Proyecto Final

Curso Seguridad Informática

INSTRUCCIONES

Crear un sitio Web (levantar un servidor Apache, por ejemplo) que presente la página de la Organización que le fue asignada en la actividad de Análisis de Riesgos. Esta aplicación Web debe contar con autenticación para sus usuarios (con login y password). Asimismo, debe contar con una base de datos para registrar, modificar o consultar información relacionada con la organización (Algo sencillo que funcione, sin pretender mucho "Look and Feel"). Debe desarrollarse en Java para facilitar el uso de herramientas de seguridad.

1. Corra un escaneo de vulnerabilidades con nessus hacia su servidor desde otro equipo.
    a. Informe los hallazgos que la herramienta arroje.
    b. Informe respecto a qué se podría hacer al aprovechar la vulnerabilidad que considere más grave de lo arrojado en el inciso a y
    c. Proponga al menos 2 controles que imposibilitarían el aprovechar esa vulnerabilidad (de forma teórica, no se requiere su implementación). (PRIMERA PRESENTACIÓN DE AVANCE AL PROFESOR EN CLASE 24 de Octubre)
2. Demuestre en su aplicación Web los ataques siguientes (para lo cual quizás deba debilitar su aplicación):
    a. SQL injection
    b. XSS
    c. Information Leakage by Improper Error Handling
    d. Malicious Execution
3. Demuestre y documente un ataque de Man In The Middle (MITM) para su Servidor Web de la Organización.
    a. Esta demostración debe colocar un tercer elemento entre el Cliente (browser) y el Servidor Web, aunque este elemento (el MITM) puede estar alojado en el cliente o en el servidor según le convenga para su demostración (puede ser manualmente usando PAROS, Fiddler o algún otro proxy).
    b. Debe al menos involucrar dos equipos de cómputo (uno donde reside el Cliente, otro donde reside el Servidor). En cualquiera de ellos puede residir el MITM.

c. Debe documentarse la herramienta utilizada o desarrollada (según el caso) para implementar el MITM.
d. Debe demostrarse el funcionamiento al profesor.
    i. Funcionamiento normal (http).
    ii. Funcionamiento normal con MITM
    iii. Funcionamiento alterando información de autenticación del Cliente o de la información que fluye entre el Cliente y el Servidor en el MITM.
    (SEGUNDA PRESENTACIÓN DE AVANCE AL PROFESOR EN CLASE 7 de Noviembre)

4. Genere certificados digitales para el Servidor Web y documente.
5. Active HTTPS (utilizando sólo el certificado del Servidor) en su servidor Web, y demuestre que el ataque de MITM sigue siendo posible, documente.
6. Genera certificados para los clientes (puede ser sólo un cliente) y documente.
7. Active HTTPS con ***autenticación mutua*** y compruebe que el ataque de MITM se mitiga, es decir que ya no es evidente para el atacante. Documente.
8. Identifique alguna herramienta que le permita hacer una prueba de caja blanca del código en java de su Servidor Web y documente los resultados (por ejemplo FindBugs).
9. Identifique alguna herramienta que le permita hacer una prueba de caja negra a su Servidor Web y documente los resultados (por ejemplo SkipFish).
   (PRESENTACIÓN DE PROYECTO PARA EVALUACIÓN AL PROFESOR EN CLASE el 28 de noviembre).