ASSIGNMENT II: SECURITY ASSESSMENT QUESTIONNAIRE

JORGE BLANCO PRIETO

Tabla de contenido

INTRODUCTION

En el presente documento se analizan y se comparan los cuestionarios definidos en la anterior tabla de contenidos. Para analizar los cuestionarios se propone una guía de preguntas seguida por la plantilla de la siguiente tabla. El objetivo tras el análisis es poder evaluar los distintos cuestionarios y escoger el más adecuado para aplicarlo en el proyecto final.

Las preguntas que se han de responder vienen fijadas en la siguiente tabla:

ID (company, release date, updates)	…
Goal of the questionnaire	…
Target users (if possible)	…
Description	…
Positive	…
Negative	…
Others	…

APPLICATION SECURITY ASSESSMENT QUESTIONNAIRE

ID (company, release date, updates)	Este cuestionario está diseñado por la ***Information Security Office (ISO)*** de la Universidad Carnegie Mellon (Pittsburgh). La última revisión de su web es del 02/11/2014.
Goal of the questionnaire	El objetivo del cuestionario es: ° Explicar el proceso para solicitar una evaluación ° Describir el conjunto de servicios de evaluación de la seguridad que ISO ofrece a los miembros de la comunidad universitaria. ° Ayudar a comprender el entorno objetivo. Proporciona claridad y consistencia. ° Analizar y solucionar vulnerabilidades del sistema. Trata de responder preguntas como si la aplicación expone los servidores y/o el software ante los ataques o si un usuario malintencionado puede acceder, modificar o destruir datos o servicios del sistema.
Target users (if possible)	Los usuarios target a los que se encuentra dirigido es la comunidad universitaria de Carnegie Mellon; no obstante, es un documento público que puede ser utilizado por cualquier usuario.
Description	El cuestionario define su necesidad para garantizar la exactitud de las estimaciones de tiempo, así como la exhaustividad de la evaluación. El cuestionario viene definido por cinco partes: - Información básica: datos personales y datos de contacto del usuario. - Información de auditoría: datos generales sobre la auditoría (ISO). - Información de seguridad de red. - Información del sistema. - Información del servicio.
Positive	El cuestionario es fácil y muy intuitivo dada la detallada explicación proporcionada por ISO. Además, se advierte en la portada el alcance de las evaluaciones. Una vez registrado el cuestionario por el usuario, ISO mantiene una reunión para su revisión junto con el usuario.
Negative	Como indica al inicio del documento, ISO no puede evaluar todas las plataformas o aplicaciones existentes. No es posible para ISO cumplir con todos los requisitos de plazos temporales. En estos casos, ISO puede contratar a socios externos para prestar el servicio de evaluación solicitado, derivando en un posible aumento de los costes (costes asociados) que repercutirán en la unidad organizativa solicitante.
Others	Hay un proceso que seguir descrito en el documento para llevar a cabo una evaluación, señalado mediante un mapa de flujo. Se ha de contactar con ISO para solicitar la evaluación e ISO debe aprobar el proyecto previo a realizar el cuestionario. Tras el registro del cuestionario, se han de llevar a cabo varias reuniones cuyo objetivo será determinar qué tipo de evaluación es la más apropiada para el proyecto en cuestión. Además, se definen varios tipos de evaluaciones que puede ofrecer ISO.

VSAQ

ID (company, release date, updates)	Este cuestionario está diseñado por Google, aunque, según como se indica en el Github, no es un producto oficial de Google (ni prototipo). Su commit inicial se da el 7 de marzo de 2016 y ha recibido 11 actualizaciones distribuidas entre 2016 y 2021.
Goal of the questionnaire	El objetivo de VSAQ (Github) es crear una aplicación de cuestionarios interactivos para apoyar las revisiones de seguridad, facilitando la recogida de información y la redistribución de los datos recogidos en forma de plantilla. Estos cuestionarios se utilizan para evaluar la seguridad de aplicaciones de terceros. Las plantillas proporcionadas se pueden utilizar para terceros o incluso para realizar una autoevaluación de un software propio.
Target users (if possible)	El Github es público así que cualquier usuario puede acceder.
Description	VSAQ (Vendor Security Assessment Questionnaires) está formado por cuatro cuestionarios en función del entorno al que se encuentra dirigido: - *Web Application Security Questionnaire* - *Security & Privacy Program Questionnaire* - *Infrastructure Security Questionnaire* - *Physical & Datacenter Security Questionnaire* En el Readme del Github se explica el procedimiento (workflow) para la revisión.
Positive	Se proporciona una vista web para rellenar los cuestionarios de manera más fácil. El repositorio proporciona instrucciones para ejecutar el proyecto (es de código abierto). Podrían llegar a editarse los cuestionarios si se requiere una evaluación más precisa y sin un backend muy elaborado.
Negative	El proyecto no muestra información detallada sobre los cuestionarios, se centra más en el despliegue del código que de su propia explicación.
Others	

APPLICATION SECURITY QUESTIONNAIRE (HIMSS)

ID (company, release date, updates)	Cuestionario de seguridad de aplicación diseñado por HIMSS (Healthcare Information and Management Systems Society). Fecha de lanzamiento en febrero del 2007 y actualmente se encuentra en la versión 2.3.
Goal of the questionnaire	El objetivo de este cuestionario es la evaluación de controles de seguridad básicos inherentes a una aplicación o sistema que creará, recibirá, mantendrá o transmitirá ePHI (datos personales relacionados con la salud). Permite comprender mejor los controles de seguridad ofrecidos y por lo tanto ayudar a evaluar las vulnerabilidades y los riesgos asociados con el uso de una aplicación o sistema.
Target users (if possible)	El cuestionario (denominado ASQ) es una herramienta de autoevaluación para que sea completada por los proveedores (organizaciones de proveedores de atención médica u otros compradores de productos médicos).
Description	El cuestionario de seguridad de la aplicación se compone de las siguientes partes: - Datos personales (información básica) de la organización médica. - Gestión del acceso (usuarios). - Información de auditoría. - Seguridad de acceso en remoto. - Protección frente a código malicioso. - Gestión de la configuración y control de cambios. - Exportación de datos y transferencia. - Otras funciones.
Positive	Cuestionario con preguntas y respuestas (Yes, No, N/A y Comment) enfocada en el tratamiento de los datos personales relacionados con salud de los usuarios. Se proporciona una sección para añadir comentarios.
Negative	El proyecto no muestra información detallada sobre los cuestionarios, se centra más en el despliegue del código que de su propia explicación.
Others	

SANS AUDITING AND ASSESSMENT

ID (company, release date, updates)	Cuestionario publicado por Ted Mina del SANS Institute. Se encuentra en la versión 1.2e, publicada en Baltimore, entre el 18 y 20 de mayo de 2001.
Goal of the questionnaire	El objetivo del documento es tratar de evaluar adecuadamente la seguridad de las aplicaciones software.
Target users (if possible)	El cuestionario es accesible de forma público.
Description	El cuestionario contiene sofisticados controles de acceso multinivel, así como niveles de seguridad. Se centra en: - Sensibilidad de los datos (confidencialidad, integridad y disponibilidad). - Recuperación y Backup. - Vulnerabilidad al fallo (hardware, software, humano, de entorno, etc.).
Positive	Cuestionario intuitivo con posibilidad de añadir comentarios a la selección de las respuestas. Posteriormente al cuestionario se encuentran recomendaciones específicas que ayudan a cumplir los requisitos de seguridad.
Negative	Cuestionario muy genérico.
Others	

VENDOR SECURITY QUESTIONNAIRE – PURDUE UNIVERSITY

ID (company, release date, updates)	Cuestionario publicado Purdue University (última version 8.4 publicada el 05 de abril de 2022). La primera versión que muestra el cuestionario es la versión 3 con fecha el 2 de octubre de 2015.
Goal of the questionnaire	Cuestionario publicado para proteger los recursos IT, información, software de terceros, aplicaciones o servicios cloud que ofrece la universidad Purdue. Trata de identificar todos los riesgos que puedan estar presentes.
Target users (if possible)	El cuestionario está orientado a miembros de la universidad de Purdue y servicios internos, aunque es accesible de manera pública.
Description	El cuestionario se divide en 4 partes: - Project Information (tab 1): descripción de la información de proyecto, así como del autor. - Data Security (tab 2): se trata con información (datos) sensible y/o restringidos. - Vendor Hosted (tab 3): El siguiente documento debe ser proporcionado por la Universidad (bajo un NDA). - Purdue Hosted (tab4): Cuestionario dirigido para el autor o el desarrollador del sistema.
Positive	Cuestionario muy específico y muy completo para obtener información acerca de los datos, hosting, etc. Se ofrecen instrucciones detalladas con el proceso a seguir.
Negative	El cuestionario está muy dirigido para Purdue University y se requiere de su supervisión y contribución para llevarlo a cabo. En el cuestionario se menciona que Tab 1 y Tab 2 (una vez completadas) deben ser revisadas por la universidad.
Others	En la parte inicial del cuestionario se ofrecen una serie de instrucciones para llevarlo a cabo. Tal y como se menciona en su web de descarga, existe un proceso enumerado para llevar a cabo el cuestionario donde se requiere la revisión de la universidad.

INFORMATION SECURITY REVIEW QUESTIONNAIRE – IT SUPPORT CUNY

ID (company, release date, updates)	Cuestionario publicado por la ciudad universitario de Nueva York (The City University of New York – CUNY) con la versión 1.2.
Goal of the questionnaire	El cuestionario tiene como objetivo facilitar la identificación de los requerimientos de seguridad para un proyecto tecnológico, aplicación o sistema de CUNY.
Target users (if possible)	Esta diseñado para miembros de CUNY, aunque puede utilizarse en ámbito público.
Description	El cuestionario se divide en 8 partes: - Data classification: clasificación de los datos que involucra el proyecto. - Use of Vendor IT services: describe el tema para adquirir servicios IT. - Identity Management, Access control and Authorization: identifica a los usuarios que tendrán acceso al producto y/o servicio IT. - Network Access and Communication: identifica el alcance de los requerimientos de acceso de red necesarios. - Data protection: Disponibilidad de la protección de datos y sus requerimientos. - Loggin and Auditing. - Business Continuity/Disaster Recovery. - Other comments.
Positive	Cuestionario que alberga distintos ámbitos a tratar.
Negative	El cuestionario se encuentra muy orientado a servicios, aplicaciones o miembros de CUNY. No utiliza preguntas cerradas.
Others	

PAYMENT CARD INDUSTRY (PCI) DATA SECURITY STANDARD

ID (company, release date, updates)	Cuestionario publicado por Security Standars Council PCI en diciembre de 2004. Actualmente se encuentra en la versión 1.0.
Goal of the questionnaire	El cuestionario tiene como objetivo tratar áreas específicas de seguridad, basadas en los requerimientos incluidos en el PCI Data Security Standard
Target users (if possible)	El cuestionario tiene como usuarios target compañías y usuarios que utilicen servicios de pagos con tarjetas (débito o crédito).
Description	El cuestionario se divide en 6 partes: - Build and Maintain a Secure Network. - Protect Cardholder Data. - Maintain a Vulnerability Management Program - Implement Strong Access Control Measures. - Regularly Monitor and Test Networks - Maintain a policy that addresses information security
Positive	Cuestionario muy completo con preguntas cerradas de Si/No con detallada descripción de los requerimientos que conforman las partes.
Negative	El cuestionario no ofrece forma de justificar respuesta (comentarios), únicamente proporciona un punto para explicar la sección por completo. El cuestionario está muy dirigido a un ámbito de aplicación (pago con tarjetas).
Others	Cuestionario que permite contestar con N/A y justificar una breve explicación. Proporciona un rating del assessment.

CONCLUSIÓN

El proyecto a evaluar en la asignatura consiste en un chatbot web (aplicación web) que responde preguntas genéricas y/o guiadas por alumnos de un curso; no obstante, no se encuentra en el ámbito universitario. En el presente documento se han analizado diversos cuestionarios donde se obtienen las siguientes conclusiones:

- Application Security Assessment Questionnaire (ASAQ): Cuestionario dirigido al ámbito académico que sigue un proceso donde la universidad Carnegie Mellon debe involucrarse al tener que realizar revisiones del mismo.
- VSAQ: Cuestionario de código abierto definido y diseñado por Google completo y propicio para aplicaciones web.
- Application Security Questionnaire (HIMSS): Cuestionario dirigido a aplicaciones que trabajen con datos sensibles (datos de salud).
- Sans Auditing and Assessment: Cuestionario muy genérico.
- Vendor Security Questionnaire: Cuestionario muy completo, aunque se encuentra dirigido a proyectos académicos y a la universidad donde fue definido. Al igual que ASAQ la universidad debe estar involucrada en la revisión del cuestionario.
- Information Security Review Questionnaire: Cuestionario muy orientado a CUNY.
- PCI Data Security Standard: Orientado a sectores de pago con tarjeta, distante del proyecto en cuestión.

Dado el análisis, se considera que el cuestionario más adecuado para el proyecto del chatbot viene dado por VSAQ.