

République Algérienne Démocratique et Populaire  
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique  
Université A-MIRA-BEJAIA

Faculté des Sciences Exactes      Département d'Informatique



# Mémoire

Présenté par

*AMIRA Abdelouahab*

Pour l'obtention du diplôme de Magister

Filaire : Informatique

Option : Cloud Computing

Thème

---

Analyse Statique d'Applications Web  
par Interprétation Abstraite

---

Soutenu le :

Devant le jury composé de :

Nom et Prénom

Grade

Mr BADACHE Nadjib

Professeur USTHB

Président

Rapporteur

Examineur

Examineur

Mr OUDJAOUT Abdelraouf

AR CERIST, Alger

Invité

Année Universitaire : 2011/2012

## Résumé

Les applications web utilisent des mécanismes de gestion de session pour pouvoir offrir des fonctionnalités avancées aux utilisateurs. Les attaques qui ciblent ces mécanismes sont considérées parmi les plus critiques selon OWASP. Une attaque par fixation de session fait partie des attaques sur les mécanismes de gestion de session. Le principe d'une attaque par fixation de session est d'amener un utilisateur légitime à utiliser un identifiant de session contrôlé par l'attaquant. Ce dernier va pouvoir usurper l'identité de l'utilisateur légitime sans même connaître ses accreditations.

Dans ce mémoire, nous présentons une nouvelle approche qui permet de vérifier automatiquement si une application Web est vulnérable aux attaques par fixation de session. Notre approche est basée sur l'interprétation abstraite qui est une théorie pour l'approximation de sémantiques de programmes et permet de concevoir des analyses statiques correctes par construction.

Nous présentons aussi le prototype d'un analyseur statique pour le langage PHP basé sur notre approche. Ce prototype nous a permis d'analyser plusieurs applications Web et de démontrer l'efficacité de notre approche.

**Mots clés :** attaques par fixation de sessions, sécurité des applications web, analyse statique de programmes, interprétation abstraite.

## Abstract

Web applications use authentication mechanisms to provide user-friendly content to users. Attacks that target these mechanisms are considered one of the most critical attacks according to OWASP. Among these attacks, we find Session fixation attacks.

In a session fixation attack, the legitimate user is forced to use a session identifier controlled by the attacker. The attacker can then use this session identifier to impersonate the legitimate user without even knowing his accreditations.

In this report, we present a novel approach that permits to verify automatically if a web application is vulnerable to session fixation attacks. Our approach is based on abstract interpretation which is a theory of the approximation of semantics and allows designing static analysers that are fully automatic and sound by construction.

We also present a prototype of a static analyser for the PHP language based on our approach. Testing this prototype on several web applications shows the efficiency of our approach.

**Keywords** : session fixation attacks, web application security, static program analysis, abstract interpretation.

---

## Table des matières

---

<b>Introduction générale</b>	<b>1</b>
Objectifs . . . . .	2
Contribution . . . . .	3
Organisation du mémoire . . . . .	3
<b>I État de l'art</b>	<b>5</b>
<b>1 La sécurité des applications Web</b>	<b>6</b>
1.1 L'évolution des applications Web . . . . .	7
1.2 Les attaques Web . . . . .	7
1.2.1 Open Web Application Security Project (OWASP) . . . . .	8
1.2.2 OWASP Top Ten : description des vulnérabilités . . . . .	9
1.3 Moyens pour sécuriser une application Web . . . . .	12
1.4 Conclusion . . . . .	13

<b>2</b>	<b>La vérification de programmes</b>	<b>14</b>
2.1	Les différentes techniques de vérification de programmes . . . . .	15
2.1.1	Les méthodes non-exhaustives de vérification de programmes informatique	15
2.1.2	Les méthodes exhaustives de vérification . . . . .	16
2.1.2.1	Définition d'une analyse formelle . . . . .	17
2.1.2.2	Analyse correcte et analyse complète . . . . .	18
2.2	Les techniques courantes exhaustives de la vérification de programmes . . . . .	19
2.2.1	Les méthodes déductives . . . . .	19
2.2.2	Le model checking . . . . .	20
2.2.2.1	Phase de modélisation . . . . .	21
2.2.2.2	Phase d'exécution . . . . .	21
2.2.2.3	Phase d'analyse . . . . .	21
2.2.3	L'interprétation abstraite . . . . .	22
2.2.4	Comparaison entre les différentes techniques . . . . .	23
2.3	Conclusion . . . . .	25
<b>3</b>	<b>L'interprétation abstraite</b>	<b>26</b>
3.1	Introduction informelle à l'interprétation abstraite . . . . .	27
3.2	L'interprétation abstraite, formellement . . . . .	29
3.2.1	La sémantique concrète $S[[ \ ]]$ . . . . .	29
3.2.2	La sémantique collectrice $S_{col}[[ \ ]]$ . . . . .	30
3.2.3	Sémantique abstraite $S^{\#}[[ \ ]]$ et approximation . . . . .	34
3.3	Quelques outils basés l'interprétation abstraite . . . . .	35
3.3.1	Astrée . . . . .	35
3.3.2	Clousot . . . . .	36
3.3.3	Coverity . . . . .	37
3.3.4	Polyspace . . . . .	37
3.4	Conclusion . . . . .	38

<b>II</b>	<b>Contribution</b>	<b>39</b>
<b>4</b>	<b>Analyse statique d'applications web par interprétation abstraite pour les attaques fixation de sessions</b>	<b>40</b>
4.1	Attaques sur le mécanisme d'authentification : Les attaques par fixation de session . . . . .	41
4.1.1	Mécanismes de gestion de session dans HTTP . . . . .	41
4.1.2	Principe d'une attaque par fixation de session . . . . .	42
4.1.3	Vérification des vulnérabilités de type fixation de session . . . . .	43
4.1.4	Exemple d'un code vulnérable . . . . .	44
4.2	Travaux existant . . . . .	45
4.3	Une approche exhaustive pour la vérification de la vulnérabilité aux attaques par fixation de sessions . . . . .	46
4.3.1	Sémantique concrète . . . . .	47
4.3.1.1	Syntaxe abstraite . . . . .	47
4.3.1.2	Environnements . . . . .	48
4.3.1.3	Sémantique des expressions . . . . .	50
4.3.2	Sémantique des commandes . . . . .	51
4.3.3	Sémantique collectrice . . . . .	51
4.3.4	Sémantique abstraite . . . . .	52
4.3.4.1	Sémantique abstraite numérique . . . . .	53
4.3.4.2	Sémantique abstraite de sessions . . . . .	53
4.3.4.3	Sémantique abstraite des classes . . . . .	54
4.3.5	Fonctions de transfert . . . . .	55
4.3.5.1	Résolution de classes . . . . .	56
4.3.5.2	Sessions . . . . .	56
4.3.6	Connexions de Galois . . . . .	59
4.3.6.1	Sessions . . . . .	59

---

4.3.6.2	Résolution de classes . . . . .	62
4.3.7	Environnement final et combinaison des abstractions . . . . .	65
4.3.7.1	Monotonicité de $\alpha_1, \gamma_1$ . . . . .	65
4.3.7.2	Connexion de Galois entre $\alpha_1, \gamma_1$ . . . . .	66
4.3.7.3	Connexion de Galois entre $\alpha_2, \gamma_2$ . . . . .	67
4.4	Conclusion . . . . .	67
<b>5</b>	<b>Mise en œuvre</b> . . . . .	<b>69</b>
5.1	Analyse du langage PHP . . . . .	70
5.1.1	Choix du compilateur PHP . . . . .	70
5.1.2	Phc (PHP compiler) . . . . .	71
5.1.2.1	Abstract Syntax Tree . . . . .	72
5.1.2.2	Représentation du langage PHP . . . . .	72
5.1.2.3	Écriture de plugins . . . . .	74
5.2	Conception de l'analyseur statique . . . . .	74
5.2.1	Architecture . . . . .	74
5.2.2	Diagramme de classes . . . . .	77
5.2.3	Limites de Phc . . . . .	77
5.2.4	Résolution de la contrainte d'inclusions dynamiques . . . . .	79
5.2.5	Résolution de la contrainte des fonctions d'inclusions non supportées . . . . .	79
5.2.6	Architecture mise à jour . . . . .	80
5.3	Tests et résultats . . . . .	82
5.3.0.1	Application 1 . . . . .	82
5.3.0.2	Application 2 . . . . .	83
5.3.0.3	Application 4 : CMS cmsmadesimple 1.11.10 . . . . .	83
5.3.0.4	Application 5 : CMS Simple PHP blog 4.6 . . . . .	83
5.3.1	Résultats . . . . .	84
5.4	Conclusion . . . . .	85

---

<b>Conclusion générale et perspectives</b>	<b>86</b>
Conclusion générale . . . . .	86
Perspectives . . . . .	87