2023年8月 更新

サービス＆セキュリティ株式会社

Webアプリケーション脆弱性診断 対象脆弱性一覧

#	脆弱性名	危険度	備考
1	認証処理の不備	高	−
2	アカウントの乗っ取り	高	−
3	OSコマンドインジェクション	高	−
4	SQLインジェクション	高	−
5	クライアントサイドSQLインジェクション	高	−
6	HTTPリクエストスマグリング	高	−
7	ASP.NETのトレース機能が有効	高	−
8	パストラバーサル	高	−
9	XML外部実体参照	高	−
10	LDAPインジェクション	高	−
11	XPathインジェクション	高	−
12	PUTメソッドが有効	高	−
13	サーバサイドリクエストフォージェリ	高	−
14	PHPコードインジェクション	高	−
15	サーバサイドのJavaScriptコードインジェクション	高	−
16	Perlコードインジェクション	高	−
17	Rubyコードインジェクション	高	−
18	Pythonコードインジェクション	高	−
19	式言語インジェクション	高	−
20	汎用コードインジェクション	高	−
21	SSIインジェクション	高	−
22	HTTPレスポンスヘッダインジェクション	高	−
23	クライアントサイドテンプレートインジェクション	高	−
24	DOMベースのJavaScriptインジェクション	高	−
25	DOMベースのWebSocketハイジャック	高	−
26	ローカルファイルパスの改ざん	高	−
27	JWTの署名検証の不備	高	−
28	JWTの脆弱なHMAC署名秘密鍵の使用	高	−
29	安全ではないデシリアライゼーション	高	−
30	Webキャッシュポイズニング	高	−
31	ASP.NETのMAC無しのViewStateが有効	高	−
32	任意の形式のファイルをアップロード可能	高	−
33	ユーザ提供ファイルのメール送付	高	−
34	SMTPコマンドインジェクション	高	−
35	外部リソース読込	高〜低	−
36	サーバサイドテンプレートインジェクション	高〜低	−
37	クロスサイトスクリプティング	高〜低	反射型、格納型、DOM型に細分化されます。
38	認証の迂回	高〜情報	−
39	認可制御の不備	高〜情報	−
40	機密情報の開示	高〜情報	−
41	ビジネスロジックの不備	高〜情報	診断対象に合わせて名称を変更して報告します。
42	クロスサイトリクエストフォージェリ	高〜情報	−
43	非暗号化通信の使用	高〜情報	−
44	クロスオリジンリソース共有の設定不備	高〜情報	−
45	XMLインジェクション	中	−
46	ASP.NETのデバッグモードが有効	中	−
47	XMLエンティティ展開	中	−
48	Cookieへのパスワードの保存	中	−
49	document.domainプロパティの改ざん	中	−
50	CSSインジェクション	中〜低	−
51	URL内に機密情報が存在	中〜低	−
52	ファイルアップロード機能における容量制限の不備	中〜低	−

53	メール本文の改ざん	中～情報	–
54	メールヘッダインジェクション	低	–
55	HTTPレスポンスへのパスワードの出力	低	–
56	Cookieへのセキュリティ属性の未設定	低	–
57	二段階認証の迂回	低	–
58	クライアントサイドXPathインジェクション	低	–
59	クライアントサイドJSONインジェクション	低	–
60	GraphQLスキーマの開示	低	–
61	GraphQLのフィールド提案が有効	低	–
62	URLクエリ文字列内に返されるパスワード	低	–
63	CAPTCHAの迂回	低	–
64	セッションIDの未更新	低	–
65	ログアウト実行時にセッションが破棄されていない	低	–
66	ログアウト機能が未実装	低	–
67	DOMベースのCookie強制	低	–
68	Ajaxリクエストヘッダの改ざん	低	–
69	マスキングされていないパスワード入力箇所	低	–
70	推測が容易なアカウント名の使用	低	–
71	リンクの改ざん	低～情報	–
72	オープンリダイレクト	低～情報	–
73	DOMベースのサービス拒否	低～情報	–
74	設定推奨ヘッダの未設定	低～情報	–
75	システムエラーメッセージの出力	低～情報	–
76	サニタイズ処理の漏れ	情報	–
77	複数のメールアドレスが登録可能	情報	–
78	外部サービスとの通信を確認	情報	–
79	Domain属性に上位ドメインが設定されたCookie	情報	–
80	Web Messagingの改ざん	情報	–
81	Web Storageの改ざん	情報	–
82	DOMベースのHTML操作	情報	–
83	ディレクトリリスティング	情報	–
84	バックアップファイルの開示	情報	–
85	テストファイルの検出	情報	–
86	HTMLコメントによる情報の開示	情報	–
87	robots.txtによる情報開示	情報	–
88	クライアントサイドプロトタイプ汚染	情報	–
89	Flashのクロスドメインポリシー	情報	–
90	Silverlightのクロスドメインポリシー	情報	–
91	安全性の低いドメインとの通信	情報	–
92	脆弱なバージョンのJavaScriptライブラリ	情報	–

・危険度「高」のうち特に危険度が高いものについて、危険度を「深刻」として報告する場合があります。

・脆弱性が存在する可能性があるものの断定できない検出について、脆弱性名を「～の可能性」として報告する場合があります。

■　オプション対応の診断項目

事前のご依頼に基づいて調査します。現在の仕様のヒアリングにて確認する場合があります。

1	有効なログインIDを収集可能	低	–
2	アカウントロックの強度	低	–
3	パスワードポリシーの強度	低	–
4	セッションタイムアウトの時間	低	–