

JURNAL PENELITIAN

**PEMANFAATAN ALGORITMA BASE64 PADA KEAMANAN *SCRIPT* PHP (STUDI KASUS
: SISTEM INFORMASI AKADEMIK UNIVERSITAS MUHAMMADIYAH JEMBER)**



Oleh :

David Heriawanto (11 1065 1227)

**JURUSAN TEKNIK INFORMATIKA
FAKULTAS TEKNIK
UNIVERSITAS MUHAMMADIYAH JEMBER
2013**

ALGORITHM USING BASE64 PHP SCRIPT ON SECURITY
(CASE STUDY: UNIVERSITY ACADEMIC INFORMATION SYSTEMS
MUHAMMADIYAH JEMBER)

Name : David Heriawanto
NIM : 11 1065 1227
Supervisor I : Daryanto, Kom., M.Kom.
Supervisor II : Ali Lutfi Muharom, S.Si.

ABSTRACT

An information system can be said to be perfect if it can maintain credibility, validity and integrity of the data and to ensure the availability of services to users of information systems. Academic Information Systems at the University of Muhammadiyah Jember using the PHP programming language, where it is not uncommon for the attacks that endanger the continuity of information systems. Within a PHP file contains the entire script command system measures.

There are algorithms encode and decode Base64, Base64 algorithm encodes processing on a text that has meaning and benefits if read by humans will be not voting for the meaning and benefits, and vice versa with processing to decode the Base64 algorithm. Base64 algorithm utilization is expected to improve the security of an information system.

Keywords: Base64, Information Systems, PHP, encode, decode.

PENDAHULUAN

1.1 Latar Belakang

Sebuah sistem informasi dapat dikatakan sempurna jika dapat menjaga kredibilitas, validitas dan integritas data serta menjamin ketersediaan layanan bagi pengguna dari sistem informasi. Untuk menjaga keamanan sistem informasi berskala besar haruslah dengan keamanan yang bertingkat, mulai jaringan sistem jaringan, hardware dan software dari sistem informasi itu sendiri.

Pada sebuah sistem informasi yang terpusat pastilah rentan terhadap serangan dan peretasan sistem, seperti halnya Sistem Informasi Akademik yang ada di Universitas Muhammadiyah Jember yang menggunakan bahasa pemrograman PHP, dimana tidak jarang terjadi serangan yang membahayakan bagi kelangsungan sistem informasi. Di dalam sebuah file PHP berisi script seluruh perintah, langkah-langkah sistem dan konfigurasi database, maka dari itu diperlukan untuk mengamankan seluruh isi script dari file PHP tersebut, agar tidak disalahgunakan oleh pihak yang tidak bertanggung jawab.

Algoritma Base64 adalah metode yang digunakan untuk melakukan encode (penyandian) terhadap data binary sehingga menjadi format yang bisa dicetak normal. Algoritma Base64 terdapat encode dan decode, pemrosesan encode dengan algoritma Base64 pada sebuah teks yang memiliki arti dan manfaat jika dibaca oleh manusia akan menjadi tidak memiliki arti dan manfaat, begitu juga sebaliknya dengan pemrosesan decode dengan algoritma Base64.

Berdasarkan uraian di atas, maka penulis ingin menanggapi masalah keamanan sistem informasi dan sebagai bahan dalam penyusunan Tugas Akhir, dengan judul Pemanfaatan Algoritma Base64 Pada Keamanan Script PHP (Studi Kasus : Sistem Informasi Akademik Universitas Muhammadiyah Jember).

2.1 Sistem Informasi

Sistem Informasi adalah kombinasi dari teknologi informasi dan aktivitas orang yang menggunakan teknologi itu untuk mendukung operasi dan manajemen. Dalam arti yang sangat luas, istilah sistem informasi yang sering digunakan merujuk kepada interaksi antara orang, proses algoritma, data, dan teknologi. Dalam pengertian ini, istilah ini digunakan untuk merujuk tidak hanya pada penggunaan organisasi teknologi informasi dan komunikasi (TIK), tetapi juga untuk cara di mana orang berinteraksi dengan teknologi ini dalam mendukung proses bisnis.

Dengan demikian, sistem informasi antar-berhubungan dengan sistem data di satu sisi dan sistem aktivitas di sisi lain. Sistem informasi adalah bentuk komunikasi sistem di mana data yang mewakili dan di proses sebagai bentuk dari memori sosial. Sistem informasi juga dapat dianggap sebagai bahasa semi formal yang mendukung manusia dalam pengambilan keputusan dan tindakan.

2.2 Sistem Informasi Akademik Universitas Muhammadiyah Jember

Sistem Informasi Akademik (SIA) di Universitas Muhammadiyah Jember merupakan sebuah sistem terpadu yang digunakan oleh kalangan akademik. Penggunaan sistem informasi ini dimaksudkan untuk menghubungkan segala sesuatu yang berhubungan dengan aktivitas akademik yang dilaksanakan di Universitas Muhammadiyah Jember. SIA didirikan tahun 2010 dan diprakarsai oleh UPT. Pusat Data dan Informasi dalam implementasinya di Universitas Muhammadiyah Jember.

Sistem Informasi Akademik (SIA) di Universitas Muhammadiyah Jember di buat dengan bahasa pemrograman PHP yang disempurnakan kembali oleh UPT. Pusat Data dan Informasi sesuai kaidah dan alur sistem yang terjadi di Universitas Muhammadiyah Jember.

2.3 PHP (Personal Home Page)

Pada awalnya PHP merupakan kependekan dari Personal Home Page (Situs personal). PHP pertama kali dibuat oleh Rasmus Lerdorf pada tahun 1995. Pada waktu itu PHP masih bernama Form Interpreted (FI), yang wujudnya berupa sekumpulan skrip yang digunakan untuk mengolah data formulir dari web.

Selanjutnya Rasmus merilis kode sumber tersebut untuk umum dan menamakannya PHP/FI. Dengan perilsan kode sumber ini menjadi sumber terbuka, maka banyak pemrogram yang tertarik untuk ikut mengembangkan PHP.

Pada November 1997, dirilis PHP/FI 2.0. Pada rilis ini, interpreter PHP sudah diimplementasikan dalam program C. Dalam rilis ini disertakan juga modul-modul ekstensi yang meningkatkan kemampuan PHP/FI secara signifikan.

Pada tahun 1997, sebuah perusahaan bernama Zend menulis ulang interpreter PHP menjadi lebih bersih, lebih baik, dan lebih cepat. Kemudian pada Juni 1998, perusahaan tersebut merilis interpreter baru untuk PHP dan meresmikan rilis tersebut sebagai PHP 3.0 dan singkatan PHP diubah menjadi akronim berulang PHP: Hypertext Preprocessing.

Pada pertengahan tahun 1999, Zend merilis interpreter PHP baru dan rilis tersebut dikenal dengan PHP 4.0. PHP 4.0 adalah versi PHP yang paling banyak dipakai pada awal abad ke-21. Versi ini banyak dipakai disebabkan kemampuannya untuk membangun aplikasi web kompleks tetapi tetap memiliki kecepatan dan stabilitas yang tinggi.

Pada Juni 2004, Zend merilis PHP 5.0. Dalam versi ini, inti dari interpreter PHP mengalami perubahan besar. Versi ini juga memasukkan model pemrograman berorientasi objek ke dalam PHP untuk menjawab perkembangan bahasa pemrograman ke arah paradigma berorientasi objek.

Contoh program “Hello World” yang ditulis menggunakan PHP adalah sebagai berikut:

```
<?php
    echo "Hello World";
?>
```

2.4 Algoritma Base64

Base64 adalah istilah umum untuk sejumlah skema pengkodean serupa yang mengkodekan data biner dan menerjemahkannya ke dalam representasi basis 64. Istilah Base64 berasal dari konten pengkodean MIME tertentu.

Skema encoding base64 biasanya digunakan ketika ada kebutuhan untuk menyandikan data biner yang perlu disimpan dan ditransfer melalui media yang dirancang untuk menangani data tekstual. Hal ini untuk memastikan bahwa data tetap utuh tanpa perubahan selama pengiriman. Base64 digunakan umum dalam beberapa aplikasi termasuk email melalui MIME, dan penyimpanan data yang kompleks dalam XML.

Transformasi Base64 termasuk dalam kriptografi dan banyak digunakan di dunia internet sebagai media data format untuk mengirimkan data. Dikarenakan hasil dari transformasi base64 berupa plaintext, maka nilai ini akan jauh lebih mudah dikirim, dibandingkan format data berupa binary.

Beberapa pemakaian dari transformasi Base64 di lapangan seperti PEM, MIME, UTF-7, dan OpenPGP. (Agus Kurniawan, Konsep dan Implementasi Cryptography Dengan .NET, 2008)

- Privacy-Enhanced Mail (PEM)

Protokol PEM adalah protokol pertama kali yang menggunakan teknik transformasi base64, yang didasarkan pada RFC 989 tahun 1987, yang terdiri dari karakter 7-bit yang digunakan oleh server mail (SMTP) dalam transfer datanya. Sekarang versi PEM yang digunakan didasarkan pada RFC 1421, yang menggunakan karakter (A..Z, a..z) dan bilangan (0..9) serta dua simbol, yaitu “+” dan “/”.

- Multipurpose Internet Mail Extension (MIME)

Multipurpose Internet Mail Extensions, menggunakan “base64” sebagai salah satu dari dua skema pengkodean biner-ke-text (yang lainnya adalah “encoding Base64 quoted-printable”). MIME ini didasarkan pada RFC 1421 versi PEM. Menggunakan 64-karakter alfabet yang sama dan mekanisme encoding seperti PEM, dan menggunakan “=” simbol untuk output padding dengan cara yang sama, seperti yang dijelaskan di RFC 1521.

MIME tidak menentukan panjang tetap untuk saluran Base64-encoded, tetapi tidak menentukan panjang maksimum 76 karakter. Selain itu menetapkan bahwa setiap karakter abjad harus diabaikan oleh decoder kompatibel, walaupun sebagian besar implementasi menggunakan pasangan CR / LF untuk membatasi baris yang disandikan.

Jadi, panjang aktual MIME-compliant data biner Base64-encoded biasanya sekitar 137% dari panjang data asli, meskipun untuk pesan yang sangat singkat overhead dapat jauh lebih tinggi karena overhead dari header. Ukuran akhir data biner dikodekan Base64-sama dengan 1,37 kali ukuran data asli + 814 byte (untuk header). Dengan kata lain, Anda dapat perkiraan ukuran data decode dengan rumus ini: $\text{byte} = (\text{string_length}(\text{encoded_string}) - 814) / 1,37$

- UTF-7

Encoding UTF-7 didasarkan pada RFC 2152, yang ada pada umumnya disebut sebagai “Modified Base64”. UTF-7 menggunakan karakter MIME base64, tetapi tidak memakai padding “=”. Karakter “=” digunakan sebagai karakter escape untuk encoding “quoted-printable”. UTF-7 juga digunakan sebagai header MIME.

- OpenPGP

OpenPGP (PGP – Pretty Good Privacy) pada RFC 2440, yang menggunakan encoding 64-radix atau kadang disebut sebagai “ASCII Amor”. Teknik encodingnya didasarkan pada teknik encoding dari MIME, tetapi ditambah dengan 24-bit CRC checksum. Nilai checksum dihitung dari data input, sebelum dilakukan proses encoding.

Berikut ini adalah contoh penggunaan dari Algoritma Base64 dalam melakukan encoding karakter.

Kutipan dari Albert Einstein :

“Imajinasi lebih penting daripada pengetahuan”

Hasil Transformasi :

“SW1hamluYXNpIGxIYmloIHBlbnRpbmcgZGFyaXBhZGEgcGVuZ2V0YWwhlYW4=“

3.1. Metode Penelitian

Merupakan bentuk kegiatan identifikasi terhadap penelitian yang dilakukan. Pada tahapan ini penulis mengelompokkannya ke dalam 3 metode yaitu:

1. Metode Observasi (penelitian).

Metode yang dilakukan dengan cara melakukan pengamatan secara sistematis aktif dan mencatat hal-hal yang diperlukan dalam pembuatan desain implementasi dan pengolahan data proses.

2. Metode Studi Pustaka.

Pengumpulan data dengan cara mengumpulkan literatur, jurnal, paper dan bacaan-bacaan yang akan dibahas dengan bersumber buku-buku yang ada kaitannya dengan judul penelitian untuk membantu menyelesaikan pembangunan dalam sistem ini.

3. Metode Dokumentasi.

Metode untuk mengarsip berkas-berkas yang terkait dengan objek penelitian meliputi berkas pendataan dan laporan hasil pengujian.

3.2. Konsep Perhitungan Algoritma Base64

Base64 menggunakan karakter A – Z, a – z dan 0 – 9 untuk 62 nilai pertama, sedangkan 2 nilai terakhir digunakan untuk symbol (+ dan /). Beberapa metode encoding lain seperti uuencode dan binhex menggunakan 64 karakter yang berbeda untuk mewakili 6 binary digit, namun metode-metode tersebut tidak disebut sebagai encoding Base64.

Pada hasil encoding diatas kata “Rio” diganti menjadi “Umlv”. Pada tabel ASCII huruf R, i, o disimpan sebagai 82, 105, 111 atau dengan kata lain 01010010, 01101001, 01101111 pada bilangan berbasis 2 (biner). Apabila ketiga byte tersebut digabungkan, maka akan dihasilkan 24 bit buffer yaitu 010100100110100101101111.

Angka tersebut harus dikonversi sehingga berbasis 64, caranya dengan membagi 24bit tersebut dengan 6. Maka

dihasilkan 4 bagian dengan masing-masing 6bit. Kemudian masing-masing bagian tersebut dikonversi ke nilai yang ada di Base64.

3.3 Desain Proses Script File PHP yang Sudah ter-Encode di Web Server

Keterangan dari gambar di atas adalah :

1. Pengguna menjalankan sistem dan mengirim perintah ke Web Server.
2. Web Server menjalankan aplikasi Web, mencari dan memanggil file PHP yang sudah ter-encode dengan algoritma Base64.
3. PHP engine melakukan pembacaan dan pemrosesan isi script PHP.
4. Jika isi file ternyata sudah ter-encode, maka PHP engine melakukan pemrosesan isi script dengan melakukan decode di dalam PHP engine.
5. Hasil decode diproses kembali ke dalam PHP engine .
6. PHP engine mengirimkan script PHP dalam bentuk HTML.
7. File HTML dikirimkan ke Web Server agar bisa diproses.
8. Web Server mengirimkan dan menampilkan hasil pemrosesan kepada pengguna.

4.1 Implementasi Script PHP Sederhana

Dalam melakukan pengujian encode script PHP dengan algoritma Base64 diawali dengan pengujian pada script sederhana. Percobaan pertama adalah pada string sederhana berikut :

```
<?>
echo "Pengujian Sederhana Algoritma Base 64";
?>
```

Gambar 4.2 Script PHP Sederhana.

Dari script PHP di atas dilakukan encode berulang sampai 10 kali sampai dengan hasil seperti berikut ini

```
<?>
x('Vm0wd2QyVkhVWGhVV0dSUFZsZG9WRlI3Wkc5V01WbDNXa1JTVjFac2JETlhhMUpUVmpGYWRH
VkdiR0ZXVjFKSVZtMXplRlI5VGtsaFJscE9ZbXRLVIZadGNFSmxSbGw0V2toV2FGSnNjSEJXYTFaaFUx
WmFjbHBFVWxwV01VcElWbTAxVjJGR1NuUIZiRkpWVmtWd2RscFdXbXRXTVhCRIZXeG9hVlpyV1R
CV01uUnZWREpHVjFOdVRtcFRSVXBZV1ZSR2QyRkdXWGhYYIVaWFZtczFIRlpYZUZOVWJVWWTJW
bXBXVjFJemFHaFpla1poVjBaT2NtRkhhRk5sYlhoWFZtMXdUMkl4VWtkWFdHaFIzGhTY1ZSV1pGTk5
SbkJHVjJzNVZXSkdjRlpXYlhSelZqRmFSbUV6YUZkaGExcGhXbFphVDJOfNrfZFRiV3hUVFZWd1dGW
nRNVFJaVm14V1RVaG9WMkpyY0ZsWmJHaFRWMVpXY1ZKcmRGUldia0pIVjJ0ak5WWlhTbFpqUldSY
VIXczFjbFpxU2tabFZsSlpZVVprVjFKWVFRbFdiWEJIVkRKT2MxcEiUbfppVjNodlZGVm9RMWRzV1ho
```

WGJYUk9VbXN4TkZkclZtdGhWazVIVTI1T1ZtSIVSbFJXTVZwWFl6RldjbHBHWkU1V01VbzFWakowVT
FVeVJrZFhia3BQVmxkU1YxUlhOVzloUmxweFVtMUdhazFyTIVoV1YzaGhZa2RGZUdOR1VsaGlSbHBv
VlhWR2ExWXIUa1poUjJoVFRUSm9kbGRzWkRSWIZscHpWMjVPV2sweWFFOVZiVEUwVmpGU1YyRk
ZPVmRpVIZZMFZqSjRVMWRzV2taU1dHaGFUVVp3ZWxreWVHRmpiVkpIV2tkc1UyRXpRbGxXYlhoaF
lqSkZIRlpzWkZkaVJscFBWV3RrZW55UIBUMD0='); ?>

5.1. Kesimpulan

Berdasarkan hasil dari pengujian dan penerapan algoritma Base64 di Sistem Informasi Akademik Universitas Muhammadiyah Jember pada bab sebelumnya maka dapat diambil beberapa kesimpulan sebagai berikut :

1. Implementasi algoritma Base64 dapat meningkatkan keamanan isi dari script pada sistem informasi berbasis PHP karena hasil encode tidak dapat dibaca langsung oleh orang yang tidak bertanggung jawab.
2. Script hasil encode dengan algoritma Base64 dapat dijalankan langsung oleh web server PHP tanpa terjadi kendala.

5.2. Saran

Adapun saran yang diharapkan untuk membantu kelanjutan ke depan dari penelitian dan pengujian yang telah dibuat yaitu :

1. Diharapkan ke depannya implementasi bukan hanya pada script isi dari PHP melainkan pada script URL pada browser pengguna.
2. Diharapkan untuk pengembangan tidak hanya menggunakan algoritma Base64 melainkan digabung dengan algoritma lain.

Daftar Pustaka

- Cashman, S., (2009), *Discovering Computers (ed. 3): Fundamental*, Penerbit Salemba, Jakarta.
- David, P., (2010), *PHP Solution: Dynamic Web Desing Made Easy, Second Edition*, Penerbit Apress, Jakarta.
- Heri, S., (2006), *Pengantar Logika Informatika, Algoritma, dan Pemrograman Komputer*, Penerbit Andi, Jakarta.
- Jimmy, L., Gaol, (2009), *Sistem Informasi Manajemen, Pemahaman dan Aplikasi*. Penerbit Gramedia, Yogyakarta.
- Kurniawan, A., (2008), *Konsep dan Implementasi Cryptography Dengan .NET*, Penerbit PC Media, Jakarta.
- Dony, A., (2008), *Pengantar Ilmu Kriptografi: Teori Analisis & Implementasi*, Penerbit Andi, STIMIK AMIKOM Yogyakarta.
- Teguh, S., (2007), *Pemanfaatan MIME Base64 Untuk Menyembunyikan Source Code PHP*, Jurnal Institut Teknologi Bandung, Bandung.