CONFIDENTIAL

2022年4月1日

株式会社AGEST　御中

「株式会社AGEST」

Webアプリケーション脆弱性診断
結果報告書

目次

1. エグゼクティブサマリー

総合評価	危険	大規模な影響を及ぼす可能性のある脆弱性が検出されました。

本診断の総合評価と、その定義は次のとおりです。

評価	解説
緊急	攻撃への利用が容易で直接的な被害を及ぼす可能性のある脆弱性が検出されました。 緊急の対策が必要です。
危険	**大規模な影響を及ぼす可能性のある脆弱性が検出されました。早急に対策が必要です。**
警告	間接的にまたは複数組み合わせることで攻撃に利用され、 実害を受ける可能性のある脆弱性を検出しました。計画的な対策が必要です。
注意	被害を受ける可能性は低い、またはサービス提供に影響は小さいものの、 対策が推奨される脆弱性を検出しました。
問題なし	脆弱性は検出されませんでした。現在の対策を継続してください。

1.1 総評

本診断において、深刻度の高い問題としてクロスサイトスクリプティングの反射型を確認しました。 ブラウザから罠リンクを押下した際にスクリプトが実行されるため、ユーザに気付かれづらく危険度が高い脆弱性となります。今回のシステムでは、CookieにHttpOnly属性が付与されているため、JavaScriptによりCookieにアクセスすることはできませんが、それ以外の攻撃に利用される危険性があります。

さらに、深刻度が中程度の問題としてCookieにセキュア属性が付与されていないことを確認しました。Cookieにセキュア属性がない場合、平文通信においてもCookieが送信されるため、セッション情報の漏洩に繋がります。

全体を通して、脆弱性の検出数は少ないですが危険度の高いものが含まれますので、早急に対策を実施してください。

1.2 検出事項一覧

本診断にて検出された脆弱性は次のとおりです。個別の解説については 3.1 以降から参照ください。

深刻度（検出数）	検出事項
Critical(0)	-
High(1)	• クロスサイトスクリプティング（反射型）
Medium(1)	• Cookieのセキュア属性不備
Low(1)	• クリックジャッキング
Info(1)	• バージョン情報の検出

2. 診断の概要

2.1 診断目的

Web アプリケーション脆弱性診断（以後、「本診断」という）は、2.3 に係る、
様々な情報セキュリティ上の脆弱性の存在についての調査と、その結果の分析及び報告を行うものです。

2.2 診断日

本診断の診断実施日は次のとおりです。

> 実施日： 2022 年 4 月 1 日～2022 年 4 月 1 日

2.3 診断対象

本診断の対象となった Web アプリケーションは次のとおりです。

- [AGEST]
    - https://agest.co.jp

No	箇所
1	画面名：トップ URL：https://agest.co.jp/
2	画面名：トップ>検索 URL：https://agest.co.jp/■■■■■■■■■■?q=&date_from=&date_to=
3	画面名：トップ>ログイン画面>ログイン URL：https://agest.co.jp/■■■■■■■■■■

※サンプルのため■■■と記載されている箇所がありますが、
実際の報告書ではマスク処理を行いません。

2.4 診断実施形態

本診断の診断実施形態は次のとおりです。

> 診断形態： リモート診断
> 診断場所： 株式会社AGEST 診断作業エリア

2.5 診断方法

本診断では、診断技術者による手動オペレーションを主とし、診断ツールを併用した診断を実施しました。

2.6 診断の観点

本診断では、下記の脆弱性定義により、表に示す脆弱性の診断を実施しました。

1. IPA「安全なウェブサイトの作り方　改訂第7版 (2021年3月31日改訂) 」
   https://www.ipa.go.jp/security/vuln/websecurity.html
2. CWE – Common Weakness EnumerationのCWE番号
   (CWE解説：https://www.ipa.go.jp/security/vuln/CWE.html を参照)
3. IPA「ウェブ健康診断仕様」
   https://www.ipa.go.jp/security/vuln/websecurity.html

No.	脆弱性名称		脆弱性の名称の定義に関する参照先	
1	SQL インジェクション		1	p.6 - 1.1
			2	CWE-89
			3	p.9 - (A)
2	OS コマンド・インジェクション		1	p.10 - 1.2
			2	CWE-78
			3	p.12 - (D)
3	ディレクトリ・トラバーサル		1	p.13 - 1.3
			2	CWE-98
			3	p.14 - (G)
4	ログイン機能の不備			
	i	推測可能なセッション ID	1	p.18 - 4-(i)
			2	CWE-330
			3	p.18 - (K)-2
	ii	URL 埋め込みのセッション ID の外部への漏洩	1	p.19 - 4-(ii)
			2	CWE-522
			3	p.18 - (K)-4,5
	iii	クッキーのセキュア属性不備	1	p.19 - 4-(iii)
			2	CWE-614
			3	p.18 - (K)-3
	iv	セッションIDの固定化	1	p.19 - 4-(iv)-a, p.20 - 4-(iv)-b
			2	CWE-384
			3	p.18 - (K)-1

5	クロスサイト・スクリプティング(XSS)		1	p.22 - 1.5
			2	CWE-79
			3	p.10 - (B)
6	利用者の意図に反した実行防止機能の不備			
	i	クロスサイト・リクエスト・フォージェリ(CSRF)	1	p.30 - 1.6
			2	CWE-352
			3	p.11 - (C)
	ii	クリックジャッキング	1	p.41 - 1.9
			2	該当なし
			3	該当なし
7	メールヘッダ・インジェクション		1	p.38 - 1.8
			2	CWE-93
			3	p.13 - (F)
8	アクセス制御と認可処理の不備			
	i	アクセス制御	1	p.46 - 1.11.1
			2	CWE-284
			3	p.20 - (L)
	ii	認可処理	1	p.46 - 1.11.2
			2	CWE-264
			3	p.20 - (L)
9	HTTP ヘッダ・インジェクション		1	p.34 - 1.7
			2	CWE-113
			3	p.16 - (I)
10	eval インジェクション		1	該当なし
			2	CWE-95
			3	該当なし
11	競合状態の脆弱性		1	該当なし
			2	CWE-366
			3	該当なし
12	意図しないファイル公開		1	該当なし
			2	CWE-425, CWE-548
			3	p.13 - (E)
13	アップロードファイルによるサーバ側スクリプト実行		1	該当なし
			2	CWE-434
			3	該当なし
14	秘密情報表示時のキャッシュ不停止		1	該当なし
			2	CWE-524
			3	該当なし
15	オープンリダイレクタ(意図しないリダイレクト)		1	該当なし
			2	CWE-601
			3	p.15 - (H)
16	クローラへの耐性		1	該当なし
			2	該当なし
			3	p.21 - (M)

2.7 深刻度の定義

本診断では、検出された情報セキュリティに係る事象について、その影響、脆弱性を利用する際に必要な条件、再現性等を考慮し、検出した事象を5段階の深刻度に分類しています。
各深刻度の定義は以下のとおりです。

深刻度	深刻度の解説
Critical	攻撃への利用が容易で直接的な被害を及ぼす可能性がある。
High	大規模な情報漏えいや改ざん、システムの乗っ取り等の影響を受ける可能性がある。
Medium	間接的に情報漏えいや改ざん、サービス妨害等の影響を受ける可能性がある。
Low	サービス提供に影響は無いものの、攻撃者にとって有益な情報を提供する可能性がある。
Info	脆弱性ではないものの、必要に応じて何らかの対策を行った方がよい。

2.8 特記事項

特になし

3. 個別検出事項

3.1 Critical

該当なし

3.2 High

3.2.1 クロスサイトスクリプティング（反射型）

深刻度：High

検出情報

ユーザが入力した文字列がサニタイズされずに出力されるためスクリプトが実行されることを検出しました。 HTTPリクエスト内の攻撃コードがWebページ上で動作するため、罠ページを利用することで改竄したWebページを表示させる等のスクリプトを利用した攻撃が可能となります。

検出事象例

- 対象URL：https://agest.co.jp/■■■■■■■■■■?q=&date_from=&date_to=
- 対象パラメータ：q
- 検査文字列：<script>alert(1)</script>

1. 対象URLにて、パラメータの値に検査文字列を挿入してリクエストを送信します。

   以下は送信したリクエストラインです。

```
GET /■■■■■■■■■■?q=<script>alert(1)</script>&date_from=&date_to= HTTP/2
```

2. サニタイズ処理されずに出力され、スクリプトが実行されることを確認します。

```
HTTP/2 200 OK
Content-Type: text/html;charset=utf-8
(ヘッダ略)

<!DOCTYPE html>
(中略)
<h1>検索結果</h1>
    <div>
        <ul>
            <li><span>&quot; <script>alert(1)</script> &quot;</span>の検索結果</li>
(以下略)
```

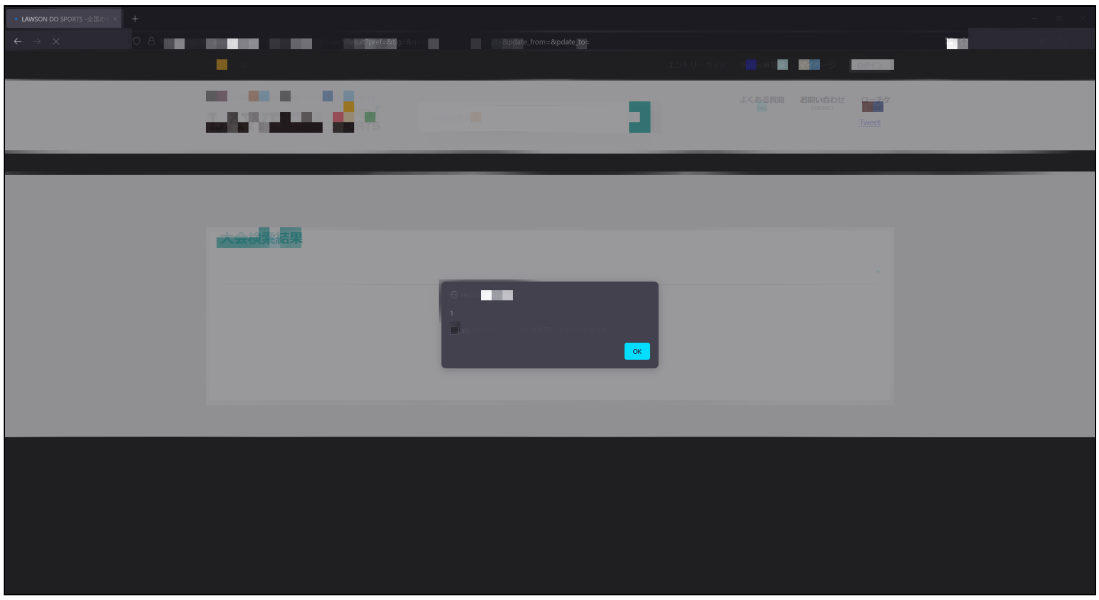

図1 スクリプトが実行される様子

推奨する対策

以下の対応を実施してください。

- クロスサイト・スクリプティング対策として、以下のような処理を実装してください。 HTMLドキュメントへ出力するすべての要素に対し、以下の文字列のエスケープ処理を行ってください。

対象文字	エスケープ後
&	&amp;
<	&lt;
>	&gt;
"	&quot;
'	&#39;

また、JavaScript 内に出力する際には、以下の文字列のエスケープ処理を推奨いたします。

対象文字	エスケープ後
¥	\¥
'	\'
"	\"
改行	\n

出力箇所が多い場合、これらの処理に漏れが発生することがあります。XSS対策用のライブラリやフレームワークの併用も検討してください。

なお、ライブラリやフレームワークを利用する際には、ベンダー情報をご確認の上適切な実装を実施してください。

また、JavaScript内などで文字列のエスケープ処理では対処できない場合も想定されますので、JavaScriptに外部入力の値を返す仕様を検討することを推奨します。

対応が困難な場合、下記の保険的対策を実施してください。

- ブラウザの機能を有効にするレスポンスヘッダを出力してください。
  【X-XSS-Protection】【Content Security Policy】

該当箇所

No	箇所
1	画面名：トップ>検索 URL：https://agest.co.jp/■■■■■■■■■■?q=&date_from=&date_to= パラメータ：q 検査文字列：<script>alert(1)</script>

3.3 Medium

3.3.1 Cookieのセキュア属性不備

深刻度：Medium

検出情報

Cookie内のセッションIDと見られる重要なパラメータにセキュア属性が付加されていないことを確認しました。 Cookieにセキュア属性がない場合、HTTPS通信で発行したCookieは、経路が暗号化されていないHTTP通信でも利用されるため、HTTP通信の盗聴によりCookie情報を不正に取得されてしまう可能性があります。

検出事象例

- 対象URL：https://agest.co.jp/■■■■■■■■■■
- セッション情報：ASP.NET_SessionId

1. 対象URLにてログインした際に発行されるCookieにセキュア属性が付与されないことを確認します。

   以下はCookieが発行された際のレスポンスヘッダとなります。

```
HTTP/2 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Set-Cookie: ASP.NET_SessionId=■■■■■■■■■■■■■■■■; path=/; HttpOnly; SameSite=Lax
Date: Mon, 07 Mar 2022 01:29:56 GMT
Content-Length: 5589
```

推奨する対策

以下の対応を実施してください。

- Cookieを発行する際にセキュア属性を付与してください。
- 常時SSL通信の環境の場合には、HTTP通信の強制による盗聴リスクはありませんが、より安全なCookieの利用のため、セキュア属性の付与を推奨します。

該当箇所

No	箇所
1	画面名：トップ>ログイン画面>ログイン URL：https://agest.co.jp/■■■■■■■■■■

3.4 Low

3.4.1 クリックジャッキング

深刻度：Low

検出情報

レスポンスにX-Frame-Optionsヘッダが出力されておらず、HTMLのiframeタグを利用することで、診断対象のwebページが表示できることを確認しました。 正規サイトを透明なiframeで呼び出し、マウスで操作するボタンやリンクなどに誘導することにより、利用者が意図しないWebアプリケーションの重要な処理が実行されてしまう可能性があります。

検出事象例

1. 診断対象にアクセスした際、レスポンスヘッダ内にX-Frame-Optionsヘッダが表示されないことを確認します。

   以下はX-Frame-Optionsが表示されていないレスポンスヘッダになります。

```
HTTP/2 200 OK
Date: Tue, 01 Mar 2022 03:11:15 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 87458
Server: Apache/2.4.6 (CentOS) PHP/7.4.13
X-Powered-By: PHP/7.4.13
Cache-Control: no-cache, private
Vary: Accept-Encoding
```

図2 フレーム内にサイトが表示される様子

推奨する対策

以下の対応を実施してください。

- HTTPレスポンスヘッダに、X-Frame-Optionsヘッダフィールドを出力し、他ドメインのサイトからのframe要素やiframe要素による読み込みを制限してください。

該当箇所

No	箇所
1	画面名：サイト全体 URL：https://agest.co.jp

3.5 Info

3.5.1 バージョン情報の検出

深刻度：Info

検出情報

レスポンスヘッダに、使用しているソフトウェアのバージョン情報が表示されていることを確認しました。
動作しているサーバやフレームワークのバージョン情報は攻撃者にとって有益な情報となる可能性があります。

検出事象例

- 検出バージョン：Apache/2.4.6 (CentOS) , PHP/7.4.13
- 対象URL：https://agest.co.jp/

1. 対象URLにアクセスした際のレスポンスヘッダにて、バージョン情報が表示されることを確認します。

   以下はバージョン情報が出力されるレスポンスヘッダになります。

```
HTTP/2 200 OK
Date: Tue, 01 Mar 2022 03:35:27 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 87698
Server: Apache/2.4.6 (CentOS) PHP/7.4.13
X-Powered-By: PHP/7.4.13
(以下略)
```

推奨する対策

以下の対応を実施してください。

- ヘッダにバージョンが表示されないようサーバの設定を行うことを推奨します。

該当箇所

No	箇所
1	画面名：サイト全体 URL：https://agest.co.jp

4. 報告書の取り扱いについて

本報告書の取り扱いについては、以下の点にご注意ください。

- 本報告書には、本システムの情報セキュリティ事象についての重要な記述が含まれていますので、取り扱いには十分注意してください。
- 本報告書に記された診断結果や評価は、診断が実施された2022年4月1日時点のものであり、将来にわたり内容を保証するものではありません。
- 本報告書の著作権は弊社が所有しており、複製や改変、第三者への開示は原則禁止とします。
  ただし、システム管理者や経営者への報告、あるいは情報セキュリティ状況改善のため、
  資料として使用する等の場合においては、貴社と弊社との間に交わされた機密保持契約の定めるところに従い、配布することを許可します。