security.txt

Article URL
security.txt

Author
SecurityHome.eu

Published: 01 June 2023

Last updated on 04 June 2023.

Â

security.txt is a File Format that can be set on websites, so when security vulnerabilities are discovered by researchers, proper reporting channels can be used.

This file is a machine-parsable format to help organizations describe their vulnerability disclosure practices to make it easier for researchers to report vulnerabilities in a secure way.

The file is stored in domain.com/.well-known/security.txt

here is an example from google

:
Contact: https://g.co/vulnz
Contact: mailto:security@google.com
Encryption: https://services.google.com/corporate/publickey.txt
Acknowledgements: https://bughunters.google.com/
Policy: https://g.co/vrp
Hiring: https://g.co/SecurityPrivacyEngJobs
Expires: 2023-12-31T18:37:07z

2 fields are mandatory :
Contact

: this can be a email-address, a website url or a telephone number. Several contacts-field are allowed.
Expires

: the date and time after which the data contained in the *security.txt*

file is considered out of date and should no longer be used. It is recommended that this date is less than a

year.

The optional but strongly recommended field *Encryption*

,
contains the URL to a file that contains the public-key (of an OpenPGP key)

More info in the RFC:
https://www.rfc-editor.org/rfc/rfc9116