

kintone 脆弱性検査結果

1 概要

2016年6月13日から2016年6月15日に、サイバーディフェンス研究所様にて kintone の脆弱性検査を実施いただきました。本資料にて検査結果を公開いたします。

2 検査結果サマリ

今回の検査では脆弱性は検出されませんでした。

3 検査対象について

2016年8月にリリースいたしました kintone に関して、公開前に検査いただきました。検査対象の機能は以下の通りです。

- 新デザイン移行のフラグ管理とリマインド
- REST API 一覧とスキーマ情報の取得
- API でのスレッドコメントの投稿
- Pageview ヒットを送信する内部 API

4 検証観点について

以下の観点で検査いただきました。

検証観点	詳細
認証セッション管理	認証セッションの発行、更新破棄といった一連サイクルにおける問題の有無を特定する他、強度の妥当性について検査します
認証 Cookie	認証セッションに Cookie を利用している場合、Cookie に付与される属性を検査します。
入出力値検証	SQL インジェクションやクロスサイトスクリプティング、ディレクトリトラバーサルなどの攻撃の起点になり得る入出力箇所を検査します。
リクエストの妥当性確認	ログインした利用者又は何らかの処理を実行しうる利用者が、悪意のあるサイトを経由したリクエストを送信することで、処理を意図せず実行させられてしまう可能性について検査します。

ロジック	課金やポイント処理等の不正利用可能性について 検査します。
アクセス制御	各利用者に与えられた権限以外の操作ができる可 能性について検査します。
重要な情報の管理	パスワードやクレジットカード、住所等の個人情報取 り扱い方法の妥当性について検査します。
メール送信機能	メール送信機能が存在するサービスの場合、宛先や 本文等を不正に設定されることでスパムメールに利 用される可能性や、連続大量送信などの迷惑行為 を受ける可能性について検査します。