セキュア要件リストサンプル

セキュア要件リストサンプル

カテゴリ	項目名	実施効果
認証	ユーザーが入力したパスワードがそのまま表示されない	肩越しに覗き込まれてアカウント奪取（ショルダーハック）されることを防ぐ
	すべての認証がサーバ側で行われる	クライアント側で不正に認証を済ませることを防止する
	ログイン機能、パスワード再設定機能、またはアカウントを忘れた場合の機能を使ってアカウント情報の取得はできない	アカウントに対する総当たり攻撃の成功率の上昇を抑止する
セッション管理	ユーザーがログアウトすると、サーバ側でもセッションが無効になる	有効なセッションを利用したなりすましの危険性を緩和する
	一定時間非アクティブ状態が続くと、セッションがタイムアウトする	有効なセッションを利用したなりすましの危険性を緩和する
アクセス制御	ユーザーは認可されている機能やデータファイル、他のリソースにのみアクセスできる	権限を無視した機能の実行を防ぐ
	センシティブなレコードが保護されており、ユーザーは認可されたオブジェクトやデータのみにアクセスできる	情報漏洩・データ改竄を防ぐ
	アプリケーションが適切に状況に応じた認可を行っており、パラメータ改ざんにより認可されていない操作ができない	想定外の操作を行われる危険性を防ぐ
悪性入力	SQLクエリなどやストアドプロシージャでプリペアドステートメントを使用している	SQLインジェクションによる情報漏洩・破壊を防ぐ
	アプリケーションのセキュリティ管理策などによってOSコマンドインジェクションが防止される	OSコマンドインジェクションによる情報漏洩、任意のコード実行を防ぐ
	アプリケーションが、反射型、格納型およびDOM型クロスサイトスクリプティング（XSS）攻撃の影響を受けない	クロスサイトスクリプティングによるサイト改ざん、なりすましを防ぐ
エラー処理とログ保存	センシティブなデータやサーバーのバージョンなどをエラーメッセージやスタックトレースに出力しない	攻撃者の既知脆弱性を狙った攻撃への意欲を緩和する
ファイルとリソース	URLのリダイレクトおよび転送において、ホワイトリストに含まれる宛先のみが許可される	リダイレクタによるフィッシングの被害を防ぐ
	アプリケーションに送信された信頼できないファイルのデータがファイル入出力コマンドで直接使用されない	パストラバーサルによる重要ファイルへのアクセスを防ぐ

本報告書に関するお問い合わせ先

fenrir.b2b.sales@fenrir.co.jp

フェンリル株式会社

大阪本社

〒530-0011 大阪府大阪市北区大深町 3-1 グランフロント大阪タワー B 14F
TEL:06-6377-7606（代表）　FAX:06-6377-7609

東京支社

〒141-0031 東京都品川区西五反田 2-27-3 A-PLACE五反田 5F
TEL:03-5719-3321（代表）　FAX:03-5719-3325

CONFIDENTIAL