ホームページいじれるくん®

セキュリティ資料

基本セキュリティ対策

対策１　ホームページいじれるくん®ログイン機能

ユーザー名パスワードで制限をかけています。その他お客さまDBと照合を行っています。ログインできなければそもそも何もできないため基本的なセキュリティはこの段階で担保されています。

対策２　ログイン後のzipファイルアップロード機能にも制限

ホームページいじれるくん®でダウンロードしたzipファイル、かつ、同じドメインのページのzipファイルでないとファイルのアップロード自体ができない仕組みです。そのため万一ブラウザでログイン後のページが表示されたPCを他の誰かに操作されても不正ファイルをアップされることはありません。

対策３　IP制限

最大３つまでIPを許可し、そのIP以外のアクセスに制限をかけることが可能です。IP制限なしでも使用できます。利便性とセキュリティとバランスを鑑みご判断いただけます。

対策４　便利機能制限

phpとcssをダウンロード＆アップロードできる高度な機能もありますが、そこまでの機能を求めない場合はそれらの機能をオフにすることで余計なリスクを回避できます。

システム内でのセキュリティ対策

対策１　返却時のトークン付与（CSRF対策）

CSRFとは、ユーザー自身が意図しない処理が実行されてしまう脆弱性または攻撃手法です。
本ツールは、サーバー側でがクライアントに対して特定の文字列（トークン）を設定しています。
ユーザーの操作に対しサーバーが「この人に送ったトークンと同じトークンがリクエストに入っているか？」と確認フローを挟むことで攻撃者からの不正なリクエストを防ぎます。
攻撃者はツールのユーザーに送信したトークンの値を知らないため不正な攻撃ができません。

対策２　ページ出力すなわち画面表示にエスケープ処理（XSS対策）

XSSとは、ユーザーがWebページにアクセスすることで不正なスクリプトが実行されてしまう脆弱性または攻撃手法です。
Webページに出力するデータのエスケープ処理を行っており、JSなどを利用したXSS攻撃に対して安全性を確保しております。

対策３　テストアップページのパスワード化およびシステム関連ファイルからの情報読み取りを遮断

テストアップするページやバックアップするページなどの閲覧にパスワード入力を必須としております。
また、設置するシステムファイルは５ファイルありますが、それらのURLを知り得たとして直接アクセスされた場合でも、ログインしていない限り不正操作や情報取得ができないよう対策しております。

システム内でのセキュリティ対策

対策4　そのほか

他のホームページいじれるくん®ユーザーから故意にファイルを自動アップされるようなことはありません。ボタンひとつで本番化やテストアップする際の自動連携機能も、お客さまの情報をDBのAPIにて照合して行う仕組みになっており、他のアタックを防御します。