



maristak

Durango Ikastetxea



GRUPO2

LIHER.R

JON.H

ANDONI.I

INFORME DE AUDITORIA EXTERNO

Auditoria básica maristak.com

Introducción:

En el presente informe se pretende resaltar las vulnerabilidades de la página web **www.maristak.com**. Se utilizarán diversas técnicas de penetración, para poder averiguar dichas vulnerabilidades, así como la forma de solucionarlas. Se adjuntará una captura de pantalla, para una información más clarificada.

Por otro lado, las técnicas y herramientas utilizadas han sido aprobadas por el cliente, para su uso en dicho objetivo. Cualquier uso que se haga de las mismas, por parte no profesional, podría estar incurriendo en un delito, tipificado en el código penal.

El informe es realizado como auditoría de seguridad de la página antes mencionada, para su posterior actualización y subsanación de los errores aquí encontrados. En ningún caso, la información que de aquí se pueda sacar, será utilizada por la empresa contratada, bajo ningún concepto.

Toda la información aquí recogida es estrictamente CONFIDENCIAL.



Índice

1.- Objetivo y Alcance	4
2.- Sumario Ejecutivo	5
3.- Recopilación de Información	6
3.1 _WHOIS	6
3.2 _MALTEGO	8
3.3 _NMAP	9
3.4 _NESSUS	11
3.5 _OWAS ZAP	13
4.- Detalle de resultado técnicos	14
5. - Vulnerabilidades y Explotación	17
5.1 _Criterio de clasificación de vulnerabilidades	17
5.2 _Resumen de vulnerabilidades detectadas.	18
5.2.1 _OpenSSH.....	19
5.2.2 _Nginx (http)	20
5.2.3 _Apache httpd 2.4.52.....	22
5.2.4 _Injeccion SQL	24
5.2.5 _ HTTP access information leak	26
7.- Conclusión	28

1.- Objetivo y Alcance:

El objetivo de este análisis de seguridad es conocer el estado de seguridad de la información de la infraestructura de tecnologías de la información y las comunicaciones de la aplicación web listada a continuación:

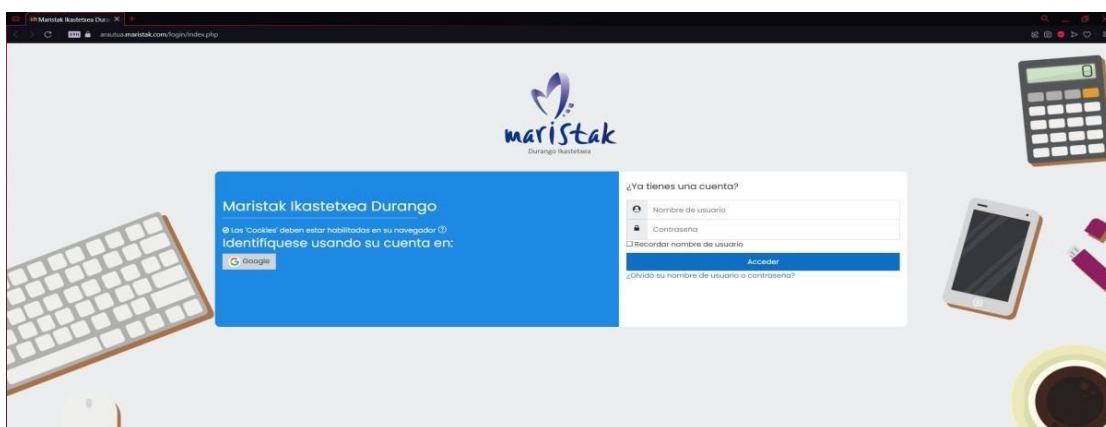
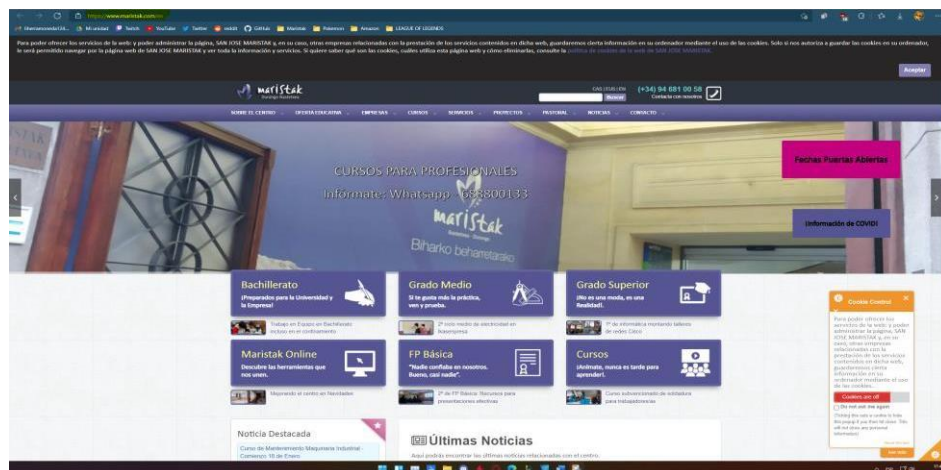
El alcance será hacia el servidor web maristak, además de los subdominios que encontremos mediante la siguiente dirección de red:

www.maristak.com

Ip: 81.47.163.249

Dominio: maristak.com

La auditoría aquí presentada es básica, para ver las vulnerabilidades que se pueden sacar, sin apenas investigación.



2.- Sumario Ejecutivo:

Se ha realizado una auditoría de seguridad sobre la aplicación web www.maristak.com y de posibles problemas que pudiera tener hacia el servidor.

Existen bastantes riesgos de seguridad en relación con la infraestructura y aplicación web analizada que podrían afectar a la integridad, confidencialidad o disponibilidad de los datos, así como del acceso al servidor.

Se han detectado vulnerabilidades de nivel alto que permiten obtener información muy sensible de la base de datos, así como otras que podrían dejar el control del servidor de la página.

Existen algunas otras vulnerabilidades de nivel bajo que no suponen hoy en día realmente un riesgo real para la aplicación, aunque se recomienda solucionarlas ya que en un futuro su nivel de riesgo podría aumentar debido a la combinación de estas con otras posibles vulnerabilidades de más nivel.

3.- Recopilación de Información:

Como inicio mediante las herramientas OSINT recogemos datos acerca del dominio en cuestión maristak.com.

Las herramientas OSINT nos permitirán mediante un conjunto de técnicas y **herramientas** para recopilar información pública, analizar los datos y correlacionarlos convirtiéndolos en datos para posteriormente analizarlos y detectar vulnerabilidades.

Mediante la información adquirida en posteriores fases se utilizará para comprobar lo segura que es la red de atacantes externos.

3.1 _WHOIS

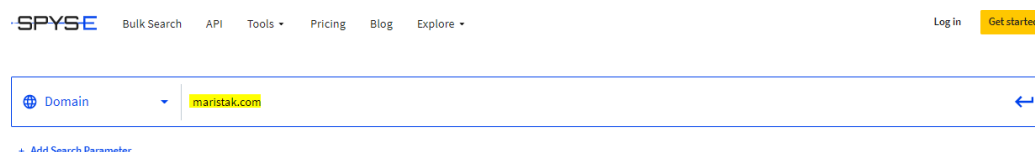


Principalmente, utilizamos la herramienta **WHOIS** la cual nos permitirá consultar los distintos contactos de un dominio registrado (titular o registrante, contacto administrativo y contacto técnico).

Además de la empresa registradora y las fechas de creación y expiración de un dominio u otras fechas relevantes, dominios, subdominios y aplicación que utilicen.

Datos recopilados del dominio (maristak.com) WHOIS:

Búsqueda de dominio:



The screenshot shows the SPYSE website header with navigation links: Bulk Search, API, Tools, Pricing, Blog, and Explore. On the right, there are links for Log in and Get started. Below the header is a search bar with a dropdown menu set to 'Domain' and the text 'maristak.com' entered. A search button with a magnifying glass icon is on the right. Below the search bar is a link that says '+ Add Search Parameter'.

En esta imagen se observan, la dirección IP del servidor: **81.47.163.249** la compañía que lo aloja y el dominio **www.maristak.com**.

También de las aplicaciones que hace uso, por ejemplo:

- Servidor web (Apache) y versión 2.4.38.
- Sistema operativo (Debian).
- Sistema de ficheros (Drupal).
- Librería de JavaScript y versión 1.10.2.
- Versiones de las aplicaciones.



maristak.com 200 SEVERE

Title: Maristak Ikastetxea | Siempre Maristak
Durango : Bachillerato-FP-Cursos

Final url: <https://www.maristak.com/es>

Registrar: Network Solutions, LLC

Scanned on 2021-08-11

DNS Records WHOIS

A: 81.47.163.249 - AS3352 - telefonica de espa...

MX: aspmx3.googlemail.com

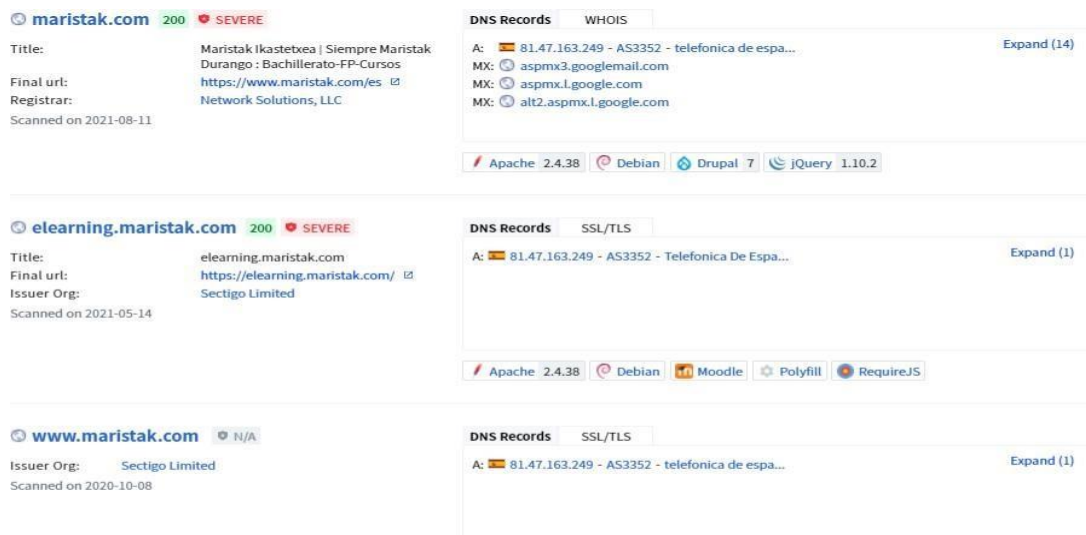
MX: aspmx.l.google.com

MX: alt2.aspmx.l.google.com

Apache 2.4.38 Debian Drupal 7 jQuery 1.10.2

Información acerca de los **subdominios** de maristak.com:

- elernig.maristak.com
- www.maristak.com
- msjdcorreio.maristak.com
- multiescola.marisak.com
- arautua.maristak.com
- asir.maristak.com
- vtecoach.maristak.com



maristak.com 200 SEVERE

Title: Maristak Ikastetxea | Siempre Maristak
Durango : Bachillerato-FP-Cursos

Final url: <https://www.maristak.com/es>

Registrar: Network Solutions, LLC

Scanned on 2021-08-11

DNS Records WHOIS

A: 81.47.163.249 - AS3352 - telefonica de espa... Expand (14)

MX: aspmx3.googlemail.com

MX: aspmx.l.google.com

MX: alt2.aspmx.l.google.com

Apache 2.4.38 Debian Drupal 7 jQuery 1.10.2

elernig.maristak.com 200 SEVERE

Title: elernig.maristak.com

Final url: <https://elernig.maristak.com/>

Issuer Org: Sectigo Limited

Scanned on 2021-05-14

DNS Records SSL/TLS

A: 81.47.163.249 - AS3352 - Telefonica De Espa... Expand (1)

Apache 2.4.38 Debian Moodle Polyfill RequireJS

www.maristak.com N/A

Issuer Org: Sectigo Limited

Scanned on 2020-10-08

DNS Records SSL/TLS

A: 81.47.163.249 - AS3352 - telefonica de espa... Expand (1)

3.2_MALTEGO



Mediante la herramienta **Maltego** que es un software enfocado principalmente hacia el análisis forense y desarrollado para **hacer** más propicio el análisis de enlaces y la minería de datos a partir de dominios IP's, emails, teléfonos, ubicaciones geográficas...

Mediante la herramienta **maltego** haremos un scanner que nos devolverá un esquema del dominio de maristak (teléfonos, subdominios, direcciones IP...)

Haremos un esquema de la arquitectura del **dominio de maristak** (maristak.com).



3.3_NMAP

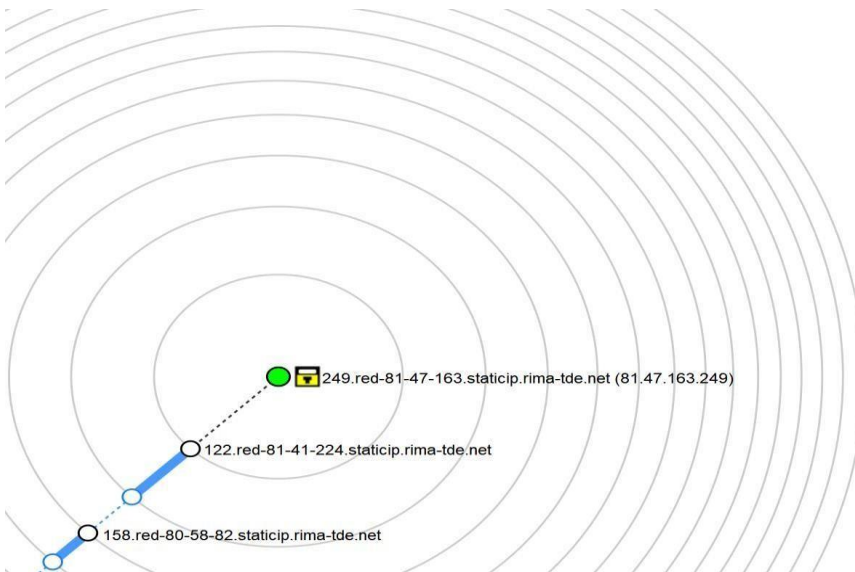


Nmap es una herramienta que se usa para determinar los hosts que se están ejecutando y los servicios que estos están ejecutando.

Una vez que la red se traza utilizando herramientas como LAN MapShot, el Nmap se puede usar para determinar los tipos de servicios y hosts que se ejecutan en la red.

Lanzaremos un escáner para detectar los puertos abiertos de la maquina servidor del sitio web.

En este escáner detectaremos puertos, direcciones IP de dispositivos, con sus respectivos equipos.



Escaneo a dirección Ip 81.47.163.249 = red pública maristak:

Zenmap

Escaneo Herramientas Perfil Ayuda (H)

Objetivo: 81.47.163.249 Perfil:

Comando: nmap -p 1-65535 -T4 -A -v -Pn 81.47.163.249

Servidores Servicios Salida Nmap Puertos / Servidores Topología Detalles del servidor Escaneos

OS Servidor

Puerto	Protocolo	Estado	Servicio	Versión
80	tcp	open	http	Apache httpd 2.4.52
443	tcp	open	http	Apache httpd 2.4.52 ((Debian))
4105	tcp	closed	shofarplayer	
4117	tcp	open	http	nginx
4118	tcp	open	ssh	OpenSSH 8.1 (protocol 2.0)
4126	tcp	open	ddrepl	
8023	tcp	open	ssh	OpenSSH 8.4p1 Debian 5 (protocol 2.0)
8080	tcp	open	http-proxy	none
28023	tcp	closed		

Zenmap

Escaneo Herramientas Perfil Ayuda (H)

Objetivo: 81.47.163.249 Perfil:

Comando: nmap -p 1-65535 -T4 -A -v -Pn 81.47.163.249

Servidores Servicios Salida Nmap Puertos / Servidores Topología Detalles del servidor Escaneos

OS Servidor

249.red-81-47-163.s

249.red-81-47-163.staticip.rima-tde.net (81.47.163.249)

Estado del servidor

Estado: up

Puertos abiertos: 7

Puertos filtrados: 65526

Puertos cerrados: 2

Puertos escaneados: 65535

Tiempo activo: 547028

Última inicialización: Wed Jan 19 02:00:08 2022

Direcciones

IPv4: 81.47.163.249

IPv6: No disponible

MAC: No disponible

Nombres de Servidores

Nombre - Tipo: 249.red-81-47-163.staticip.rima-tde.net - PTR

Sistema operativo

Nombre: Linux 4.0

Precisión: 94%

Puertos usados

Puerto-Protocolo-Estado: 80 - tcp - open

Puerto-Protocolo-Estado: 4105 - tcp - closed

Clases de OS

Tipo	Fabricante	Familia OS	Generación OS	Precisión
general purpose	Linux	Linux	4.X	94%

3.4 _NESSUS

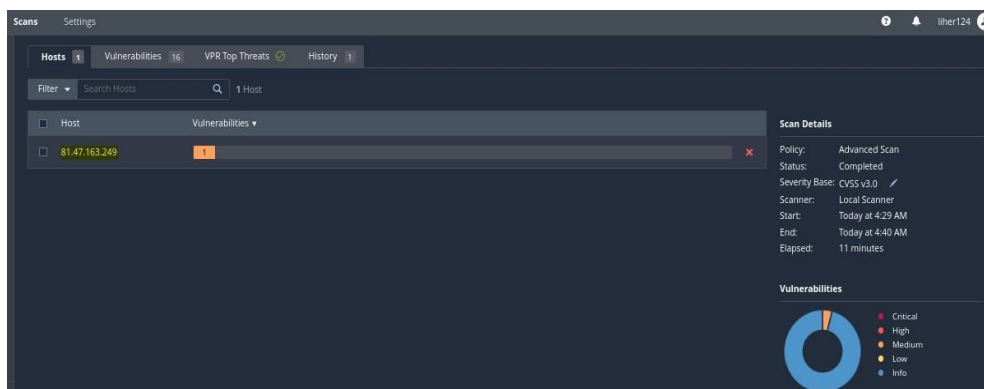


Nessus es un programa de escaneo de vulnerabilidades en diversos sistemas operativos. Consiste en realizar el escaneo en el sistema objetivo, y *nessus*, el cliente (basado en consola o gráfico) que muestra el avance e informa sobre el estado de los escaneos.

Nos permitirá realizar lo siguiente:

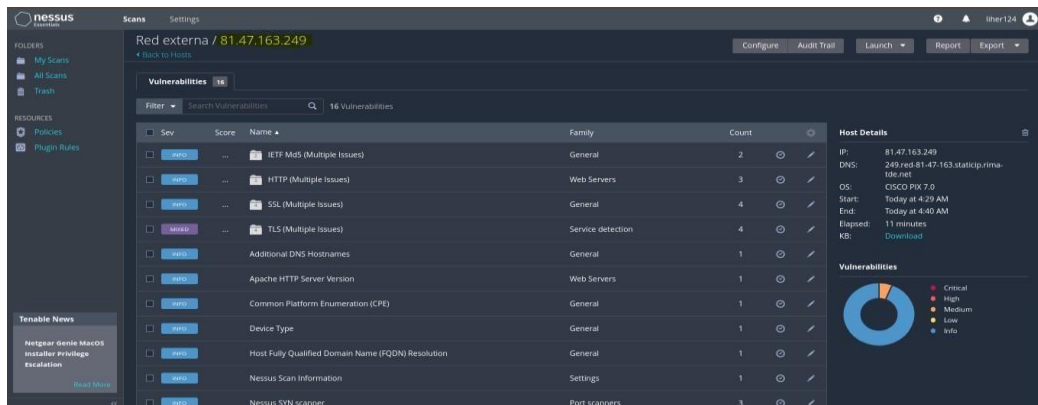
1. Escanea el servidor con la dirección IP que necesitemos.
2. Se escoge el nombre del análisis, escaneo interno y los IP de los hosts que se quieren analizar, click en RUN SCAN.
3. En la opción HOSTS muestra las vulnerabilidades en porcentajes clasificadas en 5 tipos de vulnerabilidades: Críticas, Altas, Medias, Bajas y de información.
4. Se puede ingresar a cada vulnerabilidad para una descripción más detallada.

IP 81.47.163.249 = red pública maristak



Información acerca del **sitio web**:

- Vulnerabilidades.
- Hosts.
- DNS.
- Servicios.



Red externa / 81.47.163.249

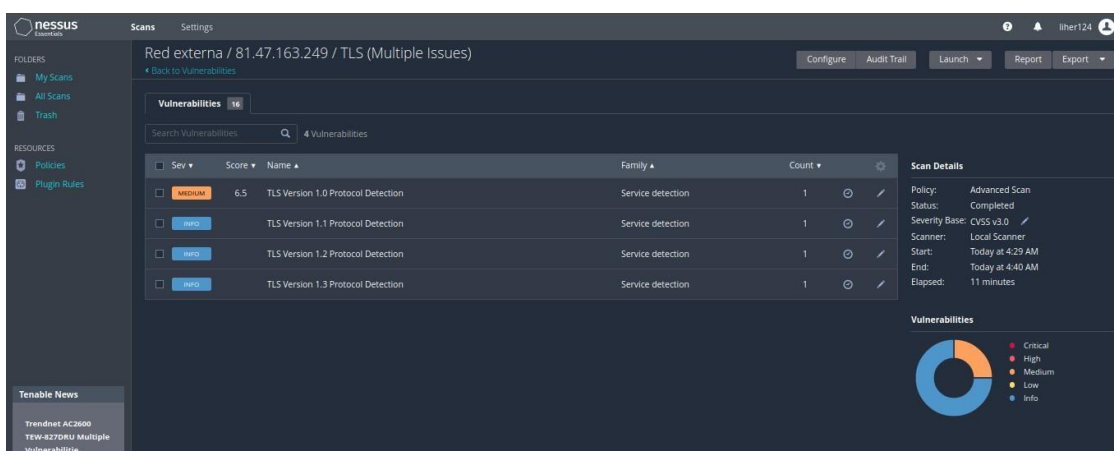
Sev	Score	Name	Family	Count
Info	...	IETF Md5 (Multiple Issues)	General	2
Info	...	HTTP (Multiple Issues)	Web Servers	3
Info	...	SSL (Multiple Issues)	General	4
Info	...	TLS (Multiple Issues)	Service detection	4
Info	...	Additional DNS Hostnames	General	1
Info	...	Apache HTTP Server Version	Web Servers	1
Info	...	Common Platform Enumeration (CPE)	General	1
Info	...	Device Type	General	1
Info	...	Host Fully Qualified Domain Name (FQDN) Resolution	General	1
Info	...	Nessus Scan Information	Settings	1
Info	...	Nessus SYN scanner	Port scanners	3

Host Details

IP: 81.47.163.249
DNS: 249.red-81-47-163.staticip.rima-tel.net
OS: CISCO PIX 7.0
Start: Today at 4:29 AM
End: Today at 4:40 AM
Elapsed: 11 minutes
KB: Download

Vulnerabilities

Donut chart showing severity distribution: Critical (red), High (orange), Medium (yellow), Low (green), Info (blue).



Red externa / 81.47.163.249 / TLS (Multiple Issues)

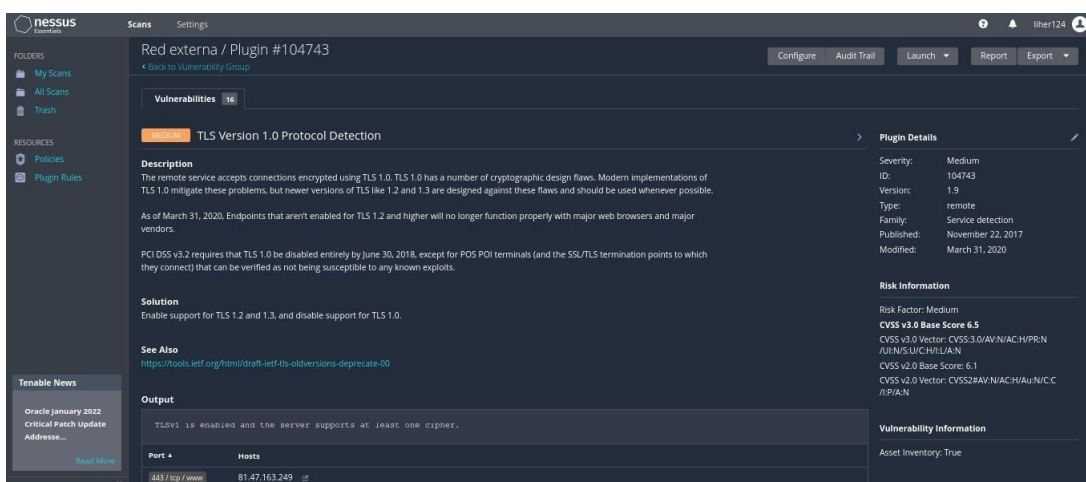
Sev	Score	Name	Family	Count
Medium	6.5	TLS Version 1.0 Protocol Detection	Service detection	1
Info	...	TLS Version 1.1 Protocol Detection	Service detection	1
Info	...	TLS Version 1.2 Protocol Detection	Service detection	1
Info	...	TLS Version 1.3 Protocol Detection	Service detection	1

Scan Details

Policy: Advanced Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 4:29 AM
End: Today at 4:40 AM
Elapsed: 11 minutes

Vulnerabilities

Donut chart showing severity distribution: Critical (red), High (orange), Medium (yellow), Low (green), Info (blue).



Red externa / Plugin #104743

Vulnerabilities

TLS Version 1.0 Protocol Detection

Description

The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible.

As of March 31, 2020, Endpoints that aren't enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS PCI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.

Solution

Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.

See Also

<https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00>

Output

TLSv1 is enabled and the server supports at least one cipher.

Port

443 / http / www

Hosts

81.47.163.249

Plugin Details

Severity: Medium
ID: 104743
Version: 1.9
Type: remote
Family: Service detection
Published: November 22, 2017
Modified: March 31, 2020

Risk Information

Risk Factor: Medium
CVSS v3.0 Base Score 6.5
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/L:N/A:N
CVSS v2.0 Base Score: 6.1
CVSS v2.0 Vector: CVSS2#AV:N/AC:H/Au:N/C:C/R:P/A:N

Vulnerability Information

Asset Inventory: True

3.5_OWAS ZAP



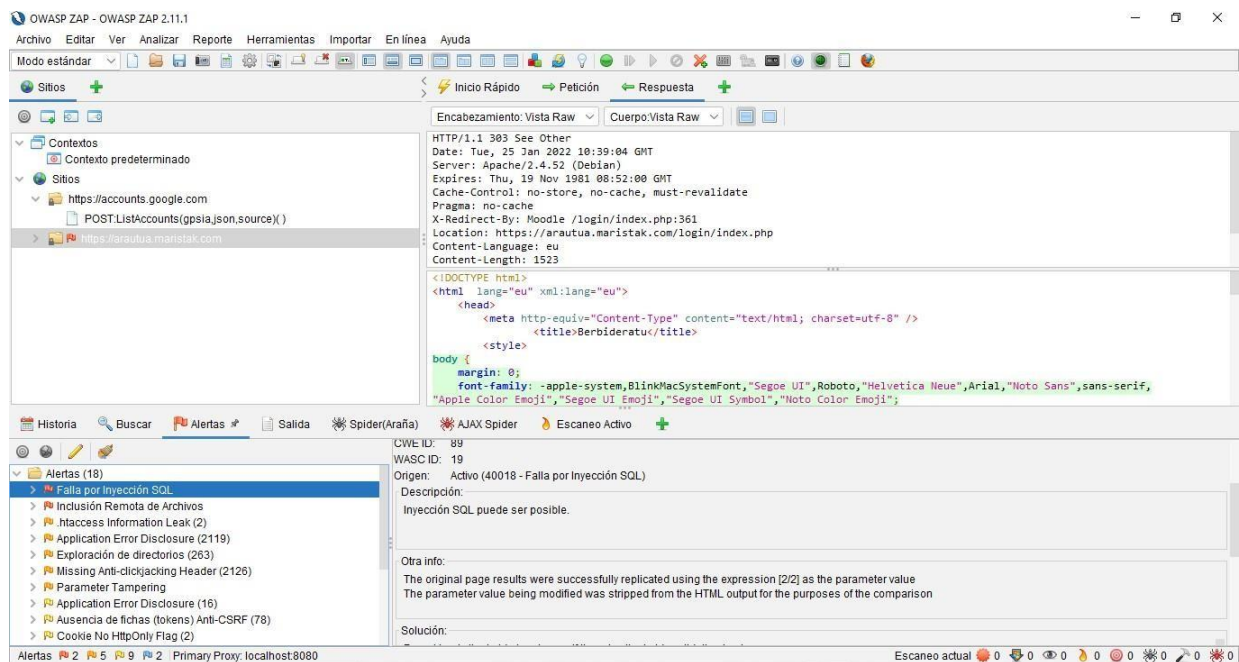
OWASP Zed Attack Proxy es una herramienta integrada para realizar pruebas de penetración, la cual permite encontrar vulnerabilidades en las aplicaciones web.

ZAP proporciona escáneres automáticos como también un conjunto de herramientas para encontrar de manera manual vulnerabilidades en seguridad.

Escaneo sito web maristak:

Como se puede observar, se nos muestra las vulnerabilidades que hay acerca de la web.

- Inyección SQL
- Inclusión Remota de Archivos
- Acceso a .htaccess
- Explotación de directorios.
- Información de páginas.



4.- Detalle de resultado técnicos:

- Sistema operativo Debian (95%)
- Servidor Web Apache/2.4.38 (97%)
- Servidor Drupal/7 (97%)

Mediante la herramienta Nmap, se ha realizado varios escáneres a esta web y hemos encontrado la siguiente información:

- Servidores (puertos, protocolos, versiones, servicios, OS....)

Zenmap

Escaneo Herramientas Perfil Ayuda (H)

Objetivo: 81.47.163.249 Perfil:

Comando: nmap -p 1-65535 -T4 -A -v -Pn 81.47.163.249

Servidores Servicios Salida Nmap Puertos / Servidores Topología Detalles del servidor Escaneos

OS: Servidor

249.red-81-47-163.s

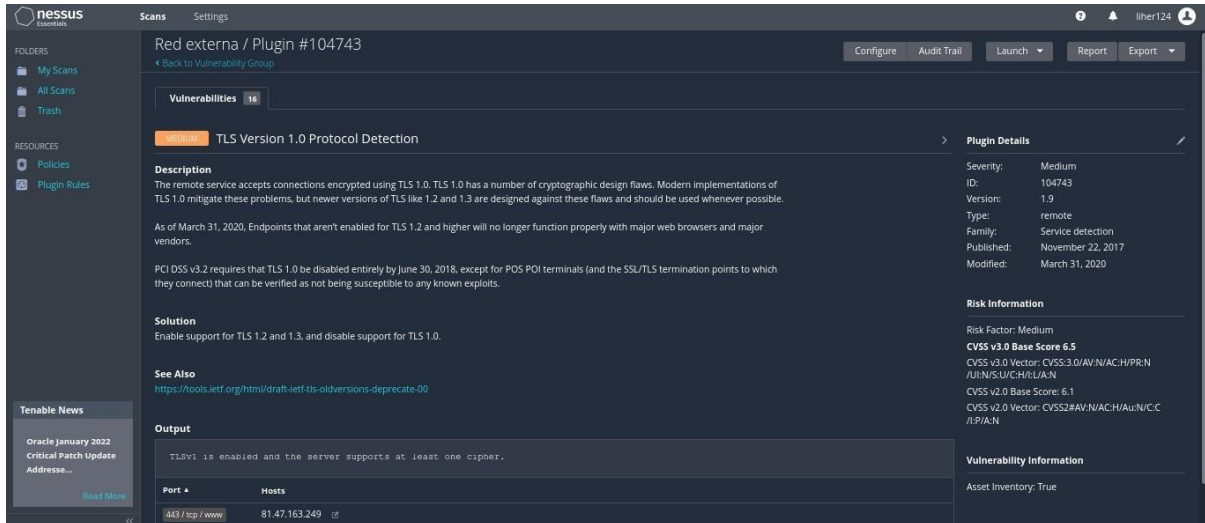
Puerto	Protocolo	Estado	Servicio	Versión
80	tcp	open	http	Apache httpd 2.4.52
443	tcp	open	http	Apache httpd 2.4.52 ((Debian))
4105	tcp	closed	shofarplayer	
4117	tcp	open	http	nginx
4118	tcp	open	ssh	OpenSSH 8.1 (protocol 2.0)
4126	tcp	open	ddrepl	
8023	tcp	open	ssh	OpenSSH 8.4p1 Debian 5 (protocol 2.0)
8080	tcp	open	http-proxy	none
28023	tcp	closed		

Red externa detección Nmap:

Puerto	Protocolo	Servicio	Version	Estado
80	tcp	http	Apache httpd 2.4.52	open
443	tcp	http	Apache httpd 2.4.52 (Debian)	open
4117	tcp	http	nginx	open
4118	tcp	ssh	OpenSSH 8.1 (protocol 2.0)	open
4126	tcp	ddrepl	none	open
8023	tcp	ssh	OpenSSH 8.4p1 (protocol 2.0)	open
8080	tcp	http-proxy	none	open
4105	tcp			closed
28023	tcp			closed

Red externa detección Nessus:

- Port -->443/tcp/www
- Hosts -->81.47.163.249
- Descripción --> TLS Versión 1.0 Protocol Detection
- Nivel --> Medium



Red externa / Plugin #104743

Vulnerabilities 16

Plugin Details

Severity: Medium
ID: 104743
Version: 1.9
Type: remote
Family: Service detection
Published: November 22, 2017
Modified: March 31, 2020

Risk Information

Risk Factor: Medium
CVSS v3.0 Base Score 6.5
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:U/A:N
CVSS v2.0 Base Score: 6.1
CVSS v2.0 Vector: CVSS2#AV:N/AC:H/Au:N/C:C/I:P/A:N

Description

The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible.

As of March 31, 2020, endpoints that aren't enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.

Solution

Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.

See Also

<https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00>

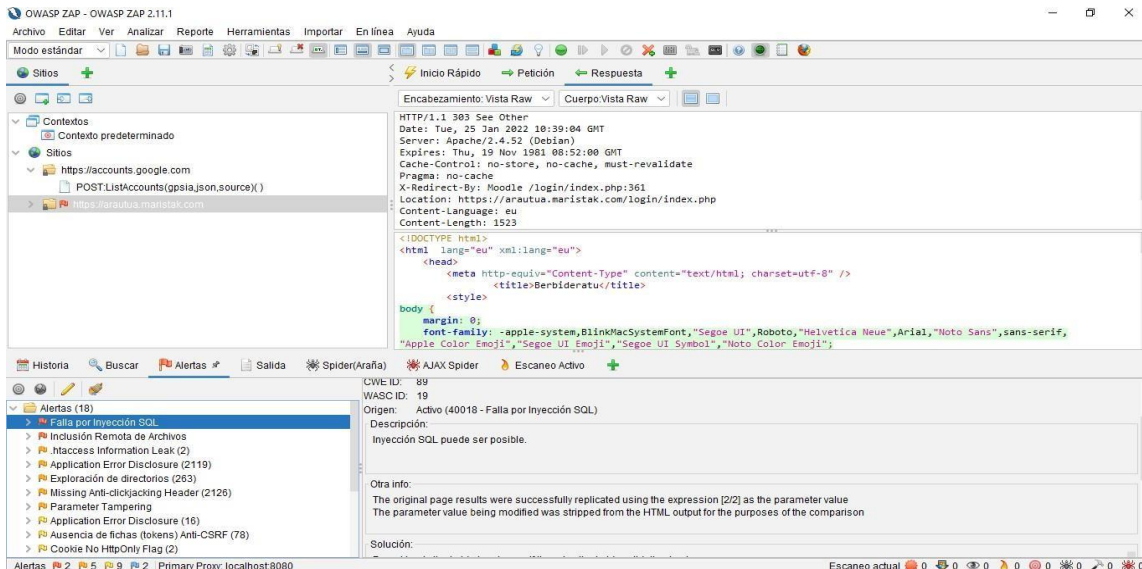
Output

TLSv1 is enabled and the server supports at least one cipher.

Port	Hosts
443 / tcp / www	81.47.163.249

Red externa detección OWASP ZAP:

Mediante la herramienta **OWASP ZAP**, se ha realizado varios escáneres a esta web y hemos encontrado la siguiente información:



OWASP ZAP - OWASP ZAP 2.11.1

Archivo Editar Ver Analizar Reporte Herramientas Importar En línea Ayuda

Modo estándar

Sitios

Contextos

Contexto predeterminado

Sitios

https://accounts.google.com

POST:ListAccounts(gpsia_json,source)()

https://arautua.maristak.com

Encabezamiento: Vista Raw

Cuerpo: Vista Raw

HTTP/1.1 303 See Other
Date: Tue, 25 Jan 2022 10:39:04 GMT
Server: Apache/2.4.52 (Debian)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
X-Redirect-By: Moodle /login/index.php:361
Location: https://arautua.maristak.com/login/index.php
Content-Language: eu
Content-Length: 1523

<!DOCTYPE html>
<html lang="eu" xml:lang="eu">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>Berbideratu</title>
<style>
body {
margin: 0;
font-family: -apple-system,BlinkMacSystemFont,"Segoe UI",Roboto,"Helvetica Neue",Arial,"Noto Sans",sans-serif,
"Apple Color Emoji","Segoe UI Emoji","Segoe UI Symbol","Noto Color Emoji";

Historia

Alertas

Alertas (18)

Falla por Inyección SQL

Inclusión Remota de Archivos

.htaccess Information Leak (2)

Application Error Disclosure (2119)

Exploración de directorios (263)

Missing Anti-clickjacking Header (2126)

Parameter Tampering

Application Error Disclosure (16)

Ausencia de fichas (tokens) Anti-CSRF (78)

Cookie No HttpOnly Flag (2)

CVSS ID: 89
WASC ID: 19
Origen: Activo (40018 - Falla por Inyección SQL)
Descripción:
Inyección SQL puede ser posible.

Otra info:
The original page results were successfully replicated using the expression [202] as the parameter value
The parameter value being modified was stripped from the HTML output for the purposes of the comparison

Solución:

Escaneo actual

Tabla con las vulnerabilidades detectadas:

Alerta	Riesgo	Estado
Falla por Inyección SQL	alto	open
Inclusión Remota de Archivos	alto	open
.htaccess Information Leak	medio	open
Application Error Disclosure	medio	open
Exploración de directorios	medio	open
Missing Anti-clickjacking Header	medio	open
Parameter Tampering	medio	open

5.- Vulnerabilidades y Explotación:

El objetivo principal de la fase de explotación es **ganar acceso a algún sistema o dispositivo aprovechando las fallas de seguridad encontradas en la fase anterior.**

Una particularidad de la fase de explotación es que las estrategias, técnicas o fallas aprovechadas pueden variar dependiendo del sistema en particular que sea analizado.

Criterio de clasificación de vulnerabilidades.

- → Un atacante podría tomar el control total sobre el host, por ejemplo, acceso a lectura y escritura del sistema de ficheros, ejecución de comandos arbitrarios.

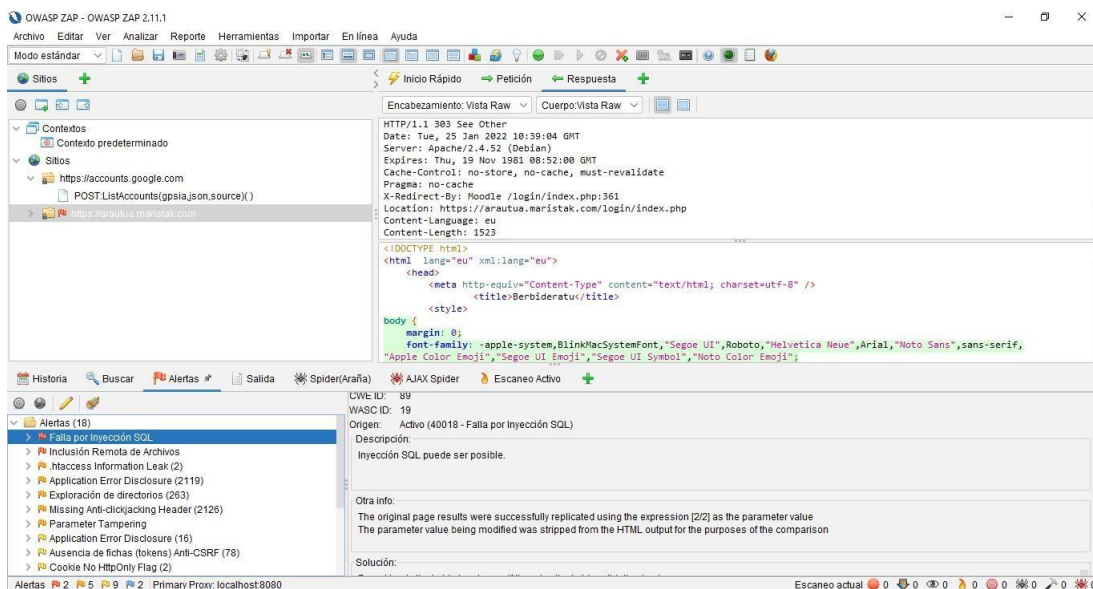
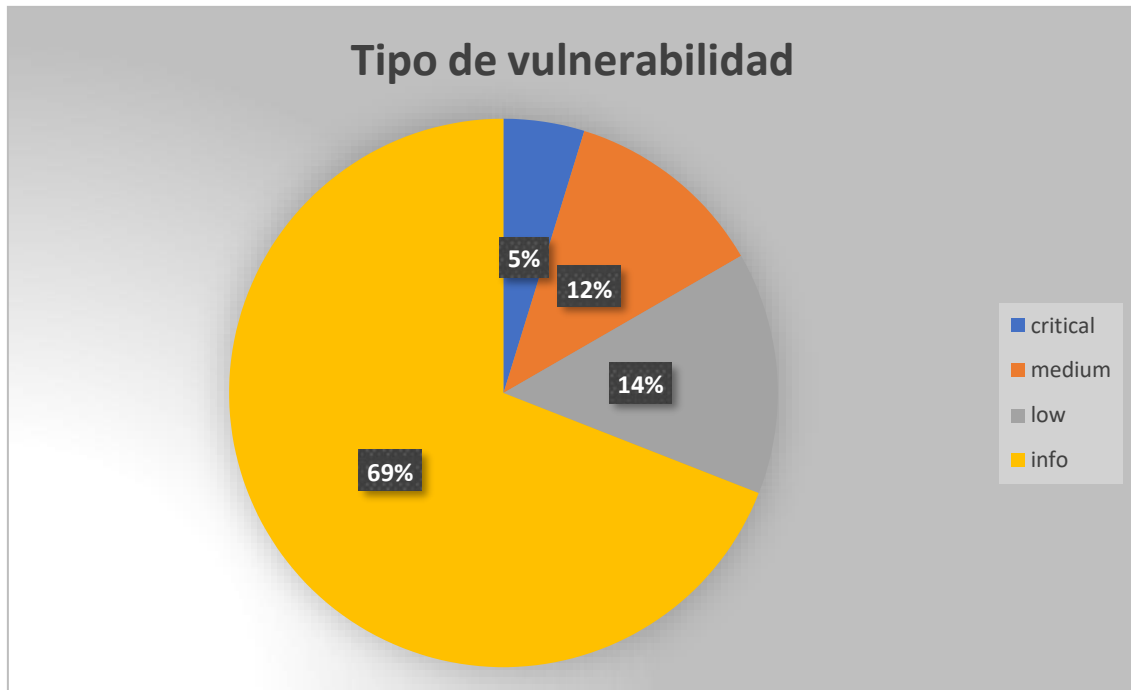
- → Acceso a información sensible en el host, incluyendo sistemas de seguridad o acceso a ficheros comprometidos, revelación de directorios y configuraciones locales...

- → Recopilación de información sensible del host, como versiones del software. Esta información puede hacer que el atacante se centre y focalice en esas versiones su arsenal, hasta conseguir su objetivo.

- → Posibilidad de recopilación de información general de host, como puertos abiertos, servicios en ejecución etc. Esta información es útil, para poder buscar las vulnerabilidades específicas.

Resumen de vulnerabilidades detectadas.

A continuación, se muestra el **listado** de las vulnerabilidades detectadas:



5.1_OpenSSH

OpenSSH (Open Secure Shell) es un conjunto de aplicaciones que permiten realizar comunicaciones cifradas a través de una red, usando el protocolo SSH.

Riesgo: ■ ■ ■ ■ 4/4

Puerto: 4118 (Open SSh 8.1 (protocolo 2.0)).

Detalles de la vulnerabilidad:

El lado del cliente en OpenSSH 8.4 tiene una discrepancia observable que conduce a una fuga de información en la negociación del algoritmo. Esto permite a los atacantes man-in-the-middle apuntar a los intentos de conexión iniciales (donde el cliente no ha almacenado en caché ninguna clave de host para el servidor).

Se ha detectado, que hay una versión 8.1 de Open SSH, la hemos revisado y hemos detectado que no es vulnerable, ya que es la versión actualizada y no hay vulnerabilidades asociadas a esa versión.

[illegible]

CVE Details

The ultimate security vulnerability database

[Iniciar sesión / Registrarse](#)

Hojas:

- [Procesadores](#)
- [Productos](#)
- [Vulnerabilidades por fecha](#)
- [Vulnerabilidades por tipo](#)

Informes:

- [Informe de actualización CVEs](#)
- [Contribución de puntuaciones CVSS](#)

Buscador:

- [Búsqueda de procesos](#)
- [Búsqueda de productos](#)
- [Búsqueda de versiones](#)
- [Búsqueda de vulnerabilidades por fabricante](#)

Top 50 :

- [Procesadores](#)
- [Puntuaciones de Cves del proveedor](#)
- [Productos](#)
- [Puntuaciones de Cves del producto](#)
- [Versiones](#)

Otro:

- [Boletines de Microsoft](#)
- [Noticias de Bugtraq](#)
- [Definiciones de CVE](#)
- [Alerta de R.CoNtacto](#)
- [Intercomunicación](#)
- [Análisis de CVE](#)
- [PRELIMINARES PRELIMINARES](#)
- [Artículos](#)

Enlaces externos :

- [Site web de NVD](#)
- [Site web de CVE](#)

Ver CVE : [v]

(por ejemplo: CVE-2009-3280 o CVE-1234 o 1234)

Ver BID : [v]

(por ejemplo: 12345)

Detalles de la vulnerabilidad : CVE-2020-14145

El lado del cliente en OpenSSH 5.7 a 8.4 tiene una discrepancia observable que conduce a una fuga de información en la negociación del algoritmo. Esto permite a los atacantes man-in-the-middle apuntar a los intentos de conexión iniciales (donde el cliente no ha almacenado en caché ninguna clave de host para el servidor). NOTA: algunos informes indican que 8.5 y 8.6 también se ven afectados.

Fecha de publicación : 2020-06-29 Fecha de última actualización : 2021-07-21

Contratar todo Expandir todo Seleccionar y copiar Desplazarse hasta « Comentarios » Enlaces externos
[Buscar en Twitter](#) [Buscar en YouTube](#) [Buscar en Google](#)

– Puntuaciones CVSS y tipos de vulnerabilidad

Puntuación CVSS Impacto de la confidencialidad Impacto en la integridad Impacto en la disponibilidad Complejidad de acceso	4.3 <i>Negativo</i> (Hay una considerable divulgación informativa). <i>Ninguno</i> (No hay impacto en la integridad del sistema). <i>Ninguno</i> (No hay ningún impacto en la disponibilidad del sistema). <i>Medio</i> (Las condiciones de acceso son algo especializadas. Algunas condiciones previas deben ser satisfechas para explotar)	Autenticación No es necesario (no se requiere autenticación para aprovechar la vulnerabilidad). Acceso obtenido Ninguno Tipo(s) de vulnerabilidad Obtener información CWE ID 250
---	---	---

– Definiciones ovales relacionadas

Título	ID de definición	Clase	Familia
RHSA-2021-4368: actualización de seguridad openssl (moderada)	oval.com:redhat:rhsa:def:2021-4368	unix	

Las definiciones de OVAL (Open Vulnerability and Assessment Language) definen exactamente lo que se debe hacer para verificar una vulnerabilidad o un parche fallido. Consulte las definiciones de OVAL si desea saber qué debe hacer para verificar una vulnerabilidad.

– Productos afectados por CVE-2020-14145

#	Tipo de producto	Vendedor	Producto	Versión	Actualizar	Edución	Lidioma
1	Aplicación	Netscape	Active In Unified Manager	-	-	-	Vulnerabilidades en los detalles de la versión
2	Hardware	Netsape	Node de crómulo HUI	-	-	-	Vulnerabilidades en los detalles de la versión
3	Aplicación	Netsape	Node de administración de HCI	-	-	-	Vulnerabilidades en los detalles de la versión
4	Hardware	Netsape	Node de almacenamiento HCI	-	-	-	Vulnerabilidades en los detalles de la versión
5	Aplicación	Netsape	Ontap Selecciones Implementar utilidad de administración	-	-	-	Vulnerabilidades en los detalles de la versión
6	Aplicación	Netsape	Fuerza sólido	-	-	-	Vulnerabilidades en los detalles de la versión
7	Aplicación	Netsape	Almacenamiento integrado en steelstore cloud	-	-	-	Vulnerabilidades en los detalles de la versión
8	Aplicación	Omniscop	Omnescop	-	-	-	Vulnerabilidades en los detalles de la versión
9	Aplicación	Omniscop	Omnescop	8.4	-	-	Vulnerabilidades en los detalles de la versión
10	Aplicación	Omniscop	Omnescop	8.5	-	-	Vulnerabilidades en los detalles de la versión
11	Aplicación	Omniscop	Omnescop	8.6	-	-	Vulnerabilidades en los detalles de la versión

5.2_Nginx (http)

NGINX es un servidor web open source de alta performance que ofrece el contenido estático de un sitio web de forma rápida y fácil de configurar. Ofrece recursos de equilibrio de carga, proxy inverso y streaming, además de gestionar miles de conexiones simultáneas.

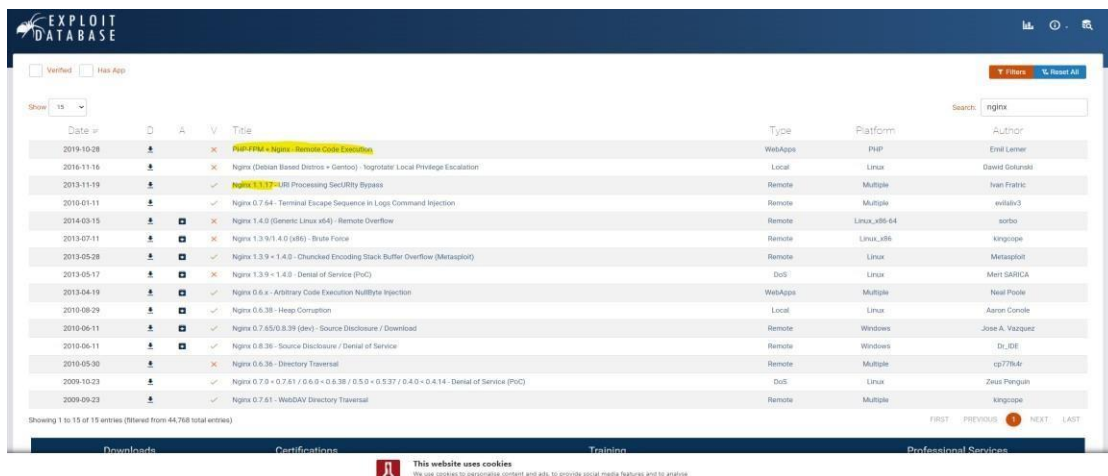
Riesgo: ■■■■ 4/4

Puerto: 4117 (Nginx).

Detalles de la vulnerabilidad:

Algunas implementaciones HTTP/2 son vulnerables a una fuga de encabezado, lo que puede conducir a una denegación de servicio. El atacante envía un flujo de encabezados con un nombre de encabezado de longitud 0 y un valor de encabezado de longitud 0, opcionalmente Huffman codificado en encabezados de 1 byte o mayores.

Algunas implementaciones asignan memoria para estos encabezados y mantienen viva la asignación hasta que la sesión muere. Esto puede consumir exceso de memoria.



Date	Type	Platform	Author
2019-10-28	WebApps	PHP	Enel Lerner
2016-11-16	Local	Linux	David Gotunski
2013-11-19	Remote	Multiple	nen Fialtic
2010-01-11	Remote	Multiple	evilal33
2014-03-15	Remote	Linux_x86-64	sofbo
2013-07-11	Remote	Linux_x86	kingpope
2013-05-28	Remote	Linux	Metasploit
2013-05-17	DoS	Linux	Mert SARICA
2013-04-19	WebApps	Multiple	Neal Poole
2010-08-29	Local	Windows	Aaron Conole
2010-06-11	Remote	Windows	Jose A. Vazquez
2010-06-11	Remote	Windows	Dr. IDE
2010-05-30	Remote	Multiple	cp7764r
2009-10-23	DoS	Linux	Zhuo Penguin
2009-09-23	Remote	Multiple	kingpope

Se ha detectado, que hay una versión 1.14 de Nginx, la hemos revisado y hemos detectado que no es vulnerable, ya que es la versión actualizada y no hay vulnerabilidades asociadas a esa versión.

CVE Details

The ultimate security vulnerability datasource

Log In Register

(e.g.: CVE-2009-1234 or 2010-1234 or 20101234)

Search
View CVE

Vulnerability Feeds & Widgets ^{New} www.itsecdb.com

[Switch to https://](#)

[Home](#)

Browse :

[Vendors](#)

[Products](#)

[Vulnerabilities By Date](#)

[Vulnerabilities By Type](#)

Reports :

[CVSS Score Report](#)

[CVSS Score Distribution](#)

Search :

[Vendor Search](#)

[Product Search](#)

[Version Search](#)

[Vulnerability Search](#)

[By Microsoft References](#)

Top 50 :

[Vendors](#)

[Vendor Cvss Scores](#)

[Products](#)

[Product Cvss Scores](#)

[Versions](#)

Other :

[Microsoft Bulletins](#)

[Bugtraq Entries](#)

[CVE Definitions](#)

[About & Contact](#)

[Feedback](#)

[CVE Help](#)

[FAQ](#)

[Articles](#)

External Links :

[NVD Website](#)

[CVE Web Site](#)

View CVE :

(e.g.: CVE-2009-1234 or

2010-1234 or 20101234)

View BID :

Vulnerability Details : CVE-2020-14145

El lado del cliente en OpenSSH 5.7 a 8.4 tiene una discrepancia observable que conduce a una fuga de información en la negociación del algoritmo. Esto permite a los atacantes man-in-the-middle apuntar a los intentos de conexión iniciales (donde el cliente no ha almacenado en caché ninguna clave de host para el servidor). NOTA: algunos informes indican que 8.5 y 8.6 también se ven afectados.

Publish Date : 2020-06-29 Last Update Date : 2021-07-21

[Collapse All](#) [Expand All](#) [Select](#) [Select&Copy](#) [Scroll To](#) [Comments](#) [External Links](#)

[Search Twitter](#) [Search YouTube](#) [Search Google](#)

- CVSS Scores & Vulnerability Types

CVSS Score	4.3
Confidentiality Impact	Partial (There is considerable informational disclosure.)
Integrity Impact	None (There is no impact to the integrity of the system.)
Availability Impact	None (There is no impact to the availability of the system.)
Access Complexity	Medium (The access conditions are somewhat specialized. Some preconditions must be satisfied to exploit)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	Obtain Information
CWE ID	200

- Related OVAL Definitions

Title	Definition Id	Class	Family
RHSA-2021:4368: openssl security update (Moderate)	oval:com.redhat.rhsa:def:20214368		unix

OVAL (Open Vulnerability and Assessment Language) definitions define exactly what should be done to verify a vulnerability or a missing patch. Check out the OVAL definitions if you want to learn what you should do to verify a vulnerability.

- Products Affected By CVE-2020-14145

#	Product Type	Vendor	Product	Version	Update	Edition	Language	
1	Application	Netapp	Active IQ Unified Manager	-	-	-	-	Version Details Vulnerabilities
2	Hardware	Netapp	Hci Compute Node	-	-	-	-	Version Details Vulnerabilities
3	Application	Netapp	Hci Management Node	-	-	-	-	Version Details Vulnerabilities
4	Hardware	Netapp	Hci Storage Node	-	-	-	-	Version Details Vulnerabilities

5.3_Apache httpd 2.4.52

El servidor HTTP apache es un servidor de red “heavy duty” que Subversion puede aprovechar. A través de un módulo propio, httpd permite servir a clientes repositorios Subversion por el protocolo WebDAV/DeltaV, el cual es una extensión sobre HTTP 1.1.

Este protocolo coge el ubicuo protocolo HTTP, núcleo de la World Wide Web, y añade la capacidad de escritura—específicamente el versionado de la misma.

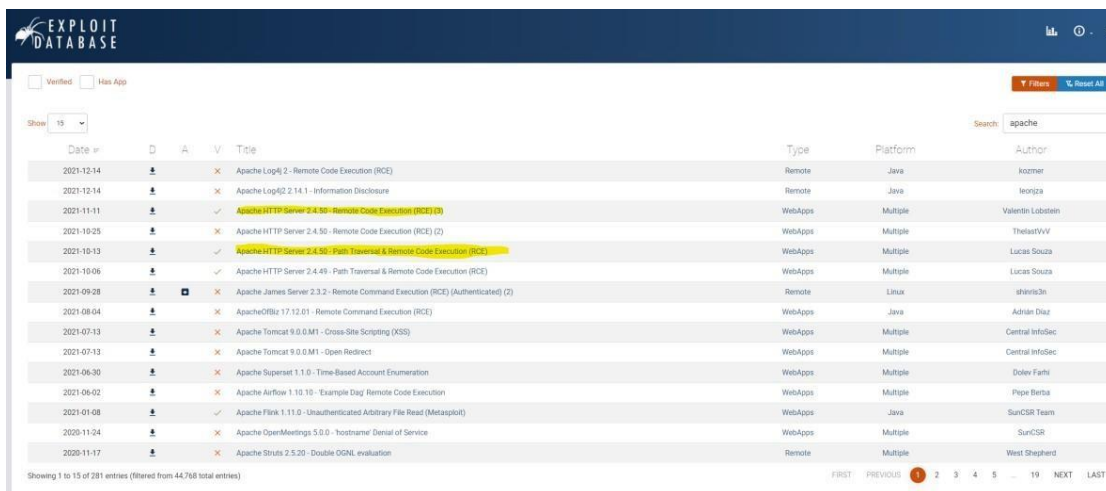
Riesgo: ■■■■ 4/4

Puerto: 80 (apache httpd 2.4.52).

Detalles de la vulnerabilidad:

Un cuerpo de solicitud cuidadosamente diseñado puede provocar un desbordamiento de búfer en el analizador multiparte mod_lua (r:parsebody()) llamado desde scripts Lua).

El equipo de Apache httpd no es consciente de un exploit para la vulnerabilidad, aunque podría ser posible crear uno. Este problema afecta a Apache HTTP Server 2.4.51 y versiones anteriores.



Date	D	A	V	Title	Type	Platform	Author
2021-12-14	✓	✗	✗	Apache Log4j 2 - Remote Code Execution (RCE)	Remote	Java	k0rn3r
2021-12-14	✓	✗	✗	Apache Log4j 2.14.1 - Information Disclosure	Remote	Java	le0n13p4
2021-11-11	✓	✓	✓	Apache HTTP Server 2.4.50 - Remote Code Execution (RCE) (2)	WebApps	Multiple	Valentin Lobstein
2021-10-25	✓	✗	✗	Apache HTTP Server 2.4.50 - Remote Code Execution (RCE) (2)	WebApps	Multiple	ThelastWV
2021-10-13	✓	✓	✓	Apache HTTP Server 2.4.50 - Path Traversal & Remote Code Execution (RCE)	WebApps	Multiple	Lucas Souza
2021-10-06	✓	✓	✓	Apache HTTP Server 2.4.49 - Path Traversal & Remote Code Execution (RCE)	WebApps	Multiple	Lucas Souza
2021-09-28	✓	✗	✗	Apache JAMES Server 2.3.2 - Remote Command Execution (RCE) (Authenticated) (2)	Remote	Linux	sh1n13n
2021-08-04	✓	✗	✗	Apache OFBiz 17.12.01 - Remote Command Execution (RCE)	WebApps	Java	Adrian Diaz
2021-07-13	✓	✗	✗	Apache Tomcat 9.0.0.M1 - Cross-Site Scripting (XSS)	WebApps	Multiple	Central InfoSec
2021-07-13	✓	✗	✗	Apache Tomcat 9.0.0.M1 - Open Redirect	WebApps	Multiple	Central InfoSec
2021-06-30	✓	✗	✗	Apache Superset 1.1.0 - Time-Based Account Enumeration	WebApps	Multiple	Dolev Farhi
2021-06-02	✓	✗	✗	Apache Airflow 1.10.10 - Example DAG Remote Code Execution	WebApps	Multiple	Pipe Berba
2021-01-08	✓	✓	✓	Apache Flink 1.11.0 - Unauthenticated Arbitrary File Read (Metasploit)	WebApps	Java	SunCSR Team
2020-11-24	✓	✗	✗	Apache OpenMessaging 5.0.0 - 'hostname' Denial of Service	WebApps	Multiple	SunCSR
2020-11-17	✓	✗	✗	Apache Struts 2.5.20 - Double OGNL evaluation	Remote	Multiple	West Shepherd

Se ha detectado, que hay una versión 2.4.51 de apache httpd, la hemos revisado y hemos detectado que no es vulnerable, ya que es la versión actualizada y no hay vulnerabilidades asociadas a esa versión.

La versión que es vulnerable 2.4.51 actualmente está en funcionamiento 4.52.

CVE Details

The ultimate security vulnerability datasource

Log In Register

Switch to https://

Home

Browse :

- Vendors
- Products
- Vulnerabilities By Date
- Vulnerabilities By Type

Reports :

- CVSS Score Report
- CVSS Score Distribution

Search :

- Vendor Search
- Product Search
- Version Search
- Vulnerability Search
- By Microsoft Reference

Top 50 :

- Vendors
- Vendor CVSS Scores
- Products
- Product CVSS Scores
- Versions

Other :

- Microsoft Bulletins
- Bugtraq Entries
- CVE Definitions
- About & Contact
- Feedback
- CVE Help
- FAQ
- Articles

External Links :

- NVD Website
- CVE Web Site

View CVE :

(e.g.: 2009-1234 or 2010-1234 or 20101234)

View BID :

(e.g.: 12345)

Search By Microsoft Reference ID :

(e.g.: ms10-001 or 979352)

Vulnerability Details : CVE-2021-44790

A carefully crafted request body can cause a buffer overflow in the mod_lua multipart parser (rparsebody()) called from Lua scripts). The Apache httpd team is not aware of an exploit for the vulnerability though it might be possible to craft one. This issue affects Apache HTTP Server 2.4.51 and earlier.

Published Date : 2021-12-30 Last Update Date : 2022-01-12

CVSS Score: 7.5

Confidentiality Impact: Partial (There is considerable informational disclosure.)

Integrity Impact: Partial (Modification of some system files or information is possible, but the attacker does not have control over what can be modified, or the scope of what the attacker can affect is limited.)

Availability Impact: Partial (There is reduced performance or interruptions in resource availability.)

Access Complexity: Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)

Authentication: Not required (Authentication is not required to exploit the vulnerability.)

Gained Access: None

Vulnerability Type(s): Overflow

CWE ID: 787

Related OVAL Definitions

Title	Definition ID	Class	Family
RHSA-2022-0143: httpd security update (Important)	oval.com.redhat.rhsa-def-20220143	unix	
RHSA-2022-0258: httpd 2.4 security update (Important)	oval.com.redhat.rhsa-def-20220258	unix	

OVAL (Open Vulnerability and Assessment Language) definitions define exactly what should be done to verify a vulnerability or a missing patch. Check out the OVAL definitions if you want to learn what you should do to verify a vulnerability.

Products Affected By CVE-2021-44790

#	Product Type	Vendor	Product	Version	Update	Edition	Language
1	Application	Apache	httpd Server	*	*	*	Version Details Vulnerabilities

Number Of Affected Versions By Product

Vendor	Product	Vulnerable Versions
Apache	httpd Server	1

References For CVE-2021-44790

- https://www.tenable.com/security/insights/2022-01 CONFIRM
- https://securitydata.com/advisories/mag-20211224-00111 CONFIRM
- https://www.tenable.com/security/insights/2022-01 CONFIRM
- https://www.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/BFSVQHX77C72AH7C4RHHU8D9WQDL4YH FEDORA FEDORA-2021-29a536c2ae

5.4_Inyeccion SQL

La inyección de SQL es un tipo de ciberataque encubierto en el cual un hacker inserta código propio en un sitio web con el fin de quebrantar las medidas de seguridad y acceder a datos protegidos. Una vez dentro, puede controlar la base de datos del sitio web y secuestrar la información de los usuarios.

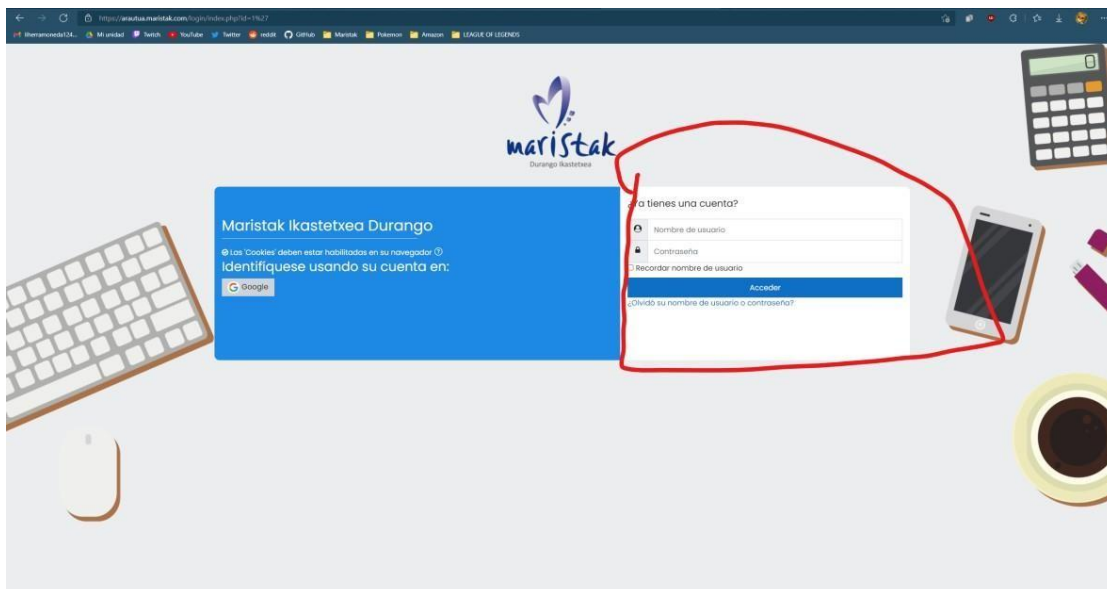
Riesgo: ■■■■ 4/4

Puerto: N/A

Detalles de la vulnerabilidad:

Mediante la herramienta SQLmap comprobaremos si es posible inyectar código SQL mediante el login de la página arautua.maristak.com/login/index.php.

En esta página tenemos la opción de iniciar con Google la cual no hay opción de hacer inyección SQL y en la otra opción de poner a mano el login como se muestra en la imagen posterior.



Iniciar la herramienta SQLmap y añadir el comando para escanear la opción de si se puede indexar código SQL.

```

root@kali: /home/kali
# sqlmap -u https://arautua.maristak.com

[!] 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 assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 22:25:37 /2022-01-30/

[22:25:37] [INFO] testing connection to the target URL
got a 303 redirect to 'https://arautua.maristak.com/login/index.php'. Do you want to follow? [Y/n] y
you have not declared cookie(s), while server wants to set its own ('MoodleSession=d3tdpeeqld0...vwp0jungs5b'). Do you want to use those [Y/n] y
[22:25:49] [INFO] checking if the target is protected by some kind of WAF/IPS
[22:25:49] [INFO] testing if the target URL content is stable
[22:25:49] [CRITICAL] no parameter(s) found for testing in the provided data (e.g. GET parameter 'id' in 'www.site.com/index.php?id=1'). You are advised to rerun with '--form s --crawl=2

[*] ending @ 22:25:49 /2022-01-30/

```

Para conseguir nombre de base de datos:

- `sqlmap -u [url] --dbs`

```

root@kali: /home/kali
# sqlmap -u https://arautua.maristak.com/login/index.php?id=1 --dbs

[!] 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 assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 22:27:42 /2022-01-30/

[22:27:42] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('MoodleSession=uthembsta6q...fgavklj6nq'). Do you want to use those [Y/n] y
[22:27:44] [INFO] testing if the target URL content is stable
[22:27:44] [WARNING] target URL content is not stable (i.e. content differs). sqlmap will base the page comparison on a sequence matcher. If no dynamic nor injectable parameters are detected, or in case of junk results, refer to user's manual paragraph 'Page comparison'
how do you want to proceed? [(C)ontinue/((s)tring/(r)egex/(q)uit)]
[22:27:48] [INFO] testing if GET parameter 'id' is dynamic
[22:27:48] [WARNING] GET parameter 'id' does not appear to be dynamic
[22:27:49] [WARNING] heuristic (basic) test shows that GET parameter 'id' might not be injectable
[22:27:49] [INFO] testing for SQL injection on GET parameter 'id'
[22:27:49] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[22:27:52] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[22:27:52] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[22:27:53] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[22:27:54] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[22:27:54] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[22:27:55] [INFO] testing 'Generic inline queries'
[22:27:55] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[22:27:56] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[22:27:56] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[22:27:57] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[22:27:58] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[22:27:58] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[22:27:59] [INFO] testing 'Oracle AND time-based blind'
it is recommended to perform only basic UNION tests if there is not at least one other (potential) technique found. Do you want to reduce the number of requests? [Y/n] y
[22:28:06] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[22:28:08] [WARNING] GET parameter 'id' does not seem to be injectable
[22:28:08] [CRITICAL] all tested parameters do not appear to be injectable. Try to increase values for '--level/' '--risk' options if you wish to perform more tests. If you suspect that there is some kind of protection mechanism involved (e.g. WAF) maybe you could try to use option '--tamper' (e.g. '--tamper=space2comment') and/or switch '--random-agent'

[*] ending @ 22:28:08 /2022-01-30/

```

Como se puede observar no deja añadir código SQL mediante el texto del login y no podremos ejecutar código SQL.

5.5_.htaccess information leak

.htaccess (abreviatura de Hipertexto Access) se define como un archivo de configuración utilizado en servidores web que se ejecutan exclusivamente en el software Apache Web Server.

Este archivo generalmente se compone de una secuencia de directivas bastante similar a los archivos de configuración estándar del servidor web Apache.

Generalmente, estas directivas son comandos de par clave-valor que especifican si una configuración debe estar activada o desactivada, pero pueden ser más complejas. La ubicación del archivo suele estar en la carpeta raíz del sitio web, pero eso dijo que también podría estar en otras ubicaciones.

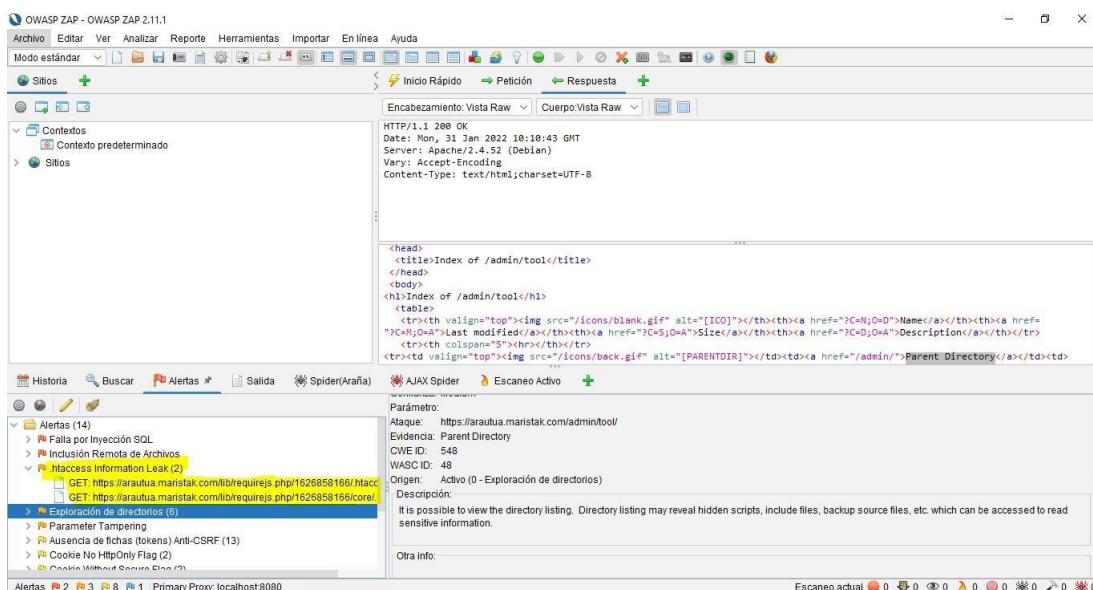
Riesgo: ■■ 2/4

Puerto: 80 (http)

Detalles de la vulnerabilidad:

Los archivos htaccess se pueden usar para modificar la configuración del software del servidor web Apache para habilitar/deshabilitar funcionalidades y características adicionales que el software del servidor web Apache tiene para ofrecer.

Mediante la URL de la página web hemos ido accediendo hasta acceder al archivo htaccess el cual nos indica la configuración del software.



OWASP ZAP - OWASP ZAP 2.11.1

Archivo Editar Ver Analizar Reporte Herramientas Importar En línea Ayuda

Modo estándar

Inicio Rápido Petición Respuesta

Encabezamiento: Vista Raw Cuerpo: Vista Raw

HTTP/1.1 200 OK
Date: Mon, 31 Jan 2022 10:10:43 GMT
Server: Apache/2.4.52 (Debian)
Vary: Accept-Encoding
Content-Type: text/html; charset=UTF-8

<head>
<title>Index of /admin/tool</title>
</head>
<body>
<h1>Index of /admin/tool</h1>
<table>
<tr><th align="top"><th align="left">Name</th><th align="right">Size</th><th align="left">Description</th></tr>
<tr><td align="top"><td align="left">../<td align="right"><td align="left">Parent Directory</td></tr>

Historia Buscar Alertas Salida Spider (Araña) AJAX Spider Escaneo Activo

Alertas (14)
Falla por Inyección SQL
Inclusión Remota de Archivos
GET: https://araua.mariastak.com/lib/requirejs.php/162858166/htacc
GET: https://araua.mariastak.com/lib/requirejs.php/162858166/core/

Exploración de directorios (6)
Parameter Tampering
Ausencia de fichas (tokens) Anti-CSRF (13)
Cookie No HttpOnly Flag (2)
Cookie Without SameSite (2)

Parámetro:
Ataque: https://araua.mariastak.com/admin/tool/
Evidencia: Parent Directory
OWID: 549
WASID: 48
Origen: Activo (0 - Exploración de directorios)
Descripción:
It is possible to view the directory listing. Directory listing may reveal hidden scripts, include files, backup source files, etc. which can be accessed to read sensitive information.
Otra info:

Alertas 2 3 8 1 Primary Proxy: localhost:8080 Escaneo actual 0 0 0 0 0 0 0 0 0 0

[illegible]

7.- Conclusión:

Los objetivos de la auditoría eran evaluar el nivel de seguridad de la infraestructura de la página web arautua.maristak.com, de manera básica.

Tal y como ha quedado reflejado en el informe, no existen vulnerabilidades graves en la web. Resulta notable las aplicaciones y los servicios del sitio web están actualizadas a la hora de pasar los escáneres con las diferentes herramientas OSINT.

Al realizar el análisis de vulnerabilidades hemos tenido problemas a la hora de explotar las mismas ya que estaban los servicios bien protegidos, por ejemplo:

- Inyección SQL.
- Inclusión remota de archivos.

La herramienta de búsqueda nos notifica que se podía realizar inyección SQL, al utilizar el programa SQLMAP hemos comprobado que la notificación era incorrecta ya que no dejaba introducir código SQL.

Adema través de la red mediante la herramienta Maltego se han detectado varios correos, teléfonos, subdominios... pueden ser existentes o no, pero son de fácil comprobación. Se recomienda un exhaustivo análisis por parte del desarrollador, para poder solucionar los problemas leves detectados.

Nota: Recordamos que esta es una auditoría básica. La cantidad de vulnerabilidades encontradas, son tantas, que se recomienda urgentemente una auditoría completa y con las correcciones correspondientes.

Duración de la auditoría: 5 días.

Duración de una auditoría normal: 3 a 7 días.