Tabla de Contenido

1. Objetivo

El documento presentado a continuación tiene como objetivo elaborar un análisis de vulnerabilidades a un Cliente https://interceramic.com, incluyendo los puertos que se encuentran abiertos al público, las versiones de software de los servicios, recomendaciones de seguridad y posibles planes de ataque que se podrían utilizar.

2. Análisis

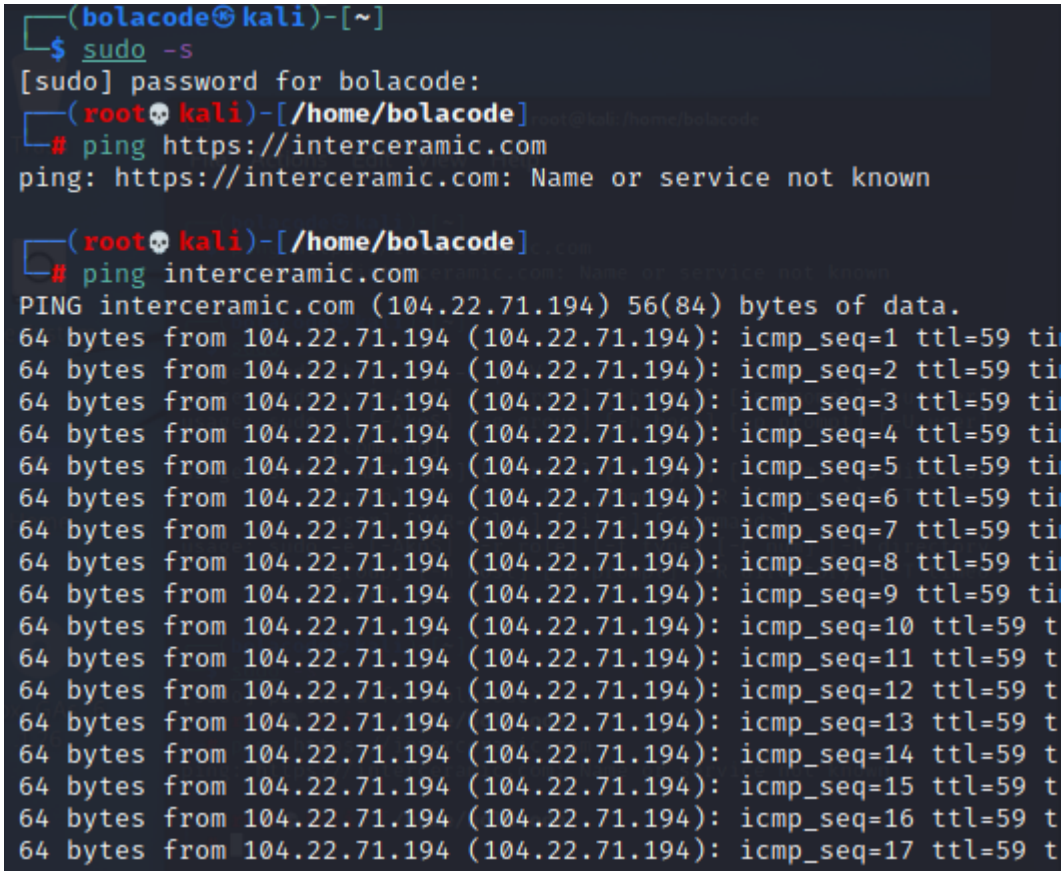


Imagen 1

El primer paso que se realizó en el análisis fue hacer un *ping* a la página del cliente en este caso https://interceramic.com con el objetivo de obtener su dirección IP (véase en la imagen 1).

```
--- interceramic.com ping statistics ---
550 packets transmitted, 548 received, 0.363636% packet loss, time 559227ms
rtt min/avg/max/mdev = 6.543/23.912/1029.677/48.350 ms, pipe 2

┌──(root💀kali)-[/home/bolacode]
└─# nmap -sn 104.22.71.194
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-08 23:35 CST
Nmap scan report for 104.22.71.194
Host is up (0.0021s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.14 seconds
```

Imagen 2

Analizando los dominios y entrando a las direcciones IP es posible concluir que cuentan con un servicio de Cloudflare network, (véase en la imagen 2).

En esta ocasión solo se está evaluando la seguridad de una página en específico: https://interceramic.com

```
┌──(root💀kali)-[/home/bolacode]
└─# nmap -sS 104.22.71.194
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-09 00:19 CST
Nmap scan report for 104.22.71.194
Host is up (0.0072s latency).
Not shown: 996 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
8080/tcp open  http-proxy
8443/tcp open  https-alt

Nmap done: 1 IP address (1 host up) scanned in 4.55 seconds
```

.

Imagen 3

Al escanear los puertos disponibles de la dirección IP, se obtuvieron puertos de servicios como TCP, ID, entre otros (véase en la imagen 3).

Es posible visualizar un poco de información al entrar a algunos de estos puertos, mientras que otros solo se encuentran totalmente restringidos.

Se logró entrar de forma directa en el navegador a los siguientes puertos:

- **80**

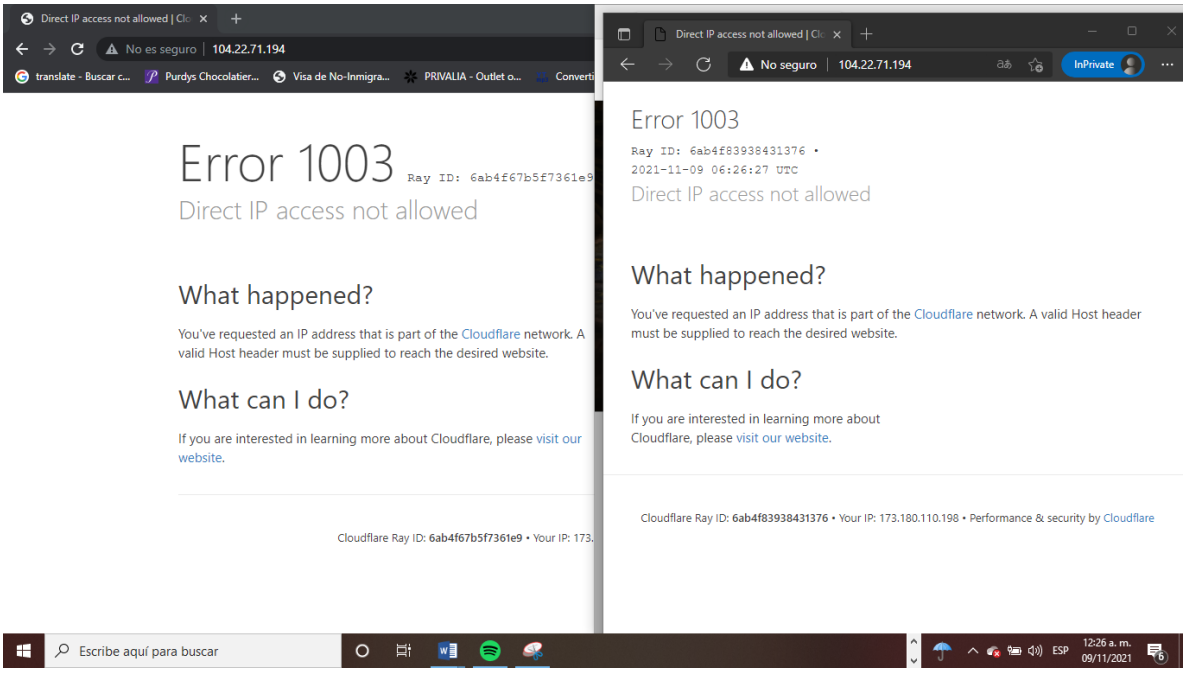


Imagen 4

- **443**

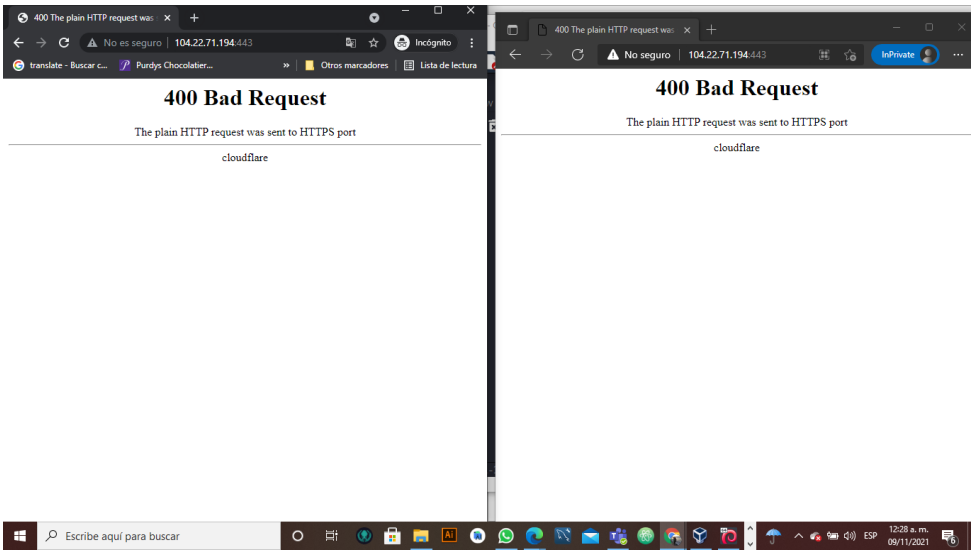


Imagen 5

- **8443**

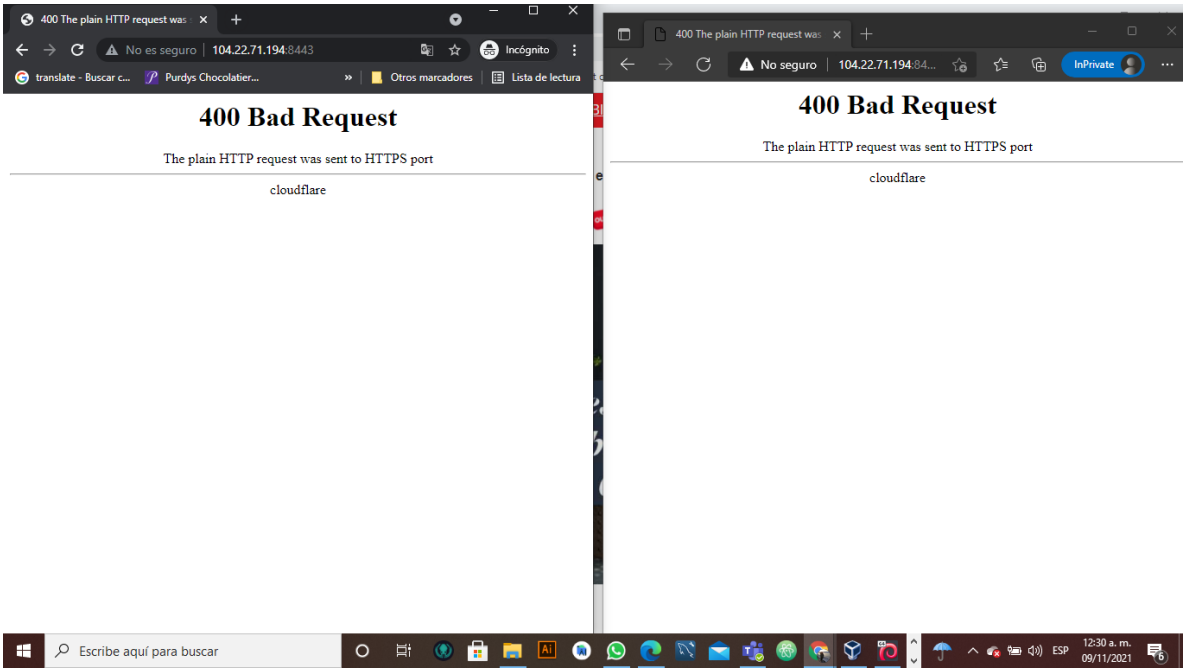


Imagen 6

- **8080**

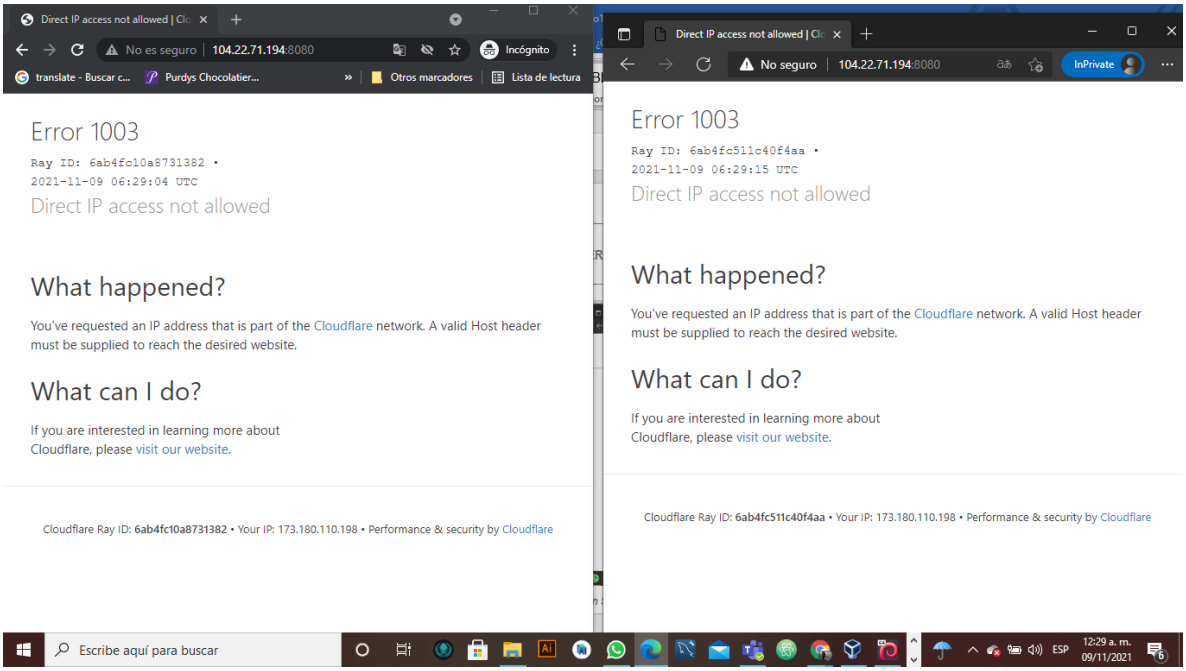


Imagen 7

3. Plan de ataque

Con la información disponible hasta el momento, es posible realizar muy pocas formas de ataque para intentar vulnerar el sitio web. Por el momento el más probable:

1. Ataque de fuerza bruta para credenciales de acceso de SSH: al comprobar que el puerto 22 se encuentra abierto (véase en la imagen 8), probablemente se pueda lanzar un ataque con la herramienta Hydra la cual viene incluida con Kali Linux y sirve para tratar de dar las credenciales de acceso. Para poder usar este método se necesita un diccionario para los posibles nombres de usuario y otro para las posibles contraseñas.

   Para poder dar el ataque don hydra se utiliza este comando:

   `hydra -L user.txt -P pass.txt 104.22.71.194 ssh`

   El “user.txt” representa los nombres de usuario y “pass.txt” las contraseñas.

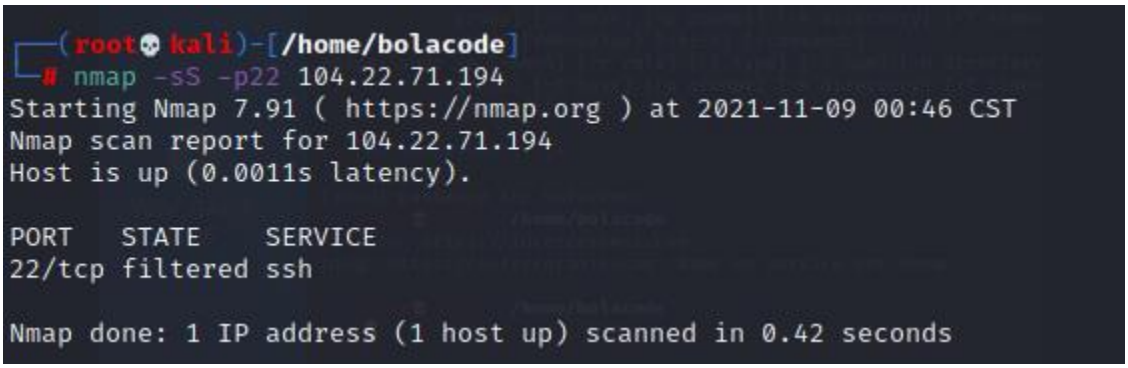
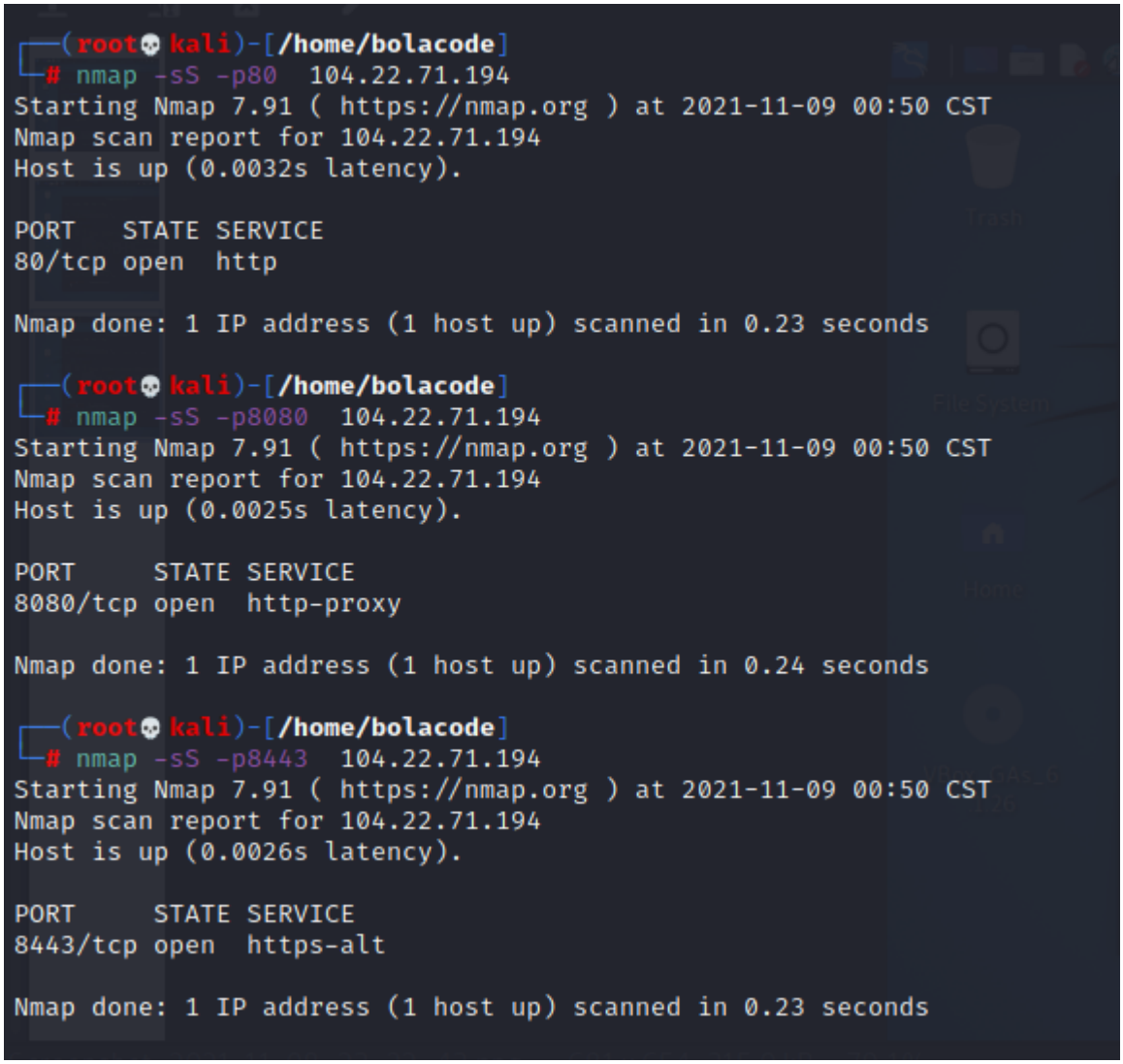


Imagen 8

2. En los demás puertos no hay tanto de donde poder sacarles información por lo que solo se analizaron, pero no hay realmente una amenaza que se pueda desarrollar para esos puertos (véase en la imagen 9 y 10).


┌──(root💀kali)-[/home/bolacode]
└─# nmap -sS -p80 104.22.71.194
Starting Nmap 7.91 (https://nmap.org) at 2021-11-09 00:50 CST
Nmap scan report for 104.22.71.194
Host is up (0.0032s latency).
PORT STATE SERVICE
80/tcp open http
Nmap done: 1 IP address (1 host up) scanned in 0.23 seconds
┌──(root💀kali)-[/home/bolacode]
└─# nmap -sS -p8080 104.22.71.194
Starting Nmap 7.91 (https://nmap.org) at 2021-11-09 00:50 CST
Nmap scan report for 104.22.71.194
Host is up (0.0025s latency).
PORT STATE SERVICE
8080/tcp open http-proxy
Nmap done: 1 IP address (1 host up) scanned in 0.24 seconds
┌──(root💀kali)-[/home/bolacode]
└─# nmap -sS -p8443 104.22.71.194
Starting Nmap 7.91 (https://nmap.org) at 2021-11-09 00:50 CST
Nmap scan report for 104.22.71.194
Host is up (0.0026s latency).
PORT STATE SERVICE
8443/tcp open https-alt
Nmap done: 1 IP address (1 host up) scanned in 0.23 seconds

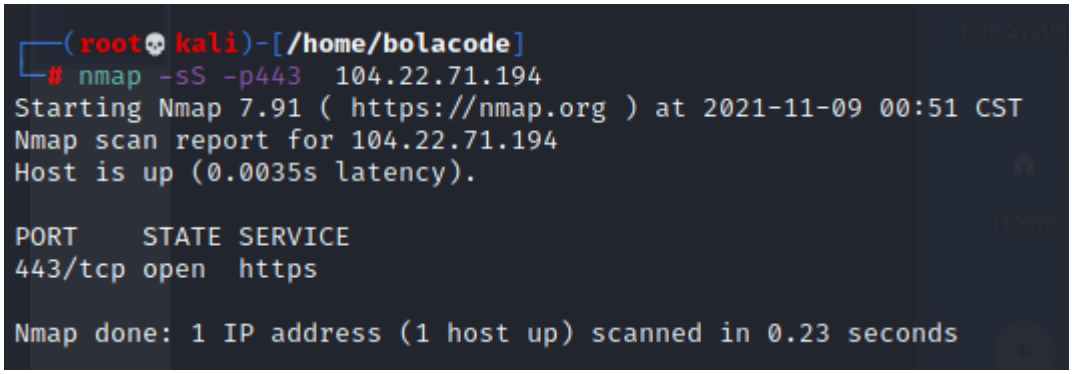

┌──(root💀kali)-[/home/bolacode]
└─# nmap -sS -p443 104.22.71.194
Starting Nmap 7.91 (https://nmap.org) at 2021-11-09 00:51 CST
Nmap scan report for 104.22.71.194
Host is up (0.0035s latency).
PORT STATE SERVICE
443/tcp open https
Nmap done: 1 IP address (1 host up) scanned in 0.23 seconds

Imagen 9 y 10

4. Análisis de vulnerabilidades

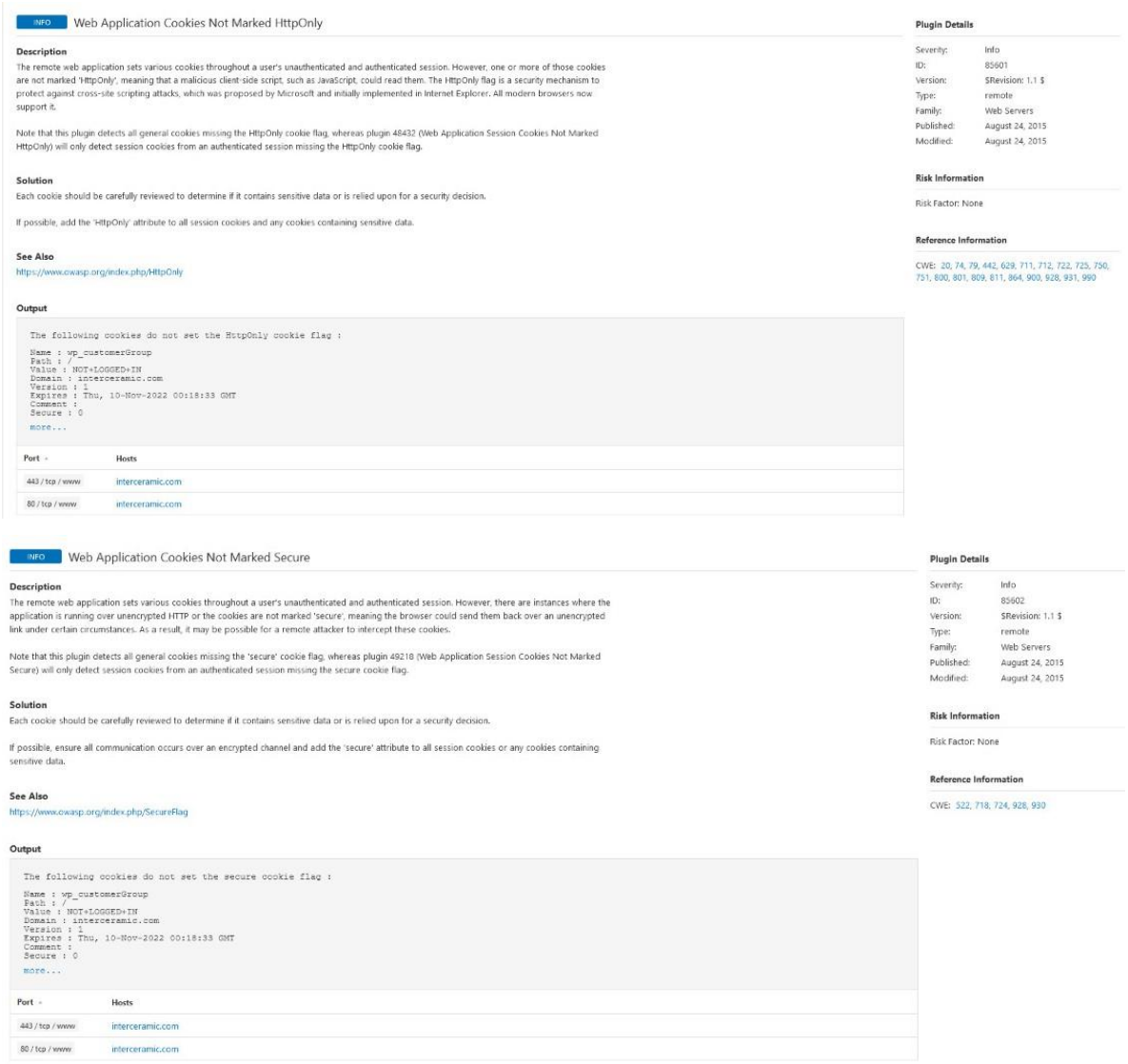
En esta sección, se muestran todos los riesgos y problemas de seguridad identificados durante el análisis del Cliente https://interceramic.com los cuales fueron analizados usando el software Nessus.

Cada una de las vulnerabilidades cuenta con recomendaciones para mitigar la vulnerabilidad y mejorar la seguridad general del software del Cliente.

4.1 Puertos abiertos.

Impacto: Durante el análisis recabamos que hay varios puertos abiertos para cualquier tipo de IP, estos al estar abiertos pueden ser vulnerables a ataques imprevistos.

Recomendación: Cerrar y bloquear lo antes posible los puertos que estén abiertos y que no se necesiten tener abiertos al público en general, ya que al estar abiertos son un vulnerables para cualquier tipo de atacante.



INFO Web Application Cookies Not Marked HttpOnly

Description

The remote web application sets various cookies throughout a user's unauthenticated and authenticated session. However, one or more of those cookies are not marked 'HttpOnly', meaning that a malicious client-side script, such as JavaScript, could read them. The HttpOnly flag is a security mechanism to protect against cross-site scripting attacks, which was proposed by Microsoft and initially implemented in Internet Explorer. All modern browsers now support it.

Note that this plugin detects all general cookies missing the HttpOnly cookie flag, whereas plugin 48432 (Web Application Session Cookies Not Marked HttpOnly) will only detect session cookies from an authenticated session missing the HttpOnly cookie flag.

Solution

Each cookie should be carefully reviewed to determine if it contains sensitive data or is relied upon for a security decision.

If possible, add the 'HttpOnly' attribute to all session cookies and any cookies containing sensitive data.

See Also

https://www.owasp.org/index.php/HttpOnly

Output

```
The following cookies do not set the HttpOnly cookie flag :

Name : wp_customerGroup
Path : /
Value : NOT+LOGGED+IN
Domain : interceramic.com
Version : 1
Expires : Thu, 10-Nov-2022 00:18:33 GMT
Comment :
Secure : 0
more...
```

Port	Hosts
443 / tcp / www	interceramic.com
80 / tcp / www	interceramic.com

Plugin Details

Severity:	Info
ID:	85601
Version:	$Revision: 1.1 $
Type:	remote
Family:	Web Servers
Published:	August 24, 2015
Modified:	August 24, 2015

Risk Information

Risk Factor: None

Reference Information

CWE: 20, 74, 79, 442, 629, 711, 712, 722, 725, 750, 751, 800, 801, 809, 811, 864, 900, 928, 931, 990

INFO Web Application Cookies Not Marked Secure

Description

The remote web application sets various cookies throughout a user's unauthenticated and authenticated session. However, there are instances where the application is running over unencrypted HTTP or the cookies are not marked 'secure', meaning the browser could send them back over an unencrypted link under certain circumstances. As a result, it may be possible for a remote attacker to intercept these cookies.

Note that this plugin detects all general cookies missing the 'secure' cookie flag, whereas plugin 49218 (Web Application Session Cookies Not Marked Secure) will only detect session cookies from an authenticated session missing the secure cookie flag.

Solution

Each cookie should be carefully reviewed to determine if it contains sensitive data or is relied upon for a security decision.

If possible, ensure all communication occurs over an encrypted channel and add the 'secure' attribute to all session cookies or any cookies containing sensitive data.

See Also

https://www.owasp.org/index.php/SecureFlag

Output

```
The following cookies do not set the secure cookie flag :

Name : wp_customerGroup
Path : /
Value : NOT+LOGGED+IN
Domain : interceramic.com
Version : 1
Expires : Thu, 10-Nov-2022 00:18:33 GMT
Comment :
Secure : 0
more...
```

Port	Hosts
443 / tcp / www	interceramic.com
80 / tcp / www	interceramic.com

Plugin Details

Severity:	Info
ID:	85602
Version:	$Revision: 1.1 $
Type:	remote
Family:	Web Servers
Published:	August 24, 2015
Modified:	August 24, 2015

Risk Information

Risk Factor: None

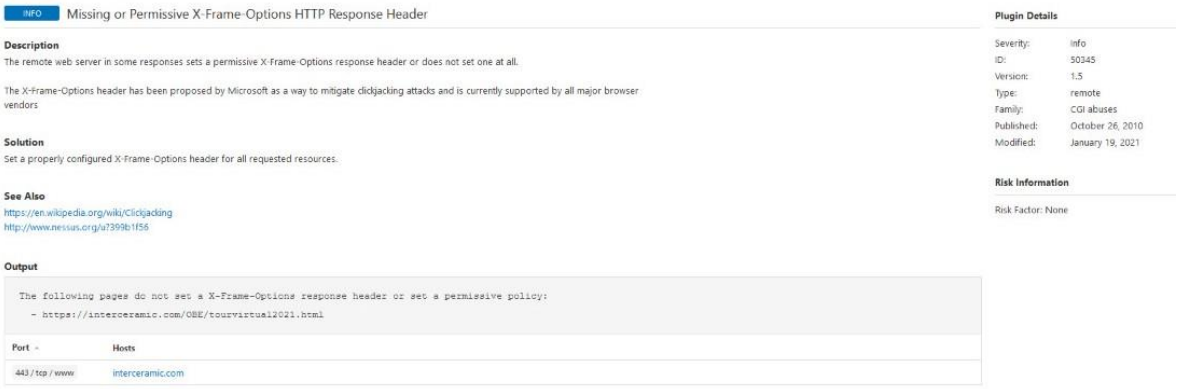
Reference Information

CWE: 522, 718, 724, 928, 930

4.2 Las *cookies* no son seguras

Impacto: Las cookies en cuestión no están señaladas como Secure y también no marcan el HttpOnly por lo que los navegadores en cuestión podrían cometer el error de usarlas sin encriptar y con un script estas se podrían leer por la persona que quiera lanzar un ataque.

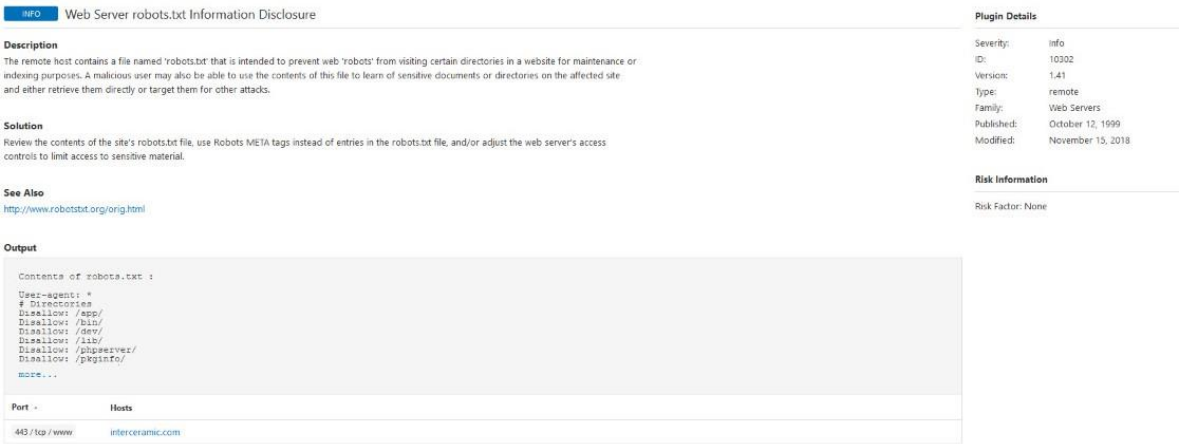
Recomendación: Se deberían de asegurar de que las cookies manejen información sensible o no todas sean etiquetas como seguras para que se mantengan encriptadas.



4.3 No se tienen directivas de X-Frame

Impacto: No cuenta con las medidas necesarias para un apartado X-frame-, por lo que el cliente podría quedar expuesto a ataques de **clickjacking** el cual por medio engañoso podría sacar información del usuario.

Recomendación: Necesitarían tener una política de seguridad de contenido la cual debería ser no permisiva por medio de X-frame.



4.4 Archivo robots.txt disponible para el público

Impacto: El archivo robots.txt, sirve para evitar los ataques de bots, los cuales son comunes en ciertas partes del sitio, este por el momento se encuentra público, por cual cualquier atacante podría ver el archivo y así obtener información sensible del cliente.

Recomendación: Es de suma importancia bloquear el archivo robots.txt al público.

5. Recomendaciones generales

Las recomendaciones para el cliente son darle prioridad a cerrar todos los puertos abiertos, ya que al estar abiertos podrían ser vulnerables a ataques por ese medio, así como también mejorar el manejo de cookies ya que compromete la información. Es muy importante arreglar y darles solución a esos detalles ya que al ser una página que cuenta con tienda en línea, esta recaba información sensible y comprometedora de todos los compradores, tales como direcciones, teléfonos, información de pago etc. Hay que tener mucho cuidado con el resguardo correcto de esa información ya que al pasar por un ataque podría afectar no solo a la tienda en línea si no a los clientes de esta en caso de que esa información pase por las manos equivocadas.

6. Elaboración y creación

Nombre y Cargo	Fecha	Rol
Hanna Siddhartha Lizarraga Ceballos Encargada de Seguridad de la Información	07/11/21	Se Redactó y agrego contenido.

7. Historial de cambios

Revisión	Descripción del cambio	Responsable	Fecha
01	Creación de documento	Hanna Siddhartha Lizarraga Ceballos	07/11/21