

本当にできる！

Webアプリケーション 脆弱性診断内製化ツール

セキュリティエンジニア不在の現場でも使えるVAddyが

本当の脆弱性診断の内製化を実現します

今までの検査では
**リリースが
間に合わない！**

毎回脆弱性診断するには
**高すぎて
手が出せない！**

脆弱性検査ツールは
**難しくて
使いこなせない！**

現実の攻撃の
約 **90%**
をカバー

※2019年7月にクラウド型
WAF[Scutum]で観測された
攻撃リクエストを元に算出

厳選された**10**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ド(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
- ブラインドSQLインジェクション
- 安全でないデシリアライゼーション
- XML外部実体攻撃(XXE)
- HTTPヘッダインジェクション
- SSRF脆弱性

VADDYは短時間で効果の高い検査を実現

VADDY



サインアップ/検査対象
URL・パラメータを登録

開発の初期段階から繰り返し
実施できます

※2017年のVAddyユーザーの
平均スキャン時間から作成

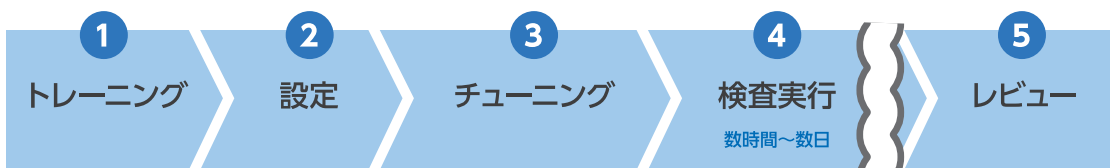
VAddyが検出するのはリスクが高い
脆弱性のため、修正の優先順位を検討
する必要はありません。

検査所要時間

約**30分**

検査完了までの時間が短いから
何度も検査実施できる！

一般的な
脆弱性検査ツール



開発元、販売元から
トレーニングを受ける

・ツールのインストール
・検査対象URL・パラメータを
登録

・アプリケーションに合わせたチューニング
(ログイン設定、CSRF設定など)
・初期設定で不要な機能を外す、必要な機
能を追加など

検査完了までの待ち時間が数時間
～数日間程度かかるため
開発の最終工程で実施

ツールが出力する膨大なレポー
トを解析し、優先順位づけをし
た後に対応の検討

検査所要時間 約**1ヶ月**

レポート

Result Details			
脆弱性検査の結果、問題を見ました。下記の詳細を確認ください。			
脆弱性種別	URL	脆弱性があるパラメータ名	検査データ
ディレクトリトラバース	/xvwa/vulnerabilities/?file=readme.txt	file	Request Response
Remote File Inclusion	/xvwa/vulnerabilities/?file=readme.txt	file	Request Response
SQLインジェクション	/xvwa/vulnerabilities/sql/	search	Request Response

発見した脆弱性一覧

```
hello :  
  
38  
aaa<script src=http://www.example.jp/vaddy1.js></script>  
12  
  
<br/>  
hello2 :
```

脆弱性を発見した際に受信したレスポンスデータ

Vulnerability	URI	Vulnerable
クロスサイトスクリプティング	?/name=aaa&name2=bbb	name

```

GET /?name=aaa%3Cscript&src=3Dhttp%3A%2F%2Fwww.example.jp%2Fvaddy1.js%3E%3C%2Fscript%3E&name2=bbb HTTP/1.1
Host: vaddytest.ichikaway.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.12; rv:57.0) Gecko/20100101 Firefox/57.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: ja,en-US;q=0.7,en;q=0.3
Referer: http://vaddytest.ichikaway.com/
Authorization: Basic eWFZdTpzaGk=
Connection: keep-alive

```

検査リクエストのデータ確認

JURL	SQL Injection	XSS	RFI	Command Injection	Directory Traversal
'xvwa/vulnerabilities/sqli/'	○	○	○	○	○
'xvwa/vulnerabilities/sqli/'	✖ 1	○	○	○	○
'xvwa/vulnerabilities/fi/'	○	○	○	○	○
'xvwa/vulnerabilities/fi/?file=readme.txt	○	○	✖ 1	○	✖ 1
'xvwa/'	○	○	○	○	○

全体の検査レポート

VAddy 基本プラン

診断10項目 全ての機能が使える

診断5項目 必要最低限の診断を

	Enterprise 年額 ¥598,000	Professional 年額 ¥198,000
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ド(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 ブラインドSQLインジェクション 安全でないデシリアライゼーション XML外部実体攻撃(XXE) HTTPヘッダインジェクション SSRF脆弱性	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ド(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
チーム機能 メンバー数	無制限／プロジェクト	50ユーザー／プロジェクト
組織管理 メンバー数	30ユーザー	
スキャン回数	無制限	無制限
スキャン上限時間	5時間／回	2時間／回
スキャン履歴	過去2年分	過去2年分
ローカル環境への検査	○	○
検査レポートダウンロード	○	○
Web API / CI連携	○	○
検査対象FQDN	3	3
基本利用料	年額 ¥598,000	年額 ¥198,000
お支払い方法	銀行振込(請求書発行)	銀行振込(請求書発行)
FQDN追加	年額 ¥100,000/FQDN	年額 ¥60,000/FQDN
組織メンバー追加	年額 ¥150,000/FQDN	

※価格は税別です。

本件に関するお問い合わせ