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 Examinateur
Mr OUDJAOUT Abdelraouf	AR	CERIST, Alger	Examinateur Invité

Année Universitaire : 2011/2012

Résumé

Les applications web utilisent des mécanismes de gestion de session pour pouvoir offrir des fonctionnalité avancées aux utilisateurs. Les attaques qui ciblent ces mécanismes sont considérées parmi les plus critiques selon OWASP. Une attaque par fixation de session fait parti 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 attaquant. Ce dernier va pouvoir usurper l'identité de l'utilisateur légitime sans même connaître ses accréditations.

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.

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

Table des matières