No.	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
1	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	パラメータ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
2				すべて	1/0	パラメータ	パラメータ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	
3				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	パラメータ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
4				型が数値のパラメータ	(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	パラメータ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
5				型が数値のパラメータ	(1)「(元の値:数値)」 (2)「(元の値)-0」 (3)「(元の値)-1」	パラメータ	パラメータ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	
6			コマンドインジェクション	すべて	|/bin/sleep 20|	パラメータ	パラメータ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				すべて	;/bin/sleep 20;	パラメータ	パラメータ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	
8				すべて	../../../../../../../bin/sleep 20|	パラメータ	パラメータ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	
9				すべて	;ping -nc 20 127.0.0.1;	パラメータ	パラメータ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	
10				すべて	&ping -nc 20 127.0.0.1&	パラメータ	パラメータ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	
11				すべて	$(../../../../../../../bin/sleep 20)	パラメータ	パラメータ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	
12			CRLFインジェクション	レスポンスヘッダに値を出力している箇所	%0d%0aSet-Cookie:(任意の値)%3D(任意の値)%3B	レスポンスヘッダに値を出力しているパラメータ	パラメータの値に検出パターンを挿入し、リクエストを送信	パラメータに改行が挿入され、新たなSet-Cookieヘッダ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ヘッダフィールド
13				レスポンスヘッダに値を出力している箇所	%0d%0a%0d%0akensa	レスポンスヘッダに値を出力しているパラメータ	パラメータ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ヘッダフィールド
14				メールメッセージのヘッダ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に値を出力しているパラメータ	パラメータ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
15			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	パラメータ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	
16				すべて	<script>alert(1)</script>	パラメータ	パラメータ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	
17				すべて	javascript:alert(1)	パラメータ	パラメータ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	
18				すべて	'+alert(1)+'	パラメータ	パラメータ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	
19				すべて	"onmouseover="alert(1)	パラメータ	パラメータ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	
20				URL	#">'><img src=x onerror=alert(1)>	パラメータ	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

No.	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
21		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	パラメータ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	
22				ファイル名を扱っている画面や機能	../../../../../../../../etc/hosts%00	パラメータ	パラメータ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	
23				ファイル名を扱っている画面や機能	../../../../../../../../windows/win.ini	パラメータ	パラメータ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	
24				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	パラメータ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	
25		XML外部エンティティ参照 (XXE)		リクエストにXMLが含まれている箇所	元の値： <?xml version="1.0" encoding="ISO-8859-1"?> <foo>test</foo> 試行例： <?xml version="1.0" encoding="ISO-8859-1"?> <!DOCTYPE foo [<!ELEMENT foo ANY > <!ENTITY xxe SYSTEM "file:///etc/hosts" >]><foo>&xxe;</foo>	XMLが格納されている箇所（パラメータ、ファイルなど）	XML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	指定する検出パターンの fooの箇所は実装に合わせて変更する 「OWASP Top10 2017」の改定を受けて追加（A4:XML外部エンティティ参照:XXE）
26				リクエストにXMLが含まれている箇所	元の値： <?xml version="1.0" encoding="ISO-8859-1"?> <foo>test</foo> 試行例： <?xml version="1.0" encoding="ISO-8859-1"?> <!DOCTYPE foo [<!ELEMENT foo ANY > <!ENTITY xxe SYSTEM "file:///c:/windows/win.ini" >]><foo>&xxe;</foo>	XMLが格納されている箇所（パラメータ、ファイルなど）	XML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	指定する検出パターンの fooの箇所は実装に合わせて変更する 「OWASP Top10 2017」の改定を受けて追加（A4:XML外部エンティティ参照:XXE）
27				リクエストにXMLが含まれている箇所	元の値： <?xml version="1.0" encoding="ISO-8859-1"?> <foo>test</foo> 試行例： <?xml version="1.0" encoding="ISO-8859-1"?> <!DOCTYPE foo [<!ELEMENT foo ANY > <!ENTITY xxe SYSTEM "http://example.com/" >]><foo>&xxe;</foo>	XMLが格納されている箇所（パラメータ、ファイルなど）	XMLに検出パターンを挿入し、リクエストを送信	http://example.com/ にアクセスが来る	http://example.com/ にアクセスが来ない	外部Webサーバを用意し、アクセスがログなどで確認できる必要がある 指定する検出パターンの foo, http://example.com の箇所は実装に合わせて変更する 「OWASP Top10 2017」の改定を受けて追加（A4:XML外部エンティティ参照:XXE）
28		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	パラメータ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ヘッダフィールド、METAタグのRefresh、JavaScriptコード（location.href、location.assign、location.replace）
29				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	パラメータ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ヘッダフィールド、METAタグのRefresh、JavaScriptコード（location.href、location.assign、location.replace）
30		シリアライズされたオブジェクト		すべて	シリアライズされた値（言語によってシリアライズ形式は変わります） ■PHPの場合 「a:4:{i:0;i:132;i:1;s:7:"Mallory";i:2;s:4:"user";i:3;s:32:"b6a8b3bea87fe0e05022f8f3c88bc960";}」のような値 ■Javaの場合 r00（小文字アール、大文字オー、数字0）から始まるBase64文字列 H4sIA（大文字エイチ、数字4、小文字エス、大文字アイ、大文字エー）から始まるBase64文字列		検出パターンがリクエストに含まれていないか確認	検出パターンが含まれている	検出パターンが含まれていない	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。 「OWASP Top10 2017」の改定を受けて追加（A8：安全でないデシリアライゼーション）
31		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	パラメータ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);
32		クリックジャッキング		確定処理の直前画面			レスポンスヘッダにX-Frame-Optionsヘッダ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	レスポンスヘッダにX-Frame-Optionsヘッダフィールドが存在し、値が「DENY」 「SAMEORIGIN」 「ALLOW-FROM (uri)」	

No.	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
33		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	認証状態を保持しているパラメータ（ex. authenticated=ueno、userid=1234）を特定し、パラメータ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	
34				ログイン機能		パラメータ	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	
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			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
37			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	同じユーザ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
38			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	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	
39				パスワード登録・変更	RfM9yY8Cwk	パラメータ	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	
40				パスワード登録・変更		パラメータ	ユーザ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	
41			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機能が存在しない	
42				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	
43			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	
44				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	ユーザ自身が新たなパスワードを設定する	
45		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	
46				認可制御が必要な箇所		パラメータ	登録データに紐づく値がパラメータ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として用いられている例：ユーザID、文書ID、注文番号、顧客番号など
47				認可制御が必要な箇所		パラメータ	hiddenパラメータや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	権限がパラメータとして用いられている例： func=admin など
48				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	
49				認可制御が必要な箇所	元の値：www.example.com/user1/profile.php 試行例：www.example.com/user2/profile.php 元の値：www.example.com/1000.csv 試行例：www.example.com/1001.csv 元の値：www.example.com/taro/index.php 試行例1：www.example.com/jiro/index.php 試行例2：www.example.com/admin/index.php	URL	既存URLのフォルダパス、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	
50		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	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αで利用されている値をユーザ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αで利用されている値を削除、もしくはパラメータ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
51				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 ・ユーザアカウントごとに差違の比較 ・同一ユーザ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
52		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	

No.	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
53				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	
54			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	レスポンスヘッダの Set-Cookieヘッダフィールド値に"HttpOnly"属性が指定されていない	レスポンスヘッダの Set-Cookieヘッダフィールド値に"HttpOnly"属性が指定されている	
55			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の規則性が伺らず推測不可	セッションIDが固定長でない場合は疑う余地がある
56		情報漏洩	クエリ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ヘッダで内容が漏洩する。Webサーバやプロキシーサーバにログとして残る。）	URLにセッションIDや機微情報が含まれていない	
57			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	レスポンスヘッダのCache-Controlヘッダフィールド値に"no-store"が指定されていない	レスポンスヘッダの Cache-Controlヘッダフィールド値に"no-store"が指定されている	
58			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	
59			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
60			HTTPS利用時のCookieのSecure属性未設定	Set-Cookieヘッダフィールドがある箇所			HTTPS利用時のSet-CookieヘッダフィールドにSecure属性があることを確認	レスポンスヘッダの Set-Cookieヘッダフィールド値に"Secure"属性が指定されていない	レスポンスヘッダの Set-Cookieヘッダフィールド値に"Secure"属性が指定されている	
61			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	
62				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	
63				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	
64				HTTPS箇所			動作対象ブラウザで証明書を確認	ブラウザで証明書の警告が出る	ブラウザ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
65			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	
66	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にアクセスして、ディレクトリ内のファイルが一覧表示されないかを確認	ディレクトリ内のファイルが一覧表示される	ディレクトリ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
67			バージョン番号表示	すべて			サーバ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	
68			不要なHTTPメソッド	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	
69			不要なHTTPメソッド	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にアクセス	Allowヘッダに GET、HEAD、POST、OPTIONS以外のメソッドが存在する（PUT、DELETE、TRACEなど）	Allowヘッダが存在しない Allowヘッダに GET、HEAD、POST、OPTIONS以外のメソッドが存在しない	
70		公開不要な機能・ファイル・ディレクトリの存在		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 / 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	