ABSTRAK

IMPLEMENTASI ALGORITMA BLOWFISH UNTUK KEAMANAN DATA LOGIN PADA WEBSITE

Nama	: Irfan Sazali
Nim	: 6404221098
Dosen pembimbing 1	: Rezki Kurniati. M.kom
Dosen pembimbing 2	: Muhammad Ikhsan Wibowo S.Kom., M.T

Abstrak

Keamanan data login merupakan aspek penting dalam sistem informasi berbasis web, khususnya pada website akademik yang menyimpan data sensitif dan memiliki akun dengan hak akses tinggi. Website Teknik Informatika Politeknik Negeri Bengkalis masih memiliki potensi kerentanan pada sistem login akibat penggunaan metode pengamanan kata sandi yang kurang optimal, sehingga berisiko terhadap serangan siber seperti *brute force attack* dan pencurian kredensial. Penelitian ini bertujuan untuk meningkatkan keamanan data autentikasi dengan mengimplementasikan algoritma Blowfish pada sistem login website. Metode penelitian yang digunakan adalah metode pengembangan sistem yang meliputi tahap identifikasi masalah, analisis kebutuhan sistem, perancangan sistem, implementasi, dan pengujian. Algoritma Blowfish diterapkan untuk mengenkripsi password sebelum disimpan ke dalam basis data, serta dikombinasikan dengan mekanisme autentikasi dua faktor berbasis OTP dan pembatasan percobaan login. Hasil penelitian menunjukkan bahwa password berhasil disimpan dalam bentuk *ciphertext* dan tidak dapat dibaca secara langsung, sistem login berjalan sesuai fungsionalitas yang diharapkan, serta mekanisme OTP efektif dalam mencegah percobaan login berulang dan serangan *brute force*. Dengan demikian, penerapan algoritma Blowfish terbukti mampu meningkatkan keamanan data login pada website akademik.

Kata kunci : Keamanan Data, Sistem Login, *Algoritma Blowfish*, *OTP, Brute Force Attack*

ABSTRACT

IMPLEMENTASI ALGORITMA BLOWFISH UNTUK KEAMANAN DATA LOGIN PADA WEBSITE

Name	: Irfan Sazali
Nim	: 6404221098
Supervisor I	: Rezki Kurniati. M.kom
Supervisor 2	: Muhammad Ikhsan Wibowo S.Kom., M.T

Abstract

Login data security is a critical aspect of web-based information systems, especially academic websites that store sensitive information and manage accounts with high access privileges. The Informatics Engineering website of Politeknik Negeri Bengkalis still presents potential vulnerabilities in its login system due to the use of less optimal password protection methods, making it susceptible to cyberattacks such as brute force attacks and credential theft. This study aims to enhance authentication data security by implementing the Blowfish algorithm in the website's login system. The research adopts a system development method that includes problem identification, system requirements analysis, system design, implementation, and testing stages. The Blowfish algorithm is used to encrypt passwords before they are stored in the database and is combined with a two-factor authentication mechanism based on One-Time Passwords (OTP) and login attempt limitations. The results indicate that passwords are successfully stored in ciphertext form and cannot be directly read, the login system functions as expected, and the OTP mechanism is effective in preventing repeated login attempts and brute force attacks; therefore, the implementation of the Blowfish algorithm is proven to enhance login data security on academic websites.

Keywords : *Data Security, Login System, Blowfish Algorithm, OTP, Brute Force Attack*