Confidential

文書番号 VAL-SC-20140716-V1

株式会社 Example　御中

Web アプリケーション診断報告書

2014 年 7 月 16 日

本報告書は、2014 年 7 月 2 日から 6 日にかけて、株式会社 Example 様「Example」の脆弱性を診断した結果を報告するものです。報告書の内容には、脆弱性に関する情報が含まれていますので、お取り扱いには十分にご注意ください。

SAMPLE

バルテス株式会社

目次

1 はじめに 1
1.1. 診断の目的 1
1.2. Web アプリケーション診断の位置づけ 1
1.3. 本報告書の取り扱いについて 1
1.4. セキュリティ対策の運用について 2

2 診断内容 3
2.1. 診断環境 3
2.2. 診断項目 4
2.3. 診断対象 5

3 診断結果概要 6
3.1. 総合評価 6
3.2. 検出された脆弱性一覧 6
3.3. 総評 7

4 診断結果詳細 8
4.1. 承認 8

5 注意事項 11
5.1. サーバ証明書の使用について 11

6 お問合せ 12
6.1. お問合せについて 12
6.2. その他のサービスについて 12

付録 A 危険度の判定基準 13

付録 B 参考文献 14

SAMPLE

1 はじめに

1.1. 診断の目的

インターネットを介した不正アクセスの多くが、Web サイトを狙った攻撃となった今日では、不正アクセス等の攻撃に耐えられる堅牢な Web システムが求められています。

堅牢な Web システムを構築するためには、システム構成要素の脆弱性を正しく認識し対処する必要があります。OS や、Web サーバおよびデータベースなどのミドルウェアの脆弱性情報は信頼のおける公的な機関から情報提供されますが、各々が構築する Web アプリケーションの脆弱性は Web システムを運用している企業が自ら調べるほか脆弱性を正しく認識することはできません。

弊社の Web アプリケーション脆弱性診断は、堅牢な Web システムを構築するために Web アプリケーションに潜在する脆弱性を弊社技術者が診断・発見し、脆弱性の種類、発見箇所および対策指針を報告いたします。弊社の Web アプリケーション脆弱性診断により、堅牢な Web システムの構築・運用に役立てていただくことを目的としています。

1.2. Web アプリケーション診断の位置づけ

堅牢な Web システムを構築・運用するためには、OS や Web サーバおよびデータベースなどのミドルウェアの脆弱性に対しても適切に対処する必要があります。また、ファイアウォールに代表されるネットワークのセキュリティ対策も不可欠です。したがって、Web アプリケーションの脆弱性診断と診断結果による対策も非常に重要であるとともに、Web サイトの各構成要素に対しても脆弱性診断とその結果による対策を施す必要があります。

本報告書が対象としているのは、Web アプリケーションの脆弱性診断のみとなっており、OS やミドルウェアなどの脆弱性に関する情報は含まれていません。別途、これらについても専門機関を利用するなどして十分な対策を行われることを推奨します。

1.3. 本報告書の取り扱いについて

本報告書には、お客様の Web アプリケーションに関するセキュリティ上の問題点が記載されています。この情報がひとたび攻撃者に渡ってしまうと、セキュリティ上の問題点を狙った不正アクセス攻撃を受け情報漏えい等の事故が発生する可能性があります。したがって、本報告書のお取り扱いには十分に注意して頂けますようお願いいたします。

SAMPLE

Copyright(c)2005-2014 VALTES CO.,LTD All Rights Reserved.

1.4. セキュリティ対策の運用について

本報告書は診断時点でのお客様のWebアプリケーションのセキュリティ上の問題点を診断した結果が記載されています。Web アプリケーションへの攻撃は日々研究され進化し続けているため、時間経過とともにセキュリティ上の問題が増加することが考えられます。

堅牢な Web システムを継続的に運用するためには、定期的に Web アプリケーションに潜んでいるセキュリティ上の問題点を正しく認識し対策を施すことをお勧めいたします。

SAMPLE

Copyright(c)2005-2014 VALTES CO.,LTD All Rights Reserved.

2 診断内容

2.1. 診断環境

2.1.1. 診断日時

- 2014 年 7 月 2 日～2014 年 7 月 6 日　　10:00～19:00

2.1.2. 診断元 IP アドレス

- 100.100.100.100

SAMPLE

Copyright(c)2005-2014 VALTES CO.,LTD All Rights Reserved.

2.2. 診断項目

主な診断項目を以下に列挙します。

区分	名称
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
	コンテンツの詐称
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
	推測可能なリソース位置
ロジックを狙った攻撃	機能の悪用
	パス・トラバーサル
	リダイレクタ
	不適切なプロセスの検証
その他	文字コード指定の混在

SAMPLE

Copyright(c)2005-2014 VALTES CO.,LTD All Rights Reserved.

2.3. 診断対象

2.3.1. 対象サイト

- Example

2.3.2. 対象 URL

- http://www.example.jp/
- http://www.example.jp/userprofile/

2.3.3. Web サイトのシステム情報

お客様情報シートに記載いただいた情報と、診断にて判明した情報をもとに記載しています。

URL	http://www.example.jp/
IP アドレス	111.111.111.111
OS	Linux
Web サーバ	WAS
アプリケーションサーバ	Apache
データベース	Oracle
開発言語	PHP

SAMPLE

Copyright(c)2005-2014 VALTES CO.,LTD All Rights Reserved.

3 診断結果概要

3.1. 総合評価

B. 比較的安全な状態です

3.1.1. 総合評価について

総合評価では、診断結果詳細にて記載されている各脆弱性の危険度（Low、Medium、High）のレベルと危険度の個数を元に下記の表のような評価をしております。なお、危険度の詳細については、付録 A を参照してください。

評価	基準
A	脆弱性が検出されなかった
B	危険度 Low の脆弱性のみ検出
C	危険度 Medium の脆弱性を検出
D	危険度 High の脆弱性を検出
E	危険度 High の脆弱性を複数検出

3.2. 検出された脆弱性一覧

脆弱性区分	脆弱性名	危険度	個数
認証	（検出なし）		
承認	不適切な承認（Cookie の Secure 属性）	Low	1
クライアント側での攻撃	（検出なし）		
コマンド実行	（検出なし）		
情報公開	（検出なし）		
ロジックを狙った攻撃	（検出なし）		
その他	（検出なし）		

SAMPLE

Copyright(c)2005-2014 VALTES CO.,LTD All Rights Reserved.

3.3. 総評

今回の診断の結果、お客様の Web サイトは入力値のチェックがほとんどのパラメータで行われており、セキュリティを意識して作られている様子が確認されました。危険度の高い問題も検出されなかったことから、Web サイトは比較的安全な状態であるといえます。しかしながら、危険度は低いのですが、いくつか問題点として指摘している事項があります。

その中でセッション管理に関係した部分を指摘しておりますが、セッション管理のような重要な情報を扱う部分につきましては、より慎重に設計・実装を行う必要があります。やや細かい部分の指摘となっておりますが、本報告書の内容を参考に脆弱性について対応し、指摘点を心がけて Web サイトを設計されることでお客様の Web サイトのセキュリティはなおいっそう高いものとなります。

なお、今回確認された問題が診断対象以外の箇所でも存在していないか、問題の検出傾向なども参考にしながら確認されるようにお願いいたします。

SAMPLE

Copyright(c)2005-2014 VALTES CO.,LTD All Rights Reserved.

4 診断結果詳細

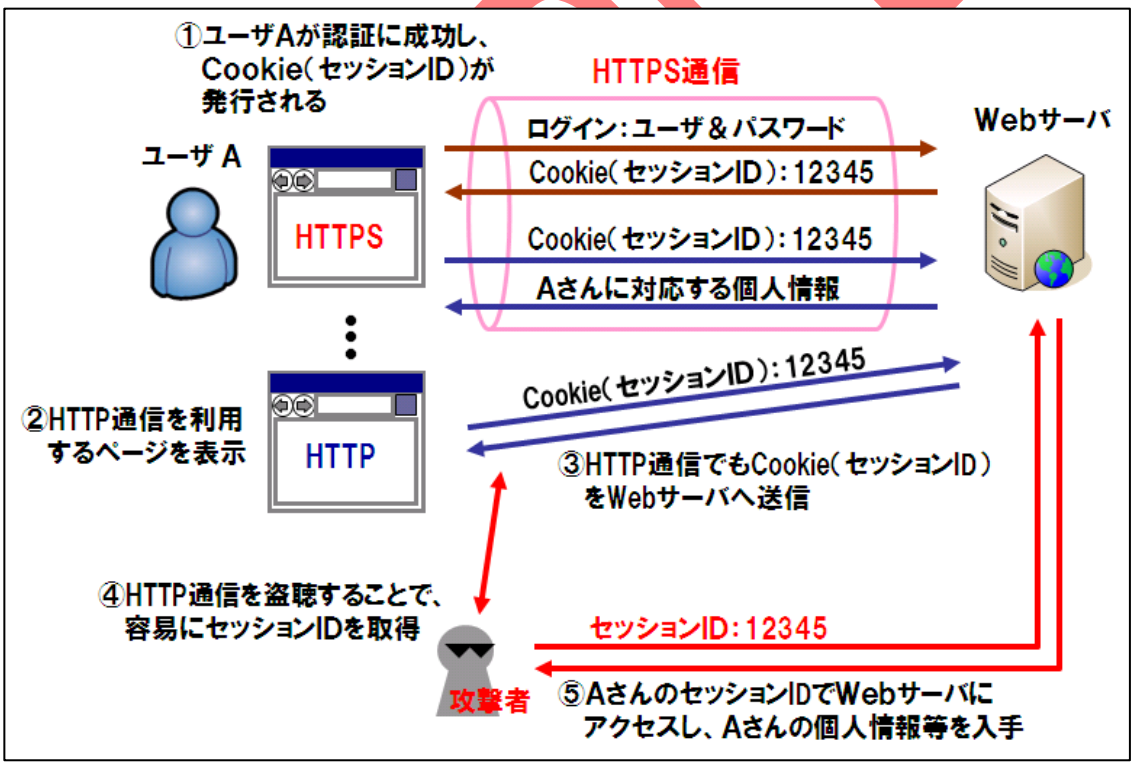
4.1. 承認

4.1.1. 不適切な承認（Cookie の Secure 属性）

(1) 危険度

Low

(2) 脆弱性概要



暗号化されている HTTPS の通信のみでなく、暗号化されていない HTTP の通信が発生した場合でも Secure 属性のついていない Cookie は Web サーバへ送信されてしまうため、攻撃者によって盗聴される可能性があります。このため、セッション ID などのような重要な情報をやり取りする Cookie には Secure 属性をつけることで暗号化されていない HTTP の通信では送信されないようにすることが重要です。

Copyright(c)2005-2014 VALTES CO.,LTD All Rights Reserved.

(3) 発生箇所

No	URL	Cookie 名
1	http://www.example.jp/userprofile/	JSESSIONID

(4) 脆弱性発生状況

【新しい報告パターン】

発生箇所を例に解説します。今回診断した Web サイトでセッション管理に使われている JSESSIONID は、レスポンスヘッダの Set-Cookie にて以下のような形式で発行されています。

```
Set-Cookie: JSESSIONID=7cf54cb18443431e31b445920606ad6ea3bb46f34
880b5dfb775bf91c681c13c; expires=Tue, 16-Mar-2032 07:04:32 GMT; pat
h=/
```

上記より、Secure 属性が設定されていないことが確認されます。

(5) 想定される脅威

重要情報であるセッション ID が盗聴されることで、なりすましが行われる可能性があります。

(6) 想定される被害

① 脆弱性悪用の実現度

攻撃者がユーザの通信路を盗聴する必要があるため、実現度は比較的低いと考えられます。

② 脆弱性悪用により想定される被害

- なりすましによる他のユーザ権限の不正利用
- なりすましによる個人情報の漏えい
- 情報漏えい等の事故を原因とするサイトの停止による機会損失
- 情報漏えい等に対する損害賠償や見舞金
- 情報漏えい等の事故による企業の信用失墜

SAMPLE

Copyright(c)2005-2014 VALTES CO.,LTD All Rights Reserved.

(7) 対策

以下のように Set-Cookie ヘッダの Secure 属性を有効にして Cookie を発行してください。

```
Set-Cookie: NAME=VALUE; ･･･省略･･･ ;secure
```

また、HTTP 用の Web ページと HTTPS 用の Web ページにまたがってセッション管理を行う場合、「Secure 属性なし」と「Secure 属性あり」の Cookie を用意し、HTTP 用には前者の Cookie を使用し、HTTPS 用には後者の Cookie を使用するようにしてください。

(8) 参考情報

PHP

PHP では設定ファイル php.ini で以下の行を追加することで、セッション管理に用いている PHPSESSID の Secure 属性を有効にすることが可能です。

```
session.cookie_secure=On
```

SAMPLE

Copyright(c)2005-2014 VALTES CO.,LTD All Rights Reserved.

5 注意事項

ここに記載されている事項は、Web サイトの安全性を一層高めるため対応されることを推奨するものです

5.1. サーバ証明書の使用について

今回の診断はテストサイトが対象でしたが、本番サイト運用開始にあたっては正式なサーバ証明書を使用していることを確認してください。

今回診断した Web サイトでは一時的に利用する目的で発行されたサーバ証明書を利用しているものと推察しますが、これは正式な証明書ではないため、Web ブラウザがセキュリティ上の警告を出力しています。

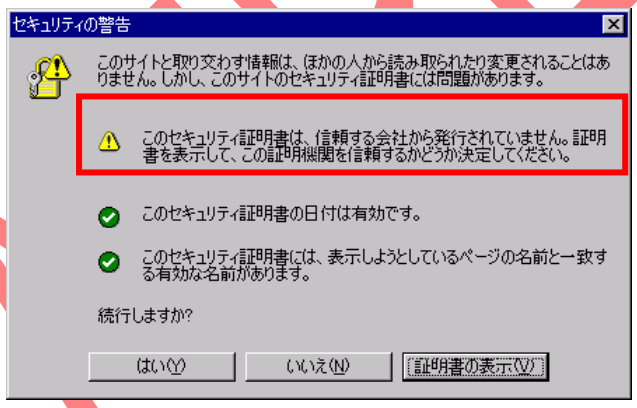


図 5-1

SAMPLE

Copyright(c)2005-2014 VALTES CO.,LTD All Rights Reserved.

6 お問合せ

6.1. お問合せについて

本報告書の内容に関するお問合せは、下記メールアドレスまでご連絡ください。お問合せの対応は、報告書提出から 1 ヶ月以内に限らせていただきます。なお、電話や FAX でのお問合せは受付けておりませんので、ご了承ください。

secure-info@valtes.co.jp

6.2. その他のサービスについて

弊社では、Web アプリケーション診断をはじめとする、「診断・防御・教育」の 3 つのアプローチでサービスを提供しております。

- プラットフォーム診断
  お客様のサーバやネットワーク機器に潜むセキュリティ上の問題点を診断します。

- Web アプリケーションファイアウォールサービス
  お客様サイトを攻撃する通信を弊社の Web アプリケーションファイアウォールが防御します。

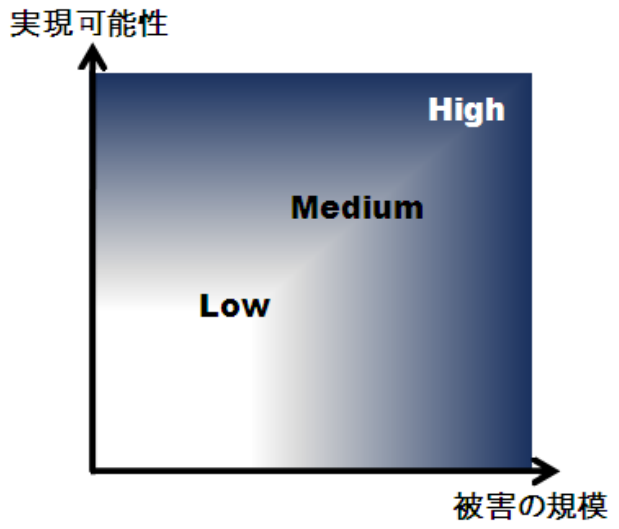
- セキュリティ教育
  Web サイト管理者、開発者の視点に立ったセキュアな Web サイト設計のための教育サービスを提供します。

SAMPLE

Copyright(c)2005-2014 VALTES CO.,LTD All Rights Reserved.

付録 A 危険度の判定基準

脆弱性の危険度は、以下の図のように攻撃の実現可能性と被害の規模を軸として High, Medium, Low の 3 段階の値に分けています。



・攻撃の実現可能性（縦軸）　：環境要因によるものや人的要因を考慮します。
・被害の規模（横軸）　：被害者数や被害の種類などを考慮します。

- High　攻撃の実現可能性が高く、被害の規模も大きい
- Medium　攻撃の実現可能性が低いかまたは被害の規模が小さい
- Low　攻撃の実現可能性が低く被害の規模も小さい

なお、実現度が低くても被害の規模が過度に大きいようであれば High と判定し、また実現度が高くても、被害の規模が小さいようであれば Low と判定します。

SAMPLE

Copyright(c)2005-2014 VALTES CO.,LTD All Rights Reserved.

付録 B 参考文献

1. セキュアプログラミング講座

http://www.ipa.go.jp/security/awareness/vendor/programming/

2. 新版 セキュアプログラミング講座

http://www.ipa.go.jp/security/awareness/vendor/programmingv2/

3. 情報処理推進機構 安全なウェブサイトの作り方

http://www.ipa.go.jp/security/vuln/documents/website_security.pdf

4. 情報処理推進機構 安全な SQL の呼び出し方

http://www.ipa.go.jp/security/vuln/documents/website_security_sql.pdf

5. NPO 日本ネットワークセキュリティ協会「2010 年 情報セキュリティインシデントに関する調査報告書」

http://www.jnsa.org/result/incident/2010.html

SAMPLE

Copyright(c)2005-2014 VALTES CO.,LTD All Rights Reserved.