Jurnal Sintaksis: Pendidikan Guru Sekolah Dasar, IPA, IPS dan Bahasa Inggris
Alamat Redaksi: STKIP Al-MaksumLangkat, Jln. Sei BatangSerangan No.04 Stabat
Vol.3, No.1, Desember 2020
e-ISSN: 2715-6176 / p-ISSN: 2715-5536
Website: http://jurnal.stkipalmaksum.ac.id/

ANALISIS KEMAMPUAN URL TERENKRIPSI BASE64 TERHADAP SERANGAN BRUTE FORCE

Tedy Putra[1)] Yudhi Andrian[2)]
[1]STKIP Al Maksum Langkat, Stabat, Indonesia
iqrastabat2015@gmail.com

ABSTRAK

Dalam pemrograman web terdapat 2 metode pengiriman data dari client ke server yaitu metode POST dan metode GET. Kelemahan dari metode GET adalah data/variabel yang dikirim dapat dilihat di URL. Pengguna dapat dengan mudah mengubah nilai data/variabel, menghasilkan informasi lain yang seharusnya tidak ditampilkan kepada pengguna. Untuk mengatasi masalah ini, dengan mengenkripsi data/variabel yang dikirim ke URL. Tujuan dari penelitian ini adalah untuk menganalisis tingkat keamanan data/variabel URL terenkripsi base64 terhadap serangan brute force. Dari hasil penelitian: dengan menggunakan URL terenkripsi base64, keamanan URL dari akses ilegal akan lebih baik. URL terenkripsi base64 masih memiliki celah saat serangan dilakukan menggunakan metode Brute Force. Namun, tingkat keberhasilan serangan ini sangat kecil. Tingkat keberhasilan serangan Brute Force pada URL terenkripsi base64 hanya 0,00892%.

Kata Kunci: Base64, Brute Force, URL, Metode GET

ABSTRACT

In web programming, there are 2 methods of sending data from client to server, namely the POST method and the GET method. The weakness of the GET method is data / variables that are sent can be seen in the URL. The user can easily change the value of the data / variable, resulting in other information that should not appear to the user. To solve this problem, by encrypting the data / variables sent to the URL. The purpose of this study was to analyze the security level of the base64 encrypted URL data / variable against brute force attacks. From the research results : by using a base64 encrypted URL, the URL security from illegal access will be better. The base64 encrypted URL still has a gap when an attack is carried out using the Brute Force method. However, the success rate of this attack is very small. The success rate of Brute Force attack on base64 encrypted URL is only 0.00892%.

Keywords: *Base64, Brute Force, URL, GET Mothode.*

Jurnal Sintaksis: Pendidikan Guru Sekolah Dasar, IPA, IPS dan Bahasa Inggris
Alamat Redaksi: STKIP Al-MaksumLangkat, Jln. Sei BatangSerangan No.04 Stabat
Vol.3, No.1, Desember 2020
e-ISSN: 2715-6176 / p-ISSN: 2715-5536
Website: http://jurnal.stkipalmaksum.ac.id/

I. PENDAHULUAN

Dalam pemrograman web, terdapat 2 metode pengiriman data dari client ke server, yaitu metode POST dan metode GET. Metode POST akan mengirimkan data atau nilai langsung ke action untuk ditampung, tanpa menampilkan pada URL. Sedangkan metode GET akan menampilkan data/nilai pada URL, kemudian akan ditampung oleh action. Kelemahan pada metode GET adalah tampilnya data/variable yang dikirimkan pada URL. Pengguna dapat dengan mudah mengubah nilai dari data/variable tersebut, sehingga menghasilkan informasi lain yang seharusnya tidak tampil pada pengguna. Untuk mengatasi kekurangan pada metode GET, salah satunya adalah dengan mengenkripsi data/variable yang dikirim pada URL. Enkripsi adalah proses mengamankan suatu informasi atau data dengan membuat informasi atau data tersebut tidak dapat dibaca tanpa bantuan pengetahuan khusus, sebaliknya dekripsi merupakan proses pengembalian informasi atau data yang sebelumnya telah dienkripsi supaya dapat dibaca Kembali.

Beberapa metode enkripsi telah diterapkan untuk mengamankan/mengenkripsi data/variable yang dikirim pada URL. Arhkan Subari dan Saiful Manan (2014) dalam penelitiannya menggunakan AESCHIPPER CLASS untuk Enkripsi URL di Sistem Informasi Akademin Fakultas Teknik Universitas Diponegoro. Arhkan Subari dan Saiful Manan menyimpulkan bahwa dengan enkripsi URL tidak menampilkan variable sebenarnya, tetapi yang ditampilkan adalah chipperteks hasil enkripsi. Arhkan Subari dan Saiful Manan juga menyimpulkan bahwa system enkripsi URL menyebabkan waktu akses menjadi lebih lama dengan selisih rata-rata 0,05 detik dibandingkan dengan system tanpa enkripsi. Aziz Pratama dan Erwin Gunadhi (2016) menerapkan kriptografi base64 untuk keamanan url (uniform resource locator) website dari serangan sql injection. Aziz Pratama dan Erwin Gunadhi menyimpulkan bahwa berdasarkan dari hasil pengujian yang telah dilakukan, diketahui bahwa sebelum diterapkannya kriptografi pada URL website, basis data dapat diakses dengan mudah menggunakan SQL injection . Sedangkan dengan diterapkannya kriptografi base64 pada URL website, informasi server dan basis data tidak dapat diakses.

Gat Gat Cooper (2018) melakukan penelitian untuk mencegah exploit url website sensitek stmik pontianak dengan algoritma blowfish. Gat Gat Cooper menyimpulkan bahwa algoritma Blowfish telah berhasil melakukan enkripsi dan dekripsi terhadap URL sehingga menghasilkan tingkat keamanan yang baik. Dari pengujian dan analisa yang telah dilakukan oleh Gat Gat Cooper menunjukkan bukti bahwa algoritma Blowfish berjalan dengan baik dalam mengenkripsi plaintext dan mendekripsi ciphertext. Syafmi Giffari Sipayung dan Guidio L (2019) melakukan analisa keamanan url yang menggunakan algoritma 3des. Syafmi Giffari Sipayung dan Guidio L menyimpulkan bahwa sebelum diterapkannya kriptografi pada URL website, basis data dapat diakses dengan mudah menggunakan SQL injection. Sedangkan dengan diterapkannya algoritma 3DES pada URL website, informasi server dan database tidak dapat diakses. Beberapa penelitian yang telah penulis sebutkan mendasari penulis untuk menganalisis lebih lanjut mengenai enkripsi pada URL website. Penulis ingin mengetahui tingkat keamanan dari data/variable URL yang terenkripsi tersebut. Penulis akan menguji tingkat keamanan URL terenkripsi base64 terhadap serangan brute force.

Jurnal Sintaksis: Pendidikan Guru Sekolah Dasar, IPA, IPS dan Bahasa Inggris
Alamat Redaksi: STKIP Al-MaksumLangkat, Jln. Sei BatangSerangan No.04 Stabat
Vol.3, No.1, Desember 2020
e-ISSN: 2715-6176 / p-ISSN: 2715-5536
Website: http://jurnal.stkipalmaksum.ac.id/

Transformasi *base*64 merupakan salah satu algoritma untuk encoding dan decoding suatu data ke dalam format ASCII, yang didasarkan pada bilangan dasar 64 atau bisa dikatakan sebagai salah satu metoda yang digunakan untuk melakukan encoding (penyandian) terhadap data *binary*. Karakter yang dihasilkan pada transformasi base64 ini terdiri dari A..Z, a..z dan 0..9, serta ditambah simbol "+" dan "/" serta satu buah karakter sama dengan (=) di dua karakter terakhir yang dipakai untuk pengisian padatau dengan kata lain penyesuaian dan menggenapkan data binary. Karakter simbol yang akan dihasilkan akan tergantung dari proses algoritma yang berjalan.

Tabel 1 Kode Index Base64 (URL and Filename Safe)

Value	*Encoding*	*Value*	*Encoding*	*Value*	*Encoding*	*Value*	*Encoding*
0	A	16	Q	32	g	48	w
1	B	17	R	33	h	49	x
2	C	18	S	34	i	50	y
3	D	19	T	35	j	51	z
4	E	20	U	36	k	52	0
5	F	21	V	37	l	53	1
6	G	22	W	38	m	54	2
7	H	23	X	39	n	55	3
8	I	24	Y	40	o	56	4
9	J	25	Z	41	p	57	5
10	K	26	a	42	q	58	6
11	L	27	b	43	r	59	7
12	M	28	c	44	s	60	8
13	N	29	d	45	t	61	9
14	O	30	e	46	u	62	-
15	P	31	f	47	v	63	_
						(*pad*)	=

Menurut Ariyus (2008) yang dikutip oleh Aziz [3], teknik enkripsi base64 sebetulnya sederhana, jika terdapat sebuah (string) bytes yang akan disandikan ke algoritma base64 maka tahapannya yaitu:

1. Pecah string bytes tersebut ke per-3 bytes.
2. Gabungkan 3 bytes menjadi 24 bit. dengan catatan 1 bytes = 8 bit, sehingga 3 x 8 = 24 bit.
3. Lalu 24 bit yang disimpan di-buffer (disatukan) dipecah-pecah menjadi 6 bit, maka akan menghasilkan 4 pecahan.
4. Masing masing pecahan diubah ke dalam nilai desimal, dimana maksimal nilai 6 bit dalah 63.
5. Terakhir, jadikan nilai-nilai desimal tersebut menjadi index untuk memilih maksimal index ke 64 atau karakter ke 63 dari penyusun base64.

Algoritma brute force adalah algoritma yang digunakan untuk mencocokan pattern dengan semua teks antara 0 dan n-m untuk menemukan keberadaan Patternteks. Algoritma brute force memecahkan masalah dengan sangat sederhana, langsung, dan jelas.

Secara rinci langkah-langkah yang digunakan algoritma brute force untuk mencocokkan string adalah, sebagai berikut:

1. Simpan semua kemungkinan huruf menjadi string.
2. Hasilkan indeks acak dari 0 hingga panjang string-1.
3. Cetak hasil pada indeks tersebut.
4. Lakukan langkah ini sebanyak n kali (di mana n adalah panjang string yang dibutuhkan).

Jurnal Sintaksis: Pendidikan Guru Sekolah Dasar, IPA, IPS dan Bahasa Inggris
Alamat Redaksi: STKIP Al-MaksumLangkat, Jln. Sei BatangSerangan No.04 Stabat
Vol.3, No.1, Desember 2020
e-ISSN: 2715-6176 / p-ISSN: 2715-5536
Website: http://jurnal.stkipalmaksum.ac.id/

II. METODE PENELITIA

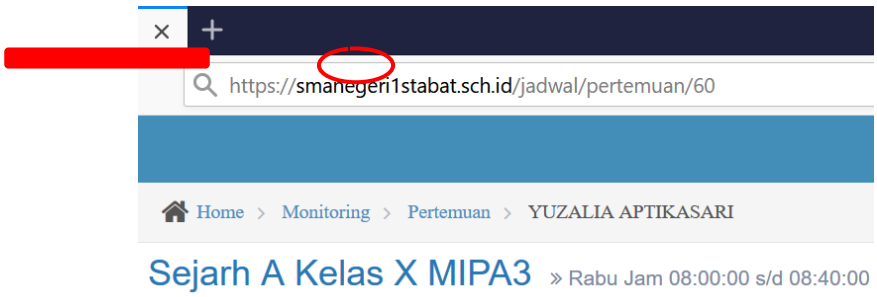
Tujuan penelitian ini adalah untuk menganalisis tingkat keamanan dari data/variable URL terenkripsi base64 terhadap serangan brute force. Untuk mencapai tujuan tersebut, penulis menggunakan aplikasi e-learning yang telah penulis rancang. Dalam aplikasi ini terdapat akses guru ke jadwal pertemuannya yang menggunakan metode GET. Langkah selanjutnya adalah penulis akan mengenkripsi data/variable yang dikirim melalui URL menggunakan metode *base*64. Kemudian hasil URL terenkripsi *base*64 akan diuji keamanannya dengan menggunakan brute force.

III. HASIL PENELITIAN DAN PEMBAHASAN

Dalam aplikasi e-learning yang penulis rancang, terdapat akses guru ke jadwal pertemuannya yang menggunakan metode GET, tampilannya ditunjukkan pada gambar 1.

Gambar 1 Tampilan Akses Guru Ke Jadwal Pertemuannya

Pada gambar 1, dapat dilihat bahwa halaman ini menggunakan metode GET, ditunjukkan pada URL "./jadwal/pertemuan/161" nilai 161 merupakan data/variable yang terhubung langsung ke database. Jika pengguna (dalam hal ini guru) mengganti nilai 161 menjadi nilai lain, maka akan tampil data jadwal pertemuan dari guru yang lain, seperti ditunjukkan pada gambar 2.



Gambar 2 Tampilan Akses Guru Ke Jadwal Pertemuan Guru Lain

Jurnal Sintaksis: Pendidikan Guru Sekolah Dasar, IPA, IPS dan Bahasa Inggris
Alamat Redaksi: STKIP Al-MaksumLangkat, Jln. Sei BatangSerangan No.04 Stabat
Vol.3, No.1, Desember 2020
e-ISSN: 2715-6176 / p-ISSN: 2715-5536
Website: http://jurnal.stkipalmaksum.ac.id/

Pada gambar 2, data/variable yang dikirim melalui URL "./jadwal/pertemuan/60" sebelumnya bernilai 161 diubah menjadi 60. Maka halaman akan menampilkan jadwal dari guru yang lain.

Langkah berikutnya penulis akan mengenkripsi data/variable yang dikirim pada URL, menggunakan metode enkripsi *base*64. Hasil URL terenkripsi *base*64 ditunjukkan pada gambar 3.

Gambar 3 Tampilan akses guru dengan URL terenkripsi *base*64

Data/variable 161 pada URL "./jadwal/pertemuan/161" dienkripsi menggunakan *base*64, menjadi "./jadwal/pertemuan/MTYx". Table 2 merupakan hasil URL terenkripsi *base*64.

Tabel 2 Hasil URL terenkripsi *base*64

URL awal	URL terenkripsi *base*64
"./jadwal/pertemuan/161"	"./jadwal/pertemuan/MTYx".
"./jadwal/pertemuan/60"	"./jadwal/pertemuan/NjA="
"./jadwal/pertemuan/10"	"./jadwal/pertemuan/MTA="
"./jadwal/pertemuan/30"	"./jadwal/pertemuan/MzA="
"./jadwal/pertemuan/101"	"./jadwal/pertemuan/MTAx"
"./jadwal/pertemuan/131"	"./jadwal/pertemuan/MTMx"
"./jadwal/pertemuan/160"	"./jadwal/pertemuan/MTYw"
"./jadwal/pertemuan/191"	"./jadwal/pertemuan/MTkx"
"./jadwal/pertemuan/261"	"./jadwal/pertemuan/MjYx"
"./jadwal/pertemuan/120"	"./jadwal/pertemuan/MTIw"

Dengan menggunakan URL terenkripsi *base*64, maka user akan sulit untuk melihat jadwal user lain. Karena untuk melihat jadwal user lain, maka kombinasi hasil enkripsi *base*64 harus sesuai dengan nilai yang tepat saat nilai tersebut didekrip. Saat kombinasi tidak sesuai, maka halaman tidak menampilkan data apapun.

Dengan cara manual akan memerlukan waktu yang lama untuk menemukan kombinasi yang sesuai dengan nilai dekripnya. Penulis merancang program brute force untuk mencoba kombinasi-kombinasi string yang sesuai agar e-learning dapat menampilkan halaman dari user lain. Pengujian pertama, penulis menggunakan 10 serangan Brute Force, hasil pengujiannya ditunjukkan pada table 3.

Jurnal Sintaksis: Pendidikan Guru Sekolah Dasar, IPA, IPS dan Bahasa Inggris
Alamat Redaksi: STKIP Al-MaksumLangkat, Jln. Sei BatangSerangan No.04 Stabat
Vol.3, No.1, Desember 2020
e-ISSN: 2715-6176 / p-ISSN: 2715-5536
Website: http://jurnal.stkipalmaksum.ac.id/

Tabel 3 Hasil URL Serangan Brute Force

No	URL Brute Force	Hasil Dekrip	Keterangan
1	"./jadwal/pertemuan/OyTr "	;$	Gagal
2	"./jadwal/pertemuan/tjBg "	0`	Gagal
3	"./jadwal/pertemuan/5Kbg "		Gagal
4	"./jadwal/pertemuan/nc7v "		Gagal
5	"./jadwal/pertemuan/yvlB "	A	Gagal
6	"./jadwal/pertemuan/l2mD "	i	Gagal
7	"./jadwal/pertemuan/XC7d "	\.	Gagal
8	"./jadwal/pertemuan/6A6q "		Gagal
9	"./jadwal/pertemuan/1NgR "		Gagal
10	"./jadwal/pertemuan/qB5B "	-A	Gagal

Pengujian berikutnya, penulis melakukan variasi serangan, yaitu 10 serangan Brute Force dilakukan sebanyak 10 kali. Kemudian 100 serangan Brute Force dilakukan sebanyak 10 kali, 1000 serangan, 10.000 serangan, 100.000 serangan, 200.000, 500.000 dan 1.000.000 serangan yamg masing-masing dilakukan sebanyak 10 kali. Hasilnya ditunjukkan pada table 4.

Tabel 4 Hasil Variasi jumlah Serangan Brute Force

Jumlah URL Brute Force	**No Pengujian**	**Keterangan**
10 URL Brute Force	1	10 Gagal
	2	10 Gagal
	3	10 Gagal
	4	10 Gagal
	5	10 Gagal
	6	10 Gagal
	7	10 Gagal
	8	10 Gagal
	9	10 Gagal
	10	10 Gagal
Total 100 URL Brute Force		**Gagal 100%**
100	1	100 Gagal
	2	100 Gagal
	3	100 Gagal
	4	100 Gagal
	5	100 Gagal
	6	100 Gagal

Jurnal Sintaksis: Pendidikan Guru Sekolah Dasar, IPA, IPS dan Bahasa Inggris
Alamat Redaksi: STKIP Al-MaksumLangkat, Jln. Sei BatangSerangan No.04 Stabat
Vol.3, No.1, Desember 2020
e-ISSN: 2715-6176 / p-ISSN: 2715-5536
Website: http://jurnal.stkipalmaksum.ac.id/

URL Brute Force	7	100 Gagal
	8	100 Gagal
	9	100 Gagal
	10	100 Gagal
Total 1.000 URL Brute Force		**Gagal 100%**
1.000 URL Brute Force	1	1.000 Gagal
	2	1.000 Gagal
	3	1.000 Gagal
	4	1.000 Gagal
	5	1.000 Gagal
	6	1.000 Gagal
	7	1.000 Gagal
	8	1.000 Gagal
	9	1.000 Gagal
	10	1.000 Gagal
Total 10.000 URL Brute Force		**Gagal 100%**
10.000 URL Brute Force	1	10.000 Gagal
	2	10.000 Gagal
	3	10.000 Gagal
	4	9.997 Gagal 3 Berhasil
	5	10.000 Gagal
	6	10.000 Gagal
	7	9.995 Gagal 5 Berhasil
	8	10.000 Gagal
	9	10.000 Gagal
	10	10.000 Gagal
Total 100.000 URL Brute Force		**Gagal 99,992 % Berhasil 0,008 %**
100.000 URL Brute Force	1	100.000 Gagal
	2	100.000 Gagal
	3	100.000 Gagal
	4	99.964 Gagal 36 Berhasil
	5	99.964 Gagal 36 Berhasil
	6	100.000 Gagal
	7	100.000 Gagal
	8	100.000 Gagal
	9	100.000 Gagal
	10	99.964 Gagal 36 Berhasil
Total 1.000.000		**Gagal 99,9892 %**

Jurnal Sintaksis: Pendidikan Guru Sekolah Dasar, IPA, IPS dan Bahasa Inggris
Alamat Redaksi: STKIP Al-MaksumLangkat, Jln. Sei BatangSerangan No.04 Stabat
Vol.3, No.1, Desember 2020
e-ISSN: 2715-6176 / p-ISSN: 2715-5536
Website: http://jurnal.stkipalmaksum.ac.id/

URL Brute Force		**Berhasil 0,0108 %**
200.000 URL Brute Force	1	200.000 Gagal
	2	200.000 Gagal
	3	199.925 Gagal 75 Berhasil
	4	200.000 Gagal
	5	200.000 Gagal
	6	200.000 Gagal
	7	200.000 Gagal
	8	199.925 Gagal 75 Berhasil
	9	200.000 Gagal
	10	200.000 Gagal
Total 2.000.000 URL Brute Force		**Gagal 99,9925 % Berhasil 0,0075 %**
500.000 URL Brute Force	1	500.000 Gagal
	2	500.000 Gagal
	3	500.000 Gagal
	4	499.817 Gagal 183 Berhasil
	5	500.000 Gagal
	6	499.817 Gagal 183 Berhasil
	7	500.000 Gagal
	8	500.000 Gagal
	9	500.000 Gagal
	10	499.817 Gagal 183 Berhasil
Total 5.000.000 URL Brute Force		**Gagal 99,98902 % Berhasil0,01098%**
1.000.000 URL Brute Force	1	1.000.000 Gagal
	2	1.000.000 Gagal
	3	1.000.000 Gagal
	4	999.634 Gagal 366 Berhasil
	5	1.000.000 Gagal
	6	1.000.000 Gagal
	7	1.000.000 Gagal
	8	999.634 Gagal 366 Berhasil
	9	1.000.000 Gagal
	10	1.000.000 Gagal
Total 10.000.000 URL Brute Force		**Gagal 99,99268 % Berhasil0,00732%**

Jurnal Sintaksis: Pendidikan Guru Sekolah Dasar, IPA, IPS dan Bahasa Inggris
Alamat Redaksi: STKIP Al-MaksumLangkat, Jln. Sei BatangSerangan No.04 Stabat
Vol.3, No.1, Desember 2020
e-ISSN: 2715-6176 / p-ISSN: 2715-5536
Website: http://jurnal.stkipalmaksum.ac.id/

Dari Tabel 4 dapat dilihat bahwa hasil pengujian untuk 10, 100, dan 1.000 URL serangan *Brute Force*, semua serangan gagal. Untuk 10.000 URL serangan *Brute Force*, pengujian ke-4 dan pengujian ke-7 terdapat serangan yang berhasil. Pada 100.000, 200.000, 500.000 dan 1.000.000 URL serangan *Brute Force* terdapat juga serangan yang berhasil. Jumlah serangan yang berhasil dari 10 kali percobaan yaitu 2 sampai 3 kali serangan yang berhasil. Jika dirata-ratakan dari 10.000 s/d 1.000.000 URL serangan Brute Force dengan masing-masing 10 kali percobaan, tingkat percobaan yang berhasil sebesar 0,00892 %.

IV. SIMPULAN

1) Kesimpulan

Dari hasil penelitian dapat diambil beberapa kesimpulan antara lain:

1. Dengan menggunakan URL terenkripsi *base*64, maka keamanan URL dari akses yang illegal akan lebih baik.
2. URL terenkripsi *base*64 masih memiliki celah saat dilakukan penyerangan dengan metode Brute Force. Namun tingkat keberhasilan penyerangan ini sangat kecil.
3. Tingkat keberhasilan serangan Brute Force pada URL terenkripsi *base*64 hanya sebesar 0,00892 %.

2) Saran

Dengan memperhatikan kesimpulan dari kegiatan penellitian ini maka peneliti menyarankan agar sistem keaamanan yang terenkripsi base64 untuk dapat digunakan agar akses ilegal dapat terblok atau dihambat dengan lebih baik.

DAFTAR PUSTAKA

Annas, et al. 2017. *Analisis Tingkat Keamanan Enkripsi Data Menggunakan Algoritma Base 64 Endcode*. Prosiding Annual Research Seminar 2017 Computer Science and ICT.

Arhkan Subari dan Saiful Manan. 2014. Implementasi AESCHIPPER CLASS untuk Enkripsi URL di Sistem Informasi Akademin Fakultas Teknik Universitas Diponegoro. *Jurnal Sistem Komputer*, .4(2).

Aziz Pratama dan Erwin Gunadhi. 2016. Penerapan Kriptografi Base64 Untuk Keamanan URL (Uniform Resource Locator) Website Dari Serangan Sql Injection. *Jurnal Algoritma*, 13(2).

Gat Gat Cooper. 2018. *Mencegah Exploit URL Website Sensitek STMIK Pontianak Dengan Algoritma Blowfis.* https://www.researchgate.net/publication/339658530.

Heny Pratiwi, et, al. 2016. Implementasi Algoritma Brute Force Dalam Aplikasi Kamus Istilah Kesehatan, *Jurnal Ilmiah Teknologi Informasi Terapan*, 2(2).

Syafmi Giffari Sipayung dan Guidio L. 2019. *A*nalisa Keamanan URL Yang Menggunakan Algoritma 3DES. *KOMIK (Konferensi Nasional Teknologi Informasi dan Komputer*, 3(1).