UNIVERSIDAD NACIONAL
RAÚL SCALABRINI ORTIZ
SAN ISIDRO

Esp. Lic. López Lio, Rodrigo

SECURITY.TXT

El archivo de texto que puede salvar el mundo

Bio

- Ex Coordinador CERT.ar
- Cybersecurity Lead PrismaMP

- Docente Fundamentos de ciberseguridad y protección IICC – UNSO
- Docente Seguridad e integridad de la información – UADE

Articulo presentado en “InFo-Cyber - Cybersecurity and Digital Forensics Journal” - UFASTA

¿De qué vamos a hablar?

RFC 9116
A file format to aid in security vulnerability disclosure

Imagen adaptada de World´s Strongest Man, producción propia.

¿De qué vamos a hablar?

Internet Engineering Task Force (IETF)
Request for Comments: 9116
Category: Informational
ISSN: 2070-1721

E. Foudil

Y. Shafranovich
Nightwatch Cybersecurity

April 2022

A File Format to Aid in Security Vulnerability Disclosure

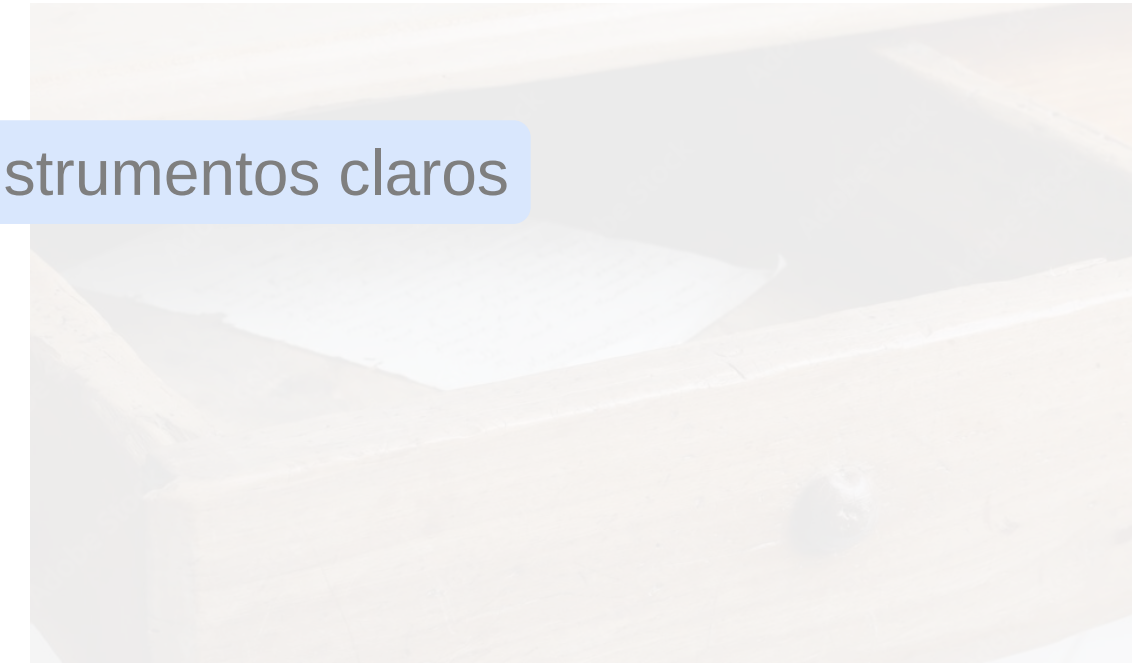
Abstract

When security vulnerabilities are discovered by researchers, proper reporting channels are often lacking. As a result, vulnerabilities may be left unreported. This document defines a machine-parsable format ("security.txt") to help organizations describe their vulnerability disclosure practices to make it easier for researchers to report vulnerabilities.

Problemas

- ¿Dónde comunicamos un hallazgo?
- ¿Ya fue reportado?
- ¿Tengo alguna vulnerabilidad?
- ¿Visibilidad?
- ¿Exposición?

Necesidad de contar con instrumentos claros



¿Cómo funciona?

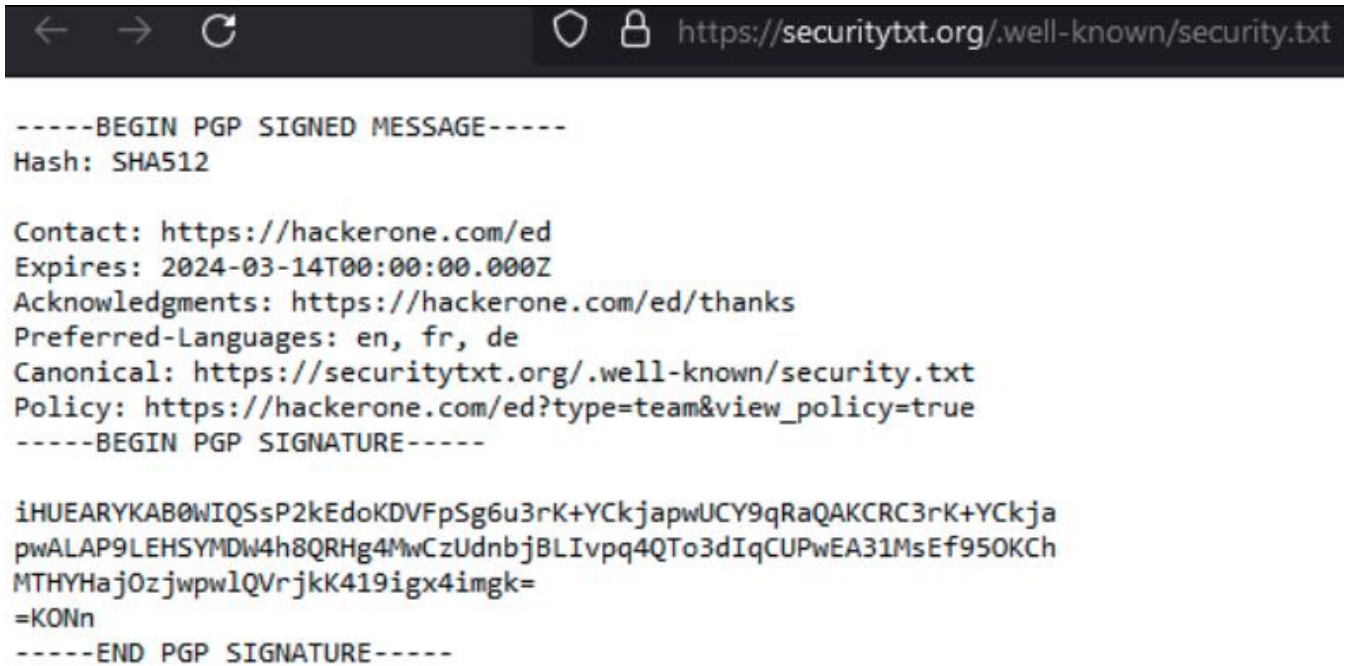
- Completar un archivo de texto con determinados campos
- Guardarlo en una ubicación predeterminada

/.well-known/

¿Cómo funciona?

/.well-known/security.txt

- Contact
- Expires
- Encryption
- Acknowledgments
- Preferred-Languages
- Canonical
- Policy
- Hiring
- CSAF



Implementando Security.txt

- Identificar servicios expuestos
- Generar archivo

Manual Generador

- Alojar
- **Gestionar**

- Contact
- Expires
- Encryption
- Acknowledgments
- Preferred-Languages
- Canonical
- Policy
- Hiring
- CSAF

Implementando Security.txt

Step 1

Create a text file called `security.txt` under the `.well-known` directory of your project.

Recent changes to the specification

The date format for Expires has changed to ISO 8601. An example of the new format is `Expires: 2021-12-31T18:37:07.000Z` .

Contact Required

A link or e-mail address for people to contact you about security issues. Remember to include "https://" for URLs, and "mailto:" for e-mails. See the full description of Contact

mailto:security@example.com

Add another alternative

Expires Required Only 1 allowed

The date and time when the content of the security.txt file should be considered stale (so security researchers should then not trust it). Make sure you update this value periodically and keep your file under review. See the full description of Expires

mm / dd / yyyy --:-- --

Add another alternative

Generate security.txt file

Step 2

You are ready to go! Publish your security.txt file. If you want to give security researchers confidence that your security.txt file is authentic, and not planted by an attacker, consider digitally signing the file with an OpenPGP cleartext signature.

Copy to clipboard

securitytxt.org

Conclusiones

- Establece un canal de comunicación claro
- Permite recibir reportes de manera oportuna
- Necesidad de repensar procedimientos de gestión de vulnes
- Recurso para ser incluido en cualquier política pública en materia de ciberseguridad

“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”

istockphoto.com / ncsc.gov.uk

Recursos

RFC 9116 A File Format to Aid in Security Vulnerability Disclosure. https://datatracker.ietf.org/doc/rfc9116/.

Security.txt https://securitytxt.org/.

Vulnerability Coordination SIG. https://www.first.org/global/sigs/vulnerability-coordination

Rodrigo López Lio

rlopezlio@unsanisidro.edu.ar

linkedin.com/in/r-l-l/

Muchas gracias!!

UNIVERSIDAD NACIONAL
RAÚL SCALABRINI ORTIZ
SAN ISIDRO

UNIVERSIDAD NACIONAL
RAÚL SCALABRINI ORTIZ
SAN ISIDRO