

ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΡΗΤΗΣ

ΤΜΗΜΑ ΕΠΙΣΤΗΜΗΣ ΥΠΟΛΟΓΙΣΤΩΝ

ΠΑΡΟΥΣΙΑΣΗ / ΕΞΕΤΑΣΗ ΜΕΤΑΠΤΥΧΙΑΚΗΣ ΕΡΓΑΣΙΑΣ

**Σαββόπουλος Αλέξανδρος
Μεταπτυχιακός Φοιτητής**

Τμήμα Επιστήμης Υπολογιστών, Πανεπιστήμιο Κρήτης

Επόπτης Μεταπτυχιακής Εργασίας: Επικ. Καθηγητής, Π. Πρατικάκης

Σ. Ιωαννίδης (επιβλέπων)

Δευτέρα, 22 Μαρτίου 2021 , ώρα 11:00 π.μ.

Join Zoom Meeting

<https://zoom.us/j/93461466895>

“ SecurityAuditor: Ένα XDriver εργαλείο προσανατολισμένο στην ασφάλεια για την αξιολόγηση των Security Header Policies”

Περίληψη

Η ασφάλεια των ιστοσελίδων είναι ένας σημαντικός παράγοντας για μια σωστή λειτουργική ιστοσελίδα. Οι προγραμματιστές των ιστοσελίδων μπορούν να ορίσουν πολιτικές ασφαλείας σε αυτές με σκοπό να αποτρέψουν διάφορες επιθέσεις που μπορούν να αποβούν μοιραίες για τη λειτουργικότητά τους. Ωστόσο, υπάρχουν πολλές περιπτώσεις όπου μπορούν να υπάρχουν εσφαλμένες διατυπώσεις κατά την εφαρμογή αυτών των πολιτικών, οι οποίες μπορούν να αξιοποιηθούν από τους επιτιθέμενους. Αυτό μπορεί να οδηγήσει σε επιθέσεις στις ιστοσελίδες με σκοπό ακόμη και τη διαρροή ιδιωτικών δεδομένων των χρηστών.

Το Selenium είναι ένα πρόγραμμα αυτόματης περιήγησης ιστοσελίδων. Μπορεί να μιμηθεί ενέργειες χρηστών καθώς αυτό μπορεί να ελέγξει ένα πρόγραμμα περιήγησης μέσω των WebDriver. Οι λειτουργίες των χρηστών μπορούν να εκτελεστούν από αυτά τα συστήματα, προκειμένου να συγκεντρωθούν πληροφορίες σχετικά με τις λειτουργίες

των ιστοσελίδων. Ωστόσο, υπάρχουν πολλά προβλήματα που μπορούν να δημιουργηθούν κατά την εκτέλεση αυτών των ενεργειών. Αυτά τα προβλήματα μπορεί να οδηγήσουν σε αποτυχία της εργασίας. Για αυτόν τον λόγο, υπάρχει το σύστημα XDriver που είναι ένα άλλο σύστημα αυτοματισμού προγράμματος περιήγησης. Περιέχει μηχανισμούς που προσφέρουν λύσεις, όταν μια εργασία αποτυγχάνει με σκοπό την επιτυχής ολοκλήρωσής τους. Προσφέρει, επίσης, λειτουργίες του συστήματος Selenium που μειώνουν την πολυπλοκότητα του κώδικα, καθώς αυτές εκτελούν τις ενέργειες του Selenium συστήματος.

Σε αυτή την εργασία υλοποιήθηκε το εργαλείο SecurityAuditor. Αυτό το εργαλείο είναι μέρος του XDriver συστήματος και χρησιμοποίησε λειτουργίες του, με σκοπό την αξιολόγηση των πολιτικών ασφαλείας. Αυτές οι πολιτικές μπορούν να εφαρμοστούν από τους προγραμματιστές των ιστοσελίδων. Εντόπιζε, επίσης, εσφαλμένες συντακτικά διατυπώσεις των πολιτικών που μπορούσαν να μειώσουν την ασφάλεια του ιστότοπου. Χρησιμοποιώντας αυτό το εργαλείο, πραγματοποιήθηκε μια μεγάλης κλίμακας μελέτη για την αξιολόγησή του. Επίσης, μέσα από αυτή την μελέτη ερευνήθηκε, εάν αυτές οι πολιτικές εφαρμόζονταν σωστά από τους προγραμματιστές των ιστοσελίδων. Παρατηρήθηκε ότι οι περισσότεροι ιστότοποι δεν είχαν υλοποιήσει τις πολιτικές, ενώ κάποιες από αυτές εντοπίστηκαν με συντακτικά λάθη ή με γνωστές εσφαλμένες διαμορφώσεις των πολιτικών. Αυτές οι περιπτώσεις μπορούσαν να μειώσουν την ασφάλεια των ιστότοπων.

Η σύγκριση των συστημάτων XDriver και Selenium ήταν μια επιπλέον μελέτη που έγινε σε αυτή την εργασία. Διεξήχθη για την αξιολόγηση των μηχανισμών χειρισμού σφαλμάτων που περιέχει το σύστημα XDriver. Αυτή η αξιολόγηση πραγματοποιήθηκε με την ταυτόχρονη εκτέλεση εργασιών σε έναν σύνολο από ιστοσελίδες και στα δύο προηγούμενα συστήματα. Συμπερασματικά, το σύστημα XDriver έδωσε λύσεις σε πολλά προβλήματα του Selenium συστήματος.

University of Crete

Computer Science Department

M.Sc. Thesis presentation / examination

Savvopoulos Alexandros

Master's Thesis Supervisor: Assistant Professor, P. Pratikakis

S. Ioannidis (Thesis CO-Advisor)

Monday, 22 March 2021, 11:00 a.m.

Join Zoom Meeting

<https://zoom.us/j/93461466895>

“SecurityAuditor: A XDriver Security Oriented Module for the evaluation of Security Header Policies”

Abstract

Website security is an important factor for a properly functional site. The developers can set Security Header policies in order to prevent various attacks that can be fatal to the functionality of the websites. However, there are many policies' misconfigurations which can be exploited by the attackers. These attacks can even lead to the users' private data leaking.

The Selenium is a browser automation framework. It emulates a user website task as it can control the web browsers through WebDrivers. The user's functionalities can be executed by this framework in order to gather information about the websites' functionalities. However, there are many problems which can be created by this framework during the execution of users' tasks. These problems may lead to a task's failure. For this reason there is another browser automation toolset named XDriver framework. It contains mechanisms, which offer solutions for task's failures in order to finish it successfully. It also offers Selenium functionalities to reduce the code complexity as it was built on the top of the Selenium framework.

In this master thesis the SecurityAuditor module was developed. This is an XDriver module that used XDriver functionalities in order to evaluate the Security Header Policies. These policies could be implemented by the websites' developers. It also detected policies' misconfigurations which could reduce the security of the website. Using this module, a large-scale study was conducted in order to evaluate it as well as to investigate if these policies were implemented correctly by the websites' developers. It was observed that most of the domains did not implement these policies and some of the policies were detected with syntax errors or known vulnerabilities (misconfigurations). Therefore, the websites' safety could be reduced.

The comparison of the XDriver with the Selenium framework was another study which was conducted in this thesis. The XDriver error handling mechanisms were evaluated, executing browser users' tasks in a number of domains for both of these frameworks. It was concluded that the XDriver solved many Selenium exceptions.