令和 4 年度 春期 情報処理安全確保支援士

＜午後Ⅰ解答・解説＞

＜問 1＞ Web アプリケーションプログラム開発のセキュリティ対策

●設問 1

［試験センターによる解答例］

(1) ア

(2) プレースホルダ（7 字）

(3) a：改行コード（5 字）

＜解説＞

(1) 改行コードは"Carriage Return（CR）"と"Line Feed（LF）"から成り、これをそのままコードで表すと、"¥r¥n"である。HTTP レスポンスヘッダではこれが URL エンコードされるため、"%0D%0A"になる。

(2) 表 1 の SQL インジェクション対策はバインド機構と呼ばれる。これは、変数部分にプレースホルダと呼ばれる特殊文字「?」を使用して SQL 文の雛形をあらかじめ用意しておき、後からそこに実際の値を割り当てて SQL 文を完成させる方法である。割り当てられる変数は完全な数値定数もしくは文字列定数として扱われるため、変数の中に SQL 文として特別な意味をもつ文字が含まれていたとしても、それらは自動的にエスケープ処理され、単なる文字として認識される。

(3) メールヘッダインジェクションは、送信先のアドレス（To）は固定で、送信者のアドレス（From）と本文をフォームから入力する仕組みになっているようなメール送信プログラムにおいて、送信者のアドレスとして、改行コードとメールヘッダを含む任意の文字列を入力することで、意図しないアドレス宛てにメールを送信させる手口である。したがって、外部からの入力の全てについて、改行コードを削除することが対策となる。

●設問２

［試験センターによる解答例］

(1) クエリ文字列の id に、未参加のプロジェクト ID を指定する。(29 字)

(2)・プロジェクトを示すパラメタを外部から指定できないから（26 字）
・セッション情報からプロジェクト ID を取得するから（24 字）

(3) b：ウ

(4) c：stmt

＜解説＞

(1) 問題文にあるように、情報選択機能では、GET リクエストのクエリ文字列に指定されたプロジェクト ID を取得し、チェックせずに利用している。GET リクエストのクエリ文字列は利用者が変更可能であるため、id の値を未参加のプロジェクト ID にすることで、未参加のプロジェクトに参加しているかのように偽ることができる。

(2) 方法 2 では、GET リクエストのクエリ文字列ではなく、セッション情報から利用者情報を取得し、当該利用者情報からプロジェクト ID を取得する。表 2 の注記にあるように、セッション ID はログイン時に発行される推測困難な値であり、cookie に格納されている。このセッション情報からプロジェクト ID を取得する方式であれば、利用者がプロジェクトを示すパラメタを外部から指定することはできないため、方法 1 の脆弱性は解決される。

(3) プレースホルダを用いて作成した SQL 文をセットしているので、該当するのは"java.sql.PreparedStatement"インタフェースである。

(4) 図 2 の 9 行目では、7 行目と 8 行目で"stmt"に格納した SQL 文に、"setInt"メソッドを用いて"projectId"の値をセットしている。したがって、 c には"stmt"が入る。

●設問３

［試験センターによる解答例］

d：情報番号 = ? AND プロジェクト ID = ?

＜解説＞

情報選択機能と同様の脆弱性があったということから、修正前には利用者が任意の情報番号を指定することで、参加していないプロジェクトの情報を表示できたと思われる。図 1 の情報管理テーブルを見ると、情報番号が主キー、プロジェクト ID が外部キーとなっているので、情報番号だけでなく、利用者が参加しているプロジェクト ID を WHERE 句の AND 条件に加えることで、上記の問題を解決できる。これをプレースホルダを用いて記述するので、［ d ］には"情報番号 = ? AND プロジェクト ID = ?"が入る。

＜問２＞ セキュリティインシデント対応

●設問１

［試験センターによる解答例］

(1) a：ア
　 b：エ

(2) 外部から LAN 側への通信の許可設定が変更される。(24 字)

(3) PC からのファイル操作ではアクセスできない領域のファイルが暗号化されたから (37 字)

＜解説＞

(1) a：ホスト名から IP アドレスを求める（名前解決）のに用いられるのは A レコードである。

b：「300 秒に設定されていた」という記述から、［ b ］に入るのは A レコードに設定された内容をキャッシュに保持できる時間を表す TTL（Time To Live）である。

(2) 表 2 のファイアウォール機能の説明にあるように、ルータ-A はインバウンド通信を全て拒否する設定となっているが、WAN 側から UPnP 機能を有効にできるとすれば、上記のファイアウォールの設定が変更され、外部から LAN 側へのインバウンド通信が許可されてしまうことが考えられる。

(3) K 氏が NAS-A を調査した結果、ファイル共有機能でも Web 操作機能でもアクセスできない/root ディレクトリ配下のファイルも暗号化されていたことが判明している。この結果が、PC からのファイル操作で暗号化されたわけではなく、