* 1. 発見した脆弱性詳細

1. クリックジャッキング

* 危険度

Low

* 解説

リンクやボタンなどの要素を隠蔽・偽装してクリックを誘い、利用者の意図しない動作をさせようとする手法。

▼再現方法

HTMLのiframeタグを使用してクリックジャッキングを行うサイトを指定して、そのサイトの上にcssで透過させたリンクやボタンを埋め込む。

上記のようなHTMLファイルを作成し、本システムのログイン画面にクリックジャッキングを行い、ログインボタンをクリックしたところ、透過させたボタンの遷移先（利用者の意図していないページ）に遷移したことからクリックジャッキングに脆弱であると判断できる。

なお、本検証で使用したソースコードは下記参照。

[使用したソースコード]

* 想定される被害・影響

・データベースサーバーシステムが停止する。

・実行中のプログラムが強制終了してしまう。

* 対策

・バリデーション（入力の検証）：データのサイズや書式などが想定どおりになっていることを確認する。

・サニタイジング（無害化）：データ内に危険なコードなどが含まれていたら実行不能な状態にする

* 備考

特になし。