VADDY

Web 脆弱性診断内製化の先行事例一覧

～人員・予算の制約のなかどう実現したのか？～

October 2018

bit forest
https://www.bitforest.jp

株式会社ビットフォレスト

Web 脆弱性診断内製化の先行事例一覧

～人員・予算の制約のなかどう実現したのか？～

はじめに

脆弱性診断の「内製化」の必要性が叫ばれて久しいものの、それを実現できている企業は実は多くありません。しかしここ 1～2 年の間に脆弱性診断内製化を支援するサービスや、それを実現するツールが次々と登場しています。特にビットフォレストが提供しているクラウド型 Web 脆弱性検査ツール「VAddy」は、価格の低さもさることながら、従来の検査ツール導入では必要とされたセキュリティテストの知識が不要で、検査速度が圧倒的に速いことから、数多くの企業で **Web アプリケーション脆弱性検査の内製化の実現**に一役買っています。

本ホワイトペーパーでは「VAddy」を活用した内製化の実現事例の中でも、従来の脆弱性診断やツールの導入が難しいとされてきた企業での事例を見ていきます。限られた予算と人員で、いかにして安全な開発体制を築いたかを知ることは、規模の大小を問わず Web サイト／ Web アプリケーションの開発運用に携わるすべての企業やプロジェクトで参考となるはずです。

Web 脆弱性診断内製化の先行事例一覧

～人員・予算の制約のなかどう実現したのか？～

目次

先行事例 1

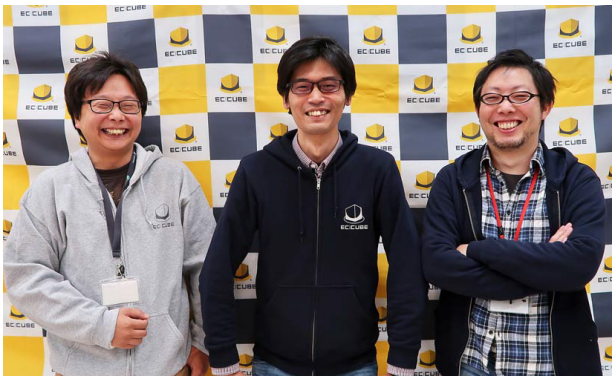
株式会社ロックオン様（EC-CUBE）
「VAddyの導入でEnd to Endテストの価値が上がった」

主な業務	サービスの規模	脆弱性検査での課題
EC サイト向け CMS 開発	日本国内では No1 シェアの E コマース用 OSS （実稼働として約3万店舗）	検査の事前準備と検査自体に時間がかかりすぎるので、 大きなプロジェクトのリリース直前にしか検査できない。

診断内製化のパターン

業種：OSS 開発　利用者：開発者　シーン：毎日の自動検査

クラウド型 Web 脆弱性検査サービス VAddy は OSS コミュニティへの VAddy 無償提供を行っています。今回は前回に引き続き、本取組の中で VAddy を導入いただいた株式会社ロックオンの EC-CUBE 開発チームにお話を伺いました。



EC-CUBE とは

2006 年 9 月にリリースした EC-CUBE はショッピングサイトの構築に特化した CMS ソフトウェアで、OSS（オープンソースソフトウェア）として配布しています。E コマース用の OSS は世界中に数多くありますが、日本国内においては EC-CUBE がダントツの No1 シェアを誇っていて、現在は実稼働として約３万店舗で使われています。

当初 EC-CUBE は自社で行っていた受託案件で利用するためのみに開発していましたが、オリジナリティの高いショッピングサイトを世の中に増やしていく目的のため、手段としてどのような形が良いのか考えた末、OSS という形態にたどり着きました。

現在弊社では EC-CUBE をベースにした個別カスタマイズ等の開発業務は行っておらず、決済代行会社様とアライアンスを結び、決済プラグインを使って決済された売上の一部を頂戴するというビジネスモデルを取っています。ですので EC-CUBE でショッピングサイトを構築していただくことや売上を上げていただくためのサポートとして、情報発信や開発コミュニティ運営なども行っています。

EC-CUBE における セキュリティ対策

一般的に「OSS の利用は自己責任」と言われます。OSS におけるセキュリティ対策も例外ではありませんが、EC-CUBE の本体部分については、以前から有償の検査ツールを利用した脆弱性検査を社内で実施しています。

また、EC-CUBE を利用してショッピングサイトを開設するショップオーナーや開発会社が脆弱性診断を実施して、そのフィードバックをいただくこともあります。

株式会社ロックオン様（EC-CUBE）

VAddyの導入でEnd to Endテストの価値が上がった

EC-CUBE マーケティングマネージャー
梶原直樹様

社内で実施している脆弱性検査については、非常に高機能なツールを利用しているということもあって、検査の開始に必要な事前準備（設定等）の工数が多くかかり、検査自体も EC-CUBE の場合は 2～3 日かかります。ですので、検査は大きなプロジェクトのリリース直前にしか行うことができませんでした。

そうした「高機能な検査ツールを有効に使えていない」という課題感から、去年の秋頃から脆弱性検査方法の見直しの検討を始めて、OWASP ZAP などの OSS ツールも含めたいくつかの検査ツールの比較を行いました。結果的には従来の検査ツールを継続して使い続けるという結論になったのですが、検査結果の判定を含めて使いこなすにはセキュリティ検査の知識が必要になるので、社内勉強会を開催して開発メンバーのスキルアップを行っています。

VAddy 導入の決め手

既に脆弱性検査方法の見直しが終わった後だったのですが、OSS への VAddy 無償提供が始まったと聞いて、せっかくなので（笑）

EC-CUBE 3 系から CI を使ったテストを回しているのですが、脆弱性検査の部分だけリリース前に実施するので良いのかという課題感がありました。いま使っている検査ツール以外にもっと気軽に日々使える検査ツールは無いかなと。

そんな中、今年の 7 月の php conference Kansai 2017 で市川さん（株式会社ビットフォレスト CTO/VAddy プロダクトリーダー）にお会いして VAddy のことをお聞きしてすぐに試してみました。VAddy は検査項目が絞られているものの、日々気軽に使いたいという我々のニーズにマッチする「ちょうど良いツール」かなという印象でした。高機能な検査ツールだと誤検知のようなものも含めて多量の検査結果が出力されるので、対応すべきか

株式会社ロックオン様（EC-CUBE）

VAddyの導入でEnd to Endテストの価値が上がった

どうかの判断も含めて日々使うには少し負荷が高いので。

EC-CUBE 事業部　部長
金陽信様

VAddyの導入でWebテスト（EtoEテスト）の価値が上がった

そんなこんなで急遽 VAddy を使ってみようと思ったのですが、導入は本当に簡単で、苦労した記憶はほとんどありません。
VAddy の検査に必要なクロールデータの作成だけは面倒に見えますが、EC-CUBE ではすでに Codeception を使った Web テスト（EtoE テスト）環境が整備されているので、それを応用すればクロールデータの作成は簡単にできます。既存のテストケースの中から VAddy の検査に必要な部分だけを抽出したテストケースを作成して、毎晩 TravisCI で自動実行しています。さくらクラウド上で docker コンテナがビルドされた後に、EtoE テストの実行、VAddy のクロールデータの作成、VAddy の脆弱性検査までの一連の流れが毎日自動で実行されています。

正直なところ EtoE テストのメンテナンスはけっこう大変なのですが、VAddy を使うようになってからそうした Web テストの価値が倍くらいに上がった気がします。**EtoE テストシナリオを頑張ってメンテナンスしていけば、通常の Web テストだけでなく脆弱性検査も同時にできるようになります**から。

もし弊社に EtoE テストが整備されていなかったとしたら、クロールデータの作成でかなり苦労したと思います。とは言え、オートクロール機能（検査対象の Web サイトを自動的に巡回して検査してくれる機能）が備わっている他のツールでも、オートクロール機能だけだと見つけられない部分が出てきます。実際にツールの検査で発見できなかった脆弱性が後になって見つかることがあって、なぜ発見できなかったかを調べると自動検査ではなくステップ操作でしか見つけられない部分だったことがあります。結局、**自動的に対象のアプリケーションをクロールしてくれる検査ツールであっても、自分たちでクロールデータを作らないといけない場面は必ず出てきます。**

EC-CUBE 事業部
奥清隆様

株式会社ロックオン様（EC-CUBE）

VAddyの導入でEnd to Endテストの価値が上がった

VAddy を使ってみて

良いことずくめです（笑）
特に検査の実行時間が短いことは本当に助かっています。EC-CUBE には多くの社外コミッターがいますが、VAddy で毎晩検査することでコミッターに対して素早いフィードバックを返すことができます。網羅性という点で他の検査ツールをメインで使うことにしたとお話しましたが、VAddy の取り回しの良さは網羅性を補って余りあると感じています。**検査回数の制限が無い**ので「大丈夫かな？」と逆に心配してしまいます。

VAddy は 5 つの検査項目しかありませんが、本当に重要な脆弱性に絞られています。脆弱性検査方法の見直し時に複数の検査ツールを比較した際は「検査項目が少なすぎる！」と思いましたが、後にいろいろ調べてみるとこれらの**現実的な驚異への対策としては十分**では無いかと思います。ツール比較時は網羅性を重視していましたが、当時このことを知っていれば、結論も変わっていたかもしれませんね。

この 5 項目が本当に重要だということをもっとアピールした方が良いと思いますよ（笑）

【参考】

2017/11/22 開催 VAddy ユーザーミートアップ Vol8 資料
「EC-CUBE での VAddy 活用事例」

https://www.slideshare.net/ec-cube-official/20171122vaddymeetupeccubevaddy

株式会社ロックオン

設立

2001 年 6 月

代表者

代表取締役社長　岩田進

所在地

【大阪本社】

〒530-0001

大阪府大阪市北区梅田 2-4-9 ブリーゼタワー 13F

【東京本社】

〒100-0006

東京都千代田区有楽町 2-2-1 X-PRESS 有楽町 12F

事業内容

1．マーケティング ロボットの提供
2．マーケティングプラットフォーム
「アドエビス」「THREe」
3．商流プラットフォーム「EC-CUBE」
4．ビッグデータの分析及び最適化
「マーケティングメトリックス研究所」

※事例取材時情報

先行事例 2

株式会社ネットフォレスト様

「VAddyの『速さ』と『手軽さ』がWebデザイナーによる脆弱性検査を実現」

主な業務	脆弱性検査での課題
ネットワークから Web コンテンツまで インターネットソリューションをワンストップで提供	脆弱性診断ツールは設定が難しく、 契約から利用開始までにかなりの時間がかかる

診断内製化のパターン

業種：受託開発　利用者：発注者　シーン：受け入れテスト

ネットワークから Web コンテンツまでインターネットソリューションをワンストップで提供する「株式会社ネットフォレスト」。自社サービスサイトの脆弱性検査や、パートナー企業から納品される Web アプリケーションの受入検査時の脆弱性検査に VAddy を利用いただいています。今回のインタビューは 2018 年 2 月 15 日にオープンしたばかりの、同社が運営する横浜のコワーキングスペース「/Bangarrow（バンガロー）」で行いました。

ネットフォレストとは

ネットフォレストは 2000 年 4 月創業の、ISP 事業（かもめインターネット）を中心とした情報システム企業です。ISP 事業はネットフォレストの前身の企業の時代（1996 年）から始めていますので、老舗の部類に入ると思います。

現在は ISP 以外にもホスティング、Web デザイン、ホテル向け VOD 事業など幅広く事業を展開しており、お客様にネットワークから Web コンテンツまでワンストップで提供できることが強みです。

私はネットワークソリューショングループという部署で ISP 事業におけるインフラの保守、VOD 事業でのネットワークの設計から機器の設定まで幅広く手がけております。それ以外には基本的には社内の技術的な部分を多く任されており、自社サービスの Web アプリケーション開発やセキュリティ周り全般も担当しております。

ライトに検査できるのが VAddy の強み

VAddy は自社の ISP サービスサイトの脆弱性検査から使い始め、最近では受託の Web コンテンツ開発案件でパートナー企業から納品される Web アプリケーションの脆弱性検査に使っています。弊社は Six Apart 社の ProNet メンバーなので、Movable Type や PowerCMS を使ったシステム開発が多く、スクラッチでの開発は問い合わせフォームなどの軽めのものが多いというのが現状です。CMS 本体の脆弱性検査を実施するのは現実的ではないので、検査の対象はそうした軽めの Web アプリケーションになります。

株式会社ネットフォレスト様

VAddy の「速さ」と「手軽さ」が Web デザイナーによる脆弱性検査を実現

VAddy 導入前はあるクラウド型 Web サイト脆弱性診断サービスの利用も検討しましたが、**そのツールは設定の難しさもさることながら契約から利用開始までにかなりの時間がかかる**ことも問題でした。例えば VAddy だと検査対象のサーバー登録はブラウザ上で実行できますが、そのツールだとサーバー登録はベンダーに申請して実施してもらう必要があります。他にも、検査のテストケースが大幅に変わる場合はあらたに別の契約を申し込まないといけないなど、細かな制約が多くありました。

おそらく、アプリケーションの機能追加がほとんど発生しないような Web サイトで、セットアップした後は放置して自動診断結果のレポートを定期的に確認するという使い方を想定して作られているのだと思います。けれども導入や設定変更に時間がかかるツールだと、私たちのように頻繁にアプリケーションが変更になる自社サイトや、案件ごとにホストもアプリケーションも異なるような Web コンテンツ開発業務には向いていません。

その点 **VAddy はあらゆる手続きが Web ブラウザで実施できますし、検査自体も圧倒的に速い**。オープンソースの脆弱性検査ツールもありますが、問い合わせフォームのような「軽めの Web アプリケーション」だけを検査したいという場合だとそれらのツールでは重すぎます。いくつかの検査ツールも検討したものの、「軽めの Web アプリケーション」をライトに検査できるツールは VAddy 以外に無かったというのが結論です。

セキュリティ要件が定義される案件が増えてきた

弊社がお請けしている Web コンテンツ開発案件ではアプリケーション開発を外部のパートナー企業に依頼することも多く、その場合弊社の Web ディレクター／デザイナーがパートナー企業から納品されるアプリケーションの受入検査を実施します。その際に一通りの機能テストは実施しますが、明確なセキュリティ要件がクライアントから提示されていない案件ではそれ以上のことは社内では実施せず、セキュリティ対策はパートナー企業におまかせしていました。

しかしながら、クライアントからの RFP にセキュリティ要件が定義されることが増えてくるにともない、弊社内でもパートナー企業から納品される Web アプリケーションの脆弱性検査を実施する必要がでてきました。

クライアントから提示されるセキュリティ要件は「クロスサイトスクリプティング（XSS）対策を講じること」といったような粒度のものが多く、特殊な攻撃に対しての対策までは求められないので、VAddy のようなライトなツールで「基本的な検査はやっています」と言えることが重要になります。

株式会社ネットフォレスト様

VAddy の「速さ」と「手軽さ」が Web デザイナーによる脆弱性検査を実現

デザイナーによる脆弱性検査がエンジニアの負荷を軽減

VAddy 導入前は社内での脆弱性検査は私たち技術部門が実施していましたが、**今では Web ディレクター／デザイナーが VAddy を使って自分たちで検査するようになりました**。クロールデータの作成（検査のシナリオ作成）は多少めんどうなものの、前述したようにもともと彼らは受入検査時の機能テストを実施していたので、それと同時にクロールデータを作成してしまえば他に特別な手間や知識が必要ありません。

もちろん、何らかの脆弱性が発見された場合は私たち技術部門が Web ディレクター／デザイナーをサポートしながらパートナー企業に修正依頼を出すことになるのですが、**脆弱性検査の実行までをデザイナーたちだけでやってくれるだけでも技術部門の負荷は大幅に軽減されます**。技術部門としては問題が発見されたときだけ対応すれば良いですからね。弊社ではデザイナーとエンジニアが席を並べて仕事をしているので、何か脆弱性が発見された場合はデザイナーたちと一緒に VAddy の検査結果画面を見ながら対策を検討しています。

自社サービスサイトの検査でも活用

VAddy の利用シーンは受託の Web コンテンツ開発だけではありません。弊社は ISP 事業などの複数の自社サービスサイトがあります。それらのサイトの Web アプリケーションは自社で開発しており、機能追加や変更が頻繁に発生します。私が開発している案件では単体テストの段階から頻繁に VAddy で検査しています。

開発の途中から Selenium のテストを作るようにしているので、動作チェックを Selenium で自動化させたあとは Selenium のテストシナリオを VAddy 用に少しカスタマイズして納品前にまとめてテストをしています。

今はまだ CI（Continuous Integration）は導入できていないのですが、ちょっと自社サービスのアプリケーション管理が煩雑になってきたので、CircleCI の導入を検討しているところです。VAddy サイトの他社さんの事例で CircleCI と VAddy を連携している会社さんも拝見しましたので、近い将来で CI と VAddy を連携したいと思っています。

株式会社ネットフォレスト様

VAddy の「速さ」と「手軽さ」が Web デザイナーによる脆弱性検査を実現

VAddy への要望

あえて言えばクロールデータの作成補助機能のようなものがあるとうれしいですね。これだけ楽に検査できるので、もっと楽したいという欲がでてきました（笑）。VAddy と CI の連携を始めたら別の要望も出てくるかもしれませんが、今のところ要望はそれくらいでしょうか。
例えば検査結果のレポート機能なども、私たちが使う限りではこれ以上の詳細なレポートは不要かなと思います。脆弱性が発見された場合はすぐに修正しますし、どこにどんな脆弱性があるかが分かれば十分です。むしろ検査ごとに詳細なレポートが作成されることで VAddy の検査速度が落ちるようなことがあったら困ります。

とは言え、社内監査や四半期ごとの PCI DSS 対策などで詳細なレポートが必要な企業もいらっしゃると思うので、そこは一回いくらという形でレポート作成オプションを出すというのはいかがでしょうか？

とにかく「速さ」と「手軽さ」は VAddy の最大の強みなので、将来機能追加をされる場合でもその強みは失わないで欲しいと思います。

株式会社ネットフォレスト

設立
2000 年 4 月

代表者
代表取締役社長　高橋佑至

所在地
横浜本社

〒221-0052　横浜市神奈川区栄町 5 番地 1
横浜クリエーションスクエア 16F

事業内容
1．Web デザイン･Web システムの開発 (企画立案から運用まで)
2．ネットワーク・サーバの設計・構築・運用
3．インターネットサービスプロバイダー事業
4．セキュリティ製品の販売・サポート (Dr.Web、脆弱性診断)
5．ホテルコンサルティング事業 (VOD システム販売等)

※事例取材時情報

先行事例 3

ヴェルク株式会社様

「VAddyは利用者がやらなくてはいけないことが少ない」

主な業務	サービスの規模	脆弱性検査での課題
業務・経営管理 システムの開発	有料導入 1000 社	自分たちでセキュリティテストをやろうとしたが 正しく使えているのか不安だった。

診断内製化のパターン

業種：自社サービス　利用者：開発者　シーン：毎日の自動検査

都内で受託開発業務と自社サービスを手がけているヴェルク株式会社。近年では自社サービス「board」における顧客サポートとセキュリティへの独自の取り組みが同業他社からの注目を浴びています。今年（2016 年）にはベストベンチャー100 にも選出されたヴェルク株式会社の代表取締役田向祐介氏にお話を伺いました。

ヴェルク株式会社について

弊社の事業の中心は Web アプリケーションやスマホアプリの受託開発業務です。もともと私が前職で業務系のシステムに携わっていたので、業務系のアプリケーション開発を強みとしていますが、ゲームなどのエンターテイメント系のシステム以外は幅広く対応できます。
2013 年からは受託開発で得たノウハウをフィードバックする形で、自社サービスの提供を始めました。特に、2014 年にリリースしたクラウド型業務・経営管理システム「board」はおかげさまで順調に売上を伸ばしています。
自社サービスの運用で得られた経験を、受託開発のお客様にも積極的に提案させて頂いています。

board

サービスリリース時から セキュリティは意識していた

board はサービスリリース当初からセキュリティに力を入れていました。
業務・経営管理システムという性質上、お預かりするデータの取扱いは特に慎重にならないといけません。もちろん、いかなるデータも重要ではあるのですが、board がお預かりするデータは会社経営の核となるものなので、「漏れてはいけない度合い」が高い。情報漏洩のリスクに対してはかなり神経質にやっています。

受託開発業務の中でお客様が診断会社に脆弱性診断を依頼されたのを何度か見てきたので、セキュリティに対する意識は自然と高まっていました。

ヴェルク株式会社様

VAddy は利用者がやらなくてはいけないことが少ない

board のリリース前には診断会社に脆弱性診断をお願いしましたが、その時 WAF[注1] の Scutum を入れる前提だったので、WAF でカバーできない領域を重点的に診断していただくようお願いしました。

現在でも機密データの暗号化はもちろんのこと、WAF や IDS・IPS[注2] などの侵入対策や弊社内アクセス管理など、考えうる対策は可能な限りとっています。

それまでもセキュリティテストツールを試してはみたが・・・

board を始める前、OWASP ZAP を使って自分たちでセキュリティテストをやろうとしたことがありましたが、正直言ってめんどくさかった（笑）

セキュリティテストツールは正しく使えないと意味がありません。自分たちの勉強不足といえばそれまでですが、当時はツールを正しく使えているのかどうかが分かりませんでした。
使い方を理解する時間が取れるのであれば強力なツールになると思いますが、私たちのようなアプリケーション開発者がカジュアルに使うにはハードルが高い。せっかくセキュリティテストをやっているのに、正しく使えてるのか不安になるようでは本末転倒だなと。

その点、VAddy は利用者がやらなくてはいけないことが少ない。クロール[注3] さえできていれば、後は自動で検査してくれます。クロールが正しく行えたかどうかのサーバーのログを見れば判断できます。VAddy は利用者の責任範囲が非常に狭いのです。

セキュリティにかけるコスト

セキュリティは非常に専門性の高い領域です。私はサービスの料金というのは専門性の高さに応じて上がるべきだと考えているので、VAddy の料金（月額 $100）は Web サービスとしては高く感じるかもしれませんが、その分の価値はあると思っています。

幸い弊社では受託開発で得た利益を board の開発に回すことができたので、セキュリティにも比較的余裕をもって費用をかけることができましたが、限られた予算の中でプロジェクトを進めなければならないスタートアップでは、セキュリティに回す予算が無いこともあるかもしれません。ただ、VAddy の料金程度のコスト（月額 $100）で安全を担保できるのであれば、やっておくべきでじゃないかと思いますね。

VAddy の導入で変わったこと

VAddy の導入をきっかけに、board の End to End テスト（以下 EtoE テスト）を整備するようになりました。VAddy を使うためには検査対象のアプリケーションを正しくクロールする必要があるのですが、board のような画面数の多いアプリケーションを手動クロールするのは現実的では無いので、EtoE テストを整備する必要があったのです。

board では EtoE テストのシナリオを、単体テスト的なものと結合テスト的なものにわけています。結合テストのシナリオには VAddy 用のクロールとしては重複する項目がたくさんあって、全てを VAddy の検査対象にすると時間がかかりすぎるので、VAddy のスキャンには単体テストのシナリオ

ヴェルク株式会社様

VAddy は利用者がやらなくてはいけないことが少ない

だけを使っています。

今は VAddy のクロールデータを 20 個くらいに分けていて、一日に一回スケジュール実行させています。CircleCI 上で VAddy Ruby クライアントツールを使って VAddy のスキャンを自動実行していて、結果は Slack に通知するようにしています。

ちなみに、VAddy にクロールデータを流す時は Selenium を使ってますが、普段は CircleCI 上で PhantomJS を使って EtoE テストを行っています。

EtoE テストの整備は確かに面倒な作業ではあります。ただ、お客様からするとブラウザで正しく操作できることが全てです。例えばサーバーサイドで Ruby のアプリケーションが正しく動いたとしても、フロントの JavaScript が動かなかったら意味が無いですよね（笑）
そういう意味でも EtoE テストは整備しておいたほうが安心です。

それ以外には、VAddy を使うことでセキュリティ知識も増えてきたことを感じています。
セキュリティは意図的にそれに触れていないと知識はなかなか入ってきません。VAddy の検査ログ（注：テストサーバーのアクセスログ）を見るとかなり勉強になりますしね。
めったにありませんが、万が一脆弱性が見つかった場合でも原因と対策を調べることで、セキュリティの知識が上がっていきます。
VAddy を使うことで日常的にセキュリティに触れるようになったことが大きいと思います。

代表取締役　田向祐介様

VAddy に望むこと

あまり思いつかないのですが、あえて言うとクロールデータのメンテナンス性が高まると良いかなと感じています。現在は一画面に収まる程度のシナリオ数ですが、これがもっと増えていった時にメンテナンスが大変になりそうなので。

検査項目は今のままで良いと思います。さほど重要じゃない検査項目が追加されてスキャン時間が長くなるのも困りますし。もし検査項目が増えるのであれば、スキャン毎に実施する検査項目が選べるようになると良いかもしれませんね。デイリーのスキャンはこれとこれ、ウィークリーのスキャンはこれとこれといった感じで。

注 1 Web Application Firewall：Web アプリケーションを狙った攻撃を防御する仕組み
注 2 Intrusion Detection System/ Intrusion Prevention System：サーバーへの侵入を検知し、防御する仕組み
注 3 検査対象となる Web アプリケーションの URL やパラメータを VAddy に記録するための設定

ヴェルク株式会社様

VAddy は利用者がやらなくてはいけないことが少ない

インタビューを終えて

今回お話を伺った中で、田向氏が非常にバランス感覚の優れた方という印象を受けました。

少ない人数で運営されている board が、製品の質だけでなく顧客サポートやセキュリティ対策で注目を集めているのは、ビジネス全体を見渡すことができる田向氏のバランス感覚によるものだと思います。

そのように考えると、board で同業他社から問い合わせが来るほどのセキュリティ対策が取られているのも当然のことかもしれません。

ヴェルク株式会社

代表者

代表取締役　田向祐介

所在地

東京都新宿区市谷田町 2-29-1 こくほ 21 ビル 5 階

事業内容

1．クラウド型業務・経営管理システム「board」
2．スマホアプリ CMS「Patto」の提供
3．Web アプリケーション・スマホアプリ開発
4．データ分析

※事例取材時情報

先行事例 4

グルー株式会社 様

「セキュリティテストの実施が営業活動での強みになる」

主な業務	脆弱性検査での課題
動画配信系サービスの開発・運用／受託開発業務	「セキュリティ品質」を意識されるお客様に対して、自社のセキュリティ対策では訴求力が弱かった。

診断内製化のパターン

業種：受託開発　利用者：開発者　シーン：納品前検査

福岡で動画配信技術を中心とした自社サービスの開発と受託開発業務を行っている、グルー株式会社 代表取締役 迫田氏に VAddy 導入の経緯とその効果を伺いました。

グルー株式会社とは

フリーランスエンジニアとして受託開発を中心に約 8 年間活動した後、自社サービスの提供を目的に、2011 年に法人化しました。現在は自社サービスと受託開発業務を並行して行っています。動画配信系のサービス（Gemediar、1meeting）の開発／運用で培った知見が受託開発にも活かされています。自社サービスは社内のエンジニア 2 人で開発していますが、受託開発業務は外部のパートナー様に協力いただきながら行っています。

自分たちだけではセキュリティテストは難しかった。

社内のエンジニアだけで開発を行っていた当初はセキュリティも含めた品質は担保できていましたが、業務の拡大とともに外部の開発パートナーさんに協力いただくようになってから、パートナーさんと自分たちとのセキュリティ意識がずれる可能性がでてきました。

受託開発業務の方でお付き合いさせていただいている大手企業様の方では、年に一回まとまった規模の脆弱性診断を実施されています。その際は弊社もお手伝いしているのですが、準備や報告も含めてかなり重い作業だなという印象を持っていたので、それを私たちだけで行うのはノウハウや予算の点で現実的ではありませんでした。

その点、VAddy は特別なセキュリティ知識が無くても使えるので、外部のパートナーさんも含めた弊社の開発チーム全体のセキュリティ品質を担保する

グルー株式会社様

セキュリティテストの実施が営業活動での強みになる

には最適なツールでした。そもそも VAddy を知る前はコードレビューによる脆弱性検査以外の方法が無いか悩んでいて、ソースコードの確認やミドルウェアやフレームワークを最新に保つ等の一般的な対策しかできていませんでしたので。

オープンソースのセキュリティテストツールも試してみましたが、お客様への訴求度という意味では少し弱かったです。やはり、セキュリティ専門の業者が提供している有償のツールを使って継続的に脆弱性検査をしていますとお伝えしたほうが安心して頂けました。

VAddy を使っていることが受託開発での強みになる

近年、クライアント企業の中でセキュリティ意識が高まっていることを感じています。クライアント企業（発注元）としては発注先が「きちんと作っているか」が当然気になりますが、中でも「セキュリティ品質」を意識されるお客様が増えてきました。

営業活動において品質を客観的にアピールすることは難しいのですが、セキュリティに関しては「VAddy を使っています」とはっきり言えるようになったことは大きいですね。自社で Web Application Firewall（編注：Scutum）を開発・運用していて、実際の攻撃に対する知見を持っている会社が作ったツールなので間違いないですよと、私たちも言いやすい。新しいお客様との打ち合わせの際では、社内で VAddy を使ったセキュリティテストを回していることをお伝えしていて、お客様もそのことに価値を感じて頂けています。

コスト的にも月 1 万円程度ですむので、自社の開発コストとして十分カバーできる範囲です。今後は弊社が提供する価値の一つとして積極的にアピールして行きたいですね。

VAddy の導入で変わったメンバーの意識

VAddy を使うようになってから、外部の開発パートナーの意識も変わってきたように感じます。

ご協力いただいている開発パートナーさんも弊社でセキュリティテストを実行していることをご存知なので、実装方法について事前に質問されることが増えました。それまでが適当だったという意味ではありませんが、VAddy の導入をきっかけに、セキュリティに限らず広い意味での品質に対する意識が以前より高まりました。

また、お客様にも継続的なセキュリティテストの実施をご理解いただいたので、「この脆弱性は大丈夫ですか？」といった類の質問はほとんど無くなりました。

今後は自社サービスにも導入していきます

現在はまだ VAddy は受託開発にしか導入できていないのですが、準備が整い次第自社サービスにも順次導入していきます。先日リリースした「”社内限定”動画学習サイト ノービル」では取り扱う顧客情報も多くなるので、早急導入しています。

グルー株式会社様

セキュリティテストの実施が営業活動での強みになる

※今回のインタビューは、グルー株式会社が提供するビデオ会議サービス「1meeting」を利用して福岡と東京を繋いで行われました。ユーザー登録不要でブラウザのみで利用できるので、手軽にビデオミーティングが始められます。通話品質も良く、快適なインタビューになりました。

グルー株式会社

代表者

代表取締役　迫田孝太

所在地

福岡市中央区荒戸 1-1-3 大濠 JOY ビル 5F

事業内容

1．動画配信に特化したインフラの提供
2．インターネット関連事業
3．ソフトウェア開発事業

※事例取材時情報

VADDY（バディ）

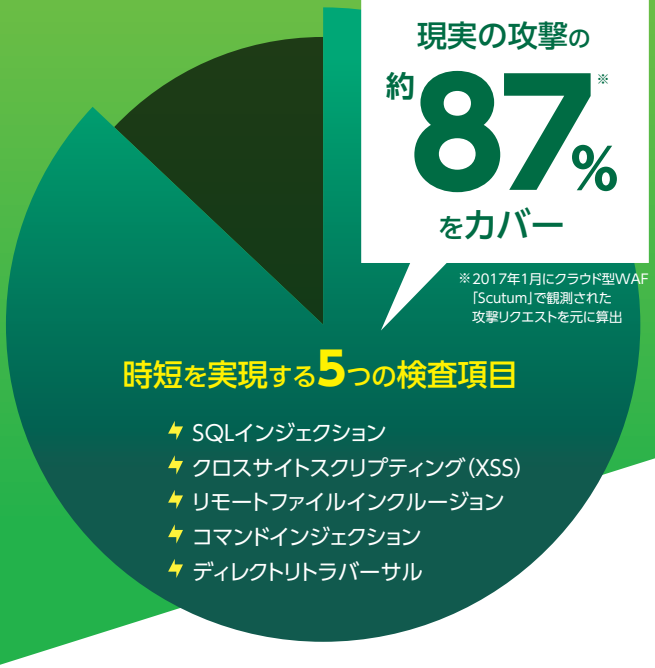
いま最も手軽で高速な クラウド型Web脆弱性検査ツール

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。

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