

☞ 早めのチェック ☜
3工程によるセキュリティ品質確保

「はじめに - 脆弱性の分類と開発工程」

2010年4月
IPA セキュリティセンター 企画グループ

〔セキュア・プログラミング講座 Webアプリケーション編 にもとづく〕
<http://www.ipa.go.jp/security/awareness/vendor/programming>

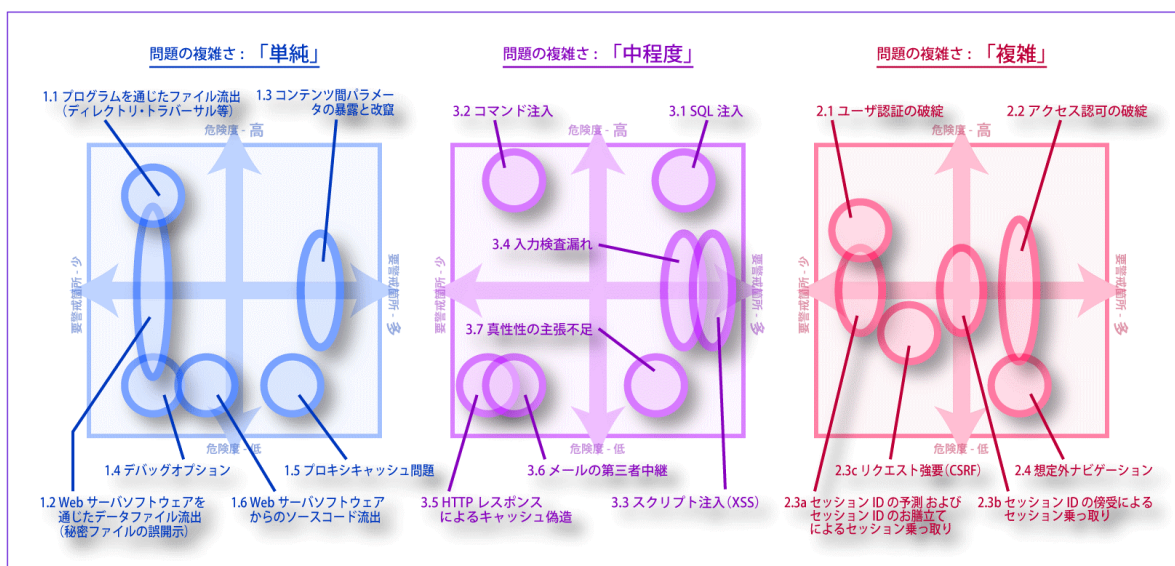


Webアプリケーション脆弱性 の分類と全体観把握

3つの観点

- Webアプリケーション脆弱性の3つの観点
 - 危険度： 攻撃によってもたらされる被害の深刻さ
 - 分類 「高」「中」「低」
 - 対策の優先度にかかわる
 - 要警戒箇所： Webサイト中の脆弱性発生を警戒すべき箇所の多さ
 - 分類 「多」「中」「少」
 - プログラム修正コストにかかわる
 - 問題の複雑さ： 攻撃と防御の仕組みの複雑さ
 - 分類 「単純」「中程度」「複雑」
 - 対策の重点を置くべき開発工程にかかわる

3つの観点からの脆弱性のマップ



※ 各項目の先頭に付いている番号は、「Webアプリケーション脆弱性対策チェックリスト」における番号

危険度

- 「危険度」——攻撃によってもたらされる被害の深刻さ
 - 高
 - 短期間の攻撃でWebサイト全体が大きな打撃を被る
 - 例 SQL注入、コマンド注入、ディレクトリトラバーサル
 - 中
 - Webサイトやユーザの一部が被害を被る
 - 例 スクリプト注入(XSS)、セッションIDの傍受によるセッション乗っ取り
 - 低
 - 低い確率でWebサイトやユーザの一部に被害が生じるか、または、攻撃者に攻撃のヒントを与える
 - 例 HTTPレスポンスによるキャッシュ偽造、デバッグオプション
- 対策の優先度にかかわる
 - できる限り脆弱性への対処を行うべきであるが、予算や期間に限りがある場合は、危険度の高いものを優先する

要警戒箇所

- 「要警戒箇所」——Webサイト中の脆弱性発生を警戒すべき箇所の多さ
 - 多
 - 画面表示項目やフォーム入力項目の規模
 - 例 スクリプト注入(XSS)、SQL注入、入力検査漏れ
 - 中
 - 画面数の規模
 - アクセス認可の破綻、プロキシキャッシュ問題
 - 少
 - サイトの一部に限定されるもの
 - コマンド注入、ユーザ認証の破綻、メールの第三者中継
- プログラム修正コストにかかわる
 - 「要警戒箇所」の多い問題は、プログラム修正コストも大きくなる
 - 予防的プログラミングを行う重点候補

問題の複雑さ

- 「問題の複雑さ」——攻撃と防御の仕組みの複雑さ
 - 単純
 - 保護し忘れていた秘密データを呼び出す等
 - 例 ディレクトリトラバーサル、秘密ファイルの誤開示、コンテンツ感パラメータの暴露と改竄
 - 中程度
 - 単一の画面に対する比較的技術を要する攻撃
 - 例 SQL注入、コマンド注入、スクリプト注入(XSS)
 - 複雑
 - 複数ページ構造の仕組みに対する攻撃
 - 例 認証の破綻、認可の破綻、セッション乗っ取り
- 対策の重点をおくべき開発工程にかかわる
 - 複雑な問題は、設計段階から準備しておく必要がある
 - 中程度の問題は、プログラミング時の考慮でも足りる場合がある

3回コース・複雑さ・工程

- セミナ3回コース・問題の複雑さ・開発工程 の関係
 - 第1回
 - 問題の複雑さ＝「単純」の脆弱性を取り上げる
 - 要件定義段階から考慮しておくことよい問題
 - プラス、総論その1「対策の分類」「開発工程」に言及
 - 第2回
 - 問題の複雑さ＝「複雑」の脆弱性を取り上げる
 - 設計段階における十分な考慮を要する問題
 - プラス、総論その2「より良いWebアプリケーション設計のヒント」
 - 第3回
 - 問題の複雑さ＝「中程度」の脆弱性を取り上げる
 - 実装段階における予防が対策の中心となる問題
 - 著名な脆弱性: SQL注入、XSS等



ご質問をどうぞ

Q & A