



SecuAlive

診断 レポート

作成日 2019年8月29日19:18
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：強制ブラウズ

()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22日18:49
終了時間	2019年8月22日18:52
実行者	TW_管理者
テンプレート	Standard
レベル	件数
CRITICAL	0
HIGH	0
MEDIUM	0
LOW	0
INFO	2

No	危険度	プラグイン名	件数
1	INFO	強制ブラウジング (PHP)	1
2	INFO	Robots.txtの検出	1

[1] 脆弱性別詳細

INFO	1	強制ブラウジング (PHP)
解説		既知のファイル、ディレクトリ名でアクセスをし、意図しない情報の公開が行われているか検査します。
リスク		公開されている情報が重要な場合、それだけで情報漏洩になります。 また公開されている情報を利用し、さらなる攻撃が行われる可能性があります。
解決方法		検出されたファイル、ディレクトリを確認し不要なものは削除するか、適切なアクセス制御をおこなってください。
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/phpmyadmin/
対象パラメータ	
診断文字列	phpmyadmin/
検知コード	200
検知ヘッダー	
検知ボディ	
検知タイム	
検知サイズ	

リクエスト 1

リクエスト

ヘッダー ボディ	<p>GET https://demo.tworks.co.jp/mutillidae/phpmyadmin/ HTTP/1.1 Connection: keep-alive Accept: */* Accept-encoding: gzip, deflate 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 Cookie: showhints=1; PHPSESSID=m4cr2e3h6q22ut66h80fubtnn0 Host: demo.tworks.co.jp</p>
-------------	--

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	1880
ヘッダー	<p>HTTP/1.1 200 OK Date: Thu, 22 Aug 2019 09:51:34 GMT Server: Apache Set-Cookie: phpMyAdmin=0khkvtb623p6qncov4ugm6p2dk0e3j1m; path=/mutillidae/phpmyadmin/; secure; HttpOnly Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: private, max-age=10800 Last-Modified: Fri, 06 Jan 2017 07:38:20 GMT Set-Cookie: pma_lang=en; expires=Sat, 21-Sep-2019 09:51:34 GMT; Max-Age=2592000; path=/mutillidae/phpmyadmin/; secure; HttpOnly Set-Cookie: pma_collation_connection=utf8_general_ci; expires=Sat, 21-Sep-2019 09:51:34 GMT; Max-Age=2592000; path=/mutillidae/phpmyadmin/; secure; HttpOnly Vary: Accept-Encoding Content-Encoding: gzip Content-Length: 1880 Connection: close Content-Type: text/html; charset=utf-8</p>

該当箇所一覧

No	メソッド	対象URL	対象 パラメータ	診断文字列	サイズ	検知 コード	検知 ヘッダ	検知 ボディ	検知 タイム	検知 サイズ
1	GET	https://demo.tworks.co.jp/mutillidae/phpmyadmin/	-	phpmyadmin/	1880	200				

[2] 脆弱性別詳細

INFO	1	Robots.txtの検出
解説		robots.txtへアクセス可能です。
リスク		robots.txtはクローラーエンジンに検出されたくないURL情報を記載します。 その為、外部へ非公開にしたいURLがrobots.txtによって公開され、攻撃者にとって有益な情報になる可能性があります。
解決方法		外部へ公開したくないURLはrobots.txtに記載せず、適切にアクセス制限を行い、外部からはアクセスできないように設定してください。
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/robots.txt
対象パラメータ	
診断文字列	/robots.txt
検知コード	200
検知ヘッダー	
検知ボディ	
検知タイム	
検知サイズ	

リクエスト 1

リクエスト

ヘッダー
ボディ

GET https://demo.tworks.co.jp/mutillidae/robots.txt HTTP/1.1
Connection: keep-alive
Accept: */*
Accept-encoding: gzip, deflate
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
Cookie: showhints=1; PHPSESSID=m4cr2e3h6q22ut66h80fubtnn0
Host: demo.tworks.co.jp

レスポンスヘッダー

レスポンスタイム

0.015

コード

200

メッセージ

OK

サイズ

126

ヘッダー

HTTP/1.1 200 OK
Date: Thu, 22 Aug 2019 09:50:42 GMT
Server: Apache
Last-Modified: Fri, 06 Jan 2017 07:38:20 GMT
ETag: "be-545681a143300-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 126
Connection: close
Content-Type: text/plain

該当箇所一覧

No	メソッド	対象URL	対象 パラメータ	診断文字列	サイズ	検知 コード	検知 ヘッダ	検知 ボディ	検知 タイム	検知 サイズ
1	GET	https://demo.tworks.co.jp/mutillidae/robots.txt	-	/robots.txt	126	200				

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はないですが、他のセキュリティ上の問題と組み合わせ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。 直接被害が発生する可能性は高くはないですが、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