

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 22 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

第1章	はじめに	1
第2章	関連研究	5
2.1	論文1	5
2.2	論文2	5
2.3	論文3	5
第3章	提案手法	6
第4章	実装	9
第5章	実験	10
第6章	結果	11
第7章	考察	12
第8章	おわりに	13

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 フレームワークは脆弱なソースコードの条件とそのソースコードを修正するプログラムを持っている。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静的に解析することで脆弱性を検出する。その後、脆弱なソースコードを保護するための関数を挿入したり、安全な関数に置き換える。挿入された関数は実

行中にアプリケーションを動的に検証し、攻撃を検出すると無毒化する。この提案手法の貢献は、Web アプリケーション開発者のソースコードを自動で修正するので、そのアプリケーションの論理的設計の不備を修正することが可能であることである。したがって VH フレームワークは通常の Web アプリケーションフレームワークでは対策できない認証の不備に対する攻撃の低減を行うことが可能である。

実効開始時に VH フレームワークは Web アプリケーション開発者のソースコードに 4 つの工程を行う。まずはじめに、Web アプリケーション開発者が実装したソースコードを実行可能な状態で VH フレームワークに格納する。次に、格納されたソースコードを解析しやすいよう形式に修正する。第三に形式を変更したソースコードを解析し修正する。そして最後に修正されたソースコードを実行可能な状態に戻す。

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解析して脆弱性の影響を緩和することが可能であるかを確認するために実験を行った。その結果、不適切な認証と SQL インジェクションの脆弱性を修正できることを確認した。

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

VH フレームワークは，コールバック関数を解析し必要であれば修正する．コールバック関数とは Web アプリケーションへのリクエストを基に，Web サーバー側で行う処理を記述した関数である．VH フレームワークは，リクエストのメソッドとパスによってコールバック関数を呼び出す．リクエストのパスとメソッドが一致するコールバック関数が存在する場合そのコールバック関数が呼び出され，その戻り値をレスポンスボディとしてクライアントに送信する．一致するコールバック関数が存在しない場合 VH フレームワークが HTTP ステータスコードを 404，レスポンスボディを Not Found にしてクライアントにレスポンスを送信する．

VH フレームワークは実行開始時に 4 つの工程によってコールバック関数を修正する．まず最初に，コールバック関数，リクエストパス，メソッドを一つの辞書式データとして VH フレームワークに格納する．この辞書式データはリストの一要素として VH フレームワークに格納される．この時点ではコールバック関数は活動中のオブジェクト，つまり実行可能

なバイナリ形式のオブジェクトである。次にコールバック関数を修正しやすくするために、VH フレームワークはコールバック関数の形式を活動中のオブジェクトから抽象構文木 (Abstract Syntax Tree: AST) に変更する。AST は、プログラムを実行可能なバイナリ状態にする処理の途中で取得される中間生成物であり、ソースコードから実行可能なオブジェクトを生成するために必要ない部分を削除した表現である。AST はバイナリよりもプログラムの論理的設計を把握しやすいため、コールバック関数の解析と修正が容易である。3 つ目がコールバック関数の解析と修正である。VH フレームワークはコールバック関数を解析し修正する脆弱性ハンドリング関数を持っている。脆弱性ハンドリング関数は格納されたコールバック関数のリストを引数として受け取りコールバック関数のリストを返す。脆弱性ハンドリング関数はコールバック関数のリストを受け取ると、脆弱性ハンドリング関数を持っている脆弱なコールバック関数の条件とその条件を満たすコールバック関数の修正方法に基づき脆弱性を検出・修正する。脆弱性ハンドリング関数はコールバック関数のリストを受け取るため、コールバック関数間の論理的な設計の誤りを脆弱性の条件にすることが可能である。具体的には、あるコールバック関数では権限を求めたページを他のコールバック関数でも同じ権限が必要になるように修正することが可能になる。この手法を用いることで、従来では自動で対策が困難な不適切な認証の不備を低減できる。また脆弱性ハンドリング関数は脆弱性ごとに複数の関数で実装されている。この実装方法により新たな脆弱性が発見された時、その脆弱性の影響を低減する新たな関数を追加で実装することが可能である。修正が終わると、VH フレームワークはコールバック関数のリストを返す。最後にコールバッ

ク関数を実行可能なオブジェクトに変更することで，修正されたコールバック関数がリクエストを処理することが可能になる．

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