診断番号	診断対象の脆弱性	診断を実施すべき箇所	検出パターン	診断を行う箇所	診断方法	脆弱性がある場合の結果	脆弱性がない場合の結果	備考
1	SQLインジェクション	すべて	「'」(シングルクォート1つ)	パラメーター	パラメーターの値に検出パターンを挿入し、リクエストを送信	DB関連のエラーが表示されるか、正常動作と挙動が異なる	DB関連のエラーは表示されない	DB関連のエラー（SQL Syntax, SQLException, pg_exec, ORA-5桁数字, ODBC Driver Managerなど）は画面に表示されることもあれば、HTMLソースに表示されることもある SQLiがあるが、エラーが画面にでない場合には正常時と挙動が異なることもある ただし、この診断手法の脆弱性の有無については確定ではなく、あくまで可能性を示唆するものである
2	SQLインジェクション	すべて	(1)「(検索キー)」だけの場合と「(検索キー)' and 'a'='a」を比較／(2)「(検索キー)」だけの場合と「(検索キー)' and 'a'='b」を比較	パラメーター	パラメーターの値に検出パターンを挿入し、リクエストを送信	(1)で同一の結果が返り(2)で異なる結果が返ってくる	(1)も(2)も同じ結果が返ってくる、または(1)も(2)も異なる結果が返ってくる	「' and 'a'='a'」の部分がSQL文の一部として機能（演算を実施）している場合には、「'a'='a'」は常に真（1）となり、判定結果に影響しないため、SQLインジェクションが可能であると判断できる ただし、この診断手法の脆弱性の有無については確定ではなく、あくまで可能性を示唆するものである
3	SQLインジェクション	型が数値のパラメーター	(1)「(検索キー:数値)」だけの場合と「(検索キー) and 1=1」を比較／(2)「(検索キー:数値)」だけの場合と「(検索キー) and 1=0」を比較	パラメーター	パラメーターの値に検出パターンを挿入し、リクエストを送信	(1)で同一の結果が返り(2)で異なる結果が返ってくる	(1)も(2)も同じ結果が返ってくる、または(1)も(2)も異なる結果が返ってくる	「 and 1=1」の部分がSQL文の一部として機能（演算を実施）している場合には、「1=1」は常に真（1）となり、判定結果に影響しないため、SQLインジェクションが可能であると判断できる ただし、この診断手法の脆弱性の有無については確定ではなく、あくまで可能性を示唆するものである
4	SQLインジェクション	すべて	「'||'」、「'|||'」、「'+'」、「'++'」	パラメーター	パラメーターの値に検出パターンを挿入し、リクエストを送信	文字列連結の演算が実行される	文字列としてそのまま評価される	DB処理が更新系の場合には実行しない方がいい場合もあるので注意
5	SQLインジェクション	すべて	1/0	パラメーター	パラメーターの値に検出パターンを挿入し、リクエストを送信	演算が実行される（ゼロ除算のエラーになる）	文字列としてそのまま評価される	
6	コマンドインジェクション	すべて	||ping -nc 10 127.0.0.1%0a|	パラメーター	パラメーターの値に検出パターンを挿入し、リクエストを送信	レスポンスが返ってくるのが20秒遅くなる	通常通りの応答速度でレスポンスが返ってくる	
7	コマンドインジェクション	すべて	../../../../../../bin/sleep 20|	パラメーター	パラメーターの値に検出パターンを挿入し、リクエストを送信	レスポンスが返ってくるのが20秒遅くなる	通常通りの応答速度でレスポンスが返ってくる	診断対象がUNIX系
8	コマンドインジェクション	すべて	;/bin/sleep 20	パラメーター	パラメーターの値に検出パターンを挿入し、リクエストを送信	レスポンスが返ってくるのが20秒遅くなる	通常通りの応答速度でレスポンスが返ってくる	診断対象がUNIX系
9	コマンドインジェクション	すべて	$(../../../../../../bin/sleep 20)	パラメーター	パラメーターの値に検出パターンを挿入し、リクエストを送信	レスポンスが返ってくるのが20秒遅くなる	通常通りの応答速度でレスポンスが返ってくる	診断対象がUNIX系
10	コマンドインジェクション	すべて	../../../../../../windows/system32/ping -n 21 127.0.0.1|	パラメーター	パラメーターの値に検出パターンを挿入し、リクエストを送信	レスポンスが返ってくるのが20秒遅くなる	通常通りの応答速度でレスポンスが返ってくる	診断対象がWindows系
11	コマンドインジェクション	すべて	&/windows/system32/ping -n 21 127.0.0.1	パラメーター	パラメーターの値に検出パターンを挿入し、リクエストを送信	レスポンスが返ってくるのが20秒遅くなる	通常通りの応答速度でレスポンスが返ってくる	診断対象がWindows系
12	CRLFインジェクション(HTTPヘッダーインジェクション)	レスポンスヘッダーに値を出力している箇所	%0d%0aSet-Cookie:(任意の値)%3D(任意の値)%3B	レスポンスヘッダーに値を出力しているパラメーター	パラメーターの値に検出パターンを挿入し、リクエストを送信	パラメーターに改行が挿入され、新たなSet-Cookieヘッダーフィールドが挿入される	診断箇所の後ろに改行されずに検出パターンの文字列が表示される	主な検査対象はSet-CookieやLocationヘッダーフィールド
13	CRLFインジェクション(HTTPレスポンス分割攻撃)	レスポンスヘッダーに値を出力している箇所	%0d%0akensa	レスポンスヘッダーに値を出力しているパラメーター	パラメーターの値に検出パターンを挿入し、リクエストを送信	パラメーターに改行コードが2つ挿入され、「kensa」文字列がHTTPボディ部分に表示される	診断箇所の後ろに改行されずに検出パターンの文字列が表示される	主な検査対象はSet-CookieやLocationヘッダーフィールド
14	CRLFインジェクション(メールヘッダーインジェクション)	メールメッセージのヘッダーに値を出力している箇所	%0d%0aTo:(任意のメールアドレス)	メールメッセージのヘッダーに値を出力しているパラメーター	パラメーターの値に検出パターンを挿入し、リクエストを送信	挿入したメールアドレス宛にメールが配送される	エラーが発生するなど、メールが配送されない	受信可能な「99@example.com」のようなメールアドレスを用意する必要がある
15	クロスサイトスクリプティング(XSS)	すべて	「>"><hr>」	パラメーター	パラメーターの値に検出パターンを挿入し、リクエストを送信	検査パターンが適切にエスケープされずに挿入される	検査パターンが適切にエスケープされて挿入される	「<>"&'」が適切にエスケープされているかを確認
16	クロスサイトスクリプティング(XSS)	すべて	<script>alert(1)</script>	パラメーター	パラメーターの値に検出パターンを挿入し、リクエストを送信	検査パターンが適切にエスケープされずに挿入される	検査パターンが適切にエスケープされて挿入される	「<>"&'」が適切にエスケープされているかを確認
17	クロスサイトスクリプティング(XSS)	すべて	javascript:alert(1);	パラメーター	パラメーターの値に検出パターンを挿入し、リクエストを送信	URI属性やJavaScriptなどのURIを指定する箇所に表示される	URI属性やJavaScriptなどのURIを指定する箇所に表示されない	
18	クロスサイトスクリプティング(XSS)	JavaScript内に文字列が挿入できる箇所	「';alert(1)//」	パラメーター	パラメーターの値に検出パターンを挿入し、リクエストを送信	スクリプトが実行される	スクリプトが実行されない	
19	クロスサイトスクリプティング(XSS)	JavaScript内に文字列が挿入できる箇所	「'%3balert(1)//」	パラメーター	パラメーターの値に検出パターンを挿入し、リクエストを送信	スクリプトが実行される	スクリプトが実行されない	
20	クロスサイトスクリプティング(XSS)	JavaScript内に文字列が挿入できる箇所	;alert(1)	パラメーター	パラメーターの値に検出パターンを挿入し、リクエストを送信	スクリプトが実行される	スクリプトが実行されない	
21	クロスサイトスクリプティング(XSS)	すべて	(URL)#"><img src=0 onerror=alert(1)>	URL	URLを検出パターンのように書き換えて、ブラウザでアクセス	スクリプトが実行される	スクリプトが実行されない	DOM based XSS
22	クロスサイトスクリプティング(XSS)	Aタグ内にURLやファイルパスを挿入できる箇所	(URL/ファイル名)#<script>alert(1)</script>	パラメーター	パラメーターの値に検出パターンを挿入し、リクエストを送信	検査パターンが適切にエスケープされずに挿入される	検査パターンが適切にエスケープされて挿入される	「<>"&'」が適切にエスケープされているかを確認
23	クロスサイトスクリプティング(XSS)	HTMLタグの属性値内に値が挿入できる箇所			属性値が「"」で囲まれているかを確認	属性値が「"」で囲まれていない	属性値が「"」で囲まれている	

診断番号	診断対象の脆弱性	診断を実施すべき箇所	検出パターン	診断を行う箇所	診断方法	脆弱性がある場合の結果	脆弱性がない場合の結果	備考
24	パストラバーサル	ファイル名を扱っている画面や機能	「./(元の値)」	ファイル名と想定されるパラメーター	パラメーターの値に検出パターンを挿入し、リクエストを送信	正常時と結果が変わらない	エラーが表示される	
25	パストラバーサル	すべて	GET //etc/hosts HTTP/1.1	HTTPリクエスト	検出パターンのリクエストを送信	/etc/hostsの内容が表示される	エラー（404 Not Found）が表示される	診断対象がUNIX系
26	パストラバーサル	ファイル名を扱っている画面や機能	「../../../../../../../../etc/hosts」他に親ディレクトリの指定方法として「..//」「.../」も組み合わせる	ファイル名と想定されるパラメーター	パラメーターの値に検出パターンを挿入し、リクエストを送信	/etc/hostsの内容が表示される	/etc/hostsの内容が表示されない	診断対象がUNIX系
27	パストラバーサル	ファイル名を扱っている画面や機能	「../../../../../../../../etc/hosts%00」他に親ディレクトリの指定方法として「..//」「.../」も組み合わせる	ファイル名と想定されるパラメーター	パラメーターの値に検出パターンを挿入し、リクエストを送信	/etc/hostsの内容が表示される	/etc/hostsの内容が表示されない	診断対象がUNIX系
28	パストラバーサル	ファイル名を扱っている画面や機能	「../../../../../../../../windows/win.ini」他に親ディレクトリの指定方法として「..//」「.../」も組み合わせる	ファイル名と想定されるパラメーター	パラメーターの値に検出パターンを挿入し、リクエストを送信	/windows/win.iniの内容が表示される	/windows/win.iniの内容が表示されない	診断対象がWindows系
29	パストラバーサル	ファイル名を扱っている画面や機能	「../../../../../../../../windows/win.ini%00」他に親ディレクトリの指定方法として「..//」「.../」も組み合わせる	ファイル名と想定されるパラメーター	パラメーターの値に検出パターンを挿入し、リクエストを送信	/windows/win.iniの内容が表示される	/windows/win.iniの内容が表示されない	診断対象がWindows系
30	オープンリダイレクト	リダイレクトが実行される画面や機能	「http://www.example.com/」	URL、もしくはURLの一部と想定されるパラメーター	パラメーターの値に検出パターンを挿入し、リクエストを送信	http://www.example.comにリダイレクトされる	http://www.example.comにリダイレクトされない	指定する検出パターンのURLの形式は必要に応じて変更する 主な検査対象は、Locationヘッダーフィールド、METAタグのRefresh、JavaScriptコード（location.href, location.assign, location.replace）
31	オープンリダイレクト	リダイレクトが実行される画面や機能	「//www.example.com/」	URL、もしくはURLの一部と想定されるパラメーター	パラメーターの値に検出パターンを挿入し、リクエストを送信	http://www.example.comにリダイレクトされる	http://www.example.comにリダイレクトされない	指定する検出パターンのURLの形式は必要に応じて変更する 主な検査対象は、Locationヘッダーフィールド、METAタグのRefresh、JavaScriptコード（location.href, location.assign, location.replace）
32	リモートファイルインクルージョン（RFI）	ファイル名を扱っている画面や機能（PHP）	「(外部サーバーのスクリプトを配置したURL)」	ファイル名と想定されるパラメーター	パラメーターの値に検出パターンを挿入し、リクエストを送信	スクリプトが読み込まれ実行される	スクリプトが読み込まれない	外部Webサーバーを用意し、PHPのスクリプトを配置する必要がある
33	クリックジャッキング	確定処理の直前画面		レスポンスヘッダー	レスポンスヘッダーにX-Frame-Optionsヘッダーフィールドが存在し、値が「DENY」「SAMEORIGIN」「ALLOW-FROM (uri)」かを確認	X-Frame-Optionsヘッダーフィールドがない／値が「DENY」「SAMEORIGIN」「ALLOW-FROM (uri)」ではない	レスポンスヘッダーにX-Frame-Optionsヘッダーフィールドが存在し、値が「DENY」「SAMEORIGIN」「ALLOW-FROM (uri)」	
34	認証回避	ログイン機能			存在しないアカウント、正しくないパスワードでログインを試行	認証が成功する	認証に失敗する	
35	ログアウト機能の不備や未実装	ログアウト機能			ログアウト機能が存在するかを確認	ログアウト機能が存在しない	ログアウト機能が存在する	
36	ログアウト機能の不備や未実装	ログアウト機能			認証で使っているセッションIDをメモする ログアウト機能を実行後、メモしたセッションIDを付与してログイン状態になることを確認	認証状態でしかアクセスできない画面や機能にアクセスできる（ログイン状態になる）	認証状態でしかアクセスできない画面や機能にアクセスできない（ログイン状態にならない）	ログアウト機能の実行時にセッションIDが破棄されていない場合に発生する
37	過度な認証試行に対する対策不備・欠落	ログイン機能			同じユーザー名でパスワードを短時間に10回間違える	アカウントロックされない	アカウントロックされる	
38	脆弱なパスワードポリシー	パスワード登録・変更機能			パスワード文字列の桁数が8文字以下、文字種が大小英字、数字の3種類が混在でない文字列を登録・変更する	脆弱なパスワード文字列が登録できる	脆弱なパスワード文字列が登録できない	
39	復元可能なパスワード保存	Webアプリケーションのソースコード、もしくはパスワードが保存されたデータベース			安全なハッシュ関数を使用し、ソルトやストレッチングが使用されているかを確認	平文やレインボーテーブルなどで復元可能な文字列で保存されている	保存されたパスワード文字列の復元は困難	ソースコードやデータベースを確認できない場合には顧客にヒアリングを行う 安全なハッシュ関数についてはCRYPTREC暗号リスト（電子政府推奨暗号リスト）を参照
40	復元可能なパスワード保存	Webアプリケーションのソースコード、もしくはパスワードが保存されたデータベース			安全な暗号アルゴリズムを使用し、暗号化の鍵を安全な方法で保存しているかを確認	安全な暗号アルゴリズムを用いていない／暗号化の鍵が安全な方法で保存されていない	保存されたパスワード文字列の復元は困難	安全な暗号アルゴリズムについてはCRYPTREC暗号リスト（電子政府推奨暗号リスト）を参照
41	復元可能なパスワード保存	パスワードリマインダー機能			パスワードリマインダー機能でパスワードを問い合わせる	登録したパスワードが返ってくる	パスワードリマインダー機能が存在しない	復元可能なパスワード保存されていないとパスワード文字列を返すことはできない
42	パスワードリセットの不備	パスワードリセット機能			アカウントに紐付いたメールアドレス以外でパスワードリセット機能が実行できるかを確認	他ユーザーのパスワードリセットが実行される	パスワードリセットが実行されない	
43	パスワードリセットの不備	パスワードリセット機能			パスワードリセット機能を実行した結果がWebページに表示されるかを確認	リセットされたパスワードがWebページに表示される	リセットされたパスワードがアカウントに紐付いたメールアドレス宛に送られる	
44	パスワードリセットの不備	パスワードリセット機能			パスワードリセット機能によって送られてきた新しいパスワードでログインできるかを確認	送られてきたパスワードでログインができる	送られてきたパスワードを使用して、ユーザー自身が新しいパスワードを登録する	

診断番号	診断対象の脆弱性	診断を実施すべき箇所	検出パターン	診断を行う箇所	診断方法	脆弱性がある場合の結果	脆弱性がない場合の結果	備考
45	パスワードリセットの不備	パスワードリセット機能			管理者権限で任意のユーザーに設定した任意のパスワードでログインできるかを確認	設定したパスワードでログインができる	設定したパスワードを使用して、ユーザー自身が新しいパスワードを登録する	
46	権限の不正な昇格	認可制御が必要な箇所	「(管理者権限や高い権限と想定される権限を表す値)」	権限が設定されていると想定されるパラメーター	パラメーターの値に検出パターンを挿入し、リクエストを送信	指定した権限で機能が実行される	指定した権限で機能が実行されない	
47	強制ブラウズ	インデックス表示されるディレクトリ			インデックス表示されたファイル名にアクセスし、アクセス権限のない機能やファイルにアクセスできるかを確認	アクセス権限のない機能やファイルにアクセスできる	アクセス権限のない機能やファイルにアクセスできない	
48	強制ブラウズ	認可制御が必要な箇所	「(他ユーザーの権限が必要な情報や機能を示す値)」	権限が必要な情報や機能を示すと想定されるパラメーター	パラメーターの値に検出パターンを挿入し、リクエストを送信	他ユーザーの権限が必要な情報が表示されたり、機能が実行できたりする	他ユーザーの権限が必要な情報が表示されたり、機能が実行できたりしない	他ユーザーの権限が必要な情報を示す値とは、たとえば文書ID、注文番号、顧客番号など
49	パラメータ操作による不正な機能の利用	認可制御が必要な箇所	「(実行されては困る値)」	実行されては困ると想定されるパラメーター	パラメーターの値に検出パターンを挿入し、リクエストを送信	権限がない機能が実行できる	権限のない機能は実行できない	
50	セッションフィクセイション(セッション固定攻撃)	ログイン機能		Set-Cookieヘッダーフィールド	ログイン成功後に新しい認証に使うセッションIDが発行されるかを確認	ログイン成功前と同じセッションIDが継続して使用される場合	ログイン成功後に新しいセッションIDが発行され、古いセッションIDは破棄される	
51	クロスサイトリクエストフォージェリ(CSRF)	CSRF対策が必要な箇所		レスポンスボディ	POSTメソッドかつリクエストメッセージ内にCSRF対策トークンがあることを確認	CSRF対策トークンがない	CSRF対策トークンがある	
52	クロスサイトリクエストフォージェリ(CSRF)	CSRF対策が必要な箇所		レスポンスボディ	CSRF対策トークンがあるリクエストメッセージからCSRF対策トークンを削除してリクエストを送信し、機能が実行されるかを確認	機能が実行される	機能が実行されない	
53	クロスサイトリクエストフォージェリ(CSRF)	CSRF対策が必要な箇所		レスポンスボディ	ユーザーAのCSRF対策トークンを記録し、ユーザーBのリクエストメッセージ内のCSRF対策トークンをそれに書き換えて機能が実行されるかを確認	機能が実行される	機能が実行されない	
54	クロスサイトリクエストフォージェリ(CSRF)	CSRF対策が必要な箇所		レスポンスボディ	CSRF対策トークンを複数集めて規則性があることを確認し、CSRF対策トークンを推測する	CSRF対策トークンに規則性があり推測可能	CSRF対策トークンの規則性が判らず推測不可	CSRF対策トークンが固定長でない場合は疑う余地がある
55	CookieのHttpOnly属性未設定	Set-Cookieヘッダーフィールドがある箇所		Set-Cookieヘッダーフィールド	Set-CookieヘッダーフィールドにHttpOnly属性があることを確認	HttpOnly属性がない	HttpOnly属性がある	
56	推測可能なセッションID	ログイン機能		Set-Cookieヘッダーフィールド	セッションIDを複数集めて規則性があることを確認し、セッションIDを推測する	セッションIDに規則性があり推測可能	セッションIDの規則性が判らず推測不可	セッションIDが固定長でない場合は疑う余地がある
57	クエリストリング情報の漏えい	すべて		URL	URLのクエリー部分に重要な情報が入っていることを確認	重要な情報が入っている	重要な情報が入っていない	特にセッションIDやCSRF対策トークン、アカウント情報など
58	キャッシュからの情報漏えい	すべて		レスポンスメッセージ	レスポンスメッセージ内で適切にキャッシュ制御を行っていることを確認	METAタグもしくはレスポンスヘッダーでCache-Controlヘッダーフィールドが存在しない、または適切に指定されていない	METAタグもしくはレスポンスヘッダーでCache-Controlヘッダーフィールド適切に指定されている	Cache-Controlヘッダーフィールド値は "private", "no-store", "no-cache", "must-revalidate"
59	パスワードフィールドのマスク不備	パスワード入力画面		inputタグ	パスワード入力に使用するinputタグのtype属性に"password"が指定されていることを確認	inputタグのtype属性が"password"ではない	inputタグのtype属性が"password"ではある	
60	エラーメッセージによる情報露出	すべて			表示されたエラーメッセージに攻撃に有用な情報がふくまれていることを確認	エラーメッセージに攻撃に有用な情報が含まれている	エラーメッセージに攻撃に有用な情報が含まれていない	攻撃に有用な情報とはソフトウェアが出力するエラーメッセージの環境情報やユーザー情報など
61	機微情報の表示	すべて			機微情報がWebページ上に表示されていることを確認	機微情報がWebページ上に表示されている	機微情報がWebページ上に表示されていない	主な機微情報としてはクレジットカード番号やPINコード
62	HTTPS利用時のSecure属性がない機微Cookie	Set-Cookieヘッダーフィールドがある箇所		Set-Cookieヘッダーフィールド	HTTPS利用時のSet-CookieヘッダーフィールドにSecure属性があることを確認	Secure属性がない	Secure属性がある	
63	機微情報の平文保存	Webアプリケーションのソースコード、もしくは機微情報が保存されたデータベース			機微情報が平文で保存されていることを確認	機微情報が平文で保存されている	機微情報が平文で保存されていない	
64	HTTPSの不適切な利用	すべて			% openssl s_client -connect (診断対象ドメイン):443 -ssl2 % openssl s_client -connect (診断対象ドメイン):443 -ssl3	接続できる	エラーで接続できない	SSL2.0/SSL3.0を指定しての接続確認
65	HTTPSの不適切な利用	すべて			HTTPS接続時にWebブラウザの警告が出ることを確認	Webブラウザに何らかの警告が出る	Webブラウザに何らかの警告が出ない	
66	HTTPSの不適切な利用	すべて			安全ではない暗号スイートが利用されていることの確認	安全ではない暗号スイートが利用されている	安全ではない暗号スイートは利用されていない	sslscanなどを使用して確認することができる
67	不要な情報の存在	すべて		HTML/JavaScriptソースコード	HTMLソースコードのコメント内に攻撃に有用な情報が含まれていることを確認	HTMLソースコードに攻撃に有用な情報が含まれている	HTMLソースコードに攻撃に有用な情報が含まれていない	攻撃に有用な情報とは設計やデータベース構造になどに係わる情報

2016年12月17日版