E-ISSN: 2985-8607, P-ISSN: 2985-8615
DOI: https://doi.org/10.38035/jgit.v1i2
Received: 27 Mei 2023, Revised: 08 Juni 2023, Publish: 15 Juni 2023

Prevalensi Penerapan RFC 9116 untuk Membantu Pengungkapan Kerentanan Keamanan Siber di Perguruan Tinggi Indonesia

Arif Rifai Dwiyanto[1]
[1]Universitas Bhayangkara Jakarta Raya, DKI Jakarta, Indonesia, arif.dwiyanto@ubharajaya.ac.id

Corresponding Author: arif.dwiyanto@ubharajaya.ac.id[1]

Abstract: *RFC 9116 or "security.txt" was created to overcome security researchers' obstacles in communicating cybersecurity issues to service owners. In this study, an evaluation was carried out on the prevalence of RFC 9116 implementation in Indonesian higher education institutions based on a database from the Research Organization Registry (ROR). The research began by designing the algorithm, implementing it, and then checking/scanning the existence of the security.txt file on the institution's main website to see whether it complies with RFC 9116. The results of the study show that the prevalence of implementing RFC 9116 in Indonesian Higher Education is only 0.2%. For this reason, it is necessary to socialize the implementation of RFC 9116 to improve the mechanism for disclosing cyber vulnerabilities in Indonesian higher education institution in responding to cyber security incidents.*

Keyword: *Vulnerability Disclosure, RFC 9116, Security.txt, Indonesian Higher Education. Incident Response*

Abstrak: RFC 9116 atau "security.txt" dibuat untuk mengatasi kendala peneliti keamanan dalam menyampaikan masalah keamanan siber kepada pemilik layanan. Dalam studi ini dilakukan evaluasi prevalensi penerapan RFC 9116, di perguruan tinggi Indonesia berdasarkan basis data dari Research Organization Registry (ROR). Penelitian dimulai dengan merancang algoritma, implementasi, dan kemudian dilakukan pengecekan/*scaning* keberadaan file security.txt di website utama institusi apakah telah sesuai dengan RFC 9116. Hasil studi menunjukkan prevalensi penerapan RFC 9116 di Perguruan Tinggi Indonesia hanya 0.2%. Untuk itu diperlukan sosialisasi penerapan RFC 9116 untuk meningkatkan mekanisme pengungkapan kerentanan siber di perguruan tinggi Indonesia dalam merespon insiden keamanan siber.

Kata Kunci: Pengungkapan Kerentanan, RFC 9116, Security.txt, Perguruan Tinggi Indonesia, Respon Insiden

PENDAHULUAN

Ketika peneliti keamanan menemukan celah keamanan siber pada sebuah layanan dan ingin melaporkannya ke pemilik layanan, peneliti tersebut bisa mengalami kesulitan untuk mengungkapkannya (Findlay, 2022). Hal ini dapat berakibat celah keamanan yang ditemukan tidak terlaporkan dan dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab.

Informasi mengenai kontak, mekanisme, dan kebijakan pelaporan kerentanan bisa saja tersedia, tetapi informasi ini tidak mudah ditemukan dan tidak terstandar. Dokumen RFC 9116 - *A File Format to Aid in Security Vulnerability Disclosure* adalah suatu standar/spesifikasi internet yang menjelaskan format file "security.txt" (Foudil, 2022). Format ini bertujuan untuk membantu organisasi dalam memberikan informasi terkait praktik pengungkapan kerentanan yang mereka terapkan. Hal ini memungkinkan peneliti keamanan untuk mengungkapkan kerentanan keamanan secara aman dan sesuai prosedur yang telah ditetapkan oleh pemilik layanan.

Beberapa organisasi besar seperti Google, Facebook, Linkedin, Github, dan Mozilla telah mengadopsi RFC 9116. Tidak hanya di perusahan, standar ini juga diterapkan di instansi pemerintahan, institusi akademik/riset, dan organisasi lainnya. Pemerintah Belanda mewajibkan seluruh situs web pemerintahan dilengkapi dengan security.txt (Forum Standaardisatie, 2023).

Rumusan masalah studi adalah pertanyaan sejauh mana prevalensi implementasi RFC 9116 di perguruan tinggi di Indonesia untuk membantu pengungkapan kerentanan keamanan siber. Studi yang dilakukan juga menghasilkan metode untuk menganalisis prevalensi penerapan standar ini.

KAJIAN PUSTAKA

Kerentanan dalam sebuah perangkat lunak atau layanan online sangat mungkin terjadi. Jika hal ini ditemukan maka diperlukan penanganan yang tepat dan cepat. Standar ISO/IEC 29147:2018 *Information technology - Security techniques - Vulnerability disclosure* menjelaskan bagaimana teknik dan kebijakan untuk menerima laporan kerentanan dan mempublikasikan informasi remediasi (ISO, 2018). Komunikasi antar pihak memegang peranan penting sehingga kemudahan untuk menemukan kontak pihak yang perlu dihubungi menjadi sangat vital dalam.

National Cyber Security Centre (NCSC) merupakan badan di Inggris yang bertanggung jawab untuk membantu melindungi organisasi dari ancaman siber telah mengeluarkan panduan *"Vulnerability Toolkit"* (NCSC, 2023). Panduan ini disediakan oleh NCSC untuk membantu organisasi mengidentifikasi, mengelola, dan mengatasi kerentanan keamanan di lingkungan digital masing-masing. Tiga komponen esensial dari panduan dari NCSC adalah:

1. Komunikasi
2. Kebijakan
3. Security.txt

Dari kedua hal tersebut dapat disimpulkan komunikasi dan kebijakan adalah kunci dari penanganan insiden keamanan siber. Salah satu sarana standar yang untuk menyampaikan pihak yang perlu dihubungi dengan menggunakan file “security.txt”.

“Security.txt” adalah salah satu elemen terpenting dalam pengungkapan kerentanan. Salah satu tantangan bagi penemu celah keamanan, adalah mengetahui siapa yang harus dihubungi untuk melaporkan temuan tersebut. Security.txt adalah standar Internet yang diusulkan dan menjelaskan siapa yang harus dihubungi, kebijakan, dan proses pengungkapan kerentanan sehingga peneliti keamanan dapat dengan cepat menemukan semua informasi yang diperlukan untuk melaporkan kerentanan.

Draf pertama “security.txt” diusulkan oleh by Edwin Foudil dan Yakov Shafranovich pada bulan September 2017 yang kemudian dijadikan standar RFC 9116 pada bulan April 2022. Standar ini terinspirasi oleh format yang sudah ada sebelumnya seperti “ads.txt”,

“humans.txt”, dan “robot.txt”. Pada saat awal pengusulan informasi yang wajib untuk dicantumkan adalah "Contact", "Encryption", "Disclosure" dan "Acknowledgement" (Foudil, 2022).

File “security.txt” berisi dua hal utama yaitu pertama kontak yaitu ke mana pelapor harus melaporkan kerentanan, misalnya melalui email atau formulir web. Kedua adalah kebijakan, informasi kebijakan bisa berupa tautan ke kebijakan organisasi dalam pengungkapan kerentanan. Informasi lain misal enkripsi bersifat opsional, jika dinyatakan maka harus disediakan tautan ke kunci publik PGP yang ingin digunakan untuk komunikasi terenkripsi. File security.txt harus dipublikasikan ke semua domain dan subdomain.

Beberapa manfaat penerapan RFC 9116 menurut Foudil adalah:

1. Transparansi dan akuntabilitas
   RFC 9116 membantu organisasi dalam menunjukkan komitmen mereka terhadap keamanan kepada para peneliti keamanan, yang pada gilirannya dapat membangun hubungan yang lebih baik.
2. Kemudahan pelaporan bagi pelapor
   RFC 9116 memberikan petunjuk yang jelas tentang bagaimana melaporkan kerentanan, sehingga peneliti keamanan dapat melakukannya dengan cepat dan mudah. Hal lain adalah dengan menggunakan format standar pelaporan dapat dilakukan melalui perangkat lunak, sama halnya dengan fungsi Robot.txt.
3. Manajemen dan respon insiden yang efektif
   RFC 9116 membantu organisasi dalam melacak dan mengelola kerentanan dengan lebih efisien, yang pada akhirnya meningkatkan tingkat keamanan secara keseluruhan.

Untuk menerapkan standar ini penyedia layanan cukup menyediakan file teks dengan nama “security.txt” pada folder yang sudah disepakati. File tersebut harus mengikuti cara penulisan yang ditetapkan dan harus dilayani melalui HTTPS. File teks tersebut dapat disimpan pada webroot contohnya https://www.example.com/security.txt atau di bawah direktori. *well-known* contohnya https://www.example.com/.well-known/security.txt sesuai RFC 8615.

Berikut ini beberapa contoh penerapan RFC 9116 di beberapa layanan daring.

1. Penerapan di Google.com

Google adalah salah satu perusahaan yang telah menerapkan RFC 9116. File security.txt google dapat diakses pada alamat https://www.google.com/.well-known/security.txt

```
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
```

Gambar 1. Penerapan RFC 9116 di Google

2. Penerapan di Facebook

Facebook adalah salah satu perusahaan yang menerapkan RFC 9116. File security.txt Facebook dapat diakses pada alamat https://www.facebook.com/security.txt]. File security.txt diletakan pada webroot situs mereka.

```
Contact: https://www.facebook.com/whitehat/report/
Acknowledgments: https://www.facebook.com/whitehat/thanks/
Hiring: https://www.facebook.com/careers/teams/security/

# Found a bug? Our bug bounty policy:
Policy: https://www.facebook.com/whitehat/info/

# What we do when we find a bug in another product:
Policy: https://www.facebook.com/security/advisories/Vulnerability-
Disclosure-Policy

Expires: Tue, 10 Oct 2023 00:23:24 -0700
```

Gambar 2. Penerapan RFC 9116 di Facebook

3. Implementasi di lokapasar/*marketplace* Indonesia

Tokopedia adalah salah satu lokapasar/*marketplace* di Indonesia yang mengalami serangan siber berupa kebocoran data pada tahun 2020 (Eloksari, 2020). File security.txt Tokopedia dapat diakses pada alamat https://www.tokopedia.com/security.txt

```
Contact: https://bounty.tokopedia.net/
Preferred-Languages: en, id
Canonical: https://www.tokopedia.com/.well-known/security.txt
Policy: https://bounty.tokopedia.net/rules
Acknowledgments: https://bounty.tokopedia.net/wall-of-fame
Hiring: https://www.tokopedia.com/careers/
Expires: 2022-01-01T00:00:00.000Z
```

Gambar 3. Penerapan RFC 9116 di Lokapasar Tokopedia

Tobias Hilbig et al telah melakukan penelitian prevalensi dan kesesuaian standar ini secara global pada tahun 2022. Namun belum ditemukan analisis penerapan standar ini untuk lingkup Indonesia lebih spesifik pada institusi perguruan tinggi.

Tabel 1. Perbandingan Tingkat Penerapan File Security.txt, Menurut Grup Peringkat Tranco Tahun 2022. (Hilbig, et al 2023)

Group	First	Last	Change (rel)	Change (abs)
100	32.0%	34.0%	6.3%	2
1k	16.1%	18.8%	16.8%	27
10k	7.9%	9.8%	22.9%	182
100k	2.4%	3.2%	31.3%	763
1M	0.7%	1.0%	28.6%	2,803

Sumber: https://doi.org/10.1145/3609234

Hasil penelitian Hilbig et al menunjukan prevalensi implementasi yang paling rendah adalah untuk kelompok satu juta web teratas, namun pertambahan implementasi untuk kelompok ini paling tinggi. Dari penelitian ini maka diambil hipotesis prevalensi implementasi di Indonesia tidak akan melebihi 0.7%.

METODE

Jenis penelitian berupa penelitian kuantitatif melalui eksplorasi empiris. Populasi penelitian adalah seluruh institusi pendidikan tinggi yang terdaftar pada basis data *Research*

Organization Registry atau ROR. Dari seluruh institusi yang dalam database ROR organisasi akan dipilih institusi perguruan tinggi yang menggunakan tautan domain *.ac.id.

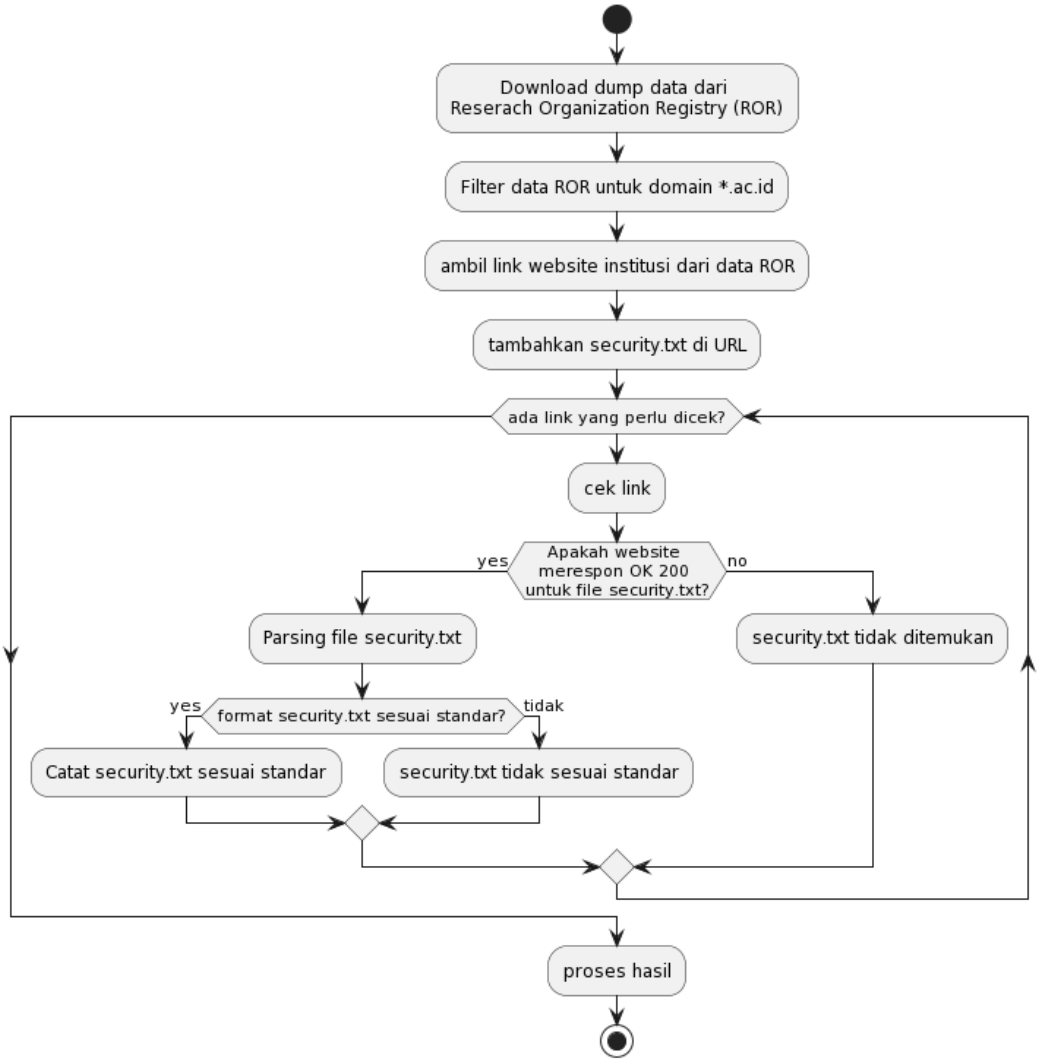
Tahap awal penelitian adalah menyusun metode/algoritma *scanning* dan *web scraping,* untuk mengambil informasi dari setiap website perguruan tinggi yang akan dianalisis. Setelah disusun algoritma kemudian akan diimplementasikan dalam salah satu bahasa pemrograman.

Tahap berikutnya adalah mengumpulkan data menggunakan skrip/aplikasi yang telah disusun sebelumnya. Waktu pengumpulan data dilakukan pada bulan November 2023.

Tahap akhir adalah analisis prevalensi dengan melihat apakah perguruan tinggi yang dianalisis menyediakan berkas security.txt dan jika menyediakan apakah penerapannya telah sesuai standar/spesifikasi RFC 9116.

HASIL DAN PEMBAHASAN

Sebelum dilakukan pengumpulan data dirancang algoritma untuk melakukan scanning dan mengolah data seperti Gambar 4.



Gambar 4. Algoritma *Scanning* Prevalensi RFC 9116

Algoritma di atas kemudian diimplementasikan dalam bahasa pemrograman Python yang dijalankan melalui aplikasi Jupyter Notebook.

Dari hasil pemrosesan data ROR ditemukan 106.346 institusi dengan struktur data seperti pada Gambar 5.

```
'id', 'name', 'types', 'status', 'links', 'aliases', 'labels',
'acronyms', 'wikipedia_url', 'established', 'addresses[0].lat',
'addresses[0].lng', 'addresses[0].geonames_city.name',
'addresses[0].geonames_city.id',
'addresses[0].geonames_city.geonames_admin1.name',
'addresses[0].geonames_city.geonames_admin1.code',
'addresses[0].geonames_city.geonames_admin2.name',
'addresses[0].geonames_city.geonames_admin2.code',
'country.country_code', 'country.country_name',
'external_ids.GRID.preferred', 'external_ids.GRID.all',
'external_ids.ISNI.preferred', 'external_ids.ISNI.all',
'external_ids.FundRef.preferred', 'external_ids.FundRef.all',
'external_ids.Wikidata.preferred', 'external_ids.Wikidata.all',
'relationships'
```

Sumber: https://doi.org/10.5281/zenodo.8436953

Gambar 5. Struktur Basis Data ROR

Field data yang diperlukan dalam penelitian ini adalah **name** dan **links**, sehingga dipilih kolom yang sesuai seperti yang terlihat pada Tabel 2.

Tabel 2. Potongan Sebagian Data dari Basis Data ROR

ROR id	name	types	links
https://ror.org/02bfwt286	Monash University	Education	http://www.monash.edu/
https://ror.org/01sf06y89	Macquarie University	Education	http://mq.edu.au/
https://ror.org/00jtmb277	University of Wollongong	Education	https://www.uow.edu.au/
https://ror.org/01nfmeh72	University of Tasmania	Education	http://www.utas.edu.au/
https://ror.org/01kpzv902	Flinders University	Education	http://www.flinders.edu.au/
https://ror.org/04ttjf776	RMIT University	Education	https://www.rmit.edu.au/
https://ror.org/01rxfrp27	La Trobe University	Education	http://www.latrobe.edu.au/
https://ror.org/04j757h98	Victoria University	Education	http://www.vu.edu.au/
https://ror.org/04r659a56	University of New England	Education	http://www.une.edu.au/
https://ror.org/02czsnj07	Deakin University	Education	http://www.deakin.edu.au/
https://ror.org/02sc3r913	Griffith University	Education	http://www.griffith.edu.au/
https://ror.org/023q4bk22	Central Queensland University	Education	https://www.cqu.edu.au/
https://ror.org/01p93h210	University of South Australia	Education	https://www.unisa.edu.au/
https://ror.org/031rekg67	Swinburne University of Technology	Education	http://www.swinburne.edu.au/
https://ror.org/006jxzx88	Bond University	Education	http://bond.edu.au/
https://ror.org/00wfvh315	Charles Sturt University	Education	http://www.csu.edu.au/
https://ror.org/04s1nv328	University of Canberra	Education	http://www.canberra.edu.au/
https://ror.org/05qbzwv83	Federation University	Education	https://federation.edu.au/
https://ror.org/048zcaj52	Charles Darwin University	Education	http://www.cdu.edu.au/
https://ror.org/05ktbsm52	Burnet Institute	Nonprofit	http://www.burnet.edu.au/
https://ror.org/00nx6aa03	Mater Research	Facility	http://research.mater.org.au/
https://ror.org/046fa4y88	The Heart Research Institute	Facility	http://www.hri.org.au/
https://ror.org/033yfkj90	Naval Postgraduate School	Education	http://www.nps.edu/
https://ror.org/04h08p482	Rolls-Royce (United Kingdom)	Company	https://www.rolls-royce.com/
https://ror.org/01zctcs90	BP (United Kingdom)	Company	http://www.bp.com/
https://ror.org/05m7zw681	Rio Tinto (United Kingdom)	Company	http://www.riotinto.com/
https://ror.org/017wrhq72	Department of Water	Govt	https://www.water.wa.gov.au/
https://ror.org/04p8ejq70	BAE Systems (United Kingdom)	Company	http://www.baesystems.com/
https://ror.org/03awtex73	Arup Group (United States)	Company	http://www.arup.com/
https://ror.org/00kv9pj15	BT Group (United Kingdom)	Company	http://www.btplc.com/

Sumber: https://doi.org/10.5281/zenodo.8436953

Dari data yang sudah dipilah kemudian disaring lagi khusus untuk institusi yang menggunakan tautan domain *.ac.id sehingga didapatkan 539 seperti contoh pada Tabel 3.

Tabel 3. Potongan Sebagian Data Dengan Tautan *.ac.id

ROR id	name	links
https://ror.org/01jf74q70	State University of Surabaya	http://www.unesa.ac.id/
https://ror.org/04ctejd88	Airlangga University	http://www.unair.ac.id/
https://ror.org/00k5x6r15	Universitas Ma Chung	https://www.machung.ac.id/
https://ror.org/04yf4aj88	University of Nusa Cendana	https://undana.ac.id/
https://ror.org/00bgzqr58	Universitas Sains dan Teknologi Jayapura	http://ustj-papua.ac.id/
https://ror.org/00yrjw682	Universitas Darussalam Ambon	http://www.unidar.ac.id/
https://ror.org/03rwzd843	Universitas Kristen Indonesia Maluku	http://ukim.ac.id/
https://ror.org/03yca6a35	Universitas Ratu Samban	https://unras.ac.id/
https://ror.org/05dj31k33	Universitas Balikpapan	https://uniba-bpn.ac.id
https://ror.org/002rphp73	Universitas Tri Dharma	https://www.untri.ac.id/
https://ror.org/005z3e143	Universitas Abulyatama	http://abulyatama.ac.id/
https://ror.org/004drcv69	Universitas Iskandar Muda	https://unidaaceh.ac.id/
https://ror.org/0240hnb85	Universitas Serambi Mekkah	http://serambimekkah.ac.id/
https://ror.org/03ga61755	Universitas Bandar Lampung	https://ubl.ac.id/
https://ror.org/00567j574	Universitas Malahayati	http://malahayati.ac.id/
https://ror.org/03zf73d71	Universitas Muhammadiyah Lampung	http://uml.ac.id/
https://ror.org/053gxvt69	Universitas Saburai	http://www.saburai.ac.id/
https://ror.org/02c733g32	Universitas Tulang Bawang Lampung	https://utb.ac.id
https://ror.org/01b15w051	Telkom Institute of Management	http://www.imtelkom.ac.id/
https://ror.org/01khe0643	Harapan Bangsa Institute of Technology	https://ithb.ac.id/

Sumber: https://doi.org/10.5281/zenodo.8436953

Kemudian dilakukan scanning terhadap 539 link perguruan tinggi tersebut. Setelah dilakukan scanning didapati satu perguruan tinggi yang telah menerapkan RFC 9161. Adapun file security.txt yang disediakan dapat dilihat pada Gambar 6.

```
# Our security contact
Contact: mailto:csirt@ubharajaya.ac.id
Contact: tel:+62-8967-1111-497
Contact: https://csirt.ubharajaya.ac.id/lapor

# Our OpenPGP key
Encryption: https://csirt.ubharajaya.ac.id/ubharajayapublic.key

# Our security acknowledgments page
Acknowledgments: https://csirt.ubharajaya.ac.id/whitehat/thanks/

# Our security policy
Policy: https://csirt.ubharajaya.ac.id/vulnerability-reporting-policy/

Preferred-Languages: en, id
Expires: 2025-01-01T00:00:00.000Z
```

Gambar 6. File security.txt Universitas Bhayangkara Jakarta Raya

Dengan demikian prevalensi penerapan RFC 9116 di Perguruan Tinggi Indonesia yang terdaftar pada basis data ROR per November 2023 baru sebesar 0,2%. Prevalensi ini di bawah 0.7% sesuai dengan hipotesis penelitian.

KESIMPULAN

Dari studi yang dilakukan didapati bahwa prevalensi implementasi RFC9116 masih sangat rendah, di bawah 0,2% dari institusi yang terdaftar pada database Research Organization Registry (ROR). Temuan ini sesuai dengan hipotesis dari penelitian yang memperkirakan prevalensi di bawah 0.7%.

Selain menjawab pertanyaan penelitian, studi ini juga menghasilkan metode/algoritma dan skrip program yang dapat digunakan untuk menganalisis prevalensi penerapan RFC 9116.

Tindak lanjut dari penelitian ini adalah perlu dilakukan sosialisasi penerapan spesifikasi ini sehingga memudahkan peneliti keamanan menyampaikan kerentanan keamanan siber. Dengan sosialisasi dan kemudahan penerapan RFC 9116 diharapkan dapat meningkatkan proses pengungkapan keamanan siber di institusi perguruan tinggi.

Dengan menggunakan file "security.txt," organisasi dapat menunjukkan komitmen mereka terhadap keamanan dan mendorong peneliti keamanan untuk berkontribusi dalam meningkatkan keamanan sistem dan layanan mereka serta meningkatkan respon insiden keamanan siber.

REFERENSI

International Organization for Standardization. (2018). The International Standard for Vulnerability Disclosure (ISO/IEC Standard No. 29147:2018).

Nottingham, M. (2019, May). Well-Known Uniform Resource Identifiers (URIs). doi:10.17487/RFC8615

Lokasari, E. A. (2020, May 22). Tokopedia data breach exposes vulnerability of personal data. The Jakarta Post. https://www.thejakartapost.com/news/2020/05/04/tokopedia- data-breach-exposes-vulnerability-of-personal-data.html

Poteat, T., & Li, F. (2021). Who You Gonna Call? An Empirical Evaluation of Website Security.Txt Deployment. Proceedings of the 21st ACM Internet Measurement Conference, 526–532. Presented at the Virtual Event. doi:10.1145/3487552.3487841

Findlay, William & Abdou, Abdelrahman. (2022). Characterizing the Adoption of Security.txt Files and their Applications to Vulnerability Notification. 10.14722/madweb.2022.23014.

Foudil, E., & Shafranovich, Y. (2022, April). A File Format to Aid in Security Vulnerability Disclosure. doi:10.17487/RFC9116

National Cyber Security Centre. (2022, November). Vulnerability Disclosure Toolkit v.2 (2nd ed.). National Cyber Security Centre UK. https://www.ncsc.gov.uk/files/NCSC-Vulnerability-disclosure-Toolkit-v2.pdf

Forum Standaardisatie (2023, May 31). Security.Txt Mandatory for Dutch Government. Retrieved October 22, 2023, from https://forumstandaardisatie.nl/nieuws/securitytxt-mandatory-dutch-government

Research Organization Registry. (2023). ROR Data (v1.34) [Data set]. Zenodo. https://doi.org/10.5281/zenodo.8436953

Hilbig, T., Geras, T., Kupris, E., & Schreck, T. (2023, October). Security.Txt Revisited: Analysis of Prevalence and Conformity in 2022. *ACM Digital Threats: Research and Practice, 4*(3). doi:10.1145/3609234