Diseño de un Pentesting para una Aplicación Web Basado en la Metodología OWASP V.4

Angelica Rueda
Facultad de Ingeniería, Escuela de Comunicaciones Militares de Colombia
Facatativá-Cundinamarca, Colombia

Resumen— A través de este proyecto se realizó el diseño de un Pentesting basado en la metodología OWASP V.4 con la finalidad de evaluar la Seguridad de la Aplicación Orfeo (Sistema Gestión Documental), El proyecto se desarrolló con base en los lineamientos definidos en los estándares reconocidos, como la norma internacional ISO 27002, lineamientos nacionales de política en Ciberseguridad y Ciberdefensa CONPES 3854 de 2016. Una vez identificado el marco normativo aplicable se realizó un diagnóstico actual de los procedimientos y metodologías definidas en el Grupo de Apoyo Nueva Era. Se analizó la información referente para elaborar el test de penetración bajo con la estrategia "Grey Box", tipo de prueba usado en el diseño desarrollado. Finalmente, y basados en la información recopilada se elaboran dos reportes finales en la fase de documentación del Pentest, Informe Ejecutivo e Informe Técnico los cuales se entregados a los directivos del Grupo de Apoyo Nueva Era.

Abstract— In this project the design of a Pentesting based on the methodology OWASP V.4 is realized. In order to evaluate the Orfeo Application Security (Document Management System) of the Colombia National Army, the project was developed based on the guidelines defined in the standards recognized as the international standard ISO 27002, and national policy guidelines in Cybersecurity and Cyberdefense as The document CONPES 3854 of 2016. Once the applicable regulatory framework was identified, a current diagnosis was made of the procedures and methodologies defined in the New. The relevant information is analyzed and the penetration test is elaborated with the strategy "Gray Box" that tests the developed design. Finally, based on the information gathered, two final reports are produced in the documentation phase of the Pentest, Executive Report and Technical Report, which were delivered to the directors of the Telematics Office.

Índice de Términos: Amenaza, Auditoria de Seguridad, Ciberseguridad, Grey Box, Pentesting, Vulnerabilidad.

I. Introducción

Durante los últimos años se observa que la seguridad en las Aplicaciones Web de los sistemas de información de las organizaciones están cada vez más comprometidas, bien sea por malware o por ataques de índole informático, sumando a errores administrativos y de gestión de la información, tales como: configuraciones mal elaboradas, errores humanos, políticas de seguridad ineficientes y otras vulnerabilidades que pueden ser explotadas por un atacante para dañar un sistemas de información. El atacante puede ser un individuo, un grupo de hackers o una Nación. Su objetivo final es alterar la operación de negocio, inutilizar las aplicaciones, los servidores y red es de comunicación de manera temporal o permanente.

Para contrarrestar esta problemática las organizaciones deben realizar pruebas de penetración de manera regular, como bien se sabe dichas auditorias son demasiado costosas, ya que es aconsejable que se realicen mínimo cada 6 meses. Es por esto, que se les asesora a la Oficina de Telemática - Coordinación Grupo de Apoyo Nueva Era, sobre el diseño y desarrollo de un Pentest de Seguridad el cual será ejecutado por los miembros del área de Seguridad de la Organización. Estas pruebas de penetración son una de las características esenciales que busca asegurar el funcionamiento de la Aplicación Orfeo Gestión documental, está aplicación maneja la información de todo el personal del Grupo de Apoyo Nueva Era y está interconectada con otra Aplicación de Recursos Humanos, por lo tanto, es necesario contar con el apoyo interno de la organización que permita salvaguardar la información y operación del negocio, o en el caso que la organización presente alguno de estos eventos:

A) El sistema de seguridad descubre nuevas amenazas.
B) Se agrega una nueva infraestructura de red.
C) Se actualiza el sistema o instala nuevo software.
D) Se configura un nuevo usuario final programa / política.

Por consiguiente, el presente proyecto se enfocó específicamente diseño un Pentesting, elaborado exclusivamente para la Grupo de Apoyo Nueva Era. Esta Oficina cuenta con 150 estaciones de trabajo y aproximadamente 500 usuarios conectados diariamente a Orfeo. Por su estatus de institución, la información es considerada una de las más sensibles del país, por ende, se debe garantizar que este documento no será accesible a terceros, de ahí parte la necesidad de conocer su estado actual a nivel de la Ciberseguridad, conocer una parte del manejo actual sobre este tema para orientarlos sobre los escenarios que debe contemplar previamente, los requerimientos mínimos que deberán tener para la ejecución de un test de penetración y qué aspectos deben ser considerados con otros mecanismos (revisión de configuraciones y procedimientos, auditoría de aplicativos, etc.) que los reportes entregados les sea de gran utilidad para el personal del área de TI.

El proyecto se desarrolla basado en la metodología OWASP V.4 adaptado en cuatro fases como lo son:

A) Recolección de la Información
B) Escaneo
C) Explotación
D) Documentación.

Figura 2. – Fases para la elaboración del Pentesting

Finalmente y basado en lo encontrado se elaboran dos reportes finales en la fase de documentación del Pentest, Informe Ejecutivo e Informe Técnico los cuales serán entregados a los directivos de la Grupo de Apoyo Nueva Era.

II. METODOLOGÍA

La metodología empleada en el diseño del Pentesting se fundamenta en una investigación de tipo cualitativa con un planteamiento inicial inductivo, se presenta un diseño flexible con hallazgos encontrados desde el inicio hasta el fin.

Contiene una perspectiva holística estudiando los elementos que rodean a la investigación del proyecto del Pentest. Basados en entrevistas, en observación directa, en analizar cada documento proporcionados. Es por ello que se categorizó por etapas como se observa en la figura 2.

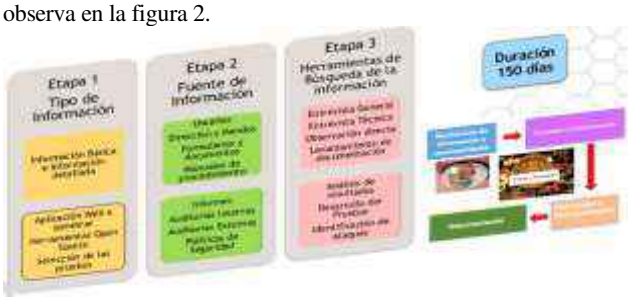


Figura 3. Etapas implementadas en la metodología

A) Etapa 1: Tipo de Información

Se busca la información de forma escalonada, se inicia con la información básica que se relaciona con el Porqué. Una vez se cuenta con esta información se procede al detalle investigar el Qué y el Cómo como estrategia de búsqueda.

B) Etapa 2: Fuente de Información

Para dar alcance a esta etapa se tuvo en cuenta dos fuentes de información para obtener un resultado confiable.

1) Población: Se tuvieron en cuenta los actores que intervienen con la Aplicación Web tanto directa como indirectamente, es decir los que interactúan con ella y con los que la protegen de posibles ataques.

2) **Muestra:** Para determinar los elementos poblacionales se implementa la primera fase del Pentesting que consiste en la Recolección de la información y haciendo un análisis descriptivo de los usuarios que intervienen con la Aplicación Web, se tomaron como referencia personal de la Oficina de Telemática como el desarrollador de la aplicación, aprendiz, administrador backup y administrador titular. Ya que son ellos los que tienen la información relevante de la arquitectura de la aplicación y conocen de fondo el funcionamiento de la herramienta. Estas personas suministraron información sobre los manuales de la aplicación, sobre las políticas, sobre la arquitectura de red y sobre la última auditoría realizada.

C) Etapa 3: Herramientas de búsqueda de la información

1) **Encuesta de Levantamiento General de la Aplicación Web:** La finalidad del resultado de esta encuesta fue determinante para poder iniciar nuestro proceso investigativo en la Oficina de Telemática, necesitábamos contar con datos que nos acercaran a la aplicación que percibiéramos la importancia de esta para los usuarios. El primer filtro fue contar con la colaboración de la Gerencia encargada, esta persona nos suministró la información inicial y determinó la necesidad de realizar el Pentest como ayuda a su dependencia. Se diseñó un cuestionario base de forma clara y concisa sobre aspectos generales y sobre algunas perspectivas del negocio, la opción de respuesta fue (SI-NO) y tiempos catalogado en meses. Se compone de 10 preguntas el cual se encuentra como Anexo al finalizar este trabajo.

2) **Encuesta para el Levantamiento de Información Técnica de la aplicación Web:**

La información solicitada en este cuestionario brinda datos enfocados a la Aplicación Web, como datos de usabilidad, datos de configuración, datos de infraestructura y datos de seguridad. La técnica usada el levantamiento de la información fue a través de cuestionarios detallados y fue realizado a los actores principales que intervienen con el funcionamiento de la aplicación, desarrollador, administrador backup y administrador principal. Ellos ofrecieron la información más relevante, dando a conocer las expectativas que tenían con la realización del Pentesting con el fin de aplicar las técnicas de ataques y contralar así las vulnerabilidades que se encuentren en el desarrollo de esta auditoría de seguridad. El propósito de usar esta técnica de entrevistas es contar con indicadores que permitan medir las vulnerabilidades iniciales y posibles amenazas como punto de partida. El objetivo de estas encuestas se basa en contar con una línea base de información, los controles actuales que tiene la aplicación. La opción de respuesta fue de texto descriptivo, el cual permite de forma libre describir la respuesta de manera abierta. Los resultados fueron factor primordial para dar inicio al Test de Penetración y para la sustentación de la importancia de la realización de este trabajo tanto para la Oficina de Telemática como para nosotros.

3) Observación directa: Este técnica fue seleccionada por su eficacia ya que es la que describe el uso de forma directa y dinámica, se observó a los actores principales interactuando con la aplicación para poder dar una respuesta más clara sobre las preguntas, en el caso del desarrollador de la aplicación sus conceptos eran cortos y debía apoyarse en la herramienta para poder explicar más su respuesta, ejemplo, en la prueba de asignación de roles, explico a través de los menús en cascada como se crea un usuario y como se le asignan los permisos, mostró la jerarquía del manejo y control de la aplicación. El beneficio de usar esta técnica para la recolección de la información es que los datos son veraces puesto que se derivan de una de las fuentes principales. Esta técnica fue la más efectiva para el proceso inicial y de muy fácil aplicación ya sumistra los datos adecuados y conductas identificadas y exactas del uso de la aplicación.

4) **Análisis de la información recolectada:** Una vez ya diligenciadas y consolidadas las estrategias de búsqueda y descripción de cada una de ellas en el diseño del Pentest, se realiza una evaluación usando el método convencional, a través de una

plantilla de Excel se tabularon las respuestas y se realizó un análisis interpretativo gráficamente.

Procentaje Seguridad de la Aplicación Web

$$\text{Seguridad} = \left(\frac{\text{Respuestas negativas}}{\text{Cantidad de Preguntas}} \right) * 100$$

$$\text{Seguridad} = \left(\frac{5}{10} \right) * 100$$

$$\text{Seguridad} = 50$$

Resultado: El 50 % de la aplicación es insegura

Figura 4. Porcentaje seguridad de la Aplicación Orfeo basado en la encuesta.

Para la encuesta de preguntas abiertas se consolido por la cantidad de participantes y el conocimiento y percepción que tienen sobre la aplicación, es decir si conocen la aplicación y como está conformada. Cada uno de los grupos de datos contiene 5 preguntas, de estas cinco preguntas se seleccionan las que el actor no conoce la aplicación. De acuerdo al cuadro 4, identificamos que los actores principales no conocen al completamente la aplicación en temas de seguridad, el índice es demasiado bajo para la importancia del rol que se tiene. Así mismo se observa el conocimiento que tiene el Administrador Backup con respecto al Desarrollador, este indica que el participante 1 conoce más de la aplicación así su rol este por debajo del rol Administrador Backup. En consecuencia, de esta información se deduce que la falta de capacitación por parte del administrador principal hacia el administrador backup es deficiente y puede traer consecuencias nefastas en caso que el participante 3 desista de su función.

Actores	Datos Generales	Datos de Usabilidad	Datos de Configuración	Datos de infraestructura	Datos de Seguridad	Total
Participante 1. Desarrollador	60%	100%	20%	60%	20%	52%
Participante 2. Admin Backup	40%	40%	60%	80%	10%	46%
Participante 3. Admin Principal	100%	100%	100%	100%	70%	94%

Cuadro 1. Participantes en la encuesta

III. RESULTADOS

Para la evaluación de la seguridad de la Aplicación Web Orfeo (Sistema de Gestión Documental) Grupo de Apoyo Nueva Era se diseñó un Pentesting basado en la Metodología OWASP V.4. Descrito en la siguiente figura 5.

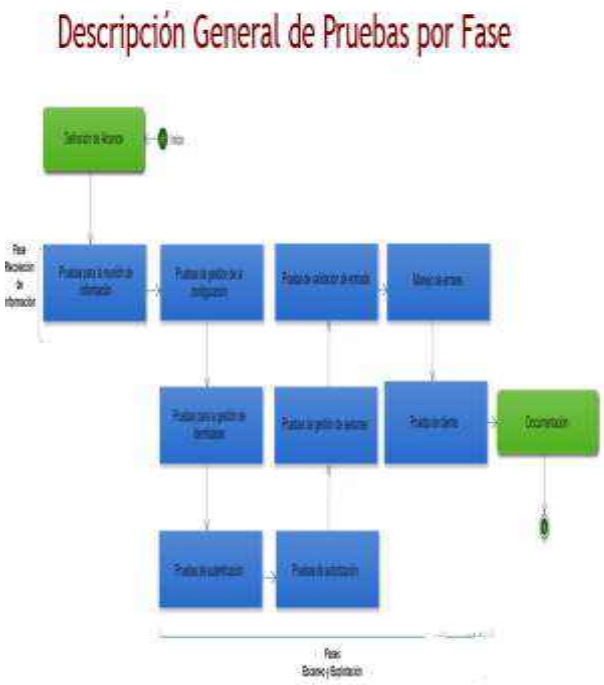
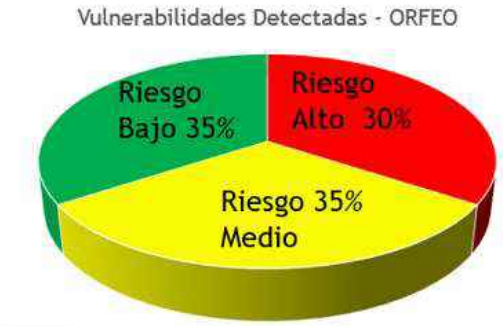


Figura 5. Descripción General de Pruebas por Fase de Pentesting

Se validó este diseño a través de la implementación de un Pentesting en los que se detectaron varias vulnerabilidades en ejecución con las siguientes pruebas.

A) Pruebas de Reunión de la Información Reconocimiento en Motores de Búsqueda
B) Prueba Definición de Roles
C) Prueba de la Política de Usuario débil o no forzada
D) Pruebas de Autenticación
E) Pruebas de Configuración de la red de prueba / infraestructura
E) Prueba de Métodos HTTP
F) Prueba de directorio trasversal
G) Pruebas para el esquema de autorización de omisión
H) Prueba de esquema de gestión de sesión
I) Prueba de las variables de sesión expuestas
J) Pruebas de secuencias de comandos de sitios cruzados reflejados
K) Pruebas de Clickjacking
L) Pruebas de SQL Injection
M) Prueba de una contraseña de texto claro
Ñ) Prueba de entrada de usuario o login
O) Prueba De fuga de información

Para el análisis las pruebas descriptas se utilizaron herramientas para el Scan – Detección de vulnerabilidades y pruebas de análisis manuales. En donde se obtiene como resultado el siguiente cuadro de riesgos.



Fuente: Autores 2017

Cuadro 2. Análisis de vulnerabilidades por gravedad y confianza

Como podemos observar para 35 pruebas realizadas de las 53 definidas en el diseño arroja vulnerabilidades de seguridad en la aplicación Orfeo, se evidencia que el 30 por ciento de Orfeo se encuentra amenazado y se confirma la necesidad de implementar el diseño propuesto.

IV. DISCUSIÓN

Este estudio se propuso con el objetivo de diseñar un Pentesting para una aplicación Web, además de orientar al Grupo de Apoyo Nueva Era basada en una metodología y a su equipo de Ciberseguridad en la realización de estas pruebas, se garantiza la calidad de la seguridad de la información de sus Aplicaciones desarrolladas o adquiridas. Los resultados de este proyecto muestran que es de vital importancia la asegurar sus sistemas frente a la mayor cantidad de posibles amenazas, además, contar con personas que se encarguen de establecer dichas medidas de seguridad y mantenerlas activas y actualizadas.

Estos resultados concuerdan con los obtenidos en estudios previos como los realizados por el proyecto Open Web Application Security (OWASP) en el Top 10 de vulnerabilidades, frecuentes en Aplicaciones Web puestas en producción. Sin embargo, muchas de las pruebas que recomienda la Metodología OWASP no fueron suficientes para detectar las vulnerabilidades por lo que se consultaron otros autores y técnicas. Debido a que los ataques informáticos evolucionan cada día y ya existen controles implementados en las infraestructuras que soportan estas aplicaciones.

Existen varias explicaciones posibles para estos resultados como los describen cada uno de los hallazgos encontrados.

A) No existe política de Seguridad para Gestión de Errores y acceso a usuarios.
B) No existe política de Seguridad para Gestión de Administración de Usuarios.
C) No se cuenta documentación de diagramas de despliegues de la aplicación.
D) No se cuenta con manuales técnicos del código fuente de la aplicación excepto el suministrado por Orfeogpl, el cual se encuentra desactualizado.
F) No existe documentación de la RFC de control de cambios realizados a la aplicación.
G) Personal inexperto en seguridad de la información.
Ineficiente configuración de la infraestructura que soporta la aplicación como lo son servidores de aplicaciones web.
H) No validación de las aplicaciones o sistemas de información que contratan con terceros.
falta de políticas de seguridad en el desarrollo de aplicaciones web seguras.

Dado el pequeño tamaño muestral se debe ser cauto al hacer interpretaciones porque solo se está analizando un 35% del total de pruebas diseñadas, además se debe tener presente que a Orfeo se le realizaron las pruebas es una aplicación Open Source, el código de desarrollo se encuentra publicado en la web lo que genera una vulnerabilidad mayor en la implementación de esta. Y por lo tanto se deben tomar medidas mayores de seguridad. El total de vulnerabilidades de catalogadas como Altas sugiere que podría existir muchas más en el momento de realizar la implementación de las 53 pruebas diseñadas y propuestas. Se sugiere que estudios futuros sobre este tema aborden las fases del ciclo de vida en el desarrollo de las aplicaciones web dado que muchos de estos hallazgos tienen origen en el diseño e implementación de las aplicaciones web.

V. CONCLUSIONES

Para concluir este artículo tengamos presente la importancia que tiene la realización de pruebas de un Pentesting a las Aplicaciones Web, en el contexto de seguridad de la información, ya que estas pruebas le dan a la organización la perspectiva de qué tipo de seguridad han implementado y si se necesita mejorar algún aspecto que se ha restringido. Si las políticas de seguridad están bien orientadas las brechas en el ciclo de vida del desarrollo serán menores en sus aplicaciones web.

En este proyecto se propuso diseñar un Pentesting para evaluar la seguridad de la Aplicación Web Orfeo (sistema de Gestión Documental) a través del diseño del Pentesting basado en la metodología OWASP V.4. El cual fue gratificancante, demostrando a través del estudio exploratorio que existen vulnerabilidades la aplicación Orfeo y que posiblemente que estas mismas amenazas existan en los demás Sistemas con los que cuenta la Oficina de Telemática Grupo de Apoyo Nueva Era.

Los hallazgos de este informe están sujetos por lo menos a 5 limitaciones: En primer lugar, las políticas de seguridad que restringen el acceso a algunos recursos del sistema, el tamaño de la muestra para las pruebas. Se sugiere que se tomen medidas en la seguridad de las aplicaciones web no solo las aplicaciones que están en ambiente de producción, sino las que se encuentran en la fase de desarrollo y pruebas.

Para finalizar debido que Orfeo es una aplicación Web Open Source se recomienda a cualquier entidad que desee implementar su código Open Source, realizar ajustes en la codificación e implementación de la infraestructura para mitigar los riesgos de seguridad que esta presenta.

VI. RECONOCIMIENTOS

A los directivos que intervinieron en la orientación de este trabajo, que permitió sacar adelante, los profesores que dejaron huella en el

trascurso de esta Especialización, especialmente al Ingeniero Jairo E. Márquez D, por inspirarnos a seguir la línea de Pentesting, por su pasión a lo que hace a través de la enseñanza y el aporte otorgado a través de su asignatura.
Igualmente, a las personas que se interesaron en esta investigación como el Ing. Fabián Blanco por su asesoramiento y ayuda para permitirnos culminar nuestro.

VII. REFERENCIAS BIBLIOGRÁFICAS

Páginas de Web:

[1] Vela Fernando (2017). Guía de Pruebas V.4 reléase Versión en Español. Recuperado de https://www. OWASP V.4.org/index.php/Sobre_ OWASP V.4

[2] ISECOM (2.017). OSSTMM Open Source Security Testing Methodology Manual. Recuperado de

http://www.isecom.org/home.html y http://www.isecom.org/mirror/OSSTMM.3.pdf

[3] Anonym.OS (2.013). Want to be hidden in the Internet? Recuperado de http://anonym-url.com/index.html.

[4] Limitations of Penetration Testing. (2016). Why Pen Testing? Why Penetration Testing is Important?

Recuperado de http://www.pen-tests.com/tag/penetration-testing

[5] Test de intrusión (III). (2007). Un informático al lado del mal. Última actualización (2.015). Recuperado de: http://www.elladodelmal.com/2015/03/test-de-intrusin-iii-de-vi.html

[6] Información Gathering. (2.011). Comunidad DragonJar. Recuperado de https://issuu.com/dragonjar/docs/information_gathering_-_gu_a_de_pentesting

[7] Universidad Nacional Abierta y a Distancia. Herramientas para Pruebas y Evaluación. (2015). Recuperado de:

http://datateca.unad.edu.co/contenidos/233016/EXE_SAM/leccin_30_herramientas_para_pruebas_y_evaluacin.html

Artículos de revistas en línea:

[8] Revista Portafolio. (2014). Sección de Negocios de Portafolio. Bogotá - Colombia.: Portafolio. Recuperado de http://www.portafolio.co/negocios/empresas/colombia-principal-fuente-ciberataques-latinoamerica-50768).

Capítulo de un libro

[9] Tori Carlos (2008). "Técnicas de Intrusión en sistemas, metodologías sobre chequeos de seguridad y Ejemplos reales. En C Mastroianni (Ed.). Inyección de código SQL (pp. 164-172). Rosario, Argentina.

[10] Kim Peter (2015). The Hacker Playbook 2 Practical Guide To Penetration Testing North Charleston. En MHID Planet (Ed.). Cross Site Scripting and Cross Site Request (pp. 149-155). South Carolina

Video:

[11] http://www.youtube.com/watch?v=sQe7d_2WG30

[12] http://www.youtube.com/watch?v=WYWDgRO6VT0