Webアプリケーションを安全にするフレームワークの新しい機能

久保田 康平

2021 年 1 月 15 日

情報知能工学専攻

概 要

本論文は，Webアプリケーションのセキュリティ機能向上を目的にしている．そのために本論文では，Webアプリケーション開発者が実装するコードを実行時に自動的に解析し，必要ならば修正する機能をWebアプリケーションフレームワークに持たせることを提案し，実装して評価を行う．Webアプリケーションはインターネットを通して世界中から誰でも接続でき，対話的に通信できるという特徴から様々な攻撃の対象になる．また，インターネットの普及に伴いWebアプリケーションの重要性は増し，同様にWebアプリケーションの防御もまた重要になっている．脆弱性攻撃は，Webアプリケーションの設計上の欠点や仕様上の問題点である脆弱性を利用する攻撃である．脆弱性攻撃の対策の一つは，Webアプリケーションに脆弱性を作らないことであり，そのためWebアプリケーション開発者はWebアプリケーションフレームワークを利用することがある．Webアプリケーションフレームワークは，Webアプリケーション開発において利用することが多いメソッドを持つライブラリである．それらのメソッドを利用すること

で効率よくアプリケーションを開発することができる．セキュリティ面において，Web アプリケーションフレームワークが提供するメソッドは脆弱性対策がなされているものが多い．したがって，Web アプリケーションフレームワークを利用した方が，利用しない時と比較して効率的にセキュアな Web アプリケーションを開発しやすい．一方で，開発者は常に完全にセキュアなコードを書くことはできないため，Web アプリケーションフレームワークを利用して，脆弱性がある Web アプリケーションを実装してしまうことがある．その理由の一つが，Web アプリケーション開発者が Web アプリケーションフレームワークを適切に利用できないことである．Web アプリケーション開発者が，フレームワークのメソッドが持つセキュリティ機能を正しく理解していなかったり，セキュリティ機能を持つメソッドを知らなかったりすることによって脆弱な Web アプリケーションが実装される．この問題に対して本論文では，Web アプリケーション開発者が実装したソースコードを修正する機能を持つ Web アプリケーションフレームワークを提案する．提案手法を実証し評価を行った結果，この機能は実装されたコードの脆弱性を一部修正でき，レスポンスタイムは提案手法を適用しなかった場合とほとんど変わらないことを確認した．実装された修正関数の蓄積は将来のアプリケーションのセキュリティの向上に寄与できるものである．

目 次

図 目 次

表 目 次

第1章

はじめに

本論文は，Web アプリケーションのセキュリティ機能向上を目的にしている．その目的の達成のために，アプリケーション開発者が実装したプログラム中の関数や引数を解析し，実行時にその関数に脆弱性があった時には修正することができる Web アプリケーションフレームワークを提案，実装し評価する．

Web アプリケーションセキュリティは，セキュリティ分野において重要である．インターネットの普及に伴い，Web システムは様々な場所や階層において様々な攻撃にさらされている．Web システムへの攻撃のうちアプリケーション層への攻撃の多くはアプリケーションのプログラムが持つ論理的な問題が原因である．そのため Web アプリケーション開発者は攻撃を回避するために，アプリケーションの論理的な問題や設計上の欠点である脆弱性を作らない実装をする必要がある．一方で，Web アプリケーション開発者は常にセキュアなコードを記述することはできず，脆弱性を残す実装をすることがある．加えて Web アプリケーション層に

はセキュリティに関するプロトコルや標準的な仕様がないため，Web アプリケーションの安全性は，Web アプリケーション開発者のセキュリティに関する知識や技術に依存する．これらの Web アプリケーションの問題を解決しセキュリティを向上するために，Web アプリケーションの自動防御手法として Web アプリケーションファイアウォール（WAF）や Web アプリケーションフレームワークの利用などが検討されている．

WAF は，Web アプリケーションを脆弱性攻撃から保護するためのシステムである．WAF は Web アプリケーションとクライアントの間に配置され，クライアントからのリクエストを監視し，リクエストが攻撃リクエストかどうかを検証する機能を持つ．攻撃を検出した場合，そのリクエストを遮断もしくは無毒化することで，Web アプリケーションへの攻撃の影響を低減する．WAF は Web アプリケーションを修正することなく，脆弱性攻撃を低減することが可能であるため，アプリケーションを直接修正できない時に有効な対策である．一方で WAF はアプリケーションを修正しないので，アプリケーション内の脆弱性を根本的に修正できないという欠点がある．また WAF はアプリケーション内の論理的な設計や仕様を知らないため，一部の脆弱性を対策することが難しい．WAF は通常，特殊文字を含むリクエストを攻撃として検出する．したがって，リクエスト内に特殊文字を含まない攻撃を WAF が検出することは難しい．

Web アプリケーションフレームワークは，Web アプリケーションを効率よく開発するために，Web 開発に多用される機能を関数やメソッドとして提供するライブラリである．自動防御手法としては，クロスサイトスクリプティング（XSS）や SQL インジェクション（SQLi）のようなインジェクション攻撃に対する入力検証と自動サニタイズという機能を提

供していることがある．自動サニタイズとは特殊文字をエスケープする機能であるサニタイズを Web アプリケーションフレームワークが行う一部の Web アプリケーションフレームワークが持つ機能である．自動サニタイズの長所は Web アプリケーションのセキュリティの一部を Web アプリケーションフレームワークが負担することが可能なことである．自動サニタイズによって Web アプリケーション開発者はサニタイズについて考慮することなく，セキュアな Web アプリケーションを実装することが可能になる．一方で自動サニタイズは限定的な対策で，インジェクション攻撃ではない攻撃を対策することが難しい．

Web アプリケーションの自動防御は Web アプリケーションの論理的な設計を検証し脆弱性の影響を低減する機能を持たないため，一部の攻撃を自動的に防御することができない．具体的には，Web アプリケーションの不適切な認証への攻撃を自動で対策する手法を Web アプリケーションフレームワークは持たない．不適切な認証は，アプリケーションの利用者が権限を所持していると主張した時に，アプリケーションがその主張が適切かどうかを証明しない，もしくは不適切に証明する脆弱性である．

この問題を解決するために，本論文ではアプリケーション開発者が実装したソースコードを解析し，必要であれば修正する Web アプリケーションフレームワークである VH フレームワーク（Vulnerability Handling Framework）を提案する．VH フレームワークは，Web アプリケーション開発者が記述したソースコードを実行開始時に解析する．

実行開始時に

第2章

関連研究

2.1　論文1

2.2　論文2

2.3　論文3

第3章

提案手法

この章では，アプリケーションフレームワークの仕組みについての説明したのちに，本論文で提案するアプリケーションフレームワークがソースコードを修正する手法について記述する．

3.1　アプリケーションフレームワーク

アプリケーションフレームワークは

3.2　ソースコードの修正

ほげ

第4章

実装

第5章

実験

第6章

結果

第7章

考察

第8章

おわりに