Tarea online HE05.

Título de la tarea: Hacking de aplicativos web.

Curso de Especialización y módulo: Ciberseguridad en Entornos de las Tecnologías de la Información - Hacking Ético.

¿Qué contenidos o resultados de aprendizaje trabajaremos?

Resultados de aprendizaje

- **RA5.** Ataca y defiende en entornos de prueba, aplicaciones web consiguiendo acceso a datos o funcionalidades no autorizadas.

Contenidos

1.- Introducción al protocolo HTTP.
    1.1.- Arquitectura de un aplicativo web.
    1.2.- Introducción al protocolo de comunicaciones HTTP.
    1.3.- Análisis de la petición HTTP.
    1.4.- Análisis de la respuesta HTTP.
    1.5.- Tipos de autenticación web.
2.- Recolección de información.
    2.1.- Pruebas de recolección de información.
    2.2.- Herramientas de recolección de información.
3.- Análisis de tráfico mediante proxies de interceptación.
    3.1.- Introducción a los proxies de interceptación.
    3.2.- OWASP ZAP proxy.
    3.3.- Burp Suite proxy.
    3.4.- Automatización de conexiones a servidores web con BurpSuite.
4.- Búsqueda de vulnerabilidades habituales en aplicaciones web.
    4.1.- Fundación OWASP.
    4.2.- Pruebas de configuración y despliegue.
    4.3.- Pruebas de gestión de identidad.
    4.4.- Pruebas de autenticación.
    4.5.- Pruebas de autorización.
    4.6.- Gestión de sesiones.
    4.7.- Validación de los puntos de entrada.
    4.8.- Análisis de los códigos de error.
    4.9.- Vulnerabilidades de la lógica de negocio.

1.- Descripción de la tarea.

Caso práctico

Una vez Pedro ha completado el curso, ha adquirido los conocimientos necesarios para poder realizar tareas propias de una auditoría de hacking ético sobre un aplicativo web.

Direct Media (Dominio público)

Al igual que hicieron sus compañeros Luis y Paloma, Pedro ha de realizar unas sesiones formativas con la finalidad de compartir estos conceptos con sus compañeros de trabajo. De esta manera, todos podrán tener, al menos, unas nociones básicas de ciertas técnicas de hacking ético en aplicativos web que ha podido aprender Pedro en el curso.

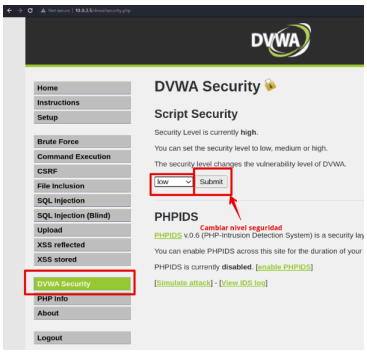
Pedro tiene pensado seguir el mismo enfoque práctico que sus compañeros han dado a este tipo de sesiones formativas dado que todos tienen claro que es el mejor sistema para poder afianzar los conceptos . De modo que configura un laboratorio de pruebas específico para esta temática y resolver de manera práctica algunas de las vulnerabilidades en aplicativos web aprendidas durante el curso.

¿Qué te pedimos que hagas?

Todos los apartados de esta práctica se realizarán sobre el portal vulnerable DVWA que se encuentra instalado en la máquina metasploitable bajo el protocolo HTTP.

Sergio Romero Redondo. *Portales Vulnerables* (CC0)

Tendréis que configurar el nivel de seguridad en "low" para poder realizar la práctica. Para ello, una vez accedáis al portal tendréis que configurar el nivel de seguridad en el apartado "DVWA Security"



Sergio Romero Redondo. *Nivel de seguridad* (CC0)

- **Apartado 1: Fuerza Bruta con BurpSuite**

  Apoyándote en el proxy de interceptación Burp Suite realiza un ataque de fuerza bruta sobre la funcionalidad "Brute Force" de Damn Vulnerable Web Application.

- **Apartado 2: Cross Site Scripting Almacenado con BurpSuite**

  Apoyándote en el proxy de interceptación Burp Suite realiza un ataque de Cross Site Scripting Almacenado sobre la funcionalidad "XSS stored" de Damn Vulnerable Web Application.

- **Apartado 3: Ejecución remota de código con BurpSuite**

  Apoyándote en el proxy de interceptación Burp Suite realiza un ataque de ejecución remota de código sobre la funcionalidad "Command Execution" de Damn Vulnerable Web Application.

- **Apartado 4: E**jecución de inyección SQL con BurpSuite

  Apoyándote en el proxy de interceptación Burp Suite realiza un ataque de inyección SQL sobre la funcionalidad "SQL injection" de Damn Vulnerable Web Application.

- **Apartado 5: Extraer datos con sqlmap**

  Apoyándote en la herramienta sqlmap extrae información de el "Banner de la Base de Datos" utilizando la vulnerabilidad de inyección SQL localizada en el apartado 4 en la funcionalidad "SQL injection" de Damn Vulnerable Web Application.

NOTA IMPORTANTE

Para los apartados en los que se solicita realizar una captura de pantalla hay que tener en cuenta que las capturas realizadas deben tener como fondo de pantalla la plataforma con tu usuario mostrando claramente la foto de tu perfil. Aquellos apartados/subapartados que no cumplan esta condición no serán corregidos.

2.- Información de interés.

Recursos necesarios y recomendaciones

Recursos necesarios

- Ordenador personal con, al menos, 4 Gigabytes de memoria RAM.
- Conexión a Internet para consultar ejemplos de la Unidad 5.
- Sistemas Operativos preferidos Kali Linux, Parrot Linux.
- Sistema Operativo de la víctima Metasploitable2.
- Navegador web.
- Proxy de interceptación Burp Suite Community Edition.
- Software para comprimir los archivos de la tarea.

Recomendaciones

- Antes de abordar la tarea:
  - Lee con detenimiento la unidad, consulta los enlaces para saber más, examina el material proporcionado por el profesor y aclara las dudas que te surjan con él.
  - Realiza el examen online de la unidad, y consulta nuevamente las dudas que te surjan. Solo cuando lo tengas todo claro, debes abordar la realización de la tarea.
- No olvides elaborar el documento explicativo.

Indicaciones de entrega

Una vez realizada la tarea, el envío se realizará a través de la plataforma. El archivo se nombrará siguiendo las siguientes pautas:

Apellido1_Apellido2_Nombre_HE05_Tarea

Asegúrate que el nombre no contenga la letra ñ, tildes ni caracteres especiales extraños. Así por ejemplo la alumna **Begoña Sánchez Mañas para la quinta unidad del MP de HE**, debería nombrar esta tarea como...

sanchez_manas_begona_HE05_Tarea

3.- Evaluación de la tarea.

Criterios de evaluación RA5

- a) Se han identificado los distintos sistemas de autenticación web, destacando sus debilidades y fortalezas.
- b) Se ha realizado un inventario de equipos, protocolos, servicios y sistemas operativos que proporcionan el servicio de una aplicación web.
- c) Se ha analizado el flujo de las interacciones realizadas entre el navegador y la aplicación web durante su uso normal.
- d) Se han examinado manualmente aplicaciones web en busca de las vulnerabilidades más habituales.
- e) Se han usado herramientas de búsquedas y explotación de vulnerabilidades web.
- f) Se ha realizado la búsqueda y explotación de vulnerabilidades web mediante herramientas software.

¿Cómo valoramos y puntuamos tu tarea?

Rúbrica de la tarea	
Apartado 1: Realiza y detalla correctamente el proceso de explotación de la vulnerabilidad de Fuerza Bruta.	2 puntos
Apartado 2: Realiza y detalla correctamente el proceso de explotación de la vulnerabilidad Cross Site Scripting Almacenado.	2 puntos
Apartado 3: Realiza y detalla correctamente el proceso de explotación de la vulnerabilidad Ejecución Remota de Código.	2 puntos
Apartado 4: Realiza y detalla correctamente el proceso de explotación de la vulnerabilidad Inyección SQL.	2 puntos
Apartado 5: Realiza y detalla correctamente el proceso de extracción de datos mediante la herramienta sqlmap.	2 puntos
Redacción clara y correcta, sin errores ortográficos	**Se resta 0,1 puntos por cada error ortográfico o**

	expresiones incorrectas.

NOTA IMPORTANTE

Aquellos apartados/subapartados en los que las capturas de pantalla no sean claras o no tengan como fondo de pantalla la plataforma con tu usuario mostrando claramente la foto de tu perfil, no serán corregidos.