PENERAPAN KRIPTOGRAFI PADA PASSWORD DAN HAK AKSES DI LOGIN WEB MENGGUNAKAN SECURE HASH ALGORITHM DAN RSA PADA WEBSITE GURUNGAJI

SKRIPSI

untuk memenuhi sebagian persyaratan
mencapai derajat Sarjana S1
pada jurusan Informatika

disusun oleh

Riyanto Widodo

13.11.7337

PROGRAM SARJANA
PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2019

PERSETUJUAN

SKRIPSI

PENERAPAN KRIPTOGRAFI PADA PASSWORD DAN HAK AKSES DI LOGIN WEB MENGGUNAKAN SECURE HASH ALGORITHM DAN RSA PADA WEBSITE GURUNGAJI

yang disusun oleh

Riyanto Widodo
13.11.7337

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 7 Agustus 2019

Dosen Pembimbing,

Ali Mustopa, M.Kom
NIK. 190302192

ii

PENGESAHAN

SKRIPSI

PENERAPAN KRIPTOGRAFI PADA PASSWORD DAN HAK AKSES DI LOGIN WEB MENGGUNAKAN SECURE HASH ALGORITHM DAN RSA PADA WEBSITE GURUNGAJI

yang disusun oleh
Riyanto Widodo
13.11.7337
telah dipertahankan di depan Dewan Penguji
pada tanggal 16 Mei 2019

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Ali Mustopa, M.kom **NIK. 190302192**	
Erni Seniwati, M.Cs **NIK. 190302231**	
Bety Wulan Sari, M.Kom **NIK. 190302254**	

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 7 Agustus 2019

DEKAN FAKULTAS ILMU KOMPUTER

Krisnawati, S.Si, MT
NIK. 190302038

iii

PERNYATAAN

Saya yang bertandatangan dibawah ini menyatakan bahwa, skripsi ini merupakan karya saya sendiri (ASLI), dan isi dalam skripsi ini tidak terdapat karya yang pernah diajukan oleh orang lain untuk memperoleh gelar akademis di suatu institusi pendidikan tinggi manapun, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis dan/atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Segala sesuatu yang terkait dengan naskah dan karya yang telah dibuat adalah menjadi tanggungjawab saya pribadi.

Yogyakarta, 7 Agustus 2019

Riyanto Widodo

NIM. 13.11.7337

iv

MOTTO

- Manusia tidak selalu benar dan tidak selamanya salah, kecuali dia yang mau selalu mengoreksi dirinya dan memperbaiki.
- Kebanggaan terbesar adalah bukan tidak pernah gagal, tetapi bangkit kembali setiap kali jatuh. (*Confusius*)
- Kebaikan tidak bernilai selama diucapkan akan tetapi akan bernilai sesudah dikerjakan.
- Keberhasilan dan kesuksesan belum terasa nikmat jika belum merasakan kegagalan, segeralah bangkit dan berdiri tegaklah setiap menemui kegagalan.

PERSEMBAHAN

Selama menyelesaikan penyusunan skripsi ini penulis telah banyak bantuan dari berbagai pihak, baik secara langsung maupun tidak langsung. Untuk itu, dengan segala kerendahan hati, penulis ingin menyampaikan ucapan terima kasih yang sebesar-besarnya kepada semua pihak yang turut membantu, khususnya :

1. Kedua orang tuaku tercinta yang selalu memberikan kasih sayang, doa serta dorongan moral maupun materil yang tak terhingga.
2. Ibu Krisnawati, S.Si, MT selaku Dekan Universitas Amikom Yogyakarta.
3. Pak Ali Mustopa, M.kom selaku Dosen Pembimbing yang telah banyak memberikan masukan ilmu, waktu dan semangat serta memberikan pengarahan kepada penulis dalam penyusunan skripsi ini.
4. Ibu Erni Seniwati, S.Kom, M.Cs dan Ibu Bety Wulan Sari, M.Kom selaku Dosen Penguji yang telah banyak memberikan masukan dan meluangkan waktunya untuk menguji penulisan skripsi ini.
5. Mas Ferdy selaku owner Gurungaji yang telah membantu dalam menyelaikan skripsi ini
6. Semua pihak yang membantu penulis dalam menyelesaikan skripsi ini.
7. Kepada Ahmad Syabani yang telah membantu dalam perancangan coding di dalam web gurungaji.
8. Kepada Rizky Pramono yang bersedia menyumbangkan bakat editing gambar pada bab 4. Pokoknya jos lah.
9. Kepada Ridwan Pamungkas yang telah meluangjan waktu untuk membantu proses kriptografi di dalam coding saya.
10. Dan untuk author terrafost yang tidak mau di sebutkan nama aslinya yang berkebangsaan scotland,terima kasih atas sebuah sumbangan rumus RSA dan Secure Hash Algorithm nya.
11. Anak – anak kontraan dota yang telah menemani dalam kehidupan yang keras ini dan menjadikan lebih berwarna terutama albert, ucup, arif, sofyan, wahyu, dan duo titixxxx.

KATA PENGANTAR

Segala puji dan syukur penulis panjatkan kehadirat Allah SWT, karena berkat rahmat, hidayah dan karunia-Nya maka penulis dapat menyelesaikan skripsi ini dengan judul : "**PENERAPAN KRIPTOGRAFI PADA PASSWORD DAN HAK AKSES DI LOGIN WEB MENGGUNAKAN SECURE HASH ALGORITHM DAN RSA PADA WEBSITE GURUNGAJI ".**

Skripsi ini diajukan untuk memenuhi salah satu syarat dalam menempuh ujian Sarjana Teknik Informatika. Penulis menyadari bahwa penyusunan skripsi ini masih banyak terdapat kekurangan dan masih jauh dari kesempurnaan, hal ini dikarenakan keterbatasan kemampuan yang penulis miliki.

Atas segala kekurangan dan ketidaksempurnaan skripsi ini, penulis sangat mengharapkan masukan, kritik dan saran yang bersifat membangun kearah perbaikan dan penyempurnaan skripsi ini. Cukup banyak kesulitan yang penulis temui dalam penulisan skripsi ini, tetapi Alhamdullilah dapat penulis atasi dan selesaikan dengan baik.

Akhir kata penulis berharap semoga skripsi ini dapat bermanfaat bagi semua pihak dan semoga amal baik yang telah diberikan kepada penulis mendapat balasan dari Allah SWT.

Yogyakarta, 7 Agustus 2019

Penulis,

Riyanto Widodo

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

INTISARI

Aplikasi web yang di gunakan dalam beberapa bidang industri tentu memerlukan keamanan yang baik untuk menjaga data-data di dalam web tersebut. Apalagi web tersebut di gunakan dalam hal perbankan, layanan publik, atau e-commerce.

Untuk menjamin keamanan pada suatu web, kita harus menggunakan beberapa metode keamanan terhadap web tersebut yang sudah memenuhi standarisasi oleh Developer atau perusahaan yang mengembangin aplikasi-aplikasi atau skema keamanan data dan informasi. Dan salah satu bagian yang sangat rentan dan penting di dalam web adalah bagian login. Dari beberapa sumber bahwa ada beberapa jenis serangan yang biasa di gunakan untuk sebuah login di web, yaitu di antaranya CSRF(Cross Site Request Forgery) dan Rainbow Table Attack. Dengan menggunakan penyisipan Random Hashed Token dan gabungan Enkripsi dari Secure Hash Algorithm dan RSA, di harapakan bisa mengamankan Password dan Hak Akses di Login tersebut.

Dan untuk mengamankan dari serangan itu, saya akan menggunakan CSRF Token, Algoritma SHA, dan Algoritma RSA sebagai metode keamanannya. Di harapkan dengan penerapan metode ini, akan meminimalisir dampak buruk dari kedua serangan tersebut.

Kata-kunci: *Kriptografi, RSA, SHA, Token-based imitigation, rainbow table, CSRF, Gurungaji, keamanan web*

ABSTRACT

Web applications that are used in several fields of industry certainly require good security to maintain data on the web. Moreover, the web is used in terms of banking, public services, or e-commerce.

To ensure security on a web, we must use several methods of security for the web that have met the standardization by developers or companies that develop applications or data and information security schemes. And one of the most vulnerable and important parts of the web is the login section. From several sources that there are several types of attacks that are commonly used for a login on the web, including CSRF (Cross Site Request Forgery) and Rainbow Table Attack. By using the Random Hashed Token insertion and the combination of Encryption from Secure Hash Algorithm and RSA, it is hoped that you can secure the Password and Access Rights at the Login.

And to secure that attack, I will use the CSRF Token, the SHA Algorithm, and the RSA Algorithm as the security method. It is expected that the application of this method will minimize the adverse effects of both attacks.

Keywords: *Cryptography, RSA, SHA, Token-based imitigation, Rainbow table, CSRF, Gurungaji, Web Security*