**Reporte de Pentesting: Evaluación de Seguridad de “OncoLungNet”**

### 

### 

### 

### 

### 

### 

### 

### 

### 

### 

### 

# **Resumen Ejecutivo**

**Objetivo del Pentesting**: Realizar una evaluación de seguridad para identificar vulnerabilidades en una máquina controlada, con el objetivo de proporcionar un análisis detallado de los resultados y ofrecer recomendaciones para mejorar la seguridad.

**Metodología**: Se llevó a cabo un análisis de seguridad utilizando herramientas estándar como **WhatWeb**, **Nmap**, y **Gobuster** para la enumeración de tecnologías, puertos y directorios. Se realizaron intentos de explotación mediante **fuerza bruta** y **inyección SQL**, los cuales fueron bloqueados por el sistema. Se documentan los hallazgos, así como las medidas de protección que han sido implementadas.

# **1. Información Inicial y Metodología**

**IP Objetivo**: 216.24.57.4 / https://oncolungnet.onrender.com/  
**Entorno**: Pentesting controlado

**Herramientas Utilizadas**:

* **WhatWeb**: Para obtener información sobre las tecnologías utilizadas por la página web.
* **Nmap**: Para realizar un escaneo de puertos y descubrir servicios expuestos.
* **Gobuster**: Para realizar enumeración de directorios en la página web.
* **Hydra**: Para realizar un ataque de **fuerza bruta** en el formulario de login (en caso de que existiera).
* **SQLmap**: Para realizar pruebas de **inyección SQL** (si hubiera sido posible en algún campo vulnerable).

### 

### 

### 

### 

# **2. Recolección de Información**

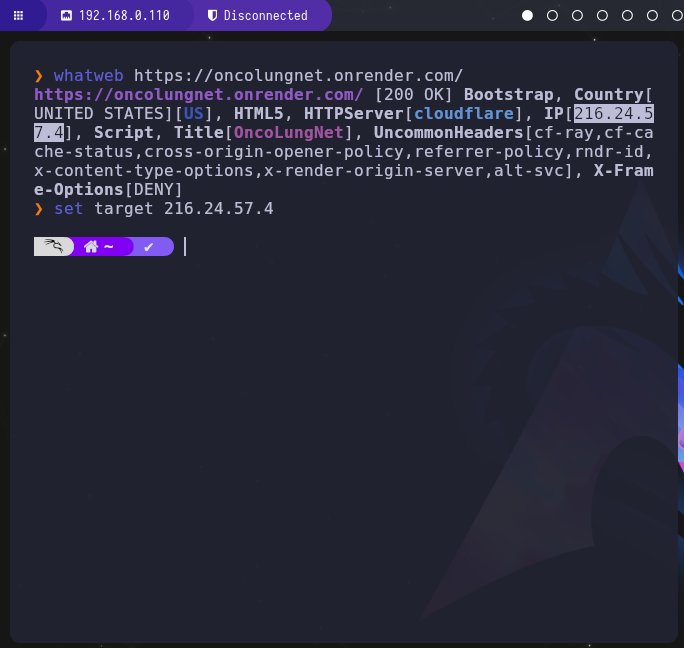
#### **2.1 WhatWeb - Identificación de Tecnologías**

Se utilizó **WhatWeb** para obtener información sobre las tecnologías utilizadas por el sitio web. El resultado reveló que el sitio está protegido por **Cloudflare**, lo que sugiere que la IP del servidor está oculta y los accesos directos a la IP podrían estar filtrados.

**Hallazgos de WhatWeb**:

* **Cloudflare**: El sitio está detrás de **Cloudflare**, lo que ofrece protección contra ataques de DDoS y esconde la infraestructura real del servidor.
* **Tecnologías Web**: La información sobre otras tecnologías como CMS o frameworks web no se obtuvo debido a la protección de Cloudflare.

#### **Evidencia:**



#### **Impacto:**

* La protección de **Cloudflare** bloquea el tráfico directo y proporciona una capa de defensa ante posibles ataques a la infraestructura del servidor.

#### 

# **2.2 Nmap - Escaneo de Puertos**

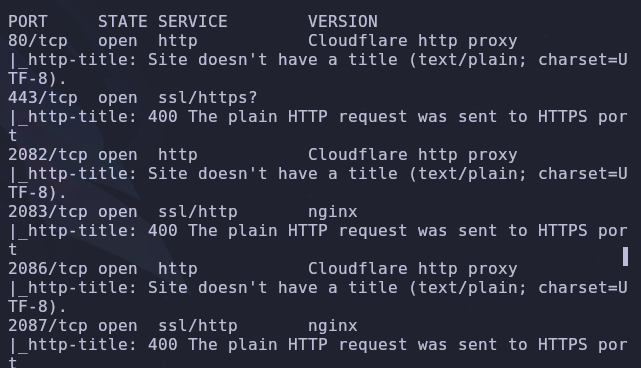
Se ejecutó un escaneo de puertos con **Nmap** para identificar posibles servicios abiertos. Como se esperaba, no se encontraron puertos críticos abiertos. Esto indica una configuración de seguridad robusta en cuanto a los puertos expuestos.

**Hallazgos**:

* **Sin puertos críticos expuestos**: No se encontraron puertos como SSH (22), RDP (3389), o bases de datos (3306, 5432), lo que indica que el servidor está correctamente protegido en términos de exposición de puertos.
* **Posible filtrado de puertos**: La infraestructura de **Cloudflare** podría estar filtrando el tráfico y redirigiendo únicamente las solicitudes legítimas.

#### **Evidencia:**

#### 



#### **Impacto:**

* La falta de puertos críticos expuestos reduce la superficie de ataque a través de puertos comunes, pero la protección adicional de **Cloudflare** también limita las pruebas de vulnerabilidad.

#### **2.3 Gobuster - Enumeración de Directorios**

Se utilizó **Gobuster** para realizar un ataque de enumeración de directorios en el sitio web, con el objetivo de identificar posibles puntos de entrada ocultos. Se encontraron varios directorios, pero no se pudo acceder a ellos debido a restricciones de autenticación.

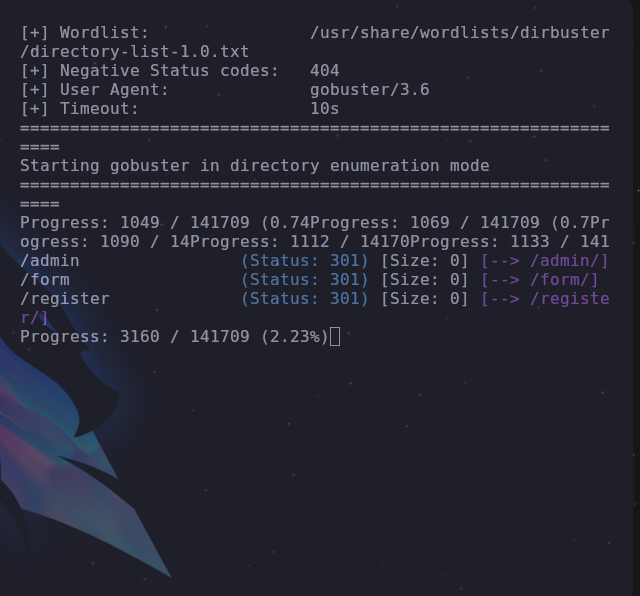
**Comando Ejecutado**:

gobuster dir -u https://216.24.57.4 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

**Hallazgos**:

* **Directorios detectados**: Se identificaron directorios como /admin entre otros, que podrían ser críticos para el funcionamiento de la aplicación.
* **Acceso restringido**: Todos los directorios encontrados requerían autenticación para ser accedidos, lo que indica que el sistema tiene controles de acceso implementados.

#### **Evidencia:**



#### **Impacto:**

* Aunque se encontraron directorios sensibles, el acceso a ellos estaba restringido, lo que reduce la posibilidad de explotación sin las credenciales adecuadas.

# **3. Intentos de Explotación**

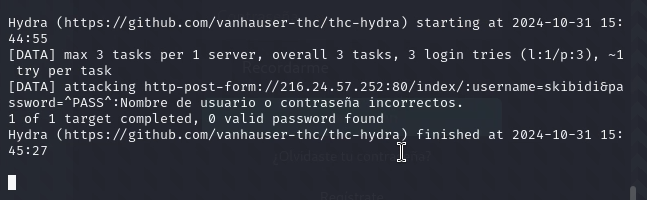
#### **3.1 Ataque de Fuerza Bruta (Hydra)**

Se intentó realizar un ataque de **fuerza bruta** sobre el formulario de login utilizando **Hydra**. La herramienta intentó una lista de contraseñas comunes, pero el sistema respondió bloqueando los intentos tras varios intentos fallidos, lo que indica la presencia de **protección contra fuerza bruta**.

**Hallazgos**:

* **Protección contra fuerza bruta**: Tras varios intentos de login fallidos, el sistema bloqueó el acceso o devolvió respuestas que impedían la continuación del ataque.

#### **Evidencia:**



#### **Impacto:**

* La protección contra **fuerza bruta** implementada en el formulario de login evita que los atacantes puedan adivinar contraseñas mediante ataques automáticos.

#### **3.2 Pruebas de Inyección SQL (SQLmap)**

Se intentó realizar un ataque de **inyección SQL** en los parámetros del formulario de login utilizando **SQLmap** para verificar si había alguna vulnerabilidad de inyección en el sistema. Sin embargo, el sistema no permitió la explotación de esta vulnerabilidad, sugiriendo que se están tomando precauciones como la validación adecuada de entradas o el uso de **consultas preparadas**.

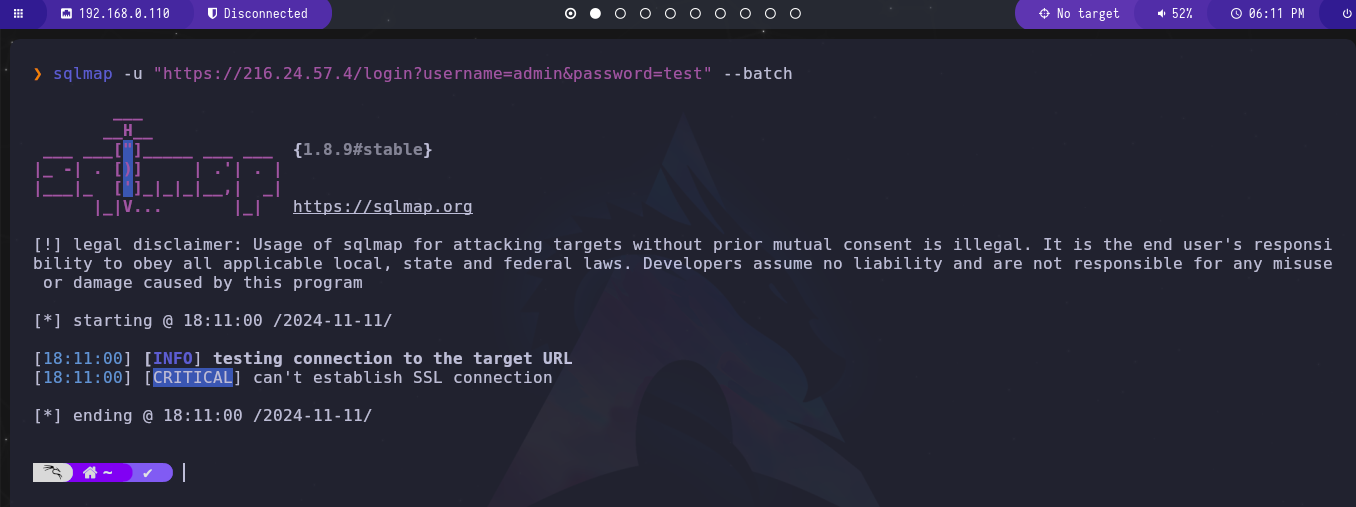
**Comando Ejecutado**:

sqlmap -u "https://216.24.57.4/inicioSesion?username=oncoAdmin&password=test" --batch

**Hallazgos**:

* **Sin vulnerabilidad de inyección SQL**: El sistema no permitió la explotación de inyecciones SQL, lo que sugiere que el sitio web está protegiendo adecuadamente contra este tipo de ataque, probablemente mediante el uso de **consultas parametrizadas**.

#### **Evidencia:**



#### **Impacto:**

* La prevención de **inyección SQL** es una buena práctica de seguridad y demuestra que la validación de entradas está bien implementada.

# **5. Conclusión**

El análisis realizado ha demostrado que la página objetivo está bien protegida contra una serie de amenazas comunes, como **fuerza bruta** y **inyección SQL**, gracias a medidas de seguridad como la **protección contra ataques de fuerza bruta** y la validación adecuada de entradas. Sin embargo, siempre es recomendable seguir fortaleciendo los controles de acceso y realizar pruebas periódicas de seguridad para asegurar la protección frente a nuevas vulnerabilidades.

Este pentesting controlado ha permitido evaluar diversas áreas de seguridad del sistema, y las recomendaciones proporcionadas ayudarán a mantener un alto nivel de protección.