VADDY

予算であきらめないで！

的確な手法をムダなく選択するために
Webアプリケーション脆弱性診断手法の違いと使い分け事例

October 2018

bit forest
https://www.bitforest.jp

株式会社ビットフォレスト

目次

予算であきらめないで！

的確な手法をムダなく選択するために Webアプリケーション脆弱性診断手法の違いと使い分け事例

はじめに

インターネットに接続された機器や Web サービスを狙ったサイバー攻撃の脅威は年々増加しています。近年では標的型攻撃による被害や、IoT 機器の脆弱性を狙った攻撃がクローズアップされがちですが、情報処理推進機構（IPA）が発表している「情報セキュリティ 10 大脅威 2018」(*1) では、Web サービスに関連する脅威が昨年に引き続き複数ランクインしています。Web サイト／ Web サービスを狙った攻撃の勢いも、一向に衰えてはいないのです。

本稿では、さまざまなサイバーセキュリティ対策のうち Web サイト／ Web サービスに関連したもの、特に Web アプリケーション脆弱性診断というジャンルに絞り、その特徴について紹介します。Web サービス事業者としても、あるいは受託開発事業者としても、今後ますます欠かすことができない Web 脆弱性診断。本稿がその理解の、一助となれば幸いです。

*1 https://www.ipa.go.jp/security/vuln/10threats2018.html

「手動」と「ツール」。診断手法の違いは何か

Web アプリケーション脆弱性診断には、大きく分けて「手動診断」と「自動診断（ツール診断）」の 2 種類のカテゴリがあります。「手動診断」は文字通り人の手を使って行うもの、「自動診断」は何らかの自動検査ツールを利用して検査するものです。厳密に言えば、「手動診断」でツールを使うこともありますし、「自動診断」でも完全自動と言うわけにはいきません。あくまでも「人の手とツールの、どちらが主か」でカテゴライズされていると理解ください。

1. 手動脆弱性診断
（セキュリティエンジニアによる診断）

ここで言う「手動」とは、サイバーセキュリティの専門知識を持つ診断員（セキュリティエンジニア）が、対象の Web アプリケーションを自らの手で検査することを意味しています。もちろん実際にはすべてを手動で検査するわけではなく、何らかの（自動）ツールを用いることがほとんどですが、その際もツールのみに頼らず、診断員の知見を駆使しながら労働集約的に検査します。

1-1. 手動脆弱性診断の優位性
～検査精度の高さ～

手動脆弱性診断の優位性は、検査精度の高さにあります。例えば、仕様上のミスに起因する脆弱性のような、機械的には発見が困難な脆弱性も発見できるなど、一般的には、手動脆弱性診断の検査精度に、自動脆弱性診断ツールの検査精度が勝ることはありません。

検査精度に圧倒的な優位性を持つ反面、人手を使って行う業務であるがゆえに、それに見合った費用や日数が必要になります。多くの脆弱性診断会社ではリクエスト数（≒画面遷移数）あるいは機能（画面）数に応じた料金が設定され、診断一回あたりの費用は数十万円～数百万円程度が一般的です。リクエスト数や機能数をベースに費用が決まるため、すべての機能の検査が求められる金融系システムなどを除き、通常は予算に合わせて重要と思われる機能／画面のみを検査対象とします。したがって、発注側が検査対象範囲を的確に絞り込めないと、手動脆弱性診断の費用が膨らんでしまいます。

非常に安価な手動脆弱性診断を提供している診断会社も存在しますが、「自動検査ツールを実行し、明らかな誤検知だけを手作業で除外して報告する」というケースもあるため、費用だけで判断するのは避けた方が無難でしょう。

1-2. 手動脆弱性診断の優位性 ～診断後の対応～

発見された脆弱性の危険度のレビューや対応方法のサポートも、手動脆弱性診断の優位点として挙げられます。脆弱性検査は一回実施して終わるものではありません。脆弱性の発見頻度は開発者や組織によって極端に異なりますが、高い確率で何らかの脆弱性が発見されます。つまり「まったく見つからない」ということは少ないため、それらを適切に判断して処理することが必要です。

診断会社によっては脆弱性が発見された際の再検査までメニューに含まれている場合もあります。ユーザー企業自身で自動脆弱性診断ツールを用いて検査する場合は、ユーザー企業自身で検出された脆弱性について判断し、対応を検討する必要がありますので、この点だけでも手動脆弱性診断会社に依頼する価値はあります。

1-3. 手動脆弱性診断の課題

手動脆弱性診断の課題としては、予算や日数の問題の他に、担当する診断員のスキルによって検査結果が異なる点が挙げられます。手動脆弱性診断は労働集約的な側面があると同時に、知識集約的な業務でもあります。ある程度は自動検査ツールで補完できるものの、経験豊かなベテラン診断員でしか見つけられない脆弱性もあるのです。前回の診断時と同じアプリケーションなのに、診断員が前回と違うと検査結果が異なるというケースもあります。この課題については、脆弱性診断業界全体で診断員のスキルの平準化を図るためのガイドラインを策定[*2]するとともに、作業の自動化を進めることでスキルのばらつきを無くす取り組みも始まっています。

また、これまでの手動脆弱性診断はセキュリティ診断会社の"専売特許"でしたが、Webアプリケーションのリリースサイクルが短くなっている昨今では、社内のセキュリティ部門で手動脆弱性診断を行うケースも増えてきています。

*2 https://www.owasp.org/index.php/Pentester_Skillmap_Project_JP

2. 自動脆弱性診断
（プログラマー等によるツールを利用した診断）

ツールによる自動脆弱性診断は、実施段階によって大きく 2 種類に分けられます。

2-1. リリース前診断用ツール

自社内の開発部門において、Web アプリケーションのリリース前に自動検査ツールを用いて実施する脆弱性診断を「リリース前診断」と定義します（自社内で行う場合でも、セキュリティ部門のエンジニアなどが手動で行う診断は「手動診断」に分類されます）。

2-1-1. リリース前診断用ツールのメリットとデメリット

リリース前診断用ツールに分類されるものには OSS（Open Source Software）／有償、クラウド型／インストール型などさまざまな提供形態があります。有償版ツールの費用は年間 100 万円～300 万円程度が一般的ですが、それらは診断会社での手動診断補助ツールとして使われるほど高性能・高機能であるため、自社で提供している Web サービスの数やリリース頻度によっては、外部に診断を依頼するよりもコストが掛からず、十分元が取れる金額だと言えます。

しかしながら、高性能・高機能であるがゆえ、ツールの学習コストが高く、検査実行時間も長くなります。そのため、一般的な開発エンジニア（プログラマー）が日々の開発工程業務の中で使いこなすにはハードルが高いと言わざるを得ません。

診断“事業”に耐えうるほどの性能・機能を持つツールは、使い手にもある程度の知識と習熟度を要求します。「1. 自社アプリケーションの知識」「2. ツールの知識」「3. セキュリティ検査の知識」の 3 つの知識は最低限必要で、2 と 3 についてはベンダーが開催するトレーニングや社内勉強会、ユーザーコミュニティによる勉強会に参加して習得する必要があります。

トレーニングを経て、十分に使いこなすことができるようになった後に留意すべき点は検査実行時間です。幅広い検査範囲を持つそれらのツールは、一回あたりの検査に数時間から数日間を要します。これは検査開始ボタンをクリックしてから検査が終了するまでの時間で、、検査前の準備や検査後のレビューは含まれません。そのため、これらのツールを利用する場合は、準備およびレビューを含めた検査時間をテスト工程の中に見積もっておくことが必要です。

これらの自動脆弱性検査ツールを十分に使いこなせれば有効な対策となります。メガベンチャーと呼ばれる Web 系企業を中心に、多くの企業の社内セキュリティチームがこれらのツールを駆使して診断を行っています。

2-1-2. クラウド型 Web 脆弱性検査ツール「VAddy」の特徴

弊社が提供しているクラウド型 Web 脆弱性検査ツール「VAddy」は広い意味ではこのカテゴリに属しますが、利用に習熟が必要な従来の自動脆弱性検査ツールとは異なり、アプリケーション開発者（プログラマー）自身が毎日の開発工程の中で脆弱性検査を実施したり、QA（品質管理）部門や検収業務で利用されることを想定して開発されています。

学習コストを掛けずに利用できるうえ、平均検査時間は 12 分と短いことから、従来は自動脆弱性検査

ツールの導入が難しかった中小規模プロジェクトやアジャイル開発環境に最適化されています。

経済産業省が行った 2016 年の報告 (*3) にあるとおり、昨今ではセキュリティ人材不足が深刻化しており、手動脆弱性診断を提供する企業では案件数の増加する一方で人員の確保が追いつかず、受注を抑制する企業も出はじめています。そうした中、「脆弱性検査の内製化」というキーワードのもと、可能な限り脆弱性検査を自社内で行う動きが活発化しており、リリース前診断用ツールに注目が集まっています。

*3 http://www.meti.go.jp/press/2016/06/20160610002/20160610002.html

2-2. リリース後診断用ツールの役割

公開されている（本番稼働中の）アプリケーションに対して定期的に検査リクエストを送信し、て脆弱性の有無を判断するタイプのツールを「リリース後診断用ツール」と定義します。主に SaaS 型で月額数千円から提供され、今回紹介するカテゴリの中では、最も安価で手軽なツールです。

脆弱性の有無を Web サービス公開後に（つまり Web アプリケーションの開発後に）確認するため、何らかの脆弱性が発見された場合、修正が完了するまでの対策は WAF（Web Application FireWall）等を緊急導入するか、脆弱性を放置するかしかありません。
そのため、既に公開済みで継続的な開発が行われていない Web サイト／ Web サービスにおいて、「脆弱性が無い」ことを確認するために使用する意味合いが強いツールです。

企業規模・業種別に見る、診断手法の使い分け事例

ここまで主要な脆弱性診断手法を紹介しましたが、大前提として、「費用」「工数」「精度」の点ですべての要求を満たす脆弱性検査手法はありません。Web アプリケーションの分野に限らず、セキュリティ対策では「堅牢性」と「扱いやすさ」とはトレードオフの関係になりますので、リソースやシーンに合わせて使い分けることが大切です。企業規模や業種ごとの違いによる、使い分けの事例を紹介します。

A 社：社員 10 名以下の Web サービス スタートアップ

VC の要求に応じる形で、サービスリリース前に手動診断を一度実施。その後の頻繁な機能追加や改修の際は、開発工程に組み込まれた VAddy で継続的に脆弱性検査を実施。サービスのメジャーバージョンアップや VC からの追加投資によって予算が確保できた時点で、あらためて手動診断を実施。

B 社：安定稼働中の Web サービス運営会社

長年システムを安定稼働させている B 社では、セキュリティテストの知識を持ったプログラマーが有償の診断ツールを使って検査していた。稼働中のアプリケーションが十分に枯れてきたことと、開発プログラマーたちのセキュアコーディングのスキルも上がったことから、有償の診断ツールで脆弱性が発見されることも無くなった。そうした状況で、高額なライセンス費用にコストメリットを見いだせなくなったため社内検査ツールを VAddy に変更。ツール費用として年間 100 万円以上削減。加えて、一回あたりの検査時間も数時間から数十分に短縮された。

C 社：Web サービス運営会社

年に一回程度のメジャーバージョンアップ前に手動診断を実施しているが、画面遷移が非常に多く、全機能を検査しようとすると 1,000 万円以上かかるため、主要な機能のみの検査を診断会社に依頼し、それ以外の画面および機能については VAddy で検査。

D 社：受託開発会社

セキュリティ意識が高く、潤沢なテスト予算が用意されている大規模案件ではリリース前に手動診断を実施。しかし最近では総予算 100 万円以下の小規模案件でも、セキュリティテストの実施が要件に入ることが増えてきた。クライアントの予算内では手動脆弱性検査が実施できないため、代替案として VAddy でのセキュリティテストを実施している。テスト工数の削減のため、担当 Web ディレクターが Web アプリケーションの動作確認時に同時にセキュリティテストを実施。

E 社：大手 Web サービス運営会社

数十を超える Web サービスを提供している E 社は数年前より社内にセキュリティチームを設置し、社内で手動診断とツール診断を行っている。
しかしアプリケーション開発チームの数に比べ、セキュリティチームの人員が圧倒的に少ないため、セキュリティチームが行う脆弱性診断がサービスリリースサイクルのボトルネックとなっている。そこでアプリケーション開発チームに VAddy 導入し、最低限の脆弱性検査を開発チーム自身に実施させることで、セキュリティチームの検査工数の削減とリリースサイクルの短縮化を目指している。

“豊富な選択肢”の中から、脆弱性診断を正しく選ぶために

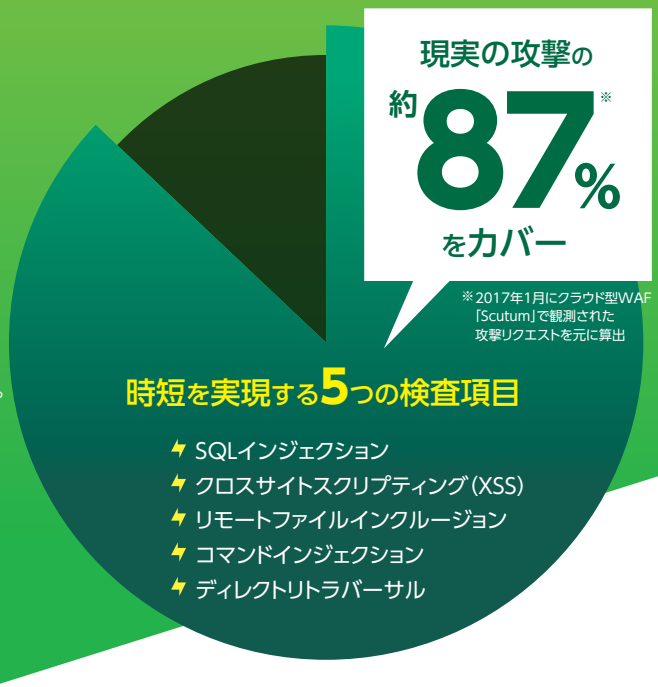
Web アプリケーションの脆弱性診断ツールは、利用者の目的や予算に応じたさまざまなツールが選択できる状況になっています。無料の OSS 診断ツールという選択肢もあるなか、「予算が無い」「時間が足りない」という言い訳が効かない時代に突入していると言っても過言ではありません。

セキュリティ対策には万人に共通の「唯一の正解」は無く、対処すべき問題は Web サイト／ Web サービスに関するものだけではありません。自社で扱っている情報の規模や重要度と利用可能なリソース（人的・金銭的・スキル）を精査し、企業やサービスの成長段階、クライアントの要望に応えられる選択肢を用意しておく必要があります。

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