UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA.

PROCESO DE TITULACIÓN

DICIEMBRE 2022 – ABRIL 2023

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

PRUEBA PRÁCTICA

PREVIO A LA OBTENCIÓN DEL TÍTULO DE:

INGENIERO EN SISTEMAS DE INFORMACIÓN

TEMA:

ANÁLISIS DE UNA METODOLOGÍA DE SEGURIDAD INFORMÁTICA PARA EL DESARROLLO DE APLICACIONES MÓVILES USANDO HERRAMIENTAS OPEN SOURCE

ESTUDIANTE:

KIARA MICHELLE GOMEZ COELLO

TUTOR:

DIAZ CHONG MIGDALIA TERESA

AÑO 2023

RESUMEN

Al aplicar una metodología de seguridad informática contribuimos a mejorar la seguridad de las aplicaciones móviles y así se evita presentar vulnerabilidades que puedan ser explotadas por usuarios malintencionados o hackers. Si el desarrollo de las aplicaciones móviles no se realiza con cuidado y atención, se corre el riesgo que algún atacante informático acceda a información confidencial o en el peor de los casos que controlen la aplicación. La utilización de herramientas de seguridad Open Source proporcionan transparencia y confianza a los usuarios, lo que logra aumentar el uso de la aplicación y reducir el riesgo de ataques. La metodología OSSTMM nos permite realizar pruebas de penetración y evaluación de seguridad en sistemas de información y tecnología, esta metodología se divide en cinco áreas las cuales permiten recabar el estado actual de las aplicaciones móviles.

Palabras claves: OSSTMM, hackers, vulnerabilidad, seguridad, aplicaciones moviles, amenazas informática.

SUMMARY

By applying an information security methodology, we contribute to improving the security of mobile applications, thereby avoiding vulnerabilities that may be exploited by malicious users or hackers. If mobile applications development is not done with care and attention, there is a risk that a cyber attacker may access confidential information or, in the worst case scenario, control the application. The use of Open Source security tools provides transparency and confidence to users, which increases the use of the application and reduces the risk of attacks. The OSSTMM methodology allows us to perform penetration testing and security evaluation on information and technology systems. This methodology is divided into five areas that allow us to gather the current state of mobile applications.

Keywords: OSSTMM, hackers, vulnerability, security, mobile applications, computer threats.

Contenido

PLANTEAMIENTO DEL PROBLEMA

Con el transcurso del tiempo la creación de aplicaciones móviles ha presentado un crecimiento notable y se ha llegado a convertir en parte fundamental de la vida cotidiana, siendo esenciales cada día ya que las aplicaciones las podemos encontrar en el ámbito laboral tanto como en empresas públicas y privadas, en la educación, entretenimientos, bancas móviles y otros mas. Obteniendo así información de vital importancia como son los datos personales, acceso a cuentas bancarias, acceso a ubicación en tiempo real, cámara, videos, audio, entre otros permisos que puede tener una app, todo esto sin duda la hace vulnerables a ataques, lo cual conlleva a la perdida de todo lo antes mencionado, causando un sinnúmero de problemas a los usuarios y a las instituciones que contratan el servicio móvil de dichas app.

El uso de una metodología de seguridad informática nos va a permitir establecer cuál será una solución para mejorar la seguridad de las apps móviles, ayudando a que no exista vulnerabilidades dentro de estas, también cuidando de los efectos y consecuencias que pueden originar la poca seguridad dentro de las apps.

Para tener la capacidad de determinar el objetivo del estudio de caso se va a recurrir al método cuantitativo, el cual nos permite obtener información mediante encuestas y se usara una metodología que tenga las mejores prácticas y estándares, es decir la guía de pruebas de OSSTMM, ya que se enfoca en las inseguridades más comunes de las aplicaciones y comprobar que no existan vulnerabilidades. ¿Y si existiese vulnerabilidades y amenazas en las aplicaciones móviles que podría suceder? Se debe reportar para que los desarrolladores corrijan el inconveniente lo antes posible.

Una de las principales desventajas que pueden presentar las aplicaciones móviles es que sino llegan a presentar un riguroso cuidado en todos los procesos, técnicas e instrumentos que se utiliza para el desarrollo de estas, dejan la posibilidad a entradas a

posibles usuarios mal intencionados o hackers, teniendo así problemas y debido a todo esto pueden ocasionar perdidas de información importante y perdidas monetarias para las instituciones que contratan el servicio móvil.

Una aplicación que no cuente con una metodología de seguridad esta propensa a presentar un desequilibrio en la fortaleza de los mecanismos de autenticación y autorización de una aplicación, los cuales pueden ser explotados por los atacantes para acceder a información no autorizada, dándoles la posibilidad de acceder y robar las secciones de los usuarios, también pueden estar expuestas a que atacantes puedan acceder a información confidencial o incluso tomar el control de la aplicación mediante una inyección de SQL.

Las aplicaciones móviles a menudo se comunican con servidores remotos para obtener datos y enviar información. Si las comunicaciones no están cifradas, los atacantes pueden interceptar y leer información confidencial. OSSTMM incluye pruebas para evaluar la seguridad de las comunicaciones entre la aplicación móvil y los servidores remotos, así mismo estas a menudo almacenan datos confidenciales en el dispositivo, como contraseñas, información de pago y datos personales. Si los datos no están almacenados de manera segura, los atacantes pueden acceder a ellos.

Todo lo antes mencionado nos lleva a plantearnos la siguiente interrogante, ¿Como el análisis de una metodología de seguridad informática para el desarrollo de aplicaciones móviles usando herramientas Open Source, nos permitirá mejorar la seguridad de las apps y evitar vulnerabilidades?

JUSTIFICACIÓN

En la actualidad, la seguridad informática se ha convertido en un tema crítico debido al aumento constante de ataques cibernéticos y debilidades en las aplicaciones móviles. Por lo tanto, es esencial implementar medidas de seguridad efectivas para proteger la información y la privacidad de los usuarios de aplicaciones móviles.

El uso de una metodología de seguridad informática para el desarrollo de aplicaciones móviles usando herramientas Open Source es fundamental para garantizar la seguridad y privacidad de los usuarios que utilizarán estas aplicaciones. Las aplicaciones móviles están expuestas a diversos riesgos y vulnerabilidades, como la explotación de vulnerabilidades de seguridad, el acceso no autorizado a datos sensibles, el malware y los ataques de ingeniería social.

Las herramientas Open Source son generalmente gratuitas y de código abierto, es decir el código fuente está disponible públicamente, lo que significa que pueden ser utilizadas, modificadas y distribuidas de manera gratuita, lo que significa que el costo de implementar la metodología de seguridad informática puede ser reducido significativamente y también son flexibles y se pueden adaptar a las necesidades específicas de cada proyecto de desarrollo de aplicaciones móviles.

Una de las principales ventajas que tiene usar herramientas Open Source en una metodología de seguridad informática es que permite proporcionar una mayor transparencia y confianza a los usuarios de las aplicaciones móviles y estas cuentan con una gran cantidad de recursos de seguridad. Si los usuarios saben que una aplicación móvil ha sido desarrollada con herramientas de seguridad Open Source, pueden tener más confianza en la seguridad de la aplicación y, por lo tanto, ser más propensos a utilizarla.

OBJETIVOS

Objetivo general.

- Analizar la factibilidad del uso de la metodología de seguridad informática para el desarrollo de aplicaciones móviles usando herramientas Open Source

Objetivo Específico

- Identificar los procesos metodológicos relacionados con la seguridad informática para el desarrollo de aplicaciones móviles usando herramientas open source.
- Conocer de manera teórica y fundamentada los aportes de la metodología seguridad informática para el desarrollo de aplicaciones móviles.
- Proponer y recomendar las estrategias importantes de la metodología de seguridad informática para el desarrollo de aplicaciones móviles usando herramientas open source.

LÍNEAS DE INVESTIGACIÒN

El presente caso de estudio está enfocado en la línea de investigación sistemas de información y comunicación, emprendimiento e innovación, sostenida por la sublíneas de investigación de redes y tecnologías inteligentes de software y hardware. Se utilizo la investigación cuantitativa porque nos permite obtener resultados favorables sobre el análisis de una metodología de seguridad informática para el desarrollo de aplicaciones móviles usando herramientas Open Source, mediante el uso de encuestas y entrevistas se pudo obtener un análisis mas detallado sobre la metodología hacer utilizada.

MARCO CONCEPTUAL

Metodologías de seguridad de app móviles

Las metodologías de desarrollo se originan como una respuesta a la crisis de los años 70 que desencadeno un conjunto de problemas relacionados al proceso de construcción de un producto software eficaz, de calidad y a tiempo, existen numerosas metodologías dotadas con variadas características que las lleva a afrontar el desarrollo de software de diferentes formas, buscando obtener un producto de calidad, al pasar los años algunas de ellas han quedado obsoletas y no responden a los nuevos desafíos, la realidad actual exige la construcción guiada por métodos adaptables a los cambios basados en la seguridad y agilidad (Lopez & Garcia, 2021).

Los cambios de requisitos de un producto software cuando se solicita su construcción y además cuando está en plena etapa de desarrollo, conlleva la utilización de metodologías modernas que dejen atrás las tradicionales, debido a que sus conceptos son muy rígidos, no permiten la adaptabilidad y no toman en cuenta la seguridad, en consecuencia, estas no permiten satisfacer las necesidades del cliente. Para afrontar esta problemática se han establecido metodologías que usan técnicas agiles, que disminuyen el tiempo de fabricación del producto software, fallos técnicos, vulnerabilidades, rigidez al cambio de requisitos y a la evolución (Lopez & Garcia, 2021).

Un producto software puede ser vulnerable, ya sea por propios fallos de construcción o por ataques provocados, para conseguir la disminución de vulnerabilidades y que el producto sea considerado seguro, se deben aplicar medidas como la integración de conceptos de seguridad en todas sus etapas de elaboración. Al utilizar una metodología de construcción que permita integrar la seguridad desde el ciclo de vida del software, se busca conseguir un producto robusto de confianza, que realice solo las funciones para lo que fue creado, minimizando comportamientos inesperados de

manera que se asegure la integridad, confiabilidad y confidencialidad (Lopez & Garcia, 2021).

Las metodologías de seguridad de apps móviles nos permiten garantizar que las apps móviles sean confiables y resguarden la privacidad e información de los usuarios que las utilizan, debido a esto se puede certificar que los usuarios no tendrían desconfianza al momento de utilizarlas. Algunas de las ventajas del uso de alguna metodología de seguridad son:

Identificar riesgos: La metodología de seguridad permite contribuir a la identificación de los posibles riesgos de seguridad de una app móvil. Los riesgos pueden contener vulnerabilidades de seguridad, probables puntos débiles y exposiciones a amenazas potenciales.

Prevenir ataques: Permite prevenir ataques de manera maliciosa en una aplicación. Al tener en cuenta todas las medidas preventivas que se deben realizar y las de seguridad, se logran disminuir muchos ataques y se protege los datos de los usuarios de dichas apps.

Mejorar la calidad: Esta también permiten perfeccionar la calidad de una aplicación móvil. Al utilizar normas de seguridad informáticas adecuadas desde un inicio, se logra impedir la insuficiencia de parches de seguridad.

Protección de datos: Ayudan a protección de la información de los usuarios. Existen diferentes tipos de datos como son los datos personales, financieros y de otra índole todos estos conviene manejarlos con suma precaución y una metodología de seguridad informática consigue que dichos datos se protejan de manera adecuada.

OSSTMM

OSSTMM es un estándar profesional para el testeo de seguridad en cualquier entorno, desde el exterior como el interior. Incluye lineamientos de acción, la ética del

tester profesional, legislación sobre testeo de seguridad y un conjunto integral de test (Ovallos, Rico, & Medina, 2020).

OSSTMM (Manual de Metodología de Pruebas de Seguridad de Código Abierto), es un marco de trabajo que sigue un enfoque científico, sistemático y metodológico para realizar pruebas de penetración y evaluación de seguridad en sistemas de información y tecnología. Este método ofrece un conjunto estandarizado de pruebas para medir la seguridad de la infraestructura tecnológica de una organización, incluyendo redes, sistemas operativos, aplicaciones, bases de datos y otros componentes. La metodología OSSTMM se divide en cinco áreas principales: información, procesos, personas, tecnología y físico.

Lo más importante en esta metodología es que los diferentes tests son evaluados y ejecutados donde sean aplicables, hasta arribar a los resultados esperados dentro de un período de tiempo determinado. Solo así el testeador habrá ejecutado el test en conformidad con el modelo OSSTMM, y por ello, el informe podrá ser considerado mínimamente exhaustivo (Ovallos, Rico, & Medina, 2020).

Las pruebas de penetración es una práctica para poner a prueba un sistema informático, red o aplicación web para encontrar vulnerabilidades que un atacante podría explotar, las pruebas de penetración pueden ser automatizadas con aplicaciones de software. De cualquier manera, el proceso incluye la recopilación de información sobre el objetivo antes de la prueba reconocimiento, la identificación de posibles puntos de entrada, intentos de entrar ya sea virtualmente o de manera real y el reporte de los resultados (Ortiz, 2020).

Aplicaciones

En la era de la información e inmediatez en la que nos encontramos las organizaciones dependen en gran medida de las aplicaciones tecnológicas para llevar a cabo tareas cotidianas como enviar mails, revisar estados de cuentas, recibir y enviar informes entre otras actividades que en la actualidad son realizadas a través de aplicaciones para dispositivos móviles (Puetate & Ibarra, 2020).

Existen diferentes tipos de aplicaciones, las cuales son:

- Aplicaciones nativas
- Aplicaciones hibridas
- Aplicaciones web progresiva

Aplicaciones Nativas

Las aplicaciones nativas son aquellas aplicaciones que se han desarrollado en el lenguaje nativo del sistema operativo en el que se va a ejecutar, por lo cual, si se requiere hacer una aplicación que se ejecute en el sistema operativo Android, se debe hacer la codificación de la aplicación en el lenguaje de programación Java o en Kotlin, y si quiere que la aplicación se ejecute en el sistema operativo iOS, se debe hacer la codificación en el lenguaje de programación Objective-C o Swift (Muñoz & Vasco, 2022).

Las aplicaciones nativas son concebidas y ajustadas para proporcionar la más excelente experiencia al usuario en la plataforma que se desenvuelven. Por ejemplo, pueden interactuar con los sensores del dispositivo, tales como la cámara, el micrófono, el GPS y los acelerómetros, lo que les concede ofrecer funciones más variadas y adaptadas en comparación con otras aplicaciones.

Aplicaciones hibridas

Las aplicaciones móviles híbridas son una combinación de tecnologías web como HTML,CSS y JavaScript, que no son ni aplicaciones móviles verdaderamente nativas, porque consisten en un WebView ejecutado dentro de un contenedor nativo, ni tampoco

están basadas en Web, porque se empaquetan como aplicaciones para distribución y tienen acceso a las APIs nativas del dispositivo (Contreras, Peña, & Santillan, 2019).

A diferencia de las aplicaciones nativas que se diseñan para una plataforma específica como iOS o Android, las aplicaciones híbridas se pueden crear para varias plataformas utilizando un solo código base, lo que las hace más rápidas y rentables de desarrollar que las aplicaciones nativas.

Aplicaciones web progresivas

Las aplicaciones web progresivas, es un término de un nuevo tipo de aplicaciones que acerca a la unificación de aplicaciones web-nativas, incrementando su funcionalidad, conforme las capacidades del dispositivo en el que se ejecuta, de ahí la palabra progresiva, web por qué se hace referencia a su desarrollo basado en tecnologías web (CAIHUARA, 2019).

Un nuevo conjunto de estándares propuestos por un grupo de investigación de Google busca unificar, mediante la introducción de funciones, como soporte sin conexión, sincronización en segundo plano e instalar el home-screen en el navegador, este enfoque se conoce como aplicaciones web progresivas (PWA) (CAIHUARA, 2019).

Es decir, que las aplicaciones web progresivas (PWA) son aplicaciones web que se han desarrollado para ofrecer una experiencia similar a las aplicaciones nativas de smartphones, tanto en su diseño como en su funcionamiento. Aunque se acceden a través de un navegador web, una vez que se han añadido a la pantalla de inicio de un dispositivo móvil, se comportan como aplicaciones independientes.

Vulnerabilidades informáticas

Consistirá en cualquier debilidad que puede explotarse para causar pérdida o daño al sistema. De esta manera, en punto más débil de seguridad de un sistema consiste en el punto más débil de seguridad de un sistema, consiste en el punto de mayor vulnerabilidad de ese sistema. Ataque Es cualquier acción que explota una vulnerabilidad (Guevara Aulestia & Quirola Valarezo, 2019)

Los ciberdelincuentes sacan provecho de las vulnerabilidades para atacar, los ataques que cometen muchas veces son de tipo ransomware, malware, phishing, entre otros tipos de ataques cibernéticos, obteniendo así acceso a información confidencial, sustrayendo datos, perpetrando fraudes financieros, entorpeciendo servicios obteniendo el control de sistemas completos.

Las vulnerabilidades en los sistemas informáticos, software, hardware, redes y otros sistemas, representan debilidades que pueden ser explotadas por atacantes con fines malintencionados. Esto incluye la obtención de acceso no autorizado, la manipulación, robo o daño de información, entre otras acciones.

Dichas vulnerabilidades pueden ser causadas por varios factores, como errores de programación, configuraciones incorrectas, falta de parches de seguridad o contraseñas débiles. Los atacantes utilizan varias técnicas para explotar estas vulnerabilidades, como el phishing, la ingeniería social, la explotación de errores de software o malware, etc. Es importante que los usuarios y las organizaciones tomen medidas preventivas para mitigar estas vulnerabilidades y proteger sus sistemas.

Es vital importancia que los usuarios y las organizaciones tengan conocimiento acerca de las vulnerabilidades en sus sistemas y tengan medidas para controlarlas y prevenirlas.

Herramientas Open-Source

Las herramientas de código abierto, conocidas también como herramientas open source, son programas de computadora cuyo código fuente se encuentra disponible públicamente y puede ser modificado, distribuido y utilizado sin restricciones por cualquier persona interesada.

Generalmente, estas herramientas son desarrolladas por una comunidad de programadores que trabajan en colaboración en línea para crear software accesible y gratuito para todos. Ejemplos de herramientas open source son el sistema operativo Linux, la suite de ofimática LibreOffice, el navegador web Firefox y la plataforma de desarrollo web Apache.

Las herramientas open source son apreciadas por su flexibilidad, transparencia y la comunidad de usuarios que contribuyen constantemente al desarrollo y mejora del software. Además, estas herramientas pueden ser personalizadas y adaptadas a las necesidades específicas de los usuarios y organizaciones, lo que las hace una opción popular en muchos ámbitos tecnológicos.

Amenazas informáticas

Según, (Muñoz, Zapata, Requena, & Ricardo, 2019)” Los riesgos informáticos son amenazas y vulnerabilidades que afectan en todos los aspectos a la empresa, y las

consecuencias pueden ser muy graves en relación a la información que se está manejando".

Muchas veces se confunde los términos amenazas con ataques informáticos, estos términos van de la mano, pero no son iguales. Las amenazas informáticas son todo tipo de acciones maliciosas destinadas a comprometer la seguridad de un sistema informático, incluso el acceso no autorizado, la eliminación de datos o la modificación de la información guardada. Las amenazas informáticas suelen contener virus informáticos, troyanos, etc.

Mientras tanto, los ataques informáticos son actividades concretas que buscan explotar las vulnerabilidades en sistemas informáticos para así obtener permisos no autorizado, perjudicar o arruinar información, o perpetrar otros tipos de actividades maliciosas. Dichos ataques son cometidos por personas, grupos u organizaciones con diferentes motivos, como es el caso de robo de información confidencial o del sabotaje.

En conclusión, las amenazas informáticas simbolizan un conjunto de posibles riesgos que podrían perjudicar la seguridad de los sistemas informáticos, por otro lado, los ataques informáticos son actividad determinadas que aprovechan estas amenazas para lograr un objetivo específico.

Ataques cibernéticos

El ciber ataque es uno de los delitos informáticos que más ha crecido del 2005, el robo de información y la afectación a instituciones públicas y privadas son las principales consecuencias de los ataques cibernéticos. Mundialmente, las organizaciones y compañías de seguridad establecen medidas para prevenir los ataques (Alvarado, 2020).

En la Seguridad Informática, no importa que equipamiento de Software o Hardware se tenga instalado, porque siempre el eslabón más débil en esta cadena de seguridad es el usuario final. De esta premisa se valen los diferentes tipos de ataque de Ingeniería Social, cuyo objetivo principal es obtener información casi directamente de los usuarios, con la finalidad de usar esta información en contra de ellos mismos (Benavides, Fuertes, & Sanchez, 2020).

Los principales ataques cibernéticos son:

Ataque de tipo phishing: Según (Bernal, Lizárraga, Pinedo, Flores, & Flores , 2019) , "El Phishing es una técnica de ingeniería social utilizada por los delincuentes, conocidos como Phishers para obtener información confidencial como nombres de usuario, contraseñas e información de tarjetas de crédito haciéndose pasar por una comunicación confiable y legítima".

Los usuarios de las aplicaciones móviles podrían estar exhibidos a ataques de phishing mediante el acceso a enlaces maliciosos que suelen ser enviados por correo electrónico, mensajes de texto o en aplicaciones de mensajería instantánea. Dichos enlaces suelen redirigir al usuario a un sitio web falso que plagia la apariencia del sitio web legítimo, con el fin de engañar al usuario para que suministre información personal.

Por esto, es primordial que los usuarios de apps sean conscientes de las posibilidades que existe de ser atacados mediante phishing y estén alerta a cualquier mensaje o solicitud que les genere sospecha que reciban a través de sus dispositivos móviles. Es favorable que los usuarios verifiquen siempre la autenticidad de cualquier solicitud antes de brindar información personal o credenciales de inicio de sesión, y que solo descarguen aplicaciones móviles de fuentes confiables y legítimas.

Ataques de inyección de código: En la actualidad el uso de aplicaciones web sea ha vuelto algo cotidiano, al igual que varias amenazas que se presentan al usar estas aplicaciones, entre las cuales están los ataques de inyección de código principalmente la inyección de código SQL (SQLI por sus siglas en ingles), que consiste en ingresar sentencias SQL a través de los medios por los cuales el usuario envía datos al servidor (Ej. formulario) para acceder a la base de datos (Chicaiza, 2022).

De manera similar a las aplicaciones web, las aplicaciones móviles también suelen ser susceptibles a ataques de inyección de código. Este tipo de ataque se produce cuando un atacante introduce código dañino en una aplicación móvil a través de una entrada de datos, como un formulario de inicio de sesión o una búsqueda de información.

Ataques de fuerza bruta: Según (Larenas & Rosero, 2020), "Un ataque de fuerza bruta es la forma de recuperar una clave probando todas las combinaciones posibles hasta encontrar aquella que permite el acceso". Este es un método de hacking muy usado para poder obtener acceso no autorizado.

Esta clase de ataque logra ser muy efectivo si tiene contraseñas débiles o predecibles, y se podría realizar utilizando algún software especializado que automatiza el proceso de adivinación de contraseñas.

No obstante, los sistemas de seguridad tienen la posibilidad de protegerse contra esta clase de ataques a través del uso de contraseñas complejas, establecer una limitación del número de intentos de inicio de sesión, la implementación de mecanismos de bloqueo de cuentas, entre otros.

Estos ataques son utilizados por hackers para tener acceso a cuentas bancarias, correos electrónicos, redes sociales, etc., lo que resulta en robo de datos personales,

financieros y empresariales. Por eso, es de suma importancia que los usuarios establezcan contraseñas seguras y cambien con frecuencia sus contraseñas para protegerse contra este tipo de ataques.

Hackers

Las personas que se conocen como hackers tienen habilidades avanzadas en el uso de la tecnología informática. Su objetivo es buscar debilidades en sistemas, redes y aplicaciones, y explotarlas para diversos fines, como el robo de información, espionaje o fraude, entre otros.

En particular, en el caso de las aplicaciones móviles, los hackers pueden causar daño de varias formas, como el uso de malware para infectar el dispositivo móvil del usuario y robar información confidencial de las aplicaciones instaladas, o mediante técnicas de ingeniería inversa para encontrar vulnerabilidades en el código fuente de la aplicación que puedan ser explotadas para acceder a datos sensibles.

En general, los hackers pueden causar graves problemas a las aplicaciones móviles y a los usuarios que las utilizan, por lo que es importante que los desarrolladores de aplicaciones y los usuarios tomen medidas de seguridad para protegerse de posibles ataques. Existen diferentes tipos de hackers, los cuales son:

Hacker ético: El hacking ético es considerado por una persona capaz de comprobar si existe la vulnerabilidad y se encarga de la seguridad en la empresa en sus datos, para después de un análisis adecuado poder presentar un informe de como está la seguridad de la empresa y así poder revelar si existe algún fallo de seguridad y poder llegar a una solución rápida sin que afecte a la institución y evitando que la información de la empresa sea atacada por personas mal intencionadas (Leon & Leon, 2021).

Hacker malicioso: Conocido también como “sombrero negro” estos son los que se encargan de robar información a las apps móviles, existen técnicas que estos hackers pueden utilizar para obtener información de aplicaciones móviles. Por ejemplo, pueden infectar un dispositivo móvil con un software malicioso que les permita robar información de las aplicaciones instaladas. También pueden emplear técnicas de ingeniería inversa para desmontar la aplicación y buscar vulnerabilidades que puedan explotar para acceder a información protegida.

Hacker sombrero gris: Los hackers de sombrero gris son hackers que no se dedican exclusivamente a actividades legales o ilegales. Por un lado, emplean sus habilidades de hacking para encontrar fallas en sistemas y redes, pero sin intención de causar daño duradero o violar la ley. Estos hackers pueden trabajar solos o en equipo, y a menudo informan a las empresas o propietarios de sistemas sobre las debilidades que han descubierto para que puedan ser solucionadas.

Además, algunos hackers de sombrero gris ofrecen sus servicios a empresas y organizaciones para hacer pruebas de penetración y evaluar la seguridad de sus sistemas. En resumen, los hackers de sombrero gris se encuentran en una zona intermedia entre la ética y la ilegalidad, ya que buscan un equilibrio entre su pasión por la tecnología y el cumplimiento de la ley.

MARCO METODOLÓGICO

METODOLOGÍA

MÉTODOS DE INVESTIGACIÓN

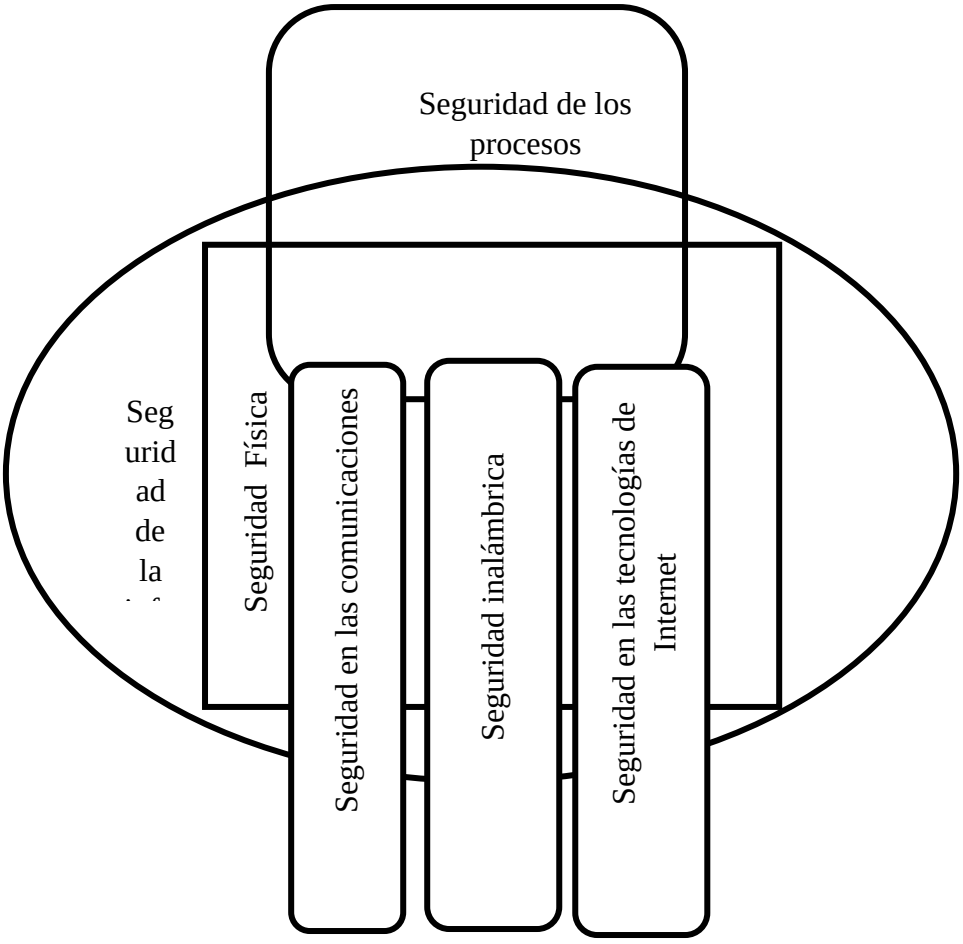
Para la elaboración de este caso de estudio se utilizaron diversos métodos de investigación científica durante las diferentes fases del desarrollo del trabajo de titulación, cuya aplicación se resume en la Tabla 1.

Tabla 1. Resumen de métodos de investigación

MÉTODOS DE INVESTIGACIÓN		APLICACIÓN	FASE DE LA INVESTIGACIÓN
Teóricos	Inductivo	• Formulación del problema a ser resuelto	Planteamiento del problema
	Deductivo	En el análisis de una metodología de seguridad informática para el desarrollo de aplicaciones móviles	Metodología
	Analítico Sintético	• Selección de las fuentes de información y elaboración de contenidos sistematizados	Marco Teórico
Empíricos	Experimentación	• Utilización de una metodología de seguridad informática para el desarrollo de aplicaciones móviles	Análisis de Resultados

METODOLOGÍA OSSTMM

Para el análisis de una metodología de seguridad informática para el desarrollo de aplicaciones móviles usando herramientas open source se utilizó la metodología OSSTMM, que se encuentra determinado por módulos como son la Seguridad de la Información (sección A), Seguridad de los Procesos (sección B), Seguridad en las tecnologías de Internet (sección C), Seguridad en las Comunicaciones (sección D), Seguridad Inalámbrica (sección E) y Seguridad Física (sección F).



A. Seguridad de la Información.

Esta fase se encuentra relacionada con la investigación de inteligencia competitiva, de privacidad y recolección de información.

B. Seguridad de los Procesos.

La seguridad de procesos se manifiesta sobre testeo de datos, seguridad y de personas, mediante preguntas utilizando diversos métodos, entre el que sobresale el uso de la ingeniería social.

C. **Seguridad en las Tecnologías de Internet**.

Se realiza un monitoreo integral de la red para establecer los servicios de los distintos sistemas, efectuando testeos de aplicaciones en la web, localización de intrusos y DoS en busca de vulnerabilidades que luego de descubrirlas, se proceda a generar una posible solución.

D. Seguridad en las Comunicaciones.

Se realiza ensayos en los emisores-receptores de datos de comunicación tales como: Central telefónica, PBX, Correo de voz, con la finalidad de encontrar posibles vulnerabilidades.

E. Seguridad Inalámbrica.

Se encarga de examinar el ámbito inalámbrico para lo cual efectúa la verificación de redes inalámbricas.

F. Seguridad Física.

Se enfoca en realizar la investigación de perímetro, reconocimiento de controles de acceso, análisis de ubicación.

Para este estudio de caso se utilizó la sección C la cual se encuentra relacionado al modulo de software, el mismo que nos permitirá ejecutar un análisis adecuado, con respecto a la seguridad informática para el desarrollo de aplicaciones moviles usando herramientas open source

RESULTADOS

Para establecer los resultados del estudio de caso lo hemos dividido en dos partes la primera relacionada a la obtención del conocimiento existente sobre la metodología de seguridad informática para el desarrollo de aplicaciones móviles usando herramientas open source. Por lo cual se procedió a realizar entrevistas y encuestas a personas con conocimiento en informática, como se demuestra en el Anexos 1, 2 y 3.

La segunda parte se realizó con el uso de una herramienta Open Source que nos permitirá determinar la seguridad informática para el desarrollo de aplicaciones móviles.

MobSF

Mobile Security Framework es un instrumento para automatizar los análisis estáticos y dinámicos de las aplicaciones para malware o pruebas de seguridad. Se encuentra formada por una plataforma establecida en un local server, en la que se sube el archivo apk para ser examinado. De acuerdo del tamaño es el tiempo de respuesta para la generación del reporte con el detalle de análisis estático del código de la aplicación determinando las vulnerabilidades, riesgo y la información de cada una de ellas.

Análisis estático

El análisis estático o también llamado código estático o SAST por sus siglas en inglés *Static Application Security Testing*, involucra la búsqueda de la seguridad de una app a

partir del código fuente, examinando los diferentes mecanismos de ésta, ya sea de manera manual o automática.

La herramienta se utiliza para realizar análisis de archivos ejecutables de Android (APK), iOS (IPA) o incluso Windows Mobile (APPX), así como también código fuente empaquetado en formato ZIP. A partir de su interfaz web, podemos subir la app a analizar y conseguir la información del archivo, como puede ser el nombre del paquete, tamaño, actividad principal, hashes, SDK de compilación, etc.

Análisis dinámico

El análisis dinámico, también conocido como DAST de *Dynamic Application Security Testing*, implica la evaluación de la app durante su ejecución para asegurar la calidad y seguridad de la aplicación durante este proceso en tiempo real**.** Se trata de un buen complemento al análisis estático pues proporciona información con relación a los recursos, las características de la app, los puntos de entrada, etc. desde el punto de vista del usuario.

El análisis dinámico nos va a permitir detectar vulnerabilidades que serían difíciles de identificar si solo llevásemos a cabo un análisis estático. El informe de análisis dinámico contendrá información útil de la app como la enumerada a continuación:

- archivos accedidos por la app durante la ejecución, apertura de puertos y gestión de conexiones de red.
- información del dispositivo a la que accedió la app durante la ejecución (como

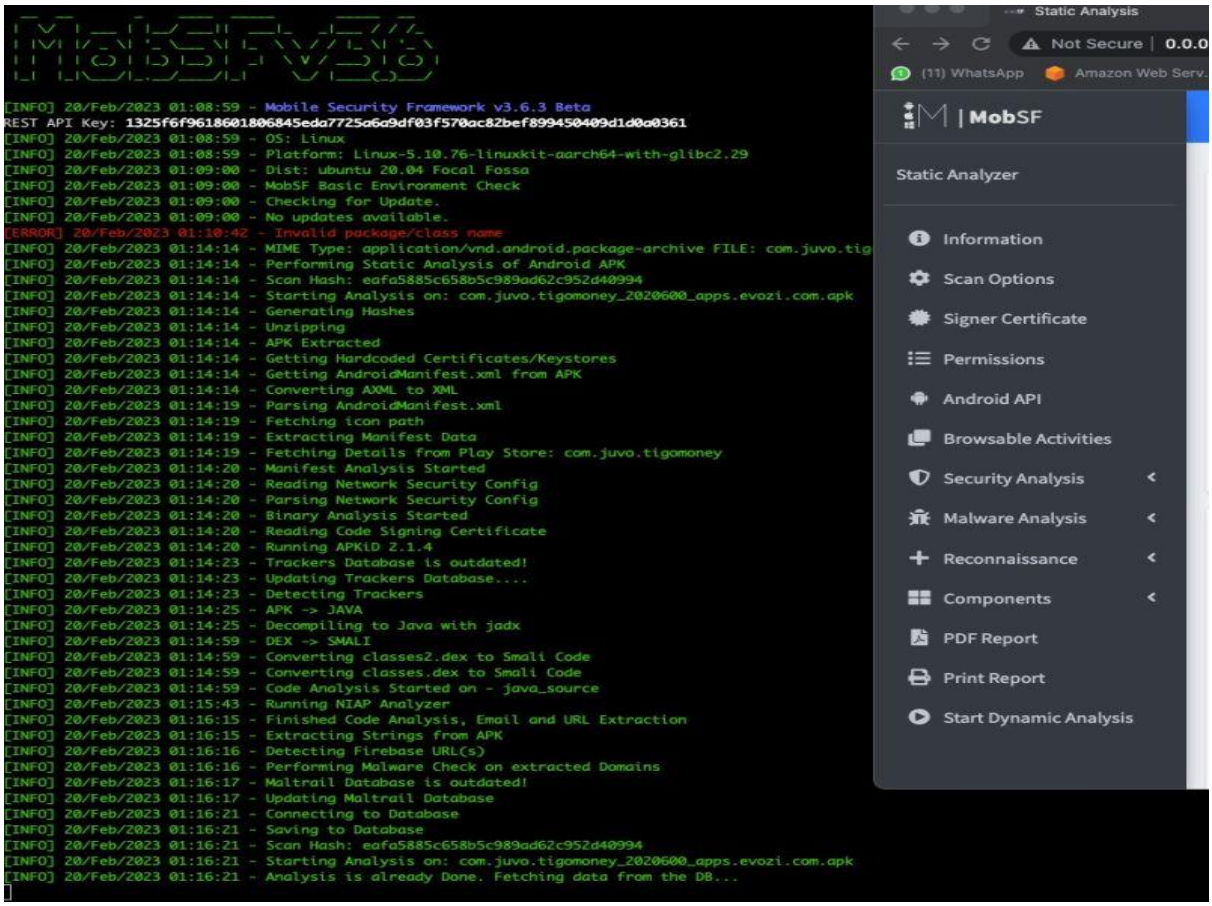


Imagen xixi: pantalla principal de **MobSF**

Imagen xixi: Detalle del resultado del análisis estático de la app

Imagen xixi: Detalle del resultado del análisis estático de la app

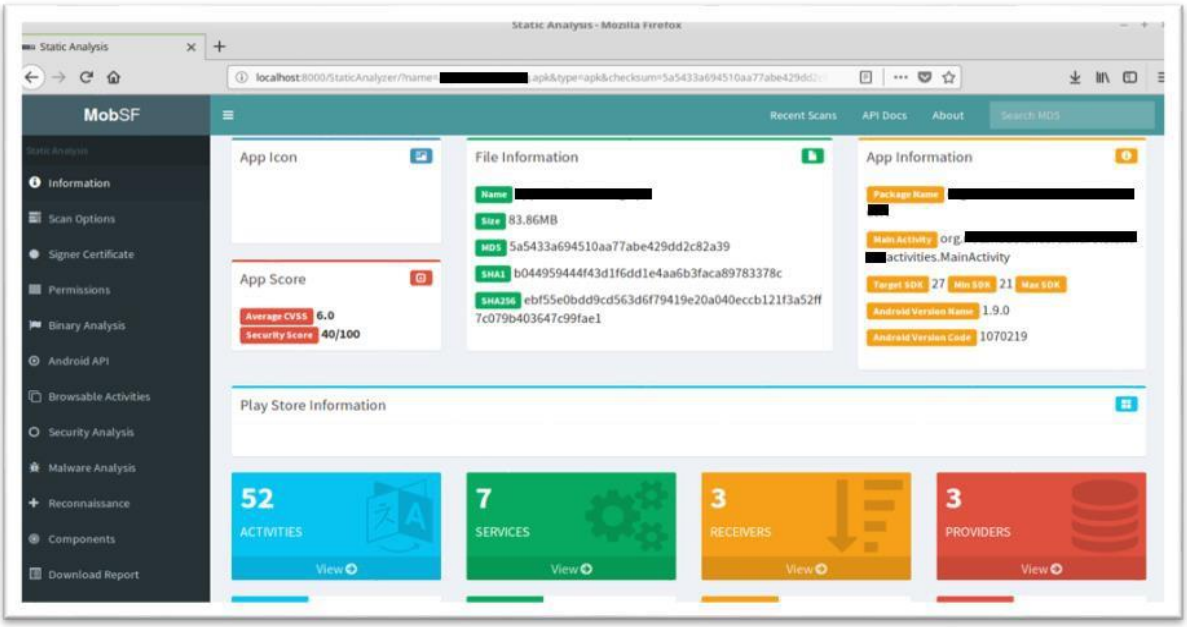


Imagen xxxx: Resultado del análisis estático de la app

El resultado del análisis también nos proporciona acceso desde su interfaz a las clases

PERMISOS	DESCRIPCIÓN	VULNERABILIDAD
android.permission.READ_PHONE STATE	Permite que la aplicación acceda a las funciones del dispositivo.	**Alto**
(android.permission.ACCESS_WIFI_ STATE	Permite que una aplicación vea la información sobre el estado de Wifi.	**Bajo**
android.permission.WAKE_LOCK	Permite que una aplicación impida que el teléfono se bloquee.	**Alto**
android.permission.ACCESS_NETW ORK_STATE	Permite que una aplicación vea el estado de todas las redes.	**Bajo**
android.permission.INTERNET	Permite que una aplicación cree	**Alto**
mobile.permission.C2D_MESSAGE	Permite que la aplicación reciba	**Firma de la aplicación**
android.permission.WRITE_EXTER NAL_STORAGE	Permite que una aplicación	**Alto**
android.permission.WRITE_CONTACTS	Permite que una aplicación acceda a la lista de contactos del teléfono.	**Alto**
android.permission.CAMERA	Permite que una aplicación	**Alto**
android.permission.ACCESS_FINE_LOCATION	Permite que una aplicación	**Alto**

java de la aplicación, así como al archivo *manifest* de ésta.

INFORME DE ANALISIS DE LOS PERMISOS DEL DISPOSITIVO

Se detectan los siguientes permisos peligrosos:

INFORME DE RESULTADOS DE ANALISIS DEL ARCHIVO

MANIFEST

Se detectan las siguientes vulnerabilidades en el archivo Manifest de la app:

Vulnerabilidad	Severidad
Debug habilitado para la app [android:debuggable=true]	**Alta**
Puede realizarse *back up* de los datos de la app [android:allowBackup=true]	**Media**
TaskAffinity activado para una Actividad: (SignatureEnrollActivity)	**Alta**
TaskAffinity activado para una Actividad: (org.xxxx.xxxx.android.xxxx.happ.scenes.signature.recover.SignatureRecoverActivity)	**Alta**
TaskAffinity activado para una Actividad: (org.xxxx.xxxx.android.xxxx.happ.scenes.signature.config.SignaturConfigChangePinActivity)	**Alta**
TaskAffinity activado para una Actividad: (org.xxxxx.xxxxx.android.xxxxxx.happ.scenes.signature.config.SignatureConfigCertificateRecoverActivity)	**Alta**
TaskAffinity activado para una Actividad: (org.xxxxx.xxxxx.android.xxxxx.happ.scenes.signature.config.SignatureConfigCertificateRecoverPinActivity)	**Alta**
Servicio no protegido (FirebaseMessagingService) [android:exported=true]	**Alta**
Receptor Broadcast protegido por un permiso cuyo nivel de protección ha de verificarse: (AppMeasurementInstallReferrerReceiver) Permiso: android.permission.INSTALL_PACKAGES [android:exported=true]	**Alta**
Receptor Broadcast protegido por un permiso cuyo nivel de protección ha de verificarse: (FirebaseInstanceIdReceiver) Permiso: com.google.android.c2dm.permission.SEND [android:exported=true]	**Alta**
Servicio no protegido (com.google.firebase.iid.FirebaseInstanceIdService) [android:exported=true]	**Alta**

INFORME DE RESULTADOS DE ANALISIS DEL CÓDIGO FUENTE

El análisis detecta los siguientes problemas en relación con algunos de los archivos .java que componen la app:

Problema	Severidad	CV
La app almacena en logs información sensible	Info	7.5
La app usa Java Hash Code, una función débil que no debería emplearse en implementaciones criptográficas de seguridad	High	4.3
La app emplea un generador de números aleatorios no seguro	High	7.5
Algunos archivos contienen información sensible *harcodeada* como nombres de usuario, *passwords*,	High	7.4
La app puede leer y escribir en el almacenamiento externo por lo que cualquier dato escrito podría ser asimismo leído por otras apps.	High	5.5
La app crea archivos temporales. La información sensible no debe ser conservada en tales archivos.	High	5.5
La app podría disponer de capacidades de detección de root.	Secure	0
Revelación de direcciones IP	Warning	4

*CVSS sistema de puntaje diseñado para proveer un método abierto y estándar que permite estimar el impacto derivado de vulnerabilidades identificadas en Tecnologías de Información

DISCUSIÓN DE RESULTADOS

De acuerdo con el análisis de la app de estudio realizado mediante la herramienta open source MobSF, alcanzamos enfatizar los siguientes resultados.

- El análisis se lo efectúo en un dispositivo con una versión de Android de API 27 (Android 8.1). La misma que se encuentra conformada por 52 Actividades, 7 servicios de los cuales 2 están exportados, 3 receptores de los cuales 2 están igualmente exportados y 3 proveedores de contenidos.
- La depuración está habilitada para la aplicación lo cual admite el acceso al asistente de depuración de clases.
- Está autorizada la posibilidad de efectuar back up de los datos de la app lo cual aprueba efectuar Backus vía daba, así como la copia de datos externamente con el uso de la depuración por USB.
- Se divisan algunas acciones con taskAffinity activado, por lo cual otras aplicaciones podrían acceder a la información de los Intents enviados a actividades referentes a otra tarea.
- Se manifiestan 2 servicios no preservados para ser compartidos con otras aplicaciones, por lo cual, quedan disponible a cualquier otra aplicación dentro del dispositivo.
- Se localizan 2 receptores broadcast resguardados por un permiso el cual no está definido en la app para ser compartidos con otras. Cualquier app maliciosa podría requerir y conseguir el permiso para interactuar con el módulo, por tal motivo se pide configurarlo a nivel firma para forzar el solo uso de las solicitudes firmadas con el mismo certificado.

- Nos encontramos con que la app emplea conexiones seguras HTTPS en todas sus comunicaciones por lo que tenemos que instalar en el dispositivo el Certificado de confianza.

- Se pudo establecer que la app efectúa el denominado Certificate o SSL Pinning, proceso en el cual se evidencia no solo que el certificado enviado por el servidor sea permitido, sino también que sea el certificado del servidor correcto para optimizar notablemente la seguridad.

CONCLUSIONES

Es fundamental identificar los procesos metodológicos relacionados con la seguridad informática en el desarrollo de aplicaciones móviles para garantizar su seguridad. El seguimiento de una metodología específica permite abordar de manera sistemática y completa los distintos aspectos relacionados con la seguridad informática, como la detección de vulnerabilidades, la gestión de riesgos, la implementación de controles de seguridad y la realización de pruebas de penetración.

Conociendo de manera teórica y fundamentada los aportes de la metodología seguridad informática para el desarrollo de aplicaciones móviles se estableció que esto es esencial para el desarrollo de aplicaciones móviles seguras. Por lo tanto, esto es una necesidad para cualquier equipo de desarrollo de aplicaciones móviles que busque construir aplicaciones seguras y confiables.

Al establecer las estrategias de la metodología de seguridad informática (OSSTMM), permite garantizar el éxito del desarrollo de aplicaciones móviles seguras y confiables utilizando herramientas open source porque al aplicar las estrategias adecuadas, los desarrolladores pueden implementar medidas preventivas y correctivas para mitigar los riesgos de seguridad en todas las fases del ciclo de vida de la aplicación móvil.

RECOMENDACIONES

La utilización de procesos metodológicos de seguridad informática idóneos para el desarrollo de aplicaciones móviles contribuye a garantizar una mayor seguridad en el uso de las mismas.

Es recomendable conocer más acerca los aportes de la metodología seguridad informática 0SSTMM, porque es esencial en el desarrollo de apps movile, mucha de esta información se la puede encontrar en libros, cursos en línea, seminarios web y conferencias relacionadas con la seguridad informática y el desarrollo de aplicaciones móviles.

Existe un sinnúmero de metodologías de seguridad informática al elegir una, es importante considerar factores como el tipo de datos que se manejan, el nivel de sensibilidad de la información, las posibles amenazas y vulnerabilidades, el costo y el tiempo de implementación. Además, es crucial contar con un equipo de profesionales en seguridad informática capacitados para implementar adecuadamente la metodología elegida y mantener la seguridad de las aplicaciones móviles a lo largo del tiempo.

REFERENCIAS

Referencias

Alvarado, J. (2020). ANÁLISIS DE ATAQUES CIBERNÉTICOS HACIA EL ECUADOR. *Aristas*, 18.

Benavides, E., Fuertes, W., & Sanchez, S. (2020). Caracterización de los ataques de phishing y técnicas para mitigarlos. Ataques: una. *Ciencia y Tecnología*, 97-104.

Bernal, M., Lizárraga, J., Pinedo, J., Flores, A., & Flores , E. (2019). PROTOCOLO PARA LA PREVENCIÓN DE ATAQUES DE PHISHING. *ReDTIS*, 34-51.

CAIHUARA, F. (2019). APLICACIONES WEB PROGRESIVAS. *CIENCIA SUR*, 61-67.

Chicaiza, C. (2022). *Repositorio Digital - EPN* . Obtenido de https://bibdigital.epn.edu.ec/bitstream/15000/22910/1/CD%2012366.pdf

Contreras, J., Peña, O., & Santillan, G. (2019). APLICACIONES HÍBRIDAS PARA DISPOSITIVOS MÓVILES. *CIENCIA ADMINISTRATIVA* , 146-152.

Guevara Aulestia, D. O., & Quirola Valarezo, L. M. (2019). *Repositorio Universidad Técnica de Ambato.* Obtenido de https://repositorio.uta.edu.ec/jspui/handle/123456789/30108

Larenas, J., & Rosero, A. (2020). Medusa herramienta para realizar ataques de fuerza bruta . *NEXOS CIENTÍFICOS* , 27–31.

Leon, M., & Leon, P. (2021). Hacking ético en el sector financiero. *Revista Académica-Investigativa De La Facultad Jurídica, Social Y Administrativa*, 83–89.

Lopez, S., & Garcia, V. (2021). Metodologías de desarrollo de software seguro con propiedades agiles. *Polo del Conocimiento*, 1027-1046.

Muñoz, H., & Vasco, D. (2022). Aportes para el desarrollo de aplicaciones móviles híbridas articuladas a estrategias de gamificación. *Lumen Gentium*, 56-74.

Muñoz, H., Zapata, L., Requena, D., & Ricardo, L. (2019). Riesgos informáticos y alternativas para la seguridad informática en sistemas contables en Colombia. *Revista venezolana de gerencia*, 528-541.

Ortiz, A. (31 de Enero de 2020). *Repositorio Institucional*. Obtenido de http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/6863/Introducci%c3%b3n%20a%20las%20pruebas%20de%20penetraci%c3%b3n..pdf?sequence=1&isAllowed=y

Ovallos, J., Rico, D., & Medina, Y. (2020). Guía práctica para el análisis de vulnerabilidades de un entorno cliente-servidor GNU/Linux mediante una metodología de pentesting. *Revista Ibérica de Sistemas e Tecnologias de Informação*, 335-350.

Puetate, G., & Ibarra, J. (2020). *Aplicaciones Moviles Hibridas* . Centro de publicaciones PUCE.

ANEXOS

ANEXO 1

UNIVERSIDAD TECNICA DE BABAHOYO

FACULTAD DE ADMINISTRACION FINANZAS E INFORMATICA

CUESTIONARIO

INTRUCCIONES

Por favor, elija la opción que considere apropiada.

1. ¿Cree usted que es importante que las aplicaciones móviles sean seguras desde el punto de vista informático?

   Si () no () tal vez ()

2. ¿Ha utilizado alguna vez una herramienta Open Source para analizar la seguridad de una aplicación móvil?

   Si () no () tal vez ()

3. ¿Cree usted que la metodología OSSTMM puede ser de utilidad para el análisis de seguridad informática en aplicaciones móviles?

   Si () no () tal vez ()

4. ¿Le gustaría conocer más sobre la metodología OSSTMM y las herramientas Open Source para el análisis de seguridad informática en aplicaciones móviles?

   Si () no () tal vez ()

5. ¿Considera usted que los desarrolladores de aplicaciones móviles deberían recibir capacitación en seguridad informática para garantizar la protección de los datos de los usuarios?

   Si () no () tal vez ()

ANEXO 2

Tabulación de las encuestas

PREGUNTA 1

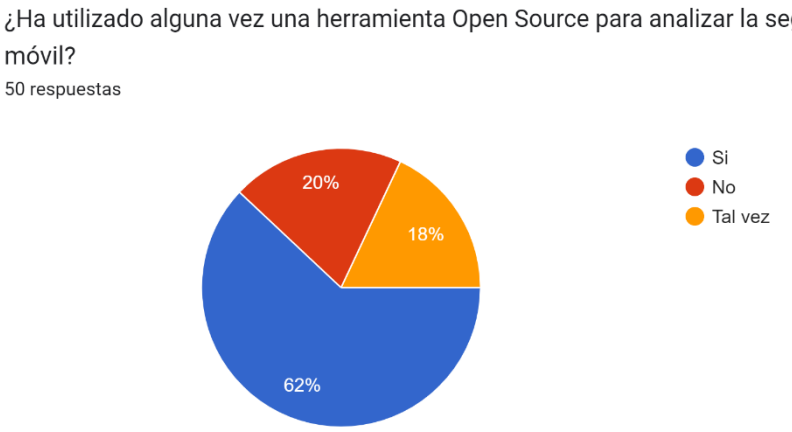
ANÁLISIS:

De los estudiantes encuestados el 66% indica que, si es importante que las aplicaciones móviles sean seguras desde el punto de vista informático, mientras que hay otro 14% indicando que no es importante, finalmente terminamos con un 20% indicando un tal vez es importante.

INTERPRETACIÓN:

Es alarmante que un 14% de los estudiantes expresen que la seguridad informática en las aplicaciones móviles no tiene importancia, lo que indica que estos estudiantes podrían no estar conscientes de los riesgos que existen en el uso de aplicaciones móviles no seguras.

PREGUNTA 2



ANÁLISIS:

De los estudiantes encuestados el 62% indica que, si ha utilizado alguna vez una herramienta Open Source para analizar la seguridad de una aplicación móvil, mientras que hay otro 20% indicando que no ha utilizado, finalmente terminamos con un 18% indicando un tal vez ha utilizado.

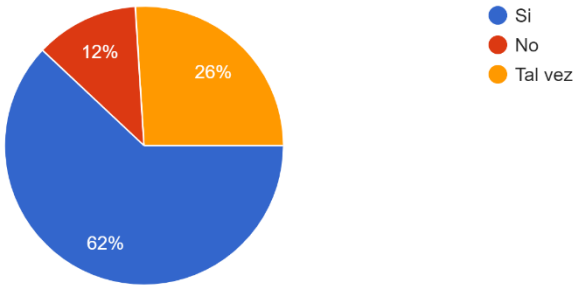
INTERPRETACIÓN:

Estos resultados indican que, aunque una gran cantidad de estudiantes ha utilizado herramientas de seguridad Open Source para analizar aplicaciones móviles, aún hay estudiantes que no conocen sobre la importancia de estas herramientas y cómo pueden utilizarse para mejorar la seguridad de las aplicaciones móviles.

PREGUNTA 3

¿Cree usted que la metodología OSSTMM puede ser de utilidad para el análisis de seguridad informática en aplicaciones móviles?

50 respuestas



ANÁLISIS:

De los estudiantes encuestados el 62% cree que la metodología OSSTMM puede ser de utilidad para el análisis de seguridad informática en aplicaciones móviles, mientras que hay otro 12% no cree esto, finalmente terminamos con un 26% cree que tal vez esta metodología puede ser de utilidad.

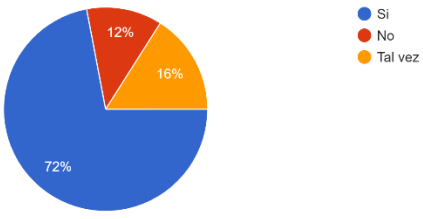
INTERPRETACIÓN:

La interpretación de los resultados indica que la mayoría de los estudiantes considera que la metodología OSSTMM es una herramienta útil para analizar la seguridad informática en aplicaciones móviles.

PREGUNTA 4

¿Le gustaría conocer más sobre la metodología OSSTMM y las herramientas Open Source para el análisis de seguridad informática en aplicaciones móviles?

50 respuestas



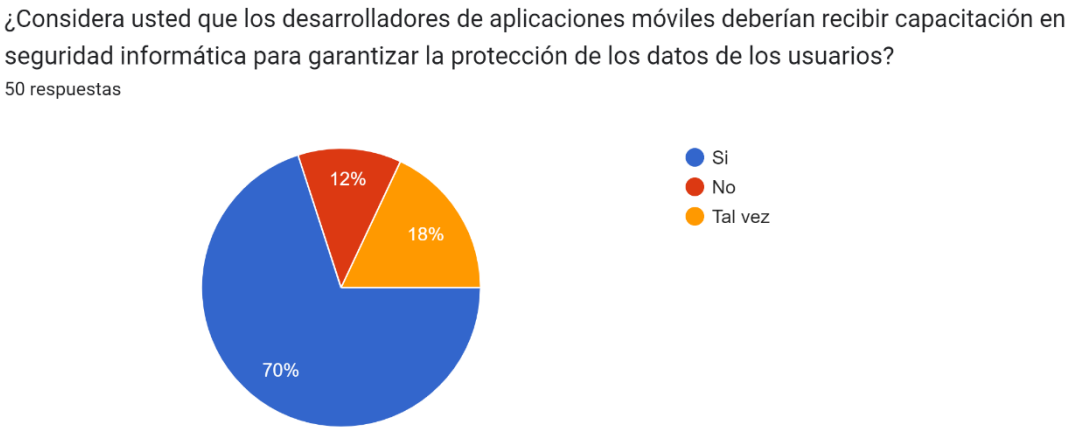
ANÁLISIS:

De los estudiantes encuestados el 72% indica que le gustaría conocer más sobre la metodología OSSTMM y las herramientas Open Source para el análisis de seguridad informática en aplicaciones móviles, mientras que hay otro 12% indicando que no le gustaría conocer, finalmente terminamos con un 16% indicando un tal vez le gustaría conocer.

INTERPRETACIÓN:

Estos resultados indican que la mayoría de los estudiantes tiene un interés en adquirir más conocimientos sobre la metodología OSSTMM y las herramientas Open Source utilizadas para el análisis de seguridad informática en aplicaciones móviles. Esta actitud positiva sugiere un deseo por mejorar la seguridad informática, así como una disposición para desarrollar habilidades y conocimientos en este campo.

PREGUNTA 5



ANÁLISIS:

De los estudiantes encuestados el 70% indica que, si considera que los desarrolladores de aplicaciones móviles deberían recibir capacitación en seguridad informática para garantizar la protección de los datos de los usuarios,

mientras que hay otro 12% indicando que no lo considera necesario, finalmente terminamos con un 18% indicando un tal vez sea necesario.

INTERPRETACIÓN:

Los resultados de la encuesta indican que la mayoría de los estudiantes que participaron en ella comprenden la importancia de la seguridad informática en las aplicaciones móviles. Además, estos estudiantes piensan que es necesario que los desarrolladores de aplicaciones móviles reciban capacitación en este tema para asegurar que los datos de los usuarios estén protegidos.

ANEXO 3

Entrevista realizada al Ing. Harry Saltos Viteri docente de la Universidad Técnica de Babahoyo

1. **¿Conoce usted qué es OSSTMM y cómo se relaciona con la seguridad informática en el desarrollo de aplicaciones móviles?**

Es un marco de trabajo de pruebas de seguridad diseñado para evaluar la seguridad de los sistemas de información, incluyendo aplicaciones móviles. Fue desarrollado por el Instituto de Seguridad de la Información de Pruebas Abiertas (ISECOM) y se enfoca en proporcionar un enfoque estructurado y detallado para la realización de pruebas de seguridad.

La metodología OSSTMM cubre diversos aspectos de la seguridad informática, desde la identificación de vulnerabilidades hasta la evaluación de riesgos y la implementación de controles de seguridad. También proporciona una serie de herramientas y técnicas para llevar a cabo pruebas de seguridad de manera efectiva.

En lo que respecta a App móviles, OSSTMM ofrece una guía para evaluar la seguridad de estas en todas sus fases de su ciclo de vida, incluyendo el diseño, desarrollo, pruebas y mantenimiento. Esto incluye la identificación de vulnerabilidades comunes en aplicaciones móviles, como la falta de autenticación adecuada, la exposición de datos sensibles y la ejecución de código malicioso.

Esto permite pruebas de seguridad muy útiles para los desarrolladores de aplicaciones móviles, ya que proporciona una estructura detallada y herramientas específicas para evaluar la seguridad de sus aplicaciones en todas las fases de su ciclo de vida. Con su ayuda, los desarrolladores pueden asegurarse de que sus

aplicaciones móviles sean seguras y protejan los datos de sus usuarios de manera efectiva

2. **¿Cuáles son las herramientas Open Source recomendadas para el análisis de seguridad informática de aplicaciones móviles con OSSTMM?**

   Existen varias herramientas de seguridad Open Source que se pueden utilizar para el análisis de seguridad de aplicaciones móviles siguiendo el marco OSSTMM, La elección de una herramienta dependerá del tipo de análisis que se quiera realizar y del nivel de experiencia del usuario en su uso.

   MobSF: Una plataforma de pruebas de seguridad automatizada para aplicaciones móviles, que permite la realización de análisis de vulnerabilidades y pruebas de penetración de manera sistemática.

   AndroBugs: Una herramienta de análisis estático para aplicaciones Android que permite identificar vulnerabilidades de seguridad en el código fuente

   Frida: Es Un framework de inyección de código que permite realizar análisis dinámico de aplicaciones móviles en tiempo de ejecución

   OWASP ZAP: Es Una herramienta de pruebas de seguridad automatizada de código abierto que permite la identificación de vulnerabilidades en aplicaciones móviles y web.

3. **¿Cómo se puede evaluar el cumplimiento de los estándares OSSTMM en el desarrollo de aplicaciones móviles?**

   Teniendo en cuanta toda una estrategia de seguimiento de las normativas de desarrollo internas de la organización

4. **¿Qué beneficios ofrece el uso de OSSTMM en el desarrollo de aplicaciones móviles frente a otras metodologías de seguridad informática?**

Beneficios de Reducción de las vulnerabilidades y fallos posteriores; sobre todo la garantía y seguridad de uso de App.

5. **¿Cómo se integra la metodología OSSTMM con el proceso de desarrollo de aplicaciones móviles y cuál es su impacto en la calidad de las mismas?**

Durante la fase de diseño: OSSTMM puede utilizarse para identificar los requisitos de seguridad necesarios para la aplicación móvil y para definir las especificaciones de seguridad que deben cumplirse durante el desarrollo.

Durante la fase de desarrollo: OSSTMM puede utilizarse para realizar pruebas de seguridad de código en la aplicación móvil y para garantizar que se sigan las mejores prácticas de seguridad durante el proceso de desarrollo.

Durante la fase de pruebas: OSSTMM puede utilizarse para realizar pruebas de penetración y otros tipos de pruebas de seguridad en la aplicación móvil antes de su lanzamiento.

Durante la fase de mantenimiento: OSSTMM puede utilizarse para realizar pruebas periódicas de seguridad en la aplicación móvil para garantizar que siga siendo segura a medida que se realizan actualizaciones y se agregan nuevas funciones.

El impacto de la integración de OSSTMM en el proceso de desarrollo de aplicaciones móviles puede ser significativo. Al incluir pruebas de seguridad en todas las fases del ciclo de vida de desarrollo, se pueden detectar y corregir vulnerabilidades de seguridad antes de que la aplicación este en ambiente de producción