PRUEBA - DOCUMENTACIÓN Y REPORTES DE HALLAZGOS DE SEGURIDAD

Autor: Carlos Aliendres

29 de agosto de 2025

INFORME EJECUTIVO – ANALISIS DE VULNERABILIDADES http://testfire.net/

Autor: Carlos Aliendres

29 de agosto de 2025

Resumen Ejecutivo:

El presente informe resume los hallazgos de la evaluación seguridad realizada al sitio http://testfire.net/ con Nessus. Nuestro análisis identifico vulnerabilidades criticas y de alto riesgo que pueden comprometer la confidencialidad, integridad y disponibilidad de nuestros activos digitales. El riesgo principal radica en la exposición a ataques de inyección de código, el acceso no autorizado a archivos, lo que puede resultar en la filtración de datos sensibles y la interrupción de servicios. En este documento se proponen acciones de mitigación prioritarias para fortalecer la seguridad del sitio.

Descripción Detallada:

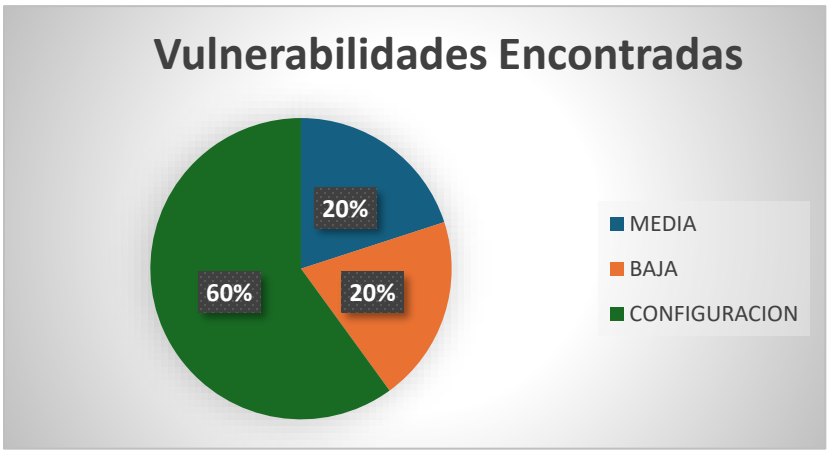
En el escaneo del sitio se identificaron 5 vulnerabilidades clave, categorizadas por su nivel de riesgo e impacto potencial. Las vulnerabilidades pueden ser aprovechadas en un ataque se identifican las siguientes:

Vulnerabilidades de medio y bajo riesgo

- Protocolo TLS versión 1.1 obsoleto: nuestros servidores podrían ser vulnerables a ataques de degradación de cifrado.
- Módulo Diffie-Hellman SSL/TLS <= 1024 bits: le permitiría a un atacante descifrar el tráfico SSL/TLS.

Vulnerabilidades de configuración:

- Certificado SSL firmado con un algoritmo hash débil: podría permitir que un atacante genere un certificado fraudulento.
- Huellas dactilares del sistema operativo detectadas: esta información puede ser utilizada por un atacante para buscar exploits específicos y acelerar el reconocimiento de un ataque.
- Tipo y versión del servidor HTTP: puede ser utilizada por un atacante para buscar vulnerabilidades específicas del servidor.



Impacto:

Estas vulnerabilidades representan impacto económico el cual puede ser significativo, ya que será el resultado directo de la explotación de estas vulnerabilidades, y los cuales pueden incluir:

- **Costos de Remediación:** incluyen los costos de recuperación, forense digital, y posibles multas por incumplimiento de normativas.
- **Pérdida de Ingresos:** Incluyen los costos por interrupción de servicios.
- **Perdida de Reputación**: representa también pérdida económica ya que disminuye significativamente las oportunidades de negocios.
- **Perdida de Propiedad Intelectual:** podría resultar en el robo de datos sensibles, propiedad intelectual o secretos comerciales.

Recomendaciones:

Para mitigar los riesgos identificados, se propone un plan de acción priorizando acciones para mejorar la seguridad del sitio:

Mitigación de Vulnerabilidades:

- **Actualización de Protocolos:** Deshabilitar TLS 1.1 y habilitar solo versiones seguras como TLS 1.2 o superior.
- **Actualización de Módulos:** Actualizar el módulo Diffie-Hellman a una versión más segura y con un tamaño de clave mayor (mayor a 1024 bits).
- **Actualización de Certificados:** Generar nuevos certificados con algoritmos hash más fuertes y seguros.
- **Encriptación de Comunicaciones**: Deshabilitar el tráfico en texto plano en el puerto 80 y forzar el uso de HTTPS en todas las comunicaciones del sitio.

INFORME TÉCNICO – ANALISIS DE VULNERABILIDADES http://testfire.net/

Autor: Carlos Aliendres

29 de agosto de 2025

Confidencial
Versión 1.0

Resumen Técnico:

Este informe detalla los hallazgos de un escaneo de vulnerabilidades en el sitio web http://testfire.net/. El objetivo fue identificar y documentar las debilidades de seguridad encontradas. El análisis reveló cinco vulnerabilidades, incluyendo una de severidad media que podría ser vulnerable a ataques de degradación de cifrado. Se recomienda la aplicación de los parches y las configuraciones de seguridad detalladas en la sección de remediación para mitigar los riesgos.

Metodología de Escaneo:

- Se utilizó la herramienta Nessus para realizar un escaneo de vulnerabilidades. El objetivo fue el dominio testfire.net. El escaneo se ejecutó con la política Basic Network Scan, evaluando la exposición del servidor a vulnerabilidades conocidas y desconfiguraciones.
- No se realiza explotaciones activas.
- Se considera niveles de Severidad: CVSS v3.0

Hallazgos de Vulnerabilidades:

Las siguientes vulnerabilidades fueron identificadas y categorizadas según su riesgo:

Nombre de la Vulnerabilidad	**SSL Certificate Signed Using Weak Hashing Algorithm (Known CA)** - Certificado SSL firmado con un algoritmo hash débil (CA conocida)
ID Plugin	**95631**
CVSS v3.0	**N/A**
Puerto Afectado	**TCP (443)**
Factor de Riesgo	Ninguno
Descripción	El servicio remoto utiliza un certificado de CA conocido en la cadena de certificados SSL, firmado mediante un algoritmo de hash criptográficamente débil (p. ej., MD2, MD4, MD5 o SHA1). Estos algoritmos de firma son vulnerables a ataques de colisión (por ejemplo, CVE-2004-2761). Un atacante puede aprovechar esto para generar otro certificado con la misma firma digital, lo que le permite hacerse pasar por el servicio afectado.
Impacto	Un atacante podría generar un certificado fraudulento con la misma firma digital.

Evidencia (Nessus)	**95631 - SSL Certificate Signed Using Weak Hashing Algorithm (Known CA)** Synopsis A known CA SSL certificate in the certificate chain has been signed using a weak hashing algorithm. Description The remote service uses a known CA certificate in the SSL certificate chain that has been signed using a cryptographically weak hashing algorithm (e.g., MD2, MD4, MD5, or SHA1). These signature algorithms are known to be vulnerable to collision attacks (CVE-2004-2761, for example). An attacker can exploit this to generate another certificate with the same digital signature, allowing the attacker to masquerade as the affected service. Note that this plugin reports all SSL certificate chains signed with SHA-1 that expire after January 1, 2017 as vulnerable. This is in accordance with Google's gradual sunsetting of the SHA-1 cryptographic hash algorithm. Note that this plugin will only fire on root certificates that are known certificate authorities as listed in Tenable Community Knowledge Article 000001752. That is what differentiates this plugin from plugin 35291, which will fire on any certificate, not just known certificate authority root certificates. Known certificate authority root certificates are inherently trusted and so any potential issues with the signature, including it being signed using a weak hashing algorithm, are not considered security issues. See Also http://www.nessus.org/u?ae636e78 https://tools.ietf.org/html/rfc3279 http://www.nessus.org/u?9bb87bf2 Solution Contact the Certificate Authority to have the certificate reissued. Risk Factor None References BID 11849 BID 33065 XREF CWE:310 Plugin Information Published: 2016/12/08, Modified: 2022/10/12 testfire.net 40
Solución - Remediación	• Establecer contacto con el ente certificador y solicitar le emisión de un nuevo certificado. • Verificar periódicamente la vigencia de los certificados y configurar alertas para su renovación.
Referencias	BID 11849 BID 33065 CWE:310

Nombre de la Vulnerabilidad	**HTTP Server Type and Version** - Tipo y versión del servidor HTTP
ID Plugin	**10107**
CVSS v3.0	**N/A**
Puerto Afectado	**TCP (443)** **TCP (80)** **TCP (8080)**
Factor de Riesgo	Ninguno
Descripción	Se detectó el tipo y versión del servidor web, **Apache-Coyote/1.1**. Esta información, aunque no es una vulnerabilidad, puede ser utilizada por un atacante para buscar *exploits* específicos.
Impacto	Información sensible que puede ser utilizada por atacantes para identificar exploits específicos contra esa versión.

Evidencia (Nessus)	**10107 - HTTP Server Type and Version**
	Synopsis
	A web server is running on the remote host.
	Description
	This plugin attempts to determine the type and the version of the remote web server.
	Solution
	n/a
	Risk Factor
	None
	References
	XREF IAVT:0001-T-0931
	Plugin Information
	Published: 2000/01/04, Modified: 2020/10/30
	Plugin Output
	tcp/80/www
	`The remote web server type is :`
	`Apache-Coyote/1.1`
	Plugin Output
	tcp/443/www
	`The remote web server type is :`
	`Apache-Coyote/1.1`
	tcp/8080/www
	`The remote web server type is :`
	`Apache-Coyote/1.1`

Solución - Remediación	• Configurar el server para ocultar la información de la cabecera HTTP sin revelar la versión ni el sistema operativo. • Implementar un **WAF (Web Application Firewall)** para limitar la exposición de información sensible.
Referencias	XREF IAVT:0001-T-0931BID 33065

Nombre de la Vulnerabilidad	**TLS Version 1.1 Deprecated Protocol** – Protocolo TLS versión 1.1 obsoleto
ID Plugin	**157288**
CVSS v3.0	**6.5**
Puerto Afectado	**TCP (443)**
Factor de Riesgo	MEDIO
Descripción	El servicio remoto acepta conexiones cifradas con TLS 1.1. TLS 1.1 no es compatible con los conjuntos de cifrado actuales ni con los recomendados. Los cifrados que admiten cifrado antes del cálculo de MAC y los modos de cifrado autenticados, como GCM, no se pueden utilizar con TLS 1.1.
Impacto	Permite ataques de downgrade y limita el uso de cifrados modernos como AES-GCM.

Evidencia (Nessus)	**157288 - TLS Version 1.1 Deprecated Protocol** Synopsis The remote service encrypts traffic using an older version of TLS. Description The remote service accepts connections encrypted using TLS 1.1. TLS 1.1 lacks support for current and recommended cipher suites. Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1 As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors. See Also https://datatracker.ietf.org/doc/html/rfc8996 http://www.nessus.org/u?c8ae820d Solution Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1. Risk Factor Medium CVSS v3.0 Base Score 6.5 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N) CVSS v2.0 Base Score 6.1 (CVSS2#AV:N/AC:H/Au:N/C:C/I:P/A:N) References XREF CWE:327 Plugin Information Published: 2022/04/04, Modified: 2024/05/14 Plugin Output tcp/443/www testfire.net 8 `TLSv1.1 is enabled and the server supports at least one cipher.`
Solución – Remediación	• Habilitar el soporte para TLS 1.2 y/o 1.3, y deshabilite el soporte para TLS 1.1. • Validar que no existan aplicaciones heredadas que dependan de TLS 1.1 antes de su desactivación.
Referencias	CWE:327

Nombre de la Vulnerabilidad	**SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)** – Módulo Diffie-Hellman SSL/TLS <= 1024 bits (bloqueo)
ID Plugin	**83875**
CVSS v3.0	**3.7**
Puerto Afectado	**TCP (443)**
Factor de Riesgo	BAJO
Descripción	El host remoto permite conexiones SSL/TLS con uno o más módulos Diffie-Hellman menores o iguales a 1024 bits. Mediante criptoanálisis, un tercero podría encontrar el secreto compartido rápidamente (dependiendo del tamaño del módulo y los recursos del atacante). Esto podría permitir que un atacante recupere el texto plano o potencialmente vulnere la integridad de las conexiones.
Impacto	Posible descifrado parcial del tráfico HTTPS en escenarios de ataque avanzado.

Evidencia (Nessus)	**83875 - SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)** Synopsis The remote host allows SSL/TLS connections with one or more Diffie-Hellman moduli less than or equal to 1024 bits. Description The remote host allows SSL/TLS connections with one or more Diffie-Hellman moduli less than or equal to 1024 bits. Through cryptanalysis, a third party may be able to find the shared secret in a short amount of time (depending on modulus size and attacker resources). This may allow an attacker to recover the plaintext or potentially violate the integrity of connections. See Also https://weakdh.org/ Solution Reconfigure the service to use a unique Diffie-Hellman moduli of 2048 bits or greater. Risk Factor Low CVSS v3.0 Base Score 3.7 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N) CVSS v3.0 Temporal Score 3.2 (CVSS:3.0/E:U/RL:O/RC:C) VPR Score 4.5 EPSS Score 0.9391 CVSS v2.0 Base Score 2.6 (CVSS2#AV:N/AC:H/Au:N/C:N/I:P/A:N) CVSS v2.0 Temporal Score 1.9 (CVSS2#E:U/RL:OF/RC:C) testfire.net 12
Solución – Remediación	• Configurar el servicio para utilizar un módulo Diffie-Hellman único de 2048 bits o más. • Revisar la suite de cifrados habilitados y desactivar los inseguros.
Referencias	BID 74733 CVE-2015-4000 XREF CEA-ID:CEA-2021-0004

Nombre de la Vulnerabilidad	**OS Fingerprints Detected** - Huellas dactilares del sistema operativo detectadas
ID Plugin	**209654**
CVSS v3.0	**N/A**
Puerto Afectado	**TCP (0)**
Factor de Riesgo	N/A
Descripción	Mediante una combinación de sondas remotas (TCP/IP, SMB, HTTP, NTP, SNMP, etc.), fue posible obtener una o más huellas digitales del sistema remoto. Si bien el resultado de mayor confianza se reportó en el complemento 11936, «Identificación del SO», aquí se reporta el conjunto completo de huellas digitales detectadas.
Impacto	Facilita a un atacante obtener información sobre el sistema operativo y preparar ataques dirigidos.

Evidencia (Nessus)	**209654 - OS Fingerprints Detected**
	
	Synopsis
	Multiple OS fingerprints were detected.
	
	Description
	Using a combination of remote probes (TCP/IP, SMB, HTTP, NTP, SNMP, etc), it was possible to gather one or more fingerprints from the remote system. While the highest-confidence result was reported in plugin 11936, "OS Identification", the complete set of fingerprints detected are reported here.
	
	Solution
	n/a
	
	Risk Factor
	None
	
	Plugin Information
	Published: 2025/02/26, Modified: 2025/03/03
	
	Plugin Output
	tcp/0
	
	`Following OS Fingerprints were found`
	
	`Remote operating system : Microsoft Windows Server 2008 R2`
	`Confidence level : 56`
	`Method : MLSinFP`
	`Type : unknown`
	`Fingerprint : unknown`
	
	`Remote operating system : Dell EMC VMX`
	`Microsoft Windows Embedded Standard 7`
	`Confidence level : 59`
	`Method : SinFP`
	`Type : embedded`
	`Fingerprint : SinFP:`
	`P1:B11113:F0x12:W8192:O0204ffff:M1380:`
	`P2:B11113:F0x12:W8192:O0204ffff010303080402080affffffff44454144:M1380:`
	`P3:B00000:F0x00:W0:O0:M0`
	`P4:191303_7_p=8080R`
	
	`Following fingerprints could not be used to determine OS :`
	`HTTP:!:Server: Apache-Coyote/1.1`
	
	`SSLcert:!:i/CN:Sectigo RSA Domain Validation Secure Server CAi/O:Sectigo Limiteds/`
	`CN:demo.testfire.net`
	`a1e98d60388b84f4bbc550d7b61bb2b0cc8961fd`
	
	testfire.net 35

Solución - Remediación	No es una vulnerabilidad que se pueda "parchear". La mitigación se centra en: • Mantener el sistema operativo y servicios actualizados. • Minimizar servicios expuestos a Internet. • Implementar filtrado de tráfico y segmentación de red para reducir la información obtenible.
Referencias	N/A

Recomendaciones Generales:

- Migrar completamente a TLS 1.2/1.3 y usar cifrados modernos.
- Reemitir certificados con algoritmos seguros (SHA-256 o superior).
- Minimizar la exposición de información sensible en cabeceras y servicios.
- Mantener un plan de parches y actualizaciones periódicas.
- Considerar la implementación de un WAF como capa adicional de seguridad.

Conclusión:

El análisis de seguridad realizado identificó vulnerabilidades principalmente relacionadas con la exposición de información y el uso de protocolos criptográficos obsoletos.

Aunque ninguna vulnerabilidad crítica fue detectada, las debilidades encontradas pueden ser utilizadas por atacantes para reconocer el entorno, explotar cifrados débiles y preparar ataques más avanzados.