VAddy脆弱性検査報告書

https://vaddy.net/ja/

検査結果

検査番号
804546-7594ad06-5cff-4295-affe-ba8b239aa643

プロジェクト名
「app3アプリ」

検査対象サーバ
- app3.vaddy-demo.com

検査日時
2024-04-23 14:52:01 - 2024-04-23 15:09:10

検査実行ユーザ
開発ユーザ

脆弱性件数
21 件

検査リクエスト総数
225 件

検査結果

検査項目	検査URL数	脆弱性件数
SQLインジェクション	11	0
ブラインドSQLインジェクション	0	0
XSS(反射型)	11	20
XSS(蓄積型)	11	0
リモートファイルインクルージョン	11	0
コマンドインジェクション	11	0
ディレクトリトラバーサル	11	0
ヘッダインジェクション	11	0
XXE	11	0
安全でないデシリアライゼーション	11	0
SSRF	11	0
非公開ファイル検査	11	0
CSRF	11	0
メールヘッダインジェクション	11	0
クリックジャッキング	11	1
バッファオーバーフロー	11	0
セッション管理不備	11	0
アクセス・認可制御不備	11	0

検査項目解説

検査対象URLのパラメータ毎に、検査用データをセットしてVAddyから検査対象サーバにHTTPリクエストを送信します。
そのレスポンスを確認し、脆弱性の有無を判定します。
以下にVAddyが検査対象としている脆弱性について解説します。

SQLインジェクション（危険度　High）

SQL文のエラーが出るような検査データを送信し、HTTPレスポンスのステータスやエラー文言などを確認します。情報漏洩や改ざんに繋がるため対策必須となります。

ブラインドSQLインジェクション（危険度　High）

画面やHTTPレスポンスステータスからはSQLインジェクションか判定できない場合でも、画面の反応速度の遅延などで脆弱性がないか判定します。 情報漏洩や改ざんに繋がるため対策必須となります。

クロスサイトスクリプティング（危険度　High/Medium）

Htmlタグを含む検査データを送信し、HTTPレスポンスでそれらがエスケープされているか確認します。検査は、反射型XSSと蓄積型XSSを確認します。 反射型は検査リクエスト送信時のレスポンスで発見したXSS、蓄積型は検査リクエスト送信後に別の画面で後から発見したXSSです。
危険度は、XSSがどのように発動するかによりますが、セッションハイジャックや、なりすましに繋がるケースもあるため対策をおすすめします。

コマンドインジェクション（危険度　High）

OSのコマンドが実行できるような検査データを送信します。コマンドが実行されたかをレスポンスを確認して判断します。情報漏洩や改ざんに繋がるため対策必須となります。

リモートファイルインクルージョン（危険度　High）

リモートファイルを読み込み、任意のコードが実行できるような検査データを送信します。コードが実行されたかをレスポンスを確認して判断します。情報漏洩や改ざんに繋がるため対策必須となります。

ディレクトリトラバーサル （危険度　High）

OS内のファイルが外部から表示できるような検査データを送信し、そのファイル内容が表示されているか確認します。情報漏洩に繋がるため対策必須となります。

ヘッダインジェクション（危険度　High/Medium）

HTTPレスポンスヘッダを動的に生成しているサイトに対し改行コードを入れるリクエストを送り、ヘッダ情報が改ざんされないか確認します。改ざんに繋がるため対策必須となります。

XXE(XML External Entity)（危険度　High）

送信されたXMLを処理するアプリケーションに対してXMLの外部実体参照が行われるXML検査データを送信し、外部参照されないか確認します。情報漏洩や改ざんに繋がるため対策必須となります。

安全でないデシリアライゼーション（危険度　High）

シリアライズされたデータを外部入力として扱っているアプリケーションに対し、改ざんしたシリアライズデータが入力可能か検査します。情報漏洩や改ざんに繋がるため対策必須となります。

SSRF（危険度　High）

外部入力のURL文字列に対して、そのまま該当URLにコンテンツを取りに行く処理があるか検査します。クラウドインフラのメタデータが取得されてしまうと情報漏洩や改ざんに繋がるため対策必須となります。

非公開ファイル検査（危険度　High）

検査対象サーバのURLパスに対して、.git/config、.svn/entriesファイル、.envファイルが公開されていないか検査します。これらのファイルが公開されている場合は機密情報の漏洩に繋がるため対策必須となります。

CSRF検査（危険度　High/Medium）

POST/PUT/DELETE/PATCHメソッド時にCSRF対策のトークンが存在するか検査します。存在しない場合はCSRF攻撃に対して脆弱なため対策が必要です。

メールヘッダインジェクション検査（危険度　High/Medium）

メールのヘッダが外部から不正に変更されないか検査します。対策が不十分な場合は迷惑メールの踏み台に使われるため対策が必要です。

クリックジャッキング検査（危険度　High/Medium）

レスポンスヘッダに「X-Frame-Options」もしくは「Content-Security-Policy: frame-ancestors」が無い場合に検出します。本検査は他の検査のレスポンスを元に判定します。1件でも検出されると以降そのFQDNでは検査を行わないため検出数はFQDNごとに最大1件になります。

バッファオーバフロー検査（危険度　High）

入力文字列を長い文字列にしてバッファオーバフローが発生しないか検査します。ミドルウェアなど構成しているアプリケーションによって対策の要・不要は異なります。

セッション管理不備の検査（危険度　High）

ログイン前後でセッションIDが変わっているか検査します。セッションIDが変化しない場合はセッション固定化攻撃に対して脆弱なため対策が必要です。

アクセス・認可制御不備の検査（危険度　High）

ログイン情報と同じものがcookieの中に入っていないか検査します。同じものが入っている場合にcookieの書き換えで他者になりすませる可能性がありますが、対策の要・不要はアプリケーションによって異なります。

検査結果詳細

スキャンID : 804546-7594ad06-5cff-4295-affe-ba8b239aa643
クロールID : 272

SQLインジェクション

Method	FQDN	URL	脆弱性件数
GET	app3.vaddy-demo.com	/	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0

ブラインドSQLインジェクション

ブラインドSQLインジェクション検査は、DBサーバの指定がない場合に未検査となります。

Method	FQDN	URL	脆弱性件数
GET	app3.vaddy-demo.com	/	-
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	-
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	-
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	-
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	-
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	-
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	-
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	-
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	-
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	-
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	-

XSS(反射型)

Method	FQDN	URL	脆弱性件数
GET	app3.vaddy-demo.com	/	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	2
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	2
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	2
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	2
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	2
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	2
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	2
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	2
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	2
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	2

XSS(蓄積型)

Method	FQDN	URL	脆弱性件数
GET	app3.vaddy-demo.com	/	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0

リモートファイルインクルージョン

Method	FQDN	URL	脆弱性件数
GET	app3.vaddy-demo.com	/	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0

コマンドインジェクション

Method	FQDN	URL	脆弱性件数
GET	app3.vaddy-demo.com	/	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0

ディレクトリトラバーサル

Method	FQDN	URL	脆弱性件数
GET	app3.vaddy-demo.com	/	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0

ヘッダインジェクション

Method	FQDN	URL	脆弱性件数
GET	app3.vaddy-demo.com	/	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0

XXE

Method	FQDN	URL	脆弱性件数
GET	app3.vaddy-demo.com	/	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0

安全でないデシリアライゼーション

Method	FQDN	URL	脆弱性件数
GET	app3.vaddy-demo.com	/	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0

SSRF

Method	FQDN	URL	脆弱性件数
GET	app3.vaddy-demo.com	/	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0

非公開ファイル検査

Method	FQDN	URL	脆弱性件数
GET	app3.vaddy-demo.com	/	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0

CSRF

Method	FQDN	URL	脆弱性件数
GET	app3.vaddy-demo.com	/	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0

メールヘッダインジェクション

Method	FQDN	URL	脆弱性件数
GET	app3.vaddy-demo.com	/	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0

クリックジャッキング

Method	FQDN	URL	脆弱性件数
GET	app3.vaddy-demo.com	/	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	1
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0

バッファオーバーフロー

Method	FQDN	URL	脆弱性件数
GET	app3.vaddy-demo.com	/	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0

セッション管理不備

Method	FQDN	URL	脆弱性件数
GET	app3.vaddy-demo.com	/	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0

アクセス・認可制御不備

Method	FQDN	URL	脆弱性件数
GET	app3.vaddy-demo.com	/	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0
GET	app3.vaddy-demo.com	/?name=aaa&name2=bbb	0

参考情報

独立行政法人 情報処理推進機構（IPA）が提供している
「ウェブアプリケーションセキュリティ実装 チェックリスト」
との対応

検査項目	検査URL数	脆弱性件数
SQLインジェクション	11	0
クロスサイトスクリプティング	11	20
コマンドインジェクション	11	0
パス名／パラメータ名の未チェック／ディレクトリトラバーサル	11	0
セッション管理の不備	11	0
CSRF	11	0
HTTPヘッダインジェクション	11	0
メールヘッダ・インジェクション	11	0
クリックジャッキング	11	1
バッファオーバーフロー	11	0
アクセス制御や認可制御の欠落	11	0

※本表はお客様が実施した検査内容と、独立行政法人 情報処理推進機構（以下、IPA）が提供している「ウェブアプリケーションセキュリティ実装 チェックリスト」との対応を表したものです。
　IPAはこの検査結果について何らかの保証を与えるものではございません。

お問い合わせ先

株式会社ビットフォレスト
VAddy事業部
info@vaddy.net