No. de /Sen	rh (\#ri	1.八朝	Main + 中華 - ・ も かか	27 m. 15 . 1641 29 . 37	40.16+ +, 62.2, 41.46	15, Mr. +-3+	整定をおする日本の公司 を定めるというというというというというというというというというというというというというと
No. 大分加 1 Webアプリケーションの施弱性	中分割 インジェクション	小分類 SQLインジェクション	診断を実施すべき箇所 すべて	ベイロード・検出パターン (シングルクォート)	機能を行う対象 パラメータ	診断方法 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	 総発性がある場合の組集 総発性がない場合 の日間達のエラーが表示され DB関連のエラーは表示 DB関連のエラー (SQL Syntax, SQL Exception, pg. seec., ORA-析数平、ODBC Driver Manager など は画面に実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、エラーが開端にでない場合では正常がと乗動が異なる でに正正常な 手動の指令と乗動が異なる でに正正常な 手動の指令と乗動が異なる でに正正常な 手動の指令と乗動が異なる でに正正常な 手動の指令と乗動が異なる でに正正常な 手動の手機を かあいまた。
							こともある ただし、この診断手法の態弱 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) 質される
3			すべて	(1) (完の値) (2) (完の値) and 'a'-'a j (3) (完の値) and 'a'-'b j	バラメータ	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 とは関一のレスポンスとな り、(2)と(3)で異なるレス ボンスが返ってくる (3) では、(3) では、(3) では、(4) では、(4) では、(5) では、
4			型が数値のパラメータ	(1) (元の体数節) (2) (元の値) and 1-1] (3) (元の値) and 1-0]	バラメータ	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 左記以外 「and 1-1」の形分がSQL文 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 「1-1」は常に賃(1)とな ポンスが返ってくる り、判定組果に影響しないた。 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)「(元の像: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)を送産して正常系の動作 を確認し、(1)を(2)を比較 して同一のレスポンスとな り、(2)を(3)で異なるレス ポンスが返せってくる
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 通常通りの応答速度でレ が20秒遅くなる 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 通常通りの応答速度でレ が20秒遅くなる 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 通常通りの応答速度でレ が20秒遅くなる 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 通常通りの応答速度でレ が20秒遅くなる 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 通常通りの応答速度でレ
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 通常通りの応答速度でレ
12			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	が20秒差くなる スポンが返ってくる パラメータに改行が挿入き 診断値所の後ろに改行き 主な診断対象はSet-Cookieや れ、新たなSet-Cookieへッ おすに検出パターンの文 locationへッダフィールド ダフィールドが挿入される 字列が表示される
13			レスポンスヘッダに値を出力している箇所	%0d%0akensa	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	タフィール Pawh、2は 6 字列を表示される パラメータに送行コードが 静断値所の後たに改行さ 2つ挿入され、「kensa」文 れずに検出パターンの文 字列がHTTPボディ部分に 景示される
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 エラーが発生するなど、 受信可能なメールアドレスを にメールが配送される メールが配送されない 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>X\$\$</s>	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 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 スケープされて挿入される 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 javascriptスキームとし 等に挿入され、javascript で有効にならない スキームとして有効になる
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 検出パターンが適切にエ ケープされずに挿入される 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 検出パターンが適切にエ ケープされずに挿入される スケープされで挿入され る
20			URL	#">'> 	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 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
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 されない

No. 大分類	中分類 小分類	診断を実施すべき箇所	ベイロード・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
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 /etc/hostsの内容が表示 れる されない	Ā
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 /windows/win.iniの内 表示される 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 /windows/win.iniの内 表示される 容が表示されない	
25	XML外部エンティティ参照 (XXE)	ラクエストにXMLが含まれている箇所	元の値: <pre></pre> <pre> <pre></pre> <p< td=""><td>XMLが格勢されている箇所(パラメー ク、ファイルなど)</td><td>XMLに検出バターンを挿入し、リクエストを送信</td><td>/etc/hostsの内容が表示さ れる えれない</td><td>採定する検出パターンの foo の簡所は実装に合わせて変更 する 「OWASP Top10 2017」の 定を受けて追加(A4:XML外 部エンティティ参照:XXE)</td></p<></pre>	XMLが格勢されている箇所(パラメー ク、ファイルなど)	XMLに検出バターンを挿入し、リクエストを送信	/etc/hostsの内容が表示さ れる えれない	採定する検出パターンの foo の簡所は実装に合わせて変更 する 「OWASP Top10 2017」の 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	> >-foo>&xe	XMLが格納されている箇所(パラメー タ、ファイルなど)	XMLに検出バターンを挿入し、リクエストを送信	/windows/win.iniの内容が /windows/win.iniの内容が 表示される 常が表示されない	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 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	プライン・ファイン・ファイン・ファイン・ファイン・ファイン・ファイン・ファイン・ファ	XMLが格納されている箇所(パラメー タ、ファイルなど)	XMLに検出バターンを挿入し、リクエストを送信	http://example.com/ に アクセスが来る 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 るを要がある 指定する検出バターンの foo http://example.com の箇所 は実装に合わせて変更する 「OWASP Top10 2017」の 定を受けて追加 (A4:XML外 能エンティティ参照: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 http://www.example. にリダイレクトされる omにリダイレクトされたない	c 指定する検出パターンのURL
29		リダイレクトが実行される顕語や機能	//www.example.com/	URL、もしくはURLの一部と想定され るバラメータ	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 http://www.example. にリダイレクトされる omにリダイレクトされ ない	c 指定する検出パターンのURL
30	シリアライズされたオブジェクト	\$~T	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:13:1::s:7:"Mallory":i:2:s:4:"user"):3::3:2:"b6a8 b3bea87ie0e05022f81c88bc960':]」のような値 ■Javaの場合 (00 (小文字アール、大文字オー、数字0) から始まるBase64 文字列 H4slA (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 検出パターンが含まれてい いない	
31	インクルードにまつわる脆弱 リモートファイルインクルージョン 性		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 ない	A部Webサーバを用意し、フ 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	確定処理の直前両面			レスポンス〜ッグにX-Frame-Options〜ッグ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 レスポンスヘッダにX- フィールドがない/製造 Frame-Optionsヘッダ 「DENY」 「SAMEORIGIN」 が「DENY」 「ALLOW-FROM (uri)」で「SAMEORIGIN」 はない、イスLOW-FROM (uri)」で「ALLOW-FROM (uri)」で「MALOW-FROM (uri)」で「M	
33	88年 總和回避	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	認証後のページを指定する 認証後のページを指定す	
4		ログイン機能		パラメータ	ス 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	る ない 認証が成功する 認証に失敗する	

No. 大分類	中分割	小分類	診断を実施すべき箇所	ペイロード・輸出パターン	操作を行う対象	除断方法	脆弱性がある場合の結果	胎弱性がたい場合 備者
35 人分類	十刀飛	ログアウト機能の不備や未実装	ログアウト機能	7~7 ロード・使山バラーン	採作を行り対象	ログアウト機能が存在するかを確認	即列生がある場合の和米 ログアウト機能が存在しな	
						The state of the s	V)	8
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	認証状態でしかアクセスで	認証状態でしかアクセス ログアウト機能の実行時に
						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		できない画面や機能にア セッションIDが破棄されてい
							スできる(ログイン状態に	クセスできない (ログイ) ない場合に発生する
27		過度な認証試行に対する対策不備や未実装	ロガイン操作		パラメータ	同じユーザタでパスワードを連続して10回開金えて確認	なる) アカウントロックさわかい	ン状態にならない) アカウントロックされる 試行するパスワードはパス
31		地及な認証時日に対する対象不開で未来教	1971 2 MRHG		\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\	同じユーリ名でパスケートを座載して10回間座えて機能) ガラントロック G4D4V	ワードポリシーに従うこと
								1 1171 1127 1
38		脆弱なパスワードポリシー	パスワード登録・変更	(空)	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	脆弱なパスワードが登録・	脆弱なパスワードが登
				1234567		在でない文字列を登録・変更できないことを確認	変更できる	録・変更できない
				abcdefg				
20			パスワード登録・変更	abcd123 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	we do a section of the day of	登録・変更できる
39			ハヘシート立脉・変更	RIMSYTOCWK	\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\	が混在している文字列を登録・変更できることを確認	立跡・変更できない	豆林・東丈できる
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	脆弱な(推測可能な)パス
							ワードが設定できる	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	パスワードリマインダ機
							てくる	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
42		パスワードリセットの不備	パスワードリセット			を確認 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	理の込まれている ユーザ本人しか受け取れな	4. 4.
		1727131111	1,000			TO TO TO TO THE WITHOUT THE WARRENCE OF THE COMMO		ない連絡先に再設定方法
							知されずにパスワードのリ	
							セットが可能	
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	ワードが送付され、そのま	ワードを設定する
ar.	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	ま使い続けられる	アクセス権限がない情報
45	お可制御の不無		85円制御か必要な国所		URL	権限の異なる後数のユーザで、本来権限のない機能のURLにアクセス	ガクセス権限がない情報や 機能が閲覧、操作できる	
							DESIGNATION THAT CO.D.	the control of the co
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	当該ユーザではアクセス権	当該ユーザではアクセス 登録データに紐づく値がパラ
						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	限がない情報や機能へアク	権限がない情報や機能へ メータとして用いられている
							セスできる	アクセスできない 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	当該ユーザではアクセス権限がない情報や機能が関	
						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	版かない情報や機能が周 覧、操作できる	権限がない情報や機能が られている例: 閲覧、操作できない func-admin など
48			認可制御が必要な箇所		URL			
48			認可制御が必要な箇所		URL		認証後のページを指定する ことでアクセスが可能であ	認証後のページを指定す
48						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 認可制御が必要な箇所	元の框:www.example.com/user1/profile.php	URL 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 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	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 アクセス権限がない情報や	認証後のベージを指定す ることでアクセスができ ない 通常ユーザではアクセス
49				元の値:www.example.com/user1/profile.php 践行例:www.example.com/user2/profile.php		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 適常ユーザではアクセス 権限がない情報や機能へ
49				試行例: www.example.com/user2/profile.php		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 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	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 アクセス権限がない情報や	認証後のベージを指定す ることでアクセスができ ない 通常ユーザではアクセス
49				試行例:www.example.com/user2/profile.php 元の値:www.example.com/1000.csv		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 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	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 アクセス権限がない情報や	認証後のページを指定す ることでアクセスができ ない 適常ユーザではアクセス 権限がない情報や機能へ
49				試行例: www.example.com/user2/profile.php		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 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	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 アクセス権限がない情報や	認証後のページを指定す ることでアクセスができ ない 適常ユーザではアクセス 権限がない情報や機能へ
49				試行例:www.example.com/user2/profile.php 元の値:www.example.com/1000.csv		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 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	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 アクセス権限がない情報や	認証後のページを指定す ることでアクセスができ ない 適常ユーザではアクセス 権限がない情報や機能へ
49				対行例: www.example.com/user2/profile.php 元の値: www.example.com/1000.csv 対行何: www.example.com/1001.csv 元の値: www.example.com/taro/index.php 剥行列: www.example.com/jiro/index.php		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 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	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 アクセス権限がない情報や	認証後のページを指定す ることでアクセスができ ない 適常ユーザではアクセス 権限がない情報や機能へ
49			認可制御が必要な箇所	終行例:www.example.com/user2/profile.php 元の値:www.example.com/1000.csv 終行例:www.example.com/1001.csv 元の値:www.example.com/taro/index.php	URL	認証状態でしか表示できないページに、ロダイン認証していない状態でアクセス 既存URLのフォルダバス、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	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 る アクセス権限がない情報や 機能が閲覧、操作できる	要証後のページを指定す ることでプクセスができ ない 通常ルーザではアクセス 権限がない情報や機能へ アクセスできない
49	クロスサイトリクエストフォ	→ ージェ y (CSRF)		対行例: www.example.com/user2/profile.php 元の値: www.example.com/1000.csv 対行何: www.example.com/1001.csv 元の値: www.example.com/taro/index.php 剥行列: www.example.com/jiro/index.php		製造状態でしか表示できないページに、ロダイン製造していない状態でアクセス 既存URLのフォルダバス、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 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	認証後のページを指定する ことでアウセスが可能である ろ アクセス権限がない情報や 機能が閲覧、操作できる 1) A~Dが含まれていない	製産級のページを指定す ることでアクセスができ ない 通常ユーザではアクセス 機関がない情報や機能へ アクセスできない 1) A ~ Dが含まれてお 祭1 CAPTCHAチェックは接奨
49	クロスサイトリクエストフォ	rージェリ(CSRF)	認可制御が必要な箇所	対行例: www.example.com/user2/profile.php 元の値: www.example.com/1000.csv 対行何: www.example.com/1001.csv 元の値: www.example.com/taro/index.php 剥行列: www.example.com/jiro/index.php	URL	認証状態でしか表示できないページに、ロダイン認証していない状態でアクセス 既存URLのフォルダバス、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	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 る アクセス権限がない情報や 機能が閲覧、操作できる 1) A~Dが含まれていない 2) A~Dが含まれていない 2) A~Dが含まれている	要証券のページを指定す ることでアクセスができ ない 通常ルーザではアクセス 権限がない情報や機能へ アクセスできない 1) A~Dが含まれてお 申1 CAPTCHAチェックは振奨 り、かつ、別ユーザの飯 案ではないが、リスク板域に
49 50	クロスサイトリクエストフォ) ージェ Ϳ (CSRF)	認可制御が必要な箇所	対行例: www.example.com/user2/profile.php 元の値: www.example.com/1000.csv 対行何: www.example.com/1001.csv 元の値: www.example.com/taro/index.php 剥行列: www.example.com/jiro/index.php	URL	製造状態でしか表示できないページに、ロダイン製造していない状態でアクセス 既存URLのフォルダバス、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 ②Cookie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 われている確定地理において、以下のいずれかの情報が含まれているかを確 影	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 る アクセス権限がない情報や 機能が閲覧、操作できる 1) A~Dが含まれていない 2) A~Dが含まれていない 2) A~Dが含まれている	製産級のページを指定す ることでアクセスができ ない 通常ユーザではアクセス 機関がない情報や機能へ アクセスできない 1) A ~ Dが含まれてお 祭1 CAPTCHAチェックは接奨
49 50	クロスサイトリクエストフォ	+ージェリ (CSRF)	認可制御が必要な箇所	対行例: www.example.com/user2/profile.php 元の値: www.example.com/1000.csv 対行何: www.example.com/1001.csv 元の値: www.example.com/taro/index.php 剥行列: www.example.com/jiro/index.php	URL	製造状態でしか表示できないページに、ロダイン製造していない状態でアクセス 既存URLのフォルダバス、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 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	超級扱いページを指定する ことでアクセスが可能である ろ アクセス練限がない情報や 機能が閲覧、操作できる 1) AーDが含まれていない 2) AーDが含まれていない 3) スーDか含まれている 3、別ユーザの値でも主常	製造機のページを指定す ることでアクセスができ ない 適常ユーザではアクセス 機能がない情報機能へ アクセスできない 1) AーDが含まれてお
49 50	ク ロスサイトリクエストフォ	rージェリ(CSRF)	認可制御が必要な箇所	対行例: www.example.com/user2/profile.php 元の値: www.example.com/1000.csv 対行何: www.example.com/1001.csv 元の値: www.example.com/taro/index.php 剥行列: www.example.com/jiro/index.php	URL	設証状態でしか表示できないページに、ロダイン認証していない状態でアクセス 医存URLのフォルダバス、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 ①Cookieなどリクエストペ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 私利用者のパスワード	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 ろ アクセス権限がない情報や 機能が閲覧、操作できる 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	要証券のページを指定す ることでアケセルができ ない 通常ユーザではアクセス 機能がない情報や構能へ アクセスできない 1) A~Dが含まれてお り、かつ、別ユーザの値 変ではないが、リスク低減に では正常に処理が行われ、なる ない ※2 Refererチェックは機災を 後と Refererチェックは機災を をおくなる
49	クロスサイトリクエストフォ	÷ージェリ (CSRF)	認可制御が必要な箇所	対行例: www.example.com/user2/profile.php 元の値: www.example.com/1000.csv 対行何: www.example.com/1001.csv 元の値: www.example.com/taro/index.php 剥行列: www.example.com/jiro/index.php	URL	製能状態でしか表示できないページに、ロダイン認能していない状態でアクセス 既存URLのフォルダバス、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 ②Cookieなどリクエストペッダに含まれた値によって、セッション管理が引 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	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 ろ アクセス様限がない情報や 機能が閲覧、操作できる 1) A~Dが含まれている が、別コーザの値でも正常 に処理が行われている が、値を削削、もしてはパ フメータンと削除した場合	認証後のページを指定す ることでアケセスができ ない 遺産ユーザではアクセス 権限がない情報や構能へ アクセスできない \$31 CAPTCHAチェックは推奨 カ、かつ、別ユーザの値 なる ない 2) Aーのが含まれてお カ、かつ、別ユーザの値 なる ない では正常に処理が行われ、なる ない では、が、リスク低減に では、が、リスク低減に ない。 では、が、リスク低減に では、が、リスク低減に では、が、リスク低減に では、が、リスク低減に では、が、リスク低減に では、アンとが開たしても正常に
49 50	クロスサイトリクエストフォ	+−ジェリ(CSRF)	認可制御が必要な箇所	対行例: www.example.com/user2/profile.php 元の値: www.example.com/1000.csv 対行何: www.example.com/1001.csv 元の値: www.example.com/taro/index.php 剥行列: www.example.com/jiro/index.php	URL	製造状態でしか表示できないページに、ロダイン製造していない状態でアクセス 度存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 関してアクセス ②Cookie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 器 長 利用者の対ストーノ C. セッションID D. CAPTCHA ②Aトのかさまれている場合に、ユーザαで利用されている値をユーザβで料	超延度のページを指定する ことでアクセスが可能である。 ろった。 アクセス様限がない情報や 機能が閲覧、操作できる リカーのか含まれているい、別ユーツの値でも正常 に処理が行われる 3) A のからまれているが、値を削除、もしくはパ フメータごと削除した場合 に処理が行われる	製造機のページを指定す ることでアクセスができ ない 通常ユーザではアクセス 機能がない情報機能へ アクセスできない 1) AーDが含まれてお り、かつ、別ユーザの値 家ではないが、リスク低減に では正常に処理がわれたな ない 変 Refererチェックは機災変 ではないが、リスク低減に ない り、たい。観やパラメー ろごと削削しても正常に 処理が行われない
49 50	クロスサイトリクエストフォ	ŧージェリ(CSRF)	認可制御が必要な箇所	対行例: www.example.com/user2/profile.php 元の値: www.example.com/1000.csv 対行何: www.example.com/1001.csv 元の値: www.example.com/taro/index.php 剥行列: www.example.com/jiro/index.php	URL	製鉱状態でしか表示できないページに、ロダイン認証していない状態でアクセス 版作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 関してアクセス 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 用ま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	超延度かページを指定する ことでアクセスが可能である 万クセス様限がない情報や 機能が関策、操作できる 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 に処理が打される 3) A~Dが含まれている が、値を削除。 してはパ フメータごと削除した場合 に処理が打される 4) Refererチェックが行わ 4) Refererチェックが行わ	及延後のページを指定す ることでアケセスができ ない 通常ユーザではアクセス 機能がない情報や機能へ アクセスできない 1) A~Dが含まれてお 切、かつ、別ユーザの値、窓ではないが、リスク低域に では正常に処理が行われな など 2 Refererチェックは推奨等 ではないが、リスク低域にな カンとも開始しても正常に 処理が行われない 3) Refererチェックが行
49 50	クロスサイトリクエストフォ	÷−ジェリ(CSRF)	認可制御が必要な箇所	対行例: www.example.com/user2/profile.php 元の値: www.example.com/1000.csv 対行何: www.example.com/1001.csv 元の値: www.example.com/taro/index.php 剥行列: www.example.com/jiro/index.php	URL	製造状態でしか表示できないページに、ロダイン製造していない状態でアクセス 度存URLのフォルダバス、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 ②Cookia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 総 利用者のバスワード B、CSRF対策トーフン C、セッションID O、CAPでIMA ②Aへ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活信し、処理が行われる小確認 (湯へのか含まれている場合に、ユーザαで利用されている値を削らしく	超延度かページを指定する ことでアクセスが可能である 万クセス様限がない情報や 機能が関策、操作できる 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 に処理が打される 3) A~Dが含まれている が、値を削除。 してはパ フメータごと削除した場合 に処理が打される 4) Refererチェックが行わ 4) Refererチェックが行わ	製産機のページを指定す なことでアクセスができ ない 通常コーザではアクセス 観察ない情報機能へ アクセスできない 3) AーOが含まれてお 申1 CAPTCHAチェックは推奨 の、かつ、別ユーザの額 定ではないが、リスク転続に では正常に製造が行われな ない 次2 Refererチェックは機災案 ではないが、リスク転減にな の、かつ、値やパラメー る ンと目開放しても正常に 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
49 50	クロスサイトリクエストフォ	+−ジェリ(CSRF)	認可制御が必要な箇所	対行例: www.example.com/user2/profile.php 元の値: www.example.com/1000.csv 対行何: www.example.com/1001.csv 元の値: www.example.com/taro/index.php 剥行列: www.example.com/jiro/index.php	URL	製造状態でしか表示できないページに、ロダイン製造していない状態でアクセス 版作URLのフォルダバス、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 ②Cookie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 お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 製 A 利用者のバスワード B. CSRF対策トークン C. セッションID O. CAPではA ②Aへの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へ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カー・サ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 (④AへDが含まれている場合に、ユーザので利用されている値を対策、もし はバラメータごと前除してリクエストを送信し、処理が行われるか確認	超延度かページを指定する ことでアクセスが可能である 万クセス様限がない情報や 機能が関策、操作できる 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 に処理が打される 3) A~Dが含まれている が、値を削除。 してはパ フメータごと削除した場合 に処理が打される 4) Refererチェックが行わ 4) Refererチェックが行わ	及延後のページを指定す ることでアケセスができ ない 通常ユーザではアクセス 機能がない情報や機能へ アクセスできない 1) A~Dが含まれてお 切、かつ、別ユーザの値、窓ではないが、リスク低域に では正常に処理が行われな など 2 Refererチェックは推奨等 ではないが、リスク低域にな カンとも開始しても正常に 処理が行われない 3) Refererチェックが行
49 50	クロスサイトリクエストフォ	rージェリ(CSRF)	認可制御が必要な箇所	対行例: www.example.com/user2/profile.php 元の値: www.example.com/1000.csv 対行何: www.example.com/1001.csv 元の値: www.example.com/taro/index.php 剥行列: www.example.com/jiro/index.php	URL	製造状態でしか表示できないページに、ロダイン製造していない状態でアクセス 度存URLのフォルダバス、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 ②Cookia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 総 利用者のバスワード B、CSRF対策トーフン C、セッションID O、CAPでIMA ②Aへ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活信し、処理が行われる小確認 (湯へのか含まれている場合に、ユーザαで利用されている値を削らしく	超延度かページを指定する ことでアクセスが可能である 万クセス様限がない情報や 機能が関策、操作できる 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 に処理が打される 3) A~Dが含まれている が、値を削除。 してはパ フメータごと削除した場合 に処理が打される 4) Refererチェックが行わ 4) Refererチェックが行わ	製産機のページを指定す なことでアクセスができ ない 通常コーザではアクセス 観察ない情報機能へ アクセスできない 3) AーOが含まれてお 申1 CAPTCHAチェックは推奨 の、かつ、別ユーザの額 定ではないが、リスク転続に では正常に製造が行われな ない 次2 Refererチェックは機災案 ではないが、リスク転減にな の、かつ、値やパラメー る ンと目開放しても正常に 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
50 51	クロスサイトリクエストフォ	r−ジェリ(CSRF)	認可制御が必要な箇所	対行例: www.example.com/user2/profile.php 元の値: www.example.com/1000.csv 対行何: www.example.com/1001.csv 元の値: www.example.com/taro/index.php 剥行列: www.example.com/jiro/index.php	URL	設証状態でしか表示できないページに、ロダイン認証していない状態でアクセス 版存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 ①Cookieなどリクエストペ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 ②本へか浴さまれている場合に、ユーザαで利用されている値をユーザルです。 ③本のか浴さまれている場合に、ユーザαで利用されている値を利能、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 ③本へか浴さまれている場合に、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 ③本のか浴さまれている場合に、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ウエストを送信し、処理が行われるか確認	超越接かべージを指定する ことでアクセスが可能である ろ フクセス様限がない情報や 機能が閲覧、操作できる 1) AーDが含まれていない 2) AーDが含まれている が、別ユーザの値でも正常 3) AーDが含まれている が、別エサの値でも正常 3) AーDが含まれている が、値を削除した場合 に処理が行われる 3) AーDが含まれている が、値を削除した場合 に処理が行われる 4) Refererチェックが行わ れていない	製造機のページを指定す ることでアクセスができ ない 通常ユーザではアクセス 機能がない情報機能へ アクセスできない 第1 CAPTCHAチェックは推奨 り、かつ、別ユーザの値 変ではないが、リスク低減に では正常に処理がわれ ない 変 Refererチェックは横災 ウ かつ、値やパラメー クごを削削しても正常に 効果を修作する の、かつ、値やパラメー が自動しても正常に 対象を修作する の、おのではないが、リスク低減に ない 対象を修作する 対象を修作する が行われない 対象を修作する が行われない が、リスを機能 が行われない 対象を修作する が行われない が、リスを機能 が行われない 対象を修作する が行われない
49 50 51	クロスサイトリクエストフォ	+−ジェリ(CSRF)	認可制御が必要な箇所 登録、送信などの確定処理	対行例: www.example.com/user2/profile.php 元の値: www.example.com/1000.csv 対行何: www.example.com/1001.csv 元の値: www.example.com/taro/index.php 剥行列: www.example.com/jiro/index.php	URL	型級技能でしか表示できないページに、ロダイン認証していない状態でアクセス 度存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 ①Cookieなどリクエスト〜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 私 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へのか含まれている場合は、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 (②Aへのか含まれている場合が、ユーザαで利用されている値を加ました。 はパテンターダンと削除してリクエストを送信し、処理が行われるか確認 (②Aへのか含まれている場合が後、もしくなアクエストを送信し、処理が行われるか確認 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対策トークンを複数集めて現りにないません。	超越接かべージを指定する ことでアクセスが可能である ろ フクセス様限がない情報や 機能が閲覧、操作できる 1) AーDが含まれていない 2) AーDが含まれている が、別ユーザの値でも正常 3) AーDが含まれている が、別エサの値でも正常 3) AーDが含まれている が、値を削除した場合 に処理が行われる 3) AーDが含まれている が、値を削除した場合 に処理が行われる 4) Refererチェックが行わ れていない	製造機のページを指定す ることでアクセスができ ない 通常ユーザではアクセス 機能がない情報機能へ アクセスできない 第1 CAPTCHAチェックは推奨 り、かつ、別ユーザの値 変ではないが、リスク低減に では正常に処理がわれ ない 変 Refererチェックは横災 ウ かつ、値やパラメー クごを削削しても正常に 効果を修作する の、かつ、値やパラメー が自動しても正常に 対象を修作する の、おのではないが、リスク低減に ない 対象を修作する 対象を修作する が行われない 対象を修作する が行われない が、リスを機能 が行われない 対象を修作する が行われない が、リスを機能 が行われない 対象を修作する が行われない
50 50	クロスサイトリクエストフォ	rージェリ(CSRF)	認可制御が必要な箇所 登録、送信などの確定処理	対行例: www.example.com/user2/profile.php 元の値: www.example.com/1000.csv 対行何: www.example.com/1001.csv 元の値: www.example.com/taro/index.php 剥行列: www.example.com/jiro/index.php	URL	型級状態でしか表示できないページに、ロダイン認証していない状態でアクセス 版作URLのフォルダバス、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 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 お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 個 A 利用者のバスワード B. CSRF対策トークン C. セッションID D. CAPTCHA ②Aへ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へDが含まれている場合に、ユーザので利用されている値を判断、もしく はバラメータごと開除してリクエストを送信し、処理が行われるか確認 ②AをBriefathの解しているようと必能し、処理が行われるの確認 ②AをBriefathの解しているにない値に変更して、リクエストを 送信し、処理が行われるの確認 ②をRefereを削除、もしくは正規のJRLではない値に変更して、リクエストを 送信し、気部が行われるの確認 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	超延度かページを指定する ことでアクセスが可能である アクセス権限がない情報や 機能が関策、操作できる 1) A~Dが含まれていない 2) A~Dが含まれていない 2) A~Dが含まれている に処理が行われる 3) A~Dが含まれている に処理が行われる 4) RefereFェックが行われていない な、値を削除した場合 た処理が行われる 4) RefereFェックが行われていない	型産級のページを指定す ることでアクセスができ ない 通常ユーザではアクセス 機能がない情報や機能へ アクセスできない 1) A~Dが含まれてお の、かつ、別ユーザの値、変ではないが、リスク低域に では正常に処理が行われな が2 Refererチェックは機関薬 ではないが、リスク低域にな り、かつ、健やパラメー のどの開除しても正常に 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 CSRF対策トークンの規 CSRF対策トークンの規 CSRF対策トークンの規 CSRF対策トークンが固定長で
50			認可制御が必要な箇所 登録、送信などの確定処理 CSRF対策トークンを使用している箇所	対行例: www.example.com/user2/profile.php 元の値: www.example.com/1000.csv 対行何: www.example.com/1001.csv 元の値: www.example.com/taro/index.php 剥行列: www.example.com/jiro/index.php	URL バラメータ	製造状態でしか表示できないページに、ロダイン製造していない状態でアクセス 度存URLのフォルダバス、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 ②Cookia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 緩 利用者のパスワード B、CSRF対策トークン C、セッションID C、APTCHA ②AへDが含まれている場合に、ユーザョ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运信し、処理が行われるか確認 (3人への合きまれている場合に、ユーザョで利用されている値を削削。もしては工作メータごと削削してリクエストを运信し、処理が行われるか確認 CSRF対策トークンを推動して規則性があることを確認し、CSRF対策トークンを推動して規則性があることを確認し、CSRF対策トークンを推動して、サンを推動して現別性があることを確認し、CSRF対策トークンを推動して規則性があることを確認し、CSRF対策トークンを推動して、場合におきないた。 同ニューザアカウトごとに恋遊の比較	超越後のページを指定する ことでアセスが可能である うとでアセスが可能である。 アクセス権限がない情報や 機能が閲覧、操作できる は、関立が行かれる が、別ユーザの値でも正常 が、別ユーザの値でも正常 が、別ユーザの値でも正常 が、他を削除、もしくはパ くり、 といったが行われる は、 といったが行われる は、 といったが行われる は、 といったが行われる は、 といったが行かれる は、 といったが行われる は、 といったが行われる は、 といったが行われる は、 といったが行われる は、 といったが行われる は、 といったが行われる は、 といったが行われる は、 といったが行われる は、 といったが行われる は、 といったが行われる は、 といったが行われる は、 といったが行われる は、 といったが行われる は、 といったが行われる は、 といったが行われる は、 といったが行われる は、 といったが行かた。 といったが行かに といったが行かた。 といったが行かに といったが といったが といったが といったが といったが といったが といったが といったが といったが といったが といったが といったが といったが といったが といったが といったが といったが といったが といったが といった といった といった といった といった といった といった といった	製産機のページを指定す ることでアクセスができ ない 通常コーザではアクセス 組織ないに特殊機能へ アクセスできない 3) A〜Oが含まれてお の、かつ、別ユーザの値 変ではないが、リスク転続に では正常に発展が計われた ない 変と Refererチェックは推奨を ではないが、リスク転続に なり、かつ、値やパラメー る っと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 3) Refererチェックが行 われており、正常に処理 が行われない CSRF対策トークンが固定長で 関性が何らず推薦不可 ない場合は疑う余地がある
50 50 51	クロスサイトリクエストフォ	セッションフィクセイション(セッション周	認可制御が必要な箇所 登録、送信などの確定処理 CSRF対策トークンを使用している箇所	対行例: www.example.com/user2/profile.php 元の値: www.example.com/1000.csv 対行何: www.example.com/1001.csv 元の値: www.example.com/taro/index.php 剥行列: www.example.com/jiro/index.php	URL	型級状態でしか表示できないページに、ロダイン認証していない状態でアクセス 版作URLのフォルダバス、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 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 お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 個 A 利用者のバスワード B. CSRF対策トークン C. セッションID D. CAPTCHA ②Aへ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へDが含まれている場合に、ユーザので利用されている値を判断、もしく はバラメータごと開除してリクエストを送信し、処理が行われるか確認 ②AをBriefathの解しているようと必能し、処理が行われるの確認 ②AをBriefathの解しているにない値に変更して、リクエストを 送信し、処理が行われるの確認 ②をRefereを削除、もしくは正規のJRLではない値に変更して、リクエストを 送信し、気部が行われるの確認 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	超起機かページを指定する ことでアクセスが可能である ろ アクセス体限がない情報や 機能が閲覧、操作できる 1) AーDが含まれている 以 別ユー切の信さ上下 3) AーDが含まれている が、別ユーサの信でも正常 に処理が行われる 3) AーDが含まれている が、仮を削除、もしくはバ フメータンと削除した場合 に処理が行われる 4) Refererチェックが行わ れていない していない していない していない ログイン成功前と同じセッ	型度級のページを指定す ることでアクセスができ ない 通常ユーザではアクセス 連常スーザではアクセス 機能がない情報機能へ アクセスできない 第1 CAPTCHAチェックは推奨 り、かつ、別ユーザの値 変ではないが、リスク低減に では正常に処理が行われ ない 2) A~Dが含まれてお っ、かつ、銀や・ヴァメー のどと削除しても正常に 対策と解や・デェックは構奨室 ではないが、リスク低減にな 3) Refererチェックが行 われており、正常に処理 が行われてが CSRF対策トータンの規 CSRF対策トータンの規 CSRF対策トータンの規 ログイン成功後に新しい
50 50 51			認可制御が必要な箇所 登録、送信などの確定処理 CSRF対策トークンを使用している箇所	対行例: www.example.com/user2/profile.php 元の値: www.example.com/1000.csv 対行何: www.example.com/1001.csv 元の値: www.example.com/taro/index.php 剥行列: www.example.com/jiro/index.php	URL バラメータ	製造状態でしか表示できないページに、ロダイン製造していない状態でアクセス 度存URLのフォルダバス、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 ②Cookia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 緩 利用者のパスワード B、CSRF対策トークン C、セッションID C、APTCHA ②AへDが含まれている場合に、ユーザョ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运信し、処理が行われるか確認 (3人への合きまれている場合に、ユーザョで利用されている値を削削。もしては工作メータごと削削してリクエストを运信し、処理が行われるか確認 CSRF対策トークンを推動して規則性があることを確認し、CSRF対策トークンを推動して規則性があることを確認し、CSRF対策トークンを推動して、サンを推動して現別性があることを確認し、CSRF対策トークンを推動して規則性があることを確認し、CSRF対策トークンを推動して、場合におきないた。 同ニューザアカウトごとに恋遊の比較	超延度かページを指定する ことでアクセスが可能である アクセス権限がない情報や 機能が関策、操作できる リカーのが含まれていない は、別ユーザの値でも正常 に処理が行われる 3) みーのか含まれている は、別エーザの値でも正常 に処理が行われる 4) 低を削除した場合 は処理が行われる 4) Refererチェックが行われていない ないない センボルカリ推測可能 ログイン成功前と同じセッション川が確核して使用さ	型産級のページを指定す ることでアクセスができない 通常ユーザではアクセス 機能がない情報や機能へ アクセスできない 1) A~Dが含まれてお の、かつ、別ユーザの紙 窓ではないが、リスク低減に では正常に処理が行われな 窓 2 Refererチェックは機関素 ではないが、リスク低減にな 3) Refererチェックに機関素 ではないが、リスク低減にな 3) Refererチェックが行 われており、正常に処理 が行われない CSRF対策トークンの規 関性が利らず推測不可 ない場合は疑う余地がある
50 50 51		セッションフィクセイション(セッション周	認可制御が必要な箇所 登録、送信などの確定処理 CSRF対策トークンを使用している箇所	対行例: www.example.com/user2/profile.php 元の値: www.example.com/1000.csv 対行何: www.example.com/1001.csv 元の値: www.example.com/taro/index.php 剥行列: www.example.com/jiro/index.php	URL バラメータ	製造状態でしか表示できないページに、ロダイン製造していない状態でアクセス 度存URLのフォルダバス、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 ②Cookia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 緩 利用者のパスワード B、CSRF対策トークン C、セッションID C、APTCHA ②AへDが含まれている場合に、ユーザョ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运信し、処理が行われるか確認 (3人への合きまれている場合に、ユーザョで利用されている値を削削。もしては工作メータごと削削してリクエストを运信し、処理が行われるか確認 CSRF対策トークンを推動して規則性があることを確認し、CSRF対策トークンを推動して規則性があることを確認し、CSRF対策トークンを推動して、サンを推動して現別性があることを確認し、CSRF対策トークンを推動して規則性があることを確認し、CSRF対策トークンを推動して、場合におきないた。 同ニューザアカウトごとに恋遊の比較	超起機かページを指定する ことでアクセスが可能である ろ アクセス体限がない情報や 機能が閲覧、操作できる 1) AーDが含まれている 以 別ユー切の信さ上下 3) AーDが含まれている が、別ユーサの信でも正常 に処理が行われる 3) AーDが含まれている が、仮を削除、もしくはバ フメータンと削除した場合 に処理が行われる 4) Refererチェックが行わ れていない していない していない していない ログイン成功前と同じセッ	製産機のページを指定す ることでアクセスができ ない。 通常ユーザではアクセス 機能がない情報機能へ アクセスできない 1) AーDが含まれてお り、かつ、別ユーザの値 変ではないが、リスク低機に では正常に処理がわれた ない ではないが、リスク低機に なり、かつ、観やパラメー クごを所われない 3) Refererチェックは機関案 ではないが、リスク低機にな り、かつ、観やパラメー クごを所能しても正常に 30 Refererチェックが行 われており、正常に処理 が行われない CSRF対策トークンの規 関性が利らず推測不可 ない場合は疑う余地がある ログイン成功機に新しい セッション/IDが操行され、古いセッション/IDが操行さ れ、古いセラッション/IDは
50 50 51 53		セッションフィクセイション(セッション周	認可制御が必要な箇所 登録、送信などの確定処理 CSRF対策トークンを使用している箇所	終行何: www.example.com/user2/profile.php 元の値: www.example.com/1000.csv 終行何: www.example.com/1001.csv 元の値: www.example.com/taro/index.php 終行何: www.example.com/jiro/index.php 終行何2: www.example.com/jiro/index.php	URL バラメータ	型級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 既存URLのフォルグパス、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 「Cookieなどリクエスト〜ッグに含まれた値によって、セッション管理が付ま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 あ A 別用者のパスワード B、CSRF対策トークン C、セッションID O、Aの子びもまれている場合に、ユーザαで利用されている値をユーザ身で利用されている値を対してリクエストを送信し、処理が行われるか確認 (3人へのが含まれている場合に、ユーザαで利用されている値を利削、してパテメータ上で削除してリクエストを送信し、処理が行われるの確認 (3人を別からまれている場合に、ユーザの日常れている値を別所、してパテメータ上で削除してリクエストを送信し、処理が行われるの確認 (3人の子がきないの場合と、ステリカルのと呼吸)にリクエストを送信し、処理が行われるの確認 CSRF対策トークンを推測 こSRF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 コーザでログインですることに完達の比較 い同ニューザでログインであるとと確認	超延度かページを指定する ことでアクセスが可能である アクセス権限がない情報や 機能が関策、操作できる リカーのが含まれていない は、別ユーザの値でも正常 に処理が行われる 3) みーのか含まれている は、別エーザの値でも正常 に処理が行われる 4) 低を削除した場合 は処理が行われる 4) Refererチェックが行われていない ないない センボルカリ推測可能 ログイン成功前と同じセッション川が確核して使用さ	型度級のページを指定することでアクセスができない 通常ユーザではアクセス 通常ユーザではアクセス 機関がない情報や機能へ アクセスできない お、カーのが含まれてお ない。 2) Aーのが含まれてお ない。 2) Aーのが含まれてお ない。 2) Aーのが含まれてお ない。 2) Aーのが含まれてお ない。 3) Referseチェックは機関薬 ではないが、リスク低減にな ない。 3) Referseチェックが行 われており、正常に処理 が行われない。 CSRF対策トークンの環 CSRF対策トークンが開定長で 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が発行され、古いセッションIDが発行され、 においセッションIDが発行され、古いセッションIDが発行され、 においセッションIDが発行され、 においセッションIDが発行され、 は、おいセッションIDが発行され、 においセッションIDが発行され、 においては、 にはいては、 においては、 にはいては、 にはい
50 50 51 52 53		セッションフィクセイション(セッション周	認可制御が必要な箇所 空縁、送信などの確定処理 CSRF対策トークンを使用している策所 ログイン機能	終行何: www.example.com/user2/profile.php 元の値: www.example.com/1000.csv 終行何: www.example.com/1001.csv 元の値: www.example.com/taro/index.php 終行何: www.example.com/jiro/index.php 終行何2: www.example.com/jiro/index.php	URL パラメータ セッションIDが接納されている箇所	製造状態でしか表示できないページに、ロダイン製造していない状態でアクセス 度存URLのフォルダバス、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 ②Cookia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 緩 利用者のパスワード B、CSRF対策トークン C、セッションID C、APTCHA ②AへDが含まれている場合に、ユーザョ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运信し、処理が行われるか確認 (3人への合きまれている場合に、ユーザョで利用されている値を削削。もしては工作メータごと削削してリクエストを运信し、処理が行われるか確認 CSRF対策トークンを推動して規則性があることを確認し、CSRF対策トークンを推動して規則性があることを確認し、CSRF対策トークンを推動して、サンを推動して現別性があることを確認し、CSRF対策トークンを推動して規則性があることを確認し、CSRF対策トークンを推動して、場合におきないた。 同ニューザアカウトごとに恋遊の比較	超起機かページを指定する ことでアクセスが可能である ろ アクセス体限がない情報や 機能が閲覧、操作できる 1) AーDが含まれている い、別ユーザの値でも正常 に処理が行われる 3) AーDが含まれている が、例ユーザの値でも正常 に処理が行われる 4) Refererチェックが行わ れていない と処理が行われる 4) Refererチェックが行わ れていない センションIDが構練して使用さ はる場合 に必理が行われる もれている もれでいる もれでも もれでいる も もれでいる もれで もれでいる もれでも もれで もれで もれで もれで もれで もれで もれで もれで もれ	型度級のページを指定す ることでアクセスができ ない 通常ユーザではアクセス 連常な一ザではアクセス 機能がない情報機能へ アクセスできない 第71 A-Dが含まれてお り、かつ、別ユーザの飯 変ではないが、リスク低減に では正常に処理がわけれた ない 2) A-Dが含まれてお っ、かつ、銀や・ヴァメー のどと削除しても正常に 効果を持ちない 3) Refererチェックは構製室 ではないが、リスク低減にな る カブとが開起しても正常に 短期が行われており、正常に処理 が行われており、正常に処理 が行われており、正常に処理 のではないが、リスク低減にな ない場合は疑う余地がある ログイン成功後に新しい セッションIDが場件さ
50 50 51 52		セッションフィクセイション(セッション周	認可制御が必要な箇所 登録、送信などの確定処理 CSRF対策トークンを使用している箇所 ログイン機能 ログイン前に機骸情報がセッション変数に移納	終行何: www.example.com/user2/profile.php 元の値: www.example.com/1000.csv 終行何: www.example.com/1001.csv 元の値: www.example.com/taro/index.php 終行何: www.example.com/jiro/index.php 終行何2: www.example.com/jiro/index.php	URL パラメータ セッションIDが接納されている箇所	型級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 既存URLのフォルグパス、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 「Cookieなどリクエスト〜ッグに含まれた値によって、セッション管理が付ま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 あ A 別用者のパスワード B、CSRF対策トークン C、セッションID O、Aの子びもまれている場合に、ユーザαで利用されている値をユーザ身で利用されている値を対してリクエストを送信し、処理が行われるか確認 (3人へのが含まれている場合に、ユーザαで利用されている値を利削、してパテメータ上で削除してリクエストを送信し、処理が行われるの確認 (3人を別からまれている場合に、ユーザの日常れている値を別所、してパテメータ上で削除してリクエストを送信し、処理が行われるの確認 (3人の子がきないの場合と、ステリカルのと呼吸)にリクエストを送信し、処理が行われるの確認 CSRF対策トークンを推測 こSRF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 コーザでログインですることに完達の比較 い同ニューザでログインであるとと確認	超越機かページを指定する ことでアクセスが可能である フクセス様限がない情報や 機能が閲覧、操作できる リカーDが含まれていない ターDが含まれていなが、別ユーザの値でも正常 に処理が行われる 3) AーDが含まれているが、値を削除、もしくはパ くが、別ユーザの値でも正常 が、原生が行われる 4) Refererチェックが行わ は、経理が行われる 4) Refererチェックが行わ はでいない でが、かり、単一のでは、 では、 では、 では、 では、 では、 では、 では、 では、 では、	型産級のページを指定す ることでアクセスができない 通常ユーザではアクセス 機能がない情報や機能へ アクセスできない 1) A~Dが含まれてお の、かつ、別ユーザの紙 変ではないが、リスク低減に では正常に処理が行われな の、かつ、銀やパラメー カンと制能しても正常に 処理が行われない 3) Refererチェックは推奨等 ではないが、リスク低減にな も 20 Refererチェックは推奨等 ではないが、リスク低減にな な 20 Refererチェックが行われない。 3) Refererチェックが行われない。 CSRF対策トークンの膜 助性が利らず推測不可 ない場合は疑う余地がある ログイン成功後に新しい セッション/Dが発行さ れ、古いセッション/Dは 微震情報人力後に新しい セッション/Dが発行さ れ、古いセッション/Dは
50 50 50 50 50 50 50 50 50 50 50 50 50 5		セッションフィクセイション(セッション周	認可制御が必要な箇所 登録、送信などの確定処理 CSRF対策トークンを使用している箇所 ログイン機能 ログイン前に機骸情報がセッション変数に移納	終行何: www.example.com/user2/profile.php 元の値: www.example.com/1000.csv 終行何: www.example.com/1001.csv 元の値: www.example.com/taro/index.php 終行何: www.example.com/jiro/index.php 終行何2: www.example.com/jiro/index.php	URL パラメータ セッションIDが接納されている箇所	型級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 既存URLのフォルグパス、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 「Cookieなどリクエスト〜ッグに含まれた値によって、セッション管理が付ま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 あ A 別用者のパスワード B、CSRF対策トークン C、セッションID O、Aの子びもまれている場合に、ユーザαで利用されている値をユーザ身で利用されている値を対してリクエストを送信し、処理が行われるか確認 (3人へのが含まれている場合に、ユーザαで利用されている値を利削、してパテメータ上で削除してリクエストを送信し、処理が行われるの確認 (3人を別からまれている場合に、ユーザの日常れている値を別所、してパテメータ上で削除してリクエストを送信し、処理が行われるの確認 (3人の子がきないの場合と、ステリカルのと呼吸)にリクエストを送信し、処理が行われるの確認 CSRF対策トークンを推測 こSRF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 コーザでログインですることに完達の比較 い同ニューザでログインであるとと確認	超起機かページを指定する ことでアクセスが可能である ろ アクセス体限がない情報や 機能が閲覧、操作できる 1) AーDが含まれている い、別ユーザの値でも正常 に処理が行われる 3) AーDが含まれている が、例ユーザの値でも正常 に処理が行われる 4) Refererチェックが行わ れていない と処理が行われる 4) Refererチェックが行わ れていない センションIDが構練して使用さ はる場合 に必理が行われる もれている もれでいる もれでも もれでいる も もれでいる もれで もれでいる もれでも もれで もれで もれで もれで もれで もれで もれで もれで もれ	型度級のページを指定することでアクセスができない 通常ユーザではアクセス 通常ユーザではアクセス 機能がない情報や機能へ アクセスできない 第71 A-Dが含まれており、かつ、別ユーザの値、変ではないが、リスク低域にてないでは正常に処理が打される。 20 A-Dが含まれており、かつ、観やパラメー カンと別能しても正常に 知恵が行われない 31 Refererチェックが行われており、正常に処理 が行われない 51 Refererチェックが行われており、正常に処理 が行われており、正常に処理 が行われており、正常に処理 が行われてが、リングが開発に対していまからが発行され、古いセッション川のは機能される 観微情報入り後に新しい セッション川のが発行され、古いセッション川のは機能される 観微情報入り後に新しい セッション川のは発音されています。

No. 大分類	中分額	小分類	診断を実施すべき箇所	ベイロード・檜出パターン	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	備者
54	1 22 700	CookieのHttpOnly属性未設定	Cookie 発行処理	1 - 1 38HC 2 V	JAIP CII JAIA	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-	レスポンスヘッダの	JM - 7
							Cookieヘッダフィールド値	Set-Cookieヘッダ	
							に"HttpOnly"属性が指定さ	フィールド値に	
							れていない	"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	セッションIDに規則性があ	セッションIDの規則性が	セッションIDが固定長でない
						ユーザアカウントごとに差異の比較	り推測可能	判らず推測不可	場合は疑う余地がある
						・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			
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や機衡情報がURLに含まれていないか確認	URLにセッションIDや機微		
								微情報が含まれていない	
							(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サーバやブロ		
							キシーサーバにログとして		
<u> </u>							残る。)		
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		
-			A company of the comp				ていない	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"である	
50		画面表示上のマスク不備	全般			いることを確認 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	"password"ではない		-h-daman or deads of the Military has he was
59		周囲表示上のマスク个個	主収			マスクリへざ情報が周囲上に表示されていないことを解認	マスクリへさ情報が周囲上 に表示されている	マスクリへさ情報が周囲 上に表示されていない	主なマスクすべき情報として
							に表示されている	上に表示されていない	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 A w & 7 / - # . K M & Z *****			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	レスポンスへ…がの 0~+	レスポンスペーダの	1 114コード、ハスソート
00		III II SFI/Amy OCOOKIE O SECULEMIE 不致足	Set-Cookie 1/2/1/20/5/mi//			on the second se	Cookieヘッダフィールド値		
						PO .	に"Secure"属性が指定され		
							ていない	属性が指定されている	
61		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		平文なのか可逆暗号なのかは
01		7 TOTAKT	, , , , , , , , , , , , , , , , , , ,			7 A 7 F 7 F 9 F 9 KI	される/メールで送られて	TTREACHMENT CARRY 7 S	判断できない
							< a		1997 4 6 184
62			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	表示されない	平文なのか可逆暗号なのかは
1 1						アスプ ド東大岡園、日廷日岡園にアクモハ			判断できない
						アステード東天岡田、日本計画田にアノとス	される/inputタグに埋まっ		判断できない
63		HTTPSの不備					される/inputタグに埋まっ ている		判断できない
63 64		HTTPSの不備	全般 HTTPS箇所			機機情報を取り扱うWebページ(フォームの表示、透信先共に)にアクセス HTTPSを使用しているコンテンツを確認(HTTPsよびHTTPSの併用)	される/inputタグに埋まっ ている	HTTPSで通信している	判断できない
63 64		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	される/inputタグに埋まっ ている HTTPで通信している HTTPSだけでアクセスすべ	HTTPSで通信している	判断できない
63 64		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	される/inputタグに埋まっ ている HTTPで通信している HTTPSだけでアクセスすべ きページがHTTPでもアク	HTTPSで通信している HTTPS以外ではアクセス	判断できない
63 64		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	される/inputタグに埋まっ ている HTTPで通信している HTTPSだけでアクセスすべ	HTTPSで通信している HTTPS以外ではアクセス できない	判断できない
		HTTPSの不偏	全般 HTTPS顯所 HTTPS顯所			機能情報を取り扱うWebページ(フォームの表示、送信先料に)にアクセス 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を使用しているコンテンツを確認(HTTPとHTTPSの混在)	される/inputタグに埋まっ ている HTTPで通信している 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とHTTPのコンテン ツが混在している	HTTPSで通信している HTTPS以外ではアクセス できない HTTPSとHTTPのコンテ ンツが混在していない	
		HTTPSの不備	全校 HTTPS箇所			機機情報を取り扱うWebページ(フォームの表示、送信先料に)にアクセス HTTPSを使用しているコンテンツを確認(HTTPおよびHTTPSの併用)	される/inputタグに埋まっ ている HTTPで通信している 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とHTTPのコンテン ツが混在している	HTTPSで通信している HTTPS以外ではアクセス できない HTTPSとHTTPのコンテ ンツが混在していない	判断できない 警告が出る場合には以下のい
		HTTPSの不備	全般 HTTPS顯所 HTTPS顯所			機能情報を取り扱うWebページ(フォームの表示、送信先料に)にアクセス 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を使用しているコンテンツを確認(HTTPとHTTPSの混在)	される/inputタグに埋まっ ている HTTPで通信している 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とHTTPのコンテン ツが混在している	HTTPSで通信している HTTPS以外ではアクセス できない HTTPSとHTTPのコンテ ンツが混在していない	
		HTTPSの不備	全般 HTTPS顯所 HTTPS顯所			機能情報を取り扱うWebページ(フォームの表示、送信先料に)にアクセス 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を使用しているコンテンツを確認(HTTPとHTTPSの混在)	される/inputタグに埋まっ ている HTTPで通信している HTTPをだけでアクセスすべ さページがHTTPでもアク セス可能となっている HTTPSとHTTPのコンテン yが混在している ブラウザで証明書の警告が	HTTPSで通信している HTTPS以外ではアクセス できない HTTPSとHTTPのコンテ ンツが混在していない ブラウザで証明書の警告	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
		HTTPSの不備	全般 HTTPS顯所 HTTPS顯所			機能情報を取り扱うWebページ(フォームの表示、送信先料に)にアクセス 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を使用しているコンテンツを確認(HTTPとHTTPSの混在)	される/inputタグに埋まっ ている HTTPで通信している HTTPをだけでアクセスすべ さページがHTTPでもアク セス可能となっている HTTPSとHTTPのコンテン yが混在している ブラウザで証明書の警告が	HTTPSで通信している HTTPS以外ではアクセス できない HTTPSとHTTPのコンテ ンツが混在していない ブラウザで証明書の警告	警告が出る場合には以下のい
		HTTPSの不備	全般 HTTPS顯所 HTTPS顯所			機能情報を取り扱うWebページ(フォームの表示、送信先料に)にアクセス 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を使用しているコンテンツを確認(HTTPとHTTPSの混在)	される/inputタグに埋まっ ている HTTPで通信している HTTPをだけでアクセスすべ さページがHTTPでもアク セス可能となっている HTTPSとHTTPのコンテン yが混在している ブラウザで証明書の警告が	HTTPSで通信している HTTPS以外ではアクセス できない HTTPSとHTTPのコンテ ンツが混在していない ブラウザで証明書の警告	響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
		HTTPSの不備	全般 HTTPS顯所 HTTPS顯所			機能情報を取り扱うWebページ(フォームの表示、送信先料に)にアクセス 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を使用しているコンテンツを確認(HTTPとHTTPSの混在)	される/inputタグに埋まっ ている HTTPで通信している HTTPをだけでアクセスすべ さページがHTTPでもアク セス可能となっている HTTPSとHTTPのコンテン yが混在している ブラウザで証明書の警告が	HTTPSで通信している HTTPS以外ではアクセス できない HTTPSとHTTPのコンテ ンツが混在していない ブラウザで証明書の警告	響告が出る場合には以下のい すれいに該当する可能性があ る。自己証明書が用いられてい る ・ 有効明度が切れている
		HTTPSの不備	全般 HTTPS顯所 HTTPS顯所			機能情報を取り扱うWebページ(フォームの表示、送信先料に)にアクセス 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を使用しているコンテンツを確認(HTTPとHTTPSの混在)	される/inputタグに埋まっ ている HTTPで通信している HTTPをだけでアクセスすべ さページがHTTPでもアク セス可能となっている HTTPSとHTTPのコンテン yが混在している ブラウザで証明書の警告が	HTTPSで通信している HTTPS以外ではアクセス できない HTTPSとHTTPのコンテ ンツが混在していない ブラウザで証明書の警告	撃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 ・自己経明書が用いられてい る ・有効期限が切れている ・施財者のポント名がサイト
		HTTPSの不備	全般 HTTPS顯所 HTTPS顯所			機能情報を取り扱うWebページ(フォームの表示、送信先料に)にアクセス 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を使用しているコンテンツを確認(HTTPとHTTPSの混在)	される/inputタグに埋まっ ている HTTPで通信している HTTPをだけでアクセスすべ さページがHTTPでもアク セス可能となっている HTTPSとHTTPのコンテン yが混在している ブラウザで証明書の警告が	HTTPSで通信している HTTPS以外ではアクセス できない HTTPSとHTTPのコンテ ンツが混在していない ブラウザで証明書の警告	警告が出る場合には以下のい すれかに該当する可能性があ 。自己証明書が用いられてい る。有効期限が切れている ・証的書のホスト名がサイト と一致してない
		HTTPSの不備	全般 HTTPS顯所 HTTPS顯所			機能情報を取り扱うWebページ(フォームの表示、送信先料に)にアクセス 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を使用しているコンテンツを確認(HTTPとHTTPSの混在)	される/inputタグに埋まっ ている HTTPで通信している HTTPをだけでアクセスすべ さページがHTTPでもアク セス可能となっている HTTPSとHTTPのコンテン yが混在している ブラウザで証明書の警告が	HTTPSで通信している HTTPS以外ではアクセス できない HTTPSとHTTPのコンテ ンツが混在していない ブラウザで証明書の警告	警告が出る場合には以下のい で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 ・右効開路が切れている ・証明書のホスト名がサイト と一致してない、 推奨されない場名アルゴリ
		HTTPSの不備	全般 HTTPS顯所 HTTPS顯所			機能情報を取り扱うWebページ(フォームの表示、送信先料に)にアクセス 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を使用しているコンテンツを確認(HTTPとHTTPSの混在)	される/inputタグに埋まっ ている HTTPで通信している HTTPをだけでアクセスすべ さページがHTTPでもアク セス可能となっている HTTPSとHTTPのコンテン yが混在している ブラウザで証明書の警告が	HTTPSで通信している HTTPS以外ではアクセス できない HTTPSとHTTPのコンテ ンツが混在していない ブラウザで証明書の警告	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 も自己証明書が用いられている ・有効期限が切れている ・起明書のホント名がサイト と一致してない ・推奨されない署名アルゴリ ズムの利用
		HTTPSの不備	全級 HTTPS箇所 HTTPS箇所 HTTPS箇所			機能情報を取り扱うWebページ(フォームの表示、送信先料に)にアクセス 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を使用しているコンテンツを確認(HTTPとHTTPSの混在) 動作対象グラウザで証明書を確認	される/inputタグに埋まっている HTTPで通信している HTTPを対けでアクセスすべ。 ホインタがHTTPでもアクセスする。 セページがHTTPでもアク セス可能となっている HTTPSとHTTPのコンテン グタウザで延明書の警告が 出る	HTTPSで通信している HTTPS以外ではアクセス できない HTTPSとHTTPのコンテンツが混在していない グ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 で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 ・右効開路が切れている ・証明書のホスト名がサイト と一致してない、 推奨されない場名アルゴリ
		HTTPSの不備	全般 HTTPS顯所 HTTPS顯所			機應情報を取り扱うWebページ(フォームの表示、送信先典に)にアクセス HTTPSを使用しているコンテンツを確認(HTTPおよびHTTPSの使用) HTTPSを使用しているコンテンツを確認(HTTPとHTTPSの混在) 動作対象プラウザで証明書を確認 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	される/inputタグに埋まっている HTTPで通信している HTTPを対けでアクセスすべ。 ホインタがHTTPでもアクセスする。 セページがHTTPでもアク セス可能となっている HTTPSとHTTPのコンテン グタウザで延明書の警告が 出る	HTTPSで通信している HTTPS以外ではアクセス できない HTTPSとHTTPのコンテ ンツが混在していない ブラウザで証明書の警告	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 も自己証明書が用いられている ・有効期限が切れている ・起明書のホント名がサイト と一致してない ・推奨されない署名アルゴリ ズムの利用
		HTTPSの不備	全級 HTTPS箇所 HTTPS箇所 HTTPS箇所			機能情報を取り扱うWebページ(フォームの表示、送信先則に)にアクセス 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を使用しているコンテンツを確認(HTTPとHTTPSの混在) 動作対象プラウザで証明書を確認 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 などに伝わる情報)」や「公園不要な情報(個人名、メールアドレス、ミド	まれる/inputタグに埋まっている HTTPで通信している HTTPを活住でアクセスすべ ホージのHTTPでもアクセスする ページのHTTPでもアクセスする セページのHTTPでもアクセスする セページの場合に メラクザで延明事の警告が 出る	HTTPSで通信している HTTPS以外ではアクセス できない HTTPSとHTTPのコンテンツが混在していない グ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 も自己証明書が用いられている ・有効期限が切れている ・起明書のホント名がサイト と一致してない ・推奨されない署名アルゴリ ズムの利用
		HTTPSの不備	全級 HTTPS箇所 HTTPS箇所 HTTPS箇所			機能情報を取り扱うWebページ(フォームの表示、逆信先料に)にアクセス HTTPSを使用しているコンテンツを確認(HTTPおよびHTTPSの使用) HTTPSを使用しているコンテンツを確認(HTTPとHTTPSの設在) 動作対象プラウザで証明書を確認 HTMLやJavaScriptなどに「攻撃に有用な情報(設計やデータペース構造になどに採わる情報)」や「公開不変な情報(例人名、メールアドレス、ミドレクラアの行権、過去か公開していたコンテンツのリンク、プライベースド	まれる/inputタグに埋まっている HTTPで通信している HTTPを活住でアクセスすべ ホージのHTTPでもアクセスする ページのHTTPでもアクセスする セページのHTTPでもアクセスする セページの場合に メラクザで延明事の警告が 出る	HTTPSで通信している HTTPS以外ではアクセス できない HTTPSとHTTPのコンテンツが混在していない グ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 も自己証明書が用いられている ・有効期限が切れている ・起明書のホント名がサイト と一致してない ・推奨されない署名アルゴリ ズムの利用
65 66 67			今般 HTTPS箇所 HTTPS箇所 HTTPS箇所			機機情報を取り扱うWebページ(フォームの表示、送信先典に)にアクセス 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を使用しているコンテンツを確認(HTTPとHTTPSの混在) 動作対象プラウザで証明書を確認 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アンツのリンク、プライベートIPアレスなど)、が含まれていることを確認	まれる/inputタダに埋まっている HTTPで通信している HTTPを指すでアクセスすべ サインラがHTTPをはファクセスする サインラが出ている HTTPSとHTTPのコンテン フが滅在している ブラウザで延明書の警告が 出る	HTTPSで通信している HTTPS以外ではアクセス できない HTTPSとHTTPのコンテ ンツが原在していない ブラウザで証明書の警告 が出ない 情報が含まれていない	署告が出る場合には以下のい すれかに該当する可能性があ 。自己証明書が用いられてい 。有効関節が出れている ・板内器のホスト名がサイト と一致してい ・推奨されない署名アルゴリ スムの利用 、不適切な離長
65 66 67 68 Webアプリケーションの動作環境へ	の節 サーバソフトウェアの設定の		全級 HTTPS箇所 HTTPS箇所 HTTPS箇所		URL	機能情報を取り扱うWebページ(フォームの表示、送信先則に)にアクセス 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を使用しているコンテンツを確認(HTTPとHTTPSの混在) 動作対象グラウザで証明書を確認 新作対象グラウザで証明書を確認 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 などに伝わる情報)」や「公園不要な情報(個人名、メールアドレス、ミドルウェアの情報、過去の公園していたコンアンツのリンク、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 Webサーバよの発見したディレクトリ内の	される/inputタグに埋まっている HTTPで通信している HTTPを通信している HTTPを放けでアクセスする ページがHTTPでもアクセスする セページがHTTPでもアクセスする セページがHTTPをHTPのコンテン アクラザで延明書の警告が 出る 情報が含まれている	HTTPSで通信している HTTPS以外ではアクセス できない HTTPS以外ではアクセス できない HTTPSとHTTPのコンテンクが混在していない ブラウザで証明書の警告 が出ない 情報が含まれていない	響告が出る場合には以下のい すれい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 と一致してか、 ・推奨されない署名アルゴリ ズムの利用 ・不適切な難長 含まれているファイルによっ
65 65 68 Webアプリケーションの動作環境へ 新項目	の診 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	全般 HTTPS箇所 HTTPS箇所 +パで		URL	機應情報を取り扱うWebページ(フォームの表示、送信先典に)にアクセス HTTPSを使用しているコンテンツを確認(HTTPおよびHTTPSの使用) HTTPSを使用しているコンテンツを確認(HTTPとHTTPSの混在) 動作対象プラウザで証明書を確認 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 などに続わる情報)」や「公園不変な情報(個人名、メールアドレス、ミド ルクェアの情報、過去の公園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 Webサーバ上の発息したディレクトリにアフセスして、ディレクトリ内の ファイルへ・展発されないかとない。	される/inputタグに埋まっている HTTPで通信している HTTPをがけてアクセスすべ さページがHTTPでもアクセスする さページがHTTPでもアク セス可能となっている HTTPSとHTTPのコンテン フが現在している ブラウザで証明書の警告が 出る 情報が含まれている ディレクトリ内のファイル が一覧表される	HTTPSで通信している HTTPS以外ではアクセス できない HTTPSとHTTPのコンテ ンツが誕在していない ブラウザで証明書の警告 が出ない 情報が含まれていない ディレクトリ内のファイ ルが一覧表示されない	響告が出る場合には以下のい すれい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 と一致してか、 ・推奨されない署名アルゴリ ズムの利用 ・不適切な難長 含まれているファイルによっ
65 66 67 68 Webアプリケーションの動作環境へ	の診 サーバソフトウェアの設定の 不備		今般 HTTPS箇所 HTTPS箇所 HTTPS箇所		URL	機機情報を取り扱うWebページ(フォームの表示、送信先則に)にアクセス 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を使用しているコンテンツを確認(HTTPとHTTPSの混在) 動作対象プラウザで証明書を確認 MTMLやJavaScriptなどに「攻撃に有用な情報(設計やデータペース構造になどに採わる情報)」や「公園不要な情報(個人名、メールアドレス、ミドルウェアの情報、過去の公園していたコンアンツのリンク、ブライベートIP アドレスなど)」が含まれていることを確認 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 P・パケアツリアンション、ミドルウェア、ブレームワークなどのパージョ	される/inputタグに埋まっている HTTPで通信している HTTPを通信している HTTPを放けでアクセスする ページがHTTPでもアクセスする セページがHTTPでもアクセスする セページがHTTPをHTPのコンテン アクラザで延明書の警告が 出る 情報が含まれている	HTTPSで通信している HTTPS以外ではアクセス できない HTTPSとHTTPのコンテ ンツが原在していない ブラウザで証明書の警告 が出ない ディレクトリ内のファイ ルが一覧表示されない バージョン等のが表示さ	響告が出る場合には以下のい すれい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 と一致してか、 ・推奨されない署名アルゴリ ズムの利用 ・不適切な難長 含まれているファイルによっ
65 65 68 Webアプリケーションの動作環境へ 新項目	の診 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 バージョン番号表示	今収 HTTPS箇所 HTTPS箇所 HTTPS箇所 すべて すべて			機應情報を取り扱うWebページ(フォームの表示、送信先用に)にアクセス HTTPSを使用しているコンテンツを確認(HTTPおよびHTTPSの使用) HTTPSを使用しているコンテンツを確認(HTTPとHTTPSの混在) 動作対象プラウザで証明書を確認 HTMLやJavaScriptなどに「攻撃に有用な情報(設計やデータペース構造になどに係わる情御)」や「と関不変な情報(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 Pアドレスなど)」が含まれていることを確認 Webザーバとか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 サーベやアブリケーション、ミドルウェア、フレームワークなどのパージョン条分が表示されないかを確認	される/inputタグに埋まっている HTTPで通信している HTTPを形けてアクセスすべ まページがHTTPでもアクセスすべ をページがHTTPでもアクセスすべ サイルのコンテンプが混在している プラウザで証明漆の警告が 出る 情報が含まれている ディレクトリ内のファイル が一覧表示される パージョン番号が表示され る	HTTPSで通信している HTTPS以外ではアクセス できない HTTPSとHTTPのコンテ ンツが誕在していない ブラウザで延明書の警告 が出ない ディレクトリ内のファイ トが一覧表示されない パージョン番号が表示さ れない	響告が出る場合には以下のい すれい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 と一致してか、 ・推奨されない署名アルゴリ ズムの利用 ・不適切な難長 含まれているファイルによっ
65 65 68 Webアプリケーションの動作環境へ 新項目	の診 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	全般 HTTPS箇所 HTTPS箇所 +パで	TRACE, TRACK	URL リクエストメンッド	機機情報を取り扱うWebページ(フォームの表示、送信先則に)にアクセス 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を使用しているコンテンツを確認(HTTPとHTTPSの混在) 動作対象プラウザで証明書を確認 MTMLやJavaScriptなどに「攻撃に有用な情報(設計やデータペース構造になどに採わる情報)」や「公園不要な情報(個人名、メールアドレス、ミドルウェアの情報、過去の公園していたコンアンツのリンク、ブライベートIP アドレスなど)」が含まれていることを確認 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 P・パケアツリアンション、ミドルウェア、ブレームワークなどのパージョ	まれる/inputタグに埋まっている HTTPで通信している HTTPを指すでフセスすべ HTTPをだけてアクセスすべ をページがHTTPでもアクセスする セス可能となっている HTTPSとHTTPのコンテン フが原住している ブラウザで延明書の警告が 出る 「ページョン番号が表示される バージョン番号が表示される TRACE、TRACKメソッド	HTTPSで通信している HTTPS以外ではアクセス できない HTTPSとHTTPのコンテ ンツが原在していない ブラウザで証明書の警告 が出ない ディレクトリ内のファイ ルが一覧表示されない パージョン番号が表示されない パージョン番号が表示されない TRACE、TRACKメソッ	響告が出る場合には以下のい すれい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 と一致してか、 ・推奨されない署名アルゴリ ズムの利用 ・不適切な難長 含まれているファイルによっ
65 65 68 Webアプリケーションの動作環境へ 新項目	の診 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 パージョン番号表示 不要なHTTPメソッド	全般 HTTPS箇所 HTTPS箇所 HTTPS箇所 すべて すべて すべて		リクエストメソッド	機能情報を取り扱うWebページ(フォームの表示、送信先則に)にアクセス 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を使用しているコンテンツを確認(HTTPとHTTPSの混在) 動作対象プラウザで証明書を確認 動作対象プラウザで証明書を確認 Webかったのでは、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 Webサーバと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 メンッドを変更してサーバにアクセス メンッドを変更してサーバにアクセス	まれる/inputタグに埋まっている HTTPで通信している HTTPを活住している HTTPを対けてアクセスする ページがHTPでもアクセスする とページがHTPでもアクセスする とイージが無住している プラウザで延明書の警告が 出る 情報が含まれている ディレクトリ内のファイル が一覧条件される 「ページョン番号が表示される 「不ACE、TRACKメソット が機能する 「TRACE、TRACKメソット が機能する	HTTPSで通信している HTTPS以外ではアクセス できない HTTPSとHTTPのコンテンツが課在していない ブラウザで延明書の警告 が出ない ディレクトリ内のファイ ルが一覧表示されない ページョン番号が表示さ 社ない ドバ機能しない ドバ機能しない	響告が出る場合には以下のい すれい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 と一致してか、 ・推奨されない署名アルゴリ ズムの利用 ・不適切な難長 含まれているファイルによっ
65 65 68 Webアプリケーションの動作環境へ 新項目	の影 サーバソフトウェアの設定の 不偏	ディレクトリリスティング バージョン番号表示	今収 HTTPS箇所 HTTPS箇所 HTTPS箇所 すべて すべて	TRACE, TRACK OPTIONS		機應情報を取り扱うWebページ(フォームの表示、送信先用に)にアクセス HTTPSを使用しているコンテンツを確認(HTTPおよびHTTPSの使用) HTTPSを使用しているコンテンツを確認(HTTPとHTTPSの混在) 動作対象プラウザで証明書を確認 HTMLやJavaScriptなどに「攻撃に有用な情報(設計やデータペース構造になどに係わる情御)」や「と関不変な情報(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 Pアドレスなど)」が含まれていることを確認 Webザーバとか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 サーベやアブリケーション、ミドルウェア、フレームワークなどのパージョン条分が表示されないかを確認	まれる/inputタグに埋まっている HTTPで通信している HTTPを近けてアクセスすべ、 は一ジが出ているでいる。 HTTPSとUTTPのコンテン フが現在している プラウザで証明書の警告が 出る 情報が含まれている ディレクトリ内のファイル が一覧表示される 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る TRACE、TRACKメット が構能する Allow〜ッダにGET、	HTTPSで通信している HTTPS以外ではアクセス できない HTTPSとHTTPのコンテ ンツが原在していない ブラウザで証明書の警告 が出ない ディレクトリ内のファイ ルが一覧表示されない パージョン番号が表示されない パージョン番号が表示されない TRACE、TRACKメソッ	響告が出る場合には以下のい すれい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 と一致してか、 ・推奨されない署名アルゴリ ズムの利用 ・不適切な難長 含まれているファイルによっ
65 65 68 Webアプリケーションの動作環境へ 新項目	の診 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 パージョン番号表示 不要なHTTPメソッド	全般 HTTPS箇所 HTTPS箇所 HTTPS箇所 すべて すべて すべて		リクエストメソッド	機能情報を取り扱うWebページ(フォームの表示、送信先則に)にアクセス 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を使用しているコンテンツを確認(HTTPとHTTPSの混在) 動作対象プラウザで証明書を確認 動作対象プラウザで証明書を確認 Webかったのでは、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 Webサーバと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 メンッドを変更してサーバにアクセス メンッドを変更してサーバにアクセス	まれる/inputタグに埋まっている HTTPで通信している HTTPを活住でアクセスすべ ホーペンがHTTPでもアクセスすべ セス可能となっている HTTPSとはTPのコンテン グが滅性している ブラウザで延明事の警告が 出る 「情報が含まれている ディレクトリ内のファイル バージョン番号が表示される TRACE、TRACKメソッド が機能する Allow・グドにGET、 HEAD、POST、OPTIONS	HTTPSで通信している HTTPS以外ではアクセス できない HTTPSとHTTPのコンテンツが原在していない ブラウザで証明書の警告 が出ない ディレクトリ内のファイ ルが一覧表示されない パージョン等号が表示さ れない TACい TACい TACい TACい Allow・フダが存在しない Allow・フダが存在しない	響告が出る場合には以下のい すれい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 と一致してか、 ・推奨されない署名アルゴリ ズムの利用 ・不適切な難長 含まれているファイルによっ
65 66 67 68 Webアプリケーションの動作環境へ 新項目	の診 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 パージョン番号表示 不要なHTTPメソッド	全般 HTTPS箇所 HTTPS箇所 HTTPS箇所 すべて すべて すべて		リクエストメソッド	機能情報を取り扱うWebページ(フォームの表示、送信先則に)にアクセス 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を使用しているコンテンツを確認(HTTPとHTTPSの混在) 動作対象プラウザで証明書を確認 動作対象プラウザで証明書を確認 Webかったのでは、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 Webサーバと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 メンッドを変更してサーバにアクセス メンッドを変更してサーバにアクセス	される/inputタグに埋まっている HTTPで通信している HTTPを洗けてアクセスすべ まページがITTPでもアクセスすべ まページがITTPでもアクセスすべ セページがITTPをHTPでもアクセスすべ おれている アクラザで証明像の警告が 出る がページョン番号が表示され スページョン番号が表示され TRACE、TRACKメソッド が機能する AllowヘッダにGET、 HEAD、POST、OPTIONS 以外のメソッドが存在する	HTTPSで通信している HTTPS以外ではアクセス できない HTTPSとHTTPのコンテ ンツが誕在していない ブラウザで証明書の警告 が出ない ディレクトリ内のファイ ルが一覧表示されない パージョン書が示まされない パージョン書がまままままままままままままままままままままままままままままままままままま	響告が出る場合には以下のい すれい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 と一致してか、 ・推奨されない署名アルゴリ ズムの利用 ・不適切な難長 含まれているファイルによっ
65 65 68 Webアプリケーションの動作環境へ 新項目	の診 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 パージョン番号表示 不要なHTTPメソッド	全般 HTTPS箇所 HTTPS箇所 HTTPS箇所 すべて すべて すべて		リクエストメソッド	機能情報を取り扱うWebページ(フォームの表示、送信先則に)にアクセス 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を使用しているコンテンツを確認(HTTPとHTTPSの混在) 動作対象プラウザで証明書を確認 動作対象プラウザで証明書を確認 Webかったのでは、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 Webサーバと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 メンッドを変更してサーバにアクセス メンッドを変更してサーバにアクセス	まれる/inputタグに埋まっている HTTPで通信している HTTPを近てアクセスすべ HTTPをだけてアクセスすべ メージが出ていた サインが展在している インのが開催している インのが開催している インのが開催している インのが開催している インのが開催している インのが開催している インのが開催している インのが開催している インのが開催している インのが表生される インのが、「RACE、TRACKメソッド が機能する Allow〜ッダにGET、 HEAD、POST、OPTIONS 以外のメソッドが存在する に対している に対している に対している 「PUT、DELEIT、TRACE、TRACE、TRACE、TRACE、TRACE、TRACE、TRACE (PUT、TRACE、TRACE) 「PUT、TRACE」、TRACE (PUT、TRACE) 「PUT、TRACE TRACE TRA	HTTPSで通信している HTTPS以外ではアクセス できない HTTPSとHTTPのコンテ ンツが開在していない ブラウザで証明書の警告 が出ない ディレクトリ内のファイ ルが一覧表示されない パージョン番号が表示されない パージョン番号が表示される いる HEACL POST、HEADL POST、	響告が出る場合には以下のい すれい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 と一致してか、 ・推奨されない署名アルゴリ ズムの利用 ・不適切な難長 含まれているファイルによっ
65 66 67 68 Webアプリケーションの動作環境へ 新項目	の診 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 パージョン番号表示 不要なHTTPメソッド	全般 HTTPS箇所 HTTPS箇所 HTTPS箇所 すべて すべて すべて		リクエストメソッド	機能情報を取り扱うWebページ(フォームの表示、送信先則に)にアクセス 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を使用しているコンテンツを確認(HTTPとHTTPSの混在) 動作対象プラウザで証明書を確認 動作対象プラウザで証明書を確認 Webかったのでは、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 Webサーバと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 メンッドを変更してサーバにアクセス メンッドを変更してサーバにアクセス	される/inputタグに埋まっている HTTPで通信している HTTPを洗けてアクセスすべ まページがITTPでもアクセスすべ まページがITTPでもアクセスすべ セページがITTPをHTPでもアクセスすべ おれている アクラザで証明像の警告が 出る がページョン番号が表示され スページョン番号が表示され TRACE、TRACKメソッド が機能する AllowヘッダにGET、 HEAD、POST、OPTIONS 以外のメソッドが存在する	HTTPSで通信している HTTPS以外ではアクセス できない HTTPSとHTTPのコンテ ンツが誕在していない ブラウザで延野書の警告 が出ない ディレクトリ内のファイ ルが一覧表示されない バージョン番号が表示さ れない TRACE、TRACKメソッ ドが機能しない Allowヘッダが存在しない。 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	響告が出る場合には以下のい すれい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 と一致してか、 ・推奨されない署名アルゴリ ズムの利用 ・不適切な難長 含まれているファイルによっ
65 65 68 Webアプリケーションの動作環境へ 新項目	不備	ディレクトリリスティング バージョン番号表示 不要なHTTPメソッド	全般 HTTPS箇所 HTTPS箇所 +ペて サペて すべて すべて すべて	OPTIONS	リクエストメソッド リクエストメソッド	機機情報を取り扱うWebページ(フォームの表示、送信先典に)にアクセス HTTPSを使用しているコンテンツを確認(HTTPおよびHTTPSの使用) HTTPSを使用しているコンテンツを確認(HTTPとHTTPSの原在) 動作対象プラウザで証明書を確認 HTMLやJavaScriptなどに「攻撃に有用な情報(設計やデータペース構造に などに転わる情報)」中 (ご網不要な情報 (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 Webサーバと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な必要 サーバでアプリケーション、ミドルウェア、フレームワータなどのバージョ メラッドを実更してサーバにアクセス メソッドを変更してサーバにアクセス	まれる/inputタグに埋まっている HTTPで通信している HTTPを近けてアクセスすべ ホージルでアクセスすべ セページがHTTPでもアクセス可能となっている HTTPSとHTTPのコンテンプが現在している プラウザで延明書の警告が 出る 精報が含まれている デイレクトリ内のファイル が一覧表される パージョン番号が表示される 「RACE、TRACKメソット が機能十ち Allow〜フダドGET、 HEAD、POST、OPTIONS は外のメソッドが存する は外のメソッドが存する は外のメソッドが存する はり、アロスにの HEAD、POST、OPTIONS は外のメソッドが存する はアリエ、DELETE、TRACE など)	HTTPSで通信している HTTPS以外ではアクセス できない HTTPSとHTTPのコンテ ンツが混在していない ブラウザで証明書の警告 が出ない デイレクトリ内のファイ ルが一覧表示されない バージョン番号が表示されない TRACE、TRACKメンァ ドが機能しない Allow〜ッダにGET、 HEAD、POST、 OPTIONS以外のメソッド ドが存在しない	響告が出る場合には以下のい すれい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 と一致してか、 ・推奨されない署名アルゴリ ズムの利用 ・不適切な難長 含まれているファイルによっ
65 66 67 68 Webアプリケーションの動作環境へ 新項目	の診 サーバソフトウェアの設定の 不備 公園不要な機能・ファイル・シ	ディレクトリリスティング バージョン番号表示 不要なHTTPメソッド	全般 HTTPS箇所 HTTPS箇所 HTTPS箇所 すべて すべて すべて	OPTIONS	リクエストメソッド リクエストメソッド	機機情報を取り扱うWebページ(フォームの表示、送信先典に)にアクセス 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を使用しているコンテンツを確認(HTTP とHTTP Sの混在) 動作対象プラウザで証明書を確認 HTML やJava Script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、ブライベートIP アドレスたど) が含まれていたコンテンツのリンク、ブライベートIP アドレスたど) が含まれているいかを確認 オンッドを変更してサーバにアクセス メソッドを変更してサーバにアクセス メソッドを変更してサーバにアクセス メソッドを変更してサーバにアクセス	まれる/inputタグに埋まっている HTTPで通信している HTTPを近けてアクセスすべ ホージルでアクセスすべ セページがHTTPでもアクセス可能となっている HTTPSとHTTPのコンテンプが現在している プラウザで延明書の警告が 出る 精報が含まれている デイレクトリ内のファイル が一覧表される パージョン番号が表示される 「RACE、TRACKメソット が機能十ち Allow〜フダドGET、 HEAD、POST、OPTIONS は外のメソッドが存する は外のメソッドが存する は外のメソッドが存する はり、アロスにの HEAD、POST、OPTIONS は外のメソッドが存する はアリエ、DELETE、TRACE など)	HTTPSで通信している HTTPS以外ではアクセス できない HTTPSとHTTPのコンテ ンツが誕在していない ブラウザで延野書の警告 が出ない ディレクトリ内のファイ ルが一覧表示されない バージョン番号が表示さ れない TRACE、TRACKメソッ ドが機能しない Allowヘッダが存在しない。 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	響告が出る場合には以下のい すれい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 と一致してか、 ・推奨されない署名アルゴリ ズムの利用 ・不適切な難長 含まれているファイルによっ
65 66 67 68 Webアプリケーションの動作環境へ 新項目	不備	ディレクトリリスティング バージョン番号表示 不要なHTTPメソッド	全般 HTTPS箇所 HTTPS箇所 +ペて サペて すべて すべて すべて	OPTIONS	リクエストメソッド リクエストメソッド	機機情報を取り扱うWebページ(フォームの表示、送信先典に)にアクセス HTTPSを使用しているコンテンツを確認(HTTPおよびHTTPSの使用) HTTPSを使用しているコンテンツを確認(HTTPとHTTPSの原在) 動作対象プラウザで証明書を確認 HTMLやJavaScriptなどに「攻撃に有用な情報(設計やデータペース構造に などに転わる情報)」中 (ご網不要な情報 (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 Webサーバと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な必要 サーバでアプリケーション、ミドルウェア、フレームワータなどのバージョ メラッドを実更してサーバにアクセス メソッドを変更してサーバにアクセス	まれる/inputタグに埋まっている HTTPで通信している HTTPを近けてアクセスすべ ホージルでアクセスすべ セページがHTTPでもアクセス可能となっている HTTPSとHTTPのコンテンプが現在している プラウザで延明書の警告が 出る 精報が含まれている デイレクトリ内のファイル が一覧表される パージョン番号が表示される 「RACE、TRACKメソット が機能十ち Allow〜フダドGET、 HEAD、POST、OPTIONS は外のメソッドが存する は外のメソッドが存する は外のメソッドが存する はり、アロスにの HEAD、POST、OPTIONS は外のメソッドが存する はアリエ、DELETE、TRACE など)	HTTPSで通信している HTTPS以外ではアクセス できない HTTPSとHTTPのコンテ ンツが混在していない ブラウザで証明書の警告 が出ない デイレクトリ内のファイ ルが一覧表示されない バージョン番号が表示されない TRACE、TRACKメンァ ドが機能しない Allow〜ッダにGET、 HEAD、POST、 OPTIONS以外のメソッド ドが存在しない	響告が出る場合には以下のい すれい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 と一致してか、 ・推奨されない署名アルゴリ ズムの利用 ・不適切な難長 含まれているファイルによっ