SAMPLE

# 脆弱性診断設計書

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

| ケースNo | 観点No | 観点分類 | 検査観点 | 検査基準 | 脆弱性 | ASVS | 検査粒度 | 検査対象 | ホスト | メソッド | URL | 画面 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | ZZ01 | – | – | – | – | | 全体 | 全て | | | | |
| 2 | ZZ03 | – | – | – | – | | 全体 | 全て | | | | |
| 3 | CV01 | 設定 | HTTPリクエストヘッダの検証要件 | CORSの Access-Control-Allow-Origin ヘッダがホワイトリストを使用してドメインを照合すること | CORSが適切に設定されていない | 14.5.3 | 全体 | – | | | | |
| 4 | VO13 | 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 | SQLインジェクションの影響を受けにくいこと | – | 5.3.4 | 全体 | – | | | | |
| 5 | VO15 | 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 | NoSQLインジェクションの影響を受けにくいこと | – | 5.3.4 | 全体 | – | | | | |
| 6 | VO19 | 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 | OSコマンドインジェクションの影響を受けにくいこと | – | 5.3.8<br>12.3.5 | 全体 | – | | | | |
| 7 | FX01 | ファイル | ファイルの実行要件 | パストラバーサルやローカルファイルインクルードの影響を受けにくいこと | – | 12.3.1<br>5.3.9 | 全体 | – | | | | |
| 8 | CD03 | 設定 | 依存性 | 不要な機能及び文書、サンプル、設定が削除されていること | 本来参照できないファイルが参照できる | 14.2.2 | 全体 | – | | | | |
| 9 | VO28 | 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 | HTTPヘッダインジェクションの影響を受けにくいこと | – | 5.3.5 | 全体 | – | | | | |
| 10 | VO17 | 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 | LDAPインジェクションの影響を受けにくいこと | – | 5.3.7<br>5.1.3 | 全体 | – | | | | |
| 11 | VO21 | 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 | XMLインジェクションの影響を受けにくいこと | – | 5.3.10 | 全体 | – | | | | |
| 12 | VD02 | バリデーション | デシリアライズ防止の要件 | XXEの影響を受けにくいこと | – | 5.5.2 | 全体 | – | | | | |
| 13 | VO23 | 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 | XPathインジェクションの影響を受けにくいこと | – | 5.3.10<br>5.1.3 | 全体 | – | | | | |
| 14 | VD01 | バリデーション | デシリアライズ防止の要件 | 悪意のあるオブジェクト生成やデータ改ざんを防ぐこと | シリアライズされたコードがサーバ・クライアント間で通信される | 5.5.1<br>5.5.3 | 全体 | – | | | | |
| 15 | VS07 | バリデーション | サニタイズ及びサンドボックスの要件 | 動的コード実行に含まれるユーザ入力がサニタイズもしくはサンドボックス化されること | ELインジェクションの影響を受ける可能性がある | 5.2.4 | 全体 | – | | | | |
| 16 | CD01 | 設定 | 依存性 | 全てのコンポーネントが最新であること | WEBコンポーネントに適切なセキュリティ設定が施されていない | 14.2.1 | 全体 | – | | | | |
| 17 | CD02 | 設定 | 依存性 | 全てのコンポーネントが最新であること | ※ このケースでは起票しない（検査手順の指示に従い起票する） | 14.2.1 | 全体 | – | | | | |
| 18 | FF09 | ファイル | SSRF保護の要件 | サーバのリクエスト送信先やデータの読み込み元が制限されており、リモートファイルインクルード及びSSRFの影響を受けにくいこと | サーバから外部への通信を強制できる | 12.6.1<br>5.2.6<br>5.3.9<br>13.1.1 | 全体 | – | | | | |
| 19 | VI01 | バリデーション | 入力バリデーション要件 | HTTPパラメタ汚染の影響を受けにくいこと | HTTPパラメタ汚染攻撃の影響を受ける可能性がある | 5.1.1 | 全体 | – | | | | |
| 20 | VS08 | バリデーション | サニタイズ及びサンドボックスの要件 | テンプレートインジェクションの影響を受けにくいこと | テンプレートインジェクション攻撃の影響を受ける可能性がある | 5.2.5 | 全体 | – | | | | |
| 21 | CE01 | 設定 | 意図しないセキュリティ暴露の要件 | 本番環境のWebサーバやアプリケーションサーバやアプリケーションフレームワークではデバッグモードが無効化されていること | デバッグモードが有効化されている | 14.3.2 | 全体 | – | | | | |
| 22 | VO01 | 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 | いかなるUnicode符号位置も安全に処理し、出力エンコーディングがユーザ指定の文字セットとロケールを保持すること | Unicodeの出力が正しくエンコーディングされない | 5.3.2 | 全体 | – | | | | |
| 23 | VO03 | 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 | 出力の適切なエスケープにより反射型XSSの影響を受けにくいこと | – | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1 | 全体 | – | | | | |
| 24 | VO04 | 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 | 出力の適切なエスケープにより保存型XSSの影響を受けにくいこと | – | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1 | 全体 | – | | | | |
| 25 | VO30 | 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 | 出力の適切なエスケープによりDOMベースXSSの影響を受けにくいこと | DOM要素の値を安全でないJavaScript関数が使用している | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1<br>5.3.6<br>5.5.4 | 全体 | – | | | | |
| 26 | ZZ06 | – | – | – | – | | 全体 | – | | | | |
| 27 | VO06 | 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 | 出力の適切なエスケープにより保存型XSSの影響を受けにくいこと | – | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1 | 全体 | – | | | | |
| 28 | SG04 | セッション | セッション管理の基本要件 | URLにセッショントークンが含まれないこと | URLにセッションIDが含まれ、セッションハイジャックの危険がある | 3.1.1<br>13.1.3 | 全体 | – | | | | |
| 29 | CH04 | 設定 | HTTPセキュリティヘッダの要件 | 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 | Content-Security-Policyヘッダが適切に設定されていない | 14.4.3 | 全体 | – | | | | |

| ケースNo | 観点No | 観点分類 | 検査観点 | 検査基準 | 脆弱性 | ASVS | 検査粒度 | 検査対象 | ホスト | メソッド | URL | 画面 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 30 | CH02 | 設定 | HTTPセキュリティヘッダの要件 | 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 | 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 | 14.4.1 | 全体 | – | | | | |
| 31 | CH01 | 設定 | HTTPセキュリティヘッダの要件 | 全てのHTTPレスポンスがContent-Typeヘッダを持つこと | Content-Typeが未定義のレスポンスが送信される場合がある | 14.4.1 | 全体 | – | | | | |
| 32 | CH03 | 設定 | HTTPセキュリティヘッダの要件 | 全てのAPIレスポンスが以下のヘッダを含むこと<br>X-Content-Type-Options: nosniff<br>Content-Disposition: attachment;filename="XXXX.json" | JSONレスポンスのXSSに対する予防的措置が適切に設定されていない | 14.4.2<br>14.4.4<br>12.3.4 | 全体 | – | | | | |
| 33 | VI05 | バリデーション | 入力バリデーション要件 | URLリダイレクトがホワイトリスト化された宛先のみ許可されること | 安全でないホストにリダイレクトされる場合がある | 5.1.5 | 全体 | – | | | | |
| 34 | CH06 | 設定 | HTTPセキュリティヘッダの要件 | 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 | Referrer-Policyヘッダが適切に設定されていない | 14.4.6 | 全体 | – | | | | |
| 35 | EH02 | エラー | エラーハンドリング | 想定外エラーが生じた際に一般的なメッセージが表示されること | 不要な開発情報が出力される | 7.4.1<br>5.1.4<br>5.2.2 | 全体 | – | | | | |
| 36 | CH05 | 設定 | HTTPセキュリティヘッダの要件 | HTTP Strict Transport Securityヘッダが全てのレスポンスに含まれること | Strict-Transport-Securityヘッダが適切に設定されていない | 14.4.5 | 全体 | – | | | | |
| 37 | CD05 | 設定 | 依存性 | アセットがコンテンツデリバリネットワーク（CDN）や外部プロバイダに外部ホスティングされている場合、サブリソース完全性（SRI）を使用してアセットの整合性を検証すること | 外部読み込みのリソース完全性が確認されていない | 14.2.3<br>10.3.2 | 全体 | – | | | | |
| 38 | CH07 | 設定 | HTTPセキュリティヘッダの要件 | 第三者サイトに埋め込まれないようX-Frame-Options またはContent-Security-Policy: frame-ancestors ヘッダを持つこと | クリックジャッキング対策ヘッダが適切に設定されていない | 14.4.7 | 全体 | – | | | | |
| 39 | CE05 | 設定 | 意図しないセキュリティ暴露の要件 | エラーメッセージがシステムコンポーネントのバージョン情報を露見させないこと | エラーメッセージにシステムのバージョン情報が含まれる場合がある | 14.3.3 | 全体 | – | | | | |
| 40 | SG02 | セッション | セッション管理の基本要件 | エラーメッセージにセッショントークンが含まれないこと | エラーメッセージにセッションIDが含まれ、セッションハイジャックの危険がある | 3.1.1 | 全体 | – | | | | |
| 41 | VI02 | バリデーション | 入力バリデーション要件 | フレームワークがMass Assignment攻撃の影響を受けにくいこと | Mass Assignment攻撃の影響を受ける可能性がある | 5.1.2 | 全体 | – | | | | |
| 42 | EO02 | エラー | ログのコンテンツ要件 | クレデンシャルや決済明細等の機微データがロギングされないこと | アプリケーションのログに機微な情報が含まれている | 7.1.1<br>7.1.2 | 全体 | – | | | | |
| 43 | DP03 | データ | 機微なプライベートデータ | 個人情報の収集と使用について明文化されオプトインでの同意が提供されていること | 個人情報の収集と使用について情報提供が十分でない | 8.3.3 | 全体 | – | | | | |
| 44 | DP02 | データ | 機微なプライベートデータ | ユーザが自身のデータを要求に応じて削除およびエクスポートする手段を持っていること | ユーザが自身のデータを削除・エクスポートできない | 8.3.2 | 全体 | – | | | | |
| 45 | DP04 | データ | 機微なプライベートデータ | 機密データが特定され取り扱いポリシーが存在すること | 機密データの特定が不十分、またはポリシーが明確でない | 8.3.4 | 全体 | – | | | | |
| 46 | MA01 | 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 | アプリケーション自動更新がセキュアな経路で取得され、デジタル署名されていること | 自動更新においてアップデートの真正性確認が十分でない | 10.3.1 | 全体 | – | | | | |
| 47 | MA02 | 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 | アプリケーションが完全性保護策を講じられていること | アプリケーションの完全性保護策が十分でない | 10.3.2 | 全体 | – | | | | |
| 48 | MA03 | 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 | アプリケーションの依存するDNSエントリ・サブドメインの乗っ取り対策が講じられていること | 依存先ドメインのDNS情報の乗っ取り対策が十分でない | 10.3.3 | 全体 | – | | | | |
| 49 | FX03 | ファイル | ファイルの実行要件 | ローカルファイルやリモートファイルの暴露や実行を防ぐために、ユーザファイルのメタデータが検証されること | ユーザ由来の信用できないデータが実行される危険がある | 12.3.2<br>12.3.3 | 全体 | – | | | | |
| 50 | FS01 | ファイル | ファイルの保管要件 | 信頼されないソースからのファイルが安全に保管されること | 信頼されないソースから得られたファイルの保管方法が安全でない | 12.4.1 | 全体 | – | | | | |
| 51 | IA02 | API | RESTful Webサービスの検証要件 | JSONやXMLの入力値がスキーマにより検証されること | XMLやJSONをサーバで受け入れる際にスキーマのバリデーションが実施されない | 13.2.2<br>13.3.1 | 全体 | – | | | | |
| 52 | TP03 | 認証 | パスワードのセキュリティ要件 | ユーザが自身のパスワードを変更できること | ユーザが自身のパスワードを変更できない | 2.1.5 | 全体 | – | | | | |
| 53 | AZ01 | アクセス制御 | その他のアクセス制御の考慮事項 | 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 | 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 | 4.3.1 | 全体 | – | | | | |
| 54 | SG05 | セッション | セッション管理の基本要件 | – | – | | ドメイン | 全て | api-vuln.vams.jp | | | |
| 55 | SB08 | セッション | セッショントークンの要件 | セッショントークンが64ビット以上のエントロピーをもつこと | ユーザ認証に固定値のトークンを使用している | 3.2.2 | ドメイン | 全て | api-vuln.vams.jp | | | |
| 56 | SB03 | セッション | セッショントークンの要件 | セッショントークンが64ビット以上のエントロピーをもつこと | セッションIDのランダム性が十分でない | 3.2.2 | ドメイン | 全て | api-vuln.vams.jp | | | |
| 57 | SC06 | セッション | Cookieベースのセッション管理 | 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 | Cookie中のセッションIDがホストオンリーでない | 3.4.4<br>3.4.5 | ドメイン | 全て | api-vuln.vams.jp | | | |
| 58 | SO01 | 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 | ログアウトによりセッショントークンが無効化されること | ログアウトしたアカウントで認証が必要な操作が実施できる | 3.3.1 | ドメイン | 全て | api-vuln.vams.jp | | | |

| ケースNo | 観点No | 観点分類 | 検査観点 | 検査基準 | 脆弱性 | ASVS | 検査粒度 | 検査対象 | ホスト | メソッド | URL | 画面 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 59 | SB06 | セッション | セッショントークンの要件 | セッショントークンがブラウザ内にセキュアな方法で保管されること | セッションIDがセキュアでない方法で保管される | 3.2.3 | ドメイン | 全て | api-vuln.vams.jp | | | |
| 60 | DC04 | データ | クライアントサイドのデータ保護 | セッション終了後に要認証データがクライアントストレージからクリアされること | ログアウト時にストレージ内のデータが残存する | 8.2.3 | ドメイン | 全て | api-vuln.vams.jp | | | |
| 61 | IA01 | API | RESTful Webサービスの検証要件 | 使用されているHTTPメソッドのみを受理すること | TRACEメソッドが受理される | 13.2.1<br>14.5.1 | ドメイン | 全て | api-vuln.vams.jp | | | |
| 62 | CE02 | 設定 | 意図しないセキュリティ暴露の要件 | レスポンスヘッダがシステムコンポーネントのバージョン情報を露見させないこと | HTTPヘッダにバージョン情報が含まれる場合がある | 14.3.3 | ドメイン | 全て | api-vuln.vams.jp | | | |
| 63 | AZ03 | アクセス制御 | その他のアクセス制御の考慮事項 | ディレクトリブラウジングが無効化されていること | サーバのファイルリスティングが有効になっている | 4.3.2 | ドメイン | 全て | api-vuln.vams.jp | | | |
| 64 | CD04 | 設定 | 依存性 | 不要な機能及び文書、設定、メタデータ等のファイルが公開されていないこと | デフォルトやサンプルファイルが適切に無効化されていない | 14.2.2<br>4.3.2<br>12.5.1 | ドメイン | 全て | api-vuln.vams.jp | | | |
| 65 | SC02 | セッション | Cookieベースのセッション管理 | Cookieベースのセッショントークンに 'Secure' 属性が付与されていること | Cookie中のセッションIDがSecure属性で保護されていない | 3.4.1 | ドメイン | 全て | api-vuln.vams.jp | | | |
| 66 | SC07 | セッション | Cookieベースのセッション管理 | Cookieベースのセッショントークンに 'HTTPOnly' 属性が付与されていること | Cookie中のセッションIDがHttpOnly属性で保護されていない | 3.4.2 | ドメイン | 全て | api-vuln.vams.jp | | | |
| 67 | SC03 | セッション | Cookieベースのセッション管理 | Cookieベースのセッショントークンに 'SameSite' 属性が付与されていること | Cookie中のセッションIDがSameSite属性でCSRFから保護されていない | 3.4.3 | ドメイン | 全て | api-vuln.vams.jp | | | |
| 68 | KA01 | – | – | – | – | | ドメイン | 全て | api-vuln.vams.jp | | | |
| 69 | KA02 | 暗号化 | アルゴリズム | Padding Oracle攻撃を防ぐこと | 暗号化された通信で暗号解読に有効な情報が表示される場合がある | 6.2.1<br>9.1.3 | ドメイン | 全て | api-vuln.vams.jp | | | |
| 70 | XG06 | 通信 | 通信のセキュリティ要件 | TLS 1.0が無効化されていること | TLS 1.0が有効になっている | 9.1.3 | ドメイン | 全て | api-vuln.vams.jp | | | |
| 71 | XG07 | 通信 | 通信のセキュリティ要件 | TLS 1.1が無効化されていること | TLS 1.1が有効になっている | 9.1.3 | ドメイン | 全て | api-vuln.vams.jp | | | |
| 72 | XG01 | 通信 | 通信のセキュリティ要件 | セキュアでないTLSアルゴリズムにフォールバックしないこと | セキュアではない暗号化アルゴリズムが使用される場合がある | 9.1.1 | ドメイン | 全て | api-vuln.vams.jp | | | |
| 73 | XG04 | 通信 | 通信のセキュリティ要件 | 最も強力なTLS暗号方式が優先されること | 強力なTLS暗号スイートがデフォルトで選択されない | 9.1.2 | ドメイン | 全て | api-vuln.vams.jp | | | |
| 74 | AO07 | アクセス制御 | 運用レベルのアクセス制御 | 強力なCSRF対策により認証の必要な機能が保護されること | CSRFトークンの強度が十分ではない | 4.2.2<br>13.2.3 | ドメイン | 全て | api-vuln.vams.jp | | | |
| 75 | DC03 | データ | クライアントサイドのデータ保護 | クライアントストレージに機微情報や個人情報を保持しないこと | 重要情報がクライアントストレージに格納される | 8.2.2 | ドメイン | 全て | api-vuln.vams.jp | | | |
| 76 | SO03 | 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 | 一定時間ごとに再認証が起こること | セッションの有効期限が長い | 3.3.2 | ドメイン | 全て | api-vuln.vams.jp | | | |
| 77 | ZZ02 | – | – | – | – | | リクエスト | !Intruderのみ実施 | https://api-vuln.vams.jp | GET | /api/user | A01_ログインユーザー情報取得 |
| 78 | ZZ07 | – | – | – | – | | リクエスト | !Intruderのみ実施 | https://api-vuln.vams.jp | GET | /api/user | A01_ログインユーザー情報取得 |
| 79 | XG05 | 通信 | 通信のセキュリティ要件 | TLSがクライアント接続に使用されること | 重要情報の表示や操作に暗号化が強制されていない | 9.1.1 | リクエスト | 重要情報表示 | https://api-vuln.vams.jp | GET | /api/user | A01_ログインユーザー情報取得 |
| 80 | DC01 | データ | クライアントサイドのデータ保護 | アンチキャッシングヘッダが設定され機微データがキャッシュされないこと | 重要情報の取得でキャッシュが無効化されていない | 8.2.1 | リクエスト | 重要情報表示 | https://api-vuln.vams.jp | GET | /api/user | A01_ログインユーザー情報取得 |
| 81 | AG04 | アクセス制御 | 一般的なアクセス制御の設計 | アクセス制御が信頼できるサービスレイヤーで強制されること | 認証の必要な機能にアクセスできる | 4.1.1<br>4.1.3<br>4.2.1<br>14.5.2 | リクエスト | !ゲストページ | https://api-vuln.vams.jp | GET | /api/user | A01_ログインユーザー情報取得 |
| 82 | VO14 | 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 | SQLインジェクションの影響を受けにくいこと | SQLインジェクションの影響を受ける可能性がある | 5.3.4 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/user | A01_ログインユーザー情報取得 |
| 83 | VO14 | 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 | SQLインジェクションの影響を受けにくいこと | SQLインジェクションの影響を受ける可能性がある | 5.3.4 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/user | A01_ログインユーザー情報取得 |
| 84 | VO16 | 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 | NoSQLインジェクションの影響を受けにくいこと | NoSQLインジェクションの影響を受ける可能性がある | 5.3.4 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/user | A01_ログインユーザー情報取得 |
| 85 | VO16 | 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 | NoSQLインジェクションの影響を受けにくいこと | NoSQLインジェクションの影響を受ける可能性がある | 5.3.4 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/user | A01_ログインユーザー情報取得 |
| 86 | VO20 | 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 | OSコマンドインジェクションの影響を受けにくいこと | OSコマンドインジェクションの影響を受ける可能性がある | 5.3.8<br>12.3.5 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/user | A01_ログインユーザー情報取得 |
| 87 | VO20 | 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 | OSコマンドインジェクションの影響を受けにくいこと | OSコマンドインジェクションの影響を受ける可能性がある | 5.3.8<br>12.3.5 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/user | A01_ログインユーザー情報取得 |

| ケースNo | 観点No | 観点分類 | 検査観点 | 検査基準 | 脆弱性 | ASVS | 検査粒度 | 検査対象 | ホスト | メソッド | URL | 画面 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 88 | VO20 | 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 | OSコマンドインジェクションの影響を受けにくいこと | OSコマンドインジェクションの影響を受ける可能性がある | 5.3.8<br>12.3.5 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/user | A01_ログインユーザー情報取得 |
| 89 | VO20 | 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 | OSコマンドインジェクションの影響を受けにくいこと | OSコマンドインジェクションの影響を受ける可能性がある | 5.3.8<br>12.3.5 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/user | A01_ログインユーザー情報取得 |
| 90 | FX02 | ファイル | ファイルの実行要件 | パストラバーサルやローカルファイルインクルードの影響を受けにくいこと | ユーザ由来のファイル名を十分な安全確認無しに利用している | 12.3.1<br>5.3.9 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/user | A01_ログインユーザー情報取得 |
| 91 | VO29 | 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 | HTTPヘッダインジェクションの影響を受けにくいこと | HTTPヘッダインジェクションの影響を受ける可能性がある | 5.3.5 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/user | A01_ログインユーザー情報取得 |
| 92 | VO18 | 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 | LDAPインジェクションの影響を受けにくいこと | LDAPインジェクションの影響を受ける可能性がある | 5.3.7<br>5.1.3 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/user | A01_ログインユーザー情報取得 |
| 93 | VO18 | 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 | LDAPインジェクションの影響を受けにくいこと | LDAPインジェクションの影響を受ける可能性がある | 5.3.7<br>5.1.3 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/user | A01_ログインユーザー情報取得 |
| 94 | VO18 | 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 | LDAPインジェクションの影響を受けにくいこと | LDAPインジェクションの影響を受ける可能性がある | 5.3.7<br>5.1.3 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/user | A01_ログインユーザー情報取得 |
| 95 | VO22 | 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 | XMLインジェクションの影響を受けにくいこと | XMLインジェクション攻撃の影響を受ける可能性がある | 5.3.10 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/user | A01_ログインユーザー情報取得 |
| 96 | VO22 | 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 | XMLインジェクションの影響を受けにくいこと | XMLインジェクション攻撃の影響を受ける可能性がある | 5.3.10 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/user | A01_ログインユーザー情報取得 |
| 97 | VO22 | 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 | XMLインジェクションの影響を受けにくいこと | XMLインジェクション攻撃の影響を受ける可能性がある | 5.3.10 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/user | A01_ログインユーザー情報取得 |
| 98 | VO24 | 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 | XPathインジェクションの影響を受けにくいこと | Xpathインジェクション攻撃の影響を受ける可能性がある | 5.3.10<br>5.1.3 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/user | A01_ログインユーザー情報取得 |
| 99 | VO24 | 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 | XPathインジェクションの影響を受けにくいこと | Xpathインジェクション攻撃の影響を受ける可能性がある | 5.3.10<br>5.1.3 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/user | A01_ログインユーザー情報取得 |
| 100 | VO05 | 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 | 出力の適切なエスケープにより反射型XSSの影響を受けにくいこと | ※このケースでは起票しない | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/user | A01_ログインユーザー情報取得 |
| 101 | VO05 | 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 | 出力の適切なエスケープにより反射型XSSの影響を受けにくいこと | ※このケースでは起票しない | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/user | A01_ログインユーザー情報取得 |
| 102 | VO05 | 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 | 出力の適切なエスケープにより反射型XSSの影響を受けにくいこと | ※このケースでは起票しない | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/user | A01_ログインユーザー情報取得 |
| 103 | VO05 | 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 | 出力の適切なエスケープにより反射型XSSの影響を受けにくいこと | ※このケースでは起票しない | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/user | A01_ログインユーザー情報取得 |
| 104 | VO05 | 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 | 出力の適切なエスケープにより反射型XSSの影響を受けにくいこと | ※このケースでは起票しない | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/user | A01_ログインユーザー情報取得 |
| 105 | VO05 | 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 | 出力の適切なエスケープにより反射型XSSの影響を受けにくいこと | ※このケースでは起票しない | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/user | A01_ログインユーザー情報取得 |
| 106 | VO05 | 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 | 出力の適切なエスケープにより反射型XSSの影響を受けにくいこと | ※このケースでは起票しない | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/user | A01_ログインユーザー情報取得 |
| 107 | VO05 | 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 | 出力の適切なエスケープにより反射型XSSの影響を受けにくいこと | ※このケースでは起票しない | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/user | A01_ログインユーザー情報取得 |
| 108 | VO05 | 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 | 出力の適切なエスケープにより反射型XSSの影響を受けにくいこと | ※このケースでは起票しない | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/user | A01_ログインユーザー情報取得 |
| 109 | VO05 | 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 | 出力の適切なエスケープにより反射型XSSの影響を受けにくいこと | ※このケースでは起票しない | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/user | A01_ログインユーザー情報取得 |
| 110 | VO07 | 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 | 出力の適切なエスケープにより反射型XSSの影響を受けにくいこと | XSS（反射型）の影響を受ける可能性がある | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/user | A01_ログインユーザー情報取得 |
| 111 | VO08 | 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 | 出力の適切なエスケープにより保存型XSSの影響を受けにくいこと | XSS（保存型）の影響を受ける可能性がある | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/user | A01_ログインユーザー情報取得 |
| 112 | VO34 | 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 | 出力の適切なエスケープによりDOMベースXSSの影響を受けにくいこと | XSS（DOM型）の影響を受ける可能性がある | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1<br>5.3.6<br>5.5.4 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/user | A01_ログインユーザー情報取得 |
| 113 | ZZ02 | – | – | – | – | | リクエスト | !Intruderのみ実施 | https://api-vuln.vams.jp | PUT | /api/user | A02_ログインユーザー情報更新 |
| 114 | ZZ07 | – | – | – | – | | リクエスト | !Intruderのみ実施 | https://api-vuln.vams.jp | PUT | /api/user | A02_ログインユーザー情報更新 |
| 115 | DC02 | データ | クライアントサイドのデータ保護 | クライアントストレージに機微情報や個人情報を保持しないこと | 重要情報がクライアントストレージに格納される | 8.2.2 | リクエスト | 重要情報入力 | https://api-vuln.vams.jp | PUT | /api/user | A02_ログインユーザー情報更新 |
| 116 | XG05 | 通信 | 通信のセキュリティ要件 | TLSがクライアント接続に使用されること | 重要情報の表示や操作に暗号化が強制されていない | 9.1.1 | リクエスト | 重要情報表示 | https://api-vuln.vams.jp | PUT | /api/user | A02_ログインユーザー情報更新 |

| ケースNo | 観点No | 観点分類 | 検査観点 | 検査基準 | 脆弱性 | ASVS | 検査粒度 | 検査対象 | ホスト | メソッド | URL | 画面 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 117 | XS06 | 通信 | 通信のセキュリティ要件 | TLSがクライアント接続に使用されること | 重要情報の表示や操作に暗号化が強制されていない | 9.1.1 | リクエスト | 重要情報入力 | https://api-vuln.vams.jp | PUT | /api/user | A02_ログインユーザー情報更新 |
| 118 | DC01 | データ | クライアントサイドのデータ保護 | アンチキャッシングヘッダが設定され機微データがキャッシュされないこと | 重要情報の取得でキャッシュが無効化されていない | 8.2.1 | リクエスト | 重要情報表示 | https://api-vuln.vams.jp | PUT | /api/user | A02_ログインユーザー情報更新 |
| 119 | AG04 | アクセス制御 | 一般的なアクセス制御の設計 | アクセス制御が信頼できるサービスレイヤーで強制されること | 認証の必要な機能にアクセスできる | 4.1.1<br>4.1.3<br>4.2.1<br>14.5.2 | リクエスト | !ゲストページ | https://api-vuln.vams.jp | PUT | /api/user | A02_ログインユーザー情報更新 |
| 120 | VO31 | 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 | SQLインジェクションの影響を受けにくいこと | – | 5.3.4 | リクエスト | フォーム入力 | https://api-vuln.vams.jp | PUT | /api/user | A02_ログインユーザー情報更新 |
| 121 | VO32 | 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 | 出力の適切なエスケープにより保存型XSSの影響を受けにくいこと | – | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1 | リクエスト | フォーム入力 | https://api-vuln.vams.jp | PUT | /api/user | A02_ログインユーザー情報更新 |
| 122 | VO14 | 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 | SQLインジェクションの影響を受けにくいこと | SQLインジェクションの影響を受ける可能性がある | 5.3.4 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | PUT | /api/user | A02_ログインユーザー情報更新 |
| 123 | VO14 | 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 | SQLインジェクションの影響を受けにくいこと | SQLインジェクションの影響を受ける可能性がある | 5.3.4 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | PUT | /api/user | A02_ログインユーザー情報更新 |
| 124 | VO16 | 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 | NoSQLインジェクションの影響を受けにくいこと | NoSQLインジェクションの影響を受ける可能性がある | 5.3.4 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | PUT | /api/user | A02_ログインユーザー情報更新 |
| 125 | VO16 | 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 | NoSQLインジェクションの影響を受けにくいこと | NoSQLインジェクションの影響を受ける可能性がある | 5.3.4 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | PUT | /api/user | A02_ログインユーザー情報更新 |
| 126 | VO20 | 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 | OSコマンドインジェクションの影響を受けにくいこと | OSコマンドインジェクションの影響を受ける可能性がある | 5.3.8<br>12.3.5 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | PUT | /api/user | A02_ログインユーザー情報更新 |
| 127 | VO20 | 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 | OSコマンドインジェクションの影響を受けにくいこと | OSコマンドインジェクションの影響を受ける可能性がある | 5.3.8<br>12.3.5 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | PUT | /api/user | A02_ログインユーザー情報更新 |
| 128 | VO20 | 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 | OSコマンドインジェクションの影響を受けにくいこと | OSコマンドインジェクションの影響を受ける可能性がある | 5.3.8<br>12.3.5 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | PUT | /api/user | A02_ログインユーザー情報更新 |
| 129 | VO20 | 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 | OSコマンドインジェクションの影響を受けにくいこと | OSコマンドインジェクションの影響を受ける可能性がある | 5.3.8<br>12.3.5 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | PUT | /api/user | A02_ログインユーザー情報更新 |
| 130 | FX02 | ファイル | ファイルの実行要件 | パストラバーサルやローカルファイルインクルードの影響を受けにくいこと | ユーザ由来のファイル名を十分な安全確認無しに利用している | 12.3.1<br>5.3.9 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | PUT | /api/user | A02_ログインユーザー情報更新 |
| 131 | VO29 | 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 | HTTPヘッダインジェクションの影響を受けにくいこと | HTTPヘッダインジェクションの影響を受ける可能性がある | 5.3.5 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | PUT | /api/user | A02_ログインユーザー情報更新 |
| 132 | VO18 | 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 | LDAPインジェクションの影響を受けにくいこと | LDAPインジェクションの影響を受ける可能性がある | 5.3.7<br>5.1.3 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | PUT | /api/user | A02_ログインユーザー情報更新 |
| 133 | VO18 | 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 | LDAPインジェクションの影響を受けにくいこと | LDAPインジェクションの影響を受ける可能性がある | 5.3.7<br>5.1.3 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | PUT | /api/user | A02_ログインユーザー情報更新 |
| 134 | VO18 | 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 | LDAPインジェクションの影響を受けにくいこと | LDAPインジェクションの影響を受ける可能性がある | 5.3.7<br>5.1.3 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | PUT | /api/user | A02_ログインユーザー情報更新 |
| 135 | VO22 | 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 | XMLインジェクションの影響を受けにくいこと | XMLインジェクション攻撃の影響を受ける可能性がある | 5.3.10 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | PUT | /api/user | A02_ログインユーザー情報更新 |
| 136 | VO22 | 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 | XMLインジェクションの影響を受けにくいこと | XMLインジェクション攻撃の影響を受ける可能性がある | 5.3.10 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | PUT | /api/user | A02_ログインユーザー情報更新 |
| 137 | VO22 | 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 | XMLインジェクションの影響を受けにくいこと | XMLインジェクション攻撃の影響を受ける可能性がある | 5.3.10 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | PUT | /api/user | A02_ログインユーザー情報更新 |
| 138 | VO24 | 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 | XPathインジェクションの影響を受けにくいこと | Xpathインジェクション攻撃の影響を受ける可能性がある | 5.3.10<br>5.1.3 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | PUT | /api/user | A02_ログインユーザー情報更新 |
| 139 | VO24 | 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 | XPathインジェクションの影響を受けにくいこと | Xpathインジェクション攻撃の影響を受ける可能性がある | 5.3.10<br>5.1.3 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | PUT | /api/user | A02_ログインユーザー情報更新 |
| 140 | VO05 | 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 | 出力の適切なエスケープにより反射型XSSの影響を受けにくいこと | ※このケースでは起票しない | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | PUT | /api/user | A02_ログインユーザー情報更新 |
| 141 | VO05 | 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 | 出力の適切なエスケープにより反射型XSSの影響を受けにくいこと | ※このケースでは起票しない | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | PUT | /api/user | A02_ログインユーザー情報更新 |
| 142 | VO05 | 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 | 出力の適切なエスケープにより反射型XSSの影響を受けにくいこと | ※このケースでは起票しない | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | PUT | /api/user | A02_ログインユーザー情報更新 |
| 143 | VO05 | 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 | 出力の適切なエスケープにより反射型XSSの影響を受けにくいこと | ※このケースでは起票しない | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | PUT | /api/user | A02_ログインユーザー情報更新 |
| 144 | VO05 | 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 | 出力の適切なエスケープにより反射型XSSの影響を受けにくいこと | ※このケースでは起票しない | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | PUT | /api/user | A02_ログインユーザー情報更新 |
| 145 | VO05 | 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 | 出力の適切なエスケープにより反射型XSSの影響を受けにくいこと | ※このケースでは起票しない | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | PUT | /api/user | A02_ログインユーザー情報更新 |

| ケースNo | 観点No | 観点分類 | 検査観点 | 検査基準 | 脆弱性 | ASVS | 検査粒度 | 検査対象 | ホスト | メソッド | URL | 画面 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 146 | VO05 | 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 | 出力の適切なエスケープにより反射型XSSの影響を受けにくいこと | ※このケースでは起票しない | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | PUT | /api/user | A02_ログインユーザー情報更新 |
| 147 | VO05 | 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 | 出力の適切なエスケープにより反射型XSSの影響を受けにくいこと | ※このケースでは起票しない | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | PUT | /api/user | A02_ログインユーザー情報更新 |
| 148 | VO05 | 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 | 出力の適切なエスケープにより反射型XSSの影響を受けにくいこと | ※このケースでは起票しない | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | PUT | /api/user | A02_ログインユーザー情報更新 |
| 149 | VO05 | 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 | 出力の適切なエスケープにより反射型XSSの影響を受けにくいこと | ※このケースでは起票しない | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | PUT | /api/user | A02_ログインユーザー情報更新 |
| 150 | VO07 | 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 | 出力の適切なエスケープにより反射型XSSの影響を受けにくいこと | XSS（反射型）の影響を受ける可能性がある | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | PUT | /api/user | A02_ログインユーザー情報更新 |
| 151 | VO08 | 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 | 出力の適切なエスケープにより保存型XSSの影響を受けにくいこと | XSS（保存型）の影響を受ける可能性がある | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | PUT | /api/user | A02_ログインユーザー情報更新 |
| 152 | VO34 | 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 | 出力の適切なエスケープによりDOMベースXSSの影響を受けにくいこと | XSS（DOM型）の影響を受ける可能性がある | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1<br>5.3.6<br>5.5.4 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | PUT | /api/user | A02_ログインユーザー情報更新 |
| 153 | ZZ02 | – | – | – | – |  | リクエスト | !Intruderのみ実施 | https://api-vuln.vams.jp | GET | /api/issues/25133/history | B01_脆弱性履歴情報取得 |
| 154 | ZZ07 | – | – | – | – |  | リクエスト | !Intruderのみ実施 | https://api-vuln.vams.jp | GET | /api/issues/25133/history | B01_脆弱性履歴情報取得 |
| 155 | ZZ05 | – | – | – | – |  | リクエスト | URLScan | https://api-vuln.vams.jp | GET | /api/issues/25133/history | B01_脆弱性履歴情報取得 |
| 156 | XG05 | 通信 | 通信のセキュリティ要件 | TLSがクライアント接続に使用されること | 重要情報の表示や操作に暗号化が強制されていない | 9.1.1 | リクエスト | 重要情報表示 | https://api-vuln.vams.jp | GET | /api/issues/25133/history | B01_脆弱性履歴情報取得 |
| 157 | DC01 | データ | クライアントサイドのデータ保護 | アンチキャッシングヘッダが設定され機微データがキャッシュされないこと | 重要情報の取得でキャッシュが無効化されていない | 8.2.1 | リクエスト | 重要情報表示 | https://api-vuln.vams.jp | GET | /api/issues/25133/history | B01_脆弱性履歴情報取得 |
| 158 | AG04 | アクセス制御 | 一般的なアクセス制御の設計 | アクセス制御が信頼できるサービスレイヤーで強制されること | 認証の必要な機能にアクセスできる | 4.1.1<br>4.1.3<br>4.2.1<br>14.5.2 | リクエスト | !ゲストページ | https://api-vuln.vams.jp | GET | /api/issues/25133/history | B01_脆弱性履歴情報取得 |
| 159 | AG03 | アクセス制御 | 一般的なアクセス制御の設計 | データがオブジェクトの直接参照に対して保護されていること | 権限のないリソースにアクセスできる | 4.1.1<br>4.1.3<br>4.1.5<br>4.2.1 | リクエスト | !リソースID無し | https://api-vuln.vams.jp | GET | /api/issues/25133/history | B01_脆弱性履歴情報取得 |
| 160 | AG03e | アクセス制御 | 一般的なアクセス制御の設計 | データがオブジェクトの直接参照に対して保護されていること | – | 4.1.1<br>4.1.3<br>4.1.5<br>4.2.1 | リクエスト | !リソースID無し | https://api-vuln.vams.jp | GET | /api/issues/25133/history | B01_脆弱性履歴情報取得 |
| 161 | VO14 | 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 | SQLインジェクションの影響を受けにくいこと | SQLインジェクションの影響を受ける可能性がある | 5.3.4 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/issues/25133/history | B01_脆弱性履歴情報取得 |
| 162 | VO14 | 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 | SQLインジェクションの影響を受けにくいこと | SQLインジェクションの影響を受ける可能性がある | 5.3.4 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/issues/25133/history | B01_脆弱性履歴情報取得 |
| 163 | VO16 | 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 | NoSQLインジェクションの影響を受けにくいこと | NoSQLインジェクションの影響を受ける可能性がある | 5.3.4 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/issues/25133/history | B01_脆弱性履歴情報取得 |
| 164 | VO16 | 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 | NoSQLインジェクションの影響を受けにくいこと | NoSQLインジェクションの影響を受ける可能性がある | 5.3.4 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/issues/25133/history | B01_脆弱性履歴情報取得 |
| 165 | VO20 | 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 | OSコマンドインジェクションの影響を受けにくいこと | OSコマンドインジェクションの影響を受ける可能性がある | 5.3.8<br>12.3.5 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/issues/25133/history | B01_脆弱性履歴情報取得 |
| 166 | VO20 | 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 | OSコマンドインジェクションの影響を受けにくいこと | OSコマンドインジェクションの影響を受ける可能性がある | 5.3.8<br>12.3.5 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/issues/25133/history | B01_脆弱性履歴情報取得 |
| 167 | VO20 | 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 | OSコマンドインジェクションの影響を受けにくいこと | OSコマンドインジェクションの影響を受ける可能性がある | 5.3.8<br>12.3.5 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/issues/25133/history | B01_脆弱性履歴情報取得 |
| 168 | VO20 | 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 | OSコマンドインジェクションの影響を受けにくいこと | OSコマンドインジェクションの影響を受ける可能性がある | 5.3.8<br>12.3.5 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/issues/25133/history | B01_脆弱性履歴情報取得 |
| 169 | FX02 | ファイル | ファイルの実行要件 | パストラバーサルやローカルファイルインクルードの影響を受けにくいこと | ユーザ由来のファイル名を十分な安全確認無しに利用している | 12.3.1<br>5.3.9 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/issues/25133/history | B01_脆弱性履歴情報取得 |
| 170 | VO29 | 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 | HTTPヘッダインジェクションの影響を受けにくいこと | HTTPヘッダインジェクションの影響を受ける可能性がある | 5.3.5 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/issues/25133/history | B01_脆弱性履歴情報取得 |
| 171 | VO18 | 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 | LDAPインジェクションの影響を受けにくいこと | LDAPインジェクションの影響を受ける可能性がある | 5.3.7<br>5.1.3 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/issues/25133/history | B01_脆弱性履歴情報取得 |
| 172 | VO18 | 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 | LDAPインジェクションの影響を受けにくいこと | LDAPインジェクションの影響を受ける可能性がある | 5.3.7<br>5.1.3 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/issues/25133/history | B01_脆弱性履歴情報取得 |
| 173 | VO18 | 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 | LDAPインジェクションの影響を受けにくいこと | LDAPインジェクションの影響を受ける可能性がある | 5.3.7<br>5.1.3 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/issues/25133/history | B01_脆弱性履歴情報取得 |
| 174 | VO22 | 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 | XMLインジェクションの影響を受けにくいこと | XMLインジェクション攻撃の影響を受ける可能性がある | 5.3.10 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/issues/25133/history | B01_脆弱性履歴情報取得 |

| ケースNo | 観点No | 観点分類 | 検査観点 | 検査基準 | 脆弱性 | ASVS | 検査粒度 | 検査対象 | ホスト | メソッド | URL | 画面 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 175 | VO22 | 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 | XMLインジェクションの影響を受けにくいこと | XMLインジェクション攻撃の影響を受ける可能性がある | 5.3.10 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/issues/25133/history | B01_脆弱性履歴情報取得 |
| 176 | VO22 | 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 | XMLインジェクションの影響を受けにくいこと | XMLインジェクション攻撃の影響を受ける可能性がある | 5.3.10 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/issues/25133/history | B01_脆弱性履歴情報取得 |
| 177 | VO24 | 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 | XPathインジェクションの影響を受けにくいこと | Xpathインジェクション攻撃の影響を受ける可能性がある | 5.3.10<br>5.1.3 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/issues/25133/history | B01_脆弱性履歴情報取得 |
| 178 | VO24 | 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 | XPathインジェクションの影響を受けにくいこと | Xpathインジェクション攻撃の影響を受ける可能性がある | 5.3.10<br>5.1.3 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/issues/25133/history | B01_脆弱性履歴情報取得 |
| 179 | VO05 | 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 | 出力の適切なエスケープにより反射型XSSの影響を受けにくいこと | ※このケースでは起票しない | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/issues/25133/history | B01_脆弱性履歴情報取得 |
| 180 | VO05 | 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 | 出力の適切なエスケープにより反射型XSSの影響を受けにくいこと | ※このケースでは起票しない | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/issues/25133/history | B01_脆弱性履歴情報取得 |
| 181 | VO05 | 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 | 出力の適切なエスケープにより反射型XSSの影響を受けにくいこと | ※このケースでは起票しない | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/issues/25133/history | B01_脆弱性履歴情報取得 |
| 182 | VO05 | 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 | 出力の適切なエスケープにより反射型XSSの影響を受けにくいこと | ※このケースでは起票しない | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/issues/25133/history | B01_脆弱性履歴情報取得 |
| 183 | VO05 | 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 | 出力の適切なエスケープにより反射型XSSの影響を受けにくいこと | ※このケースでは起票しない | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/issues/25133/history | B01_脆弱性履歴情報取得 |
| 184 | VO05 | 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 | 出力の適切なエスケープにより反射型XSSの影響を受けにくいこと | ※このケースでは起票しない | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/issues/25133/history | B01_脆弱性履歴情報取得 |
| 185 | VO05 | 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 | 出力の適切なエスケープにより反射型XSSの影響を受けにくいこと | ※このケースでは起票しない | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/issues/25133/history | B01_脆弱性履歴情報取得 |
| 186 | VO05 | 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 | 出力の適切なエスケープにより反射型XSSの影響を受けにくいこと | ※このケースでは起票しない | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/issues/25133/history | B01_脆弱性履歴情報取得 |
| 187 | VO05 | 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 | 出力の適切なエスケープにより反射型XSSの影響を受けにくいこと | ※このケースでは起票しない | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/issues/25133/history | B01_脆弱性履歴情報取得 |
| 188 | VO05 | 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 | 出力の適切なエスケープにより反射型XSSの影響を受けにくいこと | ※このケースでは起票しない | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/issues/25133/history | B01_脆弱性履歴情報取得 |
| 189 | VO07 | 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 | 出力の適切なエスケープにより反射型XSSの影響を受けにくいこと | XSS（反射型）の影響を受ける可能性がある | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/issues/25133/history | B01_脆弱性履歴情報取得 |
| 190 | VO08 | 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 | 出力の適切なエスケープにより保存型XSSの影響を受けにくいこと | XSS（保存型）の影響を受ける可能性がある | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/issues/25133/history | B01_脆弱性履歴情報取得 |
| 191 | VO34 | 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 | 出力の適切なエスケープによりDOMベースXSSの影響を受けにくいこと | XSS（DOM型）の影響を受ける可能性がある | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1<br>5.3.6<br>5.5.4 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/issues/25133/history | B01_脆弱性履歴情報取得 |
| 192 | ZZ02 | – | – | – | – | | リクエスト | !Intruderのみ実施 | https://api-vuln.vams.jp | GET | /api/issues | B02_脆弱性一覧情報取得 |
| 193 | ZZ07 | – | – | – | – | | リクエスト | !Intruderのみ実施 | https://api-vuln.vams.jp | GET | /api/issues | B02_脆弱性一覧情報取得 |
| 194 | AG04 | アクセス制御 | 一般的なアクセス制御の設計 | アクセス制御が信頼できるサービスレイヤーで強制されること | 認証の必要な機能にアクセスできる | 4.1.1<br>4.1.3<br>4.2.1<br>14.5.2 | リクエスト | !ゲストページ | https://api-vuln.vams.jp | GET | /api/issues | B02_脆弱性一覧情報取得 |
| 195 | VO14 | 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 | SQLインジェクションの影響を受けにくいこと | SQLインジェクションの影響を受ける可能性がある | 5.3.4 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/issues | B02_脆弱性一覧情報取得 |
| 196 | VO14 | 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 | SQLインジェクションの影響を受けにくいこと | SQLインジェクションの影響を受ける可能性がある | 5.3.4 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/issues | B02_脆弱性一覧情報取得 |
| 197 | VO16 | 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 | NoSQLインジェクションの影響を受けにくいこと | NoSQLインジェクションの影響を受ける可能性がある | 5.3.4 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/issues | B02_脆弱性一覧情報取得 |
| 198 | VO16 | 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 | NoSQLインジェクションの影響を受けにくいこと | NoSQLインジェクションの影響を受ける可能性がある | 5.3.4 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/issues | B02_脆弱性一覧情報取得 |
| 199 | VO20 | 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 | OSコマンドインジェクションの影響を受けにくいこと | OSコマンドインジェクションの影響を受ける可能性がある | 5.3.8<br>12.3.5 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/issues | B02_脆弱性一覧情報取得 |
| 200 | VO20 | 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 | OSコマンドインジェクションの影響を受けにくいこと | OSコマンドインジェクションの影響を受ける可能性がある | 5.3.8<br>12.3.5 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/issues | B02_脆弱性一覧情報取得 |
| 201 | VO20 | 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 | OSコマンドインジェクションの影響を受けにくいこと | OSコマンドインジェクションの影響を受ける可能性がある | 5.3.8<br>12.3.5 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/issues | B02_脆弱性一覧情報取得 |
| 202 | VO20 | 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 | OSコマンドインジェクションの影響を受けにくいこと | OSコマンドインジェクションの影響を受ける可能性がある | 5.3.8<br>12.3.5 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/issues | B02_脆弱性一覧情報取得 |
| 203 | FX02 | ファイル | ファイルの実行要件 | パストラバーサルやローカルファイルインクルードの影響を受けにくいこと | ユーザ由来のファイル名を十分な安全確認無しに利用している | 12.3.1<br>5.3.9 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/issues | B02_脆弱性一覧情報取得 |

| ケースNo | 観点No | 観点分類 | 検査観点 | 検査基準 | 脆弱性 | ASVS | 検査粒度 | 検査対象 | ホスト | メソッド | URL | 画面 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 204 | VO29 | 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 | HTTPヘッダインジェクションの影響を受けにくいこと | HTTPヘッダインジェクションの影響を受ける可能性がある | 5.3.5 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/issues | B02_脆弱性一覧情報取得 |
| 205 | VO18 | 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 | LDAPインジェクションの影響を受けにくいこと | LDAPインジェクションの影響を受ける可能性がある | 5.3.7<br>5.1.3 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/issues | B02_脆弱性一覧情報取得 |
| 206 | VO18 | 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 | LDAPインジェクションの影響を受けにくいこと | LDAPインジェクションの影響を受ける可能性がある | 5.3.7<br>5.1.3 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/issues | B02_脆弱性一覧情報取得 |
| 207 | VO18 | 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 | LDAPインジェクションの影響を受けにくいこと | LDAPインジェクションの影響を受ける可能性がある | 5.3.7<br>5.1.3 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/issues | B02_脆弱性一覧情報取得 |
| 208 | VO22 | 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 | XMLインジェクションの影響を受けにくいこと | XMLインジェクション攻撃の影響を受ける可能性がある | 5.3.10 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/issues | B02_脆弱性一覧情報取得 |
| 209 | VO22 | 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 | XMLインジェクションの影響を受けにくいこと | XMLインジェクション攻撃の影響を受ける可能性がある | 5.3.10 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/issues | B02_脆弱性一覧情報取得 |
| 210 | VO22 | 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 | XMLインジェクションの影響を受けにくいこと | XMLインジェクション攻撃の影響を受ける可能性がある | 5.3.10 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/issues | B02_脆弱性一覧情報取得 |
| 211 | VO24 | 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 | XPathインジェクションの影響を受けにくいこと | Xpathインジェクション攻撃の影響を受ける可能性がある | 5.3.10<br>5.1.3 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/issues | B02_脆弱性一覧情報取得 |
| 212 | VO24 | 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 | XPathインジェクションの影響を受けにくいこと | Xpathインジェクション攻撃の影響を受ける可能性がある | 5.3.10<br>5.1.3 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/issues | B02_脆弱性一覧情報取得 |
| 213 | VO05 | 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 | 出力の適切なエスケープにより反射型XSSの影響を受けにくいこと | ※このケースでは起票しない | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/issues | B02_脆弱性一覧情報取得 |
| 214 | VO05 | 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 | 出力の適切なエスケープにより反射型XSSの影響を受けにくいこと | ※このケースでは起票しない | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/issues | B02_脆弱性一覧情報取得 |
| 215 | VO05 | 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 | 出力の適切なエスケープにより反射型XSSの影響を受けにくいこと | ※このケースでは起票しない | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/issues | B02_脆弱性一覧情報取得 |
| 216 | VO05 | 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 | 出力の適切なエスケープにより反射型XSSの影響を受けにくいこと | ※このケースでは起票しない | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/issues | B02_脆弱性一覧情報取得 |
| 217 | VO05 | 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 | 出力の適切なエスケープにより反射型XSSの影響を受けにくいこと | ※このケースでは起票しない | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/issues | B02_脆弱性一覧情報取得 |
| 218 | VO05 | 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 | 出力の適切なエスケープにより反射型XSSの影響を受けにくいこと | ※このケースでは起票しない | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/issues | B02_脆弱性一覧情報取得 |
| 219 | VO05 | 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 | 出力の適切なエスケープにより反射型XSSの影響を受けにくいこと | ※このケースでは起票しない | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/issues | B02_脆弱性一覧情報取得 |
| 220 | VO05 | 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 | 出力の適切なエスケープにより反射型XSSの影響を受けにくいこと | ※このケースでは起票しない | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/issues | B02_脆弱性一覧情報取得 |
| 221 | VO05 | 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 | 出力の適切なエスケープにより反射型XSSの影響を受けにくいこと | ※このケースでは起票しない | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/issues | B02_脆弱性一覧情報取得 |
| 222 | VO05 | 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 | 出力の適切なエスケープにより反射型XSSの影響を受けにくいこと | ※このケースでは起票しない | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/issues | B02_脆弱性一覧情報取得 |
| 223 | VO07 | 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 | 出力の適切なエスケープにより反射型XSSの影響を受けにくいこと | XSS（反射型）の影響を受ける可能性がある | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/issues | B02_脆弱性一覧情報取得 |
| 224 | VO08 | 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 | 出力の適切なエスケープにより保存型XSSの影響を受けにくいこと | XSS（保存型）の影響を受ける可能性がある | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/issues | B02_脆弱性一覧情報取得 |
| 225 | VO34 | 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 | 出力の適切なエスケープによりDOMベースXSSの影響を受けにくいこと | XSS（DOM型）の影響を受ける可能性がある | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1<br>5.3.6<br>5.5.4 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/issues | B02_脆弱性一覧情報取得 |
| 226 | ZZ02 | – | – | – | – | | リクエスト | !Intruderのみ実施 | https://api-vuln.vams.jp | GET | /api/issues/25133 | B03_脆弱性情報参照 |
| 227 | ZZ07 | – | – | – | – | | リクエスト | !Intruderのみ実施 | https://api-vuln.vams.jp | GET | /api/issues/25133 | B03_脆弱性情報参照 |
| 228 | ZZ05 | – | – | – | – | | リクエスト | URLScan | https://api-vuln.vams.jp | GET | /api/issues/25133 | B03_脆弱性情報参照 |
| 229 | AG04 | アクセス制御 | 一般的なアクセス制御の設計 | アクセス制御が信頼できるサービスレイヤーで強制されること | 認証の必要な機能にアクセスできる | 4.1.1<br>4.1.3<br>4.2.1<br>14.5.2 | リクエスト | !ゲストページ | https://api-vuln.vams.jp | GET | /api/issues/25133 | B03_脆弱性情報参照 |
| 230 | AG03 | アクセス制御 | 一般的なアクセス制御の設計 | データがオブジェクトの直接参照に対して保護されていること | 権限のないリソースにアクセスできる | 4.1.1<br>4.1.3<br>4.1.5<br>4.2.1 | リクエスト | !リソースID無し | https://api-vuln.vams.jp | GET | /api/issues/25133 | B03_脆弱性情報参照 |
| 231 | AG03e | アクセス制御 | 一般的なアクセス制御の設計 | データがオブジェクトの直接参照に対して保護されていること | – | 4.1.1<br>4.1.3<br>4.1.5<br>4.2.1 | リクエスト | !リソースID無し | https://api-vuln.vams.jp | GET | /api/issues/25133 | B03_脆弱性情報参照 |
| 232 | VO14 | 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 | SQLインジェクションの影響を受けにくいこと | SQLインジェクションの影響を受ける可能性がある | 5.3.4 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/issues/25133 | B03_脆弱性情報参照 |

| ケースNo | 観点No | 観点分類 | 検査観点 | 検査基準 | 脆弱性 | ASVS | 検査粒度 | 検査対象 | ホスト | メソッド | URL | 画面 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 233 | VO14 | 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 | SQLインジェクションの影響を受けにくいこと | SQLインジェクションの影響を受ける可能性がある | 5.3.4 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/issues/25133 | B03_脆弱性情報参照 |
| 234 | VO16 | 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 | NoSQLインジェクションの影響を受けにくいこと | NoSQLインジェクションの影響を受ける可能性がある | 5.3.4 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/issues/25133 | B03_脆弱性情報参照 |
| 235 | VO16 | 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 | NoSQLインジェクションの影響を受けにくいこと | NoSQLインジェクションの影響を受ける可能性がある | 5.3.4 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/issues/25133 | B03_脆弱性情報参照 |
| 236 | VO20 | 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 | OSコマンドインジェクションの影響を受けにくいこと | OSコマンドインジェクションの影響を受ける可能性がある | 5.3.8<br>12.3.5 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/issues/25133 | B03_脆弱性情報参照 |
| 237 | VO20 | 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 | OSコマンドインジェクションの影響を受けにくいこと | OSコマンドインジェクションの影響を受ける可能性がある | 5.3.8<br>12.3.5 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/issues/25133 | B03_脆弱性情報参照 |
| 238 | VO20 | 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 | OSコマンドインジェクションの影響を受けにくいこと | OSコマンドインジェクションの影響を受ける可能性がある | 5.3.8<br>12.3.5 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/issues/25133 | B03_脆弱性情報参照 |
| 239 | VO20 | 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 | OSコマンドインジェクションの影響を受けにくいこと | OSコマンドインジェクションの影響を受ける可能性がある | 5.3.8<br>12.3.5 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/issues/25133 | B03_脆弱性情報参照 |
| 240 | FX02 | ファイル | ファイルの実行要件 | パストラバーサルやローカルファイルインクルードの影響を受けにくいこと | ユーザ由来のファイル名を十分な安全確認無しに利用している | 12.3.1<br>5.3.9 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/issues/25133 | B03_脆弱性情報参照 |
| 241 | VO29 | 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 | HTTPヘッダインジェクションの影響を受けにくいこと | HTTPヘッダインジェクションの影響を受ける可能性がある | 5.3.5 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/issues/25133 | B03_脆弱性情報参照 |
| 242 | VO18 | 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 | LDAPインジェクションの影響を受けにくいこと | LDAPインジェクションの影響を受ける可能性がある | 5.3.7<br>5.1.3 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/issues/25133 | B03_脆弱性情報参照 |
| 243 | VO18 | 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 | LDAPインジェクションの影響を受けにくいこと | LDAPインジェクションの影響を受ける可能性がある | 5.3.7<br>5.1.3 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/issues/25133 | B03_脆弱性情報参照 |
| 244 | VO18 | 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 | LDAPインジェクションの影響を受けにくいこと | LDAPインジェクションの影響を受ける可能性がある | 5.3.7<br>5.1.3 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/issues/25133 | B03_脆弱性情報参照 |
| 245 | VO22 | 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 | XMLインジェクションの影響を受けにくいこと | XMLインジェクション攻撃の影響を受ける可能性がある | 5.3.10 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/issues/25133 | B03_脆弱性情報参照 |
| 246 | VO22 | 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 | XMLインジェクションの影響を受けにくいこと | XMLインジェクション攻撃の影響を受ける可能性がある | 5.3.10 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/issues/25133 | B03_脆弱性情報参照 |
| 247 | VO22 | 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 | XMLインジェクションの影響を受けにくいこと | XMLインジェクション攻撃の影響を受ける可能性がある | 5.3.10 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/issues/25133 | B03_脆弱性情報参照 |
| 248 | VO24 | 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 | XPathインジェクションの影響を受けにくいこと | Xpathインジェクション攻撃の影響を受ける可能性がある | 5.3.10<br>5.1.3 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/issues/25133 | B03_脆弱性情報参照 |
| 249 | VO24 | 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 | XPathインジェクションの影響を受けにくいこと | Xpathインジェクション攻撃の影響を受ける可能性がある | 5.3.10<br>5.1.3 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/issues/25133 | B03_脆弱性情報参照 |
| 250 | VO05 | 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 | 出力の適切なエスケープにより反射型XSSの影響を受けにくいこと | ※このケースでは起票しない | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/issues/25133 | B03_脆弱性情報参照 |
| 251 | VO05 | 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 | 出力の適切なエスケープにより反射型XSSの影響を受けにくいこと | ※このケースでは起票しない | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/issues/25133 | B03_脆弱性情報参照 |
| 252 | VO05 | 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 | 出力の適切なエスケープにより反射型XSSの影響を受けにくいこと | ※このケースでは起票しない | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/issues/25133 | B03_脆弱性情報参照 |
| 253 | VO05 | 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 | 出力の適切なエスケープにより反射型XSSの影響を受けにくいこと | ※このケースでは起票しない | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/issues/25133 | B03_脆弱性情報参照 |
| 254 | VO05 | 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 | 出力の適切なエスケープにより反射型XSSの影響を受けにくいこと | ※このケースでは起票しない | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/issues/25133 | B03_脆弱性情報参照 |
| 255 | VO05 | 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 | 出力の適切なエスケープにより反射型XSSの影響を受けにくいこと | ※このケースでは起票しない | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/issues/25133 | B03_脆弱性情報参照 |
| 256 | VO05 | 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 | 出力の適切なエスケープにより反射型XSSの影響を受けにくいこと | ※このケースでは起票しない | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/issues/25133 | B03_脆弱性情報参照 |
| 257 | VO05 | 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 | 出力の適切なエスケープにより反射型XSSの影響を受けにくいこと | ※このケースでは起票しない | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/issues/25133 | B03_脆弱性情報参照 |
| 258 | VO05 | 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 | 出力の適切なエスケープにより反射型XSSの影響を受けにくいこと | ※このケースでは起票しない | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/issues/25133 | B03_脆弱性情報参照 |
| 259 | VO05 | 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 | 出力の適切なエスケープにより反射型XSSの影響を受けにくいこと | ※このケースでは起票しない | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/issues/25133 | B03_脆弱性情報参照 |
| 260 | VO07 | 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 | 出力の適切なエスケープにより反射型XSSの影響を受けにくいこと | XSS(反射型)の影響を受ける可能性がある | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/issues/25133 | B03_脆弱性情報参照 |
| 261 | VO08 | 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 | 出力の適切なエスケープにより保存型XSSの影響を受けにくいこと | XSS(保存型)の影響を受ける可能性がある | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/issues/25133 | B03_脆弱性情報参照 |

| ケースNo | 観点No | 観点分類 | 検査観点 | 検査基準 | 脆弱性 | ASVS | 検査粒度 | 検査対象 | ホスト | メソッド | URL | 画面 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 262 | VO34 | 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 | 出力の適切なエスケープによりDOMベースXSSの影響を受けにくいこと | XSS（DOM型）の影響を受ける可能性がある | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1<br>5.3.6<br>5.5.4 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/issues/25133 | B03_脆弱性情報参照 |
| 263 | ZZ02 | – | – | – | – | | リクエスト | !Intruderのみ実施 | https://api-vuln.vams.jp | GET | /api/login/organization | C01_ログイン組織情報取得 |
| 264 | ZZ07 | – | – | – | – | | リクエスト | !Intruderのみ実施 | https://api-vuln.vams.jp | GET | /api/login/organization | C01_ログイン組織情報取得 |
| 265 | AG06 | アクセス制御 | 一般的なアクセス制御の設計 | ユーザは特定の認可を与えられた機能やリソースのみにアクセスできること | 権限の無いユーザが重要情報を閲覧できる | 4.1.3 | リクエスト | ゲストページ | https://api-vuln.vams.jp | GET | /api/login/organization | C01_ログイン組織情報取得 |
| 266 | VO14 | 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 | SQLインジェクションの影響を受けにくいこと | SQLインジェクションの影響を受ける可能性がある | 5.3.4 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/login/organization | C01_ログイン組織情報取得 |
| 267 | VO14 | 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 | SQLインジェクションの影響を受けにくいこと | SQLインジェクションの影響を受ける可能性がある | 5.3.4 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/login/organization | C01_ログイン組織情報取得 |
| 268 | VO16 | 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 | NoSQLインジェクションの影響を受けにくいこと | NoSQLインジェクションの影響を受ける可能性がある | 5.3.4 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/login/organization | C01_ログイン組織情報取得 |
| 269 | VO16 | 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 | NoSQLインジェクションの影響を受けにくいこと | NoSQLインジェクションの影響を受ける可能性がある | 5.3.4 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/login/organization | C01_ログイン組織情報取得 |
| 270 | VO20 | 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 | OSコマンドインジェクションの影響を受けにくいこと | OSコマンドインジェクションの影響を受ける可能性がある | 5.3.8<br>12.3.5 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/login/organization | C01_ログイン組織情報取得 |
| 271 | VO20 | 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 | OSコマンドインジェクションの影響を受けにくいこと | OSコマンドインジェクションの影響を受ける可能性がある | 5.3.8<br>12.3.5 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/login/organization | C01_ログイン組織情報取得 |
| 272 | VO20 | 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 | OSコマンドインジェクションの影響を受けにくいこと | OSコマンドインジェクションの影響を受ける可能性がある | 5.3.8<br>12.3.5 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/login/organization | C01_ログイン組織情報取得 |
| 273 | VO20 | 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 | OSコマンドインジェクションの影響を受けにくいこと | OSコマンドインジェクションの影響を受ける可能性がある | 5.3.8<br>12.3.5 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/login/organization | C01_ログイン組織情報取得 |
| 274 | FX02 | ファイル | ファイルの実行要件 | パストラバーサルやローカルファイルインクルードの影響を受けにくいこと | ユーザ由来のファイル名を十分な安全確認無しに利用している | 12.3.1<br>5.3.9 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/login/organization | C01_ログイン組織情報取得 |
| 275 | VO29 | 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 | HTTPヘッダインジェクションの影響を受けにくいこと | HTTPヘッダインジェクションの影響を受ける可能性がある | 5.3.5 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/login/organization | C01_ログイン組織情報取得 |
| 276 | VO18 | 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 | LDAPインジェクションの影響を受けにくいこと | LDAPインジェクションの影響を受ける可能性がある | 5.3.7<br>5.1.3 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/login/organization | C01_ログイン組織情報取得 |
| 277 | VO18 | 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 | LDAPインジェクションの影響を受けにくいこと | LDAPインジェクションの影響を受ける可能性がある | 5.3.7<br>5.1.3 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/login/organization | C01_ログイン組織情報取得 |
| 278 | VO18 | 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 | LDAPインジェクションの影響を受けにくいこと | LDAPインジェクションの影響を受ける可能性がある | 5.3.7<br>5.1.3 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/login/organization | C01_ログイン組織情報取得 |
| 279 | VO22 | 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 | XMLインジェクションの影響を受けにくいこと | XMLインジェクション攻撃の影響を受ける可能性がある | 5.3.10 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/login/organization | C01_ログイン組織情報取得 |
| 280 | VO22 | 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 | XMLインジェクションの影響を受けにくいこと | XMLインジェクション攻撃の影響を受ける可能性がある | 5.3.10 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/login/organization | C01_ログイン組織情報取得 |
| 281 | VO22 | 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 | XMLインジェクションの影響を受けにくいこと | XMLインジェクション攻撃の影響を受ける可能性がある | 5.3.10 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/login/organization | C01_ログイン組織情報取得 |
| 282 | VO24 | 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 | XPathインジェクションの影響を受けにくいこと | Xpathインジェクション攻撃の影響を受ける可能性がある | 5.3.10<br>5.1.3 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/login/organization | C01_ログイン組織情報取得 |
| 283 | VO24 | 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 | XPathインジェクションの影響を受けにくいこと | Xpathインジェクション攻撃の影響を受ける可能性がある | 5.3.10<br>5.1.3 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/login/organization | C01_ログイン組織情報取得 |
| 284 | VO05 | 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 | 出力の適切なエスケープにより反射型XSSの影響を受けにくいこと | ※このケースでは起票しない | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/login/organization | C01_ログイン組織情報取得 |
| 285 | VO05 | 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 | 出力の適切なエスケープにより反射型XSSの影響を受けにくいこと | ※このケースでは起票しない | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/login/organization | C01_ログイン組織情報取得 |
| 286 | VO05 | 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 | 出力の適切なエスケープにより反射型XSSの影響を受けにくいこと | ※このケースでは起票しない | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/login/organization | C01_ログイン組織情報取得 |
| 287 | VO05 | 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 | 出力の適切なエスケープにより反射型XSSの影響を受けにくいこと | ※このケースでは起票しない | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/login/organization | C01_ログイン組織情報取得 |
| 288 | VO05 | 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 | 出力の適切なエスケープにより反射型XSSの影響を受けにくいこと | ※このケースでは起票しない | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/login/organization | C01_ログイン組織情報取得 |
| 289 | VO05 | 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 | 出力の適切なエスケープにより反射型XSSの影響を受けにくいこと | ※このケースでは起票しない | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/login/organization | C01_ログイン組織情報取得 |
| 290 | VO05 | 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 | 出力の適切なエスケープにより反射型XSSの影響を受けにくいこと | ※このケースでは起票しない | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/login/organization | C01_ログイン組織情報取得 |

| ケースNo | 観点No | 観点分類 | 検査観点 | 検査基準 | 脆弱性 | ASVS | 検査粒度 | 検査対象 | ホスト | メソッド | URL | 画面 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 291 | VO05 | 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 | 出力の適切なエスケープにより反射型XSSの影響を受けにくいこと | ※このケースでは起票しない | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/login/organization | C01_ログイン組織情報取得 |
| 292 | VO05 | 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 | 出力の適切なエスケープにより反射型XSSの影響を受けにくいこと | ※このケースでは起票しない | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/login/organization | C01_ログイン組織情報取得 |
| 293 | VO05 | 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 | 出力の適切なエスケープにより反射型XSSの影響を受けにくいこと | ※このケースでは起票しない | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/login/organization | C01_ログイン組織情報取得 |
| 294 | VO07 | 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 | 出力の適切なエスケープにより反射型XSSの影響を受けにくいこと | XSS（反射型）の影響を受ける可能性がある | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/login/organization | C01_ログイン組織情報取得 |
| 295 | VO08 | 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 | 出力の適切なエスケープにより保存型XSSの影響を受けにくいこと | XSS（保存型）の影響を受ける可能性がある | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/login/organization | C01_ログイン組織情報取得 |
| 296 | VO34 | 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 | 出力の適切なエスケープによりDOMベースXSSの影響を受けにくいこと | XSS（DOM型）の影響を受ける可能性がある | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1<br>5.3.6<br>5.5.4 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/login/organization | C01_ログイン組織情報取得 |
| 297 | ZZ02 | – | – | – | – | | リクエスト | !Intruderのみ実施 | https://api-vuln.vams.jp | GET | /api/org | D01_ログインユーザー組織情報取得(スーパーユーザー) |
| 298 | ZZ07 | – | – | – | – | | リクエスト | !Intruderのみ実施 | https://api-vuln.vams.jp | GET | /api/org | D01_ログインユーザー組織情報取得(スーパーユーザー) |
| 299 | XG05 | 通信 | 通信のセキュリティ要件 | TLSがクライアント接続に使用されること | 重要情報の表示や操作に暗号化が強制されていない | 9.1.1 | リクエスト | 重要情報表示 | https://api-vuln.vams.jp | GET | /api/org | D01_ログインユーザー組織情報取得(スーパーユーザー) |
| 300 | DC01 | データ | クライアントサイドのデータ保護 | アンチキャッシングヘッダが設定され機微データがキャッシュされないこと | 重要情報の取得でキャッシュが無効化されていない | 8.2.1 | リクエスト | 重要情報表示 | https://api-vuln.vams.jp | GET | /api/org | D01_ログインユーザー組織情報取得(スーパーユーザー) |
| 301 | AG04 | アクセス制御 | 一般的なアクセス制御の設計 | アクセス制御が信頼できるサービスレイヤーで強制されること | 認証の必要な機能にアクセスできる | 4.1.1<br>4.1.3<br>4.2.1<br>14.5.2 | リクエスト | !ゲストページ | https://api-vuln.vams.jp | GET | /api/org | D01_ログインユーザー組織情報取得(スーパーユーザー) |
| 302 | AG01 | アクセス制御 | 一般的なアクセス制御の設計 | アクセス制御が信頼できるサービスレイヤーで強制されること | 権限のない機能にアクセスできる | 4.1.1<br>4.1.2<br>4.1.3<br>4.2.1 | リクエスト | 権限差異 | https://api-vuln.vams.jp | GET | /api/org | D01_ログインユーザー組織情報取得(スーパーユーザー) |
| 303 | AG01e | アクセス制御 | 一般的なアクセス制御の設計 | アクセス制御が信頼できるサービスレイヤーで強制されること | – | 4.1.1<br>4.1.2<br>4.1.3<br>4.2.1 | リクエスト | 権限差異 | https://api-vuln.vams.jp | GET | /api/org | D01_ログインユーザー組織情報取得(スーパーユーザー) |
| 304 | VO14 | 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 | SQLインジェクションの影響を受けにくいこと | SQLインジェクションの影響を受ける可能性がある | 5.3.4 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/org | D01_ログインユーザー組織情報取得(スーパーユーザー) |
| 305 | VO14 | 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 | SQLインジェクションの影響を受けにくいこと | SQLインジェクションの影響を受ける可能性がある | 5.3.4 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/org | D01_ログインユーザー組織情報取得(スーパーユーザー) |
| 306 | VO16 | 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 | NoSQLインジェクションの影響を受けにくいこと | NoSQLインジェクションの影響を受ける可能性がある | 5.3.4 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/org | D01_ログインユーザー組織情報取得(スーパーユーザー) |
| 307 | VO16 | 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 | NoSQLインジェクションの影響を受けにくいこと | NoSQLインジェクションの影響を受ける可能性がある | 5.3.4 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/org | D01_ログインユーザー組織情報取得(スーパーユーザー) |
| 308 | VO20 | 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 | OSコマンドインジェクションの影響を受けにくいこと | OSコマンドインジェクションの影響を受ける可能性がある | 5.3.8<br>12.3.5 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/org | D01_ログインユーザー組織情報取得(スーパーユーザー) |
| 309 | VO20 | 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 | OSコマンドインジェクションの影響を受けにくいこと | OSコマンドインジェクションの影響を受ける可能性がある | 5.3.8<br>12.3.5 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/org | D01_ログインユーザー組織情報取得(スーパーユーザー) |
| 310 | VO20 | 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 | OSコマンドインジェクションの影響を受けにくいこと | OSコマンドインジェクションの影響を受ける可能性がある | 5.3.8<br>12.3.5 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/org | D01_ログインユーザー組織情報取得(スーパーユーザー) |
| 311 | VO20 | 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 | OSコマンドインジェクションの影響を受けにくいこと | OSコマンドインジェクションの影響を受ける可能性がある | 5.3.8<br>12.3.5 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/org | D01_ログインユーザー組織情報取得(スーパーユーザー) |
| 312 | FX02 | ファイル | ファイルの実行要件 | パストラバーサルやローカルファイルインクルードの影響を受けにくいこと | ユーザ由来のファイル名を十分な安全確認無しに利用している | 12.3.1<br>5.3.9 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/org | D01_ログインユーザー組織情報取得(スーパーユーザー) |
| 313 | VO29 | 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 | HTTPヘッダインジェクションの影響を受けにくいこと | HTTPヘッダインジェクションの影響を受ける可能性がある | 5.3.5 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/org | D01_ログインユーザー組織情報取得(スーパーユーザー) |
| 314 | VO18 | 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 | LDAPインジェクションの影響を受けにくいこと | LDAPインジェクションの影響を受ける可能性がある | 5.3.7<br>5.1.3 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/org | D01_ログインユーザー組織情報取得(スーパーユーザー) |
| 315 | VO18 | 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 | LDAPインジェクションの影響を受けにくいこと | LDAPインジェクションの影響を受ける可能性がある | 5.3.7<br>5.1.3 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/org | D01_ログインユーザー組織情報取得(スーパーユーザー) |
| 316 | VO18 | 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 | LDAPインジェクションの影響を受けにくいこと | LDAPインジェクションの影響を受ける可能性がある | 5.3.7<br>5.1.3 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/org | D01_ログインユーザー組織情報取得(スーパーユーザー) |
| 317 | VO22 | 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 | XMLインジェクションの影響を受けにくいこと | XMLインジェクション攻撃の影響を受ける可能性がある | 5.3.10 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/org | D01_ログインユーザー組織情報取得(スーパーユーザー) |
| 318 | VO22 | 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 | XMLインジェクションの影響を受けにくいこと | XMLインジェクション攻撃の影響を受ける可能性がある | 5.3.10 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/org | D01_ログインユーザー組織情報取得(スーパーユーザー) |
| 319 | VO22 | 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 | XMLインジェクションの影響を受けにくいこと | XMLインジェクション攻撃の影響を受ける可能性がある | 5.3.10 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/org | D01_ログインユーザー組織情報取得(スーパーユーザー) |

| ケースNo | 観点No | 観点分類 | 検査観点 | 検査基準 | 脆弱性 | ASVS | 検査粒度 | 検査対象 | ホスト | メソッド | URL | 画面 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 320 | VO24 | 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 | XPathインジェクションの影響を受けにくいこと | Xpathインジェクション攻撃の影響を受ける可能性がある | 5.3.10<br>5.1.3 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/org | D01_ログインユーザー組織情報取得(スーパーユーザー) |
| 321 | VO24 | 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 | XPathインジェクションの影響を受けにくいこと | Xpathインジェクション攻撃の影響を受ける可能性がある | 5.3.10<br>5.1.3 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/org | D01_ログインユーザー組織情報取得(スーパーユーザー) |
| 322 | VO05 | 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 | 出力の適切なエスケープにより反射型XSSの影響を受けにくいこと | ※このケースでは起票しない | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/org | D01_ログインユーザー組織情報取得(スーパーユーザー) |
| 323 | VO05 | 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 | 出力の適切なエスケープにより反射型XSSの影響を受けにくいこと | ※このケースでは起票しない | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/org | D01_ログインユーザー組織情報取得(スーパーユーザー) |
| 324 | VO05 | 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 | 出力の適切なエスケープにより反射型XSSの影響を受けにくいこと | ※このケースでは起票しない | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/org | D01_ログインユーザー組織情報取得(スーパーユーザー) |
| 325 | VO05 | 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 | 出力の適切なエスケープにより反射型XSSの影響を受けにくいこと | ※このケースでは起票しない | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/org | D01_ログインユーザー組織情報取得(スーパーユーザー) |
| 326 | VO05 | 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 | 出力の適切なエスケープにより反射型XSSの影響を受けにくいこと | ※このケースでは起票しない | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/org | D01_ログインユーザー組織情報取得(スーパーユーザー) |
| 327 | VO05 | 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 | 出力の適切なエスケープにより反射型XSSの影響を受けにくいこと | ※このケースでは起票しない | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/org | D01_ログインユーザー組織情報取得(スーパーユーザー) |
| 328 | VO05 | 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 | 出力の適切なエスケープにより反射型XSSの影響を受けにくいこと | ※このケースでは起票しない | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/org | D01_ログインユーザー組織情報取得(スーパーユーザー) |
| 329 | VO05 | 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 | 出力の適切なエスケープにより反射型XSSの影響を受けにくいこと | ※このケースでは起票しない | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/org | D01_ログインユーザー組織情報取得(スーパーユーザー) |
| 330 | VO05 | 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 | 出力の適切なエスケープにより反射型XSSの影響を受けにくいこと | ※このケースでは起票しない | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/org | D01_ログインユーザー組織情報取得(スーパーユーザー) |
| 331 | VO05 | 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 | 出力の適切なエスケープにより反射型XSSの影響を受けにくいこと | ※このケースでは起票しない | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/org | D01_ログインユーザー組織情報取得(スーパーユーザー) |
| 332 | VO07 | 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 | 出力の適切なエスケープにより反射型XSSの影響を受けにくいこと | XSS(反射型)の影響を受ける可能性がある | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/org | D01_ログインユーザー組織情報取得(スーパーユーザー) |
| 333 | VO08 | 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 | 出力の適切なエスケープにより保存型XSSの影響を受けにくいこと | XSS(保存型)の影響を受ける可能性がある | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/org | D01_ログインユーザー組織情報取得(スーパーユーザー) |
| 334 | VO34 | 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 | 出力の適切なエスケープによりDOMベースXSSの影響を受けにくいこと | XSS(DOM型)の影響を受ける可能性がある | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1<br>5.3.6<br>5.5.4 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | GET | /api/org | D01_ログインユーザー組織情報取得(スーパーユーザー) |
| 335 | ZZ02 | – | – | – | – | | リクエスト | !Intruderのみ実施 | https://api-vuln.vams.jp | PUT | /api/org | D02_ログインユーザー組織情報更新(スーパーユーザー) |
| 336 | ZZ07 | – | – | – | – | | リクエスト | !Intruderのみ実施 | https://api-vuln.vams.jp | PUT | /api/org | D02_ログインユーザー組織情報更新(スーパーユーザー) |
| 337 | XG05 | 通信 | 通信のセキュリティ要件 | TLSがクライアント接続に使用されること | 重要情報の表示や操作に暗号化が強制されていない | 9.1.1 | リクエスト | 重要情報表示 | https://api-vuln.vams.jp | PUT | /api/org | D02_ログインユーザー組織情報更新(スーパーユーザー) |
| 338 | DC01 | データ | クライアントサイドのデータ保護 | アンチキャッシングヘッダが設定され機微データがキャッシュされないこと | 重要情報の取得でキャッシュが無効化されていない | 8.2.1 | リクエスト | 重要情報表示 | https://api-vuln.vams.jp | PUT | /api/org | D02_ログインユーザー組織情報更新(スーパーユーザー) |
| 339 | AG04 | アクセス制御 | 一般的なアクセス制御の設計 | アクセス制御が信頼できるサービスレイヤーで強制されること | 認証の必要な機能にアクセスできる | 4.1.1<br>4.1.3<br>4.2.1<br>14.5.2 | リクエスト | !ゲストページ | https://api-vuln.vams.jp | PUT | /api/org | D02_ログインユーザー組織情報更新(スーパーユーザー) |
| 340 | AG01 | アクセス制御 | 一般的なアクセス制御の設計 | アクセス制御が信頼できるサービスレイヤーで強制されること | 権限のない機能にアクセスできる | 4.1.1<br>4.1.2<br>4.1.3<br>4.2.1 | リクエスト | 権限差異 | https://api-vuln.vams.jp | PUT | /api/org | D02_ログインユーザー組織情報更新(スーパーユーザー) |
| 341 | AG01e | アクセス制御 | 一般的なアクセス制御の設計 | アクセス制御が信頼できるサービスレイヤーで強制されること | – | 4.1.1<br>4.1.2<br>4.1.3<br>4.2.1 | リクエスト | 権限差異 | https://api-vuln.vams.jp | PUT | /api/org | D02_ログインユーザー組織情報更新(スーパーユーザー) |
| 342 | VO14 | 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 | SQLインジェクションの影響を受けにくいこと | SQLインジェクションの影響を受ける可能性がある | 5.3.4 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | PUT | /api/org | D02_ログインユーザー組織情報更新(スーパーユーザー) |
| 343 | VO14 | 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 | SQLインジェクションの影響を受けにくいこと | SQLインジェクションの影響を受ける可能性がある | 5.3.4 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | PUT | /api/org | D02_ログインユーザー組織情報更新(スーパーユーザー) |
| 344 | VO16 | 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 | NoSQLインジェクションの影響を受けにくいこと | NoSQLインジェクションの影響を受ける可能性がある | 5.3.4 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | PUT | /api/org | D02_ログインユーザー組織情報更新(スーパーユーザー) |
| 345 | VO16 | 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 | NoSQLインジェクションの影響を受けにくいこと | NoSQLインジェクションの影響を受ける可能性がある | 5.3.4 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | PUT | /api/org | D02_ログインユーザー組織情報更新(スーパーユーザー) |
| 346 | VO20 | 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 | OSコマンドインジェクションの影響を受けにくいこと | OSコマンドインジェクションの影響を受ける可能性がある | 5.3.8<br>12.3.5 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | PUT | /api/org | D02_ログインユーザー組織情報更新(スーパーユーザー) |
| 347 | VO20 | 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 | OSコマンドインジェクションの影響を受けにくいこと | OSコマンドインジェクションの影響を受ける可能性がある | 5.3.8<br>12.3.5 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | PUT | /api/org | D02_ログインユーザー組織情報更新(スーパーユーザー) |
| 348 | VO20 | 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 | OSコマンドインジェクションの影響を受けにくいこと | OSコマンドインジェクションの影響を受ける可能性がある | 5.3.8<br>12.3.5 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | PUT | /api/org | D02_ログインユーザー組織情報更新(スーパーユーザー) |

| ケースNo | 観点No | 観点分類 | 検査観点 | 検査基準 | 脆弱性 | ASVS | 検査粒度 | 検査対象 | ホスト | メソッド | URL | 画面 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 349 | VO20 | 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 | OSコマンドインジェクションの影響を受けにくいこと | OSコマンドインジェクションの影響を受ける可能性がある | 5.3.8<br>12.3.5 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | PUT | /api/org | D02_ログインユーザー組織情報更新(スーパーユーザー) |
| 350 | FX02 | ファイル | ファイルの実行要件 | パストラバーサルやローカルファイルインクルードの影響を受けにくいこと | ユーザ由来のファイル名を十分な安全確認無しに利用している | 12.3.1<br>5.3.9 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | PUT | /api/org | D02_ログインユーザー組織情報更新(スーパーユーザー) |
| 351 | VO29 | 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 | HTTPヘッダインジェクションの影響を受けにくいこと | HTTPヘッダインジェクションの影響を受ける可能性がある | 5.3.5 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | PUT | /api/org | D02_ログインユーザー組織情報更新(スーパーユーザー) |
| 352 | VO18 | 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 | LDAPインジェクションの影響を受けにくいこと | LDAPインジェクションの影響を受ける可能性がある | 5.3.7<br>5.1.3 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | PUT | /api/org | D02_ログインユーザー組織情報更新(スーパーユーザー) |
| 353 | VO18 | 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 | LDAPインジェクションの影響を受けにくいこと | LDAPインジェクションの影響を受ける可能性がある | 5.3.7<br>5.1.3 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | PUT | /api/org | D02_ログインユーザー組織情報更新(スーパーユーザー) |
| 354 | VO18 | 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 | LDAPインジェクションの影響を受けにくいこと | LDAPインジェクションの影響を受ける可能性がある | 5.3.7<br>5.1.3 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | PUT | /api/org | D02_ログインユーザー組織情報更新(スーパーユーザー) |
| 355 | VO22 | 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 | XMLインジェクションの影響を受けにくいこと | XMLインジェクション攻撃の影響を受ける可能性がある | 5.3.10 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | PUT | /api/org | D02_ログインユーザー組織情報更新(スーパーユーザー) |
| 356 | VO22 | 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 | XMLインジェクションの影響を受けにくいこと | XMLインジェクション攻撃の影響を受ける可能性がある | 5.3.10 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | PUT | /api/org | D02_ログインユーザー組織情報更新(スーパーユーザー) |
| 357 | VO22 | 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 | XMLインジェクションの影響を受けにくいこと | XMLインジェクション攻撃の影響を受ける可能性がある | 5.3.10 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | PUT | /api/org | D02_ログインユーザー組織情報更新(スーパーユーザー) |
| 358 | VO24 | 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 | XPathインジェクションの影響を受けにくいこと | Xpathインジェクション攻撃の影響を受ける可能性がある | 5.3.10<br>5.1.3 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | PUT | /api/org | D02_ログインユーザー組織情報更新(スーパーユーザー) |
| 359 | VO24 | 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 | XPathインジェクションの影響を受けにくいこと | Xpathインジェクション攻撃の影響を受ける可能性がある | 5.3.10<br>5.1.3 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | PUT | /api/org | D02_ログインユーザー組織情報更新(スーパーユーザー) |
| 360 | VO05 | 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 | 出力の適切なエスケープにより反射型XSSの影響を受けにくいこと | ※このケースでは起票しない | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | PUT | /api/org | D02_ログインユーザー組織情報更新(スーパーユーザー) |
| 361 | VO05 | 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 | 出力の適切なエスケープにより反射型XSSの影響を受けにくいこと | ※このケースでは起票しない | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | PUT | /api/org | D02_ログインユーザー組織情報更新(スーパーユーザー) |
| 362 | VO05 | 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 | 出力の適切なエスケープにより反射型XSSの影響を受けにくいこと | ※このケースでは起票しない | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | PUT | /api/org | D02_ログインユーザー組織情報更新(スーパーユーザー) |
| 363 | VO05 | 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 | 出力の適切なエスケープにより反射型XSSの影響を受けにくいこと | ※このケースでは起票しない | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | PUT | /api/org | D02_ログインユーザー組織情報更新(スーパーユーザー) |
| 364 | VO05 | 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 | 出力の適切なエスケープにより反射型XSSの影響を受けにくいこと | ※このケースでは起票しない | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | PUT | /api/org | D02_ログインユーザー組織情報更新(スーパーユーザー) |
| 365 | VO05 | 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 | 出力の適切なエスケープにより反射型XSSの影響を受けにくいこと | ※このケースでは起票しない | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | PUT | /api/org | D02_ログインユーザー組織情報更新(スーパーユーザー) |
| 366 | VO05 | 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 | 出力の適切なエスケープにより反射型XSSの影響を受けにくいこと | ※このケースでは起票しない | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | PUT | /api/org | D02_ログインユーザー組織情報更新(スーパーユーザー) |
| 367 | VO05 | 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 | 出力の適切なエスケープにより反射型XSSの影響を受けにくいこと | ※このケースでは起票しない | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | PUT | /api/org | D02_ログインユーザー組織情報更新(スーパーユーザー) |
| 368 | VO05 | 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 | 出力の適切なエスケープにより反射型XSSの影響を受けにくいこと | ※このケースでは起票しない | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | PUT | /api/org | D02_ログインユーザー組織情報更新(スーパーユーザー) |
| 369 | VO05 | 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 | 出力の適切なエスケープにより反射型XSSの影響を受けにくいこと | ※このケースでは起票しない | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | PUT | /api/org | D02_ログインユーザー組織情報更新(スーパーユーザー) |
| 370 | VO07 | 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 | 出力の適切なエスケープにより反射型XSSの影響を受けにくいこと | XSS(反射型)の影響を受ける可能性がある | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | PUT | /api/org | D02_ログインユーザー組織情報更新(スーパーユーザー) |
| 371 | VO08 | 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 | 出力の適切なエスケープにより保存型XSSの影響を受けにくいこと | XSS(保存型)の影響を受ける可能性がある | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | PUT | /api/org | D02_ログインユーザー組織情報更新(スーパーユーザー) |
| 372 | VO34 | 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 | 出力の適切なエスケープによりDOMベースXSSの影響を受けにくいこと | XSS(DOM型)の影響を受ける可能性がある | 5.3.3<br>5.2.1<br>5.2.7<br>5.2.8<br>5.3.1<br>5.3.6<br>5.5.4 | リクエスト | 全リクエスト | https://api-vuln.vams.jp | PUT | /api/org | D02_ログインユーザー組織情報更新(スーパーユーザー) |