KOMIK (Konferensi Nasional Teknologi Informasi dan Komputer)
Volume 3, Nomor 1, Oktober 2019
DOI: 10.30865/komik.v3i1.1612

ISSN 2597-4645 (media online)
ISSN 2597-4610 (media cetak)
Page: 349-354

ANALISA KEAMANAN URL YANG MENGGUNAKAN ALGORITMA 3DES

Syafmi Giffari Sipayung[1], Guidio L. Ginting[2]

Program Studi Teknik Informatika STMIK Budi Darma, Medan, Indonesia
Email: [1]egisipayung3@gmail.com

Abstrak

Uniform Resource Locator (URL) sebagai penghubung antar halaman atau sebagai tempat suatu folder, data, maupun file menjadikan URL merupakan tempat yang sangat strategis karena terhubung langsung dengan database. Masalah yang terdapat pada URL adalah bagian dari URL yaitu value dari parameter akan terliat pada address bar suatu browser sehingga akan memberikan informasi data yang ditampilkan pada halaman website. Masalah pada parameter tersebut merupakan celah keamanan yang bisa dimanfaatkan oleh pengguna yang berniat jahat. Pada penelitian ini akan menerapkan algoritma 3DES pada pembentukan value dari parameter URL sehingga value yang ditampilkan pada address bar akan berupa hasil enkripsi yaitu ciphertext. Dengan menerapkan algoritma 3DES pada pembangkitan URL akan memberikan keamanan pada URL tersebut, karena value dari parameter URL tidak bisa dimengerti oleh pengguna.

Kata kunci: *URL, Kemanan, Kriptografi, algoritma 3DES*

Abstract

Uniform Resource Locator (URL) as a link between pages or as a place of a folder, data, and file makes the URL a very strategic place because it is connected directly with the database. The problem with URLs is that part of the URL is that the value of the parameter will appear in the browser's address bar so that it will provide data information that is displayed on the website page. Problems with these parameters are security holes that can be exploited by malicious users. In this research, 3DES algorithm will be applied to the formation of values from URL parameters so that the value displayed in the address bar will be the result of encryption, ciphertext. Applying the 3DES algorithm to generating URLs will provide security for the URL, because the value of the URL parameter cannot be understood by the user.

Keywords: URL, security, cryptography, 3DES algorithm

1. PENDAHULUAN

URL atau Unifrom Resource Locator secara umum merupakan sebuah alamat yang merujuk ke suatu file pada website atau pada fasilitas internet lainnya. Secara umum URL berfungsi untuk mengidentifikasikan dimana sumberdaya tersedia dan mekanisme pengambilan sumberdaya itu sendiri. Pada komputer yang dimaksud dengan sumberdaya yaitu merupakan sebuah dokumen, gambar, maupun file lainnya. Contoh dari URL adalah http://www.microsoft.com/default.asp, berdasarkan contoh tersebut bisa dilihat bahwa resource atau file yang akan ditampilkan oleh halaman www.microsoft.com adalah default.asp. Dari penjelasan tersebut maka timbul suatu masalah yaitu jika resource atau value dari parameter dari suatu URL terlihat jelas dan disadari oleh pengguna yang berniat untuk mencuri atau merubah data, maka itu dapat menjadi suatu masalah keamanan website. Masalah dari keamanan url tersebut menjadi celah yang paling sering digunakan peretas untuk melakukan tindakan kejahatan terhadap Website.

Salah satu algoritma dari kriptografi adalah 3DES (Triple Data Encryption Standart), 3DES merupakan penyempurnaan dari algoritma DES dengan kelebihan melakukan 3 kali enkripsi DES dengan panjang kunci 3 kali DES 168-bit. Pada algoritma 3DES dibagi menjadi tiga tahap, setiap tahapnya merupakan implementasi dari algoritma 3DES. Setelah itu, dibuatlah beberapa pengembangan dari DES dengan cara memperbesar ruang kunci. Varian pengembangan DES yang paling dikenal adalah DES Berganda (3DES), yakni pemanfaatan DES berkali-kali untuk proses enkripsi dan dekripsinya. Double DES (3DES) mempunyai kelemahan yaitu ia dapat diserang dengan algoritma yang dikenal sebagai meet-in-the-middle-attack, yang pertama kali ditemukan oleh . Sebagai bentuk pencegahan terhadap serangan tersebut, maka digunakanlah tiga kali langkah DES. Bentuk tersebut dinamakan sebagai 3DES.

Penelitian ini menggunakan algoritma 3DES berdasarkan penelitian sebelumnya yang dilakukan oleh Drs. Akik Hidayat, M.Kom dengan judul “Enkripsi dan Dekripsi Data Menggunakan Algoritma 3DES” menyimpulkan proses enkripsi dan dekripsi suatu data dengan algoritma 3DES dilakukan dengan cara mengimplementasikan algoritma DES sebanyak tiga kali, sesuai dengan pemilihan kuncinya dan urutan proses yang dipilih, Waktu yang diperlukan untuk proses enkripsi dan dekripsi dipengaruhi oleh ukuran file, dan Waktu yang diperlukan untuk mencoba seluruh kemungkinan kunci oleh serangan brute force adalah 1,183 x 1043 tahun[1]. Penelitian kedua dilakukan oleh Saprijal dengan judul “Perancangan Aplikasi Penyandian Pada File Suara Menggunakan Algoritma 3DES” menyimpulkan teknik yang dilakukan dalam penyandian file suara yaitu dengan cara menerapkan algoritma 3DES kedalamnya yang bisa mengubah data asli ke dalam bentuk data rahasia, dan pada penyandian file suara dengan menggunakan kode algoritma 3DES akan lebih optimal jika 3DES karakter dari informasi tersebut tidak banyak walaupun frekuensi kemunculannya tinggi[2] .

2. LANDASAN TEORI

ISSN 2597-4645 (media online)
ISSN 2597-4610 (media cetak)
Page: 349-354

2.1 URL (Uniform Resource Locator)

Uniform Resource Locator (URL) adalah alamat sumber daya akses jarak jauh. URL mencakup semua pengidentifikasi sumber daya yang dimaksudkan untuk menyediakan akses online ke sumber daya menggunakan browser internet standar[5]. URL adalah singkatan dari Uniform Resource Locator yang merupakan rangkaian karakter yang berdasarkan format standar tertentu, fungsi URL yaitu untuk menunjukkan alamat dari suatu situs atau sumber misalkan seperti file, dokumen dan gambar yang ada di internet. URL merupakan susunan dari beberapa karakter seperti angka, huruf dan simbol berdasarkan standar yang sudah ditentukan, yang memiliki fungsi untuk menunjukkan sebuah alamat atau suatu sumber yang berada di internet. URL merupakan serangkaian karakter menurut standar tertentu yang bisa dipakai untuk menunjukkan sebuah alamat dari sumber, seperti gambar/file yang ada di internet.

Uniform Resource Locator atau URL dapat digambarkan sebagai berikut[5]:

1. http://dx.dio.org/10.3133/of2007-1047
   Merupakan URL untuk halaman U.S Geological Survey dan file yang ditampilkan adalah file 2007-1047.
2. http://nbn-resolving.de/urn:nbn:de:gbv:089-3321752946
   Merupakan URL untuk halaman Oliver Schmachtenberg's dengan file yang ditampilkan desertasi Nitric Oxide.

2.2 3DES (Triple Data Encryption Standard)

Pada dasarnya algoritma yang digunakan sama hanya pada Triple Data Encryption Standard (3DES) dikembangkan dengan melakukan enkripsi dan implementasi algoritma DES sebanyak tiga kali 3DES memiliki tiga buah kunci yang berukuran 168-bit (tiga kali kunci 56-bit dari des)[2]. Triple Data Encryption Standard (3DES) pengembangan dari algoritma DES (Data Encryption Standard) yang melakukan enkripsi dengan 3 langkah dari DES yang menggunakan key 168-bit (tiga kali kunci 56-bit dari DES). Tahap pertama, menggunakan kunci pertama (K1) yaitu 56-bit dari keseluruhan key dan melakukan enkripsi pada plaintext yang akan menghasilkan pra-chiphertext pertama. Tahap kedua, pra-ciphertext pertama yang dihasilkan pada tahap pertama, kemudian dioperasikan dengan kunci eksternal kedua (K2) dan melakukan proses enkripsi atau proses dekripsi (tergantung cara pengenkripsian yang digunakan) dengan menggunakan algoritma DES. Sehingga menghasilkan pra-ciphertext kedua. Tahap terakhir, pra-ciphertext kedua yang dihasilkan pada tahap kedua, dioperasikan dengan kunci eksternal ketiga (K3) dan melakukan proses enkripsi dengan menggunakan algoritma DES, sehingga menghasilkan ciphertext (C). Proses padding adalah suatu proses penambahan byte-byte dummy pada byte-byte sisa yang masih kosong pada blok plainteks, disimpan pada posisi paling terakhir, jika pada plaintext ataupun kunci kurang pada jumlah bit, maka ditambahkan padding berupa bit 0 pada akhir bit kekurangan hingga bit tersebut memiliki jumlah yang cukup.

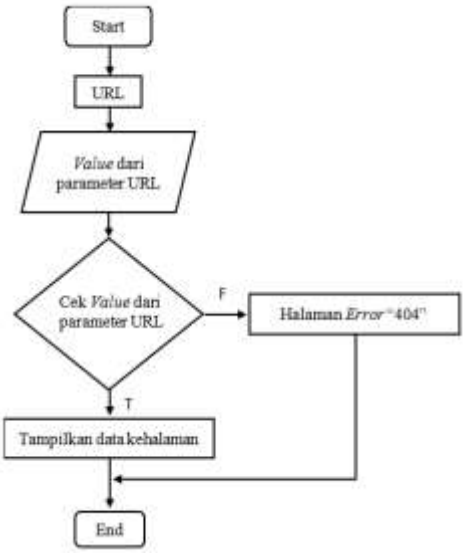
3. ANALISA DAN PEMBAHASAN

Uniform Resource Locator (URL) adalah karakter tertentu yang berupa angka, huruf, dan simbol, yang menuju ke alamat di world wide web (www). URL digunakan untuk mengidentifikasi lokasi sebuah file dalam internet. Contoh dari sebuah URL adalah http://arsip.com/mahasiswa?m= 15110361, berdasarkan contoh tersebut, struktur dari URL dapat dijelaskan sebagai berikut:

1. Http menunjukkan protokol dimana fungsinya adalah menentukan jenis server yang berhubungan dengan anda.
2. Arsip adalah nama host untuk mengakases situs web khusus.
3. Com top level domain
4. Mahasiswa adalah nama folder yang anda klik untuk membuka dokumen yang dituju, sekaligus mewakili direktori untuk pengaturan halaman web atau file.
5. M merupakan parameter yang digunakan untuk menampung file atau karakter sebagai komponen yang di-request oleh user.
6. 15110361 adalah karakter atau data yang menjadi value dari parameter.

Berdasarkan analisa yang telah dilakukan, URL memiliki masalah keamanan yang terletak pada terlihatnya value dari sebuah parameter sehingga pengguna dapat melihat karakter tersebut dengan jelas. Hal ini akan menjadi masalah ketika user yang mengakses halaman tersebut memiliki niat jahat untuk mengubah data berdasarkan isi dari parameter tersebut, karena parameter yang di-request berhubungan langsung dengan database.

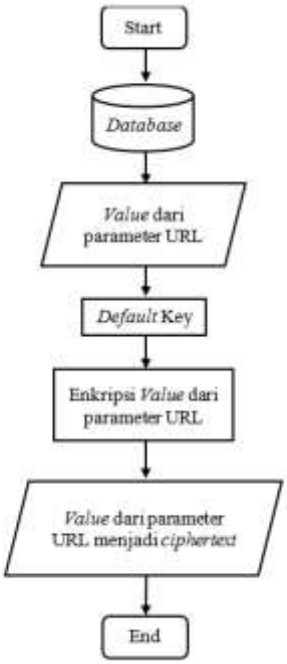
ISSN 2597-4645 (media online)
ISSN 2597-4610 (media cetak)
Page: 349-354



Gambar 1. Flowchart Url

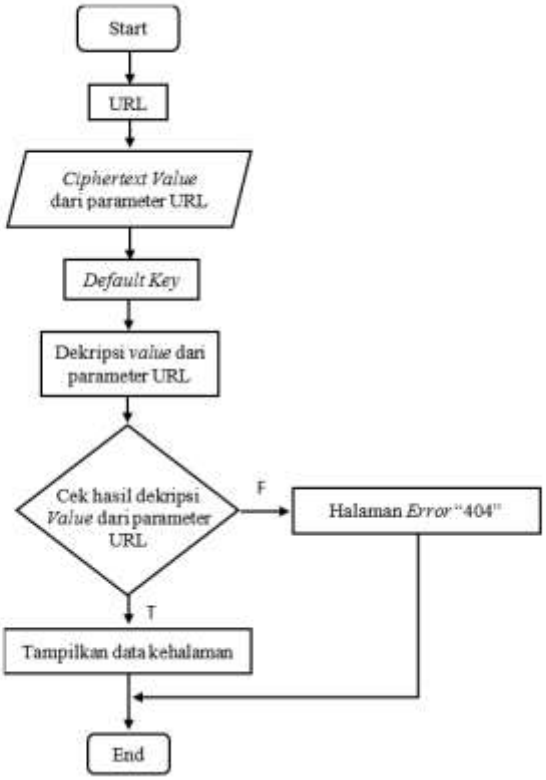
Dari gambar 3.1 diketahui bahwa value dari parameter URL diambil untuk diproses dengan cara mencocokkan value dengan data yang akan ditampilkan pada halaman, jika value dan data pada database memiliki kecocokan maka data yang sesuai dengan value akan ditampilkan pada halaman website dan address bar akan menampilkan informasi URL secara rinci. Ditampilkannya URL terutama value dari parameter akan memberikan informasi kepada pengguna bahwa ada data pada database yang cocok dengan value dari parameter, sehingga hal ini akan menjadi masalah bila diketahui oleh pengguna yang berniat jahat.

Untuk mengatasi masalah keamanan pada URL penelitian ini menggunakan algoritma Triple Data Encryption Standard (3DES) yaitu pengamanan berbasis kriptografi, dengan mengimplementasikan 3DES pada value dari parameter URL akan memberikan angka atau huruf acak pada address bar. Pengimplementasian algoritma 3DES dilakukan dengan menanamkan kunci 3DES menjadi default key pada sistem, menjadikan kunci dari 3DES tidak dapat dirubah sehingga proses enkripsi dan dekripsi akan dilakukan berdasarkan kunci tersebut. Pada pembentukan URL dilakukan dengan mengenkripsi value dari parameter yang didapat dari database sehingga akan memberikan value baru yang berupa ciphertext, tahapan dekripsi dilakukan pada controller yaitu saat pengguna melakukan aksi klik pada URL kemudian controller akan melakukan dekripsi pada value parameter sehingga value kembali ke bentuk asli dan mencocokkan value dengan data pada database yang ada, jika ada kecocokkan maka akan menampilkan data pada halaman website.



Gambar 2. Flowchart Url Dengan Enkripsi 3DES

ISSN 2597-4645 (media online)
ISSN 2597-4610 (media cetak)
Page: 349-354



Gambar 3. Flowchart Url Saat Dekripsi 3DES

Hasil implementasi 3DES pada URL akan menghasilkan value dari parameter berupa ciphertext yang telah dienkripsi sehingga pengguna akan melihat angka atau huruf yang acak pada value-nya tetapi pengguna tetap dapat me-request yang diinginkan sesuai dengan yang telah disediakan oleh administrator dan tidak dapat mengakses data langsung menggunakan URL. Contoh URL : http://arsip.com/mahasiswa?m=15110361 akan berubah menjadi http://arsip.com/mahasiswa?m=NBGGhYToB89RIl4sabFBqA==. Hasil dari algoritma 3DES menggunakan perubahan biner menjadi karakter, untuk mengatasi kendala pada URL yang tidak bisa menggunakan karakter-karakter tertentu maka biner dari hasil ciphertext akan dirubah kedalam hexa-desimal.

Berdasarkan hasil analisa yang telah dilakukan, maka penggunaan algoritma 3DES pada URL akan mencegah pengguna mengetahui arti isi dari value dari parameter, karena value berasal dari database secara tidak langsung maka pengamanan URL dengan menggunakan algoritma 3DES akan mengamankan database website.

4. IMPLEMENTASI

Algoritma kriptografi 3DES yang telah dikustomisasi diterapkan pada URL dengan menggunakan bahasa pemrograman PHP. Simulasi penerapan kriptografi 3DES yang telah dikustomisasi pada URL website dapat dilihat pada tabel 1.

Tabel 1. Penerapan Algoritma 3DES

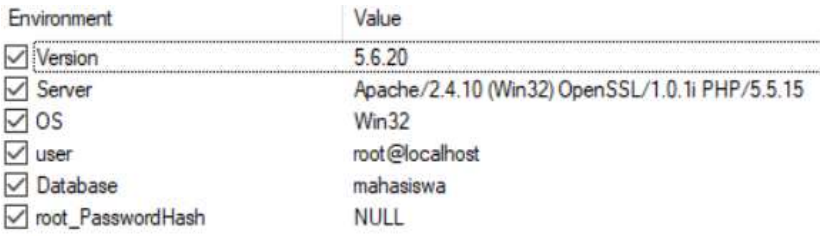
Sebelum Enkripsi 3DES	Sesudah Enkripsi 3DES
http://localhost/skripsiujicoba?m=15110361	http://localhost/skripsiujicoba?m=NBGGhYToB89RIl4sabFBqA==

Berdasarkan gambar diatas "http://localhost/skripsiujicoba/m=15110361", dengan kunci "inikuncisangatrahasia___". URL yang dienkripsi hanya pada value dari parameter URL atau pada bagian yang dapat mengidentifikasikan atribut yang berhubungan dengan data saja, dalam simulasi tersebut yang menjadi path file adalah kata "MARDIYAH". Bagian path file pada URL perlu dienkripsi, karena pada bagian tersebut terdapat informasi yang memberitahukan lokasi penyimpanan data pada storage ataupun basis data dan dapat menjadi celah bagi para hacker untuk mengakses data-data lain yang bersifat rahasia.

Pengujian keamanan dengan melakukan serangan terhadap URL website dengan metode SQL injection. SQL injection tool yang digunakan dalam pengujian ini adalah Web Cruiser Web Vulnerability Scanner. Proses pengujian akan dibagi menjadi dua bagian, yaitu pengujian website sebelum dan setelah diterapkan kriptografi algoritma 3DES.

ISSN 2597-4645 (media online)
ISSN 2597-4610 (media cetak)
Page: 349-354

Berdasarkan pengujian yang telah dilakukan terhadap URL sebelum diterapkan kriptografi algoritma 3DES, didapatkan informasi seputar server dan basis data yang digunakan. Seperti yang dapat dilihat pada gambar 4.



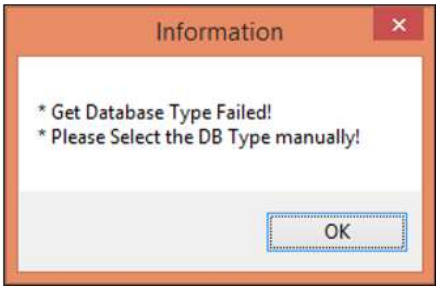
Environment	Value
Version	5.6.20
Server	Apache/2.4.10 (Win32) OpenSSL/1.0.1i PHP/5.5.15
OS	Win32
user	root@localhost
Database	mahasiswa
root_PasswordHash	NULL

Gambar 4. Informasi Sebelum Diterapkan Algoritma 3DES

Informasi tersebut kemudian dapat digunakan untuk mengakses data yang telah tersimpan pada database website, seperti nama database, tabel-tabel yang ada pada database hingga mendapatkan informasi isi record tabel. Informasi tersebut dapat dilihat pada gambar 5.

Gambar 5 *Database Website*

Berdasarkan pengujian yang telah dilakukan terhadap URL setelah diterapkan kriptografi algortima 3DES, informasi server dan basis data tidak dapat ditemukan. Seperti yang dapat dilihat pada gambar 6..



Gambar 6. Informasi Server dan Database Tidak Dapat Ditemukan

Berdasarkan pengujian yang telah dilakukan terhadap URL setelah diterapkan kriptografi algortima 3DES, Pengujian dilakukan dengan menggunakan beberapa sampel seperti pada tabel 7..

Tabel 7. Hasil Pengujian

Sampel	Keterangan
http://localhost/skripsiujicoba/m= 7bc329dcb9e8c44e	Database Tidak Terdeteksi
http://localhost/skripsiujicoba/preview.php?m=398189f697b38c134f3684e97f89b9458702ecfe0df50	Database Tidak Terdeteksi
http://localhost/skripsiujicoba/preview.php?m=4d9fc0557e9f7ee35687784f5a9838546f43af9be7b0	Database Tidak Terdeteksi
http://localhost/skripsiujicoba/preview.php?m=a3838a61a953eb4e81ccad7cbfe389b2580b684ae4732	Database Tidak Terdeteksi

ISSN 2597-4645 (media online)
ISSN 2597-4610 (media cetak)
Page: 349-354

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 algoritma 3DES pada URL website, informasi server dan database tidak dapat diakses. Hal tersebut dapat mengatasi ancaman terhadap keamanan data, terutama dari serangan SQL injection.

5. KESIMPULAN

Berdasarkan berbagai penjelasan dan hasil penelitian yang telah dilakukan, mengenai Analisa Keamanan URL Dengan Menerapkan Algoritma 3DES. Dapat disimpulkan beberapa hal, diantaranya:

1. Proses enkripsi dan dekripsi algoritma 3DES diawali dengan tahapan pembangkitan kunci dan dilakukan xor pada plaintext yang telah disubtitusikan dengan tabel PC-1 dan PC-2 sehingga akan menghasilkan enkripsi dan dekripsi. Perbedaan proses enkripsi dan dekripsi hanya terletak pada pembangkitan kunci
2. Pengamanan atau enkripsi dilakukan pada bagian URL yang menunjukkan path atau lokasi data yang disebut value dari parameter URL sehingga akan menghasilkan value yang berupa ciphertext. Untuk menampilkan data pada halaman terlebih dahulu dilakukan pengecekkan terhadap value dari parameter URL pada database, Sehingga value yang berisi ciphertext harus didekripsi terlebih dahulu sebelum dilakukan pengecekkan pada database.
3. Dengan menerapkan algoritma 3DES dalam pengamanan URL terhadap value dari suatu parameter terbukti dapat mengamankan resource website dari serangan SQL injection.

6. REFERENCES

[1] E. Dan, D. Data, and D. Algoritma, “Enkripsi dan dekripsi data dengan algoritma 3 des (,” pp. 1–11.

[2] J. P. Informatika, “PERANCANGAN APLIKASI PENYANDIAN PADA FILE SUARA MENGGUNAKAN ALGORITMA 3DES,” vol. 18, pp. 87–94, 2019.

[3] F. Rangkuti, Analisis Swot Teknik Membedah Kasus Bisnis. Jakarta: Gramedia Pustaka Utama, 1998.

[4] A. Prof. Dr. Jogiyanto HM, MBA, Analisis Dan Desain Sistem Informasi. Yogyakarta: C.V ANDI OFFSET, 2005.

[5] A. Welsh and S. Batley, RDA: resource description and access. American Library Association, 2013, 2018.

[6] U. A. Dony Ariyus, Pengantar Ilmu Kriptografi: Teori Analisis & Implementasi. Yogyakarta: C.V ANDI OFFSET, 2008.

[7] M. K. Emy Setyaningsih, S.Si., Kriptografi Dan Implementasinya Menggunakan MATLAB. Yogyakarta: C.V ANDI OFFSET, 2015.

[8] M. S. Rosa A.S, Rekayasa Perangkat Lunak. Bandung 40264: INFORMATIKA Bandung, 2018.

[9] D. M.Math., Ph.D, M.Sc., Suarga, Algoritma Pemrograman. Yogyakarta: C.V ANDI OFFSET.

[10] D. K. Agus Wahyu Widodo, Sistem Basis Data. Malang: Universitas Brawijaya Press, 2017.

[11] M. E. A. Edy Winarno ST, Buku Sakti Pemrograman PHP. Jakarta: Elex Media Komputindo, 2013.

[12] R. Yanto, Manajemen Basis Data Menggunakan MySQL. Yogyakarta: C.V ANDI OFFSET, 2016.

[13] A. Kadir, Konsep & Tuntunan Praktis Basis Data. Yogyakarta: C.V ANDI OFFSET, 2001.

[14] E. K. M Reza Faisal, Seri Belajar ASP.NET: ASP.NET Core 2 MVC & MS SQL Server dengan Visual Studio 2017. M Reza Faisal.