

平成19年度 春期 テクニカルエンジニア（情報セキュリティ） 午後I 解答例

この解答例は、独立行政法人 情報処理推進機構 情報処理技術者試験センターが公表しているものです。著作権は、同センターにありますので、その点ご注意ください。

問 1

出題趣旨：

情報システムの構成要素は多岐にわたるが、中でも顧客の要求に応じて開発されるアプリケーションプログラムのセキュリティ脆弱性を少なくすることは、ソフトウェアエンジニアリングとしても重要な課題である。

本問では、システム開発の過程で脆弱性低減のために実施すべき作業についての知識を確認した上で、脆弱性を発生させないための具体的なプログラミングにおける技術的対策に関する知識・能力を問う。

設問 1

- (1) a - スタック b - val2 c - val1
 d - 権限昇格 e - 関数呼出し f - ヒープ

設問 2

- (1) ア - 128
(2) ・ 攻撃者に読取り権限のない任意のファイルの内容が表示されてしまう。
 ・ プログラムが意図したファイル以外の任意のファイルの内容が表示されてしまう。
(3) ・ 最初のコマンドライン引数が 128 バイト未満であるという条件を論理積として加える。
 ・ `if (argc > 1 && strlen(argv[1] < 128) {`

設問 3

- ・ 変数と戻りアドレス格納部分の間に特別な数値をあらかじめ埋め込んでおき、この数値がプログラム実行時に変更されていないことを確認する。
- ・ 変数と戻りアドレス格納部分の間に乱数値をあらかじめ埋め込んでおき、この乱数値がプログラム実行時に変更されていないことを確認する。

講評：

問 1 では、C++言語におけるセキュアプログラミングについて出題した。全体として、正答率は低かった。

設問 1 では、d の正答率が低かった。バッファオーバーフローが起きると、権限昇格やシェルコードの実行などが起こり得ることを十分に認識してもらいたい。

設問 2 では、バッファオーバーフローの発生の仕組みが理解できていないと思われる解答が散見された。特に (2) で、`afile` の内容の表示についてだけ記述した解答が多かった。コマンドライン引数を変更すれば、任意のファイルの内容を表示できることに気づいてほしかった。

設問 3 も正答率が低かった。セキュアプログラミングだけでなく、コンパイラや実行環境による検知と防止機能を併せて使用することによって、バッファオーバーフローに対する多層防御が図れることを理解してほしい。

設問 2

(1) ①②

- ・集計担当者以外はアンケートの回答を閲覧できないこと
- ・従業員が匿名でアンケートに回答できること
- ・部門の担当者が提出漏れをチェックできること
- ・アンケートの回答を 1 人 1 回答に制限できること

(2) シリアル番号とその署名は各回答者しか知り得ず、また、シリアル番号の偽造は困難であるから

設問 3

(1) シリアル番号から回答者を特定できないようにする必要があるから

- (2) ・同じシリアル番号の回答がないかどうかをチェックする。
・使用していないシリアル番号の回答がないかどうかをチェックする。

講評：

問 4 では、社内のアンケートシステムにおける暗号方式について出題した。全体として、正答率は低かった。

設問 1 (2) では、“線形攻撃を行う”といった誤った解答が見られた。対象業務の特性を正しく把握した上で、暗号技術を適切に利用することを理解してほしい。

設問 2 (2) は、“各回答者しか知り得ない”、“署名が偽造できない”のどちらか一方だけを記述している解答が多かった。また、“本人しかアンケートファイルを開けないので”という解答が多かったが、自分のアンケートファイルから得られる情報を基に、他人のアンケートファイルを偽造する攻撃を防止する必要性があることを理解してほしい。

注：この解答例に関するメールでのご質問には、応じかねます。あしからずご了承ください。