Task 3

Securing the software development lifecycle (SDLC)

In this task, your knowledge will be tested within the area of application security in the context of SDLC

Here is the background information on your task

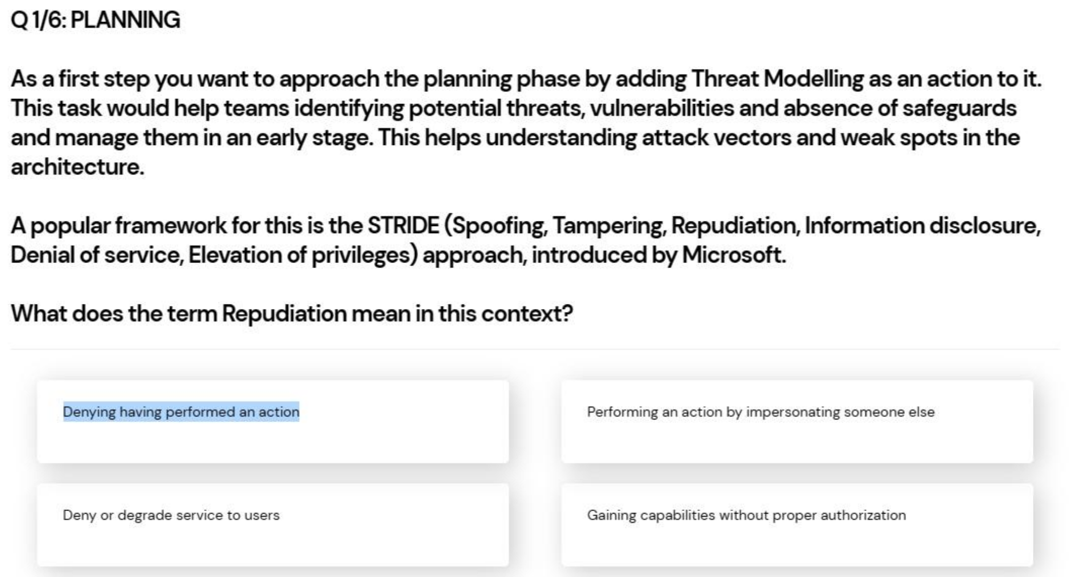
You are engaged as a security analyst in a project to help an organization increase the maturity of their security posture in their software development. The organization is an international retailer with a worldwide multi-market e-commerce platform. You are joining a team for which the main objective will be to overlook and improve the security procedures and processes for each development phase. The requested scope, which you are going to analyze, includes the following:

- Planning phase
- Requirements analysis
- Design
- Software development
- Software testing
- Operations & maintenance

Here is your task

Assess the background information and question of each task and provide your knowledge to help the organization secure its development. Good luck!

Note: As a consultant, you often need to research new subjects on your own. The link provided in section 4 will help with some background information, but it can be a good idea to search for



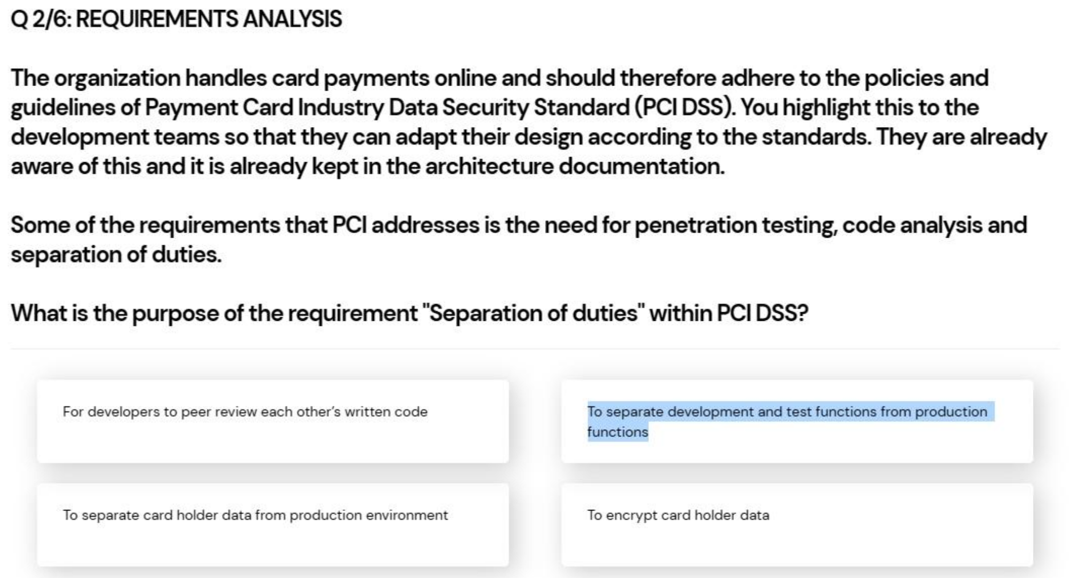
Q 1/6: PLANNING

As a first step you want to approach the planning phase by adding Threat Modelling as an action to it. This task would help teams identifying potential threats, vulnerabilities and absence of safeguards and manage them in an early stage. This helps understanding attack vectors and weak spots in the architecture.

A popular framework for this is the STRIDE (Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privileges) approach, introduced by Microsoft.

What does the term Repudiation mean in this context?

- Denying having performed an action
- Performing an action by impersonating someone else
- Deny or degrade service to users
- Gaining capabilities without proper authorization



Q 2/6: REQUIREMENTS ANALYSIS

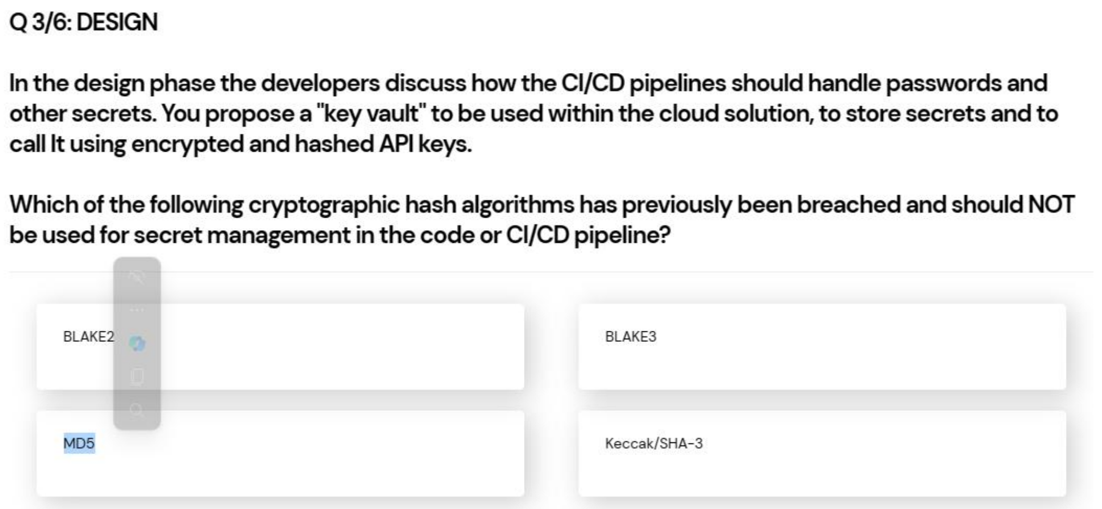
The organization handles card payments online and should therefore adhere to the policies and guidelines of Payment Card Industry Data Security Standard (PCI DSS). You highlight this to the development teams so that they can adapt their design according to the standards. They are already aware of this and it is already kept in the architecture documentation.

Some of the requirements that PCI addresses is the need for penetration testing, code analysis and separation of duties.

What is the purpose of the requirement "Separation of duties" within PCI DSS?

- For developers to peer review each other's written code
- To separate development and test functions from production functions
- To separate card holder data from production environment
- To encrypt card holder data

accenture

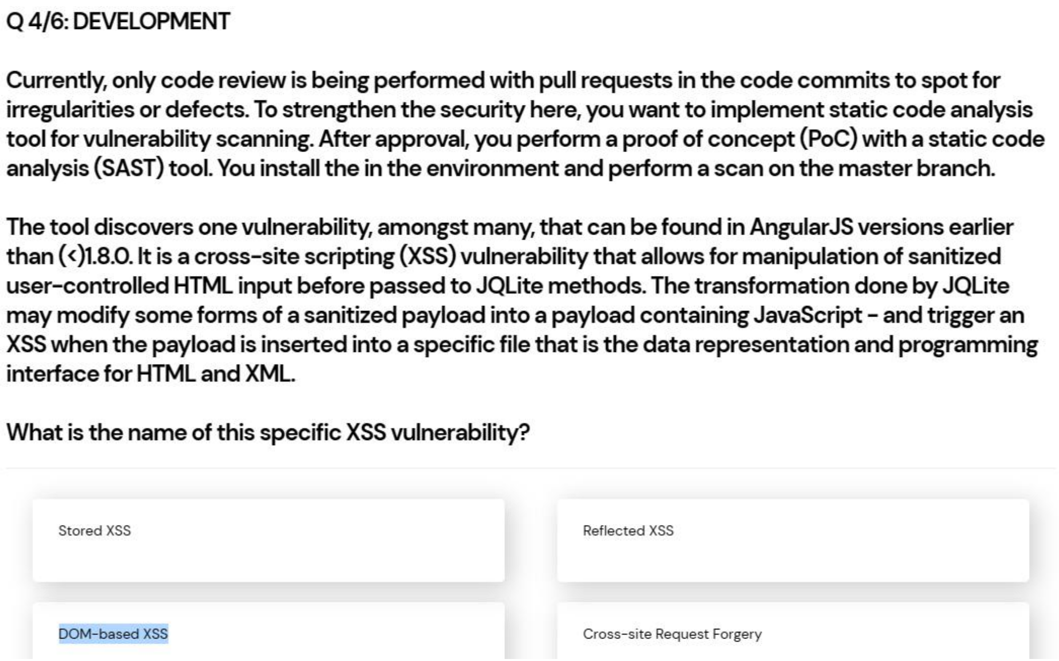


Q 3/6: DESIGN

In the design phase the developers discuss how the CI/CD pipelines should handle passwords and other secrets. You propose a "key vault" to be used within the cloud solution, to store secrets and to call It using encrypted and hashed API keys.

Which of the following cryptographic hash algorithms has previously been breached and should NOT be used for secret management in the code or CI/CD pipeline?

- BLAKE2
- BLAKE3
- MD5
- Keccak/SHA-3



Q 4/6: DEVELOPMENT

Currently, only code review is being performed with pull requests in the code commits to spot for irregularities or defects. To strengthen the security here, you want to implement static code analysis tool for vulnerability scanning. After approval, you perform a proof of concept (PoC) with a static code analysis (SAST) tool. You install the in the environment and perform a scan on the master branch.

The tool discovers one vulnerability, amongst many, that can be found in AngularJS versions earlier than (<)1.8.0. It is a cross-site scripting (XSS) vulnerability that allows for manipulation of sanitized user-controlled HTML input before passed to JQLite methods. The transformation done by JQLite may modify some forms of a sanitized payload into a payload containing JavaScript - and trigger an XSS when the payload is inserted into a specific file that is the data representation and programming interface for HTML and XML.

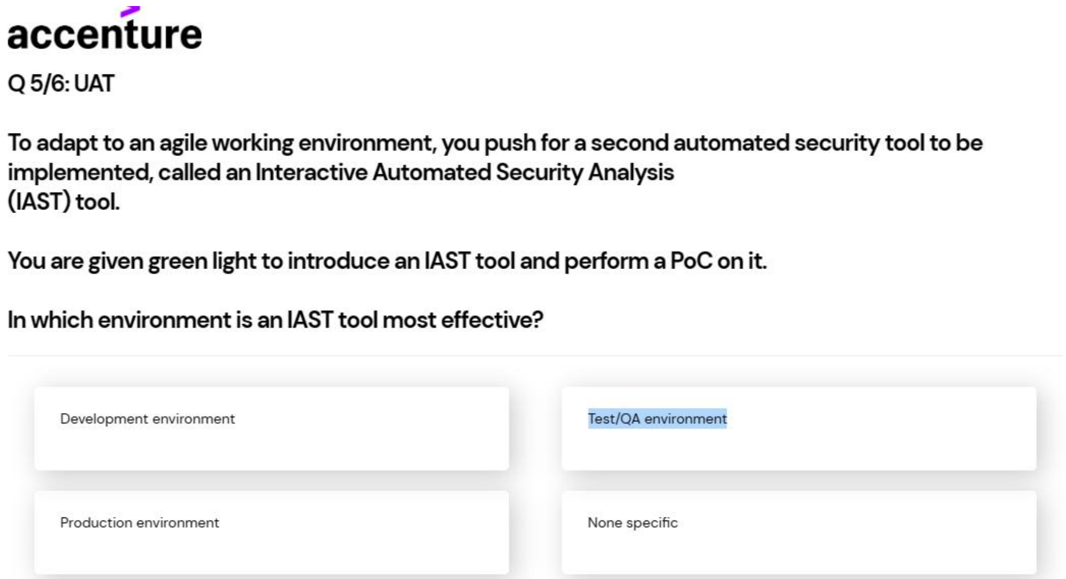
What is the name of this specific XSS vulnerability?

Stored XSS

Reflected XSS

DOM-based XSS

Cross-site Request Forgery



accenture

Q 5/6: UAT

To adapt to an agile working environment, you push for a second automated security tool to be implemented, called an Interactive Automated Security Analysis
(IAST) tool.

You are given green light to introduce an IAST tool and perform a PoC on it.

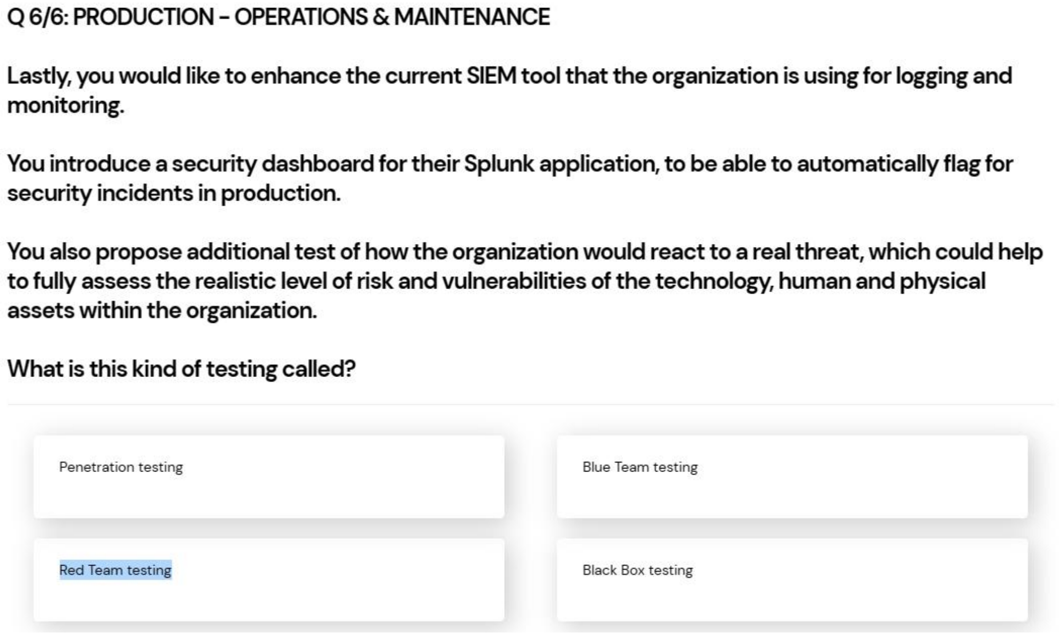
In which environment is an IAST tool most effective?

Development environment

Test/QA environment

Production environment

None specific



Q 6/6: PRODUCTION - OPERATIONS & MAINTENANCE

Lastly, you would like to enhance the current SIEM tool that the organization is using for logging and monitoring.

You introduce a security dashboard for their Splunk application, to be able to automatically flag for security incidents in production.

You also propose additional test of how the organization would react to a real threat, which could help to fully assess the realistic level of risk and vulnerabilities of the technology, human and physical assets within the organization.

What is this kind of testing called?

Penetration testing

Blue Team testing

Red Team testing

Black Box testing