セキュリティ診断手順書

「システムに許可されていない機能の実行が可能である」篇

CONFIDENTIAL

はじめに

本書の役割

「システムに許可されていない機能の実行が可能である」の確認手順

内容

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、パラメータの改ざんによる想定外の操作が不可能である

利用するツール

- ブラウザ（IE, Safari, Google Chromeいずれも可）
- ローカルプロキシ

実施対象

- 段階を踏んで処理を行う機能（A > B > C と一連で処理を行う箇所）
- 数量制限などが存在する機能 etc

前提事項

本項は、サイトにより手順が異なるためスクリーンショットは用いずに大まかな検証内容を解説する。

CONFIDENTIAL

Copyright © 2019 Fenrir Inc. All rights reserved.

作業手順

段階を踏んで処理を行う機能の場合

段階を踏んで処理を行う機能において、あえて一連の処理の途中を飛ばしてセキュリティ診断を行う。

上の図のような処理が正しい処理フローのケースで、下の図のように再認証など必須処理の一部を飛ばす。

この結果、正常時と同様に動作した場合は必須な処理を回避することができたとしてNGとなります。

数量制限などがある機能の場合

数量制限などがある機能の場合、対象機能を実行した際に発生する通信の数量制限がかかっているパラメータの値を変更して送信する。

変更前

```
http://www.example.com/classify?id=1&rank=5 HTTP/1.1・・・（以下、略）・・・
```

ユーザー評価を五段階（１から５）で行うという機能（パタメータはrank）に対して、以下のように通信内容を変更して送信する。

変更後

```
http://www.example.com/classify?id=1&rank=100 HTTP/1.1・・・（以下、略）・・・
```

設定した値がそのまま反映された場合はNGとなります。

Copyright © 2019 Fenrir Inc. All rights reserved.

FAQ

Q. エビデンスの取得方法は？

A. 実施した際のスクリーンショットを取得ください

Q. 本項目の調査において留意すべき点はどこか？

A. 以下の３点があげられます。

・飛ばしてはならないプロセスが飛ばせているか？（再認証など）
・画面上からの入力制限値を超える値で検証すること
・それが実施できた場合に直接的な被害が起きるか（※）

※検索機能の画面表示件数を100件までしか増やせないシステムで、通信改ざんで200件表示できることがわかったところで実害はでないため指摘にいたりません。ただし、大量の件数を指定することで他利用者が利用する際のパフォーマンスへの影響を発生させた場合等はNGとなります。

CONFIDENTIAL

Copyright © 2019 Fenrir Inc. All rights reserved.

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

Copyright © 2019 Fenrir Inc. All rights reserved.