



ID
ID E X

GRUPO 1

***Eneko
González,
Xabier Parra y
David Lobo.***

Informe de intrusión externo.

Auditoría externa 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

Contenido

1. Objetivo y alcance	4
2. Sumario ejecutivo	5
3. Detalles de resultados técnicos	6
4. Herramientas	7
4.1 Whois	7
4.2 Maltego	8
4.3 Nmap	9
4.4 Nessus	10
4.5 OWASP Zap	11
5. Vulnerabilidades:	12
5.1 Criterio de clasificación de vulnerabilidades.	12
5.2 Resumen de vulnerabilidades detectadas.	12
6. Enumeración de vulnerabilidades	13
7. Conclusión	15

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:

Maristak.com 81.47.163.249

Dominios: 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.

Se ha detectado varias vulnerabilidades de nivel 4 (Alto) que podría provocar que un atacante realizara consultas directamente a la base de datos para obtener información; esta es la que tiene más riesgo. También se ha detectado posible denegación de servicio, donde la página podría quedar inutilizada durante el ataque.

Existen algunas vulnerabilidades de niveles 2 y 3 donde la más importante permitiría poder engañar al usuario para enviar su identificador de sesión o incluso modificar el código de la página en la sesión del usuario para engañarle alterando su contenido.

Por otro lado, se detectan configuraciones que ayudarían a un posible atacante a determinar si un usuario existe en la aplicación y por lo tanto poder focalizar ataques sobre usuarios concretos para obtener su información de solicitud.

Existen algunas otras vulnerabilidades de nivel bajo que no suponen a día de hoy 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.

Por lo tanto, explotando las vulnerabilidades detectadas, un intruso podría llegar a realizar:

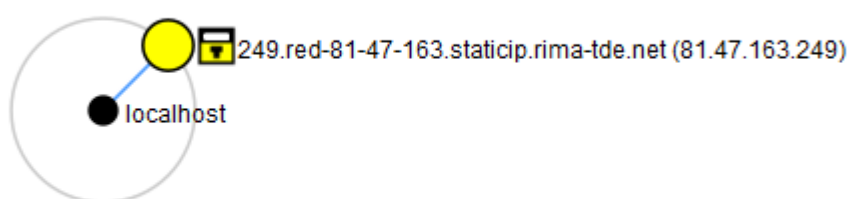
- Control del panel de administración de la página a través de ataque de inyección de SQL, entrada directa al puerto ftp, XSS y CSRF entre otras...
- Uso de credenciales en texto plano.
- Información de la base de datos de la página e información detallada de personas que participan en la misma de forma directa o indirecta (acceso a nombres, correos electrónicos y teléfonos particulares).

Recopilar información de la estructura del sistema, versiones, arquitectura, servidor web...

3. Detalles de resultados técnicos

IP 81.47.163.249

- Sistema operativo Debian (95%)
- Servidor Web Apache2.4.38 (97%)
-



Puerto	Protocolo	Servicio	Versión
80	TCP	HTTP	Apache 2.4.52
443	TCP	HTTP	Apache 2.4.52(Debian)
4117	TCP	HTTP	Nginx
4118	TCP	SSH	OpenSSHDebian 5
4126	TCP	DDERPL	
8023	TCP	SSH	OpenSsh 8.4
8080	TCP	HTTP-PROXY	

4. Herramientas

4.1 Whois

Mediante la herramienta OSINT Whois recopilaremos datos de una Base de datos pública en la que se almacenan los datos de titularidad de los dominios y sus fechas de expiración. La información del dominio (Whois) se muestra en Internet siempre, puedes hacer la consulta de cualquier dominio de Internet en nuestra pestaña Whois y verás los datos de su titular. Aquí se encuentran los datos visibles del dominio en este caso se puede apreciar la dirección IP y la compañía que les ofrece el servicio, también se pueden apreciar la versión de apache el sistema operativo...

The screenshot displays the OSINT Whois tool interface. At the top, a search bar contains 'www.maristak.com'. Below the search bar, there are buttons for 'API Request' and 'Download'. The results section shows '4 results'. The first result is for 'www.maristak.com', which is owned by 'Sectigo Limited' and was scanned on '2020-10-08'. It shows DNS records for 'A: 81.47.163.249 - telefonica de espana'. The second result is for 'maristak.com', which is marked as 'SEVERE' and was scanned on '2021-08-11'. It shows DNS records for 'A: 81.47.163.249 - telefonica de espana', 'MX: aspmx3.googlemail.com', 'MX: aspmx.L.google.com', and 'MX: alt2.aspmx.L.google.com'. It also shows the top countries as '[ES] Spain' and '[US] United States', the top HTTP status codes as '200 OK', and the top title as 'GESTION CON PERSONAS'. The interface includes a world map and various icons for different services like Apache, Debian, Drupal, and jQuery.

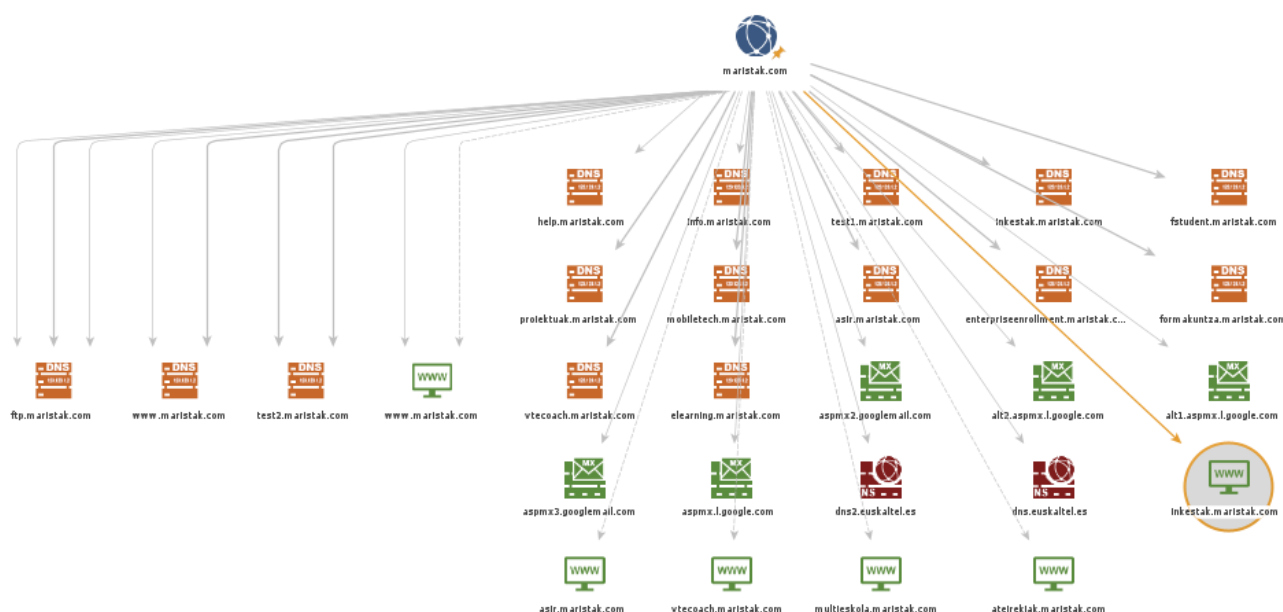
Domain	Owner	Scanned	DNS Records	WHOIS	Top Countries	Top HTTP Status Codes	Top Title
www.maristak.com	Sectigo Limited	2020-10-08	A: 81.47.163.249 - telefonica de espana		[ES] Spain 2 [US] United States 2	200 OK 3	GESTION CON PERSONAS 1
maristak.com	SEVERE	2021-08-11	A: 81.47.163.249 - telefonica de espana MX: aspmx3.googlemail.com MX: aspmx.L.google.com MX: alt2.aspmx.L.google.com				

4.2 Maltego

Esta herramienta OSINT la podemos usar en el momento de recolectar información en una auditoría. Con SpiderFoot, podremos hacer escaneos sobre un dominio, una web, una ip, un mail o una red.

para 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 IPs, emails, teléfonos, ubicaciones geográficas...


Podemos apreciar la arquitectura del dominio y sus subdominios.



4.3 Nmap

es una herramienta gratuita de código abierto para la exploración de vulnerabilidades y la detección de redes. Los administradores de red utilizan Nmap para identificar qué dispositivos se están ejecutando en sus sistemas, descubrir los hosts disponibles y los servicios que ofrecen, encontrar puertos abiertos y detectar riesgos de seguridad.

Lanzaremos un escáner a la IP del dominio para encontrar puertos abiertos y así poder pasar a la siguiente fase de explotación, también podemos apreciar la versión de los servicios lo que nos dará pistas para poder efectuar el ataque.

 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

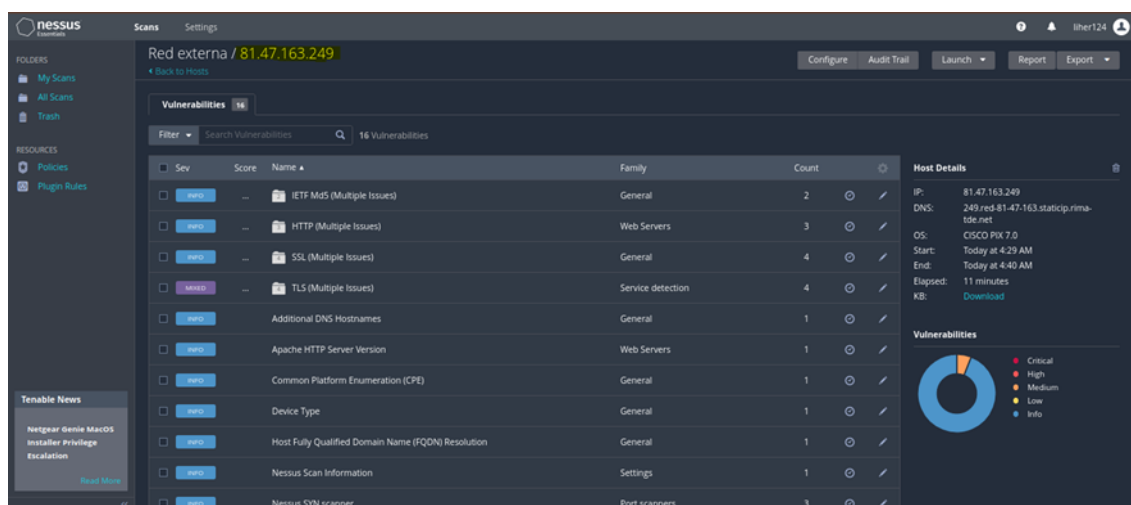
249.red-81-47-163.s

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		

4.4 Nessus

es uno de los escáneres de vulnerabilidades más populares y mejor estructurados del mercado, su alcance involucra manejo de dispositivos móviles, análisis de vulnerabilidades de sistemas operativos y aunque no es su fuerte, también realiza escaneos de aplicativos webs.

Después del análisis podemos apreciar mediante un gráfico como de seguro es el dominio las vulnerabilidades que tiene y la gravedad de ellas.



4.5 OWASP Zap

es un escáner de seguridad web de código abierto. Pretende ser utilizado como una aplicación de seguridad y como una herramienta profesional para pruebas de penetración. ... La aplicación puede desempeñarse en modo residente el cual es controlado mediante el API REST.

The screenshot displays the OWASP ZAP web application security scanner interface. The main pane shows the raw HTTP response of a GET request to `https://arautus.maristak.com/auth/autologin.php?id=1&sesskey=3f7070DPdP&wantsurl=http%3A%2F%2Fwww.google.com%2Fsearch%3Fq%3DOWASP%2520ZAP`. The response status is 200 OK. The left sidebar lists various alerts, with 'Inclusión Remota de Archivos' (Remote File Include) highlighted. The bottom pane provides details for this alert, including the URL, risk level (High), confidence (Medium), and a description of the RFI attack technique.

Alertas (19)

- Falta por Inyección SQL
- POST: `https://arautus.maristak.com/login/index.php`
- Inclusión Remota de Archivos**
- GET: `https://arautus.maristak.com/auth/autologin.php?id=1&sesskey=3f7070DPdP&wantsurl=http%3A%2F%2Fwww.google.com%2Fsearch%3Fq%3DOWASP%2520ZAP`
- Access Information Leak (2)
- Application Error Disclosure (1571)
- Exploración de directorios (244)
- Parameter Tampering
- X-Frame-Options Header Not Set (1574)
- Application Error Disclosure (15)
- Ausencia de fichas (tokens) Anti-CSRF (106)
- Cookie No HttpOnly Flag (3)

Inclusión Remota de Archivos

URL: `https://arautus.maristak.com/auth/autologin.php?id=1&sesskey=3f7070DPdP&wantsurl=http%3A%2F%2Fwww.google.com%2Fsearch%3Fq%3DOWASP%2520ZAP`

Riesgo: **High**

Confianza: Medium

Parámetro: `wantsurl`

Ataque: `http://www.google.com/search?q=OWASP%20ZAP`

Evidencia: `<title>Inicio sesión: Cuentas de Google</title>`

CWE ID: 98

WASC ID: 5









Origen: Activo (7 - Inclusión Remota de Archivos)

Descripción: Remote File Include (RFI) es una técnica de ataque muy utilizada para poder explotar los mecanismos de "Inclusión dinámica de los archivos" en las aplicaciones web. Cuando las aplicaciones web toman la entrada del usuario (URL, valor del parámetro, etc) y las cambian a los comandos de incluir los archivos, la aplicación web puede ser engañada para incluir los archivos remotos con un código maligno.

Otra info:

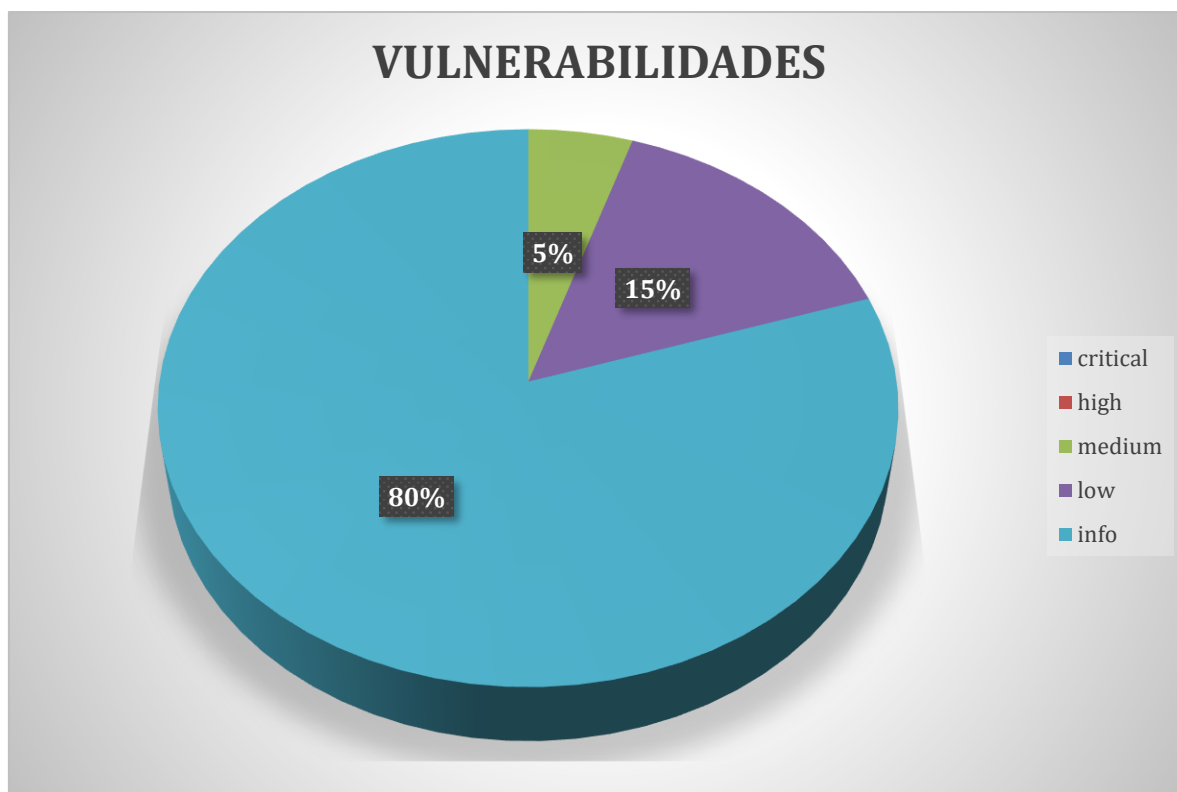
5. Vulnerabilidades:

5.1 Criterio de clasificación de vulnerabilidades.

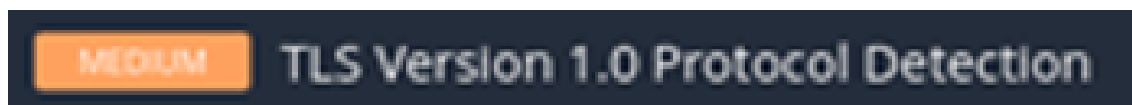
-   Un atacante podría tomar el control total sobre el host, por ejemplo, acceso a lectura y escritura del sistema de ficheros, ejecución de comandos arbitrarios.
-   Acceso a información sensible en el host, incluyendo sistemas de seguridad o acceso a ficheros comprometidos, revelación de directorios 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.

5.2 Resumen de vulnerabilidades detectadas.

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



6. Enumeración de vulnerabilidades



Riesgo: ■ ■ 2/4

Puerto: 443

Detalles de la vulnerabilidad

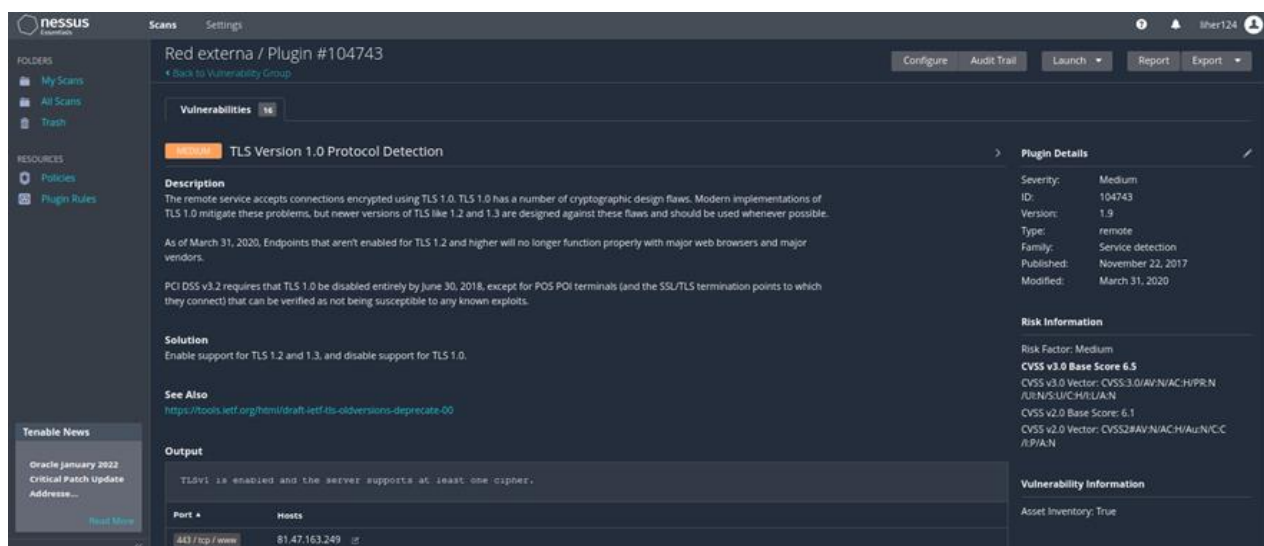
El servicio remoto acepta conexiones encriptadas usando TLS 1.0. TLS 1.0 tiene varios defectos de diseño criptográfico. Las implementaciones modernas de TLS 1.0 remedian estos problemas. A partir del 31 de marzo de 2020, los puntos finales que no estén habilitados para TLS 1.2 y versiones posteriores ya no funcionarán correctamente con los principales navegadores web y los principales proveedores.

Se recomienda

Habilite el soporte para TLS 1.2 y 1.3, y deshabilite el soporte para TLS 1.0.

Explotación de la vulnerabilidad

Mediante el Nessus se ha conseguido encontrar una vulnerabilidad de nivel medio la cual nos dará pistas a la hora de la explotación.



The screenshot shows the Nessus interface with the following details for the 'TLS Version 1.0 Protocol Detection' vulnerability (Plugin #104743):

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

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: 443 / tcp / www

Hosts: 81.47.163.249

Vulnerabilidad por inyección SQL e Inclusión remota de archivos

Riesgo: ■■■■ 4/4

Puerto: 80/443

Detalles de la vulnerabilidad

La inyección SQL es una vulnerabilidad de seguridad web que permite que un atacante interfiera con las consultas que una aplicación realiza en su base de datos. En general, permite a un atacante ver datos que normalmente no pueden recuperar.

Se recomienda

Escapar los caracteres especiales utilizados en las consultas SQL, Delimitar los valores de las consultas, Delimitar los valores de las consultas, Asignar mínimos privilegios al usuario que conectará con la base de datos, Programar bien.

Explotación de la vulnerabilidad

También se ha encontrado la vulnerabilidad de fallo por inyección SQL, pero no se conseguido explotar la vulnerabilidad, continuando con las vulnerabilidades se ha detectado inclusión remota de archivos la cual tampoco sea podido vulnerar.

The screenshot shows the Burp Suite interface. The top menu bar includes 'Historia', 'Buscar', 'Alertas', 'Salida', and 'Spider(A)'. The left sidebar shows a tree view of alerts, with 'Inclusión Remota de Archivos' selected. The main panel displays the details of this alert, including the URL, risk level, confidence, and a description of the RFI attack.

Alertas (19)

- Falla por Inyección SQL
 - POST: <https://arautua.maristak.com/login/index.php>
- Inclusión Remota de Archivos**
 - GET: <https://arautua.maristak.com/auth/oauth2/login.php?id=1&session=3fj70DPdP&wantsurl=http%3A%2F%2Fwww.google.com%2Fsearch%3Fq%3DOWASP%2520ZAP>
 - .htaccess Information Leak (2)
 - Application Error Disclosure (1571)
 - Exploración de directorios (244)
 - Parameter Tampering
 - X-Frame-Options Header Not Set (1574)
 - Application Error Disclosure (15)
 - Ausencia de fichas (tokens) Anti-CSRF (106)
 - Cookie No HttpOnly Flag (3)

Inclusión Remota de Archivos

URL: <https://arautua.maristak.com/auth/oauth2/login.php?id=1&session=3fj70DPdP&wantsurl=http%3A%2F%2Fwww.google.com%2Fsearch%3Fq%3DOWASP%2520ZAP>

Riesgo: High

Confianza: Medium

Parámetro: wantsurl

Ataque: <http://www.google.com/search?q=OWASP%20ZAP>

Evidencia: <title>Inicio sesión: Cuentas de Google</title>

CWE ID: 98

WASC ID: 5

Origen: Activo (7 - Inclusión Remota de Archivos)

Descripción:

Remote File Include (RFI) es una técnica de ataque muy utilizada para poder explotar los mecanismos de "Inclusión dinámica de los archivos" en las aplicaciones web. Cuando las aplicaciones web toman la entrada del usuario (URL, valor del parámetro, etc) y las cambian a los comandos de incluir los archivos, la aplicación web puede ser engañada para incluir los archivos remotos con un código maligno.

7. Conclusión

Después de diferente escáner con diferentes herramientas se ha llegado a la conclusión de que las vulnerabilidades encontradas no son de nivel alto lo que supone que no sean fáciles de vulnerar.

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

Tal y como ha quedado reflejado en el informe, existen una vulnerabilidad de nivel medio

Nota: Recordamos que esta es una auditoría básica. La cantidad de vulnerabilidades encontradas, son pocas, pero eso no exime de estar al tanto de las vulnerabilidades encontradas

Duración de la auditoría: 3 días

Duración de una auditoría normal: 7 a 15 días.