ブラウザゲームにおける
脆弱性チェック
について

2015年2月

株式会社サクセス

概要

- 主にブラウザゲームにおける、不正行為に対しての脆弱性の種類や対策例のまとめ

- ブラウザゲーム（サーバサイド）のプログラマ向け（オンラインであれば同様の注意が必要な項目有り）

他ユーザーへのプレゼント不正取得

［不正例］
適当なプレゼントIDを指定してプレゼント取得リクエストを送信し、他のユーザーのプレゼントを不正取得する。

［対策例］
プレゼント排出の際には指定ID以外にアクセスユーザー自身のIDとペアで確認を行う。

取得数値をマイナス指定することでのポイント改ざん

［不正例］
リクエスト中の同時実行回数にマイナス値を指定して
実行リクエストを送信し、ガチャ実行に必要なポイントを
不正増加させる。

［対策例］
リクエスト中に個数指定がある場合、マイナス値の
チェックを確実に行う。

複数同時リクエスト送信による回数制限の解除

［不正例］

アイテム取得リクエストをツールなどを使って
複数同時送信し、取得フラグが更新される前に
取得リクエストを同時実行させることで同じアイテムを
複数取得する。

［対策例］

同じユーザーからの同時リクエスト（特に更新系）は
１つが終わらない限り受付ないようにする。

CrossDomain通信が許可されているため外部APIから任意のAPIを実行できてしまう

［不正例］

ユーザがゲームにSNS連携が完了している状態で、
レスポンスを取得する不正なFlashを外部サイト上で
ユーザが閲覧することで、外部のサイトにユーザ情報を
取得されてしまう。

［対策例］

crossdomain.xmlなどのクロスドメイン許容指定を
確実に行う。

特殊文字がエスケープされていないことによる任意のスクリプト実行が可能（クロスサイトスクリプティング）

［不正例］

任意のスクリプト(<script></script>で囲ったもの）がURLから実行できるため、ユーザーのCookieが奪取される危険性がある。

［対策例］

リクエスト中の特殊文字(</>など）は確実にエスケープ（変換）を行う。

存在しないユーザーへの
メッセージ送信

［不正例］

（メッセージ送信などでポイント等の特典が得られる場合）
適当なユーザーIDへメッセージ送信リクエストを
送信することで不正にポイントを取得する。

［対策例］

メッセージの送信先のユーザーが存在することを確認する。

SQL特殊文字挿入によるデータ改ざん（SQLインジェクション）

［不正例］

任意のSQLがURLから実行できるため、DBデータ閲覧及び改ざんが可能。

［対策例］

・DB操作は必ずプレースホルダーを使用すること。

・使用できない場合はパラメータを完全に解析＆安全性を確かめること。

まとめ

・リクエストパラメータは確実にチェックしましょう。

※数値、文字列、桁数だけではなく、
正しい値（ID）であるかどうか。

・今回の事例がすべてではありません。