

午後Ⅰ試験

問1

問1では、情報共有用のWebシステムの開発を題材に、システム開発における脆弱性^{ぜい}の分析と対策方法について出題した。全体として正答率は平均的であった。

設問1(1)は、正答率がやや低かった。ウのHTML改行タグの解答が多かった。HTTPとHTMLの理解が不十分である結果と想定される。

設問2(3)は、正答率がやや低かった。StatementでもSQLの実装は可能であるが、本文に示されているプレースホルダの実装にはStatementを継承したPreparedStatementが必要である。脆弱性対策手法については、理論や用語だけではなく、その具体的な方法を理解してほしい。

設問3は、正答率がやや低かった。SQLの構文が誤っている解答が見受けられた。データベースのアクセス制御の設計、実装及びレビューを行うために、SQLの構文やE-R図の表記法を知っておいてほしい。

問2

問2では、IoT機器の製品を題材に、セキュリティインシデント対応と脆弱性対策^{ぜい}について出題した。全体として正答率は平均的であった。

設問2(3)は、正答率が平均的であった。本文に示した認証なしでアクセスできるURLでは除外リストとの比較に漏れがないように、URLデコードを行った上で、“../”などを含んだパス名を正規化してから、除外リストとの比較を行う必要があることを理解してほしい。

設問3(2)は、正答率が平均的であった。ファームウェアのアップデート時にアーカイブファイルを展開するために使っているtarコマンドが、製品Xでは不要なオプションも使える設定であり、本設問は、そのようなオプションの悪用を防ぐ対策を問うているので、sudoの設定でオプションの使用を制限するなど、具体的に解答してほしい。

設問4は、正答率が低かった。インターネット上でIoT機器を検出する方法と、それを抑止する方法を知っておいてほしい。

問3

問3では、スマートフォン向けQRコード決済サービスを題材に、決済サービスで不正利用が発生するリスクとその対策について出題した。全体として正答率は平均的であった。

設問2(4)は、正答率が低かった。公開鍵暗号の仕組みにおいて、電子証明書の有効性を確認する方法が必要となるが、このことを理解していないと思われる解答が多かった。公的個人認証サービスでは、地方公共団体情報システム機構(J-LIS)がOCSPによる方法とCRLによる方法を提供している。これらの方法について知っておいてほしい。

設問2(5)は、正答率がやや低かった。Qアプリが表示するランダムな数字について、“当該数字を撮影する”という解答が多かった。そういった方法では、撮影したのが本人なのかを確認できない。オンラインにおける本人確認手法は、今後も様々な手法が提案されられると思われるが、現在使われている最新の手法を理解してほしい。

設問3(1)は、正答率が平均的であった。オンラインサービスの設計では、どのような不正が発生するのかを洗い出して、対策を検討することを心掛けてほしい。