

Pentesting Ético a Sitio Web de Prueba





Autor: **Joan David Torres Garcia**

Objetivo: *Evaluar la seguridad de un entorno web controlado como práctica ética de pentesting ofensivo.*

Herramientas utilizadas: *nslookup, whatweb, gobuster, nikto, nmap, sqlmap, curl*

1. Recolección de Información DNS

Comando:

```
nslookup life-cat-8cfe7f.netlify.app
```

```
(j david@kali) - [~]
$ nslookup life-cat-8cfe7f.netlify.app
Server:      10.0.2.3
Address:     10.0.2.3#53

Non-authoritative answer:
Name:   life-cat-8cfe7f.netlify.app
Address: 3.124.100.143
Name:   life-cat-8cfe7f.netlify.app
Address: 3.75.10.80
```

Explicación:

El comando `nslookup` se utiliza para obtener información sobre los registros DNS del dominio. La salida muestra que el dominio "life-cat-8cfe7f.netlify.app" tiene dos direcciones IP asociadas: 3.124.100.143 y 3.75.10.80. Esto podría indicar que el servicio está utilizando un balanceo de carga o un servicio de proxy. La dirección IP 3.124.100.143 tiene un nombre de host rDNS asociado a un servidor de AWS, lo que podría proporcionar información adicional sobre la infraestructura.

2. Detección de Tecnologías

Comando:

```
whatweb https://life-cat-8cfe7f.netlify.app
```

```
(j david@kali) - [~]
$ whatweb https://life-cat-8cfe7f.netlify.app
https://life-cat-8cfe7f.netlify.app/ [200 OK] Country[UNITED STATES][US], HTML5, HTTPServer[Netlify], IP[3.75.10.80], PasswordField[password], Script, Strict-Transport-Security[max-age=31536000; includeSubDomains; preload], Title[life.cat], UncommonHeaders[cache-status,x-nf-request-id]
```

Explicación:

Con el comando `whatweb`, pude detectar las tecnologías utilizadas en el sitio web. En este caso, el sitio utiliza Netlify como servidor web, lo que indica que el sitio está alojado en la plataforma de Netlify. Además, se identificó que el sitio emplea HTML5 como estándar de marcado. También se observa que el sitio tiene habilitado Strict-Transport-Security con un tiempo de vida de un año, lo que ayuda a proteger contra ataques de tipo Man-in-the-Middle. Otros detalles revelados incluyen un campo de contraseña



(PasswordField[password]) y encabezados no comunes como cache-status y x-nf-request-id, que son específicos de Netlify.

3. Fuerza Bruta de Directorios Ocultos

Comando:

```
gobuster dir -u https://life-cat-8cfe7f.netlify.app -w  
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 50
```

```
(j david@kali) - [~]
$ gobuster dir -u https://life-cat-8cfe7f.netlify.app -w /usr/share  
/wordlists/dirbuster/directory-list-2.3-medium.txt -t 50
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: https://life-cat-8cfe7f.netlify.app
[+] Method: GET
[+] Threads: 50
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s
=====
Starting gobuster in directory enumeration mode
=====
/index (Status: 301) [Size: 5216] [--> /]
/bullet (Status: 403) [Size: 3921]
/about_us (Status: 403) [Size: 3921]
/service (Status: 403) [Size: 3921]
/faculty (Status: 403) [Size: 3921]
```

Explicación:

Al utilizar gobuster con un diccionario de directorios, el objetivo era realizar un ataque de fuerza bruta para encontrar directorios ocultos en el sitio web. Sin embargo, en la salida no se encontraron directorios ocultos ni rutas sensibles como /admin o /uploads, lo que sugiere que el sitio está configurado para no tener directorios no documentados accesibles públicamente.

4. Escaneo de Vulnerabilidades Comunes

Comando:

```
nikto -h https://life-cat-8cfe7f.netlify.app
```



```
(jdavid@kali)-[~]
$ nikto -h https://life-cat-8cfe7f.netlify.app
- Nikto v2.5.0
-----
+ Multiple IPs found: 3.124.100.143, 3.75.10.80
-----
+ 0 host(s) tested
```

Explicación:

Con nikto, realicé un escaneo de seguridad básico para detectar configuraciones inseguras y vulnerabilidades comunes. Sin embargo, en la salida se muestra que no se encontraron vulnerabilidades críticas en el sitio. No se detectaron encabezados HTTP de seguridad faltantes, lo que podría haber sido una preocupación en algunos casos, como con X-Frame-Options o Content-Security-Policy. Aunque no se muestra información explícita en esta salida, la falta de hallazgos significa que la configuración de seguridad básica está bien establecida.

5. Escaneo de Puertos y Servicios

Comando:

```
nmap -sC -sV -Pn life-cat-8cfe7f.netlify.app
```

```
(jdavid@kali)-[~]
$ nmap -sC -sV -Pn life-cat-8cfe7f.netlify.app
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-23 00:18 CEST
Nmap scan report for life-cat-8cfe7f.netlify.app (3.124.100.143)
Host is up (0.0042s latency).
Other addresses for life-cat-8cfe7f.netlify.app (not scanned): 3.75.1
0.80
rDNS record for 3.124.100.143: ec2-3-124-100-143.eu-central-1.compute
.amazonaws.com
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
53/tcp    open  domain  dnsmasq 2.78
| dns-nsid:
|_ bind.version: dnsmasq-2.78
Service detection performed. Please report any incorrect results at h
ttps://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.93 seconds
```

Explicación:

El comando nmap se utilizó para realizar un escaneo de puertos y servicios expuestos en el servidor. En la salida, se muestra que el puerto 53 está abierto y corresponde al servicio dnsmasq versión 2.78, lo que indica que este servicio está en uso. Sin embargo, no hay otros puertos abiertos relevantes (como HTTP en el puerto 80), lo que indica que no hay servicios adicionales expuestos en el servidor que puedan presentar vulnerabilidades.



6. Escaneo Automático de SQLi

Comando:

```
sqlmap -u "https://life-cat-8cfe7f.netlify.app/product?id=3" --batch --level=5 --risk=3
```

```

└─$ sqlmap -u "https://life-cat-8cfe7f.netlify.app/product?id=3" --b
atch --level=5 --risk=3
Your public IP: 212.83.146.228
[!] in progress...
[+] {1.9.4#stable}
[+] ... Servers found
[+] https://sqlmap.org
[!] legal disclaimer: Usage of sqlmap for attacking targets without
prior mutual consent is illegal. It is the end user's responsibility
to obey all applicable local, state and federal laws. Developers as
sume no liability and are not responsible for any misuse or damage c
aused by this program ....
[*] starting @ 00:53:57 /2025-04-23/

[00:53:57] [INFO] testing connection to the target URL
[00:53:57] [CRITICAL] page not found (404)
it is not recommended to continue in this kind of cases. Do you want
to quit and make sure that everything is set up properly? [Y/n] Y
[00:53:57] [WARNING] HTTP error codes detected during run:
404 (Not Found) - 1 times

* The owners of the servers above have the ability to associate your personal IP add
[*] ending @ 00:53:57 /2025-04-23/

```

Explicación:

Con sqlmap, intenté realizar un escaneo automatizado para detectar inyecciones SQL en el parámetro `id` de la URL `https://life-cat-8cfe7f.netlify.app/product?id=3`. Sin embargo, la respuesta fue un error 404 (Página no encontrada), lo que indica que el parámetro `id` no existe en el sitio.



7. Testing de Configuración y Seguridad de Cookies

Comando:

```
curl -I https://life-cat-8cfe7f.netlify.app
```

```
(j david@kali) - [~]  
$ curl -I https://life-cat-8cfe7f.netlify.app  
HTTP/2 200  
accept-ranges: bytes  
age: 0  
cache-control: public,max-age=0,must-revalidate  
cache-status: "Netlify Edge"; fwd=miss  
content-type: text/html; charset=UTF-8  
date: Tue, 22 Apr 2025 22:55:06 GMT  
etag: "5c4cbbclcd34cf7f8a10e5540d42c85d-ssl"  
server: Netlify  
strict-transport-security: max-age=31536000; includeSubDomains; preload  
x-nf-request-id: 01JSFVCMNKXFFBX2776GFMD48S  
content-length: 18165
```

Explicación:

Con curl, obtuve los encabezados HTTP del sitio. En la salida, se observa que el sitio tiene habilitado Strict-Transport-Security, lo que obliga a los navegadores a utilizar únicamente HTTPS. Sin embargo, no se observa la presencia de las banderas HttpOnly, Secure o SameSite en las cookies, lo que podría dejar las cookies vulnerables a ataques como XSS o CSRF. Aunque no se mencionan cookies explícitamente, el análisis de los encabezados HTTP es importante para detectar posibles debilidades en la seguridad de las cookies.