論文審査の要旨および学識確認結果

報告番号	甲　第　　号	氏　名	高松 勇輔

論文審査担当者：				
	主査	慶應義塾大学教授	博士(理学)	河野 健二
	副査	慶應義塾大学教授	博士(工学)	高田 眞吾
		慶應義塾大学准教授	博士(工学)	遠山 元道
		慶應義塾大学教授	工学博士	山口 高平

(論文審査の要旨)

学士 (工学), 修士 (工学) 高松勇輔君提出の学位請求論文は,「ウェブアプリケーションのロジックに依存する攻撃の自動生成による脆弱性検査に関する研究」と題し, 全 6 章で構成されている.

ウェブアプリケーションの脆弱性は深刻な不正攻撃につながっており, 個人情報の流出や金銭的な被害など多くの事例が報告されている. このような脆弱性を排除するため, 開発段階において, 脆弱性スキャナなどを用いた検査が行われている. 脆弱性スキャナなどを用いると, 脆弱性や攻撃手法に関する知識をもたない開発者でも利用しやすいという利点がある. しかし, 既存の検査手法では, ウェブアプリケーションのロジックに依存した攻撃に対する脆弱性を発見することができない. ウェブアプリケーションのロジックとは, ウェブアプリケーションが持つさまざまな機能を動作させるために必要な手順や情報のことである. 既存の検査手法では, ウェブアプリケーション毎に異なったロジックについて, その情報を獲得できないため, ロジックに依存した攻撃には対応が難しい. 本論文では, 開発段階における検査工程から自動的にロジックに関する情報を獲得し, それによってロジックに依存した攻撃に対する脆弱性検査を可能にする手法を提案している.

第 1 章では, 脆弱性検査の必要性と現状について論じ, 本研究の目的と論文の構成について述べている.

第 2 章の関連研究では, 脆弱性を検査するための既存手法について述べている. 既存手法ではウェブアプリケーションのロジックに関する情報を取得できないため, ロジックに依存した攻撃に対する脆弱性検査が不十分であることを示している.

第 3 章では, ウェブアプリケーションのロジックに依存した攻撃を自動的に実行することで, 脆弱性を検査する手法を提案している. ウェブアプリケーションの開発段階における利用を想定し, 通常の検査工程からアプリケーションに依存したロジックに関する情報を自動的に獲得する. このようにして獲得した情報から, ロジックに依存したさまざまな攻撃を自動的に実行し脆弱性の有無を検査する.

第 4 章と第 5 章では, 第 3 章で提案した手法の有効性を示すため, 従来の手法では自動検査が難しい Cross-Site Request Forgery (CSRF), session fixation, visual clickjacking という 3 種類の攻撃に対し, 脆弱性の自動検査が可能であることを示している. それぞれの攻撃に対して, 脆弱性検査に必要なロジック関連の情報を取得する方法, ロジックに依存した攻撃の生成方法, 脆弱性の有無の判定手法を述べている. また, 実際に提案手法の実装を行い, さまざまなウェブサイトで実運用されているオープンソースのウェブアプリケーションに対して脆弱性検査を行っている. その結果, 5 種類のウェブアプリケーションから 11 個の CSRF の脆弱性, 6 個の session fixation の脆弱性を検出し, 4 種類のウェブアプリケーションから 26 個の visual clickjacking の脆弱性を検出し, 提案手法の有効性を示している.

第 6 章では, 本論文で得られた成果をまとめており, 第 4 章と第 5 章で得られた結果から, 提案手法によって, ウェブアプリケーションのロジックに依存した攻撃に対し, 脆弱性検査が可能であることを結論づけている. さらにこれらの研究成果の展望についても述べている.

以上, 本論文は, ウェブアプリケーションのセキュリティを向上させるため, 既存手法では検査の難しい脆弱性に対する検査手法を実現しており, その貢献は工学上寄与するところが少なくない. よって, 本論文の著者は博士 (工学) の学位を受ける資格があるものと認める.

学識確認結果	学位請求論文を中心にして関連学術について上記審査会委員で試問を行い, 当該学術に関し広く深い学識を有することを確認した. また, 語学（英語）についても十分な学力を有することを確認した.

※　○○　○○には審査担当者氏名、△△△△には、「上記審査会委員」等と記載する。