

Esp. Lic. López Lio, Rodrigo

SECURITY.TXT

El archivo de texto que puede salvar el mundo

TLP:CLEAR

Bio

- Ex Coordinador CERT.ar
- Cybersecurity Lead PrismaMP
- Docente Fundamentos de ciberseguridad y protección IICC – UNSO
- Docente Seguridad e integridad de la información – UADE

Artículo 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



¿De qué vamos a hablar?

Internet Engineering Task Force (IETF)

E. Foudil

Request for Comments: 9116

Category: Informational

Y. Shafranovich

ISSN: 2070-1721

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?



<https://securitytxt.org/.well-known/security.txt>

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA512

Contact: <https://hackerone.com/ed>

Expires: 2024-03-14T00:00:00.000Z

Acknowledgments: <https://hackerone.com/ed/thanks>

Preferred-Languages: • Completar un archivo de texto con
Canonical: <https://securitytxt.org/.well-known/security.txt>
determinados campos

Policy: https://hackerone.com/ed?type=team&view_policy=true

-----BEGIN PGP SIGNATURE-----

- Guardarlo en una ubicación predeterminada

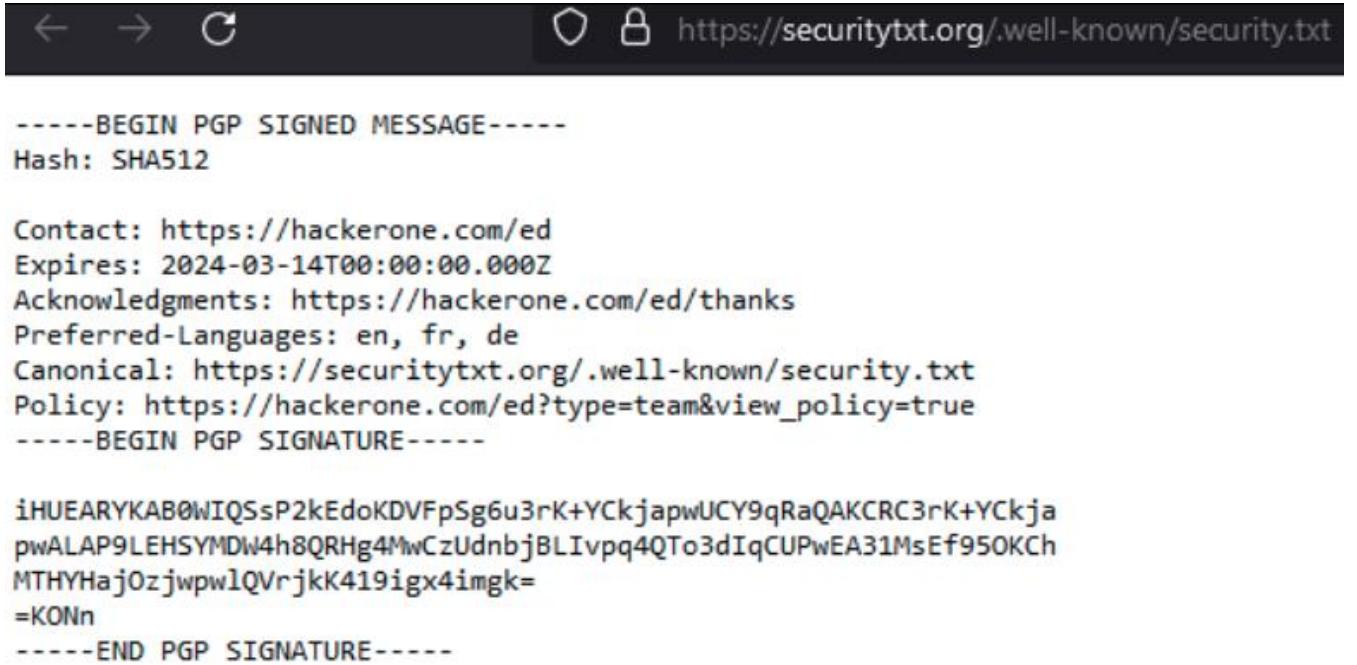
iHUEARYKAB0WIQSsP2kEdoKDVFpSg6u3rK+YCKjapwUCY9qRaQAKC62W6tj/
.well-known/
pwALAP9LEHSYMDW4h8QRHg4MwCzUdnbjBLIvpq4QTo3dIqCUPwEA31MsEf950KCh
MTHYHaj0zjwpwlQVrjkK419igx4imgk=
=KONn

-----END PGP SIGNATURE-----

¿Cómo funciona?

[./well-known/security.txt](#)

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



https://securitytxt.org/.well-known/security.txt

```
-----BEGIN PGP SIGNED MESSAGE-----  
Hash: SHA512  
  
Contact: https://hackerone.com/ed  
Expires: 2024-03-14T00:00:00.000Z  
Acknowledgments: https://hackerone.com/ed/thanks  
Preferred-Languages: en, fr, de  
Canonical: https://securitytxt.org/.well-known/security.txt  
Policy: https://hackerone.com/ed?type=team&view_policy=true  
-----BEGIN PGP SIGNATURE-----  
  
iHUEARYKAB0WIQSsP2kEdoKDVFpSg6u3rK+YCkjapwUCY9qRaQAKCRC3rK+YCkjapwALAP9LEHSYMDW4h8QRHg4MwCzUdnbjBLIvpq4QTo3dIqCUPwEA31MsEf950KChMTHYHaj0zjwpwlQVrjkK419igx4imgk=  
=KONn  
-----END PGP SIGNATURE-----
```

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

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

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](#)

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”

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