Example株式会社様

Sampleシステム

セキュリティ診断報告書

CONFIDENTIAL

2018/11/08

フェンリル株式会社

はじめに

セキュリティ診断サービスについて

「セキュリティサービス」は、デザインと技術にこだわるフェンリルが提供するサービスです。
国際的なセキュリティ基準に基づき様々なアプローチを駆使して、お客様の抱えるリスクを可視化します。
未発見事項で被害が発生した場合の補償は行わないことをあらかじめご容赦ください。

本報告書について

本報告書には、お客様のシステムに関するセキュリティリスクが記載されています。内容を元に未調査機能への水平展開を行うことを推奨します。
また第三者が本報告書を手に入れると、その内容をもとに被害が発生する可能性がありますので取り扱いには充分ご注意ください。

問い合わせについて

本報告書の内容に関する問い合わせは、１ヶ月間対応させていただきます。
下記アドレスまでメールにてご連絡ください。
fenrir.b2b.sales@fenrir.co.jp

再現手順について

指摘事項を再現する際には、Webサーバに送る通信を改ざんできるローカル・プロキシが必要な場合があります。ローカル・プロキシツールの一つであるBurpSuiteの導入法・活用法については、以下資料を参照ください。

- Getting Started With Burp Proxy
  https://support.portswigger.net/customer/portal/articles/1783118-getting-started-with-burp-prosy
- Using Burp Proxy
  https://support.portswigger.net/customer/portal/articles/1783119-using-burp-proxy

セキュア設計について

OWASP ASVS は、開発者にとってセキュア設計を考慮する上で有用な指針となります。
日本語版もリリースされているため、同文書の活用を推奨します。

実施要綱

診断日時

- 2018年12月27日〜31日　10:00 - 18:00

診断対象システム

- Sampleシステム

また、ヒアリングシート及び、診断時に取得できた情報をもとに分析した対象システムの詳細情報は以下の通りとなります。

対象ホスト	example.com
IPアドレス	203.0.113.123
OS	CentOS 6.5
Webサーバ	Apatch Tomcat / 6.0.24
データベース	Oracle Database 11g

診断対象URL

- http://example.com/productsearch
- https://example.com/login
- https://example.com/usersearch
- https://example.com/updateprofile
- https://example.com/passwordchange

診断元IPアドレス

本診断において、検証用の通信を送信した弊社IPアドレスは以下の通りです。

- 192.0.2.111

診断結果

診断結果概要

チェック項目について

以下のチェックポリシーに沿ってセキュリティ調査をしました。

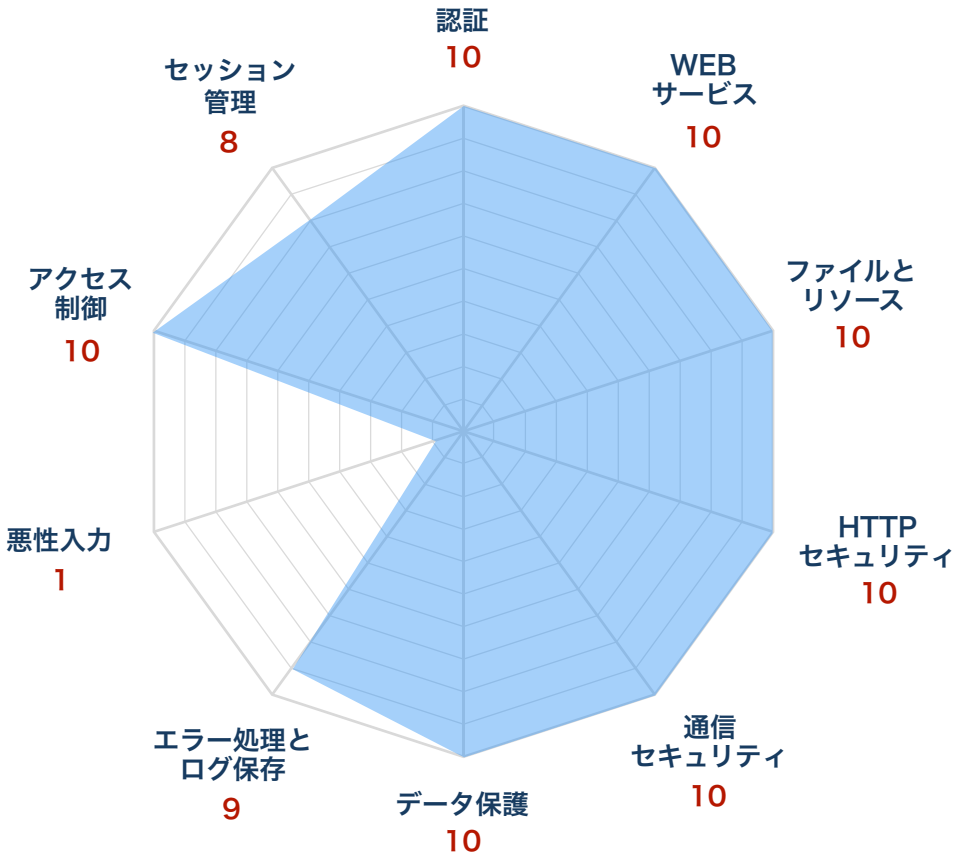
カテゴリ	項目名	作業内容	危険度	個数
認証	入力したパスワードが画面に表示される	パスワード入力時の挙動を確認します	低	0
	クライアント側で認証を済ませることができる	クライアント側での認証状態変更可否を確認します	低	0
	パスワードポリシーが強度不足である	パスワードポリシーを確認します	低	0
	パスワード変更機能が強度不足である	パスワード変更機能で旧パスワードの入力を求めるかを確認します	低	0
	資格情報などがHTTP接続で送信されている	セッション及び個人情報をHTTPで通信していないかを確認します	低	0
	パスワード回復機能が強度不足である	パスワードリカバリ機能の強度を確認します	注意	0
	エラーメッセージからアカウント情報が推測可能である	エラーメッセージの内容を確認します	低	0
	秘密の質問の答えが推測可能である	秘密の質問内容を確認します	低	0
セッション管理	ログアウト時にサーバーでセッション破棄がされていない	ログアウトに伴いセッション破棄処理を確認します	低	0
	タイムアウトの設定が不適切である	タイムアウト設定を確認します	低	0
	任意のタイミングでログアウトできない	ログアウトリンクがテスト対象に常時存在するかを確認します	低	0
	URLでセッション管理を行っている	URLクエリ、リファラにセッションが含まれないかを確認します	低	0
	セッションフィクセーション	認証前後でセッションの再生性が行われているかを確認します	低	0
	有効なセッションの値が推測できる	セッションパラメータの値の強度を確認します	低	0
	Cookieの属性設定が強度不足である	Cookieの設定状況を確認します	低	1
	アクティブなセッションの一覧が表示されない	アクティブなセッションがわかる状態かを確認します	注意	0
	パスワード変更時にアクティブなセッションの破棄が行われない	パスワード変更時の有効セッション取り扱いについて確認します	注意	0
アクセス制御	機能に対するアクセス制御が不完全である	未承認や権限昇格での機能悪用可否を確認します	高	0
	データに対するアクセス制御が不完全である	権限外のデータアクセス可否を確認します	高	0
	ディレクトリリスティング	サーバ内のディレクトリ内容確認可否を確認します	低	0
	クロスサイトリクエストフォージェリ	HTML読み込みなどによる操作強制可否を確認します	低	0
	システムに許可されていない機能の実行が可能である	制限を飛越した機能実行可否を確認します	低	0

診断結果概要

カテゴリ	項目名	作業内容	危険度	個数
悪性入力	SQLインジェクション	攻撃者による任意SQL文の実行可否を確認します	高	2
	LDAPインジェクション	攻撃者による任意LDAPクエリの実行可否を確認します	高	0
	OSコマンドインジェクション	攻撃者による任意OSコマンドの実行可否を確認します	高	0
	XPath / XML インジェクション	攻撃者による任意XMLクエリの実行可否を確認します	高	0
	クロスサイトスクリプティング	攻撃者によるjavascriptの挿入可否を確認します	中	1
	不適切なHTMLファイルを公開できる	任意のHTMLファイルを公開する機能の有無を確認します	低	0
エラー処理とログ保存	エラーメッセージから情報取得が可能である	診断中に発生した400系エラーや500系エラーメッセージなどによる、情報取得可否を確認します	注意	1
データ保護	重要情報がクライアントサイドでキャッシュされる	重要情報入力箇所でのオートコンプリート可否を確認します	注意	0
	URLクエリに個人情報を含む値が設定されている	URLクエリの内容を確認します	低	0
	キャッシュコントロールができない	重要情報出力箇所でのキャッシュコントロール状況を確認します	注意	0
	クライアントの記憶域に重要情報が保存される	重要情報に関するLocalStorage利用状況などを確認します	注意	0
通信セキュリティ	証明書の有効性に問題がある	証明書の有効性を確認します	低	0
	HSTSが設定されていない	HTTPSのサイトにおいてHSTSの利用状況を確認します	注意	0
HTTPセキュリティ	想定外のHTTPメソッドが実行可能である	システムで利用を想定していないHTTPメソッドの実行可否を確認します	注意	0
	文字コードの設定が不適切である	文字コードの設定状況を確認します	注意	0
	システムのバージョン情報が取得できる	バージョン情報の取得可否を確認します	注意	0
	APIレスポンスヘッダの設定が不十分である	APIについてレスポンスヘッダ設定を確認します	低	0
	Content Security Policy を設定していない	CSPの設定状況を確認します	注意	0
	X-XSS-Protection ヘッダが設定されていない	ブラウザにデフォルトで存在する防御機構の利用状況を確認します	注意	0
ファイルとリソース	リダイレクタ	システム外ドメインへの誘導可否を確認します	低	0
	パス・トラバーサル	公開を意図していないサーバ内リソースへのアクセス可否を確認します	高	0
	キャッシュコントロールが適切でない	重要情報出力箇所でのキャッシュコントロール状況を確認します	低	0
Webサービス	管理者でないユーザが管理機能にアクセスできる	管理機能へのアクセス可否状況について確認します	低	0
	セッションベースで認証を実施していない	APIがセッションベースで認証を行っているかを確認します	低	0
	クロスサイトリクエストフォージェリ	RESTサービスが操作の強制から保護されているかを確認します	低	0

診断結果概要

ランク　E　｜　スコア　88点



スコアは各カテゴリ10点満点とし、チェック項目に応じて算出した評価値となります。
ランクの目安は 100点が Sランク、80～99点が Aランク、60～79点が Bランク、 40~ 59点が Cランク、20～39点が Dランク、0～19点が Eランクですが、**危険度の高い指摘事項がある場合は、その限りではありません。**

カテゴリ	項目数	OK	NG
認証	8	8	0
セッション管理	9	8	1
アクセス制御	5	5	0
悪性入力	6	4	2
エラー処理とログ保存	1	0	1
データ保護	4	4	0
通信セキュリティ	2	2	0
HTTPセキュリティ	6	6	0
ファイルとリソース	5	5	0
Webサービス	3	3	0

診断結果総評

診断対象のシステムを調査した結果、基本的にはユーザから渡されるデータ内容のチェックが行われていることを確認しました。ただし、一部のパラメータについてチェック漏れがあり、その結果お客様が保有する顧客情報の流出やデータ改ざんに繋がるSQLインジェクションの脆弱性を発見しました。本報告書の内容を確認し、早急に対策を行うことを強く推奨します。

その他に以下のセキュリティリスクが確認されましたので、合わせて対応を行うことを推奨いたします。

- なりすましやフィッシングの危険性をもつクロスサイトスクリプティングが発見されました。本セキュリティリスクは、ユーザの入力値においてhtmlタグに相当する記号のエスケープを行なっていないために発生したものです。
- 対象システムでセッションを維持しているCookieにSecure属性が付与されていないことが判明しました。

その他、セキュリティリスクにはあたりませんが、攻撃者の好奇心を喚起する事項も確認されましたので合わせてご確認ください。
最後に、本診断で対象とした機能は対象システムの一部となるため、対象外の機能についても本報告書の内容をもとにお客様にて確認を行うことを推奨いたします。

指摘事項

対象のシステムを調査した結果、以下のセキュリティリスクが検出されました。

カテゴリ	項目名	危険度	個数
セッション管理	Cookieの属性設定が強度不足である	低	1
悪性入力	SQLインジェクション	高	2
	クロスサイトスクリプティング	中	1
エラー処理	エラーメッセージから情報が取得される	注意	1

診断結果詳細

1. Cookieの属性設定が強度不足である

危険度：低

脆弱性概要

システムを利用するユーザのセッション情報をCookieを用いて管理していますが、対象のCookieにSecure属性が付与されていません。
そのため、HTTP通信においてもHTTPS通信同様にCookieが通信内容に含まれてしまい、盗聴によりセッションを搾取される可能性があります。

危険度及び想定される被害

通信内容を盗聴された場合にセッションを搾取される危険性はありますが、実現可能性及び技術的な難易度から実行には一定の制限があると言えます。

発生箇所

診断対象の下記箇所で指摘事項が発生しています。

No	URL	Cookie名
1	https://example.com/login	JSESSIONID

再現手順

発生箇所No.1を例に解説します。対象のシステムでは、JSESSIONIDを利用してログインユーザのセッションを管理していますが、JSESSIONIDはログイン時に以下のように設定されています。

```
Set-Cookie: JSESSIONID=CF4B36A3FE9E51BD63F5A7DF057B4C21; Path=/
```

設定内容から、対象の Cookie に Secure 属性が付与されていません。

対策

対象のCookieに、Secure属性を付与するようにしてください。

```
Set-Cookie: JSESSIONID=CF4B36A3FE9E51BD63F5A7DF057B4C21; Path=/; secure
```

2. SQLインジェクション

危険度：高

脆弱性概要

本脆弱性は、データベースに対して操作を行う機能について入力された値の検証が不十分であるために攻撃者が挿入したSQL文をシステムが実行してしまう脆弱性です。

危険度及び想定される被害

本脆弱性を悪用された場合、対象機能でアクセスできるデータ・実行権限にはよるもののデータ改ざん・流出などの被害が発生します。

発生箇所

診断対象の下記箇所で指摘事項が発生しています。

No	URL	パラメータ名
1	https://example.com/updateprofile	name
2	https://example.com/updateprofile	age

再現手順

発生箇所No.2を例に解説します。
システムにログインしたユーザが登録情報を編集した際に以下の通信が発生します。

```
post http://example.com/updateprofile http/1.1
host: example.com
・・・（中略）・・・
name=John&age=32&・・・（中略）・・・
```

ここで、パラメータ「age」に対して以下の値を設定して送信します。

```
1. age=32-(select sleep(20) from information_schema.tables)
2. age=32-(select sleep(10) from information_schema.tables)
3. age=32-(select sleep(10) from hogehoge)
```

検証用に挿入された値は、MySQLで実行可能なSQL文でsleep関数で指定している値及び指定しているテーブル名が異なります。
その結果、次のように応答時間に差異が発生しました。

4. 診断結果詳細

No	応答時間
1	20.3秒
2	10.2秒
3	0.4秒

以上の結果から攻撃者が挿入したSQL文が実行されたことがわかります。

- No. 1, 2 で指定している値に紐づき応答時間に差異が発生したこと
- 実在しないテーブルを指定した No.3 で直ちに応答が戻ってきたこと

以上により、対象箇所についてはSQLインジェクションの脆弱性があると言えます。

対策

本指摘事項への根本的な対策は、以下の通りです。
ユーザーから渡された値を用いてSQL文を作成する際に、プリペアードステートメントやストアドプロシージャを用いるようにしてください。
参考として、Javaにおけるプリペアードステートメント実装例を以下に記載します。

```
String sql = "SELECT * FROM sampletable WHERE sampleparam=?";
PreparedStatement stmt = con.prepareStatement(sql);
stmt.setString(1, param); // ? の場所に値を埋め込む
ResultSet rs = stmt.executeQuery();
```

また、保険的な対策としては以下の対策が考えられます。

- 各機能においてデータベースへの実行ユーザ権限を最小限にする
- ホワイトリストで入力値の検証を行う

参考情報

- 安全なSQLの呼び出し方
  https://www.ipa.go.jp/files/000017320.pdf
- SQL injection Precention Cheat Sheet
  https://www.owasp.org/index.php/SQL_Injection_Prevention_Cheat_Sheet

3. クロスサイトスクリプティング

危険度：中

脆弱性概要

対象システムがレスポンスデータをユーザに渡す際に、ユーザが入力した値もしくは登録したデータをそのまま含んでしまうことからユーザからスクリプトなどを含むデータを渡された場合に、サイトを通して被害者のブラウザでそのスクリプトが実行されてしまう脆弱性です。

危険度及び想定される被害

本脆弱性を悪用された場合、サイトを利用するユーザがなりすましやフィッシングなどの被害に遭う危険性があります。
また、「クロスサイトスクリプティング」は有名な脆弱性でもあるため、システムを運営するお客様のブランドイメージの損失に繋がる可能性があります。

発生箇所

診断対象の下記箇所で指摘事項が発生しています。

No	URL	パラメータ名
1	https://example.com/usersearch	searchword

再現手順

発生箇所No.1を例に解説します。
対象システムのユーザ検索機能において発生する通信において、以下のようにスクリプトを含むデータを設定して送信します。

```
post http://example.com/usersearch http/1.1
host: example.com
・・・（中略）・・・
searchword=test<script>alert(document.cookie)</script>&option1=on
&・・・（以降、略）・・・
```

その結果、レスポンスとして以下のようなデータを受け取ります。

```
HTTP/1.1 200 OK
Date: Tue, 27 Dec 2017 10:04:08 GMT
・・・（以降、略）・・・
<html>
<body>
・・・（中略）・・・
test<script>alert(document.cookie)</script> の検索結果
・・・（以降、略）
```

レスポンス内容にユーザから渡されたデータがそのまま含まれているため、
スクリプトが実行され結果としてcookieの内容が表示されます。

対策

本指摘事項への対策は、以下の通りです。
ユーザから入力されたデータを出力する際にスクリプト実行に関係する以下の記号をHTMLエスケープ文字に変換するようにしてください。

- & ⇒ &
- < ⇒ <
- > ⇒ >
- " ⇒ "
- ' ⇒ '
- / ⇒ /

また、スクリプトでセッション管理に利用するCookieが搾取されないように対象のCookieにhttponly属性を付与するようにしてください。

参考情報

- XSS (Cross Site Scripting) Prevention Cheat Sheet
  https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet

4. エラーメッセージから情報が取得される

危険度：注意

脆弱性概要

システム内でエラーが発生した際に受け取るデータの中に、攻撃者が攻撃を行う際に有用な情報が含まれています

危険度及び想定される被害

本事項は、単独で直接的な被害をもたらすものではありません。
ただし、本事項から得た情報は他の脆弱性を利用した攻撃に有用なものであり、また攻撃者の好奇心を喚起するため、攻撃を行われる可能性を助長するものであると言えます。

発生箇所

診断対象の下記箇所で指摘事項が発生しています。

No	URL	パラメータ名
1	https://example.com/useredit	searchword

再現手順

発生箇所No.1を例に解説します。
実際には存在しない下記URLにアクセスします。

```
http://example.com/useredit
```

その結果、以下のようなレスポンスを受け取ります。

```
HTTP/1.1 404 Not Found
Date: Tue, 27 Dec 2017 11:09:01 GMT
Server: Apache-Coyote/1.1
・・・（中略）・・・
<html><head><title>Apache Tomcat/6.0.24 - Error report</title>
・・・（以降、略）・・・
```

レスポンスには、サーバ情報が含まれるため攻撃者は対象サーバの既知脆弱性をついた攻撃を狙う可能性があります。

対策

サーバ側でエラーが発生した場合には、カスタムエラーページへ誘導するように修正するほうが望ましいと言えます。

以下は、Apache Tomcat におけるカスタムエラーページの設定例となります。

```
<error-page>
<error-code>404</error-code>
<location>/404.html</location>
</error-page>
<error-page>
<error-code>500</error-code>
<location>/500.html</location>
</error-page>
```

本報告書に関するお問い合わせ先

fenrir.b2b.sales@fenrir.co.jp

フェンリル株式会社

大阪本社

〒530-0011 大阪府大阪市北区大深町 3-1 グランフロント大阪タワー B 14F
TEL:06-6377-7606（代表）　FAX:06-6377-7609

東京支社

〒141-0031 東京都品川区西五反田 2-27-3 A-PLACE五反田 5F
TEL:03-5719-3321（代表）　FAX:03-5719-3325

CONFIDENTIAL