SecuAlive

診断 レポート

作成日 2019年8月29日19:15
作成者 ユーザー管理者

診断対象情報

グループ名	デモ用グループ
プロジェクト名	デモ用プロジェクト
サイト名	デモ用プロジェクト
サイトURL	https://demo.tworks.co.jp/mutillidae/

[1] 診断サマリー：ページ診断

ページ名	デモページ診断

()の中の値はレポート出力選択を行わない場合の合計です。

開始時間	2019年8月16日11:26
終了時間	2019年8月16日11:27
実行者	トライアルユーザー
クローリング	PROXYクローリング
対象URL数	4
テンプレート	トライアル
ログイン名	-

レベル	件数
CRITICAL	0
HIGH	8
MEDIUM	0
LOW	0
INFO	0

No	危険度	プラグイン名	件数
1	HIGH	SQLインジェクション（エラーメッセージ）	2
2	HIGH	SQLインジェクション(Time)	2
3	HIGH	クロスサイトスクリプティング	4

[1] 診断対象URL一覧

No	Method	ページ名	ターゲットURL
1	GET		https://demo.tworks.co.jp/mutillidae/
2	GET		https://demo.tworks.co.jp/mutillidae/
3	GET		https://demo.tworks.co.jp/mutillidae/index.php?page=pen-test-tool-lookup.php
4	POST		https://demo.tworks.co.jp/mutillidae/index.php?page=pen-test-tool-lookup.php

[1] 脆弱性別詳細

HIGH　2	SQLインジェクション（エラーメッセージ）
解説	外部から入力された値の正当性チェックを行なわずにSQLクエリで使用しているため、エラーが発生し画面にSQLエラーメッセージが表示されています。
リスク	使用しているデータベースの情報などの内部情報がエラーメッセージで表示されるため、取得した情報を足掛かりに攻撃される可能性があります。 また、エラーが発生する操作を連続して実行した場合、サーバーリソースの消費などによるレスポンス低下などの影響が発生する可能性があります。
解決方法	外部から取得した値をサーバー側でそのまま再利用するのではなく、値の正当性チェックを行い、SQLエラーメッセージは画面に表示しないでください。
その他情報	
CVSS2.0	
CVSS2.0 Vector	
CVSS3.0	
CVSS3.0 Vector	

検知情報

URL	https://demo.tworks.co.jp/mutillidae/index.php?page=pen-test-tool-lookup.php
対象パラメータ	ToolID
診断文字列	'
検知コード	
検知ヘッダー	
検知ボディ	MySQL server version You have an error in your SQL syntax
検知タイム	
検知サイズ	

[リクエストグループ ： 1]

リクエスト　1

リクエスト	
ヘッダー ボディー	POST https://demo.tworks.co.jp/mutillidae/index.php?page=pen-test-tool-lookup.php HTTP/1.1 Accept-encoding: gzip, deflate Accept: */* User- agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.79 Safari/537.36 Edge/14.14393 Content-type: application/x-www-form-urlencoded Accept-language: ja,en-US;q=0.7,en;q=0.3 Authorization: Basic dHdvcmtzOnR3dGVzdDEyMyE= Connection: keep-alive Upgrade-insecure-requests: 1 Referer: https://demo.tworks.co.jp/mutillidae/index.php?page=pen-test-tool-lookup.php Host: demo.tworks.co.jp Cookie: showhints=1; PHPSESSID=02ksec9smkmt8e3g7v3ja0iuh7 Content-length: 99 ToolID=0923ac83-8b50-4eda-ad81-f1aac6168c5c%27&pen-test-tool-lookup-php-submit-button=Lookup%2BTool
レスポンスヘッダー	
レスポンスタイム	0.038
コード	200
メッセージ	OK
サイズ	10252
ヘッダー	HTTP/1.1 200 OK Date: Fri, 16 Aug 2019 02:27:16 GMT Server: Apache Logged-In-User: X-XSS-Protection: 0 Strict-Transport-Security: max-age=0 Vary: Accept-Encoding Content-Encoding: gzip Content-Length: 10252 Connection: close Content-Type: text/html;charset=UTF-8

レスポンスボディ検出箇所

00910 : <tr><td class="error-label">File</td><td class="error-detail">/opt/mutillidae/classes/MySQLHandler.php</td></tr>
00911 : <tr><td class="error-label">Message</td><td class="error-detail">/opt/mutillidae/classes/MySQLHandler.php on line 211: Error executing query:

connect_errno: 0
errno: 1064
error: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near ''0923ac83-8b50-4eda-ad81-f1aac6168c5c''' at line 2
client_info: mysqlnd 5.0.12-dev - 20150407 - $Id: b5c5906d452ec590732a93b051f3827e02749b83 $
host_info: 127.0.0.1 via TCP/IP

) Query:
			SELECT	tool_id, tool_name, phase_to_use, tool_type, comment
			FROM 	pen_test_tools WHERE tool_id = '0923ac83-8b50-4eda-ad81-f1aac6168c5c''; (0) [Exception]
00912 : </td></tr>

該当箇所一覧

No	ﾒｿｯﾄﾞ	対象URL	対象 ﾊﾟﾗﾒｰﾀ	診断文字列	ｻｲｽﾞ	検知 ｺｰﾄﾞ	検知 ﾍｯﾀﾞｰ	検知 ﾎﾞﾃﾞｨ	検知 ﾀｲﾑ	検知 ｻｲｽﾞ
1	POST	https://demo.tworks.co.jp/mutillidae/index.php?page=pen-test-tool-lookup.php	ToolID	'	10252			MySQL server ve ...		
2	POST	https://demo.tworks.co.jp/mutillidae/index.php?page=pen-test-tool-lookup.php	ALL	'	10252			MySQL server ve ...		

[2] 脆弱性別詳細

HIGH　2	SQLインジェクション(Time)
解説	外部から入力された値がそのままSQLクエリに使用されています。
リスク	外部から受け渡される値を変更することにより、認証回避、本来の検索されないデータの表示や、権限のないデータの更新が行われる可能性があります。
解決方法	SQLインジェクション攻撃への最適な対策は、プログラム言語のデータベースライブラリに用意されているサーバサイドプリペアードステートメント※ の使用です。 プリペアードステートメントを使用するのが困難な場合は、外部から入力される値がSQLとして解釈されないよう、適切にエスケープ処理を行って下さい。 今回の場合であれば、特殊記号をエスケープする関数をSQL作成時に常に使用していることを確認してください。 また、保険的対策として、入力された値の文字種を厳密にチェックすることも有効です。 さらに、適切にエラー処理を行い、SQLエラーメッセージがブラウザへのレスポンスに含まれないようしてください。
その他情報	
CVSS2.0	6.4
CVSS2.0 Vector	AV:N/AC:L/Au:N/C:P/I:P/A:N
CVSS3.0	9.4
CVSS3.0 Vector	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:L

検知情報

URL	https://demo.tworks.co.jp/mutillidae/index.php?page=pen-test-tool-lookup.php
対象パラメータ	ToolID
診断文字列	'|(select sleep(10) from information_schema.tables)|'
検知コード	
検知ヘッダー	
検知ボディ	
検知タイム	10.021
検知サイズ	

[リクエストグループ ： 1]

リクエスト　1

リクエスト	
ヘッダー ボディー	POST https://demo.tworks.co.jp/mutillidae/index.php?page=pen-test-tool-lookup.php HTTP/1.1 Accept-encoding: gzip, deflate Accept: */* User- agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.79 Safari/537.36 Edge/14.14393 Content-type: application/x-www-form-urlencoded Accept-language: ja,en-US;q=0.7,en;q=0.3 Authorization: Basic dHdvcmtzOnR3dGVzdDEyMyE= Connection: keep-alive Upgrade-insecure-requests: 1 Referer: https://demo.tworks.co.jp/mutillidae/index.php?page=pen-test-tool-lookup.php Host: demo.tworks.co.jp Cookie: showhints=1; PHPSESSID=02ksec9smkmt8e3g7v3ja0iuh7 Content-length: 165 **ToolID**=0923ac83-8b50-4eda-ad81-f1aac6168c5c**%27%7C%28select+sleep%2810%29+from+information_schema.tables%29%7C%27**&pen-test-tool-lookup-php-submit-button=Lookup%2BTool
レスポンスヘッダー	
レスポンスタイム	**10.021**
コード	
メッセージ	
サイズ	-
ヘッダー	

該当箇所一覧

No	ﾒｿｯﾄﾞ	対象URL	対象 ﾊﾟﾗﾒｰﾀ	診断文字列	ｻｲｽﾞ	検知 ｺｰﾄﾞ	検知 ﾍｯﾀﾞｰ	検知 ﾎﾞﾃﾞｨ	検知 ﾀｲﾑ	検知 ｻｲｽﾞ
1	POST	https://demo.tworks.co.jp/mutillidae/index.php?page=pen-test-tool-lookup.php	ToolID	'|(select sleep(10) from information_schema.tables)|'					10.021	
2	POST	https://demo.tworks.co.jp/mutillidae/index.php?page=pen-test-tool-lookup.php	ALL	'|(select sleep(10) from information_schema.tables)|'					10.025	

[3] 脆弱性別詳細

HIGH　4	クロスサイトスクリプティング
解説	パラメーターにJavaScriptを挿入することにより任意のプログラムを実行することが可能です。
リスク	この脆弱性を悪用して、システムおよび利用ユーザーに被害が発生することが懸念されます。悪用例としては以下のことが考えられます。 ・セッションハイジャックによる機密情報、個人情報の漏洩 ・ユーザーが意図しない情報の送信 ・悪質なページへの誘導 ・表示ページの改竄 また、モバイル環境を対象としたサイトなど、JavaScript が実行される可能性が低いサイトであっても、HTMLを直接書き換えることで、ページの改竄、悪質なページへの誘導といった攻撃に利用される可能性があります。 Jsonデータの場合、ブラウザ側で表示前に特殊文字（<,>,",'等）のエスケープをエスケープしていない場合は、 Domによるクロスサイトスクリプティングが行われる可能性があります。 JsonレスポンスでContent-Type: application/jsonでなくContent-Type: text/htmlだった場合、 Jsonエスケープでは問題なくとも、ブラウザ上ではHTMLとして処理されJavascriptが実行されます。
解決方法	この脆弱性に対応するには、Web アプリケーションにおいて出力部分に応じた文字列の適切なエスケープ/エンコード処理を行うことが必要です。 「&」→「&」 「<」→「<」 「>」→「>」 「"」→「"」 「'」→「'」 Web アプリケーション開発時に以下を原則とすることで、クロスサイトスクリプティングを含め、多くの脆弱性による影響を大幅に緩和することが可能です。 ・入力値の形式や文字種別、桁数を厳密に定義し、正しい入力値のみを受け付けるように処理する。 　例：電話番号の値には10-12 桁の半角数字のみを許可など ・JavaScript などを使用したクライアント側での入出力チェックに依存せず、サーバー側で入出力チェックを行う。 なお、クロスサイトスクリプティングの原因は文字列処理が適切にされていないことに起因するため、本指摘事項以外にも、文字列処理を行う全ての部分に注意する必要があります。そのため指摘部分への対策だけではなく、アプリケーション全体の確認と対策を推奨いたします。 上記に加えて見落としや文字列処理の漏れを防止するため、以下のような対策が望まれます。 ・アプリケーションの出力に応じ、エスケープやエンコード処理を行う関数、ライブラリ、クラスを整備して使用する。 ・Web アプリケーションフレームワークを使用し、文字列処理やデータベースアクセスなどの重要な処理を一元化する。 また、システムの仕様上HTMLタグの入力を許可する場合は、全てのタグを許可するのではなく、必要最低限のタグのみを許可してください。 許可すべきではない要素例 ・スクリプトタグ ・フレーム関連タグ ・イベントハンドラ
その他情報	
CVSS2.0	5.8
CVSS2.0 Vector	AV:N/AC:M/Au:N/C:P/I:P/A:N
CVSS3.0	6.1
CVSS3.0 Vector	CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

検知情報

URL	https://demo.tworks.co.jp/mutillidae/index.php?page=scan%22+onMouseOver%3Dalert%28_1320__40840_%29%2F%2F%22
対象パラメータ	page
診断文字列	scan" onMouseOver=alert(_1320__40840_)//"
検知コード	
検知ヘッダー	

検知ボディ	<td></td><td>|</td> <td><a href="index.php?do=toggle-bubble-hints&page=scan" onMouseOver=alert(_1320__40840_)//"">
	<td><a href="index.php?do=toggle-security&page=scan" onMouseOver=alert(_1320__40840_)//"">
	<td><a href="index.php?do=toggle-enforce-ssl&page=scan" onMouseOver=alert(_1320__40840_)//"">

検知タイム	

検知サイズ	

[リクエストグループ ： 1]

リクエスト　1

リクエスト	
ヘッダー ボディー	GET https://demo.tworks.co.jp/mutillidae/index.php?page=scan%22+onMouseOver%3Dalert%28_1320__40840_%29%2F%2F%22 HTTP/1.1 Accept-encoding: gzip, deflate Accept: */* User- agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.79 Safari/537.36 Edge/14.14393 Accept-language: ja,en-US;q=0.7,en;q=0.3 Authorization: Basic dHdvcmtzOnR3dGVzdDEyMyE= Connection: keep-alive Upgrade-insecure-requests: 1 Referer: https://demo.tworks.co.jp/mutillidae/ Host: demo.tworks.co.jp Cookie: showhints=1; PHPSESSID=02ksec9smkmt8e3g7v3ja0iuh7

レスポンスヘッダー	
レスポンスタイム	0.029
コード	200
メッセージ	OK
サイズ	7620
ヘッダー	HTTP/1.1 200 OK Date: Fri, 16 Aug 2019 02:26:40 GMT Server: Apache Logged-In-User: X-XSS-Protection: 0 Strict-Transport-Security: max-age=0 Vary: Accept-Encoding Content-Encoding: gzip Content-Length: 7620 Connection: close Content-Type: text/html;charset=UTF-8

レスポンスボディ検出箇所

00069 : <td>|</td>
00070 : <td>Toggle Hints</td><td>|</td> <td>Show Popup Hints</td>
00071 : <td>|</td>

00071 : <td>|</td>
00072 : <td>Toggle Security</td>
00073 : <td>|</td>

00073 : <td>|</td>
00074 : <td>Enforce SSL</td>
00075 : <td>|</td>

該当箇所一覧

No	ﾒｿｯﾄﾞ	対象URL	対象 ﾊﾟﾗﾒｰﾀ	診断文字列	ｻｲｽﾞ	検知 ｺｰﾄﾞ	検知 ﾍｯﾀﾞｰ	検知 ﾎﾞﾃﾞｨ	検知 ﾀｲﾑ	検知 ｻｲｽﾞ
1	GET	https://demo.tworks.co.jp/mutillidae/index.php?page=pen-test-tool-lookup.php	page	scan" onMouseOver=alert(_1320__40840_)//"	7620			<td><a href="in ...		
2	POST	https://demo.tworks.co.jp/mutillidae/index.php?page=pen-test-tool-lookup.php	page	scan" onMouseOver=alert(_1320__40855_)//"	7623			<td><a href="in ...		
3	GET	https://demo.tworks.co.jp/mutillidae/index.php?page=pen-test-tool-lookup.php	page	_1320_SCAN<"'><script>alert(document.cookie)</script>_40840_	7639			"'><script>aler ...		
4	POST	https://demo.tworks.co.jp/mutillidae/index.php?page=pen-test-tool-lookup.php	page	_1320_SCAN<"'><script>alert(document.cookie)</script>_40855_	7643			"'><script>aler ...		

危険度について

診断で検出された問題は下記の基準で危険度を決定しています。
危険度:HIGH以上は早急な対応が必要になる問題です。

危険度	判定基準
CRITICAL	パスワード漏えい、管理者権限昇格など、システム全体に影響する問題です。 これらの問題が発生する可能性が極めて高く、即日対応する必要があります。
HIGH	情報漏洩や、なりすましなど、ユーザー被害が発生する可能性が高い問題です。 クロスサイトスクリプティングやSQLインジェクションなどの問題があり、インシデント報告やOWASP TOP10などで上位を占めるセキュリティ上の問題です。 このことから、早急に対応する必要があります。
MEDIUM	システムの設定情報や管理情報の漏洩等、システムに対する攻撃手段を提供する可能性がある問題です。 直接被害が発生する可能性は高くないですが、他のセキュリティ上の問題と組み合わさるとレベルが上がる可能性があります。 問題になる可能性があるため対策を検討してください。
LOW	バージョン情報表示や、バナー情報表示など、攻撃者の興味を引く可能性のある問題です。 直接悪用されるよりは、このレベルの情報から攻撃手法を絞っていくことがあります。 予防するうえで対策を検討してください。
INFO	品質やセキュリティのさらなる向上のために弊社が推奨する項目です。

暗号スイート確認の安全度

暗号スイート確認で検出された安全度はA～Fまでの7段階で分けれられています。
A -> F の順に安全度が下がっていきます。
安全度のレベル付は

Qualys SSL Labs Rating Guide - https://www.ssllabs.com/projects/rating-guide/

を参考におこなっています。

暗号スイート確認は

nmap - https://nmap.org/

を利用して行っています。

ご要望、不具合等のご連絡は下記までメール願います。

連絡先	secualive_admin@tworks.co.jp

株式会社トレードワークス