VADDY

膨大な攻撃統計データから導き出された Webアプリ脆弱性検査ツールの最適な“バランス”とは

～87%の攻撃への対策を「平均12分のスキャン」と「月額2万円」で実現～

October 2018

bit forest
https://www.bitforest.jp

株式会社ビットフォレスト

目次

はじめに

規模の大小を問わず、公開 Web サイトへの攻撃は絶えることがありません。日々の攻撃の痕跡は運営している Web サイトのアクセスログからもうかがい知れますが、すべての攻撃データを分析･分類し、それを元に防御対策を行うのは非常に難易度が高く、限られたサイトでしか実現できないことでしょう。

今回は実際の攻撃の統計データを元に、優先的に留意すべき Web アプリケーション脆弱性と、脆弱性検査ツールにおける要素同士のトレードオフの関係性を見ていきます。

これがリアル！
Webアプリケーションへの攻撃傾向

弊社はクラウド型 Web Application Firewall（WAF）の Scutum を開発・運用 (*1) しています。Scutum は 2500 以上 (*2) のサイトを守り、実際の攻撃データを分析して防御力の向上に役立てています。

2017 年 1 月に Scutum で観測したすべての攻撃リクエスト約 37 万件を分類したデータを見ると、Web アプリケーションへの攻撃の中でも、攻撃者側に高い技術力を必要としないものが上位を占めています。その上位 5 種類は以下の攻撃です。

- SQL インジェクション
- クロスサイトスクリプティング（XSS）
- ディレクトリトラバーサル
- リモートファイル実行（RFI）
- コマンドインジェクション

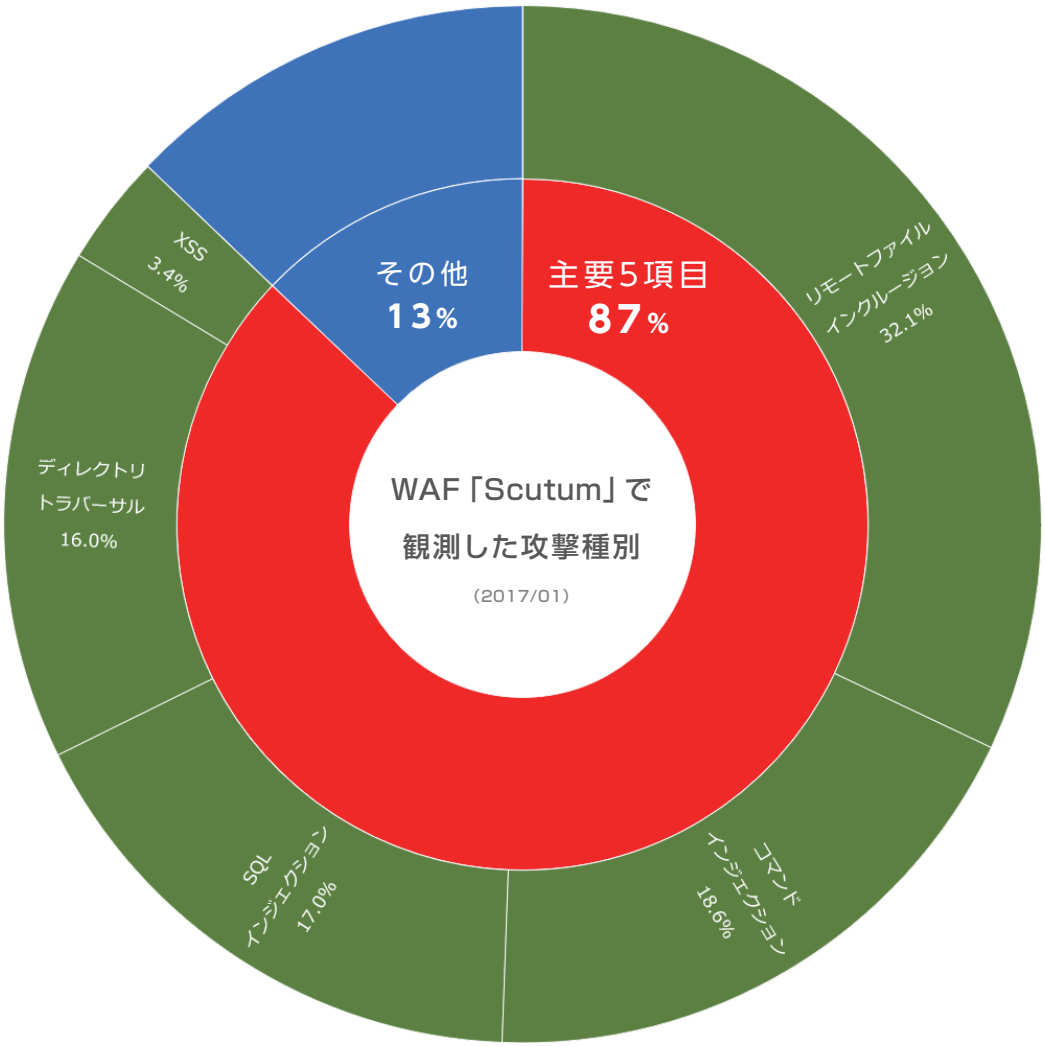
これらは、情報漏洩やサイト改ざんなどのリスクが高い攻撃で、発生時の被害も甚大です。この 5 種類の攻撃だけで、実際の攻撃リクエスト数全体の 87% を占めます (*3)（*4)。

※次ページグラフを参照

*1：Scutum のサービス提供は株式会社セキュアスカイ・テクノロジー
*2：2017 年 12 月現在
*3：その他にはこのような攻撃が多くなっています。
・バックアップファイルの探索
・バージョン管理ファイル設置の不備を突いた攻撃
これらは公開領域に非公開データを置いていないか探索する攻撃リクエストであり、ファイルの取り扱いにを注意して対応する必要があります。
*4：この攻撃の傾向や順位については、株式会社ジェイピー・セキュアが公開している、Web サイトへの攻撃統計「JP-Secure Labs Report Vol.2」でも同様の傾向が見られます。
https://www.jp-secure.com/document/labs/JP-Secure_labs_Report_Vol.02.pdf

膨大な攻撃統計データから導き出された Webアプリ脆弱性検査ツールの最適な“バランス”とは

～87%の攻撃への対策を「平均12分のスキャン」と「月額２万円」で実現～



これらのデータからも、まず行うべきは上位５種、87%を占める攻撃への対策といえます。残りの13% の攻撃への対策を目指すのであれば、多機能な脆弱性検査ツールや手動診断サービスを利用する必要があり、その実現には一般的に多額の費用と膨大な時間を要します。予算や開発スケジュール、開発サイクル等がマッチしないプロジェクトにおいては、より現実的な選択肢を検討する必要に迫られることでしょう。

以下では、脆弱性検査ツールの特徴について紹介します。手動診断サービスよりは一般的に費用と時間を抑えやすい脆弱性検査ツールですが、タイプによってそのバランスはさまざまです。特に、Webアプリケーション防御の最初のハードルともいえる「87%」、約９割をどのようなバランスでカバーするかという点を念頭に置いて見ていきます。

動的検査ツールの優位性

Web アプリケーションの脆弱性検査ツールには、ソースコードを解析する「静的検査」と、実際に HTTP リクエストを送信して外部から診断する「動的検査」があります。

静的検査ツールは検査の手間がかからない反面、実際にプログラムを動かして検査するわけではなく、問題ないものを問題と指摘する誤検知が多い傾向にあります。

動的検査ツールは、検査対象の画面の動きをシナリオにして再現しながら検査していくため、検査シナリオ作りの手間はかかりますが、プログラムが実際に稼働している状態での検査となり、静的検査よりも正確な検査ができます。

動的検査における「トレードオフ」を理解する

動的検査を行う場合、セキュリティを優先するならば、予算も時間も潤沢に準備し、専任のセキュリティエンジニアが広範囲にわたって高度な検査を実施するのが理想ですが、予算・時間・人員リソースに限りのある企業が多いのが実情です。そこで、検査を効果的に行うには、動的検査ツールにおける要素同士の「トレードオフ」の関係性を理解する必要があります。

動的検査のトレードオフ①
「検査項目数」と「検査時間」

動的検査において、所要時間は検査項目（検査する脆弱性の種類）の数と検査対象パラメータ（例：フォーム画面の入力項目）の数に応じて長くなります。各「対象」について、各「項目」を検査するごとに、検査ツールから HTTP リクエストが送信され、サーバからのレスポンスを待つ時間が必要となるため、所要時間は際限なく伸びる可能性があります。
また、検査対象のサーバスペックやプログラムの作り方が原因となって HTTP レスポンスが遅くなる場合には、検査時間はさらに増加します。

多機能な動的検査ツールの多くは、深刻なものから軽微なものまで大小さまざまなリスクの検査を広範囲に行おうとするため、小規模なアプリケーションでは数時間、中規模以上のアプリケーションでは 1 日以上の検査時間を要することが多々あります。その検査時間の長さがアプリケーションのリリースサイクルに合わず、数か月に 1 回しか実行されなかっ

たり、プロジェクトによっては 1 回も利用できないといったケースも少なくありません。

さらに、さまざまなリスクの検査を実行した結果、数多くの問題が発見された場合、比較的リスクの低い問題をどの範囲で修正するか、アプリケーション開発者が逐一判断しなければなりません。その検証にも多くの時間が割かれてしまいます。

動的検査のトレードオフ②
「機能」と「コスト」

多くの検査ツールでは機能を拡張し、設定画面や設定項目を増やす傾向があります。その理由は、セキュリティエンジニア向けに設計・開発されたツールとして、より多くの項目を検査できるように、また、より細かく設定できるようにしたいというエンジニア側のニーズに応えるためです。そのため動的検査ツールを活用するには、セキュリティエンジニアがトレーニングを受け、時間をかけて使い方を学習する必要があります。

社内に専任のセキュリティエンジニアがいて、すべての Web アプリケーションの脆弱性検査をカバーできていれば、そのような高機能なツールを使っていても問題ありませんが、専任者がいない場合は社内の誰かが兼務する必要があります。そのため、動的検査ツールの機能が増えるほど学習コストも増し、さらに日々運用するツールであるため、可視化しにくい人的コストも継続して発生します。

トレードオフを克服できる
VAddy の特長

予算・時間・人員リソースが限られた現場で、本当に役立つ脆弱性検査ツールが VAddy です。他の動的検査ツールとは設計思想が異なり、Web アプリケーションエンジニア、QA（品質保証）、発注者など、セキュリティエンジニア以外の方でも利用でき、検査回数の上限もありません。誰でも気軽に何度でも検査できる VAddy の特長を紹介します。

VAddy の特長①
設定項目を減らし、
検査時間を大幅に圧縮

弊社が提供する VAddy は、検査項目を「被害時のリスクが高く、攻撃数が多いもの」に検査項目を限定し、短時間で効果的な検査を短時間で行えるようサービスを設計しています。具体的な検査項目は、Web アプリケーションの攻撃傾向の章で述べた攻撃の 9 割弱を占める下記の 5 つを検査対象としています。

- SQL インジェクション
- クロスサイトスクリプティング
- ディレクトリトラバーサル
- リモートファイル実行
- コマンドインジェクション

開発期間のなかで、リリース前に常に検査を実行したり、アプリケーションのすべての画面をカバーした検査を実行する時間を確保できるように検査項目を絞ったことで、VAddy の全有料ユーザ (*5) の平均検査時間は 1 回あたり約 12 分となっています。検査時間の速さは、日々の運用を行いながら継続的

に検査を実施するうえで、非常に重要な要素となります。

*5：トライアルユーザを除く

VAddy の特長②
エンジニア以外でも利用でき、学習コストを抑制

VAddy では設定項目を極力少なくしているため、Web アプリケーション開発者だけでなくデザイナーや発注者、QA 担当者などでも簡単に利用でき、日々の運用も手間がかかりません。
唯一の設定項目は、検査対象画面の正常遷移を VAddy に伝えるシナリオ作成（クロール）です。これはブラウザを使って実際の検査対象のアプリケーションを操作し、その操作を記録します。つまり VAddy で検査を行うとき、利用者が行うのは検査したい Web アプリケーションの画面の操作だけです。他の動的検査ツールで検査を正しく行うには、シナリオ作成のクロール作業に加えて、細かな設定を施す必要があります。

VAddy では検査に際して行うべき設定の情報を、クロールデータから自動で判断して利用しています。例えばログインセッションが切れた場合は、自動的にログインし直したり、フォーム画面の CSRF 対策トークンが切れた場合は自動で再取得して検査します。一般的な動的検査ツールで必要となる細かな設定を、ユーザーが行う必要がないため、専用のトレーニングや日々の学習コストがかからず、エンジニアでなくとも利用できるのです。

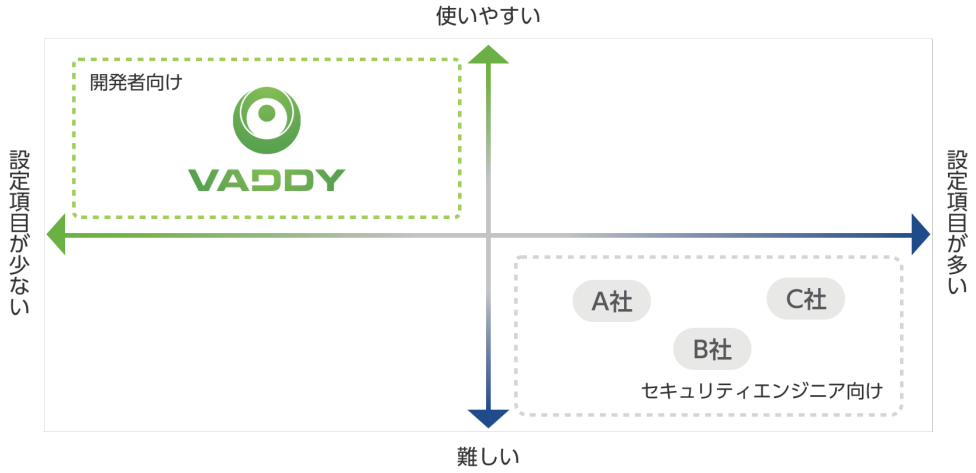
また最近では、社内のセキュリティエンジニアだけでは検査が追いつかず、Web アプリケーション開発者が事前に最低限の脆弱性検査を行う、検査の内製化傾向が強くなっています。このような、セキュリティエンジニア以外のスタッフが脆弱性検査をするときにも VAddy が活用されています。

VAddy の特長③
柔軟で安価な料金設定を実現

従来の有償脆弱性検査ツールの価格は年間で 100 万円を越えるものが多いうえ、使いこなせるようになるまでにはトレーニング期間も必要です。有償ライセンス製品ではインストール台数や稼働台数の制限があるほか、同じプロジェクトで複数の企業が利用する場合に追加予算が掛かってしまうこともあります。いっぽう、無償の脆弱性検査ツールであれば、サポート体制が十分ではないがゆえに、自分たちで運用方法や検査方法を学習する運用コストがかかります。

VAddy の料金は Professional プランが月額約 2 万円（年額では 19 万 8,000 円 (*6)）で、最低利用期間も 1 か月からに設定しています。プロジェクトの期間や特性に合わせて年に数か月ずつ断続的に利用するなど、柔軟な利用も可能です。
どのプランもスキャン（検査）回数は無制限で、回数を気にせず気軽に検査を実行できます。また、Professional プラン以上のプランであれば、「1 プロジェクトあたり最大 50 ユーザー」「基本利用料で 3FQDN まで利用可能」となっており、追加ランニングコストも最小限に抑えられます。

*6：税抜



VAddy の特長④
検査の自動実行を、無料で容易に

他の動的検査ツールが、セキュリティエンジニア向けツールとして検査項目の増加や機能拡充を指向する一方、VAddy はそれとは逆の発想で、大小さまざまなプロジェクトの現場で、日々の開発フローの中で使えるツールとして開発しています。

そのため、VAddy はインストールや実行環境の運用などが不要なクラウド型の脆弱性検査ツールとして誕生しました。さらにその後、検査の自動実行を簡単に実現できるよう、VAddy では API を公開し、API を通して検査の実行や結果の確認などが行えるようにしています。そのためのツール（Jenkins プラグイン、VAddy コマンドツールなど）も無料で利用できます。

まとめ

多くの開発現場では、人的リソースや予算、納期の制約から脆弱性検査を実施できないケースが多くあります。しかし Web サイト規模の大小に関係なく、Web アプリケーションの脆弱性を狙った攻撃は日々発生しています。Web アプリケーション開発者への教育を徹底していても、技術レベルの高い開発者が作ったものであっても、些細な人為的ミスから脆弱性の発生につながるケースをゼロに抑えるのは非常に難しいことです。

そのため、脆弱性検査ツールや診断サービスを利用し、脆弱性を排除した状態でリリースを続けるべきですが、そのためには人件費、ライセンス費など大きなコストがつきものです。

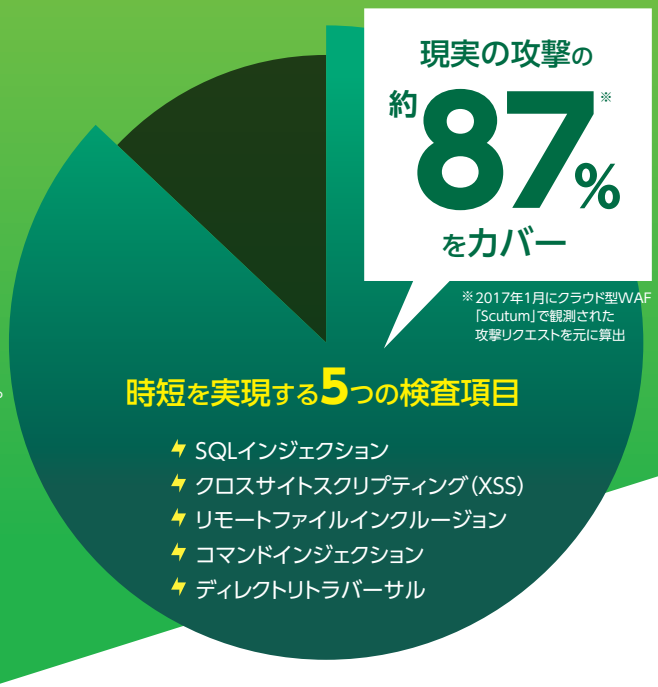
さまざまなコストの制約を受けずに幅広い現場で脆弱性検査を実施できるよう、従来の動的検査ツールとは一線を画す思想で開発した VAddy は、87%の攻撃への対策を「平均 12 分のスキャン」と「月額約 2 万円」で実現しています。VAddy には無料トライアル期間も用意されています。以下の URL のサインアップフォームからユーザ登録をすると、すべての機能が 1 週間無料で利用できます。
VAddy が提供する“制約を受けない”脆弱性検査の快適性を、一度試してはいかがでしょうか。

https://console.vaddy.net/ja/signup

VADDY（バディ）

いま最も手軽で高速な クラウド型Web脆弱性検査ツール

脆弱性検査の内製化準備はお済みですか?
VAddyならWebアプリケーション開発者でも簡単に脆弱性検査できます。



時短を実現する5つの検査項目

- SQLインジェクション
- クロスサイトスクリプティング（XSS）
- リモートファイルインクルージョン
- コマンドインジェクション
- ディレクトリトラバーサル


面倒な設定は不要

平均検査時間12分


トレーニング不要

料金プラン

		手軽に脆弱性検査をはじめてみるなら	VAddyの基本機能が全て使える	セキュリティエンジニアのサポート付き	VAddy＋マニュアル検査で幅広い脆弱性に対応
		Starter 月額 ￥6,000	**Professional** 月額 ￥19,800	**Platinum** 年額 ￥598,000	**Platinum +** 年額 ￥898,000
検査項目	SQLインジェクション検査	○	○	○	○
	XSS検査	○	○	○	○
	RFI検査		○	○	○
	コマンドインジェクション検査		○	○	○
	ディレクトリトラバーサル検査		○	○	○
チーム機能	チームメンバー	5ユーザー／FQDN	50ユーザー／FQDN	50ユーザー／FQDN	50ユーザー／FQDN
機能	スキャン回数	無制限	無制限	無制限	無制限
	スキャン上限時間	30分／回	2時間／回	2時間／回	2時間／回
	スキャン履歴	過去1年分	過去2年分	過去2年分	過去2年分
	ローカル環境への検査		○	○	○
外部連携	CI連携	○	○	○	○
	Web API	○	○	○	○
サポート	製品サポート	○	○	○	○
	脆弱性サポート*1 *2			10チケット	10チケット
	マニュアル検査*1 *3				50リクエスト
料金	基本利用料(3FQDNまで)	月額 ￥6,000	月額 ￥19,800 年額 ￥198,000 年額だと2ヶ月分お得	年額 ￥598,000	年額 ￥898,000
	FQDN追加	月額 ￥2,000/FQDN	月額 ￥6,000/FQDN 年額 ￥60,000/FQDN 年額だと2ヶ月分お得	年額 ￥60,000/FQDN	年額 ￥60,000/FQDN
お支払い方法		クレジットカードのみ	クレジットカード ／銀行振込(請求書発行)	銀行振込(請求書発行)	銀行振込(請求書発行)
				SHIFT SECURITY	SHIFT SECURITY

※価格は税別です
*1 株式会社SHIFT SECURITYが提供します。
*2 VAddyで発見された脆弱性への対処方法などをチャットでサポートします。
*3 OWASP TOP10に準拠した手動診断を実施します。

VAddyに関するお問い合わせ

03-5577-2032
受付時間 平日 10:00～18:00

株式会社ビットフォレスト VAddy事業部（担当：西野・市川）
info@vaddy.net　@vaddynet

https://vaddy.net/ja/

bit forest
https://www.bitforest.jp

株式会社ビットフォレスト

東京本社
東京都千代田区神田錦町 1-17-5 神田橋 PR-EX 8F
TEL : 03-5577-2032　FAX : 03-5577-2034

福岡オフィス
福岡県福岡市中央区天神 2-14-35
野村不動産天神ビル 4F