大分類	中分類	小分類	診断を実施すべき箇所	ペイロード・検出パターン	操作を行う対象	診断方法	脆弱性がある場合の結果	脆弱性がない場合	備考
Webアプリケーションの脆弱性	インジェクション	SQLインジェクション	すべて	'(シングルクォート)	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 SQLインジェクションがあるが、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
			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	
			すべて	(1)「(元の値)」 (2)「(元の値)' and 'a'='a」 (3)「(元の値)' and 'a'='b」	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)を送信して正常系の動作を確認し、(1)と(2)を比較して同一のレスポンスとなり、(2)と(3)で異なるレスポンスが返ってくる	左記以外	「' 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
			型が数値のパラメーター	(1)「(元の値:数値)」 (2)「(元の値) and 1=1」 (3)「(元の値) and 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	(1)を送信して正常系の動作を確認し、(1)と(2)を比較して同一のレスポンスとなり、(2)と(3)で異なるレスポンスが返ってくる	左記以外	「 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
			型が数値のパラメーター	(1)「(元の値:数値)」 (2)「(元の値)-0」 (3)「(元の値)-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	(1)を送信して正常系の動作を確認し、(1)と(2)を比較して同一のレスポンスとなり、(2)と(3)で異なるレスポンスが返ってくる	左記以外	
		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	
			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	
			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	
			すべて	;ping -nc 20 127.0.0.1;	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	
			すべて	&ping -nc 20 127.0.0.1&	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	
			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	
		CRLF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	主な診断対象はSet-CookieやLocationヘッダーフィールド
			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	主な診断対象はSet-CookieやLocationヘッダーフィールド
			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	受信可能なメールアドレスを用意する必要がある
		クロスサイトスクリプティング(XSS)	すべて	">'><s>XSS	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	検出パターンが適切にエスケープされずに挿入される	検出パターンが適切にエスケープされて挿入される	
			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	検出パターンが適切にエスケープされずに挿入される	検出パターンが適切にエスケープされて挿入される	
			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コード等に挿入され、javascriptスキームとして有効になる	javascriptスキームとして有効にならない	
			すべて	'+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	検出パターンが適切にエスケープされずに挿入される	検出パターンが適切にエスケープされて挿入される	
			すべて	"onmouseover="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	検出パターンが適切にエスケープされずに挿入される	検出パターンが適切にエスケープされて挿入される	
			URL	#">'><img src=x onerror=alert(1)>	パラメーター	検出パターンをURLの最後尾に追記して、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	アドレスバーのURLを直接編集した場合はリロードが必要となる場合が多いことに留意
	パストラバーサル	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	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	
			ファイル名を扱っている画面や機能	../../../../../../../etc/hosts%00	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	
			ファイル名を扱っている画面や機能	../../../../../../../windows/win.ini	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	
			ファイル名を扱っている画面や機能	../../../../../../../windows/win.ini%00	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	
	オープンリダイレクト	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 主な診断対象は、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）
			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 主な診断対象は、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）
	インクルードにまつわる脆弱性	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	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、スクリプトを配置する必要がある スクリプト例 phpinfo();sleep(15);

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)」	
認証	認証回避	認証が必要な箇所		認証状態を保持しているパラメーター	認証状態を保持しているパラメーター（ex. authenticated=ueno、userid=1234）を特定し、パラメーター値を変更して認証後のページにアクセス	認証後のページを指定することでアクセスが可能である	認証後のページを指定することでアクセスができない	
		ログイン機能		パラメーター	正しいアカウントとパスワードの組み合わせ以外でログインを試行	認証が成功する	認証に失敗する	
	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	
		ログアウト機能			認証で使っているセッションIDをメモし、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
	過度な認証試行に対する対策不備や未実装	ログイン機能		パラメーター	同じユーザー名でパスワードを連続して10回間違えて確認	アカウントロックされない	アカウントロックされる	試行するパスワードはパスワードポリシーに従うこと
	脆弱なパスワードポリシー	パスワード登録・変更	(空) 1234567 abcdefg abcd123	パラメーター	パスワード文字列の桁数が8文字未満、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・変更できないことを確認	脆弱なパスワードが登録・変更できる	脆弱なパスワードが登録・変更できない	
		パスワード登録・変更	RfM9yY8Cwk	パラメーター	パスワード文字列の桁数が8文字以上、かつ文字種が大小英字、数字の3種類が混在している文字列を登録・変更できることを確認	登録・変更できない	登録・変更できる	
		パスワード登録・変更		パラメーター	ユーザー名と同じパスワードが登録・変更できないことを確認	脆弱な(推測可能な)パスワードが設定できる	脆弱な(推測可能な)パスワードが設定できない	
	復元可能なパスワード保存	パスワード登録・変更			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て確認	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	
		全般			設定したパスワードが、いずれかのページで表示や埋め込まれていないことを確認	レスポンスにパスワードが埋め込まれている	パスワードが埋め込まれていない	
	パスワードリセットの不備	パスワードリセット			パスワードリセットを実行して、再設定時に本人確認をしていることを確認	ユーザー本人しか受け取れない連絡先に再設定方法が通知されずにパスワードのリセットが可能	ユーザー本人しか受け取れない連絡先に再設定方法が通知される	
		パスワードリセット			パスワードリセットを実行して、ユーザー自身による新たなパスワード設定が強制されることを確認	システムが生成したパスワードが送付され、そのまま使い続けられる	ユーザー自身が新たなパスワードを設定する	
認可制御の不備		認可制御が必要な箇所		URL	権限の異なる複数のユーザーで、本来権限のない機能のURLにアクセス	アクセス権限がない情報や機能が閲覧、操作できる	アクセス権限がない情報や機能が閲覧、操作できない	
		認可制御が必要な箇所		パラメーター	登録データに紐づく値がパラメーターにより指定されている場合、そのID類を変更して当該ユーザーではアクセス権限がない情報や機能へアクセス	当該ユーザーではアクセス権限がない情報や機能へアクセスできる	当該ユーザーではアクセス権限がない情報や機能へアクセスできない	登録データに紐づく値がパラメーターとして用いられている例： ユーザーID 文書ID 注文番号 顧客番号 など
		認可制御が必要な箇所		パラメーター	hiddenパラメーターやCookieなどの値で権限クラスを指定していると推測される場合に、値を変更、追加などを行うことで当該ユーザーではアクセス権限がない情報や機能を閲覧、操作	当該ユーザーではアクセス権限がない情報や機能が閲覧、操作できる	当該ユーザーではアクセス権限がない情報や機能が閲覧、操作できない	権限がパラメーターとして用いられている例： func=admin など
		認可制御が必要な箇所		URL	認証状態でしか表示できないページに、ログイン認証していない状態でアクセス	認証後のページを指定することでアクセスが可能である	認証後のページを指定することでアクセスができない	
		認可制御が必要な箇所	元の値：www.example.com/user1/profile.php 施行例：www.example.com/user2/profile.php 元の値：www.example.com/1000.csv 施行例：www.example.com/1001.csv 元の値：www.example.com/taro/index.php 施行例1：www.example.com/jiro/index.php 施行例2：www.example.com/admin/index.php	URL	既存URLのフォルダーパス、ファイル名などから推測を行い、URLの一部を変更してアクセス	アクセス権限がない情報や機能が閲覧、操作できる	通常ユーザーではアクセス権限がない情報や機能へアクセスできない	
セッション管理の不備	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		セッションIDが格納されている箇所	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	
		ログイン前に機微情報がセッション変数に格納されていると想定できる箇所		セッションIDが格納されている箇所	機微情報を入力した後に新しいセッションIDが発行されるかを確認	機微情報入力前と同じセッションIDが継続して使用される場合	機微情報入力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	
	クロスサイトリクエストフォージェリ(CSRF)	登録、送信などの確定処理		パラメーター	①Cookieなどリクエストヘッダに含まれた値によって、セッション管理が行われている確定処理において、以下のいずれかの情報が含まれているかを確認 A. 利用者のパスワード B. CSRF対策トークン C. セッションID D. CAPTCHA ②A～Dが含まれている場合に、ユーザーαで利用されている値をユーザーβで利用されている値に変更してリクエストを送信し、処理が行われるか確認 ③A～Dが含まれている場合に、ユーザーαで利用されている値を削除、もしくはパラメーターごと削除してリクエストを送信し、処理が行われるか確認 ④Refererを削除、もしくは正規のURLではない値に変更して、リクエストを送信し、処理が行われるか確認	1) A～Dが含まれていない 2) A～Dが含まれているが、別ユーザーの値でも正常に処理が行われる 3) A～Dが含まれているが、値を削除、もしくはパラメーターごと削除した場合に処理が行われる 4) Refererチェックが行われていない	1) A～Dが含まれており、かつ、別ユーザーの値では正常に処理が行われない 2) A～Dが含まれており、かつ、値やパラメーターごと削除しても正常に処理が行われない 3) Refererチェックが行われており、正常に処理が行われない	※1 CAPTCHAチェックは推奨案ではないが、リスク低減になる ※2 Refererチェックは推奨案ではないが、リスク低減になる

			CSRF対策トークンを使用している箇所			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 ・ユーザーアカウントごとに差違の比較 ・同一ユーザーでログインするごとに差違の比較	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
		CookieのHttpOnly属性未設定	Cookie 発行処理			Set-CookieのHttpOnly属性が付与されているかを確認	レスポンスヘッダーの Set-Cookieヘッダーフィールド値に"HttpOnly"属性が指定されていない	レスポンスヘッダーの Set-Cookieヘッダーフィールド値に"HttpOnly"属性が指定されている	
		推測可能なセッションID	セッションID発行時			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 ・ユーザーアカウントごとに差異の比較 ・発行時の日時による差異の比較 ・発行回数による差異の比較	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
	情報漏洩	クエリーストリング情報の漏洩	すべて			セッションIDや機微情報がURLに含まれていないか確認	URLにセッションIDや機微情報が含まれている（同じスキームの）他サイトに遷移した際に、Refererヘッダーで内容が漏洩する。Webサーバーやプロキシーサーバーにログとして残る。）	URLにセッションIDや機微情報が含まれていない	
		キャッシュからの情報漏洩	機微情報が含まれる画面			レスポンス内で適切にキャッシュ制御を行っていることを確認	レスポンスヘッダーのCache-Controlヘッダーフィールド値に"no-store"が指定されていない	レスポンスヘッダーのCache-Controlヘッダーフィールド値に"no-store"が指定されている	
		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			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"である	
		画面表示上のマスク不備	全般			マスクすべき情報が画面上に表示されていないことを確認	マスクすべき情報が画面上に表示されている	マスクすべき情報が画面上に表示されていない	主なマスクすべき情報としてはクレジットカード番号やPINコード、パスワード
		HTTPS利用時のCookieのSecure属性未設定	Set-Cookieヘッダーフィールドがある箇所			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	レスポンスヘッダーの Set-Cookieヘッダーフィールド値に"Secure"属性が指定されていない	レスポンスヘッダーの Set-Cookieヘッダーフィールド値に"Secure"属性が指定されている	
		パスワードの平文保存	パスワードリセット			パスワードリセットを実行	登録したパスワードが表示される/メールで送られてくる	再設定画面に遷移する	平文なのか可逆暗号なのかは判断できない
			パスワード変更画面、管理者画面			パスワード変更画面、管理者画面にアクセス	登録したパスワードが表示される/inputタグに埋まっている	表示されない	平文なのか可逆暗号なのかは判断できない
		HTTPSの不備	全般			機微情報を取り扱うWebページ(フォームの表示、送信先共に)にアクセス	HTTPで通信している	HTTPSで通信している	
			HTTPS箇所			HTTPSを使用しているコンテンツを確認(HTTPおよびHTTPSの併用)	HTTPSだけでアクセスすべきページがHTTPでもアクセス可能となっている	HTTPS以外ではアクセスできない	
			HTTPS箇所			HTTPSを使用しているコンテンツを確認(HTTPとHTTPSの混在)	HTTPSとHTTPのコンテンツが混在している	HTTPSとHTTPのコンテンツが混在していない	
			HTTPS箇所			動作対象ブラウザーで証明書を確認	ブラウザーで証明書の警告が出る	ブラウザーで証明書の警告が出ない	警告が出る場合には以下のいずれかに該当する可能性がある ・自己証明書が用いられている ・有効期限が切れている ・証明書のホスト名がサイトと一致してない ・推奨されない署名アルゴリズムの利用 ・不適切な鍵長
		不要な情報の存在	すべて			HTMLやJavaScriptなどに「攻撃に有用な情報（設計やデータベース構造になどに係わる情報）」や「公開不要な情報（個人名、メールアドレス、ミドルウェアの情報、過去の公開していたコンテンツのリンク、プライベートIPアドレスなど）」が含まれていることを確認	情報が含まれている	情報が含まれていない	
Webアプリケーションの動作環境への診断項目	サーバソフトウェアの設定の不備	ディレクトリーリスティング	すべて		URL	Webサーバ上の発見したディレクトリーにアクセスして、ディレクトリー内のファイルが一覧表示されないかを確認	ディレクトリー内のファイルが一覧表示される	ディレクトリー内のファイルが一覧表示されない	含まれているファイルによってリスクは異なる
		バージョン番号表示	すべて			サーバーやアプリケーション、ミドルウェア、フレームワークなどのバージョン番号が表示されていないかを確認	バージョン番号が表示される	バージョン番号が表示されない	
		不要なHTTPメソッド(TRACE, TRACK)	すべて	TRACE、TRACK	リクエストメソッド	メソッドを変更してサーバーにアクセス	TRACE、TRACKメソッドが機能する	TRACE、TRACKメソッドが機能しない	
		不要なHTTPメソッド(OPTIONS)	すべて	OPTIONS	リクエストメソッド	メソッドを変更してサーバーにアクセス	Allowレスポンスヘッダーに GET、HEAD、POST、OPTIONS以外のメソッドが存在する（PUT、DELETE、TRACEなど）	Allowレスポンスヘッダーが存在しない Allowレスポンスヘッダーに GET、HEAD、POST、OPTIONS以外のメソッドが存在しない	
		公開不要な機能・ファイル・ディレクトリーの存在	すべて	.bak, .old, .org, file.html~, /admin/, /test/, test.html など	拡張子 / 既存ディレクトリー / ファイル名	サンプルファイルや、バックアップファイルなど、アプリケーションの動作に不必要なファイルの有無を確認 不特定多数に公開する必要がないファイルの有無を確認	該当するファイルがある	該当するファイルがない	