InFo-Cyber. Journal of Cybersecurity and Digital Forensics.
Volumen 1, Número 1. Año 2026. ISSN: en trámite.
https://revistas.ufasta.edu.ar/index.php/InFoCyber/index

INFO-CYBER CYBERSECURITY AND DIGITAL FORENSICS JOURNAL

Security.txt: El archivo de texto que puede salvar el mundo

Security.txt: The text file that could save the world

R. López Lio

Universidad Nacional Scalabrini Ortiz. San Isidro, Buenos Aires (Argentina)
lopezlio@gmail.com

https://orcid.org/0009-0000-3015-245X

Artículo de reflexión

Recibido: 22-06-2024. Aceptado: 24-02-2025. Publicado: 03-03-2026.

Universidad FASTA. Facultad de Ingeniería; Mar del Plata, Argentina.

Resumen

Este documento se refiere a la importancia del archivo security.txt para la adopción de una forma clara de dar a conocer los canales de contacto de una organización para recibir información acerca de vulnerabilidades relacionadas con sus servicios / aplicaciones expuestos, así como también del proceso de madurez de las organizaciones sobre sus procesos de gestión de vulnerabilidades.

Palabras clave

divulgación de vulnerabilidad, política de divulgación, gestión de vulnerabilidades

Abstract

This document refers to the importance of the security.txt file for adopting a clear way of publicizing an organization's contact channels for receiving information about vulnerabilities related to its exposed services/applications, as well as the maturity process of organizations regarding their vulnerability management processes.

Keywords

vulnerability disclosure, disclosure policy, vulnerability management.

RODRIGO LÓPEZ LIO es egresado de CAECE en Seguridad Informática (2015), posgrado en Análisis de Inteligencia Estratégica (2016) en el Instituto de Inteligencia de las Fuerzas Armadas. Tiene experiencia en seguridad de la información, investigaciones, equipos de respuesta a incidentes y es docente universitario en materias de ciberseguridad

I. INTRODUCCIÓN

¿Un archivo de texto? Sí, un simple archivo de texto. Estamos hablando del archivo Security.txt [1]. Este archivo, hoy en día, ya es un estándar (en abril de 2022 se publica finalmente como el RFC 9116) [2] que permite a quienes publican un sitio web dar a conocer las políticas de seguridad adoptadas y datos de contacto para quienes deseen reportar un fallo o vulnerabilidad.

¿Cómo es que un archivo va a salvarnos?

La propuesta del estándar surgió de la necesidad de los investigadores de seguridad de contar con canales claros de comunicación al momento de reportar un hallazgo.

Solo falta hacer la prueba uno mismo, visitar un sitio cualquiera y localizar los contactos del sitio, leer los términos y condiciones, recorrer la estructura del sitio y difícilmente encontraremos los correos de las áreas de seguridad o los pasos para reportar o la clave PGP utilizada. Y sí, es verdad que ya existe una convención acerca de la utilización de cuentas <SECURITY@domain> en el RFC 2142 [3], pero al margen de la adopción o no de estas cuentas de correo, estas no permiten identificar las prácticas o procesos definidos por la organización para la notificación de vulnerabilidades.

Esta situación tiende a dificultar las tareas de cualquier investigador de seguridad o de las propias áreas de seguridad y, en otras escalas, la de los CERT/CSIRT gubernamentales.

El estándar, propuesto por primera vez por Ed Foudil y Yakov Shafranovich, es un archivo que debe colocarse en la ubicación "/.well-known/security.txt" de un dominio; de esta manera, el archivo puede ser localizado y cualquier investigador (A.K.A researcher) de seguridad puede contactar a la organización en caso de que descubra una vulnerabilidad.

II. IMPLEMENTACIÓN

La implementación de security.txt es bastante sencilla. El archivo debe contener información de contacto, como una dirección de correo electrónico, y puede incluir otros datos, como la clave pública de cifrado, políticas de divulgación coordinada, etc.

El archivo debe contener una serie de campos que son de carácter obligatorio y otros opcionales.

-Contact: Campo de carácter requerido; se indica cuál será el canal de contacto a utilizar para comunicarse con la organización. Se sugiere indicar una dirección de correo del área de seguridad de la información.

- Expires: También es un campo requerido; se debe indicar para indicar la fecha a partir de la cual el archivo debe considerarse obsoleto. Será importante entonces mantenerlo actualizado.

- Encryption: Se utiliza para indicar que se encuentra disponible la clave PGP a fin de que las comunicaciones sean cifradas. Es relevante mencionar que las claves no deben aparecer en este campo, sino que se indicará la ubicación donde se puede ubicar la clave. Este campo es opcional.

-Acknowledgments: Permite indicar el reconocimiento que realiza la organización a aquellas personas u organizaciones que han colaborado anteriormente. El campo es opcional y se indica la ubicación donde se encuentran los agradecimientos.

- Policy: En este campo se especifica la ubicación de la política, que permite ampliar los detalles y pasos a seguir para el reporte de vulnerabilidades. El campo es opcional.

También se incluyen los campos *Preferred-Languages*; *Canonical*; *Hiring* y CSAF como opcionales.

Una vez que el archivo es completado con los campos, es recomendable firmarlo digitalmente antes de publicarlo. Como se mencionó anteriormente, el archivo debe alojarse bajo el directorio "/.well-known/". El archivo debe contener una serie de campos que son de carácter obligatorio y otros opcionales.

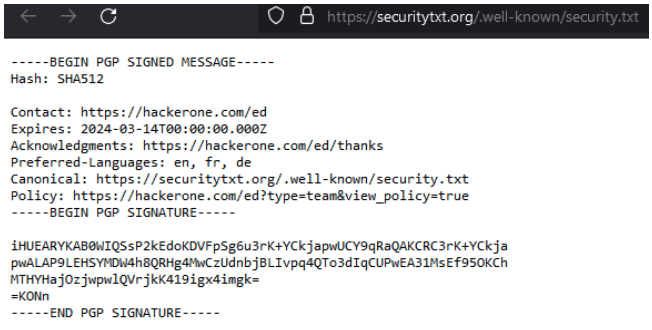

Fig. 1. Archivo Security.txt del sitio securitytxt.org.

Y eso sería todo, o casi todo.

III. BENEFICIOS Y DESAFÍOS

El uso de security.txt presenta varios beneficios. Principalmente, establece un canal de comunicación claro. Facilita la divulgación de vulnerabilidades. Permite a las organizaciones recibir los informes de seguridad de manera oportuna.

Es conveniente mencionar que la mera existencia de este archivo no debe ser considerada como un permiso para la ejecución de pruebas y análisis. Es muy recomendable revisar la utilización del campo Policy.

Sin embargo, también existen desafíos.

Lo primero que se nos puede venir a la mente es que la adopción de security.txt aún no es universal. No todas las organizaciones públicas o privadas lo han adoptado, ya sea por desconocimiento o falta de madurez. Lo segundo, que las organizaciones deben repensar sus procedimientos de gestión de vulnerabilidades. Se debe desarrollar qué hará la organización cuando sea contactada, por el canal que ahora definió, e informada de la existencia de una vulnerabilidad en el proyecto que tiene expuesto. ¿Cómo gestionará esta comunicación?, ¿cómo la remediará?, ¿cómo responderá? En fin, ¿cómo empezará a gestionar a partir de ahora?

Por otro lado, una incorrecta configuración de este archivo, o la falta de actualización de este, podría hacer llegar informes a partes no autorizadas, por lo que resulta de vital importancia el mantener actualizado dicho archivo.

A nivel de políticas públicas y estrategias de ciberseguridad, podemos destacar que el primer borrador del RFC fue propuesto en el 2017, y desde entonces, dependencias de gobiernos y distintas organizaciones lo han ido adoptando. Desde Estados Unidos, al recomendarlo en la BOD 20-01 [4] sobre las políticas de divulgación de vulnerabilidades y posteriormente en los CPGs (Cybersecurity Performance Goals) del CISA [5]. Reino Unido en 2020 publicó su Vulnerability Disclosure Toolkit [6], en donde se incluye la utilización del archivo y es respaldado por la Data Standards Authority [7], y a nivel gubernamental han ido más allá, permitiendo la notificación de reportes a través de HackerOne [8]. La Confederación Suiza también promueve su utilización [9] y puede observarse en el sitio de los autores que Italia, Alemania y Australia también. Sin dudas, es un excelente recurso para ser incluido en cualquier política pública en materia de ciberseguridad.

Inicialmente, aquí en Argentina se hizo una primera prueba a través del CERTar [10] en 2021. No obstante, a la fecha del presente artículo no se observa la presencia en sitios de gobierno.

Por otro lado, es esperable y deseable que las herramientas utilizadas para automatizar ciertos análisis de vulnerabilidades incorporen la existencia o no de este archivo en el *target* evaluado.

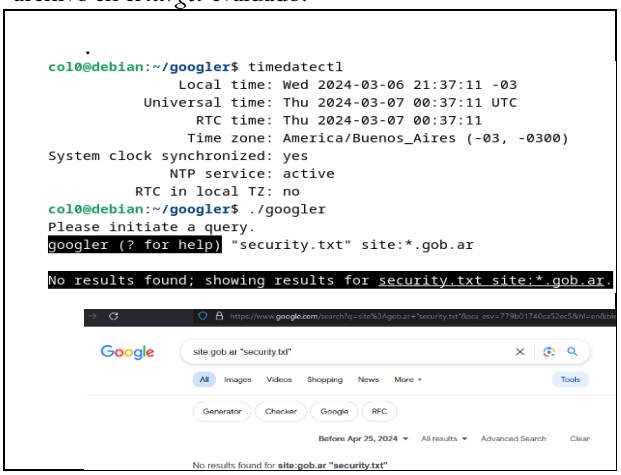

Fig.2. Resultados de búsqueda de security.txt en dominios .gob.ar.

IV. CONCLUSIONES

A pesar de estos desafíos, Security.txt representa un paso importante hacia la mejora y madurez de la comunicación en seguridad. Con una adopción más amplia y una mayor conciencia, Security.txt tiene el potencial de convertirse en una herramienta valiosa en la lucha contra las amenazas informáticas.

Si pensamos en el tiempo que pasa desde una vulnerabilidad descubierta hasta que es parcheada, en el que una organización tarda en descubrir la existencia de una vulnerabilidad en sus servicios o aplicaciones, o en el tiempo que se requiere para localizar a los responsables de efectuar los cambios, estamos hablando de un archivo que puede reducir drásticamente la exposición de una organización a un compromiso.

Habilitar los canales adecuados, dar a conocer el cómo y poder recibir notificaciones de hallazgos y reducir los tiempos de exposición.

Si lo pensamos a gran escala, como podría ser la implementación de Security.txt dentro de una política pública de ciberseguridad, por ejemplo, en cualquier servicio, aplicación o sitio publicado por parte del Sector Público Nacional, los informes de hallazgos de cualquier *researcher* llegarían oportunamente y se reducirían los tiempos de exposición. Por otro lado, ningún oportunista

se vería tentado de publicar un hallazgo en ninguna red social, ya que no existirían excusas para no realizar las notificaciones de manera adecuada. Pero para aquellos que lo implementen: "Don't ignore the report. Respond promptly to the finder and thank them. Feedback encourages engagement and they"ll be more inclined to help you again in the future" [11]

Sin duda, algo sobre lo que hay que aprender y aprehender. Lo peor que podría ocurrir al implementar Security.txt sería ignorar las comunicaciones recibidas. Es de prever que las organizaciones deban esforzarse (desarrollando nuevas capacidades) por entender los reportes recibidos para poder gestionarlos adecuadamente.

La implementación del estándar y el exponer públicamente un contacto de seguridad a la comunidad de seguridad en general fomenta un entorno de colaboración, animando a un gran número de personas expertas en seguridad a contribuir a la seguridad de una organización.

Security.txt no cubre el ciclo de vida completo de la gestión de vulnerabilidades; el estándar facilita una alerta temprana muy valiosa, pero aun así las organizaciones deberán trabajar sobre el desarrollo de sus procesos de clasificación y *triage* de vulnerabilidades [12].

AGRADECIMIENTO

A Ed Foudil por el tiempo dedicado a responder mis consultas.

REFERENCIAS

[1] "Digital Signature" [En línea]. *Disponible: https://www.rfc-editor.org/rfc/rfc9116#name-digital-signature*

[2] "Security.txt," *Security.txt Project*. [En línea]. Disponible: https://securitytxt.org/

[3] E. Foudil y Y. Shafranovich, "A File Format to Aid in Security Vulnerability Disclosure," IETF, RFC 9116, abr. 2022. [En línea]. Disponible: https://datatracker.ietf.org/doc/rfc9116/

[4] D. Crocker, "Mailbox Names for Common Services, Roles and Functions," IETF, RFC 2142, may. 1997. [En línea]. Disponible: https://www.ietf.org/rfc/rfc2142.txt

[5] Cybersecurity and Infrastructure Security Agency (CISA), "BOD 20-01: Develop and Publish a Vulnerability Disclosure Policy," 2020. [En línea]. Disponible: https://www.cisa.gov/news-events/directives/bod-20-01-develop-and-publish-vulnerability-disclosure-policy

[6] Cybersecurity and Infrastructure Security Agency (CISA), "Cybersecurity Performance Goals," 2023. [En línea]. Disponible: https://www.cisa.gov/cross-sector-cybersecurity-performance-goals

[7] National Cyber Security Centre (NCSC), "Vulnerability Disclosure Toolkit," 2020. [En línea]. Disponible: https://www.ncsc.gov.uk/information/vulnerability-disclosure-toolkit

[8] Data Standards Authority, "security.txt," *GOV.UK*. [En línea]. Disponible: https://alphagov.github.io/data-standards-authority/standards/securitytxt/

[9] National Cyber Security Centre (NCSC), "Vulnerability Reporting." [En línea]. Disponible: https://www.ncsc.gov.uk/information/vulnerability-reporting

[10] National Cyber Security Centre (NCSC) Suiza, "security.txt," *Confederación Suiza*. [En línea]. Disponible: https://www.ncsc.admin.ch/ncsc/en/home/infos-fuer/infos-unternehmen/aktuelle-themen/security-txt.html

[11] CERT.ar, "security.txt," Repositorio GitHub. [En línea]. Disponible: https://github.com/cert-ar/security.txt

[12] National Cyber Security Centre (NCSC), "Vulnerability Disclosure Toolkit," versión PDF, 2020. [En línea]. Disponible: https://www.ncsc.gov.uk/files/NCSC-Vulnerability-disclosure-Toolkit-v2.pdf

[13] E. Foudil, comunicación personal, abr. 2024.