



UNIVERSIDAD AUTÓNOMA DE CHIAPAS

FACULTAD DE CONTADURÍA Y ADMINISTRACIÓN
CAMPUS 1

ING. EN DESARROLLO Y TECNOLOGÍAS DE SOFTWARE

MATERIA: Analisis De Vulnerabilidades

ACTIVIDAD: ACT. 1.1 Investigar los conceptos de vulnerabilidades:

ALUMNOS:
Gabriel Omar Fuentes Chacon

DOCENTE: : Luis Gutiérrez Alfaro

FECHA: 25/01/2023



Herramientas de vulnerabilidades:

Nmap:

Descripción: Nmap, abreviatura de Network Mapper, es una herramienta de código abierto altamente versátil utilizada para explorar y evaluar la seguridad de redes. Su funcionalidad abarca la detección de hosts, servicios y sistemas operativos en una red, proporcionando información detallada que incluye la versión de software y configuraciones específicas.

Uso común: Nmap se emplea extensamente para realizar escaneos de puertos, identificación de sistemas operativos, ejecución de scripts personalizados y exploración de servicios en una red.

Descripción: Joomscan se especializa en la identificación de vulnerabilidades específicas en sitios web desarrollados en Joomla, un sistema de gestión de contenidos. La herramienta realiza análisis de seguridad exhaustivos, buscando debilidades comunes y específicas de este CMS.

Uso común: Su aplicación principal radica en la detección de vulnerabilidades conocidas en sitios web Joomla a través de escaneos especializados.

```
3 require File.expand_path("../../config/environment", __FILE__)
4 # Prevent database truncation if the test fails
5 abort("The Rails environment is running in production mode")
6 require 'spec_helper'
7 require 'rspec/rails'
8
9 require 'capybara/rspec'
10 require 'capybara/rails'
11
12 Capybara.javascript_driver = :webkit
13 Category.delete_all; Category.create!
14 Shoulda::Matchers.configure do |config|
15   config.integrate do |with|
16     with.test_framework :rspec
17     with.library :rails
18   end
19 end
20
21 # Add additional requires below this line, as needed
22
23 # Requires supporting ruby files within the same directory as
24 # this file or explicitly
25 # run as spec/support/ and its subdirectories
26 # in _spec.rb will both be required by default
27 # run twice. It is recommended that you do not name
28 # end with _spec.rb. You can configure this
29 # option on the command line.
30 # option on the command line.
```

Herramientas de vulnerabilidades:

Wpscan:

Descripción: Wpscan se ha diseñado para evaluar la seguridad de sitios web basados en WordPress. Realiza escaneos minuciosos en busca de vulnerabilidades, configuraciones débiles y otras amenazas potenciales en la plataforma.

Uso común: Es utilizado habitualmente para identificar y corregir vulnerabilidades en sitios web que utilizan WordPress, así como para llevar a cabo auditorías de seguridad.

Nessus Essentials:

Descripción: Nessus es una herramienta integral de escaneo de vulnerabilidades que ayuda en la identificación proactiva de amenazas en sistemas informáticos. Nessus Essentials, su versión gratuita, proporciona funcionalidades avanzadas para realizar escaneos de seguridad en redes, sistemas y aplicaciones.

Uso común: Nessus Essentials se utiliza comúnmente para realizar evaluaciones de seguridad exhaustivas, identificar vulnerabilidades y fortalecer la postura de seguridad de una infraestructura.



Herramientas de vulnerabilidades:

Vega:

Descripción: Vega es una herramienta de prueba de seguridad para aplicaciones web que simplifica la identificación y explotación de vulnerabilidades. Ofrece funciones específicas para analizar sitios web en busca de fallos de seguridad, lo que facilita la corrección proactiva de las debilidades identificadas.

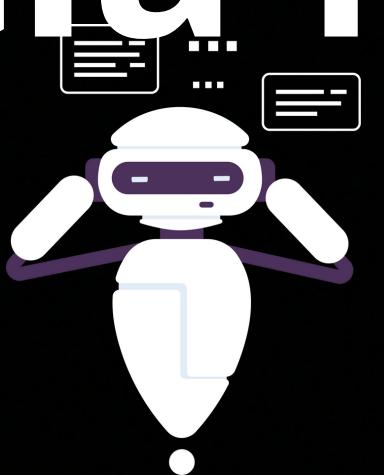


Uso común: Vega se aplica en el análisis de seguridad de aplicaciones web, proporcionando una interfaz intuitiva para identificar y abordar vulnerabilidades.

```
state={  
  products: storeProducts  
}  
  
render() {  
  return (  
    <React.Fragment>  
      <div className="py-5">  
        <div className="container">  
          <Title name="our" title="</Title>  
          <div className="row">  
            <ProductConsumer>  
              {(value) => {  
                console.log(value);  
              }}  
            </ProductConsumer>  
          </div>  
        </div>  
      </div>  
    </React.Fragment>  
  );  
}
```

Inteligencia Misceláneo:

Gobuster:



Descripción: Gobuster, una herramienta de fuerza bruta, se emplea para descubrir directorios y archivos ocultos en servidores web. Durante las fases de enumeración en pruebas de penetración, Gobuster permite identificar recursos no accesibles de manera convencional.

Uso común: Gobuster se utiliza para mejorar la comprensión de la topología de un sitio web, descubriendo recursos ocultos y áreas de posibles vulnerabilidades.

Dumpster Diving:

Descripción: Dumpster Diving involucra la búsqueda de información valiosa en desechos físicos de una organización, como documentos impresos o discos duros desecharados. Esta práctica puede revelar datos sensibles que podrían haber sido descartados de manera inadecuada.

Uso común: Se aplica para recopilar información sensible que ha sido desecharada de manera inadecuada, mejorando así la inteligencia obtenida en la fase de reconocimiento.

Inteligencia Miseláneo:

Ingeniería Social:

Descripción: La ingeniería social implica la manipulación de individuos para obtener información confidencial o realizar acciones específicas. Utiliza tácticas no tecnológicas, como engaños y manipulación psicológica, para explotar aspectos comportamentales y sociales.



Uso común: La ingeniería social se utiliza para obtener información confidencial mediante la manipulación psicológica de personas, a menudo aprovechando la confianza y la falta de conciencia de seguridad.

Inteligencia Activa:

Análisis de dispositivos y puertos con Nmap:

Descripción: Nmap se utiliza para realizar análisis activos de dispositivos y puertos en una red. Proporciona detalles sobre los servicios en ejecución y los sistemas operativos presentes, facilitando la evaluación de la postura de seguridad.

Parámetros y opciones de escaneo de Nmap:

Nmap ofrece una amplia variedad de parámetros y opciones de escaneo para personalizar exploraciones. Estos incluyen configuraciones de velocidad, rangos de puertos y otros ajustes avanzados para adaptarse a las necesidades específicas de cada escenario.



Inteligencia Activa:

Full TCP Scan:

Descripción: Un escaneo TCP completo con Nmap implica la exploración de todos los 65,535 puertos TCP posibles en un sistema. Este enfoque exhaustivo permite identificar todos los servicios en ejecución, brindando una visión completa de la infraestructura.

Stealth Scan:

Descripción: El "Stealth Scan" en Nmap, conocido también como escaneo sigiloso, busca minimizar la detección al no enviar paquetes que puedan alertar a los sistemas de seguridad. Esta técnica es valiosa en entornos sensibles a la detección de escaneos intrusivos.

Fingerprinting:

Descripción: El fingerprinting implica la identificación de servicios y sistemas operativos en una red mediante el análisis de las respuestas de los servicios a paquetes específicos. Esto permite obtener información detallada sobre las configuraciones y versiones de software presentes.

Inteligencia Activa:

Zenmap:

Descripción: Zenmap, una interfaz gráfica de usuario para Nmap, simplifica la configuración y ejecución de escaneos de seguridad. Proporciona una representación visual de los resultados, facilitando la interpretación y el análisis de la información recopilada.

Análisis Traceroute:

Descripción: El análisis de traceroute implica rastrear la ruta que sigue un paquete de datos desde el origen hasta el destino. Muestra todos los nodos intermedios (routers) a lo largo del camino, proporcionando una visión detallada de la topología de la red y posibles puntos de congestión o vulnerabilidades.

BIBLIOGRAFIA

Saucedo, A. L. H., & Miranda, J. M. (2015). Guía de ataques, vulnerabilidades, técnicas y herramientas para aplicaciones web. ReCIBE. Revista electrónica de Computación, Informática, Biomédica y Electrónica, (1).

Franco, D. A., Perea, J. L., & Tovar, L. C. (2013). Herramienta para la Detección de Vulnerabilidades basada en la Identificación de Servicios. Información tecnológica, 24(5), 13-22.