

7.1 脆弱性診断の概要

プラットフォーム診断 Webサイトを構成するサーバやネットワーク機器など(IPアドレスがあるもの)に既知の脆弱性がないかを調べる。通常、脆弱性スキャナで調べる。

アプリケーション診断 Webアプリケーションに対して、未知の脆弱性がないかを確認する。

	ツールによる診断	手動による診断
動的診断 ブラックボックス診断	OWASP ZAP 自動診断	OWASP ZAP 手動診断
ソースコード診断 ホワイトボックス診断	RIPS	—

7.2 脆弱なアプリケーションBad Todo

OWASP ZAP を立ち上げてから、Firefoxから以下のURLにアクセス

<http://example.jp/todo/>



こんにちは、ゲストさん

一覧 新規追加 インポート エクスポート 問い合わせ ログイン

検索

<input type="checkbox"/>	ID	todo	登録日	期限	完了	添付ファイル	公開
<input type="checkbox"/>	admin	パソコンを買う	2018-03-04	2018-03-05			OK
<input type="checkbox"/>	wasbook	以来の原稿を書く	2018-03-20	2018-03-27		memo.txt	OK

削除 完了 エクスポート

Copyright © 2018 Hiroshi Tokumaru All Rights Reserved.

アカウントを追加して、そのアカウントに対して、脆弱性診断する手順であったが、アカウント追加がうまくできなかったため、アカウントID「wasbook」PWD「wasbook」を使用して脆弱性診断を行った。