**Hệ thống quản lý sản xuất**

**Tài liệu security**

**2020年　7月 (初版発行)**

はじめに

本仕様書は、ケービーソフトウェア（株）のパッケージソフトである 『生産管理システム』のセキュリティの仕様について纏めたものである。

参考文献：

　　・独立行政法人　情報処理推進機構

「安全なSQLの呼び出し方.pdf」

「安全なウェブサイトの作り方.pdf」

**目　次**

[2020年　7月 (初版発行) 0](#_Toc45627901)

[第１章 SQLインジェクション対策 3](#_Toc45627902)

[第１節 クエリビルダの使用 3](#_Toc45627903)

[第２節 DBエラーメッセージ 3](#_Toc45627904)

[第２章 OSコマンドインジェクション対策 4](#_Toc45627905)

[第１節 OSコマンドの使用時の注意点 4](#_Toc45627906)

[第３章 パス名パラメータの未チェック／ディレクトリ・トラバーサル 5](#_Toc45627907)

[第１節 Webサーバ内のファイル名の取り扱い 5](#_Toc45627908)

[第４章 セッション管理の不備 6](#_Toc45627909)

[第１節 セッションID 6](#_Toc45627910)

[第２節 セッションIDの再発行 6](#_Toc45627911)

[第５章 クロスサイト・スクリプティング 7](#_Toc45627912)

[第１節 エスケープ処理 7](#_Toc45627913)

[第２節 HTMLタグ 7](#_Toc45627914)

[第３節 <script>要素 7](#_Toc45627915)

[第４節 文字コードの指定 7](#_Toc45627916)

[第５節 7](#_Toc45627917)

[第６章 クロスサイト・リクエスト・フォージェリ 8](#_Toc45627918)

[第１節 秘密情報の一致による確認 8](#_Toc45627919)

[第７章 HTTPヘッダ・インジェクション 9](#_Toc45627920)

[第１節 header関数の使用 9](#_Toc45627921)

[第８章 メールヘッダ・インジェクション 10](#_Toc45627922)

[第１節 対象外 10](#_Toc45627923)

[第９章 クリックジャッキング 11](#_Toc45627924)

[第１節 X-Frame-Options ヘッダフィールド 11](#_Toc45627925)

[第１０章 バッファオーバーフロー 12](#_Toc45627926)

[第１節 対象外 12](#_Toc45627927)

[第１１章 アクセス制御や認可制御の欠落 13](#_Toc45627928)

[第１節 ログイン 13](#_Toc45627929)

[第２節 アクセス権 13](#_Toc45627930)

[第１２章 改定履歴 14](#_Toc45627931)

# Chính sách SQL injection

## sử dụng query builder

* Do có cơ thế bind tự động, nên sẽ sử dụng query builder của Laravel
* Do method row, method whereRow không được bind nên không được sử dụng

→　Trường hợp cần phải sử dụng thì phải có sự cho phép của project leader bên KBS

　　　（giả sử là method whereRow、thì có thể bind giá trị 1 cách an toàn bằng param thứ 2）

## DB error message

* Không hiển thị nguyên DB error message vào browser

# Chính sách OS Command injection

## các điểm cần chú ý khi sử dụng OS command

* Trường hợp sử dụng các hàm số có khả năng gây nguy hiểm như （「exec」「system」「passthru」「proc\_open」「shell\_exec」「popen」）thì không sử dụng các giá trị mà user input để làm param

# Chưa check path name parameter/directory traversal

## xử lý file name trong web server

* Không set trực tiếp file name bằng Hidden và Request parameter
* Không set file name trên URL
* Khi mở file thì chỉ định directory cố định, trường hợp file name được chỉ định động thì phải check xem có bao gồm directory name không

# không chuẩn bị quản lý session

## sessionID

* làm sessionID trở nên khó đoán。（không tự tạo sessionID）
* không lưu trữ sessionID ở URL param (lưu trữ ở cookie)

Thay đổi SESSION\_DRIVER của file .env của Laravel thành cookie

* Để đề phòng thì cần xác nhận setting php.ini như sau

　　　　　session.sid\_length = 32

　　　　　session.use\_cookies = 1

　　　　　session.use\_only\_cookies = 1

## Phát hành lại sessionID

* sau khi login thành công thì thực hiện phát hành lại sessionID (sử dụng method regenerate của Laravel)

# Cross-site scripting

## Xử lý escape

* Sử dụng chức năng xử lý escape của Laravel (gói element bằng {{}}), xử lý escape với toàn bộ element xuất ra

## HTML tag

* Trường hợp xuất HTML tag, phải đảm bảo giá trị thuộc tính được để trong dấu ngoặc kép 「“」

## <script> element

* Không tự động tạo nội dung element <script></script>

## Set code ký tự

* Thực hiện set code ký tự （charset）cho field Content-Type của HTTP Response header

Xử lý bằng Laravel middleware。

## Hiển thị message

* không sử dụng giá trị nhập của user vào window.alert、confirm

# Cross-site request forgery

## xác nhận dựa trên khớp thông tin bí mật

* Khi gửi request trong form tag của Laravel view, thì ghi 「@csrf」

※POST、PUT、DELETE request làm đối tượng（nếu không ghi sẽ báo lỗi）

# HTTP Header injection

## Sử dụng hàm header

* Không xuất trực tiếp HTTP Response header、mà sử dụng hàm 「header」。

# Mail header injection

## Ngoài đối tượng

* do không dự định sử dụng mail nên để làm ngoài đối tượng (trường hợp sử dụng sẽ mô tả ở đây)

# Click jacking

## X-Frame-Options header field

* Xuất X-Frame-Options header filed vào HTTP response header

Xử lý bằng Laravel Middleware。

* Trường hợp cần sử dụng iframe、set 「SAMEORIGIN」。

# Buffer overflow

## Ngoài đối tượng

* Do PHPkhông thể thao tác trực tiếp memory nên để làm ngoài đối tượng。

# アクセス制御や認可制御の欠落 thiếu kiểm soát tiếp cận và kiểm soát

## login

* sử dụng userID khi login Windows、để làm single sign-on。

## quyền tiếp cận

* trong user ID khi login Windows、điều tra user master、giới hạn các chức năng có thể sử dụng。
* Trường hợp hiển thị màn mà user không có quyền hiển thị thì sẽ trở về màn top menu

# 改定履歴

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ＮＯ | 内 容 | 承認 | 担当 | 日付 |
| ０ | 初版発行 |  | 西田 | 2020-7-1 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |