تحسين نهج ضبابية الصندوق الأسود لتطبيقات الويب الحديثة

اسيل سعيد الصاعدي

إشراف: أ.د. أميمة بنت عمر بامسق و د.عبيرعادل الهذلي

المستخلص:

تلعب تطبيقات الويب دوراً أساسياً في حياتنا اليومية فهي جزء لا يتجزأ من العديد من تفاعلاتنا الرقمية، مثل التعليم والرعاية الصحية والخدمات المالية. ويعد أمان هذه التطبيقات أمراً بالغ الأهمية وذلك لما تحتويه من بيانات خاصة وحساسة تمت مشاركتها من قبل المستخدم والتي بدورها أصبحت هدفاً جذاباً للمخترقين وعرضة لأنواع مختلفة من الهجمات التي تعمل على استغلال ثغراتها الأمنية. وكما يعد اكتشاف تلك الثغرات بطريقة آلية أمراً صعباً نظراً لما تتضمنه التطبيقات من التعقيدات المتزايدة والاعتماد على السمات الديناميكية والتي غالباً تتم برمجتها باستخدام الجافا سكربت. إن وجود مثل هذه التعقيدات والسمات تحسن من أداء التطبيقات وسهولة استخدامها إلا انها تجعل التحليل الأمني لتطبيقات الويب أكثر تعقيداً وصعوبة. في هذه الاطروحة، نقدم نهجاً يعالج تلك الصعوبات وذلك باستخدام التحليل الديناميكي لعمل محاكاة لعمليات الاختراق الحقيقة من خلال استخدام تقنيات الصندوق الأسود للتقييم الأمني والتي تهدف إلى استكشاف أعمق للبنية التحتية في التطبيقات. إضافة إلى ذلك، يقوم نهجنا بإجراء تحليل لعمليات التحقق من صحة النموذج من جانب العميل والذي بدوره يؤدي إلى تعزيز التغطية وبالتالي الوصول إلى المزيد من الثغرات الأمنية. تم تطبيق النهج في نظام وقمنا بتقييم فعاليته من خلال استخدام تطبيقات الويب الحقيقة المفتوحة المصدر. تمكن النظام من الوصول إلى ٢٠٧ من العناوين الفريدة وإرسال ١٠٢ نموذجاً بشكل صحيح وتم العثور عن ٣٢ ثغرة أمنية. إضافة إلى ذلك، فقد أظهرت المقارنة التفصيلية مع تقنيات الصندوق الأسود أن هذا النظام تفوق على عليها من خلال عدة جوانب وهي: التغطية، وعدد الثغرات الأمنية المكتشفة والأداء.

An Enhanced Black-Box Fuzzing Approach for Modern Web Applications

by

Aseel Saeed Alsaedi

Supervisor: Prof. Omaimah Omar Bamasag and Dr. Abeer Adil Alhuthali

Abstract:

Web applications are essential in our daily lives as they are embedded in many digital interactions, such as education, health care, and financial services. The security of these applications is critical because we frequently share private and sensitive data through the application, which attracts malicious actors to target web applications for exploiting vulnerabilities. However, proactively detecting these vulnerabilities automatically is challenging because of the increasing complexity and heavy dependency on dynamic features, often programmed in JavaScript. While this dynamism and complexity enable increasingly beneficial applications, they also make security analyses of the web applications harder. In this thesis, we propose an approach that addresses the difficulties presented in modern web applications by utilizing a dynamic analysis technique in a black-box fashion to explore the applications' space. In addition, our approach performs client-side validation analyses resulting in enhanced coverage that detects a broader range of vulnerability types. We evaluated the implementation of our method using real-world modern web applications. The system discovered 207 unique URLs, successfully submitted 102 web forms, and safely exploited 32 security vulnerabilities automatically. A detailed comparison with state-of-art black-box fuzzing approaches suggests that our system outperforms others in the coverage, number of detected vulnerabilities, and performance.

.