

VAddy脆弱性検査報告書



<https://vaddy.net/ja/>

検査結果

検査番号

130-6a5a3e7f-b6b7-4d78-b0db-60aad64f7eb4

プロジェクト名

「http://demo.vaddy-demo.com/xss/」

検査対象サーバ

- demo.vaddy-demo.com

検査日時

2021-09-22 11:00:03 - 2021-09-22 11:00:37

検査実行ユーザ

test3 vaddy3

脆弱性件数

4 件

検査リクエスト総数

51 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	4	0
ブラインドSQLインジェクション	4	0
XSS(反射型)	4	2
XSS(蓄積型)	4	0
リモートファイルインクルージョン	4	0
コマンドインジェクション	4	0
ディレクトリトラバース	4	0
ヘッダインジェクション	4	0
XXE	4	0
安全でないデシリアライゼーション	4	0
SSRF	4	0
非公開ファイル検査	4	1

検査結果（検査項目追加オプション）

検査項目	検査URL数	脆弱性件数
CSRF	4	0
メールヘッダインジェクション	4	0
クリックジャッキング	4	1
バッファオーバーフロー	4	0
セッション管理不備	4	0
アクセス・認可制御不備	4	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インジェクションが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うか確認します。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。

検査項目追加オプションの項目解説

CSRF検査

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

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

クリックジャッキング対策ができていないか検査します。レスポンスヘッダにX-Frame-Optionsがなければ検知します。

バッファオーバーフロー検査

入力文字列を長い文字列にしてバッファオーバー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

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

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。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 : 130-6a5a3e7f-b6b7-4d78-b0db-60aad64f7eb4
クローलID : 361

SQLインジェクション

Method	FQDN	URL	脆弱性件数
GET	demo.vaddy-demo.com	/favicon.ico	0
GET	demo.vaddy-demo.com	/	0
GET	demo.vaddy-demo.com	/xss/	0
GET	demo.vaddy-demo.com	/xss/?name=aa&tel=	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	demo.vaddy-demo.com	/favicon.ico	0
GET	demo.vaddy-demo.com	/	0
GET	demo.vaddy-demo.com	/xss/	0
GET	demo.vaddy-demo.com	/xss/?name=aa&tel=	0

XSS(反射型)

Method	FQDN	URL	脆弱性件数
GET	demo.vaddy-demo.com	/favicon.ico	0
GET	demo.vaddy-demo.com	/	0
GET	demo.vaddy-demo.com	/xss/	0
GET	demo.vaddy-demo.com	/xss/?name=aa&tel=	2

XSS(蓄積型)

Method	FQDN	URL	脆弱性件数
GET	demo.vaddy-demo.com	/favicon.ico	0
GET	demo.vaddy-demo.com	/	0
GET	demo.vaddy-demo.com	/xss/	0
GET	demo.vaddy-demo.com	/xss/?name=aa&tel=	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	demo.vaddy-demo.com	/favicon.ico	0
GET	demo.vaddy-demo.com	/	0
GET	demo.vaddy-demo.com	/xss/	0
GET	demo.vaddy-demo.com	/xss/?name=aa&tel=	0

コマンドインジェクション

Method	FQDN	URL	脆弱性件数
GET	demo.vaddy-demo.com	/favicon.ico	0
GET	demo.vaddy-demo.com	/	0
GET	demo.vaddy-demo.com	/xss/	0
GET	demo.vaddy-demo.com	/xss/?name=aa&tel=	0

ディレクトリトラバーサル

Method	FQDN	URL	脆弱性件数
GET	demo.vaddy-demo.com	/favicon.ico	0
GET	demo.vaddy-demo.com	/	0
GET	demo.vaddy-demo.com	/xss/	0
GET	demo.vaddy-demo.com	/xss/?name=aa&tel=	0

ヘッダイnjekション

Method	FQDN	URL	脆弱性件数
GET	demo.vaddy-demo.com	/favicon.ico	0
GET	demo.vaddy-demo.com	/	0
GET	demo.vaddy-demo.com	/xss/	0
GET	demo.vaddy-demo.com	/xss/?name=aa&tel=	0

XXE

Method	FQDN	URL	脆弱性件数
GET	demo.vaddy-demo.com	/favicon.ico	0
GET	demo.vaddy-demo.com	/	0
GET	demo.vaddy-demo.com	/xss/	0
GET	demo.vaddy-demo.com	/xss/?name=aa&tel=	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	demo.vaddy-demo.com	/favicon.ico	0
GET	demo.vaddy-demo.com	/	0
GET	demo.vaddy-demo.com	/xss/	0
GET	demo.vaddy-demo.com	/xss/?name=aa&tel=	0

SSRF

Method	FQDN	URL	脆弱性件数
GET	demo.vaddy-demo.com	/favicon.ico	0
GET	demo.vaddy-demo.com	/	0
GET	demo.vaddy-demo.com	/xss/	0
GET	demo.vaddy-demo.com	/xss/?name=aa&tel=	0

非公開ファイル検査

Method	FQDN	URL	脆弱性件数
GET	demo.vaddy-demo.com	/favicon.ico	0
GET	demo.vaddy-demo.com	/	0
GET	demo.vaddy-demo.com	/xss/	1
GET	demo.vaddy-demo.com	/xss/?name=aa&tel=	0

CSRF (検査項目追加オプション)

Method	FQDN	URL	脆弱性件数
GET	demo.vaddy-demo.com	/favicon.ico	0
GET	demo.vaddy-demo.com	/	0
GET	demo.vaddy-demo.com	/xss/	0
GET	demo.vaddy-demo.com	/xss/?name=aa&tel=	0

メールヘッダインジェクション (検査項目追加オプション)

Method	FQDN	URL	脆弱性件数
GET	demo.vaddy-demo.com	/favicon.ico	0
GET	demo.vaddy-demo.com	/	0
GET	demo.vaddy-demo.com	/xss/	0
GET	demo.vaddy-demo.com	/xss/?name=aa&tel=	0

クリックジャッキング (検査項目追加オプション)

Method	FQDN	URL	脆弱性件数
GET	demo.vaddy-demo.com	/favicon.ico	1
GET	demo.vaddy-demo.com	/	0
GET	demo.vaddy-demo.com	/xss/	0
GET	demo.vaddy-demo.com	/xss/?name=aa&tel=	0

バッファオーバーフロー (検査項目追加オプション)

Method	FQDN	URL	脆弱性件数
GET	demo.vaddy-demo.com	/favicon.ico	0
GET	demo.vaddy-demo.com	/	0
GET	demo.vaddy-demo.com	/xss/	0
GET	demo.vaddy-demo.com	/xss/?name=aa&tel=	0

セッション管理不備 (検査項目追加オプション)

Method	FQDN	URL	脆弱性件数
GET	demo.vaddy-demo.com	/favicon.ico	0
GET	demo.vaddy-demo.com	/	0
GET	demo.vaddy-demo.com	/xss/	0
GET	demo.vaddy-demo.com	/xss/?name=aa&tel=	0

アクセス・認可制御不備 (検査項目追加オプション)

Method	FQDN	URL	脆弱性件数
GET	demo.vaddy-demo.com	/favicon.ico	0
GET	demo.vaddy-demo.com	/	0
GET	demo.vaddy-demo.com	/xss/	0
GET	demo.vaddy-demo.com	/xss/?name=aa&tel=	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	4	0
クロスサイトスクリプティング	4	2
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	4	0
セッション管理の不備	4	0
CSRF	4	0
HTTPヘッダインジェクション	4	0
メールヘッダ・インジェクション	4	0
クリックジャッキング	4	1
バッファオーバーフロー	4	0
アクセス制御や認可制御の欠落	4	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ありません。

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