

1-1.XSS（クロスサイトスクリプティング）とは何か。Webアプリケーションにおけるリスクとともに説明せよ。

1-2.反射型XSSと格納型XSSの違いを簡潔に説明せよ。

1-3. XSSの攻撃に悪用されるHTMLタグや属性の例を2つ挙げて説明せよ。

1-4. XSSの被害により攻撃者が得ることができる情報や実行可能な行動を3つ挙げよ。

1-5. 開発時にXSSの脆弱性を防ぐために必要な出力時の処理を説明せよ。

1-6. CSP（Content Security Policy）とは何か。XSS対策としての効果を述べよ。

1-7. XSSの検出に用いられる代表的な自動診断ツールを1つ挙げ、その特徴を簡潔に述べよ。

1-8. XSS脆弱性を含むWebアプリケーションが持つ、信頼性・ユーザビリティ上のリスクを説明せよ。

1-9. 開発者が入力値のサニタイズを行う際に注意すべき点を1つ挙げて説明せよ。

1-10. XSSの脆弱性があったとしても、セッションハイジャックを防ぐためにWebアプリケーションが行うべき対策を1つ挙げて説明せよ。