

1. **PARTE I**

| **1. Antecedentes Personales** |
| --- |
| A continuación, se presenta una tabla en la que debes completar la información solicitada. |

| Nombre estudiante | **Sebastian Acevedo** |
| --- | --- |
| Rut | **19.442.989-4** |
| Carrera | **Ing. en Informatica** |
| Sede | **San Joaquín** |

| Nombre estudiante | **Maximiliano Einer Hilmer Hernández** |
| --- | --- |
| Rut | **16.959.571-2** |
| Carrera | **Ing. en Informatica** |
| Sede | **San Joaquín** |

| Nombre estudiante | **Benjamin Ramirez** |
| --- | --- |
| Rut | **20.793.545-k** |
| Carrera | **Ing. en Informatica** |
| Sede | **San Joaquín** |

| Nombre estudiante | **Jose Valdebenito** |
| --- | --- |
| Rut | **19.114.584-4** |
| Carrera | **Ing. en Informatica** |
| Sede | **San Joaquín** |

| **2. Descripción Proyecto APT** |
| --- |
| Es una herramienta de automatización para detectar y mitigar riesgos en el desarrollo de software. Permite analizar flujos web, identificar fallos de seguridad y generar informes detallados a partir de scripts de JMeter. |

| Nombre del proyecto | ***RobotPentester*** |
| --- | --- |
| Área (s) de desempeño(s) | *Ciberseguridad, control de calidad y automatizaciones de procesos.* |
| Competencias | *Análisis y planificación de requerimientos informáticos, calidad de software, gestión de proyectos informaticos, programacion de software, arquitectura de software* |

| **3. Fundamentación Proyecto APT** |
| --- |
| A continuación, se presentan distintos campos que debes completar con la información solicitada. Esta sección busca que describas en detalle tu proyecto y justifiques su relevancia y pertinencia. |

| Relevancia del proyecto APT | ***Análisis de Ciberseguridad Automatizado:***  *Implementa pruebas de ciberseguridad en todas las etapas del desarrollo.*  *Asegura una evaluación continua y sistemática.*  ***Mayor Cobertura de Vulnerabilidades:***  *Amplía el alcance de las pruebas para incluir tanto el frontend como el backend.*  *Identifica una gama más amplia de posibles vulnerabilidades.*  ***Integración con Herramientas de Ciberseguridad:***  *Utiliza diversas herramientas como OWASP ZAP, Metasploit, entre otras.*  *Mejora la detección y mitigación de vulnerabilidades.*  ***Informes y Accionables:***  *Genera informes de seguridad detallados.*  *Proporciona insights claros y accionables para los equipos de desarrollo.*  ***Fomento de la Cultura de Ciberseguridad a través de I+D:***  *Colabora en la investigación y desarrollo utilizando herramientas de código abierto.*  *Contribuye a una cultura de ciberseguridad proactiva y robusta en toda la organización.* |
| --- | --- |
| Descripción del Proyecto APT | *Esperamos crear un sistema que permita probar los desarrollos antes de su puesta en producción, lo cual mejorará los tiempos y reducirá los costos. Este sistema generará un reporte con las fallas o vulnerabilidades detectadas, en un proceso que podría completarse en sólo unas pocas horas. Evitando de esta forma recurrir a costosas pruebas realizadas por empresas externas.* |
| Pertinencia del proyecto con el perfil de egreso | ***Levantamiento y Análisis de Requerimientos:***  *RobotPentester requiere un análisis detallado de los requisitos de seguridad en el desarrollo de software, lo cual es una competencia clave del perfil de egreso.*  ***Desarrollo, Adaptación y/o Integración de Sistemas Computacionales:***  *La herramienta se integra con diversas tecnologías de ciberseguridad como OWASP ZAP y Metasploit, lo que implica habilidades en desarrollo y adaptación de sistemas.*  ***Integración de Tecnologías de Información:***  *RobotPentester facilita la integración de múltiples herramientas de ciberseguridad, alineándose con la competencia de integración de tecnologías de información.*  ***Desarrollo de Soluciones Tecnológicas:***  *La creación y personalización de scripts de JMeter para pruebas de seguridad es un claro ejemplo de desarrollo de soluciones tecnológicas.*  ***Seguridad de Sistemas Computacionales:***  *La principal función de RobotPentester es identificar y mitigar vulnerabilidades, directamente relacionado con la seguridad de sistemas computacionales.*  ***Aseguramiento de la Calidad del Software:***  *La herramienta mejora la calidad del software mediante la detección y corrección de fallos de seguridad.*  ***Gestión de Proyectos Informáticos:***  *Implementar y gestionar el uso de RobotPentester en un entorno de desarrollo requiere habilidades de gestión de proyectos.*  ***Gestión de la Información y Servicios de Soporte:***  *Los informes detallados generados por RobotPentester proporcionan información valiosa para la gestión y soporte de sistemas.*  ***Ética y Valores Cristianos:***  *Promover una cultura de ciberseguridad proactiva y ética es fundamental para el uso responsable de herramientas como RobotPentester.*  ***Trabajo en Equipo y Resolución de Problemas:***  *La colaboración en la investigación y desarrollo de soluciones de ciberseguridad fomenta el trabajo en equipo y la resolución de problemas.*  ***Innovación y Aprendizaje Permanente:***  *La integración de nuevas herramientas y técnicas de ciberseguridad en RobotPentester promueve la innovación y el aprendizaje continuo.* |
| Relación con los intereses profesionales | *Se centra en los intereses profesionales de la ciberseguridad y en el desarrollo de herramientas automatizadas que mejoren la calidad y seguridad de los proyectos de software. El Proyecto RobotPentester está directamente relacionado con estos intereses, ya que me permite explorar y aplicar conocimientos en la automatización de pruebas de seguridad y en la integración de diferentes herramientas de ciberseguridad.* |
| Factibilidad de desarrollo del Proyecto APT | *El proyecto RobotPentester es factible dentro del tiempo y recursos disponibles durante el semestre.*   * *Duración del semestre: El proyecto se puede dividir en fases manejables que corresponden a la duración del semestre, asegurando que cada etapa se complete dentro del tiempo asignado, además de contar con la ayuda de la empresa ACHS, la cual tuvo la idea de desarrollar este proyecto, por lo cual ya contamos con una base en la cual podemos desarrollar y mejorar nuestro proyecto.* * *Horas asignadas a la asignatura: Las horas asignadas son suficientes para abordar el desarrollo y pruebas de la herramienta en diferentes entornos, además de ser proactivos y usar horas semanales para aprender nuevas tecnologías y desarrollar el proyecto.* * *Materiales requeridos: Los materiales necesarios, como acceso a Docker, JMeter, OWASP ZAP, y recursos de servidores, están disponibles y son accesibles.* * *Factores externos facilitadores: El uso de tecnologías de código abierto y la existencia de bibliografía y recursos en línea para la integración de estas herramientas facilitan el desarrollo del proyecto.* * *Factores externos que podrían dificultar: La complejidad en la integración de múltiples herramientas podría ser un desafío. Para mitigarlo, se considerará la posibilidad de empezar con una integración básica e ir aumentando la complejidad progresivamente.* |

1. **PARTE II**

| **4. Objetivos** |
| --- |
| En este apartado debes definir objetivos generales y específicos del Proyecto APT. Es importante aclarar que los objetivos se deben plantear en forma clara, concisa y sin dar mayores explicaciones, es decir, deben entenderse por sí solos. Se sugiere redactarlos utilizando un verbo en infinitivo, pues ello obliga a precisar acciones concretas. |

| Objetivo general | *Desarrollar una herramienta automatizada que detecte y mitigue riesgos en el desarrollo de software, optimizando tiempos y costos, y asegurando la calidad mediante la identificación temprana de vulnerabilidades en flujos web.* |
| --- | --- |
| Objetivos específicos | ***Implementar*** *un sistema de pruebas de seguridad automatizadas que permita la evaluación continua de vulnerabilidades en frontend y backend.*  ***Integrar*** *herramientas de ciberseguridad como OWASP ZAP y Metasploit para mejorar la detección y mitigación de fallos en el software.*  ***Desarrollar*** *scripts personalizados en JMeter para analizar y simular diferentes escenarios de seguridad en aplicaciones web.*  ***Generar*** *informes detallados que proporcionen recomendaciones accionables para la corrección de vulnerabilidades detectadas.* |

| **5. Metodología** |
| --- |
| En el siguiente apartado deberás describir la metodología, propia de tu disciplina, que utilizarás para resolver el proyecto APT antes descrito, incluyendo las etapas y métodos de trabajo. |

| Descripción de la Metodología |
| --- |
| *Para resolver el problema identificado en el Proyecto APT, se utilizará una arquitectura basada en tecnología Docker. Esta arquitectura permitirá aislar y gestionar de manera eficiente las diferentes herramientas necesarias para el análisis y evaluación de ciberseguridad en la plataforma web. Docker proporcionará la capacidad de contenerizar cada herramienta de forma independiente, asegurando que cada una opere en su entorno óptimo y minimizando las posibles interferencias entre ellas.*  *En primer lugar, se configurarán contenedores específicos para cada una de las herramientas de ciberseguridad requeridas. Particularmente, JMeter se implementará para realizar pruebas de rendimiento y carga sobre la plataforma, lo que permitirá medir su capacidad y comportamiento bajo diferentes escenarios de estrés. Para asegurar la interceptación y el análisis del tráfico generado durante estas pruebas, se utilizará OWASP ZAP como proxy. Este proxy capturará todas las solicitudes y respuestas, proporcionando un contexto detallado del tráfico web, lo cual será crucial para los análisis posteriores.*  *Una vez capturado el tráfico y completadas las pruebas de rendimiento, se procederá a realizar un escaneo activo de la plataforma web utilizando OWASP ZAP. Este escaneo se enfocará en detectar vulnerabilidades dentro del entorno de producción, aprovechando la información recopilada durante las fases anteriores. Al concluir el escaneo, se generará un informe detallado en formato HTML, que presentará de manera clara y organizada las vulnerabilidades encontradas, priorizando aquellas que representen un mayor riesgo para la seguridad de la plataforma.*  *Finalmente, el informe generado servirá como base para la corrección y mitigación de las vulnerabilidades identificadas, asegurando que la plataforma web cumpla con los estándares de seguridad requeridos.* |

| **6. Evidencias** |
| --- |
| A continuación, describe qué evidencias serán evaluadas en el informe de avance y en el informe final de tu proyecto APT. Estas evidencias deben ser acordadas con tu docente. Se entenderá por evidencia los productos que se desarrollen durante el proyecto y cuyo propósito sea visibilizar o documentar cómo se ha implementado el trabajo. |

| **Tipo de evidencia**  **(avance o final)** | **Nombre de la evidencia** | **Descripción** | **Justificación** |
| --- | --- | --- | --- |
| **Avance** | **Video 1** | **Video de oene de Hitler** | **Se verá reflejado en lo que estamos trabajando** |
| **Avance** | **Video 2** | **Video del script** | **Se verá reflejado en lo que estamos trabajando** |
| **Avance** | **Demo 1** | **Demo inicial de una funcionalidad** | **Se verá plasmado una pequeña parte de nuestro trabajo** |
| **Final** | **Demo final** | **Mostraremos la ejecución de nuestro proyecto de forma muy específica debido a que nuestra ejecución total dura en promedio 1 a 2 horas** | **Dado que el objetivo del proyecto es realizar un barrido exhaustivo de la plataforma para detectar vulnerabilidades, se llevarán a cabo numerosas pruebas. Debido al tiempo limitado disponible, se priorizará aquellas pruebas que puedan completarse dentro de ese marco temporal.** |

| **7. Plan de Trabajo** |
| --- |
| En la siguiente tabla define la planificación de tu Proyecto APT de acuerdo a lo requerido. |

| **Plan de Trabajo Proyecto APT** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| Competencia o unidades de competencias | Nombre de Actividades/Tareas | Descripción Actividades/Tareas | Recursos | Duración de la actividad | Responsable[[1]](#footnote-0) | Observaciones |
| *Análisis y planificación de requerimientos informáticos* | | *Análisis de Requerimientos de Seguridad* | | --- |  |  | | --- | | *Identificar y documentar los requisitos de seguridad para el proyecto RobotPentester.* | *Reuniones, Documentos de requisitos, Herramientas de análisis* | *3 semanas* | *Sebastian Acevedo* | *Escribe las dificultades o facilitadores que se podrían presentar durante la ejecución de cada una de las actividades propuestas para llevar a cabo el plan de trabajo.* |
| *calidad de software* | *Caja Negra, Caja Gris* | *Caja negra: Realizaremos pruebas sin tener conocimiento del sistema interno*  *Caja Gris: tendremos conocimiento parcial de lo que maneja el sistema, lo que nos permitirá una combinación de pruebas tanto internas como externas* | *Pruebas caja negra:*  *Nmap, Metasploit, burp suit, OWASP ZAP*  *Pruebas caja Gris:*  *SQLMap y Jmeter* | *2 semanas* | *Maximiliano Hilmer* |  |
| *Gestión de proyectos informáticos* | *Evaluación, gestión de proyecto y de riesgos* | *Evaluación de proyecto*  *Gestión de proyecto*  *Gestión del riesgo* | *Word, excel, proyect y Visual Studio* | *2 semanas* | *Sebastian Acevedo* |  |
| *programación de software* | *POO python, consultas API Owasp ZAP* | *POO: Implementar POO con python para manejar de manera mas versátil los métodos a usar*  *ZAP: Usar una librería de python para consumir los recursos de Owasp ZAP a través de su API y así usar esta herramienta de forma mas flexible* | *- Visual Studio Code*  *- Python*  *- Owasp ZAP* | *7 semanas* | *José Valdebenito -*  *Benjamín Ramirez* |  |
| *Arquitectura de software* | *Definición de arquitectura* | *Definir cantidad de contenedores y funciones de cada uno.* | *Dockers* | *3 semanas* | *Maximiliano Hillmer* |  |

| **8. Carta Gantt** |
| --- |
| Busca un formato de Carta Gantt que te acomode y organiza en este las actividades planificadas en el punto anterior considerando el periodo asignado para el desarrollo de tu Proyecto APT. Debes mantener la temporalidad del periodo académico en el desarrollo de las tres fases que contempla la Asignatura de Portafolio de Título. |

| **Actividad** | **Fase 1** | | | | **Fase 2** | | | | | | | | | | | | **Fase 3** | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **S 1** | **S 2** | **S 3** | **S 4** | **S 5** | **S 6** | **S 7** | **S 8** | **S 9** | **S 10** | **S 11** | **S 12** | **S 13** | **S 14** | **S 15** | **S 16** | | **S 17** | **S 18** |
| *Evaluación, gestión de proyecto y de riesgos* | **x** | **x** |  |  |  |  |  |  |  |  |  |  |  |  |  |  | |  |  |
| *Análisis de Requerimientos de Seguridad* |  | **x** | **x** |  |  |  |  |  |  |  |  |  |  |  |  |  | |  |  |
| *Definición de arquitectura* |  | **x** | **x** | **x** |  |  |  |  |  |  |  |  |  |  |  |  | |  |  |
| *POO python, consultas API Owasp ZAP* |  |  |  |  | **x** | **x** | **x** | **x** | **x** | **x** | **x** | **x** | **x** |  |  |  | |  |  |
| *Evaluación, gestión de proyecto y de riesgos* |  |  |  |  |  |  |  |  |  |  |  |  |  | **x** | **x** |  | |  |  |

1. En caso de que el Proyecto APT sea grupal, en esta columna deben indicar el nombre de los responsables de cada tarea o actividad. Esto posteriormente permitirá diferenciar la evaluación por cada integrante. [↑](#footnote-ref-0)