Rworks

阪急阪神東宝グループ

法人向けセキュリティパッケージ

MSPがご提案する セキュリティ対策 サポートサービス。

株式会社アールワークスは、Managed Service Provider (MSP) として、
2001年よりシステム運用・セキュリティ管理サービスをご提供しています。

ツールによる脆弱性診断と、エンジニアによる分析・脆弱性解消。

＜定期対策にお薦め！＞

脆弱性診断ツールによる自動診断。エンジニアによる分析と脆弱性の解消までをワンストップでご提供。

SECURE AID

システムインフラの脆弱性診断、診断結果の分析、脆弱性の解消を代行

ツールによる脆弱性診断

OS・ミドルウェア・ネットワークの脆弱性を、「tenable.io™」を利用し自動診断いたします。tenable.io™ は、Tenable Network Security 社が提供する、サーバー・ネットワークシステムに対する脆弱性診断ツールです。脆弱性検知スキャナーには世界中で広く利用されている Nessus を用い定期診断を実施、診断結果を可視化し隠れたリスクを早期に把握できます。**tenable.io™ が提供する最新の脆弱性パターン用い、OS・ミドルウェア・ネットワークの脆弱性を診断します。**

診断項目

- Linux OS kernel 診断
- Windows OS kernel 診断
- FreeBSD OS kernel 診断
- HP-UX OS kernel 診断
- Solaris OS kernel 診断
- AIX OS kernel 診断
- ネットワーク機器 OS ファームウェア診断
- DoS 脆弱性診断
- バックドア有無診断
- DNS 脆弱性診断
- FTP サーバー脆弱性診断
- メールサーバー脆弱性診断
- Webサーバー脆弱性診断
- CMSソフトウェア脆弱性診断
  （バージョンに基づく診断）

脆弱性の分析

脆弱性診断結果とお客様システム固有の情報を合わせエンジニアが分析し、脆弱性のお客様システムへの重要度と対策を提示いたします。脆弱性対策の優先度、ユーザへのサービス提供への影響有無、影響がある場合の次善策などを、ご判断いただけます。

分析に利用する、お客様のシステム情報（例）

システム構成
- ネットワーク構成、IPアドレス情報
- パケットフィルタリング設定
- OSの種類とバージョン（RedHat Linux, Ubuntu Linux, Windows Serverなど）
- インストールされているミドルウェアとそのバージョン（apache, nginx, IIS, MySQL, PostgreSQL, MSSQL, perl, php など）
- 起動しているデーモン (httpd, sshd, ftpd など)
- ディレクトリ構成とパーミッション
- システム(OS) ユーザの登録状況

システムが提供しているサービス
- サイトの種類（ECサイト、予約サイト、情報ポータルサイト、ゲームサイト、など）
- サイトの主な機能（会員管理機能、通販のカート機能、情報検索機能、など）
- 主なユーザ（個人ユーザ、企業ユーザ、PCユーザ、スマホユーザ、など）

制約条件
- 動作要件（ブラウザにてアクセス、専用アプリにてアクセス、など）
- ブラウザ動作要件（サービス仕様として、バージョン X 以上の IE 対応、フィーチャーフォン対応をうたっている、など）

脆弱性の解消

診断・分析結果に基づき、弊社技術者がお客様に代わってシステムの脆弱性の解消を実施いたします。

対応内容

サーバー
- OS kernel、ライブラリのアップデート
- OS kernelパラメータ設定調整
- ミドルウエアのアップデート
- 脆弱性を回避するためのミドルウエアの設定調整

ネットワーク機器
- ネットワーク機器のファームウエアアップデート
- 脆弱性を回避するためのネットワーク機器設定調整

※お客様独自アプリケーション（開発ベンダにより作成されたものを含む）の修正対応は、ご提供外となります。
※対応作業は、リモートから実施します。対象サーバーやネットワーク機器へのログイン権限(管理者権限含む)を提供いただきます。
※有償OS(RedHat Enterprise Linux等)の場合は、アップデートパッケージを入手できるベンダーとのサポート契約をお客様にて締結いただいていることが条件となります。本番環境に対して対応を行う前にステージング環境に対して対応・確認を行う場合は、お客様にてステージング環境を準備いただくものとします。

ツールによるWebアプリケーションの脆弱性診断。

＜サービスリリース前の対策、定期対策にお薦め！＞

Webアプリケーションの脆弱性を自動診断。
最新の脆弱性情報をもとに、非侵入型スキャンをご提供。

Webアプリケーション診断

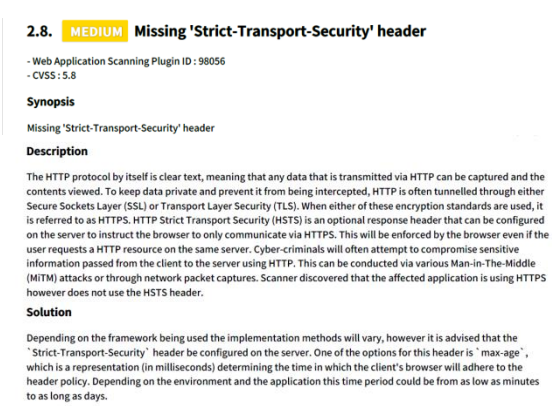
WEBアプリケーションの脆弱性を「tenable.io™ Web Application Scanning」を利用し、自動診断を行います。診断項目は、「NIST/NVD (CVSS Base Score)」に準拠しています。

tenable.io™ は、Tenable Network Security 社が提供する、Webアプリケーションの脆弱性診断ツールです。最新の脆弱性情報をもとに実施した診断結果は隠れたリスク可視化し、早期対処を可能にします。

区分	診断項目	診断内容
WEBサーバーミドルウェア	バックドア有無 書き込み可能なディレクトリ有無	誰でも書き込み可能なディレクトリの存在や、バックドアの存在を診断します。
	アクセス制御の状況 不要機能の有効化の有無	.htaccessなどによるアクセス制御設定の不備の有無や、公開ウェブサーバとして無効化されているべき設定が有効になっていないかどうかを診断します。(例: HTTP TRACE など)
	意図しない公開ウェブコンテンツ有無	サーバ情報を出力するサンプルプログラムへアクセスできる状態になっているかどうかや、バージョン管理ツールの管理ファイルなど、通常は外部に公開すべきではないプログラムやファイルの存在を確認します。(例: info.php, CVS/Entries など)
	CMSソフトウエア	Drupal, Joomla!, WordPress に関して、各ソフトウエア特有の脆弱性有無を診断します。
	その他ウェブサーバソフトウエア	WebDAV や Cookie の扱い、パストラバーサルなどの脆弱性有無を診断します。
WEBアプリケーション	認証、および、セッション	HTTP経由でのアプリケーションへの(ログイン認証によらない)ログインができるかを確認します。 (ログインアカウント・パスワードのbrute forceアタックは行いません。) また、セッショントークンの不正利用可否の確認をします。
	OSコマンドインジェクション コードインジェクション	フォームへ不正な内容を入力することによる、ユーザが任意のプログラムをサーバで実行可能な脆弱性の有無を確認します。
	インジェクション	SQL、noSQL、コード、LDAPに対するインジェクションの脆弱性有無を確認します。
	クロスサイトリクエストフォージェリ	意図しないリクエストがクライアントから送信された場合に、それを正しいリクエストとしてWebサーバが解釈してしまう脆弱性の有無を確認します。
	クロスサイトスクリプティング(XSS)	HTML要素のevent tag、パス、スクリプトコンテンツ、HTML tag などにより、XSS攻撃ができるような脆弱性がWebサーバに存在するかどうかを確認します。
	データエクスポージャー	ソースコード、システム内部のプライベートIPアドレス、バックアップファイルなどが外部から参照できる状態になっているかどうかを確認します。
	ファイルのインクルード	ローカルもしくは外部のファイルをインクルードして動作するコンテンツがあるかどうかを確認します。

診断レポート（英語）

検出された脆弱性を4段階で分析。対処方法も詳細にご提示いたします。



2.8. MEDIUM Missing 'Strict-Transport-Security' header

- Web Application Scanning Plugin ID : 98056
- CVSS : 5.8

Synopsis

Missing 'Strict-Transport-Security' header

Description

The HTTP protocol by itself is clear text, meaning that any data that is transmitted via HTTP can be captured and the contents viewed. To keep data private and prevent it from being intercepted, HTTP is often tunnelled through either Secure Sockets Layer (SSL) or Transport Layer Security (TLS). When either of these encryption standards are used, it is referred to as HTTPS. HTTP Strict Transport Security (HSTS) is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. This will be enforced by the browser even if the user requests a HTTP resource on the same server. Cyber-criminals will often attempt to compromise sensitive information passed from the client to the server using HTTP. This can be conducted via various Man-in-The-Middle (MiTM) attacks or through network packet captures. Scanner discovered that the affected application is using HTTPS however does not use the HSTS header.

Solution

Depending on the framework being used the implementation methods will vary, however it is advised that the `Strict-Transport-Security` header be configured on the server. One of the options for this header is `max-age`, which is a representation (in milliseconds) determining the time in which the client's browser will adhere to the header policy. Depending on the environment and the application this time period could be from as low as minutes to as long as days.

診断の流れ

お申込み	「SECURE-AID Apps 利用規約」をご参照の上、「セキュリティ診断実施同意書」をご記入・ご提出。
スキャン実施	２営業日以内に、当社にてスキャン設定、診断実施。
結果レポート自動送信	診断結果レポートを、ご指定のメールアドレスに自動通知。
脆弱性対応再診断	お客様にて脆弱性対応後、当社へご連絡いただき、再スキャンを実施。レポートにて、脆弱性が解消されていることを確認いただく。 （※再診断は初回より60日以内に実施するものとします）

SECURE-AID と SECURE-AID Apps の脆弱性診断項目 比較表

診断レイヤ	診断内容(主なもの)		SECURE-AID		SECURE-AID Apps	
OS	Linux OS kernel 診断		○		×	
	Windows OS kernel 診断		○		×	
	FreeBSD OS kernel 診断		○		×	
	HP-UX OS kernel 診断		○		×	
	Solaris OS kernel 診断		○		×	
	AIX OS kernel 診断		○		×	
	ネットワーク機器 OS ファームウエア診断		○		×	
ミドルウエア (一般に公開・配布されているパッケージソフトウエアを含む)	DoS脆弱性診断		○		×	
	バックドア有無診断		○	Web,ftp,メールサーバなど	△	Webサーバ機能のみ対象
	DNS脆弱性診断		○	キャッシュポイズニング、ACLバイパスなど	×	
	FTPサーバー脆弱性診断		○	バッファオーバーフロー、デフォルトパスワード、anonymous ftp 有効確認など	×	
	メールサーバー脆弱性診断		○	権限昇格、リモートコマンド実行など	×	
	Webサーバー脆弱性診断	アクセス制御・不要機能の有効化設定状況診断	○		○	
		意図しない公開コンテンツ有無診断	○	以下の漏洩有無 ・CSVディレクトリ ・バージョン番号 ・.htaccess ・info.php や、apache およびモジュールの status 情報ページなど ・その他	○	以下の漏洩有無 ・バックアップディレクトリ ・バックアップファイル ・クレジットカード番号 ・CVS/SVNユーザ ・メールアドレス ・プライベートIPアドレス ・ソースコード
		その他Webサーバソフトウエア診断(WebDAVの脆弱性、書き込み可能ディレクトリの存在など)	○		○	
		クロスサイトスクリプティング	○		○	
		SQLインジェクション	○	Apache 等ミドルウェアの過去バージョンで見つかっている脆弱性の診断	○	
	CMSソフトウエア診断(WordPress, Joomla!など)	クロスサイトスクリプティング	△	バージョン情報に基づく診断	○	プログラムコード診断
		SQLインジェクション	△	バージョン情報に基づく診断	○	プログラムコード診断
アプリケーション (お客様独自開発のソフトウエア)	認証および、セッション		×		○	
	Webアプリフォームへの不正データ入力によるコード実行		×		○	
	クロスサイトリクエストフォージェリ		×		○	
	クロスサイトスクリプティング(XSS)		×		○	
	ファイルのインクルード		×		○	
	○○インジェクション		×		○	SQL、noSQL、コード、LDAP インジェクション診断