Q0001

セキュア開発・脆弱性管理
タグ：STRIDE
用語：STRIDEの確認ポイント1：なりすまし、改ざん、否認、情報漏えい、サービス妨害、権限昇格で脅威を分類する手法

次の説明に最も合う用語はどれか。なりすまし、改ざん、否認、情報漏えい、サービス妨害、権限昇格で脅威を分類する手法

A. STRIDE
B. SAST
C. IAST
D. CVE

答え・解説

Q0001 正答：A. STRIDE

解説：STRIDEは、なりすまし、改ざん、否認、情報漏えい、サービス妨害、権限昇格で脅威を分類する手法。ほかの選択肢は目的又は適用場面が異なる。

Q0002

セキュア開発・脆弱性管理
タグ：STRIDE
用語：STRIDEの確認ポイント2：なりすまし、改ざん、否認、情報漏えい、サービス妨害、権限昇格で脅威を分類する手法

STRIDEの説明として最も適切なものはどれか。

A. 実行せずにソースコードなどを解析して脆弱性を検出する手法
B. なりすまし、改ざん、否認、情報漏えい、サービス妨害、権限昇格で脅威を分類する手法
C. 実行時の内部情報と外部テストを組み合わせて脆弱性を検出する手法
D. 公開された脆弱性へ一意な識別番号を付ける仕組み

答え・解説

Q0002 正答：B. なりすまし、改ざん、否認、情報漏えい、サービス妨害、権限昇格で脅威を分類する手法

解説：STRIDEの要点は「なりすまし、改ざん、否認、情報漏えい、サービス妨害、権限昇格で脅威を分類する手法」である。名称が似た概念でも、対象とする処理や目的を区別する。

Q0003

セキュア開発・脆弱性管理
タグ：STRIDE
用語：STRIDEの確認ポイント3：なりすまし、改ざん、否認、情報漏えい、サービス妨害、権限昇格で脅威を分類する手法

用語と説明の組合せとして適切なものはどれか。論点は「STRIDE」である。

A. SAST：なりすまし、改ざん、否認、情報漏えい、サービス妨害、権限昇格で脅威を分類する手法

B. IAST：なりすまし、改ざん、否認、情報漏えい、サービス妨害、権限昇格で脅威を分類する手法

C. STRIDE：なりすまし、改ざん、否認、情報漏えい、サービス妨害、権限昇格で脅威を分類する手法

D. CVE：なりすまし、改ざん、否認、情報漏えい、サービス妨害、権限昇格で脅威を分類する手法

答え・解説

Q0003 正答：C. STRIDE：なりすまし、改ざん、否認、情報漏えい、サービス妨害、権限昇格で脅威を分類する手法

解説：正しい組合せは「STRIDE：なりすまし、改ざん、否認、情報漏えい、サービス妨害、権限昇格で脅威を分類する手法」。用語だけでなく、何を守り、何を処理する概念かを確認する。

Q0004

セキュア開発・脆弱性管理
タグ：STRIDE
用語：STRIDEの確認ポイント4：なりすまし、改ざん、否認、情報漏えい、サービス妨害、権限昇格で脅威を分類する手法

「STRIDE」は、なりすまし、改ざん、否認、情報漏えい、サービス妨害、権限昇格で脅威を分類する手法。

A. ○

B. ×

答え・解説

Q0004 正答：○

解説：正しい。STRIDEはなりすまし、改ざん、否認、情報漏えい、サービス妨害、権限昇格で脅威を分類する手法。実務では対象、目的、前提条件を併せて確認する。

Q0005

セキュア開発・脆弱性管理
タグ：STRIDE
用語：STRIDEの確認ポイント5：なりすまし、改ざん、否認、情報漏えい、サービス妨害、権限昇格で脅威を分類する手法

組織が「なりすまし、改ざん、否認、情報漏えい、サービス妨害、権限昇格で脅威を分類する手法」ために採用すべき概念又は仕組みはどれか。

A. STRIDE
B. SAST
C. IAST
D. CVE

答え・解説

Q0005 正答：A. STRIDE

解説：この目的に対応するのはSTRIDEである。なりすまし、改ざん、否認、情報漏えい、サービス妨害、権限昇格で脅威を分類する手法という機能・考え方を持つためである。

Q0006

セキュア開発・脆弱性管理
タグ：STRIDE
用語：STRIDEの確認ポイント6：なりすまし、改ざん、否認、情報漏えい、サービス妨害、権限昇格で脅威を分類する手法

「STRIDE」について、誤解を避けるための説明として最も適切なものはどれか。

A. 公開された脆弱性へ一意な識別番号を付ける仕組み
B. なりすまし、改ざん、否認、情報漏えい、サービス妨害、権限昇格で脅威を分類する手法
C. 実行時の内部情報と外部テストを組み合わせて脆弱性を検出する手法
D. 実行せずにソースコードなどを解析して脆弱性を検出する手法

答え・解説

Q0006 正答：B. なりすまし、改ざん、否認、情報漏えい、サービス妨害、権限昇格で脅威を分類する手法

解説：STRIDEはなりすまし、改ざん、否認、情報漏えい、サービス妨害、権限昇格で脅威を分類する手法。似た用語との違いは、対象、時点、責任又は処理方法にある。

Q0007

セキュア開発・脆弱性管理
タグ：STRIDE
用語：STRIDEの確認ポイント7：なりすまし、改ざん、否認、情報漏えい、サービス妨害、権限昇格で脅威を分類する手法

「STRIDE」は、実行せずにソースコードなどを解析して脆弱性を検出する手法。

A. ○
B. ×

答え・解説

Q0007 正答：×

解説：誤り。記述はSASTの説明である。STRIDEはなりすまし、改ざん、否認、情報漏えい、サービス妨害、権限昇格で脅威を分類する手法。

Q0008

セキュア開発・脆弱性管理
タグ：STRIDE
用語：STRIDEの確認ポイント8：なりすまし、改ざん、否認、情報漏えい、サービス妨害、権限昇格で脅威を分類する手法

次の状況で中心となる論点はどれか。「なりすまし、改ざん、否認、情報漏えい、サービス妨害、権限昇格で脅威を分類する手法」ことが求められている。

A. IAST
B. CVE
C. SAST
D. STRIDE

答え・解説

Q0008 正答：D. STRIDE

解説：中心となる論点はSTRIDEである。判断では、説明中の目的語と処理の方向を手掛かりにする。

Q0009

セキュア開発・脆弱性管理
タグ：STRIDE
用語：STRIDEの確認ポイント9：なりすまし、改ざん、否認、情報漏えい、サービス妨害、権限昇格で脅威を分類する手法

「なりすまし、改ざん、否認、情報漏えい、サービス妨害、権限昇格で脅威を分類する手法」という特徴を持つものを選べ。

A. STRIDE
B. CVE
C. IAST
D. SAST

答え・解説

Q0009 正答：A. STRIDE
解説：STRIDEが該当する。定義はなりすまし、改ざん、否認、情報漏えい、サービス妨害、権限昇格で脅威を分類する手法であり、他の候補とは機能が異なる。

Q0010

セキュア開発・脆弱性管理
タグ：SAST
用語：SASTの確認ポイント1：実行せずにソースコードなどを解析して脆弱性を検出する手法

次の説明に最も合う用語はどれか。実行せずにソースコードなどを解析して脆弱性を検出する手法

A. DAST
B. SAST
C. ファジング
D. CWE

答え・解説

Q0010 正答：B. SAST
解説：SASTは、実行せずにソースコードなどを解析して脆弱性を検出する手法。ほかの選択肢は目的又は適用場面が異なる。

Q0011

セキュア開発・脆弱性管理
タグ：SAST
用語：SASTの確認ポイント2：実行せずにソースコードなどを解析して脆弱性を検出する手法

SASTの説明として最も適切なものはどれか。

A. 稼働中アプリケーションへ入力を送り外部から脆弱性を検出する手法
B. 大量の異常・予測困難な入力を与えて不具合を検出する試験
C. 実行せずにソースコードなどを解析して脆弱性を検出する手法
D. ソフトウェアの弱点の種類を体系的に分類した一覧

答え・解説

Q0011 正答：C. 実行せずにソースコードなどを解析して脆弱性を検出する手法

解説：SASTの要点は「実行せずにソースコードなどを解析して脆弱性を検出する手法」である。名称が似た概念でも、対象とする処理や目的を区別する。

Q0012

セキュア開発・脆弱性管理
タグ：SAST
用語：SASTの確認ポイント3：実行せずにソースコードなどを解析して脆弱性を検出する手法

用語と説明の組合せとして適切なものはどれか。論点は「SAST」である。

A. DAST：実行せずにソースコードなどを解析して脆弱性を検出する手法
B. ファジング：実行せずにソースコードなどを解析して脆弱性を検出する手法
C. CWE：実行せずにソースコードなどを解析して脆弱性を検出する手法
D. SAST：実行せずにソースコードなどを解析して脆弱性を検出する手法

答え・解説

Q0012 正答：D. SAST：実行せずにソースコードなどを解析して脆弱性を検出する手法

解説：正しい組合せは「SAST：実行せずにソースコードなどを解析して脆弱性を検出する手法」。用語だけでなく、何を守り、何を処理する概念かを確認する。

Q0013

セキュア開発・脆弱性管理
タグ：SAST
用語：SASTの確認ポイント4：実行せずにソースコードなどを解析して脆弱性を検出する手法

「SAST」は、実行せずにソースコードなどを解析して脆弱性を検出する手法。

A. ○
B. ×

答え・解説

Q0013 正答：○

解説：正しい。SASTは実行せずにソースコードなどを解析して脆弱性を検出する手法。実務では対象、目的、前提条件を併せて確認する。

Q0014

セキュア開発・脆弱性管理
タグ：SAST
用語：SASTの確認ポイント5：実行せずにソースコードなどを解析して脆弱性を検出する手法

組織が「実行せずにソースコードなどを解析して脆弱性を検出する手法」ために採用すべき概念又は仕組みはどれか。

A. DAST
B. SAST
C. ファジング
D. CWE

答え・解説

Q0014 正答：B. SAST

解説：この目的に対応するのはSASTである。実行せずにソースコードなどを解析して脆弱性を検出する手法という機能・考え方を持つためである。

Q0015

セキュア開発・脆弱性管理
タグ：SAST
用語：SASTの確認ポイント6：実行せずにソースコードなどを解析して脆弱性を検出する手法

「SAST」について、誤解を避けるための説明として最も適切なものはどれか。

A. ソフトウェアの弱点の種類を体系的に分類した一覧
B. 大量の異常・予測困難な入力を与えて不具合を検出する試験
C. 実行せずにソースコードなどを解析して脆弱性を検出する手法
D. 稼働中アプリケーションへ入力を送り外部から脆弱性を検出する手法

答え・解説

Q0015 正答：C. 実行せずにソースコードなどを解析して脆弱性を検出する手法

解説：SASTは実行せずにソースコードなどを解析して脆弱性を検出する手法。似た用語との違いは、対象、時点、責任又は処理方法にある。

Q0016

セキュア開発・脆弱性管理
タグ：SAST
用語：SASTの確認ポイント7：実行せずにソースコードなどを解析して脆弱性を検出する手法

「SAST」は、稼働中アプリケーションへ入力を送り外部から脆弱性を検出する手法。

A. ○
B. ×

答え・解説

Q0016 正答：×

解説：誤り。記述はDASTの説明である。SASTは実行せずにソースコードなどを解析して脆弱性を検出する手法。

Q0017

セキュア開発・脆弱性管理
タグ：SAST
用語：SASTの確認ポイント8：実行せずにソースコードなどを解析して脆弱性を検出する手法

次の状況で中心となる論点はどれか。「実行せずにソースコードなどを解析して脆弱性を検出する手法」ことが求められている。

A. SAST
B. ファジング
C. CWE
D. DAST

答え・解説

Q0017 正答：A. SAST

解説：中心となる論点はSASTである。判断では、説明中の目的語と処理の方向を手掛かりにする。

Q0018

セキュア開発・脆弱性管理
タグ：SAST
用語：SASTの確認ポイント9：実行せずにソースコードなどを解析して脆弱性を検出する手法

「実行せずにソースコードなどを解析して脆弱性を検出する手法」という特徴を持つものを選べ。

A. CWE
B. SAST
C. ファジング
D. DAST

答え・解説

Q0018 正答：B. SAST

解説：SASTが該当する。定義は実行せずにソースコードなどを解析して脆弱性を検出する手法であり、他の候補とは機能が異なる。

Q0019

セキュア開発・脆弱性管理
タグ：DAST
用語：DASTの確認ポイント1：稼働中アプリケーションへ入力を送り外部から脆弱性を検出する手法

次の説明に最も合う用語はどれか。稼働中アプリケーションへ入力を送り外部から脆弱性を検出する手法

A. IAST
B. セキュリティコードレビュー
C. DAST
D. 協調的脆弱性開示

答え・解説

Q0019 正答：C. DAST

解説：DASTは、稼働中アプリケーションへ入力を送り外部から脆弱性を検出する手法。ほかの選択肢は目的又は適用場面が異なる。

Q0020

セキュア開発・脆弱性管理
タグ：DAST
用語：DASTの確認ポイント2：稼働中アプリケーションへ入力を送り外部から脆弱性を検出する手法

DASTの説明として最も適切なものはどれか。

A. 実行時の内部情報と外部テストを組み合わせて脆弱性を検出する手法
B. 実装を人又はツールで確認し脆弱な処理を発見する活動
C. 発見者と提供者が修正・公表時期を調整して脆弱性情報を扱う方法
D. 稼働中アプリケーションへ入力を送り外部から脆弱性を検出する手法

答え・解説

Q0020 正答：D. 稼働中アプリケーションへ入力を送り外部から脆弱性を検出する手法

解説：DASTの要点は「稼働中アプリケーションへ入力を送り外部から脆弱性を検出する手法」である。名称が似た概念でも、対象とする処理や目的を区別する。

Q0021

セキュア開発・脆弱性管理
タグ：DAST
用語：DASTの確認ポイント3：稼働中アプリケーションへ入力を送り外部から脆弱性を検出する手法

用語と説明の組合せとして適切なものはどれか。論点は「DAST」である。

A. DAST：稼働中アプリケーションへ入力を送り外部から脆弱性を検出する手法
B. IAST：稼働中アプリケーションへ入力を送り外部から脆弱性を検出する手法
C. セキュリティコードレビュー：稼働中アプリケーションへ入力を送り外部から脆弱性を検出する手法
D. 協調的脆弱性開示：稼働中アプリケーションへ入力を送り外部から脆弱性を検出する手法

答え・解説

Q0021 正答：A. DAST：稼働中アプリケーションへ入力を送り外部から脆弱性を検出する手法

解説：正しい組合せは「DAST：稼働中アプリケーションへ入力を送り外部から脆弱性を検出する手法」。用語だけでなく、何を守り、何を処理する概念かを確認する。

Q0022

セキュア開発・脆弱性管理
タグ：DAST
用語：DASTの確認ポイント4：稼働中アプリケーションへ入力を送り外部から脆弱性を検出する手法

「DAST」は、稼働中アプリケーションへ入力を送り外部から脆弱性を検出する手法。

A. ○
B. ×

答え・解説

Q0022 正答：○

解説：正しい。DASTは稼働中アプリケーションへ入力を送り外部から脆弱性を検出する手法。実務では対象、目的、前提条件を併せて確認する。

Q0023

セキュア開発・脆弱性管理
タグ：DAST
用語：DASTの確認ポイント5：稼働中アプリケーションへ入力を送り外部から脆弱性を検出する手法

組織が「稼働中アプリケーションへ入力を送り外部から脆弱性を検出する手法」ために採用すべき概念又は仕組みはどれか。

A. IAST
B. セキュリティコードレビュー
C. DAST
D. 協調的脆弱性開示

答え・解説

Q0023 正答：C. DAST

解説：この目的に対応するのはDASTである。稼働中アプリケーションへ入力を送り外部から脆弱性を検出する手法という機能・考え方を持つためである。

Q0024

セキュア開発・脆弱性管理
タグ：DAST
用語：DASTの確認ポイント6：稼働中アプリケーションへ入力を送り外部から脆弱性を検出する手法

「DAST」について、誤解を避けるための説明として最も適切なものはどれか。

A. 発見者と提供者が修正・公表時期を調整して脆弱性情報を扱う方法
B. 実装を人又はツールで確認し脆弱な処理を発見する活動
C. 実行時の内部情報と外部テストを組み合わせて脆弱性を検出する手法
D. 稼働中アプリケーションへ入力を送り外部から脆弱性を検出する手法

答え・解説

Q0024 正答：D. 稼働中アプリケーションへ入力を送り外部から脆弱性を検出する手法

解説：DASTは稼働中アプリケーションへ入力を送り外部から脆弱性を検出する手法。似た用語との違いは、対象、時点、責任又は処理方法にある。

Q0025

セキュア開発・脆弱性管理
タグ：DAST
用語：DASTの確認ポイント7：稼働中アプリケーションへ入力を送り外部から脆弱性を検出する手法

「DAST」は、実行時の内部情報と外部テストを組み合わせて脆弱性を検出する手法。

A. ○
B. ×

答え・解説

Q0025 正答：×

解説：誤り。記述はIASTの説明である。DASTは稼働中アプリケーションへ入力を送り外部から脆弱性を検出する手法。

Q0026

セキュア開発・脆弱性管理
タグ：DAST
用語：DASTの確認ポイント8：稼働中アプリケーションへ入力を送り外部から脆弱性を検出する手法

次の状況で中心となる論点はどれか。「稼働中アプリケーションへ入力を送り外部から脆弱性を検出する手法」ことが求められている。

A. セキュリティコードレビュー
B. DAST
C. 協調的脆弱性開示
D. IAST

答え・解説

Q0026 正答：B. DAST

解説：中心となる論点はDASTである。判断では、説明中の目的語と処理の方向を手掛かりにする。

Q0027

セキュア開発・脆弱性管理
タグ：DAST
用語：DASTの確認ポイント9：稼働中アプリケーションへ入力を送り外部から脆弱性を検出する手法

「稼働中アプリケーションへ入力を送り外部から脆弱性を検出する手法」という特徴を持つものを選べ。

A. 協調的脆弱性開示
B. セキュリティコードレビュー
C. DAST
D. IAST

答え・解説

Q0027 正答：C. DAST

解説：DASTが該当する。定義は稼働中アプリケーションへ入力を送り外部から脆弱性を検出する手法であり、他の候補とは機能が異なる。

Q0028

セキュア開発・脆弱性管理
タグ：IAST
用語：IASTの確認ポイント1：実行時の内部情報と外部テストを組み合わせて脆弱性を検出する手法

次の説明に最も合う用語はどれか。実行時の内部情報と外部テストを組み合わせて脆弱性を検出する手法

A. ファジング
B. CVSS
C. STRIDE
D. IAST

答え・解説

Q0028 正答：D. IAST

解説：IASTは、実行時の内部情報と外部テストを組み合わせて脆弱性を検出する手法。ほかの選択肢は目的又は適用場面が異なる。

Q0029

セキュア開発・脆弱性管理
タグ：IAST
用語：IASTの確認ポイント2：実行時の内部情報と外部テストを組み合わせて脆弱性を検出する手法

IASTの説明として最も適切なものはどれか。

A. 実行時の内部情報と外部テストを組み合わせて脆弱性を検出する手法
B. 大量の異常・予測困難な入力を与えて不具合を検出する試験
C. 脆弱性の深刻度を基本・現状・環境評価基準で数値化する仕組み
D. なりすまし、改ざん、否認、情報漏えい、サービス妨害、権限昇格で脅威を分類する手法

答え・解説

Q0029 正答：A. 実行時の内部情報と外部テストを組み合わせて脆弱性を検出する手法

解説：IASTの要点は「実行時の内部情報と外部テストを組み合わせて脆弱性を検出する手法」である。名称が似た概念でも、対象とする処理や目的を区別する。

Q0030

セキュア開発・脆弱性管理
タグ：IAST
用語：IASTの確認ポイント3：実行時の内部情報と外部テストを組み合わせて脆弱性を検出する手法

用語と説明の組合せとして適切なものはどれか。論点は「IAST」である。

A. ファジング：実行時の内部情報と外部テストを組み合わせて脆弱性を検出する手法
B. IAST：実行時の内部情報と外部テストを組み合わせて脆弱性を検出する手法
C. CVSS：実行時の内部情報と外部テストを組み合わせて脆弱性を検出する手法
D. STRIDE：実行時の内部情報と外部テストを組み合わせて脆弱性を検出する手法

答え・解説

Q0030 正答：B. IAST：実行時の内部情報と外部テストを組み合わせて脆弱性を検出する手法

解説：正しい組合せは「IAST：実行時の内部情報と外部テストを組み合わせて脆弱性を検出する手法」。用語だけでなく、何を守り、何を処理する概念かを確認する。

Q0031

セキュア開発・脆弱性管理
タグ：IAST
用語：IASTの確認ポイント4：実行時の内部情報と外部テストを組み合わせて脆弱性を検出する手法
「IAST」は、実行時の内部情報と外部テストを組み合わせて脆弱性を検出する手法。

A. ○
B. ×

答え・解説

Q0031 正答：○
解説：正しい。IASTは実行時の内部情報と外部テストを組み合わせて脆弱性を検出する手法。実務では対象、目的、前提条件を併せて確認する。

Q0032

セキュア開発・脆弱性管理
タグ：IAST
用語：IASTの確認ポイント5：実行時の内部情報と外部テストを組み合わせて脆弱性を検出する手法
組織が「実行時の内部情報と外部テストを組み合わせて脆弱性を検出する手法」ために採用すべき概念又は仕組みはどれか。

A. ファジング
B. CVSS
C. STRIDE
D. IAST

答え・解説

Q0032 正答：D. IAST
解説：この目的に対応するのはIASTである。実行時の内部情報と外部テストを組み合わせて脆弱性を検出する手法という機能・考え方を持つためである。

Q0033

セキュア開発・脆弱性管理
タグ：IAST
用語：IASTの確認ポイント6：実行時の内部情報と外部テストを組み合わせて脆弱性を検出する手法

「IAST」について、誤解を避けるための説明として最も適切なものはどれか。

A. 実行時の内部情報と外部テストを組み合わせて脆弱性を検出する手法
B. なりすまし、改ざん、否認、情報漏えい、サービス妨害、権限昇格で脅威を分類する手法
C. 脆弱性の深刻度を基本・現状・環境評価基準で数値化する仕組み
D. 大量の異常・予測困難な入力を与えて不具合を検出する試験

答え・解説

Q0033 正答：A. 実行時の内部情報と外部テストを組み合わせて脆弱性を検出する手法

解説：IASTは実行時の内部情報と外部テストを組み合わせて脆弱性を検出する手法。似た用語との違いは、対象、時点、責任又は処理方法にある。

Q0034

セキュア開発・脆弱性管理
タグ：IAST
用語：IASTの確認ポイント7：実行時の内部情報と外部テストを組み合わせて脆弱性を検出する手法

「IAST」は、大量の異常・予測困難な入力を与えて不具合を検出する試験。

A. ○
B. ×

答え・解説

Q0034 正答：×

解説：誤り。記述はファジングの説明である。IASTは実行時の内部情報と外部テストを組み合わせて脆弱性を検出する手法。

Q0035

セキュア開発・脆弱性管理
タグ：IAST
用語：IASTの確認ポイント8：実行時の内部情報と外部テストを組み合わせて脆弱性を検出する手法

次の状況で中心となる論点はどれか。「実行時の内部情報と外部テストを組み合わせて脆弱性を検出する手法」ことが求められている。

A. CVSS
B. STRIDE
C. IAST
D. ファジング

答え・解説

Q0035 正答：C. IAST

解説：中心となる論点はIASTである。判断では、説明中の目的語と処理の方向を手掛かりにする。

Q0036

セキュア開発・脆弱性管理
タグ：IAST
用語：IASTの確認ポイント9：実行時の内部情報と外部テストを組み合わせて脆弱性を検出する手法

「実行時の内部情報と外部テストを組み合わせて脆弱性を検出する手法」という特徴を持つものを選べ。

A. STRIDE
B. CVSS
C. ファジング
D. IAST

答え・解説

Q0036 正答：D. IAST

解説：IASTが該当する。定義は実行時の内部情報と外部テストを組み合わせて脆弱性を検出する手法であり、他の候補とは機能が異なる。

Q0037

セキュア開発・脆弱性管理
タグ：ファジング
用語：ファジングの確認ポイント1：大量の異常・予測困難な入力を与えて不具合を検出する試験

次の説明に最も合う用語はどれか。大量の異常・予測困難な入力を与えて不具合を検出する試験

A. ファジング
B. セキュリティコードレビュー
C. CVE
D. SAST

答え・解説

Q0037 正答：A. ファジング

解説：ファジングは、大量の異常・予測困難な入力を与えて不具合を検出する試験。ほかの選択肢は目的又は適用場面が異なる。

Q0038

セキュア開発・脆弱性管理
タグ：ファジング
用語：ファジングの確認ポイント2：大量の異常・予測困難な入力を与えて不具合を検出する試験

ファジングの説明として最も適切なものはどれか。

A. 実装を人又はツールで確認し脆弱な処理を発見する活動
B. 大量の異常・予測困難な入力を与えて不具合を検出する試験
C. 公開された脆弱性へ一意な識別番号を付ける仕組み
D. 実行せずにソースコードなどを解析して脆弱性を検出する手法

答え・解説

Q0038 正答：B. 大量の異常・予測困難な入力を与えて不具合を検出する試験

解説：ファジングの要点は「大量の異常・予測困難な入力を与えて不具合を検出する試験」である。名称が似た概念でも、対象とする処理や目的を区別する。

Q0039

セキュア開発・脆弱性管理
タグ：ファジング
用語：ファジングの確認ポイント3：大量の異常・予測困難な入力を与えて不具合を検出する試験

用語と説明の組合せとして適切なものはどれか。論点は「ファジング」である。

A. セキュリティコードレビュー：大量の異常・予測困難な入力を与えて不具合を検出する試験
B. CVE：大量の異常・予測困難な入力を与えて不具合を検出する試験
C. ファジング：大量の異常・予測困難な入力を与えて不具合を検出する試験
D. SAST：大量の異常・予測困難な入力を与えて不具合を検出する試験

答え・解説

Q0039 正答：C. ファジング：大量の異常・予測困難な入力を与えて不具合を検出する試験

解説：正しい組合せは「ファジング：大量の異常・予測困難な入力を与えて不具合を検出する試験」。用語だけでなく、何を守り、何を処理する概念かを確認する。

Q0040

セキュア開発・脆弱性管理
タグ：ファジング
用語：ファジングの確認ポイント4：大量の異常・予測困難な入力を与えて不具合を検出する試験

「ファジング」は、大量の異常・予測困難な入力を与えて不具合を検出する試験。

A. ○
B. ×

答え・解説

Q0040 正答：○

解説：正しい。ファジングは大量の異常・予測困難な入力を与えて不具合を検出する試験。実務では対象、目的、前提条件を併せて確認する。

Q0041

セキュア開発・脆弱性管理
タグ：ファジング
用語：ファジングの確認ポイント5：大量の異常・予測困難な入力を与えて不具合を検出する試験

組織が「大量の異常・予測困難な入力を与えて不具合を検出する試験」ために採用すべき概念又は仕組みはどれか。

A. ファジング
B. セキュリティコードレビュー
C. CVE
D. SAST

答え・解説

Q0041 正答：A. ファジング

解説：この目的に対応するのはファジングである。大量の異常・予測困難な入力を与えて不具合を検出する試験という機能・考え方を持つためである。

Q0042

セキュア開発・脆弱性管理
タグ：ファジング
用語：ファジングの確認ポイント6：大量の異常・予測困難な入力を与えて不具合を検出する試験

「ファジング」について、誤解を避けるための説明として最も適切なものはどれか。

A. 実行せずにソースコードなどを解析して脆弱性を検出する手法
B. 大量の異常・予測困難な入力を与えて不具合を検出する試験
C. 公開された脆弱性へ一意な識別番号を付ける仕組み
D. 実装を人又はツールで確認し脆弱な処理を発見する活動

答え・解説

Q0042 正答：B. 大量の異常・予測困難な入力を与えて不具合を検出する試験

解説：ファジングは大量の異常・予測困難な入力を与えて不具合を検出する試験。似た用語との違いは、対象、時点、責任又は処理方法にある。

Q0043

セキュア開発・脆弱性管理
タグ：ファジング
用語：ファジングの確認ポイント7：大量の異常・予測困難な入力を与えて不具合を検出する試験

「ファジング」は、実装を人又はツールで確認し脆弱な処理を発見する活動。

A. ○
B. ×

答え・解説

Q0043 正答：×

解説：誤り。記述はセキュリティコードレビューの説明である。ファジングは大量の異常・予測困難な入力を与えて不具合を検出する試験。

Q0044

セキュア開発・脆弱性管理
タグ：ファジング
用語：ファジングの確認ポイント8：大量の異常・予測困難な入力を与えて不具合を検出する試験

次の状況で中心となる論点はどれか。「大量の異常・予測困難な入力を与えて不具合を検出する試験」ことが求められている。

A. CVE
B. SAST
C. セキュリティコードレビュー
D. ファジング

答え・解説

Q0044 正答：D. ファジング

解説：中心となる論点はファジングである。判断では、説明中の目的語と処理の方向を手掛かりにする。

Q0045

セキュア開発・脆弱性管理
タグ：ファジング
用語：ファジングの確認ポイント9：大量の異常・予測困難な入力を与えて不具合を検出する試験

「大量の異常・予測困難な入力を与えて不具合を検出する試験」という特徴を持つものを選べ。

A. ファジング
B. SAST
C. CVE
D. セキュリティコードレビュー

答え・解説

Q0045 正答：A. ファジング

解説：ファジングが該当する。定義は大量の異常・予測困難な入力を与えて不具合を検出する試験であり、他の候補とは機能が異なる。

Q0046

セキュア開発・脆弱性管理
タグ：セキュリティコードレビュー
用語：セキュリティコードレビューの確認ポイント1：実装を人又はツールで確認し脆弱な処理を発見する活動

次の説明に最も合う用語はどれか。実装を人又はツールで確認し脆弱な処理を発見する活動

A. CVSS
B. セキュリティコードレビュー
C. CWE
D. DAST

答え・解説

Q0046 正答：B. セキュリティコードレビュー

解説：セキュリティコードレビューは、実装を人又はツールで確認し脆弱な処理を発見する活動。ほかの選択肢は目的又は適用場面が異なる。

Q0047

セキュア開発・脆弱性管理
タグ：セキュリティコードレビュー
用語：セキュリティコードレビューの確認ポイント2：実装を人又はツールで確認し脆弱な処理を発見する活動

セキュリティコードレビューの説明として最も適切なものはどれか。

A. 脆弱性の深刻度を基本・現状・環境評価基準で数値化する仕組み
B. ソフトウェアの弱点の種類を体系的に分類した一覧
C. 実装を人又はツールで確認し脆弱な処理を発見する活動
D. 稼働中アプリケーションへ入力を送り外部から脆弱性を検出する手法

答え・解説

Q0047 正答：C. 実装を人又はツールで確認し脆弱な処理を発見する活動

解説：セキュリティコードレビューの要点は「実装を人又はツールで確認し脆弱な処理を発見する活動」である。名称が似た概念でも、対象とする処理や目的を区別する。

Q0048

セキュア開発・脆弱性管理
タグ：セキュリティコードレビュー
用語：セキュリティコードレビューの確認ポイント3：実装を人又はツールで確認し脆弱な処理を発見する活動

用語と説明の組合せとして適切なものはどれか。論点は「セキュリティコードレビュー」である。

A. CVSS：実装を人又はツールで確認し脆弱な処理を発見する活動
B. CWE：実装を人又はツールで確認し脆弱な処理を発見する活動
C. DAST：実装を人又はツールで確認し脆弱な処理を発見する活動
D. セキュリティコードレビュー：実装を人又はツールで確認し脆弱な処理を発見する活動

答え・解説

Q0048 正答：D. セキュリティコードレビュー：実装を人又はツールで確認し脆弱な処理を発見する活動

解説：正しい組合せは「セキュリティコードレビュー：実装を人又はツールで確認し脆弱な処理を発見する活動」。用語だけでなく、何を守り、何を処理する概念かを確認する。

Q0049

セキュア開発・脆弱性管理
タグ：セキュリティコードレビュー
用語：セキュリティコードレビューの確認ポイント4：実装を人又はツールで確認し脆弱な処理を発見する活動

「セキュリティコードレビュー」は、実装を人又はツールで確認し脆弱な処理を発見する活動。

A. ○
B. ×

答え・解説

Q0049 正答：○

解説：正しい。セキュリティコードレビューは実装を人又はツールで確認し脆弱な処理を発見する活動。実務では対象、目的、前提条件を併せて確認する。

Q0050

セキュア開発・脆弱性管理
タグ：セキュリティコードレビュー
用語：セキュリティコードレビューの確認ポイント5：実装を人又はツールで確認し脆弱な処理を発見する活動

組織が「実装を人又はツールで確認し脆弱な処理を発見する活動」ために採用すべき概念又は仕組みはどれか。

A. CVSS
B. セキュリティコードレビュー
C. CWE
D. DAST

答え・解説

Q0050 正答：B. セキュリティコードレビュー

解説：この目的に対応するのはセキュリティコードレビューである。実装を人又はツールで確認し脆弱な処理を発見する活動という機能・考え方を持つためである。

Q0051

セキュア開発・脆弱性管理
タグ：セキュリティコードレビュー
用語：セキュリティコードレビューの確認ポイント6：実装を人又はツールで確認し脆弱な処理を発見する活動

「セキュリティコードレビュー」について、誤解を避けるための説明として最も適切なものはどれか。

A. 稼働中アプリケーションへ入力を送り外部から脆弱性を検出する手法
B. ソフトウェアの弱点の種類を体系的に分類した一覧
C. 実装を人又はツールで確認し脆弱な処理を発見する活動
D. 脆弱性の深刻度を基本・現状・環境評価基準で数値化する仕組み

答え・解説

Q0051 正答：C. 実装を人又はツールで確認し脆弱な処理を発見する活動

解説：セキュリティコードレビューは実装を人又はツールで確認し脆弱な処理を発見する活動。似た用語との違いは、対象、時点、責任又は処理方法にある。

Q0052

セキュア開発・脆弱性管理
タグ：セキュリティコードレビュー
用語：セキュリティコードレビューの確認ポイント7：実装を人又はツールで確認し脆弱な処理を発見する活動

「セキュリティコードレビュー」は、脆弱性の深刻度を基本・現状・環境評価基準で数値化する仕組み。

A. ○
B. ×

答え・解説

Q0052 正答：×

解説：誤り。記述はCVSSの説明である。セキュリティコードレビューは実装を人又はツールで確認し脆弱な処理を発見する活動。

Q0053

セキュア開発・脆弱性管理
タグ：セキュリティコードレビュー
用語：セキュリティコードレビューの確認ポイント8：実装を人又はツールで確認し脆弱な処理を発見する活動

次の状況で中心となる論点はどれか。「実装を人又はツールで確認し脆弱な処理を発見する活動」ことが求められている。

A. セキュリティコードレビュー
B. CWE
C. DAST
D. CVSS

答え・解説

Q0053 正答：A. セキュリティコードレビュー

解説：中心となる論点はセキュリティコードレビューである。判断では、説明中の目的語と処理の方向を手掛かりにする。

Q0054

セキュア開発・脆弱性管理
タグ：セキュリティコードレビュー
用語：セキュリティコードレビューの確認ポイント9：実装を人又はツールで確認し脆弱な処理を発見する活動

「実装を人又はツールで確認し脆弱な処理を発見する活動」という特徴を持つものを選べ。

A. DAST
B. セキュリティコードレビュー
C. CWE
D. CVSS

答え・解説

Q0054 正答：B. セキュリティコードレビュー

解説：セキュリティコードレビューが該当する。定義は実装を人又はツールで確認し脆弱な処理を発見する活動であり、他の候補とは機能が異なる。

Q0055

セキュア開発・脆弱性管理
タグ：CVSS
用語：CVSSの確認ポイント1：脆弱性の深刻度を基本・現状・環境評価基準で数値化する仕組み

次の説明に最も合う用語はどれか。脆弱性の深刻度を基本・現状・環境評価基準で数値化する仕組み

A. CVE
B. 協調的脆弱性開示
C. CVSS
D. IAST

答え・解説

Q0055 正答：C. CVSS

解説：CVSSは、脆弱性の深刻度を基本・現状・環境評価基準で数値化する仕組み。ほかの選択肢は目的又は適用場面が異なる。

Q0056

セキュア開発・脆弱性管理
タグ：CVSS
用語：CVSSの確認ポイント2：脆弱性の深刻度を基本・現状・環境評価基準で数値化する仕組み

CVSSの説明として最も適切なものはどれか。

A. 公開された脆弱性へ一意な識別番号を付ける仕組み
B. 発見者と提供者が修正・公表時期を調整して脆弱性情報を扱う方法
C. 実行時の内部情報と外部テストを組み合わせて脆弱性を検出する手法
D. 脆弱性の深刻度を基本・現状・環境評価基準で数値化する仕組み

答え・解説

Q0056 正答：D. 脆弱性の深刻度を基本・現状・環境評価基準で数値化する仕組み

解説：CVSSの要点は「脆弱性の深刻度を基本・現状・環境評価基準で数値化する仕組み」である。名称が似た概念でも、対象とする処理や目的を区別する。

Q0057

セキュア開発・脆弱性管理
タグ：CVSS
用語：CVSSの確認ポイント3：脆弱性の深刻度を基本・現状・環境評価基準で数値化する仕組み

用語と説明の組合せとして適切なものはどれか。論点は「CVSS」である。

A. CVSS：脆弱性の深刻度を基本・現状・環境評価基準で数値化する仕組み
B. CVE：脆弱性の深刻度を基本・現状・環境評価基準で数値化する仕組み
C. 協調的脆弱性開示：脆弱性の深刻度を基本・現状・環境評価基準で数値化する仕組み
D. IAST：脆弱性の深刻度を基本・現状・環境評価基準で数値化する仕組み

答え・解説

Q0057 正答：A. CVSS：脆弱性の深刻度を基本・現状・環境評価基準で数値化する仕組み

解説：正しい組合せは「CVSS：脆弱性の深刻度を基本・現状・環境評価基準で数値化する仕組み」。用語だけでなく、何を守り、何を処理する概念かを確認する。

Q0058

セキュア開発・脆弱性管理
タグ：CVSS
用語：CVSSの確認ポイント4：脆弱性の深刻度を基本・現状・環境評価基準で数値化する仕組み

「CVSS」は、脆弱性の深刻度を基本・現状・環境評価基準で数値化する仕組み。

A. ○
B. ×

答え・解説

Q0058 正答：○

解説：正しい。CVSSは脆弱性の深刻度を基本・現状・環境評価基準で数値化する仕組み。実務では対象、目的、前提条件を併せて確認する。

Q0059

セキュア開発・脆弱性管理
タグ：CVSS
用語：CVSSの確認ポイント5：脆弱性の深刻度を基本・現状・環境評価基準で数値化する仕組み

組織が「脆弱性の深刻度を基本・現状・環境評価基準で数値化する仕組み」ために採用すべき概念又は仕組みはどれか。

A. CVE
B. 協調的脆弱性開示
C. CVSS
D. IAST

答え・解説

Q0059 正答：C. CVSS

解説：この目的に対応するのはCVSSである。脆弱性の深刻度を基本・現状・環境評価基準で数値化する仕組みという機能・考え方を持つためである。

Q0060

セキュア開発・脆弱性管理
タグ：CVSS
用語：CVSSの確認ポイント6：脆弱性の深刻度を基本・現状・環境評価基準で数値化する仕組み

「CVSS」について、誤解を避けるための説明として最も適切なものはどれか。

A. 実行時の内部情報と外部テストを組み合わせて脆弱性を検出する手法
B. 発見者と提供者が修正・公表時期を調整して脆弱性情報を扱う方法
C. 公開された脆弱性へ一意な識別番号を付ける仕組み
D. 脆弱性の深刻度を基本・現状・環境評価基準で数値化する仕組み

答え・解説

Q0060 正答：D. 脆弱性の深刻度を基本・現状・環境評価基準で数値化する仕組み

解説：CVSSは脆弱性の深刻度を基本・現状・環境評価基準で数値化する仕組み。似た用語との違いは、対象、時点、責任又は処理方法にある。

Q0061

セキュア開発・脆弱性管理
タグ：CVSS
用語：CVSSの確認ポイント7：脆弱性の深刻度を基本・現状・環境評価基準で数値化する仕組み

「CVSS」は、公開された脆弱性へ一意な識別番号を付ける仕組み。

A. ○
B. ×

答え・解説

Q0061 正答：×

解説：誤り。記述はCVEの説明である。CVSSは脆弱性の深刻度を基本・現状・環境評価基準で数値化する仕組み。

Q0062

セキュア開発・脆弱性管理
タグ：CVSS
用語：CVSSの確認ポイント8：脆弱性の深刻度を基本・現状・環境評価基準で数値化する仕組み

次の状況で中心となる論点はどれか。「脆弱性の深刻度を基本・現状・環境評価基準で数値化する仕組み」ことが求められている。

A. 協調的脆弱性開示
B. CVSS
C. IAST
D. CVE

答え・解説

Q0062 正答：B. CVSS

解説：中心となる論点はCVSSである。判断では、説明中の目的語と処理の方向を手掛かりにする。

Q0063

セキュア開発・脆弱性管理
タグ：CVSS
用語：CVSSの確認ポイント9：脆弱性の深刻度を基本・現状・環境評価基準で数値化する仕組み

「脆弱性の深刻度を基本・現状・環境評価基準で数値化する仕組み」という特徴を持つものを選べ。

A. IAST
B. 協調的脆弱性開示
C. CVSS
D. CVE

答え・解説

Q0063 正答：C. CVSS

解説：CVSSが該当する。定義は脆弱性の深刻度を基本・現状・環境評価基準で数値化する仕組みであり、他の候補とは機能が異なる。

Q0064

セキュア開発・脆弱性管理
タグ：CVE
用語：CVEの確認ポイント1：公開された脆弱性へ一意な識別番号を付ける仕組み

次の説明に最も合う用語はどれか。公開された脆弱性へ一意な識別番号を付ける仕組み

A. CWE
B. STRIDE
C. ファジング
D. CVE

答え・解説

Q0064 正答：D. CVE

解説：CVEは、公開された脆弱性へ一意な識別番号を付ける仕組み。ほかの選択肢は目的又は適用場面が異なる。

Q0065

セキュア開発・脆弱性管理
タグ：CVE
用語：CVEの確認ポイント2：公開された脆弱性へ一意な識別番号を付ける仕組み

CVEの説明として最も適切なものはどれか。

A. 公開された脆弱性へ一意な識別番号を付ける仕組み
B. ソフトウェアの弱点の種類を体系的に分類した一覧
C. なりすまし、改ざん、否認、情報漏えい、サービス妨害、権限昇格で脅威を分類する手法
D. 大量の異常・予測困難な入力を与えて不具合を検出する試験

答え・解説

Q0065 正答：A. 公開された脆弱性へ一意な識別番号を付ける仕組み

解説：CVEの要点は「公開された脆弱性へ一意な識別番号を付ける仕組み」である。名称が似た概念でも、対象とする処理や目的を区別する。

Q0066

セキュア開発・脆弱性管理
タグ：CVE
用語：CVEの確認ポイント3：公開された脆弱性へ一意な識別番号を付ける仕組み

用語と説明の組合せとして適切なものはどれか。論点は「CVE」である。

A. CWE：公開された脆弱性へ一意な識別番号を付ける仕組み
B. CVE：公開された脆弱性へ一意な識別番号を付ける仕組み
C. STRIDE：公開された脆弱性へ一意な識別番号を付ける仕組み
D. ファジング：公開された脆弱性へ一意な識別番号を付ける仕組み

答え・解説

Q0066 正答：B. CVE：公開された脆弱性へ一意な識別番号を付ける仕組み

解説：正しい組合せは「CVE：公開された脆弱性へ一意な識別番号を付ける仕組み」。用語だけでなく、何を守り、何を処理する概念かを確認する。

Q0067

セキュア開発・脆弱性管理
タグ：CVE
用語：CVEの確認ポイント4：公開された脆弱性へ一意な識別番号を付ける仕組み

「CVE」は、公開された脆弱性へ一意な識別番号を付ける仕組み。

A. ○
B. ×

答え・解説

Q0067 正答：○

解説：正しい。CVEは公開された脆弱性へ一意な識別番号を付ける仕組み。実務では対象、目的、前提条件を併せて確認する。

Q0068

セキュア開発・脆弱性管理
タグ：CVE
用語：CVEの確認ポイント5：公開された脆弱性へ一意な識別番号を付ける仕組み

組織が「公開された脆弱性へ一意な識別番号を付ける仕組み」ために採用すべき概念又は仕組みはどれか。

A. CWE
B. STRIDE
C. ファジング
D. CVE

答え・解説

Q0068 正答：D. CVE

解説：この目的に対応するのはCVEである。公開された脆弱性へ一意な識別番号を付ける仕組みという機能・考え方を持つためである。

Q0069

セキュア開発・脆弱性管理
タグ：CVE
用語：CVEの確認ポイント6：公開された脆弱性へ一意な識別番号を付ける仕組み

「CVE」について、誤解を避けるための説明として最も適切なものはどれか。

A. 公開された脆弱性へ一意な識別番号を付ける仕組み
B. 大量の異常・予測困難な入力を与えて不具合を検出する試験
C. なりすまし、改ざん、否認、情報漏えい、サービス妨害、権限昇格で脅威を分類する手法
D. ソフトウェアの弱点の種類を体系的に分類した一覧

答え・解説

Q0069 正答：A. 公開された脆弱性へ一意な識別番号を付ける仕組み

解説：CVEは公開された脆弱性へ一意な識別番号を付ける仕組み。似た用語との違いは、対象、時点、責任又は処理方法にある。

Q0070

セキュア開発・脆弱性管理
タグ：CVE
用語：CVEの確認ポイント7：公開された脆弱性へ一意な識別番号を付ける仕組み

「CVE」は、ソフトウェアの弱点の種類を体系的に分類した一覧。

A. ○
B. ×

答え・解説

Q0070 正答：×

解説：誤り。記述はCWEの説明である。CVEは公開された脆弱性へ一意な識別番号を付ける仕組み。

Q0071

セキュア開発・脆弱性管理
タグ：CVE
用語：CVEの確認ポイント8：公開された脆弱性へ一意な識別番号を付ける仕組み

次の状況で中心となる論点はどれか。「公開された脆弱性へ一意な識別番号を付ける仕組み」ことが求められている。

A. STRIDE
B. ファジング
C. CVE
D. CWE

答え・解説

Q0071 正答：C. CVE

解説：中心となる論点はCVEである。判断では、説明中の目的語と処理の方向を手掛かりにする。

Q0072

セキュア開発・脆弱性管理
タグ：CVE
用語：CVEの確認ポイント9：公開された脆弱性へ一意な識別番号を付ける仕組み

「公開された脆弱性へ一意な識別番号を付ける仕組み」という特徴を持つものを選べ。

A. ファジング
B. STRIDE
C. CWE
D. CVE

答え・解説

Q0072 正答：D. CVE

解説：CVEが該当する。定義は公開された脆弱性へ一意な識別番号を付ける仕組みであり、他の候補とは機能が異なる。

Q0073

セキュア開発・脆弱性管理
タグ：CWE
用語：CWEの確認ポイント1：ソフトウェアの弱点の種類を体系的に分類した一覧

次の説明に最も合う用語はどれか。ソフトウェアの弱点の種類を体系的に分類した一覧

A. CWE
B. 協調的脆弱性開示
C. SAST
D. セキュリティコードレビュー

答え・解説

Q0073 正答：A. CWE

解説：CWEは、ソフトウェアの弱点の種類を体系的に分類した一覧。ほかの選択肢は目的又は適用場面が異なる。

Q0074

セキュア開発・脆弱性管理
タグ：CWE
用語：CWEの確認ポイント2：ソフトウェアの弱点の種類を体系的に分類した一覧

CWEの説明として最も適切なものはどれか。

A. 発見者と提供者が修正・公表時期を調整して脆弱性情報を扱う方法
B. ソフトウェアの弱点の種類を体系的に分類した一覧
C. 実行せずにソースコードなどを解析して脆弱性を検出する手法
D. 実装を人又はツールで確認し脆弱な処理を発見する活動

答え・解説

Q0074 正答：B. ソフトウェアの弱点の種類を体系的に分類した一覧

解説：CWEの要点は「ソフトウェアの弱点の種類を体系的に分類した一覧」である。名称が似た概念でも、対象とする処理や目的を区別する。

Q0075

セキュア開発・脆弱性管理
タグ：CWE
用語：CWEの確認ポイント3：ソフトウェアの弱点の種類を体系的に分類した一覧

用語と説明の組合せとして適切なものはどれか。論点は「CWE」である。

A. 協調的脆弱性開示：ソフトウェアの弱点の種類を体系的に分類した一覧
B. SAST：ソフトウェアの弱点の種類を体系的に分類した一覧
C. CWE：ソフトウェアの弱点の種類を体系的に分類した一覧
D. セキュリティコードレビュー：ソフトウェアの弱点の種類を体系的に分類した一覧

答え・解説

Q0075 正答：C. CWE：ソフトウェアの弱点の種類を体系的に分類した一覧

解説：正しい組合せは「CWE：ソフトウェアの弱点の種類を体系的に分類した一覧」。用語だけでなく、何を守り、何を処理する概念かを確認する。

Q0076

セキュア開発・脆弱性管理
タグ：CWE
用語：CWEの確認ポイント4：ソフトウェアの弱点の種類を体系的に分類した一覧

「CWE」は、ソフトウェアの弱点の種類を体系的に分類した一覧。

A. ○
B. ×

答え・解説

Q0076 正答：○

解説：正しい。CWEはソフトウェアの弱点の種類を体系的に分類した一覧。実務では対象、目的、前提条件を併せて確認する。

Q0077

セキュア開発・脆弱性管理
タグ：CWE
用語：CWEの確認ポイント5：ソフトウェアの弱点の種類を体系的に分類した一覧

組織が「ソフトウェアの弱点の種類を体系的に分類した一覧」ために採用すべき概念又は仕組みはどれか。

A. CWE
B. 協調的脆弱性開示
C. SAST
D. セキュリティコードレビュー

答え・解説

Q0077 正答：A. CWE

解説：この目的に対応するのはCWEである。ソフトウェアの弱点の種類を体系的に分類した一覧という機能・考え方を持つためである。

Q0078

セキュア開発・脆弱性管理
タグ：CWE
用語：CWEの確認ポイント6：ソフトウェアの弱点の種類を体系的に分類した一覧

「CWE」について、誤解を避けるための説明として最も適切なものはどれか。

A. 実装を人又はツールで確認し脆弱な処理を発見する活動
B. ソフトウェアの弱点の種類を体系的に分類した一覧
C. 実行せずにソースコードなどを解析して脆弱性を検出する手法
D. 発見者と提供者が修正・公表時期を調整して脆弱性情報を扱う方法

答え・解説

Q0078 正答：B. ソフトウェアの弱点の種類を体系的に分類した一覧

解説：CWEはソフトウェアの弱点の種類を体系的に分類した一覧。似た用語との違いは、対象、時点、責任又は処理方法にある。

Q0079

セキュア開発・脆弱性管理
タグ：CWE
用語：CWEの確認ポイント7：ソフトウェアの弱点の種類を体系的に分類した一覧

「CWE」は、発見者と提供者が修正・公表時期を調整して脆弱性情報を扱う方法。

A. ○
B. ×

答え・解説

Q0079 正答：×

解説：誤り。記述は協調的脆弱性開示の説明である。CWEはソフトウェアの弱点の種類を体系的に分類した一覧。

Q0080

セキュア開発・脆弱性管理
タグ：CWE
用語：CWEの確認ポイント8：ソフトウェアの弱点の種類を体系的に分類した一覧

次の状況で中心となる論点はどれか。「ソフトウェアの弱点の種類を体系的に分類した一覧」ことが求められている。

A. SAST
B. セキュリティコードレビュー
C. 協調的脆弱性開示
D. CWE

答え・解説

Q0080 正答：D. CWE

解説：中心となる論点はCWEである。判断では、説明中の目的語と処理の方向を手掛かりにする。

Q0081

セキュア開発・脆弱性管理
タグ：CWE
用語：CWEの確認ポイント9：ソフトウェアの弱点の種類を体系的に分類した一覧

「ソフトウェアの弱点の種類を体系的に分類した一覧」という特徴を持つものを選べ。

A. CWE
B. セキュリティコードレビュー
C. SAST
D. 協調的脆弱性開示

答え・解説

Q0081 正答：A. CWE

解説：CWEが該当する。定義はソフトウェアの弱点の種類を体系的に分類した一覧であり、他の候補とは機能が異なる。

Q0082

セキュア開発・脆弱性管理
タグ：協調的脆弱性開示
用語：協調的脆弱性開示の確認ポイント1：発見者と提供者が修正・公表時期を調整して脆弱性情報を扱う方法

次の説明に最も合う用語はどれか。発見者と提供者が修正・公表時期を調整して脆弱性情報を扱う方法

A. STRIDE
B. 協調的脆弱性開示
C. DAST
D. CVSS

答え・解説

Q0082 正答：B. 協調的脆弱性開示

解説：協調的脆弱性開示は、発見者と提供者が修正・公表時期を調整して脆弱性情報を扱う方法。ほかの選択肢は目的又は適用場面が異なる。

Q0083

セキュア開発・脆弱性管理
タグ：協調的脆弱性開示
用語：協調的脆弱性開示の確認ポイント2：発見者と提供者が修正・公表時期を調整して脆弱性情報を扱う方法

協調的脆弱性開示の説明として最も適切なものはどれか。

A. なりすまし、改ざん、否認、情報漏えい、サービス妨害、権限昇格で脅威を分類する手法
B. 稼働中アプリケーションへ入力を送り外部から脆弱性を検出する手法
C. 発見者と提供者が修正・公表時期を調整して脆弱性情報を扱う方法
D. 脆弱性の深刻度を基本・現状・環境評価基準で数値化する仕組み

答え・解説

Q0083 正答：C. 発見者と提供者が修正・公表時期を調整して脆弱性情報を扱う方法

解説：協調的脆弱性開示の要点は「発見者と提供者が修正・公表時期を調整して脆弱性情報を扱う方法」である。名称が似た概念でも、対象とする処理や目的を区別する。

Q0084

セキュア開発・脆弱性管理
タグ：協調的脆弱性開示
用語：協調的脆弱性開示の確認ポイント3：発見者と提供者が修正・公表時期を調整して脆弱性情報を扱う方法

用語と説明の組合せとして適切なものはどれか。論点は「協調的脆弱性開示」である。

A. STRIDE：発見者と提供者が修正・公表時期を調整して脆弱性情報を扱う方法
B. DAST：発見者と提供者が修正・公表時期を調整して脆弱性情報を扱う方法
C. CVSS：発見者と提供者が修正・公表時期を調整して脆弱性情報を扱う方法
D. 協調的脆弱性開示：発見者と提供者が修正・公表時期を調整して脆弱性情報を扱う方法

答え・解説

Q0084 正答：D. 協調的脆弱性開示：発見者と提供者が修正・公表時期を調整して脆弱性情報を扱う方法

解説：正しい組合せは「協調的脆弱性開示：発見者と提供者が修正・公表時期を調整して脆弱性情報を扱う方法」。用語だけでなく、何を守り、何を処理する概念かを確認する。

Q0085

セキュア開発・脆弱性管理
タグ：協調的脆弱性開示
用語：協調的脆弱性開示の確認ポイント4：発見者と提供者が修正・公表時期を調整して脆弱性情報を扱う方法

「協調的脆弱性開示」は、発見者と提供者が修正・公表時期を調整して脆弱性情報を扱う方法。

A. ○
B. ×

答え・解説

Q0085 正答：○

解説：正しい。協調的脆弱性開示は発見者と提供者が修正・公表時期を調整して脆弱性情報を扱う方法。実務では対象、目的、前提条件を併せて確認する。

Q0086

セキュア開発・脆弱性管理
タグ：協調的脆弱性開示
用語：協調的脆弱性開示の確認ポイント5：発見者と提供者が修正・公表時期を調整して脆弱性情報を扱う方法

組織が「発見者と提供者が修正・公表時期を調整して脆弱性情報を扱う方法」ために採用すべき概念又は仕組みはどれか。

A. STRIDE
B. 協調的脆弱性開示
C. DAST
D. CVSS

答え・解説

Q0086 正答：B. 協調的脆弱性開示

解説：この目的に対応するのは協調的脆弱性開示である。発見者と提供者が修正・公表時期を調整して脆弱性情報を扱う方法という機能・考え方を持つためである。

Q0087

セキュア開発・脆弱性管理
タグ：協調的脆弱性開示
用語：協調的脆弱性開示の確認ポイント6：発見者と提供者が修正・公表時期を調整して脆弱性情報を扱う方法

「協調的脆弱性開示」について、誤解を避けるための説明として最も適切なものはどれか。

A. 脆弱性の深刻度を基本・現状・環境評価基準で数値化する仕組み
B. 稼働中アプリケーションへ入力を送り外部から脆弱性を検出する手法
C. 発見者と提供者が修正・公表時期を調整して脆弱性情報を扱う方法
D. なりすまし、改ざん、否認、情報漏えい、サービス妨害、権限昇格で脅威を分類する手法

答え・解説

Q0087 正答：C. 発見者と提供者が修正・公表時期を調整して脆弱性情報を扱う方法

解説：協調的脆弱性開示は発見者と提供者が修正・公表時期を調整して脆弱性情報を扱う方法。似た用語との違いは、対象、時点、責任又は処理方法にある。

Q0088

セキュア開発・脆弱性管理
タグ：協調的脆弱性開示
用語：協調的脆弱性開示の確認ポイント7：発見者と提供者が修正・公表時期を調整して脆弱性情報を扱う方法

「協調的脆弱性開示」は、なりすまし、改ざん、否認、情報漏えい、サービス妨害、権限昇格で脅威を分類する手法。

A. ○
B. ×

答え・解説

Q0088 正答：×

解説：誤り。記述はSTRIDEの説明である。協調的脆弱性開示は発見者と提供者が修正・公表時期を調整して脆弱性情報を扱う方法。

Q0089

セキュア開発・脆弱性管理
タグ：協調的脆弱性開示
用語：協調的脆弱性開示の確認ポイント8：発見者と提供者が修正・公表時期を調整して脆弱性情報を扱う方法

次の状況で中心となる論点はどれか。「発見者と提供者が修正・公表時期を調整して脆弱性情報を扱う方法」ことが求められている。

A. 協調的脆弱性開示
B. DAST
C. CVSS
D. STRIDE

答え・解説

Q0089 正答：A. 協調的脆弱性開示

解説：中心となる論点は協調的脆弱性開示である。判断では、説明中の目的語と処理の方向を手掛かりにする。

Q0090

セキュア開発・脆弱性管理
タグ：協調的脆弱性開示
用語：協調的脆弱性開示の確認ポイント9：発見者と提供者が修正・公表時期を調整して脆弱性情報を扱う方法

「発見者と提供者が修正・公表時期を調整して脆弱性情報を扱う方法」という特徴を持つものを選べ。

A. CVSS
B. 協調的脆弱性開示
C. DAST
D. STRIDE

答え・解説

Q0090 正答：B. 協調的脆弱性開示

解説：協調的脆弱性開示が該当する。定義は発見者と提供者が修正・公表時期を調整して脆弱性情報を扱う方法であり、他の候補とは機能が異なる。