VAddy脆弱性検査報告書

Sample

https://vaddy.net/ja/

検査結果

検査番号

804510-5eee4910-82a6-4d03-bed2-f201fbaa4f8b

プロジェクト名

「サイト検査 サンプル」

検査対象サーバ

- www.example.com
- vaddy.example.com

検査日時

2018-11-29 18:01:47 - 2018-11-29 18:02:06

検査実行ユーザ

TestUser1

脆弱性件数

2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	5	0
クロスサイトスクリプティング(XSS)	5	2
コマンドインジェクション	5	0
リモートファイルインクルージョン	5	0
ディレクトリトラバーサル	5	0

検査項目内容

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。

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。

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。

検査結果詳細

スキャンID: 804510-5eee4910-82a6-4d03-bed2-f201fbaa4f8b
クロールID: 76 (テストシナリオ1)

SQLインジェクション

Method	FQDN	URL	脆弱性件数
GET	www.example.com	/xss_reflects/	0
GET	www.example.com	/xss-reflects/edit/44	0
POST	www.example.com	/xss-reflects/edit/44	0
GET	vaddy.example.com	/	0
GET	vaddy.example.com	/?name=aaa&name2=bbb	0

反射型XSS

Method	FQDN	URL	脆弱性件数
GET	www.example.com	/xss_reflects/	0
GET	www.example.com	/xss-reflects/edit/44	0
POST	www.example.com	/xss-reflects/edit/44	0
GET	vaddy.example.com	/	0
GET	vaddy.example.com	/?name=aaa&name2=bbb	1

蓄積型XSS

Method	FQDN	URL	脆弱性件数
GET	www.example.com	/xss_reflects/	0
GET	www.example.com	/xss-reflects/edit/44	0
POST	www.example.com	/xss-reflects/edit/44	0
GET	vaddy.example.com	/	0
GET	vaddy.example.com	/?name=aaa&name2=bbb	1

コマンドインジェクション

Method	FQDN	URL	脆弱性件数
GET	www.example.com	/xss_reflects/	0
GET	www.example.com	/xss-reflects/edit/44	0
POST	www.example.com	/xss-reflects/edit/44	0
GET	vaddy.example.com	/	0
GET	vaddy.example.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	www.example.com	/xss_reflects/	0
GET	www.example.com	/xss-reflects/edit/44	0
POST	www.example.com	/xss-reflects/edit/44	0
GET	vaddy.example.com	/	0
GET	vaddy.example.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	www.example.com	/xss_reflects/	0
GET	www.example.com	/xss-reflects/edit/44	0
POST	www.example.com	/xss-reflects/edit/44	0
GET	vaddy.example.com	/	0
GET	vaddy.example.com	/?name=aaa&name2=bbb	0

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