

République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Centre de Recherche sur l'Information Scientifique et Technique



Mémoire pour l'obtention du diplôme
de Post Graduation Spécialisée en Sécurité Informatique

Thème

METHODES ET OUTILS D'ANALYSE DE CODES

Réalisé par :

- BENAMOR Lotfi
- GHEZAL Abdesselem

Encadré par :

- Mme. BENMEZIANE Souad,
Chargée de recherche

Soutenu devant le jury :

- Dr. TANDJAOUI Djamel, Président.
- Mr. AMIRA Abdelouahab, Examineur.
- Mr. OUADJAOUT Abderaouf, Examineur.

Février 2013

Remerciements

Nous adressons nos vifs remerciements à Mme. BENMEZIANE Souad, notre encadreur et enseignante au CERIST pour son entière disponibilité, ses conseils, ses encouragements et surtout leur modestie.

Nous tenons à remercier le Dr. TANDJAOUI Djamel d'avoir accepté de présider cet honorable jury.

Nous remercions Mr AMIRA Abdelouahab et Mr OUADJAOUT Abderaouf pour nous avoir fait l'honneur de juger notre travail.

Nous remercions notamment tous nos enseignantes et enseignants au CERIST pour nous avoir enrichi nos connaissances dans le domaine de la sécurité informatique.

Nous remercions toutes les personnes qui nous ont aidés afin que nous puissions réaliser ce travail et à leur tête.

Enfin, nous remercions aussi toute l'équipe de l'administration de la formation pour leur entière disponibilité.

.

SOMMAIRE

LISTE DES FIGURES	6
LISTE DES TABLEAUX.....	7
INTRODUCTION GENERALE	1
CHAPITRE I : ANALYSE DE CODE SOURCE : ETAT DE L'ART	3
I.1 INTRODUCTION	4
I.2 QUALITE LOGICIELLE.....	4
I.3 ANALYSE DE CODE SOURCE.....	5
I.4 VULNERABILITES DES LOGICIELS	6
I.4.1 VALIDATION DES ENTREES.....	6
I.4.2 EXCEPTIONS	6
I.4.3 BUFFER OVERFLOWS	7
I.5 ANATOMIE DE L'ANALYSE DE CODE SOURCE	7
I.5.1 PHASE EXTRACTION DES DONNEES	8
I.5.2 PHASE DE LA REPRESENTATION INTERNE	8
I.5.3 PHASE EXPLORATION DE LA REPRESENTATION (ANALYSE).....	13
I.6 LES DOMAINES D'APPLICATION DE L'ANALYSE DE CODE SOURCE.....	13
I.6.1 LA RECHERCHE DES ERREURS DE PROGRAMMATION (DEBOGAGE).....	13
I.6.2 LA DETECTION DE CLONE	14
I.6.3 LA RETRO-INGENIERIE (L'INGENIERIE INVERSE).....	14
I.6.4 LA FIABILITE LOGICIELLE.....	14
I.6.5 LA SECURITE CRITIQUE	14
I.7 LES TYPES D'ANALYSE DE CODE SOURCE	15
I.7.1 STATIQUE VS DYNAMIQUE	15
I.7.2 CORRECT VS COMPLET	15
I.7.3 FLUX SENSIBLE VS FLUX INSENSIBLE	15
I.7.4 CONTEXTE SENSIBLE VS CONTEXTE INSENSIBLE.....	16
I.8 L'ANALYSE STATIQUE DE CODE SOURCE	16
I.8.1 DEFINITION	16
I.8.2 OBJECTIFS	16
I.8.3 TECHNIQUES D'ANALYSE STATIQUE DU CODE SOURCE.....	17
a. Model checking.....	17
b. Analyse du flot de contrôle et flot de données	18
I.8.4 INTERETS DE L'ANALYSE STATIQUE	18
I.8.5 LIMITATIONS DE L'ANALYSE STATIQUE	18
I.9 L'ANALYSE DYNAMIQUE DE CODE SOURCE	19
I.9.1 DEFINITION	19
I.9.2 BESOINS DE L'ANALYSE DYNAMIQUE	19
I.9.3 TECHNIQUES D'ANALYSE DYNAMIQUE DU CODE SOURCE	20
I.9.4 LES AVANTAGES DE L'ANALYSE DYNAMIQUE.....	20
I.9.5 INCONVENIENTS DE L'ANALYSE DYNAMIQUE	20
I.10 L'ANALYSE HYBRIDE DE CODE SOURCE	21
I.10.1. INTRODUCTION	21
I.10.2. APPROCHE COLCOMBET-FRADET	21
I.10.3. SOFT-TYPING.....	22
I.10.4. APPROCHE DE CHANDER ET. AL.....	22
I.11 COMPARAISON ENTRE L'ANALYSE STATIQUE ET L'ANALYSE DYNAMIQUE	23
I.12 CONCLUSION	24

CHAPITRE II: OUTILS D'ANALYSE DE CODE SOURCE	25
II.1 INTRODUCTION.....	26
II.2 LES CRITERES D'EVALUATION DES OUTILS D'ANALYSE DE CODE SOURCE	26
II.2.1 INSTALLATION	26
II.2.2 CONFIGURATION	26
II.2.3 RAPPORT	27
II.2.4 ERREURS TROUVEES	27
II.4 OUTILS D'ANALYSE DYNAMIQUE DU CODE SOURCE.....	27
II.4.1 VALGRIND	27
II.4.2 PYLINT	28
II.5 OUTILS D'ANALYSE STATIQUE DU CODE SOURCE.....	28
II.5.1 OUTILS D'ANALYSE DE CODE SOURCE JAVA.....	28
II.5.2 OUTILS D'ANALYSE DE CODE SOURCE C/C++	29
II.5.3 OUTILS D'ANALYSE DE CODE SOURCE PHP.....	30
II.5.4 OUTILS D'ANALYSE DE CODE SOURCE MULTI-LANGUAGE.....	31
II.5.5 OUTILS D'ANALYSE MICROSOFT .NET	32
II.6 BIBLIOTHEQUE DES OUTILS D'ANALYSE DE CODE SOURCE.....	33
II.7 CONCLUSION	34
CHAPITRE III : LES APPLICATIONS WEB : CODES ET MENACES	35
III.1 INTRODUCTION	36
III.2 DEFINITIONS.....	36
III.3 TECHNOLOGIES	36
III.3.1 CGI/PERL	37
III.3.2 COLDFUSION	37
III.3.3 JAVA.....	37
III.3.4 LAMP.....	38
III.3.5 MICROSOFT .NET	38
III.4 LES TOP 10 - 2010 RISQUES APPLICATIFS SECURITE.....	38
A1- INJECTION SQL	39
A2- CROSS SITE SCRIPTING (XSS)	40
A3- VIOLATION DE GESTION D'AUTHENTIFICATION ET DE SESSION	41
A4- REFERENCES DIRECTES NON SECURISEE A UN OBJET	41
A5- FALSIFICATION DE REQUETE INTER-SITE (CSRF).....	42
A6- MAUVAISE CONFIGURATION SECURITE.....	42
A7- STOCKAGE CRYPTOGRAPHIQUE NON SECURISE	42
A8- DEFAILLANCE DANS LA RESTRICTION DES ACCES A UNE URL.....	42
A9- PROTECTION INSUFFISANTE DE LA COUCHE TRANSPORT.....	42
A10- REDIRECTION ET RENVOIS NON VALIDES	43
III.5 CONCLUSION.....	43
CHAPITRE VI : PARTIE PRATIQUE	44
VI.1 INTRODUCTION	45
VI.2 L'OUTIL D'ANALYSE DE CODE SOURCE RIPS	45
VI.2.1 PRESENTATION DE RIPS	45
VI.2.2 LA TECHNIQUE D'ANALYSE DU RIPS	45
VI.2.3 CONFIGURATION DE RIPS	46
VI.2.4 LA CONSTRUCTION DU MODELE.....	47
VI.2.5 L'INTERFACE WEB DE RIPS	48
VI.3 L'OUTIL D'ANALYSE DE CODE SOURCE YASCA	49
VI.3.1 PRESENTATION DE YASCA	49
VI.3.2 INSTALLATION.....	49
VI.3.3 FONCTIONNEMENT	50

VI.4 APPLICATIONS.....	51
VI.4.1 ANALYSE DE CODE SOURCE DU SITE 1 AVEC RIPS	51
a. Constat des vulnérabilités	54
b. Discussion	55
c. Elimination des vulnérabilités	56
VI.4.2 ANALYSE DE CODE SOURCE DU SITE 2 AVEC RIPS	56
a. Constat des vulnérabilités	58
b. Discussion	58
VI.4.3 ANALYSE DE CODE SOURCE DU SITE1 AVEC YASCA	59
VI.4.4 ANALYSE DE CODE SOURCE DU SITE2 AVEC YASCA	61
VI.5 COMPARAISON ENTRE LES RESULTATS D'ANALYSE DU RIPS ET YASCA:	62
CONCLUSION GENERALE.....	65