クラウド型Webアプリケーション脆弱性診断ツール

VAddy - バディ-

Webアプリケーション脆弱性診断をすべての人へ

VADDY

運営会社紹介／沿革／業務内容

運営会社紹介

株式会社ビットフォレスト

所在地	［東京本社］ 東京都千代田区神田錦町1-17-5 Daiwa神田橋ビル 8F ［福岡オフィス］ 福岡県福岡市中央区天神4-6-28 天神ファーストビル 6F
代表者	代表取締役　高尾 都季一

沿革

2002年2月	有限会社ビットフォレストとして設立
2007年1月	株式会社ビットフォレストに商号変更
2009年6月	Scutum販売開始
2015年9月	VAddy販売開始
2024年10月	Loggol販売開始

業務内容

運用フェーズで守る

- クラウド型Webアプリケーションファイアウォール
  「Scutum」の開発・運用
  https://www.scutum.jp/

Scutum

開発フェーズで守る

- クラウド型Web脆弱性診断ツール
  「VAddy」の開発・運用・販売
  https://vaddy.net/ja/

VADDY

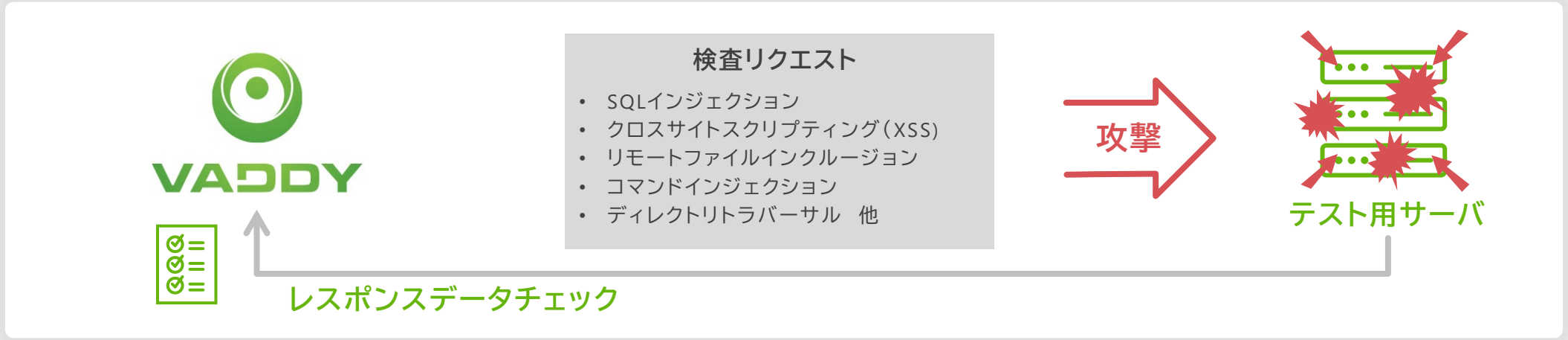
現状を正しく把握する

- Web攻撃ログ分析ツール
  「Loggol」の開発・運用・販売
  https://www.loggol.jp/

Loggol

VAddyとは？

2015年に製品化された、もっとも手軽で高速な
ブラックボックス型Web脆弱性検査ツールです。



こんな方々にご利用いただいています

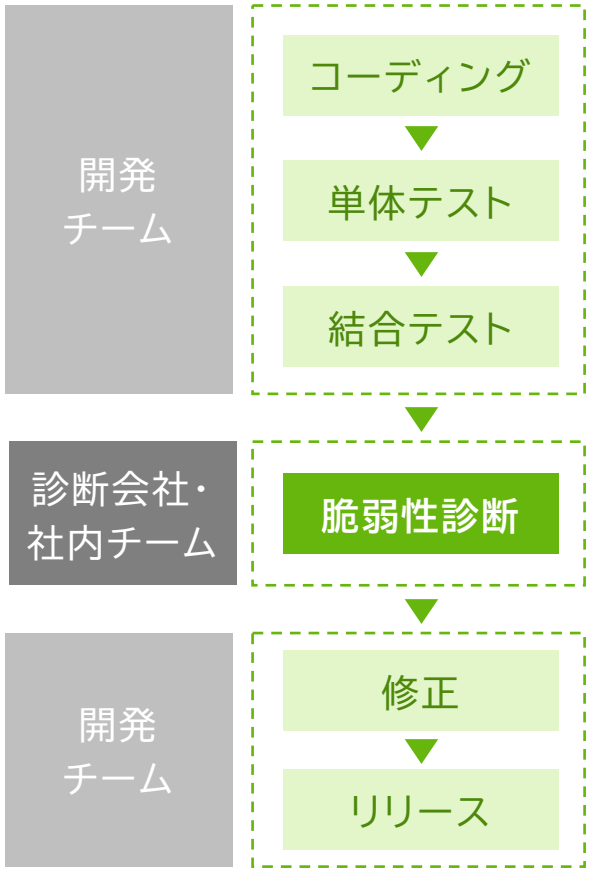
- 開発部門
- 品質管理部門
- インフラ部門
- 情報システム部門

こんな場面でご利用いただいています

- 開発途中で検査
- 受け入れテスト時に検査
- 納品／リリース前に検査
- 毎日の定期検査

これまでのWebアプリケーション脆弱性診断の課題

通常、脆弱性診断は全ての開発工程が終了した後に、
外部の診断会社や社内のセキュリティ部門（品質管理部門）で実施されます。



費用の問題

外部の診断会社に
依頼する場合の費用は
一回検査で
数十万円～数百万円

自社で行う場合も既存の脆弱性検査ツールの費用は
年間200万程度～

隠れた費用として、開発工程の
最後で実施することによる
手戻りコストも見逃せない

工期の問題

診断会社に依頼する場合の期間は
数日～数週間

特に診断の依頼が増える年末／
年度末は依頼から着手まで長時間
待たされることも

自社で診断ツールを利用する場合、
設定～検査～検査結果の解析まで
一週間程度～

手戻りによる
開発工程への影響

スキルの問題

自社で診断ツールを利用する場合

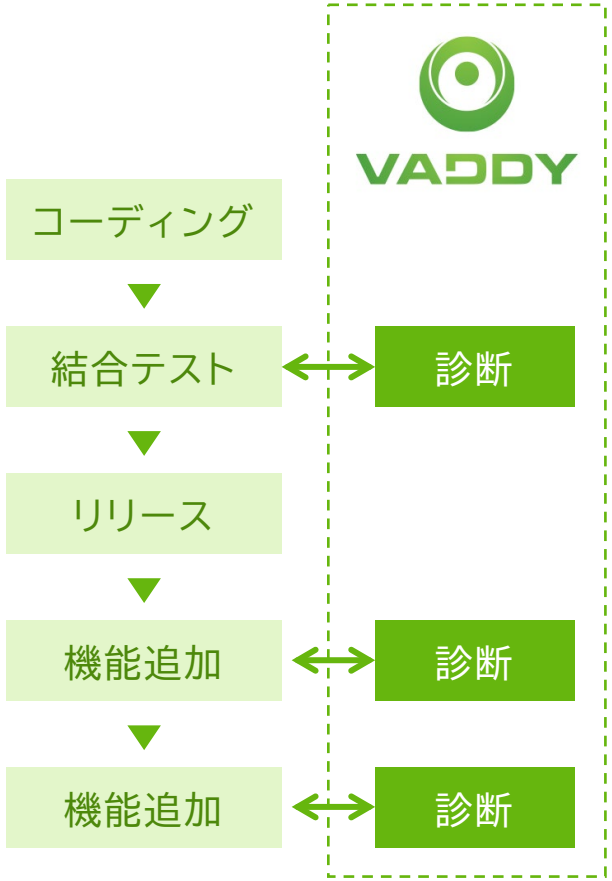
初めて脆弱性診断ツールを利用
する場合、メーカーが提供している
トレーニングプログラム
を受けることが必須

診断結果を適切に判断し、
改修指示を出すためにも
知見が必要

SaaS型サービスで、機能追加や改修ごとの検査、
小規模プロジェクトでの脆弱性検査は**事実上不可能**

Webアプリケーション脆弱性検査を全ての人へ

開発の初期段階から**何度でも**。
費用やスケジュールを気にすること無く脆弱性検査を実施できます。



費用の問題	工期の問題	スキルの問題
VAddyは**完全月額固定料金** 何度検査を実施しても 料金に変動なし	Webサイトからのサインアップから **最短10分で検査を開始**	事前のトレーニングは不要。 **インターネットに触れている方であれば、利用可能**
初期費用無し、 **最低利用期間1ヶ月**から ご利用可能	平均検査時間12分という **高速な検査**で毎日の検査を実現	全てのお客様が**オンラインマニュアルとチャットサポートだけで**脆弱性診断を実現
診断サイクルに合わせて **契約／停止が自由**	開発の初期段階から継続的に診断を実施することで、 **開発の手戻りを大幅に削減**	必要最低限の診断により、 診断結果の**解析負荷を低減**

もう脆弱性検査が「できない」理由はありません

最低限の工数でIPA基準+αの脆弱性を診断

- Webアプリケーション
- フレームワーク
- ミドルウェア
- OS
- サーバー
- ネットワーク

VAddy Advancedプランの検査項目（18個）

情報処理推進機構（IPA）
安全なウェブサイトの作り方チェックリスト

- SQLインジェクション
- ブラインドSQLインジェクション
- クロスサイト・スクリプティング
- コマンドインジェクション
- ディレクトリトラバーサル
- HTTPヘッダインジェクション
- CSRF
- メールヘッダインジェクション
- クリックジャッキング
- バッファオーバーフロー
- セッション管理の不備
- アクセス・認可制御の不備

＋

実際に観測される攻撃の上位から選定された基準

- リモートファイルインクルージョン
- 安全でないデシリアイゼーション
- XXE
- SSRF脆弱性
- 非公開ファイル検査
- Evalインジェクション

IPAのチェックリストに実際の攻撃データから選定された診断項目を追加

市場における手動脆弱性診断と診断ツールの位置づけ

検査内容

自動ツール診断向け製品群

開発／情シス／QA向け

VADDY

年間20万円～／ライセンス

セキュリティエンジニア向け

他社A

他社B

年間200～300万円／ライセンス

手動脆弱性診断

100万円～／回

費用

追加オプション／プランで一般的な脆弱性診断基準にも対応

Advancedプラン

IPA 安全なウェブサイトの作り方（チェックリスト）	
1	SQLインジェクション
2	OSコマンド・インジェクション
3	パス名パラメータの未チェック／ディレクトリトラバーサル
4	セッション管理の不備
5	クロスサイトスクリプティング
6	CSRF（クロスサイト・リクエスト・フォージェリ）
7	HTTPヘッダ・インジェクション
8	メールヘッダ・インジェクション
9	クリックジャッキング
10	バッファオーバーフロー
11	アクセス制御や認可制御の欠落

手動脆弱性診断チケット付きプラン

OWASP TOP 10 2021	
A1	アクセス制御の不備
A2	暗号化の失敗
A3	インジェクション
A4	安全が確認されない不安な設計
A5	セキュリティの設定ミス
A6	脆弱で古くなったコンポーネント
A7	識別と認証の失敗
A8	ソフトウェアとデータの整合性の不具合
A9	セキュリティログとモニタリングの失敗
A10	サーバーサイドリクエストフォージェリ(SSRF)

検査できる環境、組織管理機能

検査できる環境、アプリケーション

- フォーム認証（ログイン画面）を含むアプリケーション
- SSO（Single Sign On）を利用するアプリケーション
- 複数のFQDNをまたぐアプリケーション
- REST APIサーバ
- SPA
- URLパスに含まれるパラメータ
- CSRF対策トークンを含むアプリケーション
- イントラネット内や開発PC上のアプリケーション（1FQDNのみ）

検査例

例えば、検査したいURLが下記の場合
http://example.com/search.php?keyword1=foo&keyword2=bar

keyword1のデータ foo を検査用のデータに差し替えて検査対象サーバに送ります。
そのレスポンスの状況を確認して、脆弱性の有無を判定します。
http://example.com/search.php?keyword1=**foo**&keyword2=ba
http://example.com/search.php?keyword1=**foo<script>vaddy</script>&**keyword2=bar...

keyword1 の検査が完了した後に、同じように**keyword2**に対しても検査を実行します。

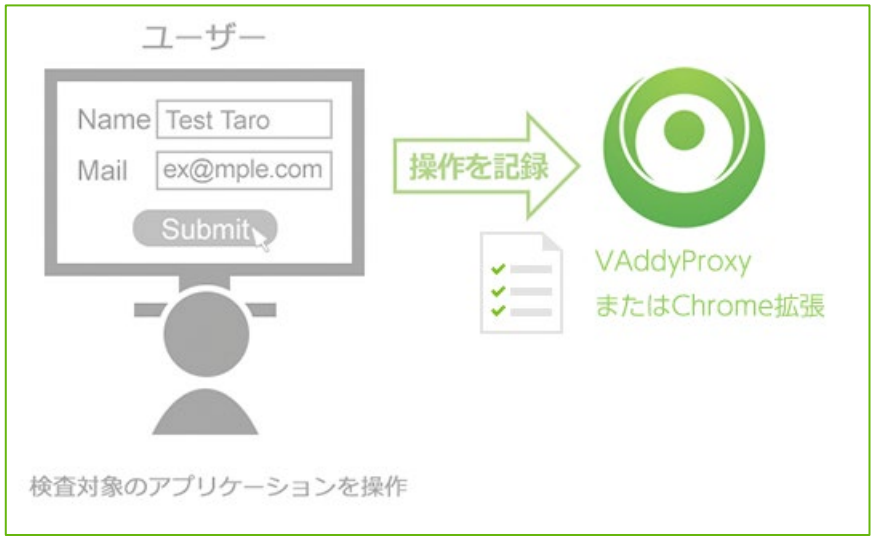
組織管理機能

共同利用する**ユーザーを一元管理**することができます。
自社社員の「誰がどのように」VAddyアカウントを
利用しているかをひと目で把握できます。

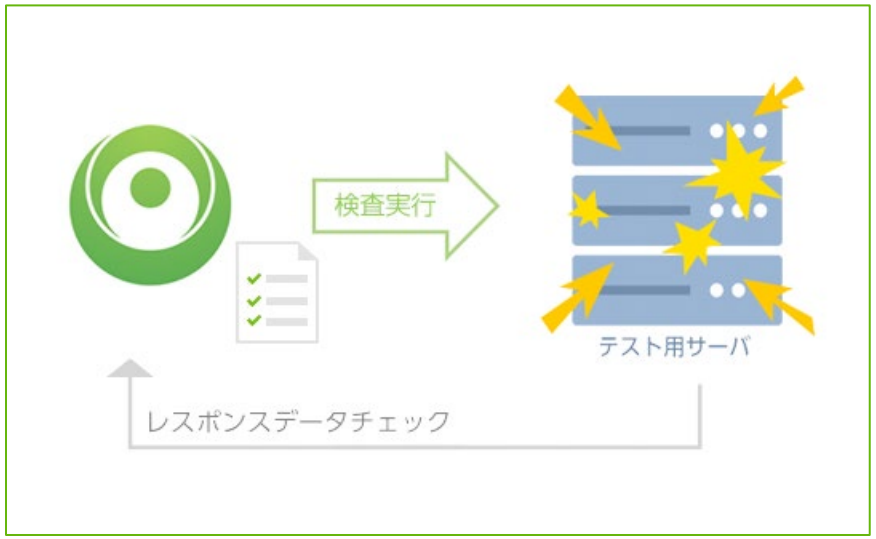
Advanced / Enterpriseプラン

VAddyの検査の流れ

VAddyは**お客様が作成したテストシナリオ**に沿った検査を実施します。



1. お客様のアプリケーションの操作（画面遷移）をテストシナリオとしてVAddyに記録します。



2. 作成されたテストシナリオに沿って検査を実施します。

- **アプリケーションを理解しているお客様**自身でテストシナリオを作成することで**網羅的に検査**が可能
- 機能ごとにシナリオを作成して**小さいサイクルでの診断を実施**

レポート

発見した脆弱性一覧

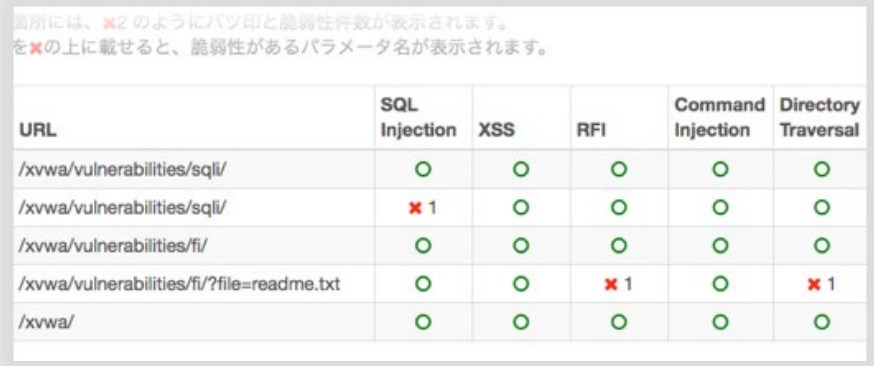
脆弱性があったURL、パラメータ名、脆弱性の種別が表示されます。

リクエストデータ

脆弱性を発見した際に送信した検査リクエストのデータが参照できます。
お手元で問題の再現をする際に便利です。

レスポンスデータ

脆弱性を発見した際に受信したレスポンスデータが参照できます。
どのようなエラーだったのか、XSSの場合はhtmlのどの箇所が
エスケープされていなかったのか確認できます。



全体の検査レポート

脆弱性の発見の有無に関わらず、どのURLに検査したのか、
問題があったURLはどこかをレポートで一覧表示します。
全体の把握や、上長への報告などにご利用に便利です。

VAddyご利用プラン

お客様のご利用シーンに合わせたプランをご用意しています。

診断 18 項目
全ての機能が使える

Advanced

IPA「安全なウェブサイトの作り方(チェックリスト)」全項目と合わせて診断ができるプラン

月額 99,800円

診断 11 項目
必要最低限の診断を

Enterprise

組織管理機能と幅広い検査項目を備えたプラン。アカウント管理が必要な大規模組織向けプラン

月額 59,800円

診断 5 項目
手軽にお試し

Professional

攻撃の発生頻度が高い5つの脆弱性を効率的に検査。組織の規模や業種を問わずご利用いただけるミニマムプラン

月額 19,800円

Vaddyの年間ライセンスに、SHIFT SECURITYの手動脆弱性診断を＋（プラス）！

脆弱性診断・検査といえば SHIFT SECURITY

Advanced
＋ 手動脆弱性診断

Advanced +

年額 1,398,000円

Enterprise
＋ 手動脆弱性診断

Enterprise +

年額 998,000円

Professional
＋ 手動脆弱性診断

Professional +

年額 598,000円

VAddy基本プラン料金

		Advanced	Enterprise	Professional
検査項目数		18（IPA対応）	11	5
チーム機能	チームメンバー	無制限／FQDN	無制限／FQDN	50ユーザー／FQDN
組織管理	組織メンバー	30ユーザー	30ユーザー	
機能	スキャン回数	無制限	無制限	無制限
	スキャン上限時間	8時間／回	5時間／回	2時間／回
	スキャン一括実行	✓	-	-
	スキャン同時実行	3	3	1
	ローカル環境への検査	✓	✓	✓
	検査可能サイト数（FQDN）	3	3	3
料金	基本利用料（税別）	月額 99,800円 年額 998,000円	月額 59,800円 年額 598,000円	月額 19,800円 年額 198,000円

手動脆弱性診断付きプラン

脆弱性診断・検査といえば SHIFT SECURITY

VAddyの基本プラン（年間ライセンス）に、
セキュリティ対策のエキスパート「SHIFT SECURITY」によるサポートが付いたプランです。

各プランに付属する診断チケットは、**OWASP TOP10（※）に準拠した手動脆弱性診断**の他、プラットフォーム診断、脆弱性対応サポートなど幅広い用途でご利用いただけます。

※ **OWASP TOP10**
米国のNPO団体、OWASP (Open Web Application Security Project) が、
四年に一度発表している「最も重大なウェブアプリケーションリスクトップ10」

OWASP TOP 10 2021	
A1	アクセス制御の不備
A2	暗号化の失敗
A3	インジェクション
A4	安全が確認されない不安な設計
A5	セキュリティの設定ミス
A6	脆弱で古くなったコンポーネント
A7	識別と認証の失敗
A8	ソフトウェアとデータの整合性の不具合
A9	セキュリティログとモニタリングの失敗
A10	サーバーサイドリクエストフォージェリ(SSRF)

		Advanced ＋ 手動脆弱性診断	Enterprise ＋ 手動脆弱性診断	Professional ＋ 手動脆弱性診断
		Advanced ＋	**Enterprise ＋**	**Professional ＋**
VAddy		Advanced 年間契約	Enterprise 年間契約	Professional 年間契約
診断チケット		20チケット		
料金	基本料金（年額）	1,398,000円	998,000円	598,000円
	追加診断チケット	150,000円／10チケット		

VAddyオプション料金

		Advanced	Enterprise	Professional
検査可能サイト数追加	FQDN追加*	月額 10,000円/FQDN 年額 100,000円/FQDN	月額 10,000円/FQDN 年額 100,000円/FQDN	月額 6,000円/FQDN 年額 60,000円/FQDN
組織メンバー追加		月額 15,000円/10ユーザー 年額 150,000円/10ユーザー	月額 15,000円/10ユーザー 年額 150,000円/10ユーザー	

*追加したいFQDNが多数の場合はお問い合わせください。

VAddy料金例

Advancedを
10FQDNで利用する場合

VAddy Advanced	99,800円
FQDN追加	70,000円 （10,000x7）
月額合計	169,800円 （税抜）

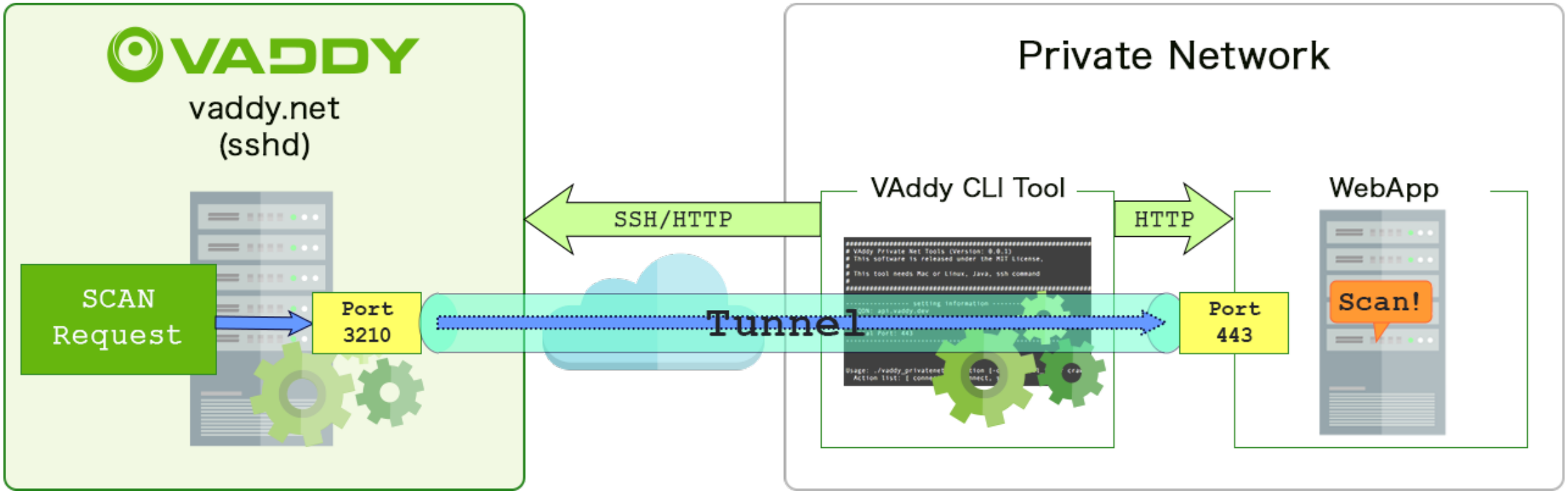
Vaddy検査項目

			Advanced	Enterprise	Professional
検査項目	SQLインジェクション	※	✓	✓	✓
	ブラインドSQLインジェクション	※	✓	✓	
	XSS	※	✓	✓	✓
	RFI		✓	✓	✓
	コマンドインジェクション	※	✓	✓	✓
	ディレクトリトラバーサル	※	✓	✓	✓
	安全でないデシリアイゼーション		✓	✓	
	XXE		✓	✓	
	HTTPヘッダインジェクション	※	✓	✓	
	SSRF脆弱性		✓	✓	
	非公開ファイル検査		✓	✓	
	CSRF	※	✓		
	メールヘッダ・インジェクション	※	✓		
	クリックジャッキング	※	✓		
	バッファオーバーフロー	※	✓		
	セッション管理の不備	※	✓		
	アクセス・認可制御の不備	※	✓		

（※）独立行政法人情報処理推進機構（IPA）の安全なウェブサイトの作り方に掲載されている脆弱性の種類

ローカル環境への診断 - PrivateNet版

- ssh コマンドのポート転送機能を利用して、インターネット上の VAddy サーバーとローカルネットワークの Web アプリとの間でトンネルを作成し、安全な経路で VAddy から Web アプリにアクセスします。
- 動作環境: Linux / FreeBSD / macOS (いずれも x86)



VAddyの利用シーン

業態	受託開発会社	SaaSベンダー	SaaSベンダー
利用サイクル	納品前	開発工程	リリース前
利用者	開発チーム／ディレクター	開発チーム	QA（品質管理）チーム／インフラチーム
備考	• セキュリティチェックシート対策 • 全ての案件で自主的に診断を実施することをルール化 • 動作確認の「ついでに」脆弱性診断	• 開発工程での診断の実施で手戻りコスト削減 • 定期診断／納品前診断との併用 • 新人トレーニングの一環	• セキュリティチェックシート対策 • 脆弱性診断を品質管理の一環と定義

業態	OSS開発会社	その他	その他
利用サイクル	開発工程	定期診断	受入検査
利用者	開発チーム	情報システム部門	プロジェクトマネージャー
備考	• コミッターの品質管理 • 診断の完全自動化	• セキュリティを兼任する「一人情シス」 • 複数のWebサイトを順に定期診断	• 開発を外部委託した場合、動作確認と併せて診断

導入企業

集英社

ManpowerGroup

BIPROGY

オージス総研

KDDI Web Communications

SEPTENI

DENTSU DIGITAL

NHS

ECOMOTT

carview

Everidays

EC CUBE

beyond

他 約500社　2024年1月現在

本資料についてのお問い合わせ

株式会社ビットフォレスト
VAddy事業部

info@vaddy.net

VAddy
http://vaddy.net/ja/

VAddy技術ブログ
http://blog-ja.vaddy.net/

X(Twitter)
https://x.com/vaddynet