SAMPLE

脆弱性診断報告書

多言語対応・タイムゾーン切り替え機能のリリース前診断

2023年2月実施

サービスサイト： https://s-4.jp/

KRAF

KRAF 御中

S4_多言語対応、タイムゾーン切り替え_脆弱性診断
脆弱性診断報告書（Web アプリケーション診断）

報告書提出日：2023年 02 月 17 日

本報告書について
本報告書は以下の脆弱性診断について、その結果を報告します。

診断期間
2023年 02 月 15 日 ～ 2023年 02 月 17 日

診断種別
Web アプリケーション診断

診断プラン
ゴールド

診断手法
1. 作業者によるマニュアル診断
2. ツールによる診断（主な使用ツール： Burp Suite Professional）

※ 診断結果に対しては弊社にて過検知等の判定とリスク評価を行っております。

接続元 IP アドレス
- 18.177.84.51
- 118.238.251.106
- 124.219.173.135
- 210.161.166.180
- 223.134.12.144

診断対象リクエスト
本書の末尾に記載

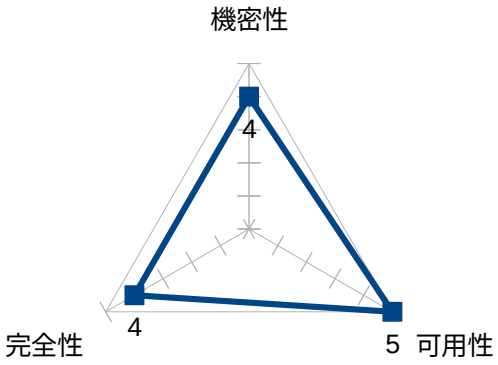
総評

評点 99 点 (/100 点)

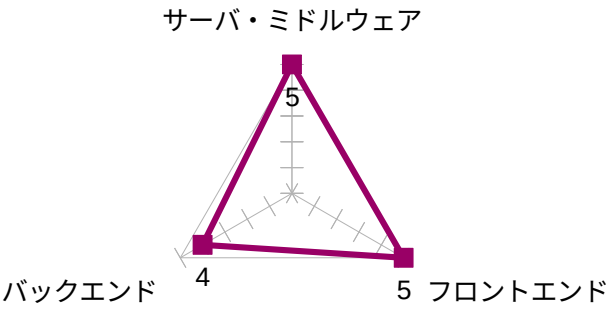
※ この評点は各脆弱性の深刻度に応じた点数により、減点法で計算しています。
評点が高い場合でも改修すべき脆弱性を含む場合がございますので、各脆弱性の詳細をご確認ください。

ここでは脆弱性を「セキュリティ要素」と「システム要素」の観点から 5 段階で評価します。5 段階評価は目安ですので、詳細なリスクと必要な対策は検査項目一覧と各脆弱性の詳細情報を確認ください。
(0: 重大な問題あり ～ 5: 問題なし)

【セキュリティ要素別】



【システム要素別】



セキュリティ要素	説明
機密性	機密性が低い場合、個人情報等の漏えい等のリスクが生じます
完全性	完全性が低い場合、情報の改ざん等のリスクが生じます
可用性	可用性が低い場合、サービス停止等のリスクが生じます

システム要素	説明
サーバ・ミドルウェア	OS や http サービスなどのミドルウェアの問題を表します
バックエンド	認証や入力フォーム、ロジック、出力処理の問題を表します
フロントエンド	古い jQuery や CSS, JS や HTML 記述の問題を表します

コメント:
今回、注意レベルの脆弱性が検出されています。

指摘内容の詳細は各項目を参照ください。

検査項目一覧

「脆弱性の種類(観点)」と「画面」毎に検査数と異常が検知された検査数を示します。
※ 複数の検査で同一の脆弱性を検出する場合があるため、脆弱性の数と検査数は一致しません。
※ この表は検査項目の精度を把握するのにご利用ください。

テスト要素	観点	検査数	緊急	重要	警告	注意	情報
合計		370	0	0	0	1	4
アクセス制御	一般的なアクセス制御の設計	16					
アクセス制御	運用レベルのアクセス制御	1					
アクセス制御	その他のアクセス制御の考慮事項	2				1	
設定	依存性	5					
設定	意図しないセキュリティ暴露の要件	3					
設定	HTTP セキュリティヘッダの要件	7					3
設定	HTTP リクエストヘッダの検証要件	1					
データ	クライアントサイドのデータ保護	8					
データ	機微なプライベートデータ	3					
エラー	エラーハンドリング	1					
エラー	ログのコンテンツ要件	1					
ファイル	SSRF 保護の要件	1					
ファイル	ファイルの保管要件	1					
ファイル	ファイルの実行要件	10					
API	RESTful Web サービスの検証要件	2					
その他	その他	20					
暗号化	アルゴリズム	1					
アプリ汚染	デプロイされたアプリケーションの完全性制御	3					
セッション	セッショントークンの要件	3					
セッション	Cookie ベースのセッション管理	4					1
セッション	セッション管理の基本要件	3					
セッション	セッションのログアウト及びタイムアウトの要件	2					
認証	パスワードのセキュリティ要件	1					
バリデーション	デシリアライズ防止の要件	2					
バリデーション	入力バリデーション要件	3					
バリデーション	出力エンコーディング及びインジェクション防止の要件	254					
バリデーション	サニタイズ及びサンドボックスの要件	2					
通信	通信のセキュリティ要件	10					

画面	検査数	緊急	重要	警告	注意	情報
合計	370	0	0	0	1	4
A01_ログインユーザー情報取得	36					
A02_ログインユーザー情報更新	40					
B01_脆弱性履歴情報取得	38					
B02_脆弱性一覧情報取得	34					
B03_脆弱性情報参照	36					
C01_ログイン組織情報取得	34					
D01_ログインユーザー組織情報取得(スーパーユーザー)	38					
D02_ログインユーザー組織情報更新(スーパーユーザー)	38					
その他	76				1	4

脆弱性一覧

#	深刻度	CVSSv3	脆弱性
1	注意	2.7	社外からの管理サイトへのアクセスに十分な認証が設定されていない
2	情報	0.0	Content-Type に文字コードが未定義のテキストレスポンスが送信される場合がある
3	情報	0.0	Content-Security-Policy ヘッダが適切に設定されていない
4	情報	0.0	Referrer-Policy ヘッダが適切に設定されていない
5	情報	0.0	Cookie 中のセッション ID がホストオンリーでない

深刻度は CVSSv3 に基づき以下のように定義しています。

深刻度	説明	CVSSv3	スコア
緊急	直ちに対策することを推奨する指摘事項です。 緊急レベルの指摘事項は以下のような傾向があるため、多くの場合にリスクを許容できません。 ・機密性・完全性・可用性の何れかに重大な問題が生じる恐れがある ・攻撃の難易度が低いため、攻撃を受ける頻度と攻撃成功の危険性が高い サービスが保持する情報によってはサービス一時停止やネットワークの一時遮断などの暫定措置が推奨されます。 脆弱性の例) 認証回避による成りすまし、サーバ上での任意コード実行(SQL/コマンドインジェクション 等)	9.0～10.0	-50
重要	緊急ほどではありませんが、早急な対策を推奨する指摘事項です。 依然として、攻撃の難易度が低く、攻撃成功時の影響が大きい傾向にあるため注意してください。 脆弱性の例) 罠サイトによるアカウント奪取(セッションハイジャック, XSS)、アクセス制御不備による権限外の情報更新	7.0～8.9	-10
警告	可能であれば対策することを推奨する指摘事項です。 警告レベルの脆弱性は以下のような傾向があります。 ・攻撃難易度は低いが、攻撃成功時の影響が限定的(一部の利用者しか被害を受けない 等) ・攻撃成功時の影響は大きいが、攻撃が比較的困難(中間者攻撃や内部ネットワークへの接触が必要 等) ただし、他の脆弱性と組み合わせることで、結果として緊急に相当する脆弱性に繋がる場合もあるため、リスク受容判断ではご注意下さい。 脆弱性の例) 罠サイトによる特定情報の改竄(CSRF, XSS)、ファイルリスティング	4.0～6.9	-5
注意	比較的軽微な指摘事項です。 対策についてはリスクに応じてご検討ください。 注意レベルで報告される脆弱性の多くは攻撃成立条件が厳しい(物理的接触が必要 等)か、攻撃成功時の影響が限定的(情報の価値が低い 等)です。 ただし、影響が限定的であっても、他の脆弱性の足掛かりになる場合もあるためご注意下さい。 脆弱性の例) PC 内キャッシュを通した情報漏えい、暗号化(SSL)の設定不備	0.1～3.9	-1
情報	リスクの顕在化していない指摘事項です。 直ちに被害を受ける恐れは小さいため、今後の開発で参考としてください。	0.0	

IPA, 共通脆弱性評価システム CVSS v3 概説 https://www.ipa.go.jp/security/vuln/CVSSv3.html

各指摘事項の詳細項目について

①指摘事項 ID　：本書内で識別される指摘事項の ID となります。
②画面（No・画面・URL）：各項目は本書末尾の「診断対象リクエスト」の一覧に対応しています。
画面名は、弊社でリクエスト確認を行った際の操作・機能から名称をつけています。
③報告 ID　：指摘事項が複数の画面・URL で検出された場合に、対象を識別する ID となります。
納品物内の「脆弱性報告一覧.xlsx」の ID と対応しています。
また、エビデンスフォルダ内の No にも対応しています。
④再現方法　：指摘事項の再現方法を記載しています。同一指摘事項が複数の画面・URL で検出された場合は、代表的なものを記載しています。
その他の再現方法については「脆弱性報告一覧.xlsx」をご参照ください。

※ 本項はサンプルとなります※

1

#1. SQL インジェクションの影響を受ける可能性がある

検査項目	SQL インジェクションの影響を受けにくいこと
概要	SQL インジェクションの脆弱性があります。
観点	バリデーション:出力エンコーディング及びインジェクション防止の要件
CVSSv3	緊急 9.9 / 重要 / 警告 / 注意 / 情報 CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H
対応基準	ASVS-5.3.4
CWE	89
画面	2 / 3
脅威	意図しない SQL が実行されるリスクがあります。 これにより、権限の無い閲覧・削除・更新処理のリスクが生じます。 また、複文の実行が可能な場合は任意のデータ操作やシステムコマンドの実行などのリスクが生じます。
対策	SQL 文の組み立てにはフレームワークなどが提供する機能を利用して下さい。 SQL 組み立て機能の例としては JDBC の prepareStatement などがあります。 この機能を利用せず、文字列操作でユーザ入力を SQL 文に挿入すると SQL インジェクションの危険が生じます。 独自に SQL 文のエスケープ処理を行う事も重要コードの信頼性が低下するため推奨されません。
参考	OWASP Code Review Guide (https://owasp.org/www-pdf-archive/OWASP_Code_Review_Guide_v2.pdf)
4 再現方法	0. 以下のアカウントを使用する。 【ID/PW】: testXX@kraf.jp / test1234 1. ログインする。 2. TOP ページへ遷移し検索機能を実施する。 3. 該当のパラメタに直接スクリプトを挿入して該当リクエストを送信する。 発行リクエスト:https://hoge.fuga/example/test.php?search=test 該当パラメタ名:search 3.1 送信したコマンド:test'%20and%20'1'%3d'1 デコード後の値:test' and '1'='1 3.2 送信したコマンド:test'%20and%20'1'%3d'0 デコード後の値:test' and '1'='0 4.以下の操作結果になることを確認する。 評価式が正しい 3.1 の場合:検索結果が正しく表示される。 評価式が誤っている 3.2 の場合:検索結果が 0 件となる。
特記事項	

No	画面	URL	報告 ID
hoge.fuga			
1	A01.TOP ページ_検索_実行	GET /example/test.php?search=test	1

脆弱性詳細

#1. 社外からの管理サイトへのアクセスに十分な認証が設定されていない

検査項目	管理インターフェースが適切な多要素認証により保護されていること
概要	社外からの管理サイトへのアクセスに十分な認証が設定されていません。
観点	アクセス制御:その他のアクセス制御の考慮事項
CVSSv3	緊急 / 重要 / 警告 / 注意 2.7 / 情報 CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N
対応基準	ASVS-4.3.1
CWE	419
画面	No: 000 / 画面: その他 / URL: / 報告 ID: 6 サイト全体
脅威	管理機能へのアクセス制限が不十分なため、管理機能が攻撃に晒されるリスクがあります。 [具体的な攻撃例(IP 制限がない場合)] 1. 悪意あるユーザが社外から管理サイトへアクセスする。 2. ブルートフォースや既知の脆弱性を用いて管理サイトを利用・攻撃する [具体的な攻撃例(認証がない場合)] 1. 悪意あるユーザが管理サイトへアクセス可能なネットワークに侵入する 2. 管理サイトへアクセス、操作をする
対策	社外からアクセスできないよう、管理機能に IP 制限、またはクライアント証明書による制限を設定して下さい。 また、社内の許可されたメンバーのみが管理機能にアクセスできるよう、アプリケーションの認証機構、または Basic/Digest 認証で権限を制御してください。
参考	Apache2 アクセス制御 (http://httpd.apache.org/docs/2.4/howto/auth.html) Tomcat アクセス制御 (http://tomcat.apache.org/tomcat-8.0-doc/config/host.html#Request_Filters)
再現方法	1. 下記の URL にアクセスする。 https://s4-vuln.vams.jp 2. 手順 1 のアクセスに IP 制限、クライアント証明書による制限がないことを確認する。 3. 手順 1 の URL で管理画面が表示されることを確認する。
特記事項	

#2. Content-Type に文字コードが未定義のテキストレスポンスが送信される場合がある

検査項目	全ての HTTP レスポンスが Content-Type ヘッダに安全な文字セットを持つこと
概要	Content-Type に文字コードが未定義のテキストレスポンスが送信される場合があります。
観点	設定:HTTP セキュリティヘッダの要件
CVSSv3	緊急 / 重要 / 警告 / 注意 / 情報 0.0 CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:N/I:N/A:N
対応基準	ASVS-14.4.1
CWE	173
画面	No / 画面 / URL / 報告 ID サイト全体 000 / その他 / / 3
脅威	意図しない文字コードで内容が表示・解釈されるリスクがあります。 これにより、HTML 構文要素のエスケープを実施していても UTF-7 によりこのエスケープを回避することで XSS が可能になるリスクがあります。 例えば以下の文字列は<script>alert('document.cookie')</script> を UTF-7 でエンコードした文字列です。 この文字列には HTML エスケープが必要な文字が含まれませんが、UTF-7 としてデコードされると JavaScript が実行されます。 +ADw-script+AD4-alert('document.cookie')+ADw-/script+AD4- ここでは XSS 脆弱性の発生を確認していないため、情報レベルでの報告となります。 ※実際に脆弱性が確認された場合は別途報告しております。
対策	スクリプトやテキストに対しては Content-Type に文字コードを指定してください。 これにより、文字列が UTF-7 として表示されることを防止します。 なお、HTML 中の <meta> 要素で指定する方法は一定程度の効果はありますが、meta タグを攻撃者によって挿入・改ざんされる可能性があること、また設定漏れが起きる懸念があることから推奨しておりません。HTTP ヘッダに記載することが望ましい対応となります。
参考	Secure Headers (https://www.owasp.org/index.php/OWASP_Secure_Headers_Project)
再現方法	1. レスポンスのヘッダを確認する。 2. Content-Type に文字コードが未定義となっていることを確認する。 以下のリクエストで検出されました。 GET /
特記事項	

#3. Content-Security-Policy ヘッダが適切に設定されていない

検査項目	XSS 攻撃を緩和するためにコンテンツセキュリティポリシーが設定されていること
概要	レスポンスに Content-Security-Policy ヘッダが適切に設定されていません。
観点	設定:HTTP セキュリティヘッダの要件
CVSSv3	緊急 / 重要 / 警告 / 注意 / 情報 0.0 CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:C/C:N/I:N/A:N
対応基準	ASVS-14.4.3
CWE	1021
画面	No: 000 / 画面: その他 / URL: / 報告 ID: 2 サイト全体
脅威	※ これは対象システムに XSS が存在した場合に被害を緩和するための予防的措置です。 Content-Security-Policy により HTML 中のインラインスクリプトや eval 関数が適切に規制されていません。 これにより、XSS の脆弱性が存在した場合に被害を抑止できない可能性があります。
対策	全てのレスポンスに Content-Security-Policy（CSP） を適切なパラメタとともに付与することで、XSS のリスクを緩和できます。 CSP のパラメタとして以下のような例が挙げられます。 Content-Security-Policy: default-src 'self'; script-src 'self'; この場合、インラインスクリプト（script タグ および onclick 等のイベントハンドラ）が許可されていないため、XSS 攻撃により埋め込まれても実行されません。 なお、CSP ヘッダには以下の非推奨キーワードを用いないことを推奨いたします。 非推奨キーワード: 'unsafe-inline', 'unsafe-eval' これらはそれぞれ、インラインスクリプトの利用と eval（および同様の Text→JavaScript 変換関数）の利用を明示的に許可します。 いずれも XSS が存在する場合に攻撃に利用しやすくなります。 また、'nonce-'キーワードを用いることで特定のインラインスクリプトを許可できますが、 根本的にインラインスクリプトを用いないことを推奨します。 Content-Security-Policy による規制は以下に限定されます。 Chrome, Firefox, Edge, Safari7 以上
参考	OWASP Secure Headers Project (https://owasp.org/www-project-secure-headers/) Content Security Policy (https://owasp.org/www-community/controls/Content_Security_Policy)
再現方法	1. レスポンスヘッダを確認する。 2. Content-Security-Policy ヘッダが適切に設定されていないことを確認する。 Content-Security-Policy ヘッダに default-src が設定されていません。 Content-Security-Policy: frame-ancestors 'none' ※対象については、添付ファイルをご参照ください。
特記事項	

#4. Referrer-Policy ヘッダが適切に設定されていない

検査項目	Referrer-Policy ヘッダが適切に no-referrer や same-origin 等に設定されていること
概要	レスポンスに Referrer-Policy ヘッダが適切に設定されていません。
観点	設定:HTTP セキュリティヘッダの要件
CVSSv3	緊急 / 重要 / 警告 / 注意 / 情報 0.0 CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:N/A:N
対応基準	ASVS-14.4.6
CWE	116
画面	No / 画面 / URL / 報告 ID サイト全体 000 / その他 / / 4
脅威	ブラウザの Referrer を介し、ページの URL が外部サイトに共有されます。 秘匿しているページのパスや、URL に含まれる重要情報がある場合、それらが漏えいするおそれがあります。 Referrer を取得するにはページ内に URL を埋め込む必要があるため、情報レベルでの報告となります。
対策	Referrer-Policy ヘッダをレスポンスに付与し、パス情報を外部に提供しないようにしてください。 このようなディレクティブには以下があります。 ・外部サイトに Referrer を提供しない - same-origin - no-referrer ・外部サイトにオリジン情報のみを提供する(パスを提供しない) - origin-when-cross-origin - strict-origin-when-cross-origin - origin - strict-origin 複数設定する場合は、優先したいディレクティブを後方にしてください。 例. origin-when-cross-origin ポリシーを指定するが、対応しないブラウザでは same-origin ポリシーとする。 Referrer-Policy: same-origin, origin-when-cross-origin なお、HTML 中の <meta> 要素で指定する方法は一定程度の効果はありますが、meta タグを攻撃者によって挿入・改ざんされる可能性があること、また設定漏れが起きる懸念があることから推奨しておりません。HTTP ヘッダに記載することが望ましい対応となります。
参考	MDN web docs (https://developer.mozilla.org/ja/docs/Web/HTTP/Headers/Referrer-Policy)
再現方法	1. レスポンスのヘッダを確認する。 2. Referrer-Policy ヘッダが設定されていないことを確認する。 ※対象については、添付ファイルをご参照ください。
特記事項	

#5. Cookie 中のセッション ID がホストオンリーでない

<table>
<tr><td>検査項目</td><td>Cookie ベースのセッショントークンが '__Host-' プレフィックスと適切な path 属性を付与され、セッション Cookie の信頼性を向上させること</td></tr>
<tr><td>概要</td><td>Cookie 中のセッション ID の設定が当該ホストに限定されていません。</td></tr>
<tr><td>観点</td><td>セッション:Cookie ベースのセッション管理</td></tr>
<tr><td>CVSSv3</td><td>
<table>
<tr><th>緊急</th><th>重要</th><th>警告</th><th>注意</th><th>情報</th></tr>
<tr><td></td><td></td><td></td><td></td><td>0.0</td></tr>
</table>
CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:N/A:N
</td></tr>
<tr><td>対応基準</td><td>ASVS-3.4.4, ASVS-3.4.5</td></tr>
<tr><td>CWE</td><td>16</td></tr>
<tr><td>画面</td><td>
<table>
<tr><th>No</th><th>画面</th><th>URL</th><th>報告 ID</th></tr>
<tr><td colspan="4">api-vuln.vams.jp</td></tr>
<tr><td>000</td><td>その他</td><td></td><td>1</td></tr>
</table>
</td></tr>
<tr><td>脅威</td><td>対象の Cookie に対して、平文 HTTP 通信での設定や Domain 属性が禁止されていません。

そのため、以下の方法でセッション ID が書き換えられるおそれがあります。
・平文 HTTP の中間者攻撃でレスポンスに Set-Cookie ヘッダを付与される
・サブドメインが乗っ取られた場合にドメインレベルの Cookie を設定される

セッション ID が書き換えられると、セッションフィクセーション脆弱性がある場合にユーザのログインセッションが乗っ取られるおそれがあります。

リスクの顕在化する条件が限定されるため、情報レベルでの指摘としています。</td></tr>
<tr><td>対策</td><td>セッション ID が以下を満たすようにしてください。

(1) Cookie 名に '__Host-' プレフィックスを付与する
(2) Secure 属性を設定する
(3) オリジンが HTTPS である
(4) Domain 属性を設定しない
(5) path 属性を '/' に設定する

※(2)～(5)は(1)の Cookie が正常に動作するための要件でもあります。

これにより、中間者攻撃やサブドメインによる Cookie 設定を防止できます。ただし、同一ホストの異なるポートによる Cookie 設定を防止することはできません。</td></tr>
<tr><td>参考</td><td>MDN web docs (https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Set-Cookie)</td></tr>
<tr><td>再現方法</td><td>0. 以下のアカウントを利用しログインする。
【ID/PW】sft.test.ss01.003@gmail.com / t7rwudZ23Ywg (スーパーユーザー)
1. Set-Cookie ヘッダが付与されるリクエストのレスポンスを確認する。
2. Set-Cookie ヘッダに記載されているセッション ID に '__Host-' プレフィックスが付与されていないことを確認する。

【詳細】
[リクエスト]
GET /api/user HTTP/1.1

[レスポンス]
HTTP/1.1 200 OK
Set-Cookie:
s4_vuln_session=eyJpdiI6InBwdVY0Qzd1bGN0YTNFZjJvYzhVdlE9PSIsInZhbHVlIjoidlUxejJqL29IRFhXdWVTb2JBTEwybzNjL2VJODErVHJaZGk5MG44M0lxQ2FpWTVqREdCQ1R6TDJLWS9YbENoMWNWNEdNS0xFbWY1SDNDUlJOMytYbDV2eU5kUFZJOWxpYWJJTitKWW9NOUxuenYzSW1QOEY4QU5mYzVsZC91eHQiLCJtYWMiOiI0YW</td></tr>
</table>

	NkNzVlNTQwNTYxNDVlZjFlZjRjZmYyYmViYmIwZGJkMWE3Y2EyZTIwNmJjMzIyYjkwMDBhZjdkZDkxMDcwIiwidGFnIjoiIn0%3D; expires=Thu, 16 Feb 2023 09:34:47 GMT; Max-Age=28800; path=/; domain=.vams.jp; secure; httponly; samesite=lax
特記事項	

セッション情報

＜　セッション情報　＞		
パラメタ名/値(例)	s4_vuln_session	eyJpdiI6IjdDYnpNQ2ovcWJISjVmSk1RYTVaQUE9PSIsInZhbHVlIjoic1NIQVpnQzFGRFN3TnMxZ1BMQ1hrUkhJNDhsTmxHd0R4czdldmNrNnloWW50d2o1Z1FpaUhEMnREVXJQSVB6bXYzZ3pqZFpxSjZWMGIvWE1WREtCTDFCaHE0eld3b1FaYzFqdlMrZDBNYU41NHljL1FXbm1nUkNqdWQrRXo0bDIiLCJtYWMiOiIzYzRiZTU5ODYzYWIzZDQ5ZDkzOGEwODRmZTY3ZmMxOTRkNjEwYWIzMzdjMDRhY2JjYzliNDcwZGFkOTY0MGIxIiwidGFnIjoiIn0%3D
セッション種別	サーバサイドセッション	
保存方法	Cookie	
送信方法	Cookie	
Secure 属性		
HttpOnly 属性		
Samesite 属性		
__Host-プレフィックス	なし	
エンコード	0	
デコード結果	{"iv":"7CbzMCj/qbHJ5fJMQa5ZAA==","value":"sSHAZgC1FDSwNs1gPLCXkRHI48lNlGwDxs7evck6yhYntwj5gQiiHD2tDUrPIPzmv3gzjdZqJ6V0b/XMVDKBL1Bhq4zWwoQZc1jvS+d0MaN54yc/QWnmgRCjud+Ez4l2","mac":"3c4be59863ab3d49d938a084fe67fc194d610ab337c04acbcc9b470dad9640b1","tag":""}	
有効期間	10 時間以内	

診断対象リクエスト
対象ドメイン: api-vuln.vams.jp

#	画面名	メソッド	パス
001	A01_ログインユーザー情報取得	GET	/api/user
002	A02_ログインユーザー情報更新	PUT	/api/user
003	B01_脆弱性履歴情報取得	GET	/api/issues/25133/history
004	B02_脆弱性一覧情報取得	GET	/api/issues
005	B03_脆弱性情報参照	GET	/api/issues/25133
006	C01_ログイン組織情報取得	GET	/api/login/organization
007	D01_ログインユーザー組織情報取得(スーパーユーザー)	GET	/api/org
008	D02_ログインユーザー組織情報更新(スーパーユーザー)	PUT	/api/org

用語解説

CVSS（共通脆弱性評価システム、Common Vulnerability Scoring System）

CVSS は、情報システムの脆弱性に対するオープンで汎用的な評価手法であり、ベンダーに依存しない共通の評価方法を提供しています。CVSS を用いると、脆弱性の深刻度を同一の基準の下で定量的に比較できるようになります。また、ベンダー、セキュリティ専門家、管理者、ユーザ等の間で、脆弱性に関して共通の言葉で議論できるようになります。

- 引用元：IPA「共通脆弱性評価システム CVSS v3 概説」
  https://www.ipa.go.jp/security/vuln/CVSSv3.html

CWE（共通脆弱性タイプ一覧、Common Weakness Enumeration）

CWE は、ソフトウェア及びハードウェアの一般的な脆弱性種別の一覧です。実装やコード、設計、アーキテクチャにおける、攻撃に脆弱となりうる問題について分類されています。CWE を用いて識別することで、その脆弱性を共通言語で議論する、一般的な対策方法を確認する等が可能となります。

- IPA「共通脆弱性タイプ一覧 CWE 概説」
  https://www.ipa.go.jp/security/vuln/CWE.html

XSS（クロスサイト・スクリプティング、Cross-site Scripting）

XSS は HTML や XML 等を動的に生成する仕組みを設けている場合に、セキュリティ上の問題となるものです。XSS により攻撃者のスクリプトがブラウザ上で実行されると情報漏えいやユーザの意図しない操作が実行されるリスクがあります。

CSRF（クロスサイト・リクエスト・フォージェリ、Cross-site Request Forgery）

CSRF は第三者が意図したリクエストを強制送信させることで任意のコマンドを実行できるため、情報改竄・情報漏洩に加えて、他のサーバへの攻撃に悪用されるなどのリスクがあります。

EICAR テストファイル

EICAR テストファイルはアンチマルウェアソフトの動作を確認するためのテストファイルです。このファイルは無害ですが、多くのアンチマルウェアソフトでは検査用ファイルとして登録されており、マルウェアとして検知されます。

セキュリティ動向
ここでは各種機関からの注意喚起を元に情報セキュリティにおける動向について紹介します。

Microsoft 製品の脆弱性
2023 年 1 月 11 日（日本時間）に Microsoft 製品に関する脆弱性の修正プログラムが公表されています。
これらの脆弱性を悪用された場合、アプリケーションプログラムが異常終了したり、攻撃者によってパソコンを制御されたりして、様々な被害が発生するおそれがあります。

- https://www.ipa.go.jp/security/ciadr/vul/20230111-ms.html
- https://www.jpcert.or.jp/at/2023/at230002.html

Adobe Acrobat および Reader の脆弱性
アドビ社から Adobe Acrobat および Reader に関する脆弱性（APSB23-01）が公表されています。
アドビ社からは、過去に攻撃者の標的になったことのない脆弱性としてアナウンスがされておりますが、悪用された場合、不正なコードが実行される恐れのある緊急度がクリティカルの脆弱性も含まれているため、修正プログラムを適用することを推奨します。

- https://www.ipa.go.jp/security/ciadr/vul/20230111-adobereader.html
- https://www.jpcert.or.jp/at/2023/at230001.html

Oracle Java の脆弱性
Oracle 社から Java SE に関する脆弱性が公表されています。
同社からは攻撃された場合の影響が大きい脆弱性であることがアナウンスされているため、できるだけ早急に修正プログラムを適用してください。

- https://www.ipa.go.jp/security/ciadr/vul/20230118-jre.html
- https://www.jpcert.or.jp/at/2023/at230003.html

DNS サーバ BIND の脆弱性
DNS サーバの BIND に、リモートからのサービス運用妨害（DoS）の脆弱性が存在します。
この脆弱性が悪用された場合、意図しないサービスの停止が発生する可能性があります。
脆弱性を悪用した攻撃はまだ確認されていませんが、今後攻撃が発生する可能性があるため、DNS サーバ管理者はアップデートを適用してください。

- https://www.ipa.go.jp/security/ciadr/vul/alert20230126.html
- https://www.jpcert.or.jp/newsflash/2023012601.html

Windows 8.1 のサポート終了に伴う注意喚起
2023 年 1 月 10 日（米国時間）に、Windows 8.1、Windows 7 ESU、Windows Server 2008 ESU、Windows Server 2008 R2 ESU のサポートが終了しました。
サポート終了後はセキュリティ更新プログラムの提供がなくなり、セキュリティリスクが高まります。
同ソフトウェア製品の利用者においては、サポートが継続している後継製品、または代替製品への移行などの対応が望まれます。また、OS だけでなく、アプリケーションもサポートが順次終了していくため、あわせて対策が必要です。

- https://www.ipa.go.jp/security/announce/win8_1_eos.html

特記事項

免責事項

本脆弱性診断は診断対象のアプリケーションにアクセスし、一般的な利用者の立場で解析・検査ツール等を利用して行うブラックボックステスト手法にて診断を実施しております。ブラックボックステストの特性上、本報告書の指摘事項は再現性・網羅性について完全に保証するものではないことをご了承ください。
また、本報告書指摘事項について対策を実施する際は、貴社の責任において実施くださるようお願いいたします。

お問い合わせ

本報告書に関するご質問・お問い合わせを本報告書提出後、1ヶ月間承ります。