

Tabla de Contenido

Introducción	1
1. Antecedentes Generales	4
1.1. Introducción al Pentesting	4
1.2. Herramientas de Pentesting	6
1.3. Objetivos	8
1.3.1. Objetivo General	8
1.3.2. Objetivos Específicos	8
1.4. Solución Propuesta	9
1.5. Resultados Esperados	10
1.6. Alcances	10
1.7. Caso Práctico: Contexto Fintual	10
2. Diseño de la Solución	12
2.1. Análisis de la situación actual	12
2.2. Selección de aplicaciones web vulnerables como ambientes de verificación	12
2.3. Selección de herramientas de análisis de vulnerabilidades	13
2.4. Configuración del ambiente de trabajo y de las herramientas seleccionadas	13
2.5. Estudio de uso, validación de funcionamiento y automatización de las herramientas seleccionadas	14
2.6. Estudio de arquitectura y programación de la solución propuesta	14
2.7. Validación de la solución propuesta	16
2.7.1. Métricas	16
2.7.2. Verificación de detección básica	16
2.7.3. Fintual: validación con una aplicación web en producción	17
2.8. Integración de la herramienta desarrollada en el ambiente de desarrollo de Fintual	17
2.9. Integración Módulo Adicional	18
3. Implementación de la Solución	20
3.1. Módulo User Config Parser: Configuración del usuario	21
3.2. Módulo Env: Ambientes	21
3.3. Módulo Env Manager: Administrador de Ambientes	21
3.4. Módulo APT2 Manager: Administrador de APT2	22
3.5. Módulo APT2: Automated Penetration Testing Tool	22
3.6. Módulo Scanner Master: Gestor de herramientas de detección de vulnerabilidades	23

3.6.1. Módulo Argument Parser: Gestor de argumentos de ejecución	24
3.6.2. Scanner: Herramienta de detección de vulnerabilidades	24
3.6.3. Módulo Results Parser: Gestor de resultados	25
3.7. Módulo Analyzer: Ingreso de falsos positivos	26
3.8. Módulo Reporter: Visualización de datos	27
4. Resultados	29
4.1. OWASP Mutillidae II - PHP	30
4.2. Google Gruyere - Django	32
4.3. OWASP Railsgoat - Ruby on Rails	34
4.4. Fintual - Ruby on Rails	35
5. Discusión	37
5.1. Evaluación de los resultados	37
5.2. Trabajo futuro	40
5.3. Open source	40
Conclusión	41
Bibliografía	42
Anexo A: Flujos de la Solución	44
A.1. Flujo de la solución desarrollada en el entorno local	44
A.2. Flujo de la herramienta en el ambiente de desarrollo de Fintual	44
Anexo B: Glosario	47
Anexo C: Dashboard	49