4852-12818-1-SM

by Nurina Septiani

Submission date: 31-Jul-2022 03:57PM (UTC+0700)
Submission ID: 1877115088
File name: 4852-12818-1-SM.docx (475.1K)
Word count: 2231
Character count: 14629

JIKO (Jurnal Informatika dan Komputer)
Vol. x, No. x, April 2019, hlm. x-x
DOI: 10.33387/jiko

Akreditasi KEMENRISTEKDIKTI, No.36/E/KPT/2019
p-ISSN: 2614-8897
e-ISSN: 2656-1948

PERANCANGAN WEB DEFACEMENT MONITORING DENGAN MENGGUNAKAN METODE KOMPARASI NILAI HASH1

Nurina I Septiani[1], Agung Sediyono[2], Abdul Rochman[3]

[1,2,3]Program Studi Teknik Informatika Fakultas Teknologi Industri Universitas Trisakti
Email: [1]nurina064001800511@std.trisakti.ac.id, [2]agung.sediyono@trisakti.ac.id, [3]abdul.rochman@trisakti.ac.id

Abstrak

Laman *website* merupakan sarana penyampaian informasi penting bagi sebuah perusahaan. Untuk itu perlu dijaga keutuhannya dari segala usaha perubahan informasi. Salah satu yang sering terjadi adalah *Web Defacement*. Saat ini pemantauan masih dilakukan secara manual dan pendeteksian perubahan tampilan dari halaman *website* tidak diketahui secara cepat. Supaya kerusakan informasi dapat diperbaiki dalam waktu singkat diperlukan *Web Defacement Monitoring (WDM)*. Penelitian ini mengusulkan pembuatan aplikasi WDM dengan menggunakan metoda Komparasi Nilai Hash SHA1. Aplikasi ini dapat mendeteksi adanya perubahan tampilan visual pada konten *text* dalam halaman *website*. Sebagai tindakan perlindungan atas serangan keamanan informasi dari *web defacement*, perlu dilakukan pemantauan tampilan dari halaman *website* pada sistem aplikasi. Hasil percobaan menunjukan aplikasi ini mampu mendeteksi sekecil apapun perubahan *text* yang ada pada laman *website*.

Kata kunci: *Web Defacement, Keamanan Informasi, Hash SHA1*

DESIGN OF WEB DEFACEMENT MONITORING USING THE SHA1 HASH VALUE COMPARISON METHOD

Abstract

Webpages are important pages that is used by a company to publish its information. Therefore, it is important to keep the information integrity in every page. Till now, hacker tries to hack information integrity on website namely web defacement. To cop this issue, we need to design Web Defacement Monitoring (WDM). This research proposes WDM using the SHA1 Hash Value Comparison method. This website application that can detect changes in the visual appearance of text content on web pages. As a protection measure for information security attacks from web defacement, it is necessary to monitor the appearance of web pages on the application system. Experiment result show that this application performs to detect any changing text in webpage even only one character.

Keywords: *Web Defacement, Information Security, Hash SHA1*

1. PENDAHULUAN

Pada keamanan sistem informasi, *threat* (ancaman keamanan informasi) merupakan keadaan dimana kerentanan yang dimiliki oleh suatu sistem memungkinkan dieksploitasi atau dimanfaatkan oleh pihak yang tidak bertanggung jawab untuk melakukan serangan keamanan informasi. Ancaman yang mengeksploitasi kerentanan tersebut dapat menyebabkan hilangnya kerahasiaan, keutuhan, dan ketersediaan dari aset bisnis. Ancaman selalu ada sehingga tidak bisa dihilangkan namun bisa dikendalikan.

Menurut UU ITE No 11 tahun 2008, "Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agar Informasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik". Dalam UU ITE tersebut dikatakan melakukan manipulasi, manipulasi disini adalah merubah halaman *website* atau sejenisnya menjadi tidak sesuai akan mendapatkan sanksi hukum. Aksi peretasan yang biasa terjadi pada *website* adalah *web defacement*. *Web Defacement* merupakan serangan pada satu halaman *web* atau situs *web* dengan melakukan perubahan tampilan visual pada konten yang tidak sah. Serangan ini dilakukan secara sebagian atau diganti sepenuhnya dengan merubah konten halaman *web*, mengganti halaman *web* sepenuhnya ataupun menghapus halaman *web*.

Organisasi XYZ yang mengelola keamanan aset informasi Data Center (DC) Kementerian ABC harus melindungi kerahasiaan, keutuhan, dan ketersediaan aset informasi. Sebagai tindakan perlindungan atas

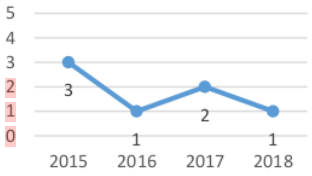
serangan keamanan informasi pada sistem aplikasi dari *web defacement*, Organisasi XYZ secara berkala melakukan pemantauan tampilan dari halaman *website* pada sistem aplikasi. Saat ini, pemantauan tampilan dari suatu *website* pada sistem aplikasi masih dilakukan secara manual dan pendeteksian perubahan tampilan dari halaman *website* tidak diketahui secara cepat. Hal tersebut dapat menyebabkan terekspos nya kejadian tersebut oleh media nasional sehingga berdampak pada menurunnya reputasi Kementerian ABC. Berdasarkan data 3 tahun terakhir, kejadian *web defacement* yang mengeksploitasi *web* Kementerian ABC dan terekspos oleh media nasional mengalami peningkatan.

Dalam mengatasi permasalahan tersebut, penulis mengajukan aplikasi *Web Defacement Monitoring* yang dapat mendeteksi perubahan tampilan halaman *web* dan mengirimkan notifikasi hasil pendeteksiannya. Pengiriman notifikasi berguna untuk mempercepat penanganan kejadian *web defacement*.

2. STUDI PUSTAKA

Berdasarkan laporan status keamanan siber di Asia Tenggara tahun 2019 yang dirilis oleh SPI, negara-negara di Asia Tenggara masih memiliki kerentanan yang tinggi terhadap kejahatan dan penerobosan keamanan siber. Di Indonesia, serangan siber telah menerobos sekitar 80% domain publik dan menjadikan Indonesia sebagai negara dengan risiko tertinggi dalam keamanan teknologi informasi. Serangan siber yang disoroti dalam laporan ini adalah *web dafacement* yang terus meningkat terhadap domain .id. Setidaknya 12 web insititusi pemerintah pernah terkena *defacement*. Jumlah serangan *web defacement* di Indonesia diungkapkan oleh salah satu organisasi pengawasan keamanan informasi di Indonesia, id-SIRTII/CC, dalam APCERT Annual Report 2018, yaitu sebanyak 16.939 insiden. Dari keseluruhan insiden tersebut, 37% terjadi pada domain .id dan 63% terjadi pada domain internasional.

Di Kementerian ABC, pengelolaan *Data Center* dan sistem yang di-*hosting* di dalamnya dilakukan oleh Organisasi XYZ. Salah satu tugas Organisasi XYZ adalah mendeteksi dan menindaklanjuti upaya penerobosan keamanan sistem informasi terhadap sistem yang dipantau di *Data Center*. Jumlah sistem TIK dengan kategori *hosting* yang dipantau sebanyak 205 sistem dengan 43 di antaranya merupalan sistem TIK dengan tingkat kritikalitas tinggi atau sangat tinggi berdasarkan penilaian *Business Impact Analysis* (BIA), diakses oleh publik/masyarakat, dan mempresentasikan citra Kementerian ABC. Organisasi XYZ memiliki *tool* untuk memantau, mendeteksi, dan menangkal serangan siber ke seluruh sistem TIK tersebut. Meskipun demikian, *tool* tersebut belum memiliki kemampuan untuk menginformasikan serangan siber yang berhasil masuk, termasuk *web defacement*. Pengendalian internal yang dilakukan masih sebatas pengecekan terhadap perubahan ilegal pada halaman web secara manual halaman web setiap pagi dan sore hari. Proses ini memerlukan waktu yang tidak sebentar. Hal ini menyebabkan insiden *web defacement* terlebih dahulu terekspos oleh media lokal sebelum sempat ditangani oleh Organisasi XYZ. Insiden *web defacement* yang terekspos oleh media lokal sebelum sempat ditangani selama 4 tahun terakhir dapat dilihat sebagaimana gambar 1.



Gambar 1. Tren Web Defacement yang terekspos media lokal selama 4 tahun terakhir

Sementara itu, sejak tahun 2019, insiden *web defacement* menjadi perhatian pimpinan Kementerian ABC dengan menjadikan kemungkinan terjadinya *web defacement* sebagai salah satu risiko yang memiliki level signifikan terhadap reputasi Kementerian ABC. Menteri ABC bahkan menyatakan bahwa tingkat selera risiko keamanan informasi adalah *zero tolerance* atau tidak ada toleransi terhadap kejadian tersebut. Dengan demikian, insiden *web dafecement* sebagaimana grafik 1 tidak dapat ditolerir meskipun jumlahnya sedikit. *Tool* yang dimiliki oleh Organisasi XYZ belum memenuhi harapan Menteri ABC. Pendeteksian yang lambat menyebabkan penanganan insiden yang lambat pula. Organisasi XYZ membutuhkan *tool* yang mampu mendeteksi *web defacement* dengan cepat dan menyampaikan anomali hasil pendeteksiannya ke *email* petugas keamanan informasi agar dapat ditangani sebelum insiden tersebut terekspos oleh media lokal.

Terdapat beberapa teknik dalam mendeteksi dan memonitor *website defacement* yang dikelompokkan ke dalam teknik *anomaly-based detection*. Cara kerja teknik *anomaly-based detection* adalah dengan menggunakan "profil" halaman web dalam kondisi normal untuk selanjutnya dimonitor dan dibandingkan dengan profil halaman web yang berjalan. Dengan menggunakan teknik ini, perubahan terbaru pada halaman web dapat terdeteksi namun sulit untuk mendeteksi perubahan yang signifikan antara halaman yang dimonitor dengan profil yang ditentukan mengingat konten dari halaman web selalu berubah-ubah.

Pada pendeteksian perubahan tampilan halaman web, penelitian ini menggunakan metode algoritma SHA1 hashing. Dalam prosesnya, data daftar URL master dari database terlebih dahulu diambil

kemudian langkah selanjutnya yang dilakukan yaitu melakukan perulangan pengecekan hasil crawlimg url untuk mengambil data halaman *website* terkini. Setelah proses tersebut berhasil, hasil crawling url yang berupa text dihapus semua karakter whitespace menyambung menjadi 1 teks panjang tanpa jeda (string). Kemudian string tersebut dipotong tanpa jeda sesuai dengan panjang n yang diinginkan dan disimpan dalam bentuk list (chunk). Setiap chunk potongan string dienkripsi menggunakan SHA1. Selanjutnya hash awal dengan hash terkini dibandingkan untuk mendapatkan hasil komparasi.

Dalam penelitian ini, metode yang digunakan untuk mendeteksi *web defacement* adalah metode Algoritma SHA1 *Hashing* untuk melakukan pendeteksian perubahan tampilan dari suatu website. Dalam rangka memenuhi hal tersebut, diperlukan pembangunan aplikasi yang dapat mengirimkan anomali hasil pendeteksian *web defacement* ke pengguna aplikasi. Fitur ini diperlukan oleh petugas keamanan informasi di Organisasi XYZ dalam mendeteksi adanya insiden *web defacement* agar dapat ditangani sesegera mungkin. Dengan demikian, *output* dalam penelitian ini adalah aplikasi *Web Defacement Monitoring* berdasarkan metode algoritma SHA1 *hashing* beserta hasil pengujian terhadap keakurasian perubahan data pada beberapa halaman web di sistem TIK yang memiliki tingkat kritikalitas tinggi atau sangat tinggi di Kementerian ABC.

3. METODOLOGI PENELITIAN

Metodologi penelitian yang digunakan adalah Metode *Prototyping*, dengan tahapan sebagai berikut:

1. *Requirements Analysis*
   Pada tahap ini, dilakukan beberapa hal yaitu:
   a. Penggalian informasi kebutuhan user, yang dapat dituangkan dalam Aplikasi *Web Defacement Monitoring*
   b. Pengumpulan data dukung yang dibutuhkan dalam membangun Aplikasi *Web Defacement Monitoring*
   c. Melakukan pemetaaan antara kebutuhan dan data dukung yang telah didapatkan, kemudian melakukan analisis dari data tersebut.
2. *Design and Planning*
   Pada tahap ini, dilakukan beberapa hal yaitu:
   a. Membuat *design* atau rancang aplikasi. Perancangan aplikasi yang digambarkan dalam bentuk *Use Case Diagram, Class Diagram dan Activity Diagram*.
   b. Identifikasi komponen / ruang lingkup dalam aplikasi *Web Defacement Monitoring*.
   c. Melakukan perancangan *user interface*.
3. *Code*
   Dalam tahap ini mulai dilakukan pembangunan Aplikasi *Web Defacement Monitoring*, dengan melakukan pengkodean atau menuangkan rancangan aplikasi yang telah dibuat sebelumnya ke dalam bentuk aplikasi dengan menggunakan bahasa pemrograman *python*.
4. *Tests*
   Dalam tahap ini, dilakukan *testing performance* Aplikasi *Web Defacement Monitoring* yang telah selesai dibangun.
5. *Release*
   Dalam tahap ini, dilakukan *release* Aplikasi *Web Defacement Monitoring* dengan cara melakukan *hosting* aplikasi tersebut ke *server local* atau *development*. Pada tahap ini, harus dipastikan bahwa integrasi antara fitur yang sudah dan akan dilakukan *release* untuk dapat berjalan dengan baik ketika proses *release* selesai dilakukan.

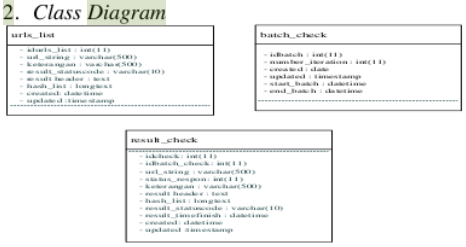
4. HASIL DAN PEMBAHASAN

1. *Use Case Diagram*

Pada perancangan aplikasi *Use Case Diagram* terdapat 2 aktor dan 5 use case. Perancangan *Use Case Diagram* dapat dilihat pada Gambar 2.

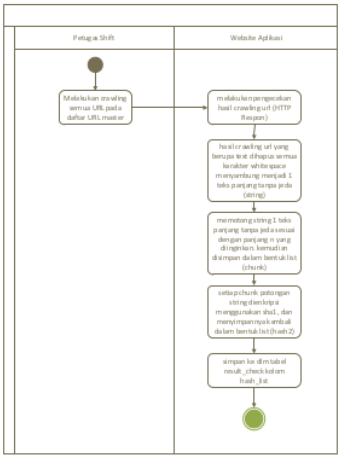
Gambar 2. *Use Case Diagram Aplikasi Web Defacement Monitoring*

2. *Class Diagram*

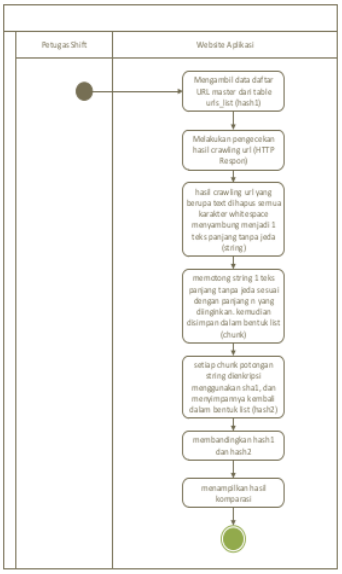


Gambar 3. *Class Diagram Aplikasi Web Defacement Monitoring*

3. *Activity Diagram*



Gambar 4. *Activity Diagram* saat *Crawl Master*



Gambar 5. *Activity Diagram* saat melakukan cek deface

Gambar 6. *Activity Diagram* saat mengirim telegram

4. Penjelasan mengenai *Web Defacement Monitoring* Dengan Menggunakan Metode Komparasi Nilai Hash SHA1

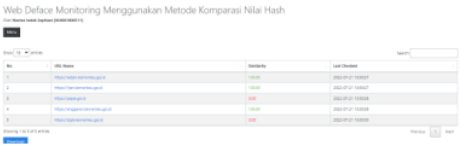
4.1. Halaman Utama

Pada halaman utama, user akan diberikan 2 pilihan menu, yang pertama yaitu adalah *Dashboard* dan yang kedua adalah Program.

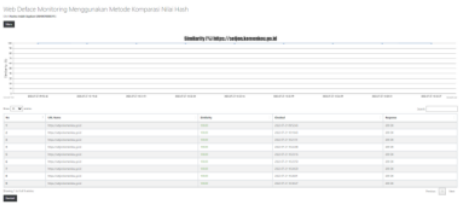
Gambar 7. Halaman Utama

4.2 Dashboard dan Grafik

Tampilan berikut merupakan tampilan pada halaman *dashboard* yang menampilkan nilai dari komparasi hash. Nilai 0 yang berarti hasil pengecekan halaman *website* tidak sama dengan aslinya, dan nilai 100 yang berarti sama dengan aslinya.



Gambar 8. Halaman Dashboard



Gambar 9. Halaman Detail *Dashboard*

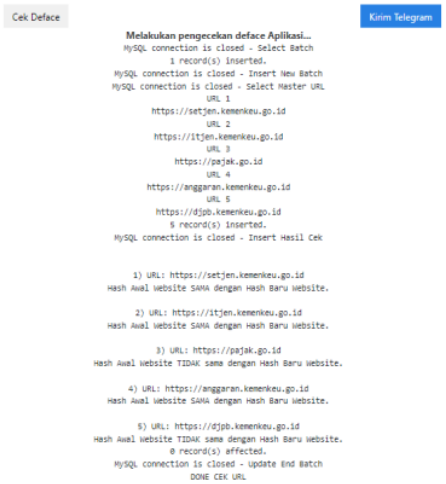
Apabila diklik pada setiap *url name* maka tampilan akan diarahkan ke halaman detail yang menampilkan grafik dari hasil pengecekan pada setiap *batch*. Grafik yang disajikan adalah diagram garis.

15

4.3 Halaman Program

Gambar 10. Halaman Program

Halaman Program merupakan halaman yang memiliki 2 menu yaitu Cek Deface dan Kirim Telegram.



Gambar 11. Hasil Proses Cek Deface

Pada gambar diatas menunjukkan proses saat user menjalankan menu Cek Deface. Proses pertama kali yang dilakukan ialah mengambil data daftar *URL master* dari *database*, kemudian langkah selanjutnya yang dilakukan yaitu melakukan perulangan pengecekan hasil *crawlimg url* untuk mengambil data halaman *website* terkini. Setelah proses tersebut berhasil, hasil *crawling url* yang berupa *text* dihapus semua karakter *whitespace* menyambung menjadi 1 teks panjang tanpa jeda (*string*). Kemudian *string* tersebut dipotong tanpa jeda sesuai dengan panjang n yang diinginkan dan disimpan dalam bentuk list (*chunk*). Setiap *chunk* potongan *string* dienkripsi menggunakan SHA1. Selanjutnya hash awal dengan hash terkini dibandingkan untuk mendapatkan hasil komparasi.

4.4 Hasil Pengecekan pada Telegram

Gambar 1. Halaman Kirim Telegram

Pada halaman proses Kirim Telegram, hanya menunjukkan jumlah total URL di cek, jumlah halaman URL yang normal serta nama url yang terindikasi deface.

5. KESIMPULAN

Web Defacement Monitoring Dengan Menggunakan Metode Komparasi Nilai Hash SHA1 merupakan *website application* yang telah berhasil dibangun sesuai dengan kebutuhan untuk mendeteksi perubahan tampilan halaman *web* dan mengirimkan notifikasi hasil pendeteksiannya. Penelitian dan pembangunan *Web Defacement Monitoring* dengan menggunakan Metode Komparasi Nilai Hash SHA1.

6. DAFTAR PUSTAKA

[1] R. Hidayat, 2010, Cara Praktis Membangun Website Gratis. Jakarta: Penerbit PT Elex Media Komputindo.

[2] Rashmi K. Verma, 2015, *Implementation of Web Defacement Detection Technique, International Journal of Innovations in Engineering and Technology* (IJI), vol 6 edisi 1, 134-135.

[3] Andi M. Panji, 2018, Aplikasi Pengujian Celah Keamanan Pada Aplikasi Berbasis Web, Fakultas Teknik Informatika Universitas Islam Indonesia. Yogyakarta, pp. 2-3

[4] BPPT CSIRT, 2014, Panduan Penanganan Insiden Web Defacement, Jakarta, Kementerian Komunikasi dan Informatika RI

[5] Muhammad S. Hasibuan, 2018, Analisis Serangan Deface Menggunakan Backdoor Shell Pada Website, Techno.COM, vol 17 no. 4, 416-417.

[6] Solichin, 2018, Pemrograman Web dengan PHP dan MySQL. Versi 1.0, Jakarta.

[7] Ogedebe, P.M & Jacob, B.P, 2012, Software Prototyping: A Strategy to Use When User Lacks Data Processing Experience. ARPN Journal of Systems and Software. vol. 2 no.6.

[8] Amanda, Yovi. 2020. "Apa itu Deface Website? Bagaimana Cara Mengatasinya?". Tersedia [https://www.niagahoster.co.id/blog/deface-adalah], diakses pada 1 Juli 2021

[9] Maryam Rambonang, Yosafat. 2015. "Klien Autentikasi Menggunakan Algoritman SHA-1 Dengan Protokol Two Way Challenge-Response pada Transaksi Web-based" (hlm.). Yogyakarta: Universitas Sanata Dharma.

[10] L. Shklar dan R. Rosen, Web Application Architecture: Principles, protocols and practices. Inggris: 2003. [e-book] Tersedia: https://www.semanticscholar.org/.

[11] Y. Yudhanto dan H. A. Prasetyo, Mudah Menguasai Framework Laravel. Bandung: Penerbit Informatika, 2018, hal. 50.

[12] P. Safira, Amera. 2021. "CodeIgniter: Pengertian, Keunggulan, & Cara Menggunakannya",. Tersedia [https://www.goldenfast.net/blog/codeigniter-adalah/]. diakses pada 1 Juli 2022

[13] Dwi Kusuma, Afrizal. 2019. "Penggunaan Telegram Bot Pada Telegram Messeger Dengan Metode Webhooks Untuk Sistem Peminjaman Infratruktur Di UIN Maulana Malik Ibrahim

Malang" (hlm. 13). Malang: UIN Maulana Malik Ibrahim.
[14] A. Solichin, Pemrograman Web dengan PHP dan MySQL. Versi 1.0, Jakarta: 2018. [ebook] Tersedia: [https://www.researchgate.net/publication/303288753_Pemrograman_Web_dengan_PHP_dan_MySQL.] diakses pada 1 Juli 2022
[15] M. Muslihudin dan Oktafianto, Analisis dan Perancangan Metode Sisem Informasi Menggunakan Metode Terstruktur dan UML. Yogyakarta: Penerbit Andi, 2016, hal. 58-63.

4852-12818-1-SM

ORIGINALITY REPORT

14%	12%	6%	4%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	publikasi.dinus.ac.id Internet Source	2%
2	repository.atmaluhur.ac.id Internet Source	2%
3	www.coursehero.com Internet Source	1%
4	Submitted to Royal Holloway and Bedford New College Student Paper	1%
5	Submitted to Universitas Brawijaya Student Paper	1%
6	Agatha Elisabet, Syah Alam, Indra Surjati. "Peningkatan Koefisien Refleksi Antena Mikrostrip 28 GHz dengan Slit", Jurnal Ecotipe (Electronic, Control, Telecommunication, Information, and Power Engineering), 2022 Publication	1%
7	ejournal.uksw.edu Internet Source	1%

8	journal.stmikglobal.ac.id Internet Source	1 %
9	doku.pub Internet Source	<1 %
10	jurnas.stmikmj.ac.id Internet Source	<1 %
11	digilib.uin-suka.ac.id Internet Source	<1 %
12	www.doria.fi Internet Source	<1 %
13	core.ac.uk Internet Source	<1 %
14	journals.upi-yai.ac.id Internet Source	<1 %
15	Nanda Diaz Arizona. "Aplikasi Pengolahan Data Anggaran Pendapatan Dan Belanja Desa (APBDES) Pada Kantor Desa Bakau Kecamatan Jawai Berbasis Web", CYBERNETICS, 2017 Publication	<1 %
16	adoc.pub Internet Source	<1 %
17	ejournal.unma.ac.id Internet Source	<1 %

18	text-id.123dok.com Internet Source	<1 %
19	jurnal.batan.go.id Internet Source	<1 %
20	eprints.ums.ac.id Internet Source	<1 %
21	fti.trisakti.ac.id Internet Source	<1 %
22	repo.unand.ac.id Internet Source	<1 %
23	www.hortichain.org Internet Source	<1 %
24	www.zonareferensi.com Internet Source	<1 %
25	media.neliti.com Internet Source	<1 %
26	journal.unj.ac.id Internet Source	<1 %

Exclude quotes	On	Exclude matches	Off
Exclude bibliography	Off		