CONFIDENTIAL

SAMPLE

○○○○○株式会社　御中

Web アプリケーション標準診断
診断結果報告書
【速報】

脆弱性診断後 3 営業日以内に提出いたします。
本診断結報告書では危険度の高い脆弱性(Medium 以上)の技術的な対処方法・対策方法の説明を報告いたします。

平成○○年○月○日

株式会社ソフテック

CONFIDENTIAL

SAMPLE

【資料改編履歴】

日 付	内 容	承 認	作成/更新
平成○○年○月○日	第一版作成	○○	○○

目　　次

1　目的

本診断結果報告書【速報】は、平成〇〇年〇月〇日に実施した Web アプリケーション標準診断において、深刻な影響を与えることが懸念される脆弱性をより早くご報告するために、診断結果の一部を抽出、要約したものです。

深刻な影響を与えることが懸念される脆弱性をより早くご報告することで、正式な診断結果報告書を待つことなく、脆弱性への対応を行うことが可能です。

なお、本診断結果報告書【速報】はあくまでも現時点での調査結果・要約という位置づけの報告であり、最終的な診断結果報告書とは内容が異なる場合もございますので、ご了承下さい。

2　診断対象

本診断における診断対象は以下の通りです。

〇〇〇〇〇サイト　(20 画面)

	画面名称	URL	備考 ※1
画面イメージ(1)PC			
1	契約者ログイン②	https://XXXXXXXX/PayEntry.jsp https://XXXXXXXX/PayEntry.jsp	5.画面イメージ (1)PC-①
2	ご契約内容確認③	https://XXXXXXXX/PayEntryDetails.jsp	5.画面イメージ (1)PC-①
3	注意事項④	https://XXXXXXXX/PayEntryDetails2.jsp https://XXXXXXXX/PayEntryKiyaku_inc.jsp	5.画面イメージ (1)PC-①
4	カード情報/ メールアドレス入力⑤	https://XXXXXXXX/PayEntryInput.jsp	5.画面イメージ (1)PC-②
5	ヘルプ： ご利用可能カード⑥	https://XXXXXXXX/PayEntryInputHelp.jsp	5.画面イメージ (1)PC-②
6	ヘルプ： セキュリティコード⑦	https://XXXXXXXX/PayEntryInputHelp2.jsp	5.画面イメージ (1)PC-②
7	入力内容確認⑧	https://XXXXXXXX/PayEntryConfirm.jsp	5.画面イメージ (1)PC-③

	画面名称	URL	備考 ※1
8	登録結果確認⑨	https://XXXXXXXX/PayEntryEnd.jsp	5.画面イメージ (1)PC-③
9	契約者ログアウト⑩	https://XXXXXXXX/Logout.jsp	5.画面イメージ (1)PC-③
10	カード情報/ メールアドレス入力⑤ （「カード情報修正」 ボタン)	https://XXXXXXXX/PayEntryInput.jsp	5.画面イメージ (1)PC-②
画面イメージ(2)モバイル			
11	契約者ログイン②	https://XXXXXXXX/PayEntryDetails.jsp	5.画面イメージ (2)モバイル
12	ご契約内容確認③	https://XXXXXXXX/PayEntryDetails.jsp	5.画面イメージ (2)モバイル
13	カード情報/ メールアドレス入力⑤	https://XXXXXXXX/PayEntryInput.jsp	5.画面イメージ (2)モバイル
14	入力内容確認⑧	https://XXXXXXXX/PayEntryConfirm.jsp	5.画面イメージ (2)モバイル
15	登録結果確認⑨	https://XXXXXXXX/PayEntryEnd.jsp	5.画面イメージ (2)モバイル
16	契約者ログアウト⑩	https://XXXXXXXX/Logout.jsp	5.画面イメージ (2)モバイル
17	カード情報/メールアドレス入力⑤ （「画面訂正・入力画面へ戻る」ボタン）	https://XXXXXXXX/PayEntryInput.jsp?	5.画面イメージ (2)モバイル
18	ヘルプ A：利用可能 クレジットカード	https://XXXXXXXX/PayEntryConfirm.jsp	5.画面イメージ (2)モバイル
19	ヘルプ B： セキュリティコード	https://XXXXXXXX/PayEntryConfirm.jsp	5.画面イメージ (2)モバイル

	画面名称	URL	備考 ※1
20	ヘルプ C： カード支払い方法	https://XXXXXXXX/PayEntryConfirm.jsp	5.画面イメージ (2)モバイル

※1　URL 及び URL のパラメータについては検査時点において有効だったものを記載しております。
　　また、POST パラメータについては割愛させて頂いております。

※2　「仕様書.pdf」において、診断対象画面が記載されている章番号になります。

△△△△△サイト　(10 画面)

	画面名称	URL	備考 ※1
画面イメージ(1)PC			
21	契約者ログイン②	https://YYYYYYYY/PayEntry.jsp https://YYYYYYYY/PayEntry.jsp	5.画面イメージ (1)PC-①
22	ご契約内容確認③	https://YYYYYYYY/PayEntryDetails.jsp	5.画面イメージ (1)PC-①
23	注意事項④	https://YYYYYYYY/PayEntryDetails2.jsp https://YYYYYYYY/PayEntryKiyaku_inc.jsp	5.画面イメージ (1)PC-①
24	カード情報/ メールアドレス入力⑤	https://YYYYYYYY/PayEntryInput.jsp	5.画面イメージ (1)PC-②
25	ヘルプ： ご利用可能カード⑥	https://YYYYYYYY/PayEntryInputHelp.jsp	5.画面イメージ (1)PC-②
26	ヘルプ： セキュリティコード⑦	https://YYYYYYYY/PayEntryInputHelp2.jsp	5.画面イメージ (1)PC-②
27	入力内容確認⑧	https://YYYYYYYY/PayEntryConfirm.jsp	5.画面イメージ (1)PC-③
28	登録結果確認⑨	https://YYYYYYYY/PayEntryEnd.jsp	5.画面イメージ (1)PC-③
29	契約者ログアウト⑩	https://YYYYYYYY/Logout.jsp	5.画面イメージ (1)PC-③

	画面名称	URL	備考 ※1
30	カード情報/ メールアドレス入力⑤ （「カード情報修正」 ボタン）	https://YYYYYYYY/PayEntryInput.jsp	5.画面イメージ (1)PC-②

※3　URL 及び URL のパラメータについては検査時点において有効だったものを記載しております。
　　また、POST パラメータについては割愛させて頂いております。

※4　「仕様書.pdf」において、診断対象画面が記載されている章番号になります。

3　診断結果要約

現時点で本診断において確認されている脆弱性の内、危険性が高いと考えられる脆弱性について以下に示します。

なお、脆弱性の確認では Web ブラウザとして Mozilla Firefox を使用しているため、それ以外の Web ブラウザでは再現しない場合があります。
また、本章に記載されている URL や HTML、検出根拠の内容は診断時において有効だったものを記載しており、アクセスの度に変化するパラメータ等によりそのままの形では再現出来ない場合がございますので、あらかじめご了承ください。

3－1　クロスサイトスクリプティング

対象サイト	△△△△△サイト
診断項目	クロスサイトスクリプティング
危険度	High

対象サイトにおいて、クロスサイトスクリプティングを確認しております。

クロスサイトスクリプティングとは、入力フォームや URL に含まれるパラメータ等からユーザに設定された文字列について、十分なチェックを行わずに HTML 中に埋め込んで表示するために引き起こされる、Web アプリケーション脆弱性の代表的なものです。細工された文字列を入力フォーム等のパラメータに与えることで、JavaScript を含む任意の HTML 要素を埋め込み、ユーザの意図しない不正なプログラムのダウンロード、ページの偽装やセッション ID の不正取得等を行われる可能性があります。

図 3-1-1～図 3-1-4 は、対象サイトにおいて確認されたクロスサイトスクリプティングを検証したものです。

△△△△△サイトにおけるのお問い合わせページ（図 3-1-1）を表示するリクエスト内容（図 3-1-2）の URL に対して、JavaScript を含む細工された文字列を追加（図 3-1-3）してリクエストを送信すると、追加した JavaScript が実行（図 3-1-4）されることを確認しています。

このことから、任意の JavaScript が埋め込み可能な状態となっており、クロスサイトスクリプティングが存在すると確認できます。

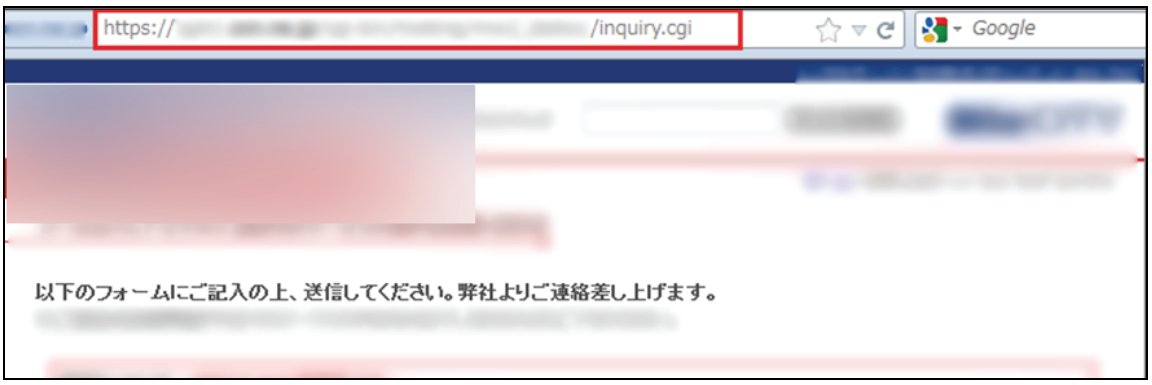

図 3-1-1　△△△△△サイトお問い合わせページ

```
GET /cgi-bin/[redacted]/inquiry.cgi HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:10.0.2) Gecko/20100101 Firefox/10.0.2
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
Accept-Encoding: gzip, deflate
Connection: keep-alive
```

図 3-1-2　図 3-1-1 にアクセスする際のリクエスト内容

```
GET /cgi-bin/[redacted]/inquiry.cgi?="><script>alert('xss')</script> HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:10.0.2) Gecko/20100101 Firefox/10.0.2
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
Accept-Encoding: gzip, deflate
Connection: keep-alive
```

図 3-1-3　図 3-1-2 のリクエスト内容の URL に JavaScript を含む文字列を追加

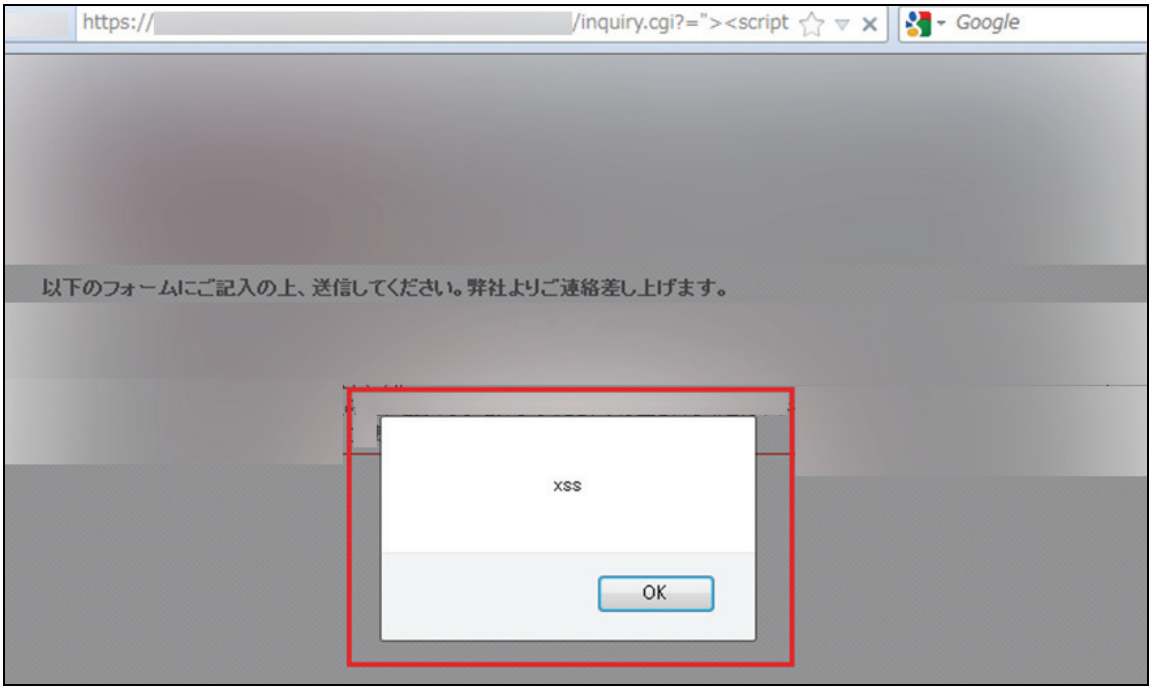

図 3-1-4　図 3-1-3 の内容でリクエストを実行した結果（JavaScript 実行）

クロスサイトスクリプティングは Web サーバや Web アプリケーションに対する直接的な不正侵入やサービス妨害に繋がることはありませんが、ユーザが通常にページアクセスを行うだけで第三者サイトに設置されたウイルスやマルウェア等のダウンロードが行われることに悪用されたり、ページ偽装を行うことによりユーザの認証情報や個人情報を不正取得するために悪用されたり、ログイン中のセッションを奪うために cookie 等を不正取得するために悪用されたりする深刻な脆弱性となることがあります。

対象サイトは個人情報を保持する Web サイトであり、本脆弱性はフィッシング詐欺に悪用される可能性がありますので、対策を実施することを推奨します。

クロスサイトスクリプティングへの対策としては、一般的には以下の２つの方法が考えられます。

1. 問題を起こす可能性のある文字を影響が出ないように変換してから出力（無毒化、サニタイジング）

パラメータ等、ユーザから入力されたデータや Web ブラウザから Web サーバに送信されたデータの内容を HTML 中に埋め込む際に、以下のように文字単位で変換処理を行うことで、HTML において特別な意味を持つ文字を単なる文字として Web ブラウザに解釈させることが可能です。
この変換処理を一般的には無毒化・サニタイジングと呼びます。また、変換後の文字列は実体参照と呼ばれます。

変換前	変換後
<	<
>	>
&	&
″	"
’	'

クロスサイトスクリプティングは<>のように HTML として特別な意味を持つ文字を埋め込むことにより引き起こされますので、無毒化を行った上で出力することでこの脆弱性の影響を受けないようにすることが可能です。

なお、タグ属性の値は必ずダブルクォート記号（″）、もしくはシングルクォート記号（’）で囲うようにしてください（例：<input type="text" value="1">）。囲っていない場合は、無毒化を行った場合でもクロスサイトスクリプティングの影響を受ける可能性があります。ダブルクォート記号とシングルクォート記号が混在している場合も問題が生じる場合がありますので、サイト全体で統一することを推奨します。

上記は一般的な対策ですが、値が埋め込まれている箇所によっては前述の文字単位の変換では不十分な場合もありますので、実際に対策を行う際には独立行政法人 情報処理推進機構（IPA）が公開している資料についても参照することを推奨します。

セキュアプログラミング講座 Web アプリケーション編
第 7 章 エコーバック対策 スクリプト注入
http://www.ipa.go.jp/security/awareness/vendor/programmingv2/contents/601.html

安全なウェブサイトの作り方
http://www.ipa.go.jp/security/vuln/websecurity.html

2. Web アプリケーションファイアウォール（WAF）でのアクセス拒否

Web アプリケーションファイアウォールを導入することで、Web アプリケーションの修正を行わずに不正なアクセスを拒否することが可能です。

Web アプリケーションファイアウォールは全ての Web アプリケーションの脆弱性に対応出来るものではありませんが、一般的なクロスサイトスクリプティングや SQL インジェクション、コマンドインジェクション等の脆弱性については大部分の不正アクセスを拒否することが可能です。

すぐに Web アプリケーションの修正が出来ないようなケースでは有効な対策方法となります。

安全なウェブサイトの作り方
http://www.ipa.go.jp/security/vuln/websecurity.html

Web アプリケーションファイアウォールの必要性（@IT）
http://www.atmarkit.co.jp/fsecurity/rensai/waf01/waf01.html

Web Application Firewall 読本
http://www.ipa.go.jp/security/vuln/documents/waf.pdf

前者は Web アプリケーションの修正、後者はシステムの導入となりますが、可能であれば根本的な対策である前者の対策を行うことが推奨されます。

表 3-1-1 は、本診断において検出された「クロスサイトスクリプティング」の一覧です。

表 3-1-1　「クロスサイトスクリプティング」の一覧

対象サイト/画面名称
△△△△△サイト／お問い合わせページ
対象 URL
https://www.example.com/cgi-bin/xxxxxxx/inquiry.cgi

対象パラメータ
－（Query String）
危険度
High

	検出根拠
	対象 URL に対して、JavaScript を含む文字列を追加した以下の URL にアクセスを行うことで、URL に追加した JavaScript が実行されることを確認しました。 https://www.example.com/cgi-bin/xxxxxxx/inquiry.cgi?=''><script>alert('xss')</script>
	備考
	なし

4　その他の脆弱性一覧

現時点で本診断において検出されている脆弱性の内、「3　診断結果要約」にて示した脆弱性以外のものについて表 4-1 に示します。

なお、これらの脆弱性につきましては全て危険度 Low となります。各脆弱性の詳細・対策につきましては診断結果報告書に記載させて頂きます。

表 4-1　その他の脆弱性一覧

脆弱性名称（診断項目）	脆弱性内容
テストファイルの存在（強制ブラウジング）	対象サイト/画面名称、対象 URL
	http://www.example.com/test.html
	概要
	診断対象の Web サーバにおいて、テスト用の HTML ファイルと推測されるファイルの存在を確認しております。 管理されていないテスト用のファイルが Web サーバ上に存在する場合、本来公開すべきではないシステム情報等が漏洩する可能性もありますので、該当のファイルについて確認し、必要の無いものであれば削除することを推奨します。 なお、意図的に設置しているものであれば問題はありませんが、その場合でも、外部に公開しても問題の無い内容であるか確認することを推奨します。
文字コードの未設定（サードパーティ製品の未設定）	対象サイト/画面名称、対象 URL
	http://www.example.com/information/index.html 等
	概要
	診断対象の Web サーバ上にある一部の画面について、HTTP 応答ヘッダ Content-Type の charset 属性が存在しないことを確認しています。 Content-Type は、HTTP クライアントに対してコンテンツの種類を通知するための HTTP 応答ヘッダですが、文字コードの設定が正しく行われていない場合、一部の Web ブラウザにおいて文字コードの不整合によるクロスサイトスクリプティングが発生することがありますので、Web サーバの設定により標準の文字コードを設定することを推奨します。

5　危険度の判定基準

本診断結果報告書【速報】では検出された各脆弱性について、表 5-1 を基に危険度を判定し記載しています。

危険度は、検出された各脆弱性への対策の際に、どの脆弱性を優先的に修正すべきか判断するための目安として記載しているものです。

表 5-1　危険度の判定基準

危険度	判定基準
Critical	直接的に深刻な被害を及ぼすことが懸念される脆弱性。 SQL インジェクション等が該当します。
High	フィッシング詐欺等、受動的な攻撃により個人情報等の重要な情報を奪われるような被害が想定される重大な脆弱性。 Critical との違いは、Critical は攻撃者が能動的に攻撃を行うことが可能な脆弱性を対象としているのに対し、High はユーザが罠にかかるのを待つような受動的な手法が採られる脆弱性を対象としています。 クロスサイトスクリプティング等が該当します。
Medium	他の脆弱性と組み合わせることによって被害を受けることが想定される脆弱性。ディレクトリリスティングなどが該当します。
Low	Medium 以上に該当せず、被害を受ける可能性が低いと考えられる脆弱性。サードパーティ製品の設定ミスなどが該当します。

判定基準はあくまでも目安であり、脆弱性の検出された箇所・内容等により判定基準とは異なる危険度を脆弱性に与えることもありますので、ご了承下さい。

6　実施した診断項目一覧

本診断において実施した診断項目は以下の通りです。

クロスサイトスクリプティング

クロスサイトスクリプティングとは Web アプリケーションソフトウェアの脆弱性で、「サイトを跨ってスクリプトを実行する」という意味です。

Web アプリケーションで、入力されたデータの内容を充分チェックせずに HTML 内に出力していると、HTML 内に JavaScript などの任意のコードを埋め込むことができてしまいます。このような状態を「クロスサイトスクリプティング脆弱性がある」と言います。

例として、任意のタグがそのまま書き込めてしまう掲示板が挙げられます。悪意あるユーザが「<script>」などの HTML タグを含む内容を投稿すると、投稿内容を閲覧したときにスクリプトが実行されてしまう危険性があります。スクリプトの内容によっては cookie データの盗聴や改竄などが可能なため、商取引に使った cookie を横取りして、本人になりすまして物品の購入を行なったり、cookie を認証やセッション管理に使っているサイトに侵入したりするなど、より広範かつ深刻な損害を与える可能性があります。

ステルスコマンド

外部から任意の OS のコマンドや SSI(サーバサイドインクルード)などを実行することが可能な状態であることです。ユーザの入力がそのままシェルや SSI にコマンドとして渡せるようになっているとこのような事態が発生します。

SQL インジェクション

「インジェクション(injection)」とは「注入」という意味で、SQL データベースに対し、外部から任意の SQL を実行することができる状態を指します。任意のデータを抽出できてしまうことが問題となります。

例として、あるユーザが他のユーザのデータを見たり、パスワード情報を得たりできてしまう可能性があります。また、SQL の種類や設定によってはデータベースの改竄や削除ができてしまったり、さらにはサーバ内で任意のコマンドを実行することができてしまったりする危険性があります。

バッファオーバーフロー

想定よりも長いデータを処理しきれない場合に発生します。バッファが溢れる(オーバーフローする)ことを意味します。

本来書き込まれるべきメモリ領域からデータが溢れ、本来書き込まれてはならない別の領域に書き込まれてしまいます。その結果として何が起きるのかは様々ですが、任意のコードを実行されてしまうこともあり、致命的なセキュリティホールになる危険性があります。

既知の脆弱性

OS や Web サーバ、アプリケーションサーバ、サードパーティ製ツールなどの持つ一般的に広く知られている脆弱性のことです。

攻撃者はこれらの脆弱性を悪用することによって、アクセス権限の不正取得、機密情報の奪取、データ破壊等が行えるようになります。これらの問題の多くは主にベンダからのパッチプログラムの適用により解消できます。

強制ブラウジング

意図していないコンテンツが公開ディレクトリ上にあるために、第三者が URL を直接入力することでそれらのページやデータを取得できてしまうことです。これらは攻撃者に攻略の糸口となるヒントを与えたり、機密情報の漏洩をもたらされたりします。

例えば、アプリケーションのソースコードが公開ディレクトリにそのまま置かれている場合や、CSV などでまとめた顧客情報が漏洩してしまう場合などが考えられます。

hidden フィールドの操作

HTML の入力フォームの一つである hidden フィールドは、フォームの値を画面上には表示させずにアプリケーションに渡すことができます。これはページ間でのデータの受渡しによく使用されています。しかし、hidden フィールドに指定した値はクライアント側で容易に変更できてしまうため、値の信頼性はありません。

この hidden フィールドによって重要なデータをやり取りしている場合、アプリケーションによっては、アクセスコントロールを迂回されたり、予期せぬ動作を引き起こしたりします。

例えば、商取引サイトにおいて hidden フィールドに商品の価格を設定している場合には、hidden フィールドの改竄により商品の価格を不正に操作されてしまいます。

サードパーティ製品の設定ミス

サードパーティ製品の設定にミスがある状態です。主に人為的なミスが考えられますが、製品によっては初期状態からセキュリティ上、問題のある設定になっているものも見受けられます。
これらの情報は攻撃者に攻略のヒントを与えてしまうため、攻撃が成功する可能性を高くしてしまいます。

バックアップファイルの検出

バックアップファイルと思われるものがサーバ上に存在する状態です。インタープリタ言語などによる動的なページを生成しているサイトにおいて、ファイルを変更した際にバックアップを設定した以外の拡張子のファイル名にした場合、処理が実行されずにソースコードが表示されてしまう可能性があります。

人為的にバックアップファイルを保存している場合や、エディタにより自動的にバックアップファイルが残っている場合に問題となります。

バックドア、デバッグオプション

アプリケーションの開発段階で使用されていたデバッグ用のオプションやバックドアがそのまま残されている状態です。これらを攻撃者に不正に利用されてしまう可能性があります。

HTML 中のコメント

HTML の中に重要な情報がコメントとして書かれている状態です。例えば、管理者のユーザ ID やパスワードの一部などが書かれている場合、それだけで不正にアクセスされてしまう可能性があります。

ディレクトリトラバーサル

Web サーバやアプリケーションサーバが通常表示させることの可能なルートディレクトリを越えて、ディレクトリをさかのぼることが出来てしまう状態のことを言います。システム構成が知られている場合には、パスワードなどの機密ファイルが漏洩したり、任意のコマンドを指定し実行される可能性があります。

典型的なパターンとしては、URL に「../」を多量に使用することで Unix 系のパスワードファイルが格納されている「/etc/passwd」ファイルを取得しようとすることが挙げられます。

不適切なエラーハンドリング

Web アプリケーションのエラー処理を行う際の画面表示内容が適切でない状態です。システムの情報を表示することは開発者にとって有用ですが、攻撃者にとっても有用であり攻略のヒントを与えてしまうため、攻撃が成功する可能性を高くしてしまいます。

例えば、SQL の実行エラーが表示されてしまっている場合には、攻撃者はその情報を見て任意の SQL を実行しようとします。

パラメータの改竄

Web アプリケーションが通常使用しているパラメータの値を不正な値に変更したり削ったりすることで、情報の漏洩やアクセスコントロールを迂回することが可能な状態です。
不正なメタ文字や、制御文字などをパラメータに入力することで予期せぬ動作を引き起こします。

Web サービスの脆弱性

Web サービスに特化した脆弱性です。Web サービスは一般の Web アプリケーションに存在する SQLインジェクションやクロスサイトスクリプティングなどの脆弱性の他にも XML 攻撃などの特殊なものがあります。

クロスサイトリクエストフォージェリ

クロスサイトリクエストフォージェリとは、記事の投稿や商品の購入等、永続的な影響を与えるリクエストが発行されるページに正規のユーザを誘い込むことで、正規ユーザに意図しない操作を実行させることが可能な脆弱性です。

確認ページの無い記事投稿ページや、本来受け付けるべきではない外部のリンクやフォームから発行されたリクエストをそのまま処理してしまうような Web サイト等でよく見られる脆弱性で、意図しない商品の購入や記事の投稿等の被害をユーザに与える危険性があります。

セッション管理の脆弱性

セッション管理とは、あるアクセスが特定のユーザからのものであることを識別管理することを意味します。その識別情報をセッション追跡パラメータといいます。一般的には cookie によるセッション管理がよく行われています。セッション追跡パラメータはユーザを識別するための重要な情報であり、漏洩した場合にはなりすましの被害に遭遇する可能性があります。

例えば、セキュアでない cookie を使用したり、URL をパラメータにしたりしている場合には、セッション追跡パラメータが暗号化されずにネットワーク上を流れるため、盗聴によって内容が漏洩する可能性があります。

また、ユーザ毎に識別が行われていなかったり、アクセスコントロールが正常でないページが存在したりすることもあるため、正しくセッション管理を行う必要があります。

以上