

## INTISARI

Saat ini di web service penerimaan karyawan baru pada PT. Sumber Graha Sejahtera masih terbilang rawan akan adanya pencurian data. sehingga dengan rawannya pencurian, maka dari pihak HRD menginginkan adanya web service dengan sebuah keamanan. Dengan memberikan data penting pada web service tentunya ada peluang kemungkinan terjadinya kebocoran data, maka dari itu web service yang dibuat sangat memerlukan sebuah teknik keamanan. Teknik keamanan yang digunakan bernama kriptografi yang dimana peneliti menggunakan teknik password hash dengan algoritma blowfish untuk mengamankan web service, yang mana diharapkan dapat meminimalisir dari ancaman yang tidak diinginkan seperti dari para hacker. Tujuan dari penelitian ini adalah menggunakan pengamanan satu arah, yaitu password hash dan dengan algoritma blowfish atau biasa dikenal dengan bcrypt untuk mengamankan web service dari serangan luar. Pengamanan satu arah ini hanya mengenkripsi plain text menjadi chipper text, dan tidak bisa sebaliknya. Berdasarkan analisis yang diperoleh password hash dapat diterapkan di dalam sebuah web service saat melakukan Register. Teknik password hash dengan menggunakan algoritma blowfish diharapkan bisa meminimalisir kemungkinan terjadinya pencurian bahkan meskipun terjadi pencurian maka akan membutuhkan waktu yang lama untuk memecahkan plain text yang telah dienkripsi menjadi chipper text.

Kata kunci : Web service, Password Hash, Chipper Text, Algoritma Blowfish.

## ***ABSTRACT***

Currently on the web service for new employees at PT. Sumber Graha Sejahtera is still prone to data theft. with the vulnerability of theft, HRD wants a web service with a security. By providing important data on the web service, of course there is the possibility of data leakage, therefore the web service that is created really requires a security technique. The security technique used is called cryptography, where the researcher uses a password hash technique with the blowfish algorithm to secure the web service, which is expected to minimize unwanted threats such as from hackers. The purpose of this research is to use one-way security, namely hashed passwords and the blowfish algorithm or commonly known as bcrypt to secure web service from outside attacks. This one-way security only encrypts plain text into cipher text, and can't do the other way around. Based on the analysis obtained, the password hash can be applied to a web service when registering. The hash password technique using the blowfish algorithm is expected to minimize the possibility of theft even if the theft occurs it will take a long time to decipher the encrypted plain text into cipher text.

*Key word : Web service, Password Hash, Algorithm Blowfish.*