example株式会社様
「example」セキュリティ診断計画書

Ver.1.0.0

作成日：2014年1月1日

バルテス株式会社

example株式会社様		バルテス	
承認	担当	承認	担当

改訂履歴

改訂日	バージョン	作成者	改訂内容及び理由
2014/1/1	Ver.1.0.0	VALTES	初版　作成

目次

1. 背景

example株式会社様（以下、example様）にて「example」を構築するに当たり
セキュリティの観点から第三者機関により客観的なセキュリティ診断を実施し、
発見された脆弱性に対して適切な対策を行うことでセキュアなサービスとして公開する要件を満たす為

2、目的

診断の目的は以下のとおりです。

1　Webシステムにセキュリティ面でのリスクがないかを確認します
　（以下、Webアプリケーション診断）

3. 診断対象

診断対象を以下に記載します

No	対象システム	使用技術	その他備考
1	example	別途ヒアリング	

4、診断概要

本診断は、下記の概要をもって行います。

ⅰ.Webアプリケーションセキュリティ診断

お客様システムに脆弱性がないかを以下の手段で診断します

1 診断用ツールを用いて、脆弱性の可能性がありそうな箇所を検知します（ツール診断）

2 1で検知した箇所について、重要と思われる箇所を手動で検証します（手動診断）

（参考）弊社サービスの特色について

ツール診断で用いる、弊社独自ツールの利点は以下の通りです。

1 攻撃性の低い診断用リクエストを用いて、診断を行います

2 診断リクエストの送信間隔など、お客様のリクエストに合わせて診断方針を柔軟に変更可能です

3 診断対象の特性に合わせて検出パターンを設定できるなど誤検知を少なくする工夫で
手動診断を効率的にサポートします

また、弊社のWebアプリケーションセキュリティ診断のサービス特徴は以下の通りです。

高い脆弱性検出率

熟練した技術者の診断ノウハウを手順化し、弊社独自のツールを利用することにより、
リーズナブルかつ高い脆弱性検出率を誇るサービスを提供します。

無償再診断

診断終了後、脆弱性の改修はお客様に大きな負担となります。
改修時のお問い合わせ対応や再診断も無償で実施し、対策完了までをフルサポートします。

綿密な診断計画

診断対象サイトの事前調査を行い、詳細な画面遷移図を作成します。
それをもとに、環境・ご予算に合わせた診断範囲、診断方法を提案します。

5、診断項目

Webアプリケーションセキュリティ診断の診断項目例は以下の通りとなります。

★:手動診断でないと検出できない脆弱性

脆弱性区分	脆弱性名	
認証	パスワードポリシー	★
	不適切な認証	★
	脆弱なパスワードリマインダ	★
承認	セッションの推測	★
	不適切な承認	★
	セッションの固定	★
クライアント側での攻撃	クロスサイトスクリプティング（XSS）	
	コンテンツの詐称	
	CSRF（Cross Site Request Forgeries）	★
コマンドの実行	バッファオーバーフロー	
	書式文字列攻撃	
	LDAPインジェクション	
	OSコマンドインジェクション	
	SQLインジェクション	
	SSIインジェクション	
	XPathインジェクション	
情報公開	ディレクトリインデクシング	
	ソース記載による情報漏えい	
	パストラバーザル	
	推測可能なリソース位置	
ロジックを狙った攻撃（Logic Attack）	機能の悪用	★
	リダイレクタ	
	不適切なプロセスの検証	★

6、診断対象/非対象

Webアプリケーションセキュリティ診断の対象/非対象の例を以下に記載します。

診断手法	対象範囲
診断対象	事前調査及び調整の結果、診断対象に選定した通信
診断対象外	事前調査により判明した重複機能や優先度順で見送った通信など

※診断対象への算定基準は、以下の通りです。

1 ログイン、DB検索・更新等の重要処理
2 POSTリクエストでデータを投入しているもの（URL内クエリでない分警戒度が低くなる傾向がある為）
3 GETリクエストでデータを投入しているもの
ただし、同じURLに同じパラメータ群を投げている箇所につきましては原則、一つを代表し他の箇所は重複として診断対象から外していきます。また、同じ機能を既に診断対象に入れている場合は優先度を下げていきます。

7、終了判定基準

本診断における終了判定基準は、以下に基づいて行います。

1 画面遷移図上で合意した診断範囲に関してツール診断・手動診断が終了したこと

8、参照資料

本診断において、御社より提供頂いた参照資料等を以下に記載します。

参照ドキュメント・環境

No	ドキュメント名
1	exampledoc.docx

9、成果物

本診断の成果物を以下に記載します。

成果物名	成果物概要	主な項目	項目概要
画面遷移図	URL情報等を記載し、 診断対象を確定します	対象	該当通信が診断対象かを判定します
		手動	手動診断を行う箇所かどうかを判定します
診断結果報告書	脆弱性診断結果を 報告します	診断概要	診断対象や診断日時を記録します
		診断結果	システムへの総合的な評価を記載します
		指摘事項詳細	脆弱性の詳細な内容・対応を記載します
		特記事項	特記すべき事項を記載します
速報	危険度の高い脆弱性 発見時に脆弱性を 報告します	指摘事項詳細	脆弱性の詳細な内容・対応を記載します

10、必要機材

本診断において使用する機材を以下に記載します。

● バルテスで準備する機材

機材名	スペック	必要数
診断機	N/A	1

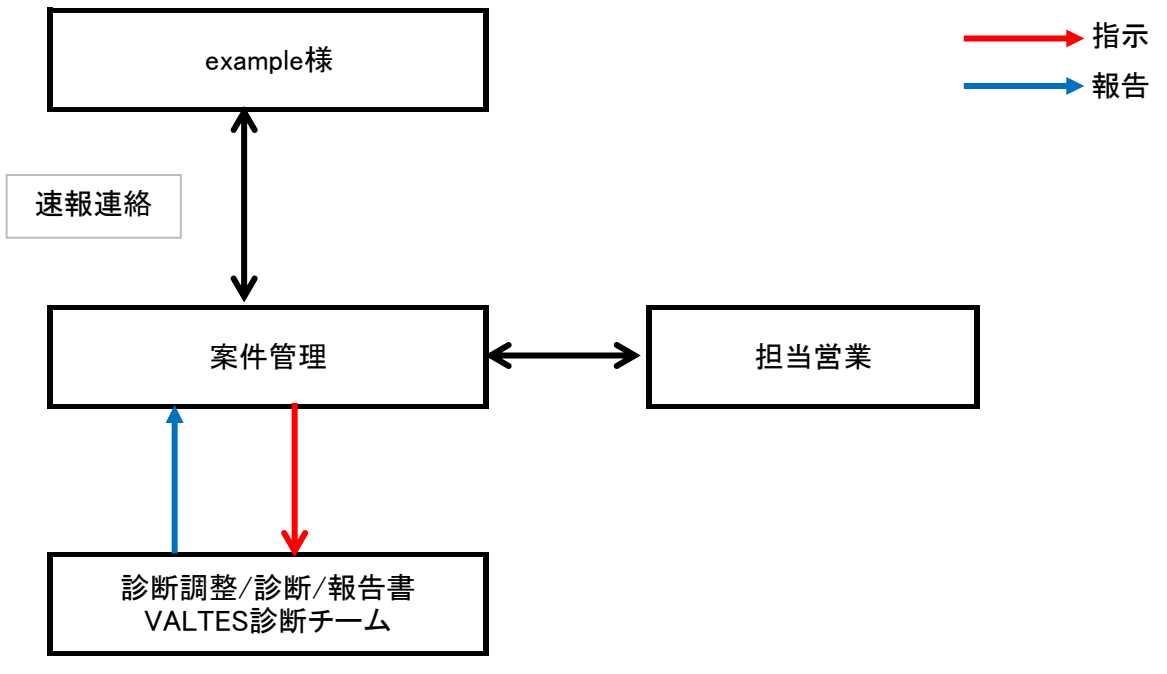
● example様にご貸与頂く機材

特にありません

11、診断体制

本診断における診断体制を以下に記載します。

ⅰ. 体制イメージ



ⅱ. 診断作業場所

本診断は下記の作業場所からシステムにアクセスして行います。

＜大阪本社テストセンター＞

住所　：　大阪府大阪市中央区安土町3-5-12　御堂筋安土町ビル7F
TEL　：　06-6267-6500
IP　：　別途連携させていただきます。

ⅲ. 連絡先

役割	氏名	メールアドレス
案件管理		
担当営業		
診断調整/診断/報告書		

12、スケジュール

本診断は、下記のスケジュールに沿って行います。「再診断」以降の作業時期については、調整可能です。

※診断員のスケジュールにより、スケジュールの変更が発生する場合がございます。その際は調整させてください。

作業内容	スケジュール				
	1month	2month	3month	4month	5month
マイルストーン		▲ ▲			
ドキュメント提供	■				
診断範囲策定	■	■			
診断範囲合意		▲			
WEBアプリ診断		■			
報告書作成		■	▲		
再診断					

13、インシデント及び再診断に関しまして

インシデントは下記でご報告させて頂きます。

レベル	説明	具体例
高	攻撃の実現可能性が高く、被害の規模も大きい	SQLインジェクション
中	攻撃の実現可能性が低いかまたは被害の規模が小さい	クロスサイトスクリプティング
低	攻撃の実現可能性が低く被害の規模も小さい	情報漏えい（エラーメッセージ）
注意事項	脆弱性ではないが、お客様のサイトのセキュリティを なおいっそう高くするための推奨項目	CookieのSecure属性 HTTP通信の制限

再診断につきまして

再診断は、中以上のインシデントに関して、無料診断させて頂きます。

再診断の期間は、報告書納品後、1ヶ月とさせて頂きます。（それ以上かかる場合はご相談とさせてください）

再診断の結果につきましては、報告書を更新もしくは再診断用作成用のフォーマットを用いて、納品させて頂きます。

14、料金

頂いた資料とサイト調査から通信を確認し、優先度を考慮の上集計した結果は以下の通りです。

詳細な診断対象につきましては、「画面遷移図」を参照いただければ幸いです。

対象システム	診断対象（最大）	診断対象（最小）	備考
example	20	10	
総計	20	10	

ツール診断が可能である事を前提とした、診断プランは以下の通りです。

プラン名	単位数	今回料金	診断期間	実施期間（※1）
WEB診断	20リクエスト	¥xxx,xxx	1週間程度	2週間程度

（※1）　診断及び報告書作成までにかかる期間を指します

15、コミュニケーション、報告体制

本診断では、下記の要領に基づいて報告を行うものとします。

報告内容	手段	時間
開始連絡/終了連絡	メール	10:00 , 18:00
速報（※1）	PDF	
その他、システムに関する質問/調整等	メール/Tel	10:00 - 18:00

（※1）　以下の理由から、診断の後半で報告する事になります。

・ツール診断で検知した脆弱性の可能性がある箇所を、手動診断で調査して始めて脆弱性かどうかが確定する為

・手動診断でしか検知できない脆弱性の中に、速報に値する脆弱性が存在する為

16、予見できるリスクとその対応

診断業務を行う上において、予見できるリスクとその対応について以下に記します。

予見できるリスク	対応策
ツール診断でのメール発行・データ改竄（消し込み等）	メール発行については、作業日をお客様に伝達します
お客様環境起因（リソース等）によるツール実行遅延	診断範囲をお客様と合意の上、再設定させてください
脆弱性の大量検出による作業遅延	診断範囲をお客様と合意の上、再設定させてください
弊社起因による診断作業の遅延	お客様と合意のうえ、診断時間・診断日を延長させてください
DoS攻撃（オプション）によるシステムダウン	発生時にお客様に連絡し、復旧依頼を出させていただきます
大量のテストデータ（※1）が必要なケースが存在する	テストデータの作成・投入を依頼させてください
AWS上にあるシステムを診断すること	事前にアマゾンに脆弱性診断を告知する必要があります お客様からアマゾンへ告知を行ってください

（※1）　診断対象によっては、大量のユーザーアカウント（ユーザー削除操作）や
資金等（購入・決済等）を準備頂く必要がございます。

17、特記事項

特記事項は特にありません。