violation de Gestion d'authentification et de Session	12
4.1. Les vulnérabilités de la gestion d'authentification et session.....	12
4.2. Exemple de scénarios d'attaque	13
5. Manque de contrôle d'accès au niveau fonctionnel	13
5.1. Les vulnérabilités du manque de contrôle d'accès.....	14
5.2. Exemple de scénarios d'attaque	14
Conclusion.....	15

Chapitre 2 : Concepts de bases sur l'authentification et le contrôle d'accès	16
Introduction	16
1. Présentation de l'authentification	17
1.1. Identification et authentification	17
1.2. Facteurs d'authentifications	18
1.3. Méthodes de vérification	19
1.4. Les principaux protocoles d'authentification	20
1.6. Enjeux de l'authentification	24
2. Présentation du contrôle d'accès	25
2.1. Les types de contrôles d'accès	26
2.2. Les fonctionnalités des contrôles d'accès	26
2.3. Les Méthodes de contrôle d'accès	27
2.4. Des éléments fondamentaux dans le contrôle des droits d'accès	32
Conclusion	37
Partie II : Etude du langage Java et des APIs dédiées à la sécurité	38
Introduction	38
Chapitre 3 : Java et la sécurité	39
Introduction	39
1. Présentation de Java	39
1.1. L'environnement de développement de Java	40
1.2. Les concepts de base de la programmation en Java	40
2. Caractéristiques de Java	43
3. Les APIs de Java dédiées à la sécurité	45
3.1. La sécurité dans les spécifications du langage	45
3.2. La sécurité dans le contrôle des droits d'une application	45
3.3. La sécurité dans les APIs du Java	47
4. Principaux outils de sécurité fournis avec le SDK	48
5. Principaux packages de sécurité du java	49
Conclusion	50
Partie III : Conception d'une solution de gestion des droits d'accès basée sur utilisateur	51
Introduction	51
Chapitre 4 : Formalisation et analyse de la problématique et choix de la solution proposée	52
Introduction	52
1. Cadre général du projet	52
2. Spécification des besoins du projet	52
3. Extraction de quelques règles de base à partir du sujet	53
4. Architecture globale de la solution	54
5. Choix des composants adéquats à la solution proposée	54
5.1 Le processus d'authentification	55
1.2. Le processus du contrôle d'accès	56
6. Présentation du cas d'étude « Gestion de laissez-passer	58
6.1. Contexte générale du cas d'étude	58
6.2. Architecture globale du cas d'étude	59
6.3. Modèle relationnel du cas d'étude	60
6.4. Les fonctionnalités minimums de chaque profil de la personne	61
6.5. La liste des permissions prédéfinis dans l'application métier	63
Conclusion	65
Chapitre 5 : Modélisation et conception de la solution	66
Introduction	66
1. Aperçu sur l'UML	66
1.1. Les principaux diagrammes de l'UML	66
1.2. La démarche de conception à suivre	67

2.	Etape d'élaboration de diagramme de cas d'utilisation	67
2.1.	L'identification des acteurs	67
2.2.	L'identification des cas d'utilisation	68
3.	Elaboration de diagramme de séquence	71
3.1.	Diagramme de séquence de l'authentification	72
3.2.	Diagramme de séquence de Gérer les rôles	73
3.3.	Diagramme de séquence de gérer les droits d'accès	74
4.	Etape d'élaboration de diagramme des classes	75
4.1.	Descriptions des classes	75
4.2.	Diagramme de classe	76
5.	Le Modèle Relationnel	80
5.1.	Règles de passage du modèle objet à un modèle relationnel	80
5.2.	La transformation du diagramme de classes en modèle relationnel	80
	Conclusion.....	81

Partie IV : Mise en œuvre et intégration de la solution à une application Java 82

Introduction	82
--------------------	----

Chapitre 6 : Présentation de l'environnement de développement.....83

Introduction	83
1. Environnement matériel.....	83
2. Langage de programmation Java	83
3. L'environnement de développement intégré (IDE) NetBeans	83
4. L'outil de conception ArgoUML	84
5. Le système de gestion de base des données MySQL	84
6. Le Workbench	84
7. Le langage SQL	85
8. Le driver JDBC	85
Conclusion.....	86

Chapitre 7 : Présentation générale de l'applicatif de la solution87

Introduction	87
1. Description globale de l'interface principale de l'application.....	87
2. Fenêtre de l'authentification des utilisateurs	88
3. Principaux espaces de l'application métier	88
4. Principaux interfaces de l'espace de l'administrateur de la solution	92
Conclusion.....	97

Conclusion de la partie	98
-------------------------------	----

Conclusion Générale	99
----------------------------------	-----------

Références bibliographiques	viii
--	-------------