

脆弱性学習サイト「Terminal X」企画書

作成日: 2025年7月4日

1. 企画概要

本企画は、システムの脆弱性に関する授業課題の一環として、意図的に脆弱性を組み込んだWebアプリケーションを設計・開発するものである。

テーマとして「ダークウェブに存在するような、法外な商品を扱うECサイト」を設定。ユーザーがハッカー向けのレトロなOSを操作しているかのような独特のUI/UXを提供することで、攻撃・防御の学習体験をより没入感のあるものにすることを目的とする。

プロジェクト名は「Terminal X」とする。

2. コンセプト

2.1. テーマ: 「ターミナルOS」風UI

サイト全体を一つのOSのようにデザインし、ユーザーは「秘密の端末を操作している」かのような体験を得る。一般的なECサイトの親切で美しいUIとは一線を画し、無機質さ、秘密の操作感、レトロなハッキング感を重視する。

- 配色: 黒い背景に、緑や琥珀色のテキストを基本とする。
- フォント: 全て等幅フォントで統一し、コード感を演出する。
- インターフェース: コマンド入力欄や、ウィンドウシステムのような演出を取り入れる。
- アイコン: 一般的なアイコンは使用せず、[BRACKET] のようなテキスト表現に置き換える。



2.2. 学習目的

以下の代表的な脆弱性を意図的に実装し、その攻撃手法と対策について実践的に学ぶ。

- SQLインジェクション (SQLi)
- クロスサイトスクリプティング (XSS)
- 不安全なダイレクトオブジェクト参照 (IDOR)
- 認証・認可の不備(なりすまし)
- パラメータ改ざん

3. システム構成(案)

ユーザー情報に基づき、低成本で実現可能な構成を提案する。

- バックエンド: Python(cgi)
- データベース: SQLite

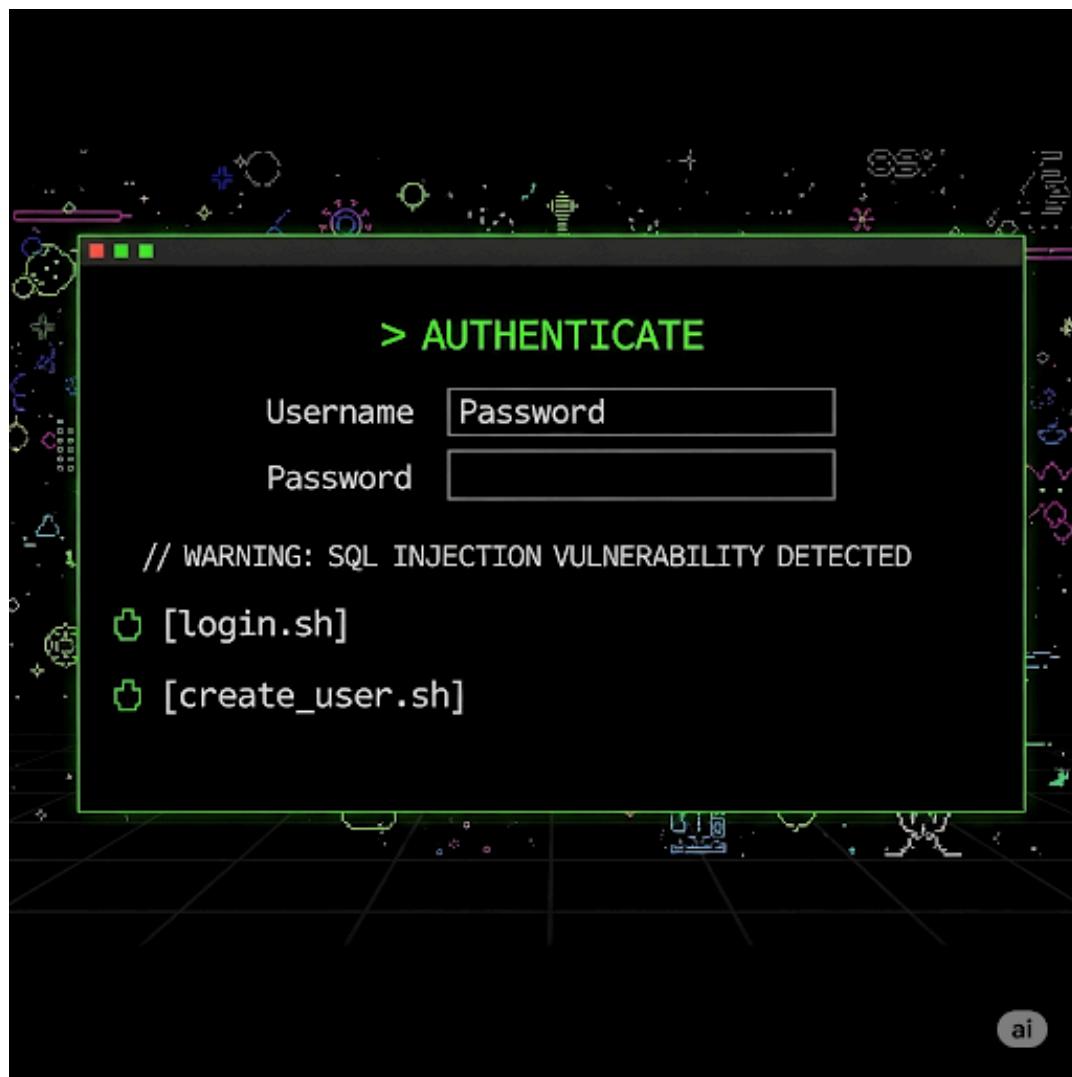
- フロントエンド: HTML, CSS
- ホスティング: ローカル環境

4. 画面設計・UIモックアップ

これまでに生成したUIのイラスト一覧。

4.1. ログイン／登録画面

機能: ユーザー認証を行う。



4.2. マイページ画面

機能: ユーザーが自身の登録情報を管理する。



4.3. 商品一覧ページ

機能: 販売されている商品の一覧を表示する。ファイルリストのようなUI。

!

The screenshot shows a game interface with a central table titled "PRODUCT_CATALOG". The table lists items with their IDs, names, and prices. The columns are labeled "STELS ID SELLR" and "Price". The table has 8 rows. Row 1 contains a small icon of a shield-like logo. Rows 2, 3, 4, and 5 each contain a different type of cipher-related item. Rows 6, 7, and 8 contain "Enigma_Pack" items. The "Price" column uses BTC for most items except for the last one which uses USD (\$). The background shows some UI elements like "PLEST", "ST555", and "BUBBS".

STELS ID SELLR		Price
1	Item_X123	0,05 BTC
2	Item	1,20 BTC
3	Cipher_003	5,00 BTC
5	Cipher_007	1,20 BTC
5		3,40 BTC
4	Cipher_007	3,50 BTC
4	Enigma_Pack	1,00 BTC
6	Engma_Pack	2,60 BTC
7	Vendor_A5	3,50 BTC
8	BlackOps_420	\$,50 BTC

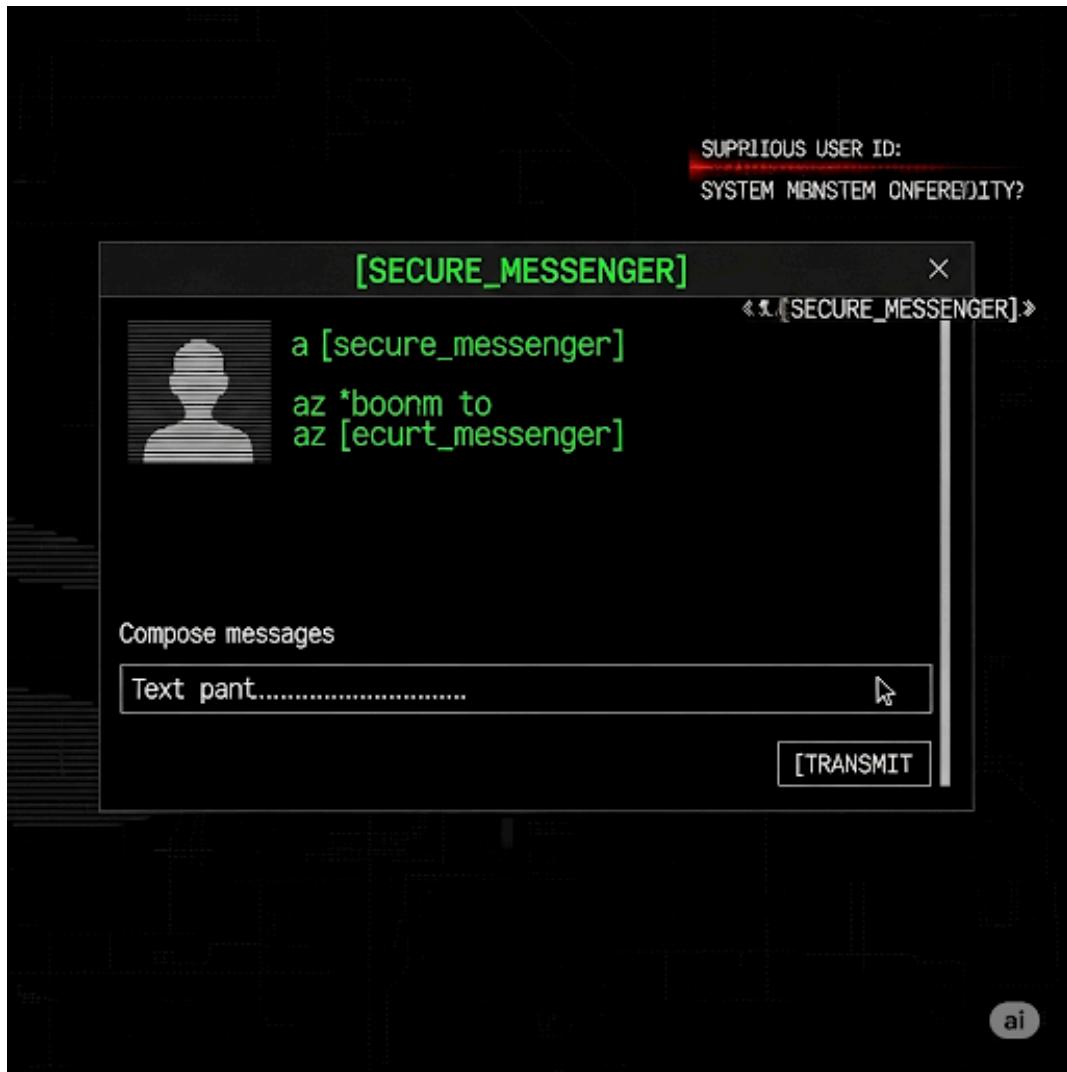
4.4. 商品詳細ページ

機能: 個別商品の詳細情報を表示する。



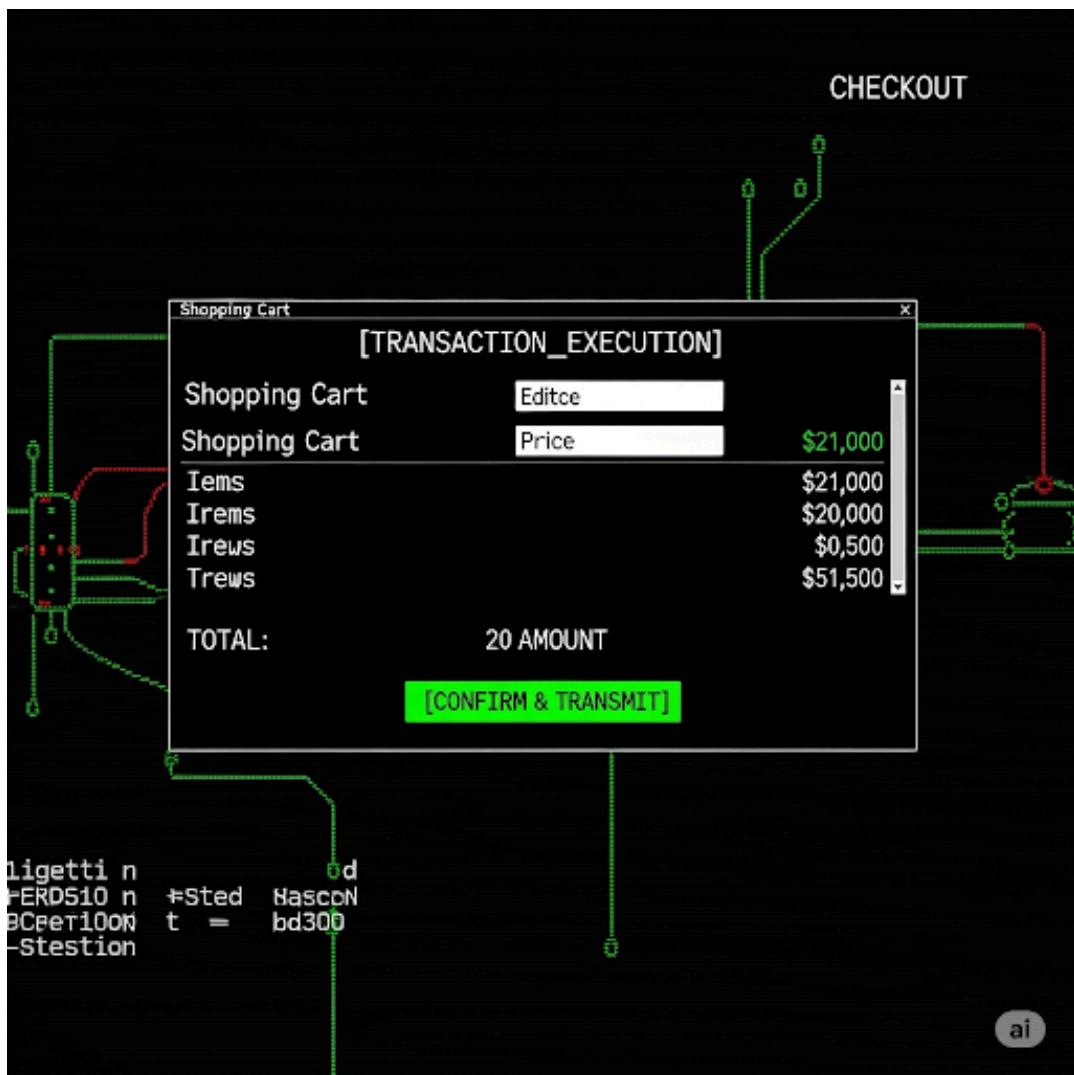
4.5. DMページ

機能: ユーザー間でダイレクトメッセージを送受信する。!



4.6. 決済ページ

機能: 商品の購入手続きをを行う。



4.7. 購入履歴ページ

機能: 過去の購入履歴をログファイルのように表示する。



5. 実装する脆弱性一覧

ページ	主な機能	実装する脆弱性	攻撃シナリオの例
ログイン画面	認証	SQLインジェクション	不正なSQL文で認証を回避し、管理者としてログインする。
マイページ	ユーザー情報管理	IDOR	URLのIDを書き換え、他人のアカウント情報を閲覧・改ざんする。
商品詳細	レビュー表示	Stored XSS	レビューに悪性スクリプトを埋め込み、閲覧者のクッキーを窃取する。
DMページ	メッセージ送受信	認証不備(なりすまし)	送信者IDを偽装し、管理者になりすましてフィッシングDMを送る。
決済ページ	購入処理	パラメータ改ざん	商品の価格をブラウザ

ページ	主な機能	実装する脆弱性	攻撃シナリオの例
			上で不正に書き換え、0円などで購入する。
購入履歴	履歴閲覧	IDOR	URLのIDを書き換え、他人の購入履歴(機密情報)を閲覧する。

6.まとめ

本プロジェクト「Terminal X」を通じて、攻撃者の視点からシステムを分析・実践することで、机上の学習だけでは得られない脆弱性への深い理解を目指す。独創的なUI/UXは、学習へのモチベーションを高め、記憶に残る課題制作に貢献すると考える。

7. 別UIコンセプト案

「ターミナルOS」風UIとは異なるアプローチのUIデザイン案。

7.1. コンセプト1:『グリッチアート / ヴェイパーウェイヴ』スタイル

コンセプト:「壊れかけのデジタル空間」90年代の個人サイトのような、バグやデータ破損で崩壊しかけているウェブサイトを表現。不安定さが逆に不気味さを醸し出す。



7.2. コンセプト2:『ミニマリスト / 黒塗り文書』スタイル

コンセプト:「極秘の機密文書データベース」政府機関の機密データベースに不正アクセスしているかのような、冷たく無機質なUI。触れてはいけない情報を扱う、知能的で冷徹な闇市場の雰囲気を演出。



7.3. コンセプト3:『深海生物 / アビス』スタイル

コンセプト:「未知の深海に存在する、静かで美しい生態系」グロテスクさを排し、深海で自ら発光する生物たちの神秘的で少し不気味な美しさを表現。「静かで、底知れず、何が潜んでいるかわからない」という深淵のような恐怖を演出。

