ascentic/

6. Taller de pentesting

Manos a la obra

6.a Una aplicación insegura

…o dos

ascentic/

OWASP Juice Shop

https://owasp.org/www-project-juice-shop/

OWASP WebGoat

https://owasp.org/www-project-webgoat/

ascentic/

6.b Herramientas de pen-testing

… más algunas de base

Aislamiento del entorno de trabajo

Buscamos

- Un entorno controlado y aislado
- Optamos por ejecutar máquinas virtuales:
  - Vagrant para el control
  - VirtualBox como software de virtualización
  - Dentro del mismo instalaremos Docker (script)
- Alternativas durante el curso
  - Utilizar otro proveedor de virtualización
  - Crear manualmente una imagen propia, Ubuntu 20.04 based (Ubuntu, mint …)
  - Kali linux

Herramientas generales

Instalamos en la máquina virtual:

- git
- Chrome, Firefox
- Docker
- node/npm
- VSCode
- ZAP

Pentesting – Atendiendo al conocimiento del sistema

Puede ser realizado por equipos internos o externos.

- Black Box: Desconocemos detalles internos del sistema
- White Box: Podemos llegar a tener acceso a la documentación, fuentes…
- Grey Box: Escenario intermedio

Pen-testing

- OWASP ZAP (DEMO)
  - Proxy
  - Spider
  - Atacante
  - Automatización
- Burp Suite (alternativa)
- Metasploit (demasiado agresiva)
- … más muchas otras que vamos a encontrar en

https://owasp.org/www-project-web-security-testing-guide/v41/6-Appendix/A-Testing_Tools_Resource

ascentic/

6.c Ejecución de diferentes ataques

Comienza el taller