

Mémoire de fin d'études

Pour l'obtention du diplôme de Post Graduation Spécialisée en

SECURITE INFORMATIQUE

Thème

**CONCEPTION ET DEVELOPPEMENT D'UNE
APPLICATION WEB SECURISEE POUR
L'EVALUATION DE LA PAPS**

(Prime d'Amélioration des Performances Scientifiques)

Présenté par :

- **BOUHEDIR Hamza.**
- **KASSA BAGHDOUCHE Mohammed.**

Dirigé par :

- **Mr. NOUALI Omar (CERIST).**
- **Mme. BENSTTITI Imène (CERIST).**

Devant le jury :

- **Mme BENMEZIANE Souad, présidente.**
- **Mr BOUCENNA Fateh, examinateur.**
- **Mr KRINAH Abdelghani, examinateur.**

Année : 2015

Remerciements

Nous tenons à remercier vivement, en premier lieu, nos encadrateurs Mr NOUALI Omar, et Mme BESETTITI Imène pour leur patience, sympathie et conseils. Ils ont toujours su nous guider et nous conseiller. Leur confiance en nos capacités était pour nous une grande source de motivation.

Un grand merci est adressé à l'ensemble des enseignants de notre formation PGS/SI. Ils étaient toujours à la disposition des élèves. Nous n'oublions pas de remercier tous les membres du service formation du CERIST.

Nous remercions aussi les membres du jury qui ont accepté de juger notre travail.

A tous ceux qui nous ont aidé dans notre tâche, nous leur dirons merci.

Encore mille fois merci.

Dédicace

*C'est avec un grand plaisir que Je dédie ce travail aux êtres qui me
sont les plus chers*

*À mes précieux parents pour leur amour, affection et
compréhension.*

*Mon père pour sa patience, ses encouragements et ses sacrifices.
Ma mère pour l'éducation qu'elle m'a inculquée et toutes les peines
qu'elle s'est données pour ma réussite.*

*A ma grande mère et mon grand-père, que Dieu leur accorde une
saine et longue vie*

A mes chères soeurs

A ma famille

A Wissem et Abdelouahed

À tous mes amis et collègues de la promotion

À mes collègues, en particulier :

Cdt HAMMADACHE Mustapha, Nabila et Samy

A Mon binôme Mohammed et toute sa famille.

*A Ceux qui remplissent mon coeur, sans que ma plume ne puisse
les porter dans ce simple Dédicace*

HAMZA

Dédicace

Avec un immense plaisir, Je dédie ce modeste travail:

A la mémoire de mes chères parents, pour ses sacrifices depuis qu'ils m'ont mis au monde jusqu'au dernier instant de leurs vies.

A ma très chère femme Amira.

A Mes très chers frères: Amar, Naim, Housseem.

A Toute ma famille, particulièrement mon oncle Messoud et sa femme.

A Mon binôme Hamza BOUHEDIR pour sa sagesse et patience infinies.

A Mes amis Abd eloueheb, Charraf eddine, Azzou, Kharzoute, Bilou, Fares, Brahim, et tous les autres.

Toute la promotion PGS 2014.

Résumé

Notre mémoire se concentre sur la conception et la réalisation d'une application Web sécurisée pour le calcul de la prime d'amélioration des performances scientifiques au niveau du CERIST. Cette application fonctionne de la manière suivante : inscription, authentification, remplissage de fiches d'activités semestrielles, évaluation et déconnexion, tous ceci dans un environnement sécurisé.

La sécurité de cette application se base principalement sur le projet OWASP, et spécifiquement sur les TOP 10 des failles de sécurité des applications Web en implémentant les mécanismes nécessaires. Ainsi, d'autres mécanismes sont utilisés pour la sécurisation des serveurs et du trafic échangé.

Ce présent rapport, résumera le déroulement de toutes les étapes du projet.

Mots clés : PAPS, Application Web, Sécurité Web, OWASP.

ملخص

يتمحور تقريرنا حول تصميم و إعداد تطبيق ويب مدعم بآليات الأمن و الحماية من أجل حساب منحة تحسين الكفاءات العلمية للمستخدمين على مستوى مركز البحث و التطوير في الإعلام العلمي و التقني. هذا التطبيق يشتغل على الطريقة التالية : تسجيل، دخول ، ملئ استمارة النشاطات النصف سنوية، تقييم و خروج، و هذا ضمن وسط مؤمن.

تأمين و حماية هذا التطبيق يعتمد بصفة أساسية على المشروع OWASP، و خاصة على الأفضل 10 ثغرات الخاصة بتطبيقات الويب وذلك ببرمجة الآليات اللازمة، وكذا، برمجة آليات أخرى من أجل تأمين و حماية الموزعات و المعلومات المتبادلة.

و هذا التقرير يلخص جميع مراحل المشروع .

Sommaire

INTRODUCTION GENERALE.....	1
----------------------------	---

CHAPITRE I. LE WEB

Introduction	2
1. Définition.....	2
1.1. Les sites statiques	2
1.2. Les sites dynamiques.....	2
2. Serveur d'applications	3
3. Fonctionnement d'un serveur d'applications	3
4. Serveur Web / Serveur d'applications.....	5
5. Le serveur d'applications Tomcat	5
Conclusion.....	7

CHAPITRE II. SECURITE DES APPLICATIONS WEB

Introduction	8
1. Définition.....	9
2. Les besoins de sécurité	10
3. Sécurité des applications web.....	10
3.1. Les risques de sécurité applicatifs	11
3.2. Mécanismes de sécurité des applications Web	11
3.3. Le niveau de sécurité d'une application Web	12
3.3.1. Sécurisation du trafic.....	12
3.3.2. Sécurisation de la base de données	13
3.3.3. Sécurisation au niveau développement des pages Web	16
3.3.4. Sécurisation du serveur Web.....	24
Conclusion.....	25

CHAPITRE III. ÉTUDE DE L'EXISTANT

INTRODUCTION	26
1. Description de l'existant	26
2. Procédure d'évaluation	26
2.1. Critères et facteurs de 1-5 (fixés par l'arrêté n°736 du 15/12/2010).....	26
2.2. Niveau de performance	27
2.3. Coefficient d'importance par responsabilité	27
2.4. Période d'évaluation.....	29
2.5. Système de notation	29
3. Critique de l'existant.....	30
4. Solution proposée	30
5. Étude des besoins.....	31
5.1. Besoins fonctionnels	31
5.1.1. Inscription des utilisateurs.....	31
5.1.2. Consultation et rédaction des rapports	31
5.1.3. Évaluation des rapports	31
5.1.4. Mise à jour de la base de données par l'administrateur	32
5.2. Besoins non fonctionnels	32
5.2.1. Fiabilité.....	32
5.2.2. Gestion des erreurs	32
5.2.3. Ergonomie et bonne Interface	32
5.2.4. Sécurité.....	32
Conclusion.....	33

CHAPITRE IV. ÉTUDE CONCEPTUELLE

Introduction	34
1. Conception générale.....	34
1.1. Cycle de vie	34
1.1.1. Définition	34
1.1.2. Les activités d'un cycle de vie	34
1.1.3. Quelques exemples de modèles de cycles de vie	35

1.2.	Méthodologie de conception	37
1.3.	Conception et architecture.....	37
2.	Conception détaillé.....	38
2.1.	Les diagrammes de cas d'utilisation	38
2.1.1.	Définition	38
2.1.2.	Composition du diagramme de cas	38
2.1.3.	Les acteurs de notre projet	39
2.1.4.	Diagrammes de cas d'utilisation de notre application	40
2.2.	Les diagrammes d'activités	41
2.2.1.	Définition	41
2.2.2.	Composition d'un diagramme d'activités	42
2.2.3.	Les activités de notre application	42
2.2.4.	Les diagrammes d'activité de notre application.....	43
2.3.	Diagramme de séquences	46
2.3.1.	Définition	46
2.3.2.	Composition d'un diagramme de séquences	46
2.3.3.	Les diagrammes de séquences de notre application.....	47
2.4.	Diagramme de classes	51
2.4.1.	Définition	51
2.4.2.	La composition d'un diagramme de classes.....	51
2.4.3.	Diagramme de classes de notre application	52
2.5.	Schéma Relationnel.....	52
2.6.	Diagramme de déploiement	53
Conclusion.....		54

CHAPITRE V. REALISATION

Introduction	55
1. Environnement de travail.....	55
1.1. Environnement matériel	55
1.2. Atelier de génie logiciel	55
1.2.1. Langage de programmation.....	55
1.2.2. Environnement de développement	55

1.2.3. Outil de Conception	56
1.2.4. Serveur d'application	56
1.2.5. Système de gestion de base de données	56
2. Implémentation.....	56
2.1. Le protocole HTTPS	56
2.1.1. Génération du Keystore.....	57
2.1.2. Création du connecteur SSL.....	57
2.1.3. Forçage d'utilisation de SSL	58
2.2. Sécurisation du serveur d'applications	59
2.3. Sécurisation du serveur de base de données MySQL	61
2.3.1. Sécuriser les accès.....	61
2.3.2. Interdire complètement l'accès distant pour le compte root.....	61
2.3.3. Supprimer les bases de tests	62
2.4. Sécurité au niveau des pages web	62
2.4.1. L'inscription	62
2.4.2. L'authentification	62
2.4.3. Vérification de la session	63
2.4.4. Les injections SQL	63
2.4.5. Référence direct non sécurisé à un objet.....	65
2.4.6. Cross-Site Scripting (XSS).....	66
2.4.7. Falsification de requête inter sites (CSRF)	68
2.4.8. Le contrôle d'accès au niveau fonctionnel	70
2.4.9. Sécurisation des données sensibles	70
3. Présentation de l'application.....	71
3.1. Structure de l'application	71
3.2. La charte graphique	72
3.3. La page d'accueil	74
3.4. L'espace d'inscription	75
3.5. Espace privé	76
3.6. Espace de rédaction du rapport semestriel	77
3.7. Consultation des équipes.....	79
3.8. Consultation de la liste des chercheurs	80

3.9.	Consultations des rapports semestriels.....	80
3.10.	Espace d'évaluation.....	81
3.11.	Espace d'impression : (Exemple : Fiche d'évaluation).....	82
3.12.	Espace d'administration : Menu principal	83
3.13.	Espace d'administration : Gestion des chercheurs	84
3.14.	Espace d'administration : Ajouter une division	84
3.15.	Espace d'administration : Modifier une équipe	85
3.16.	Espace d'administration : Supprimer un projet.....	85
3.17.	Espace d'administration : Consultation des chercheurs	86
Conclusion.....		86
CONCLUSION GENERALE ET PERSPECTIVES		87
BIBLIOGRAPHIE		89
ANNEXES		91
LISTE D'ACRONYMES		104