

PERANCANGAN SISTEM KEAMANAN WEBSITE DENGAN KONFIGURASI FILE.HTACCESS

Rico Septiandi¹, Siti Madinah Ladjamuddin², Ewin Suciana³

Teknik Informatika - ISTN Jakarta^{1,2}, Yayasan Al-Hikmah Citra Raya³

Jl Moh Kahfi II, Srengseng Sawah, Jagakarsa^{1,2}, Blok J11 No 21 Graha Lestari Citra Raya³

septiandi.riko@gmail.com¹, citymadinah07@istn.ac.id², sucianaewin@gmail.com³

Abstrak

Saat ini perkembangan teknologi informasi memainkan peranan yang sangat penting dalam berbagai aspek kehidupan, Internet merupakan jaringan komputer global di seluruh dunia sebagai media komunikasi dan informasi modern yang dapat memberikan serta menampilkan berbagai informasi dan data kepada publik. Sistem keamanan website dengan konfigurasi file.Htaccess dibangun dengan tujuan untuk untuk melindungi website tersebut dari pencurian informasi yang sering terjadi pada saat ini. Sistem pengamanan ini sangat berguna untuk melindungi informasi dari serangan cracker. Karena pencurian data di Internet tidak dapat diketahui jika cracker tersebut mengambil informasi tanpa merusak sistem. Lain halnya dengan pencurian informasi yang sering terjadi dalam dunia nyata. Perancangan sistem keamanan webste ini dibuat dengan konfigurasi file.Htaccess dan Notepad ++. Tidak sedikit website yang menggunakan system otentikasi yang banyak di tembus oleh para cracker, mereka banyak mengincar website ini karena diduga menyimpan informasi yang rahasia. Perlu cara khusus dalam mengamankan website seperti ini. Dengan adanya sistem keamanan website menggunakan konfigurasi file.htaccess ini merupakan salah satu sarana untuk mengamankan halaman website.

Kata Kunci: Keamanan Website, File.Htaccess

Abstract

Currently the development of information technology plays a very important role in various aspects of life, the Internet is a global computer network around the world as a medium of communication and modern information that can provide and display various information and data to the public. Website security system with the configuration file.Htaccess built with the aim to to protect the website from the theft of information that often occur at this time. This security system is very useful to protect information from cracker attacks. Because data theft on the Internet can not be known if the cracker is taking information without damaging the system. Another case with the theft of information that often occurs in the real world. The design of webste security system is made with the configuration file.Htaccess and Notepad ++. Not a few websites that use a lot of authentication system penetrated by the crackers, they are eyeing this website for allegedly storing confidential information. Need a special way in securing a website like this. With the website security system using the configuration file.htaccess this is one means to secure the website page.

Keywords: Website Security, File.Htaccess

1. PENDAHULUAN

1.1. Latar Belakang

Pada masa era globalisasi ini komputer sangat penting dalam kebutuhan informasi yang akurat, tepat dan cepat dalam menyajikan data yang sangat lengkap merupakan salah satu tujuan penting. Dengan peningkatan kebutuhan akan informasi di dunia maya membuat para developer website berlomba-lomba menyajikan berbagai macam layanan sehingga para pengguna akan betah berkunjung ke dalam websitenya. Dari masa-masa ke masa teknologi website mengalami perkembangan yang begitu pesatnya dan kini bahkan memeralihkan aplikasi dektop yang selama ini kita kenal menjadi aplikasi berbasis web. Selain itu tidak sedikit diantara pengguna internet yang memanfaatkan *traffic* pengguna internet tersebut. Dari mulai bisnis online ataupun yang lainnya.

Website merupakan halaman yang dibangun untuk menyampaikan sebuah informasi. Ada banyak website yang tersedia di internet, dari mulai website personal hingga website milik pemerintahan. Informasi yang disampaikan pun beragam, ada yang sekedar menyampaikan informasi kepada seluruh pengunjung ada juga yang menggunakan system otentikasi dalam menyampaikannya. Tidak sedikit website yang menggunakan system otentikasi yang banyak di jebol oleh para *cracker*, mereka banyak mengincar website ini karena diduga menyimpan informasi yang rahasia. Perlu cara khusus dalam mengamankan website seperti ini. Dari uraian diatas maka timbul keinginan untuk membahas dan merancang suatu sistim yang dapat mengamankan website seperti tersebut.

1.2. Tujuan Penelitian

Tujuan penelitian ini untuk memberitahukan cara mengamankan halaman administrator menggunakan konfigurasi file.Htaccess, sehingga pengguna internet dapat melindungi website mereka dari serangan cracker.

2. LANDASAN TEORI

2.1. Metode Penelitian

Analisa Perancangan Sistem

1. Analisa Sistem

Seiring dengan perkembangan teknologi informasi saat ini serta untuk meningkatkan efesiensi kerja dan waktu, dalam mempermudah pekerjaan itu banyak cara yang dapat digunakan dalam menyampaikan sebuah informasi kepada seseorang. Salah satunya dengan media internet jika berbicara internet, kita tidak pernah bisa melepaskan kaitan antara internet dengan sebuah website.

Website merupakan halaman yang dibangun untuk menyampaikan sebuah informasi tapi belakangan ini para pemilik website merasa khawatir terhadap halaman serta informasi mereka di internet karena keberadaan para *cracker* yang pada umumnya mencari informasi penting dalam website tersebut dan mengambil alih kepemilikan website tersebut. Adapula yang hanya merubah tampilan halaman utama dari website tersebut. Tidak sedikit memang yang telah menjadi korban akibat ulah para *cracker* ini. Untuk memulai membangun suatu program mengenai sistem keamanan halaman website dengan menggunakan konfigurasi file .htaccess maka merencanakan alur kerja berdasarkan kebutuhan suatu website yang akan menggunakan sistem keamanan ini.

2. Analisa Sumber Daya

Dalam analisa ini berisi mengenai sumber daya yang dibutuhkan untuk merancang sistem keamanan halaman admin dengan konfigurasi file .htaccess, dilihat dari kebutuhan sumber daya perangkat keras, perangkat lunak serta alat pengujian yang dibutuhkan dalam *penelitian ini*.

3. Analisa Perangkat Keras

Tabel-1 Spesifikasi Perangkat Keras

Perangkat	Spesifikasi
Processor	Intel® inside CPU@ 1.6Ghz
RAM	4096 MB
Harddisk	259

4. Analisa Perangkat Lunak

Tabel-2 Spesifikasi Perangkat Lunak

Perangkat Lunak	Yang Digunakan
Sistem Operasi	Windows 8
Web Browser	Mozilla Firefox
Code Editor	Notepad ++

1.4. Alat Pengujian

1. Analisa Sistem Berjalan

Menganalisa suatu sistem yang sedang berjalan merupakan salah satu tahap untuk menganalisa suatu sistem akankah sesuai dengan tujuan utama sistem itu sendiri yaitu mengamankan halaman admin pada suatu website.

Analisa sistem dalam suatu perancangan sangat penting karena fungsi dari analisa itu sendiri yaitu untuk mengetahui bagaimana sistem itu berjalan agar sistem yang dibuat dapat menghasilkan output yang diinginkan dan dapat mencapai tujuan yang direncanakan.

2. Kode File.Htaccess Berjalan

Pada file .htaccess yang sedang berjalan ini masih belum ada kode keamanannya dan masih berisi suatu komen yang sudah disediakan.

```
##
# @package Joomla
# @copyright Copyright (C) 2005 - 2014 Open Source Matters. All rights reserved.
# @license GNU General Public License version 2 or later; see LICENSE.txt
##

##
# READ THIS COMPLETELY IF YOU CHOOSE TO USE THIS FILE!
#
# The line just below this section: 'Options +FollowSymLinks' may cause problems
# with some server configurations. It is required for use of mod_rewrite, but may already
# be set by your server administrator in a way that disallows changing it in
# your .htaccess file. If using it causes your server to error out, comment it out (add # to
# beginning of line), reload your site in your browser and test your self url's. If they work,
# it has been set by your server administrator and you do not need it set here.
##

## Can be commented out if causes errors, see notes above.
Options +FollowSymLinks

## Mod_rewrite in use.

RewriteEngine On

## Begin - Rewrite rules to block out some common exploits.
# If you experience problems on your site block out the operations listed below
# This attempts to block the most common type of exploit 'attempts' to Joomla!
#
# Block out any script trying to base64_encode data within the URL.
RewriteCond %{QUERY_STRING} base64_encode[^\(\)]*([^\)]*) [OR]
# Block out any script that includes a <script> tag in URL.
```

Gambar-1 Kode file .Htaccess Berjalan.

1.5. Analisa Sistem Usulan

Analisa system usulan adalah dimana analis system mengidentifikasi masalah- masalah kebutuhan pemakai, menyatakan secara spesifik sasaran yang harus dicapai untuk memenuhi kebutuhan pemakai, masalah alternative, metode pemecaha yang paling tepat, merencanakan dan menerapkan rancangan systemnya.

Kode File.Htaccess Usulan

Mengetahui kendala yang ada, maka dirancang sebuah sistem keamanan halaman website menggunakan konfigurasi file.htaccess dengan memasukan beberapa kode perintah pada file.Htaccess

```

ErrorDocument 400 /errors/400.html
ErrorDocument 401 /errors/401.html
ErrorDocument 403 /errors/403.html
ErrorDocument 404 /errors/404.html
ErrorDocument 500 /errors/500.html

DirectoryIndex mainpage.html
DirectoryIndex mainpage.html index.cgi index.php index.html

order deny,allow
deny from 123.456.789.000
deny from 456.78.90.
deny from .bing.com
allow from all

Redirect permanent /oldpage.html http://www.mydomain.com/newpage.html
Redirect permanent /olddirectory http://www.mydomain.com/newdirect

RewriteEngine on
RewriteCond %{HTTP_REFERER} !^$
RewriteCond %{HTTP_REFERER} !^http://(www\.)?namadomain.com/.*$ [NC]
RewriteRule \.(gif|jpg)$ - [F]

RewriteEngine on
RewriteCond %{HTTP_REFERER} !^$
RewriteCond %{HTTP_REFERER} !^http://(www\.)?mydomain.com/.*$ [NC]
RewriteRule \.(gif|jpg)$ http://www.mydomain.com/dontsteal.gif [R,L]

order allow,deny
deny from all

RewriteEngine On
RewriteBase /
RewriteCond %{REQUEST_FILENAME} !-f
RewriteCond %{REQUEST_FILENAME} !-d
RewriteRule . /index.php [L]

AddType application/octet-stream .doc .xls .pdf

```

Gambar-2 Tampilan Halaman Website Usulan

Perancangan

Perancangan dilakukan 2 langkah penelitian, dimana langkah pertama untuk melakukan penelitian web sebelum mengimplementasikan sistem dan langkah ke 2 untuk web yang telah diterapkan sistem keamanan.

1. Langkah Pertama

Dalam tahap ini, web target diuji coba sistem keamanan yang ada. Penelitian ini dilakukan untuk mendapatkan data dengan alat pengujian terhadap web yang belum diimplementasikan sistem keamanan baru. Data tersebut berupa hasil keamanan yang diterapkan dalam website tersebut.

2. Langkah Kedua

Dalam tahap ini diimplementasikan sistem keamanan yang baru terhadap web, tahap implementasi ini meliputi

- a. Implementasi secara internal
- b. Optimasi secara eksternal

Setelah melakukan tahap implementasi, dilakukan analisa menggunakan alat pengujian yang sama dengan tahap pertama, yaitu penggunaan search engine secara langsung serta khususnya analisa terhadap sistem keamanan dalam website tersebut. Setelah melakukan penelitian dalam dua tahap, dilakukan pembahasan terhadap hasil pengujian baik pengujian pada tahap pertama maupun pada tahap kedua.

Metode Sistem Keamanan Website

Dalam penelitian ini menggunakan dua penerapan metode Sistem Keamanan Website. Dua penerapan tersebut adalah penerapan secara internal dan penerapan secara eksternal.

1. Penerapan Sistem Secara Internal

Penerapan metode Sistem secara internal dilakukan untuk keamanan dari sisi web itu sendiri.

2. Penerapan Dengan .Htaccess

Dalam penerapan metode sistem ini akan dilakukan teknik-teknik yang dapat membuat sebuah url menjadi :

- Mem-proteksi Folder / Melindungi Folder dengan password
- Mengalihkan pengunjung website dengan otomatis
- Membuat halaman pesan tampilan error
- Menolak pengunjung dengan IP Address tertentu
- Merubah ekstensi file
- Hanya mengizinkan pengunjung dengan IP Address tertentu
- Mengizinkan/Menolak list direktori

3. Penerapan Sistem Keamanan Secara Umum

Disamping menerapkan metode sistem editor file htaccess, juga di terapkan metode lain. Namun penerapan ini hanya sebagai pelengkap saja, Metode tersebut antara lain adalah sebagai berikut :

- Password Direktori
- Instalasi Modul URL Rewrite

4. Penerapan Metode SEO Secara Eksternal

Metode SEO secara eksternal dilakukan di luar website, ini dimaksudkan untuk membantu keamanan secara internal. Metode secara eksternal adalah sebagai berikut :

5. Penggunaan Google Webmaster Tool

Google web master adalah fasilitas yang disediakan oleh google dalam optimalisasi dan keamanan website. Google web master sangat membantu untuk melengkapi optimalisasi serta keamanan web dari internal web.

3.HASIL DAN PEMBAHASAN

3.1. Implementasi Sistem

Setelah dianalisis dan dirancang secara rinci dan teknologi telah diseleksi dan dipilih. Tiba saatnya, sistem untuk di implementasikan. Implementasi sistem adalah langkahlangkah atau prosedur yang dilakukan dalam menyelesaikan desain sistem yang telah disetujui, untuk menguji, menginstal, dan memulai sistem baru atau sistem yang diperbaiki untuk menggantikan sistem yang lama, sedangkan tahap implementasi sistem merupakan tahap meletakkan sistem agar sistem dapat siap untuk dioperasikan. Tahap implementasi sistem terdiri dari langkah-langkah sebagai berikut ini :

1. Menerapkan rencana implementasi
2. Melakukan kegiatan implementasi
3. Tindak lanjut implementasi

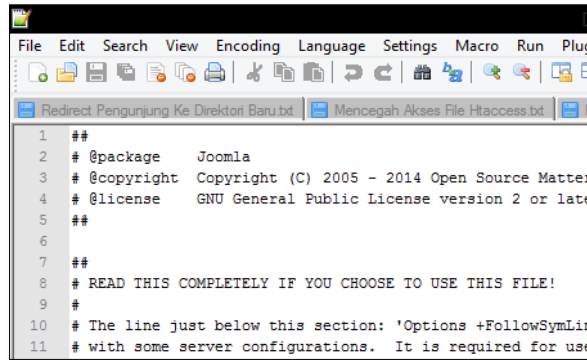
3.2. Tujuan Implementasi

1. Mengkaji rangkaian sistem baik dari segi software maupun hardware sebagai sarana pengolahan data dan penyaji informasi.
2. Menyelesaikan rancangan sistem yang ada dalam dokumen sistem yang baru atau yang telah disetujui.
3. Memastikan bahwa pemakai dapat mengoperasikan dengan mudah terhadap sistem yang baru dan mendapat informasi yang baik dan jelas.
4. Memperhitungkan bahwa sistem telah memenuhi permintaan pemakai yaitu dengan menguji sistem secara menyeluruh.
5. Memastikan bahwa sistem telah berjalan lancar dengan mengontrol dan melakukan instalasi secara benar.

Implementasi Input Kode

Custom HTTP Error

1. Buka file htaccess yang telah di download menggunakan notepad++



```

1  ##
2  # @package      Joomla
3  # @copyright    Copyright (C) 2005 - 2014 Open Source Matter
4  # @license      GNU General Public License version 2 or late
5  ##
6
7  ##
8  # READ THIS COMPLETELY IF YOU CHOOSE TO USE THIS FILE!
9  #
10 # The line just below this section: 'Options +FollowSymLin
11 # with some server configurations. It is required for use

```

Gambar 3 Editor File Htaccess

2. Ketikkan *script* berikut dalam baris terakhir file htaccess

```

ErrorDocument 400 /errors/400.html
ErrorDocument 401 /errors/401.html
ErrorDocument 403 /errors/403.html
ErrorDocument 404 /errors/404.html
ErrorDocument 500 /errors/500.html

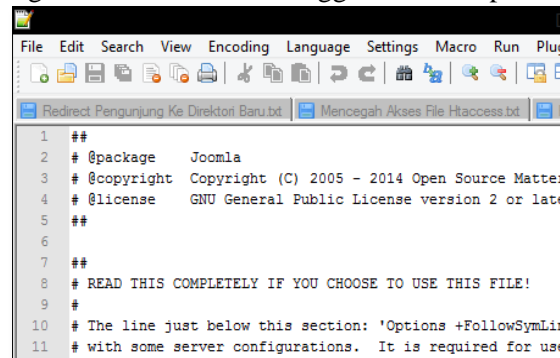
```

Gambar 4 Script Custom HTTP Error

Gambar diatas menjelaskan penambahan *script* untuk memberikan informasi pesan error pada sebuah website sangat penting karena bisa membantu para pengunjung dalam mengetahui apa yang sedang terjadi. Dengan file `.htaccess` kita dapat mengubah halaman *error* pada *server*, dengan mendefinisikan sesuai dengan keinginan kita sendiri.

Change Default Home Page

1. Buka file htaccess yang telah di download menggunakan notepad++



```

1  ##
2  # @package      Joomla
3  # @copyright    Copyright (C) 2005 - 2014 Open Source Matter
4  # @license      GNU General Public License version 2 or late
5  ##
6
7  ##
8  # READ THIS COMPLETELY IF YOU CHOOSE TO USE THIS FILE!
9  #
10 # The line just below this section: 'Options +FollowSymLin
11 # with some server configurations. It is required for use

```

Gambar 5 Editor File Htaccess

2. Ketikkan *script* berikut dalam baris terakhir file htaccess

```

DirectoryIndex mainpage.html
DirectoryIndex mainpage.html index.cgi index.php index.html

```

Gambar 6 Script Change Default Home Page

Kondisi ini menunjukkan bahwa file `.htaccess` dapat digunakan untuk mengubah nama default halaman depan web. Agar user bisa mengakses website kita hanya dengan nama domain saja (`http://www.nama_web.com`) tanpa harus menulis nama file secara jelas (`http://www.nama_web.com/file.html`), kita harus mempunyai file index di root direktori. Nama file yang bisa diterima antara lain `index.html`, `index.htm`, `index.cgi`, `index.php` dll. Pastikan bahwa file tsb bernama `index.*` Ada tingkatan dalam pemberian nama tersebut. Jika kita punya `index.cgi` & `index.html` di *root* direktori maka server akan menampilkan `index.cgi` karena `.cgi` memiliki tingkatan yang lebih tinggi daripada `.html`

Dengan `.htaccess`, kita bisa mendefinisikan file index tambahan atau bisa juga mengubah urutan tingkatannya. Untuk mendefinisikan `mainpage.html` sebagai halaman index, kita dapat menambahkan kode berikut ke file `.htaccess` : `DirectoryIndex mainpage.html`

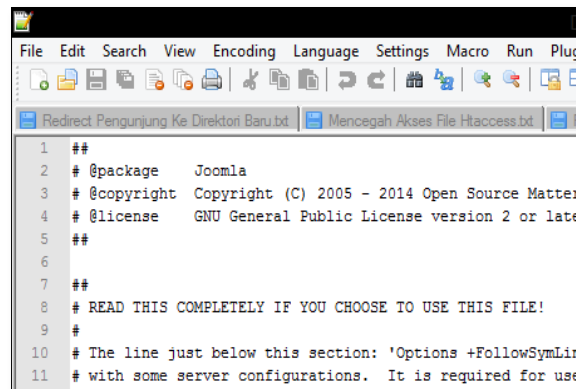
Hal ini akan membuat *server* mencari file bernama `mainpage.html`. Jika *server* menemukannya maka *server* akan menampilkannya. Tapi bila tidak, maka *server* akan menampilkan *error* 404 Missing Page. Untuk mengubah urutan tingkatan, kita dapat memasukkan perintah

DirectoryIndex dengan nama-nama file dalam satu baris. Urutan penulisan file tersebut menentukan urutan tingkatan, contohnya:

DirectoryIndex mainpage.html index.cgi index.php index.html

Block Users From Accessing Your Website

1. Buka file htaccess yang telah di download menggunakan notepad++



Gambar 7 Editor File Htaccess

2. Ketikan *script* berikut dalam baris terakhir file htaccess

```

order deny,allow
deny from 123.456.789.000
deny from 456.78.90.
deny from .bing.com
allow from all
  
```

Gambar 8 Script Block Users From Accessing Your Website

Jika kita menginginkan mem-blok access untuk beberapa user, dimana kita mengetahui IP / domainname yang digunakannya, kita dapat menambahkan kode berikut :

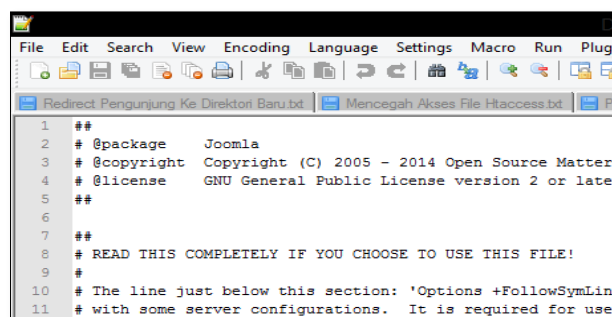
```

order deny,allow
deny from 123.456.789.000
deny from 456.78.90.
deny from .bing.com
allow from all
  
```

Pada contoh di atas, user dg IP 123.456.789.000 akan diblok. Semua user antara 456.78.90.000 sampai 456.78.90.999 akan diblok. Dan semua user yang berasal dari bing.com akan diblok. Jika mereka mencoba mengakses website kita, maka akan tampil error 403 Forbidden ("You do not have permission to access this site")

Redirect Pengunjung Ke Direktori Baru

1. Buka file htaccess yang telah di download menggunakan notepad++



Gambar 9 Editor File Htaccess

2. Ketikan *script* berikut dalam baris terakhir file htaccess

```

Redirect permanent /oldpage.html http://www.mydomain.com/newpage.html
Redirect permanent /olddirectory http://www.mydomain.com/newdirect
  
```

Gambar 10 Script Redirect

Misalkan kita membuat ulang seluruh website kita, me-rename halaman & direktori. Maka pengunjung halaman lama akan mendapat *error 404 File Not Found*. Masalah tersebut dapat diatasi dengan melakukan *redirect* dari halaman lama ke halaman yang baru. Contohnya bila halaman lama kita adalah oldpage.html dan halaman baru adalah newpage.html maka perintahnya adalah:

Redirect permanent /oldpage.html http://www.mydomain.com/newpage.html

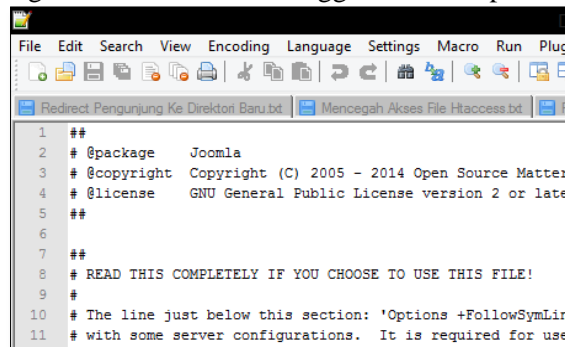
Jika kita me-rename (mengganti nama) direktori, maka perintahnya adalah:

Redirect permanent /olddirectory http://www.mydomain.com/newdirect

Perhatikan bahwa nama direktori yang lama ditulis dengan *relative path*, sementara yang baru ditulis dengan URL *absolut*

Prevent Hot Linking and Bandwidth Leeching

1. Buka file htaccess yang telah di download menggunakan notepad++



Gambar 11 Editor File Htaccess

2. Ketikkan *script* berikut dalam baris terakhir file htaccess

```
RewriteEngine on
RewriteCond %{HTTP_REFERER} !^$
RewriteCond %{HTTP_REFERER} !^http://(www\.)?namadomain.com/.*$ [NC]
RewriteRule \.(gif|jpg)$ - [F]

RewriteEngine on
RewriteCond %{HTTP_REFERER} !^$
RewriteCond %{HTTP_REFERER} !^http://(www\.)?mydomain.com/.*$ [NC]
RewriteRule \.(gif|jpg)$ http://www.mydomain.com/dontsteal.gif [R,L]
```

Gambar 12 Script Hot Linking and Bandwidth Leeching

Untuk mencegah orang lain me-link secara langsung ke direktori image anda dari website mereka, biasanya ada orang mengambil gambar dari website kita, tapi tetap menggunakan link di *server host* kita, ini tentu akan merugikan bagi kita karena dapat mengurangi bandwith di hosting kita, untuk mengatasi hal ini kita dapat menambahkan kode berikut:

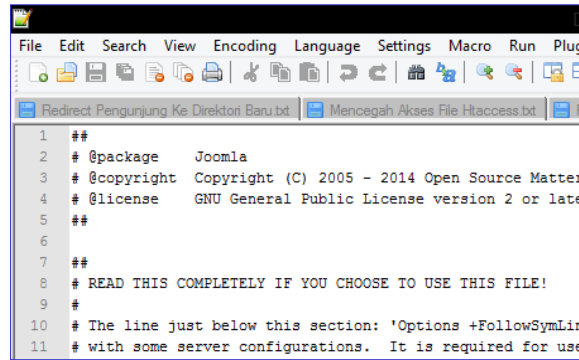
```
RewriteEngine on
RewriteCond %{HTTP_REFERER} !^$
RewriteCond %{HTTP_REFERER} !^http://(www\.)?namadomain.com/.*$ [NC]
RewriteRule \.(gif|jpg)$ - [F]
```

Perintah tersebut akan membuat direktori image hanya bisa diakses bila user sedang mengakses www.namadomain.com Jika kita merasa jengkel, kita bisa membuat sebuah image alternatif bila direktori image di-link oleh orang lain. Contohnya kita membuat image alternatif dengan nama `nogambar.gif` yang bertuliskan: “Gambar dari web lain kunjungi <http://namadomain.com> untuk melihat gambar sebenarnya.” Maka kita dapat menambahkan kode berikut:

```
RewriteEngine on
RewriteCond %{HTTP_REFERER} !^$
RewriteCond %{HTTP_REFERER} !^http://(www\.)?mydomain.com/.*$ [NC]
RewriteRule \.(gif|jpg)$ http://www.mydomain.com/dontsteal.gif [R,L]
```

Mencegah Akses File Htaccess

1. Buka file htaccess yang telah di download menggunakan notepad++



```

1  ##
2  # @package    Joomla
3  # @copyright  Copyright (C) 2005 - 2014 Open Source Matter
4  # @license    GNU General Public License version 2 or late
5  ##
6
7  ##
8  # READ THIS COMPLETELY IF YOU CHOOSE TO USE THIS FILE!
9  #
10 # The line just below this section: 'Options +FollowSymLin
11 # with some server configurations. It is required for use

```

Gambar 13 Editor File Htaccess

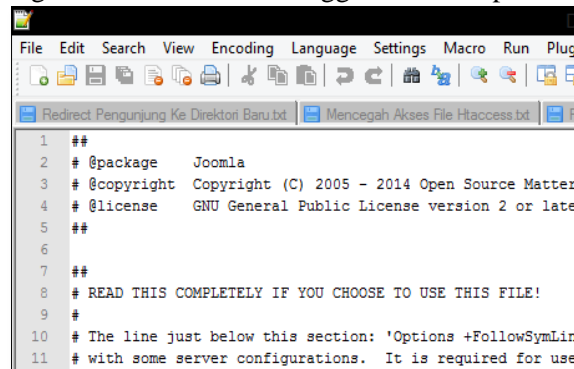
2. Ketikkan *script* berikut dalam baris terakhir file htaccess

```
order allow,deny
deny from all
```

Gambar 14 Script Mencegah Akses File Htaccess

Rewriting URLs

1. Buka file htaccess yang telah di download menggunakan notepad++



```

1  ##
2  # @package    Joomla
3  # @copyright  Copyright (C) 2005 - 2014 Open Source Matter
4  # @license    GNU General Public License version 2 or late
5  ##
6
7  ##
8  # READ THIS COMPLETELY IF YOU CHOOSE TO USE THIS FILE!
9  #
10 # The line just below this section: 'Options +FollowSymLin
11 # with some server configurations. It is required for use

```

Gambar 15 Editor File Htaccess

2. Ketikkan *script* berikut dalam baris terakhir file htaccess

```
RewriteEngine On
RewriteBase /
RewriteCond %{REQUEST_FILENAME} !-f
RewriteCond %{REQUEST_FILENAME} !-d
RewriteRule . /index.php [L]
```

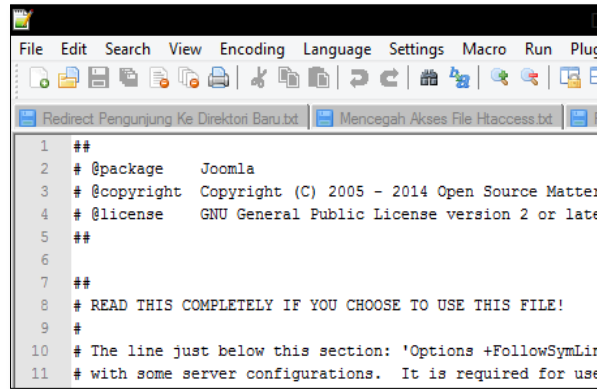
Gambar 16 Script Rewriting URLs

Agar kita dapat melakukan pengaturan pada permalink kita agar lebih SEO friendly kita dapat menambahkan kode berikut ini:

```
RewriteEngine On
RewriteBase /
RewriteCond %{REQUEST_FILENAME} !-f
RewriteCond %{REQUEST_FILENAME} !-d
RewriteRule . /index.php [L]
```

MIME Types

1. Buka file htaccess yang telah di download menggunakan notepad++



```

1  ##
2  # @package Joomla
3  # @copyright Copyright (C) 2005 - 2014 Open Source Matter
4  # @license GNU General Public License version 2 or late
5  ##
6
7  ##
8  # READ THIS COMPLETELY IF YOU CHOOSE TO USE THIS FILE!
9  #
10 # The line just below this section: 'Options +FollowSymLin
11 # with some server configurations. It is required for use

```

Gambar 17 Editor File.Htaccess

2. Ketikkan *script* berikut dalam baris terakhir file htaccess

```
AddType application/octet-stream .doc .xls .pdf
```

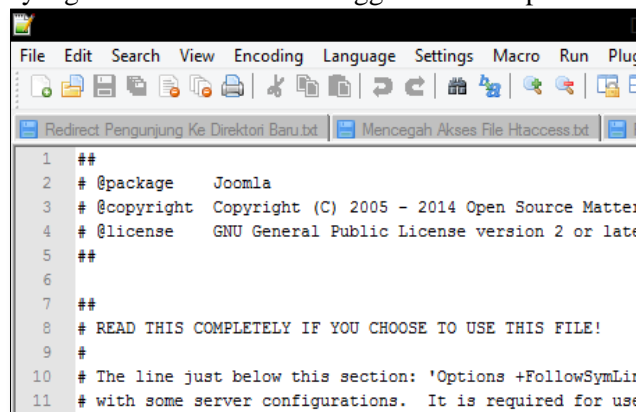
Gambar 18 Script Rewriting URLs

Memerintah server untuk mengenali jenis file-file yang belum didaftarkan dalam sistem server. Contohnya :

```
AddType application/octet-stream .doc .xls .pdf
```

Cache Control

1. Buka file htaccess yang telah di download menggunakan notepad++



```

1  ##
2  # @package Joomla
3  # @copyright Copyright (C) 2005 - 2014 Open Source Matter
4  # @license GNU General Public License version 2 or late
5  ##
6
7  ##
8  # READ THIS COMPLETELY IF YOU CHOOSE TO USE THIS FILE!
9  #
10 # The line just below this section: 'Options +FollowSymLin
11 # with some server configurations. It is required for use

```

Gambar 19 Editor File Htaccess

2. Ketikkan *script* berikut dalam baris terakhir file htaccess

```
# 480 weeks
Header set Cache-Control "max-age=290304000, public"
# 2 DAYS
Header set Cache-Control "max-age=172800, public, must-revalidate"
# 2 HOURS
Header set Cache-Control "max-age=7200, must-revalidate"
```

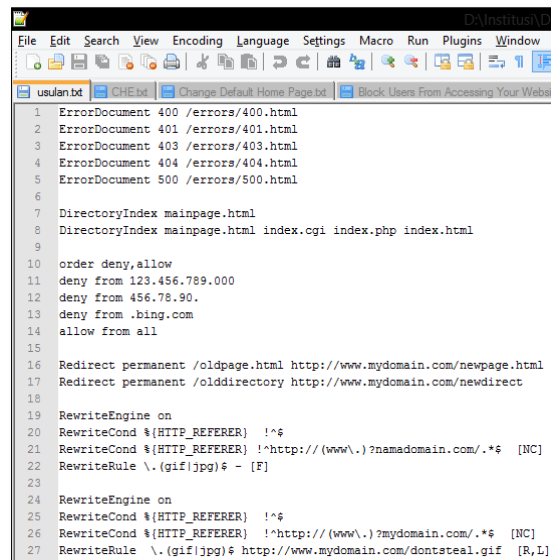
Gambar 20 Script Cache Control

File .htaccess bisa mengendalikan caching pada web browser sehingga dapat mengurangi penggunaan bandwidth atau aktivitas yang ada didalam server. Contohnya:

```
# 480 weeks
Header set Cache-Control "max-age=290304000, public"
# 2 DAYS
Header set Cache-Control "max-age=172800, public, must-revalidate"
# 2 HOURS
Header set Cache-Control "max-age=7200, must-revalidate"
```

Save File Htaccess

1. Save as file htaccess yang telah di edit menggunakan editor notepad ++



```

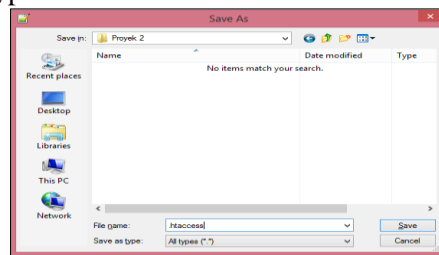
1 ErrorDocument 400 /errors/400.html
2 ErrorDocument 401 /errors/401.html
3 ErrorDocument 403 /errors/403.html
4 ErrorDocument 404 /errors/404.html
5 ErrorDocument 500 /errors/500.html
6
7 DirectoryIndex mainpage.html
8 DirectoryIndex mainpage.html index.cgi index.php index.html
9
10 order deny,allow
11 deny from 123.456.789.000
12 deny from 456.78.90.
13 deny from .bing.com
14 allow from all
15
16 Redirect permanent /oldpage.html http://www.mydomain.com/newpage.html
17 Redirect permanent /olddirectory http://www.mydomain.com/newdirect
18
19 RewriteEngine on
20 RewriteCond %{HTTP_REFERER} !^$
21 RewriteCond %{HTTP_REFERER} !^http://(www\.)?namadomain.com/*$ [NC]
22 RewriteRule \.(gif|jpg)$ - [F]
23
24 RewriteEngine on
25 RewriteCond %{HTTP_REFERER} !^$
26 RewriteCond %{HTTP_REFERER} !^http://(www\.)?mydomain.com/*$ [NC]
27 RewriteRule \.(gif|jpg)$ http://www.mydomain.com/dontsteal.gif [R,L]

```

Gambar 20 Editor File Htaccess

2. Isikan

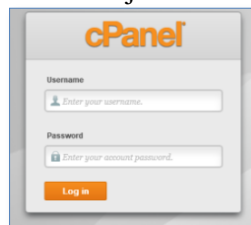
File Name : .htaccess
 Save As Type : All Types



Gambar 21 Save As File .htaccess

Upload File .htaccess

1. Lakukan login ke *cpanel hosting* website objek.

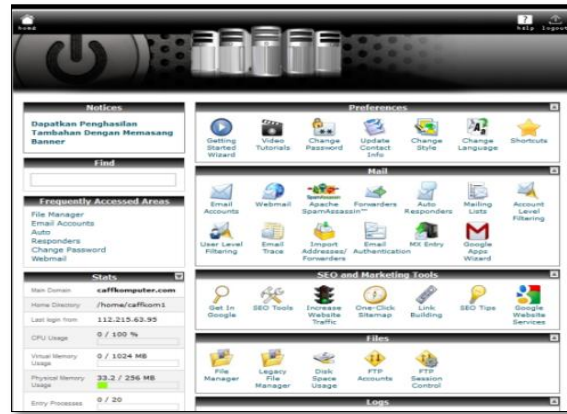


Gambar 22 Login Cpanel

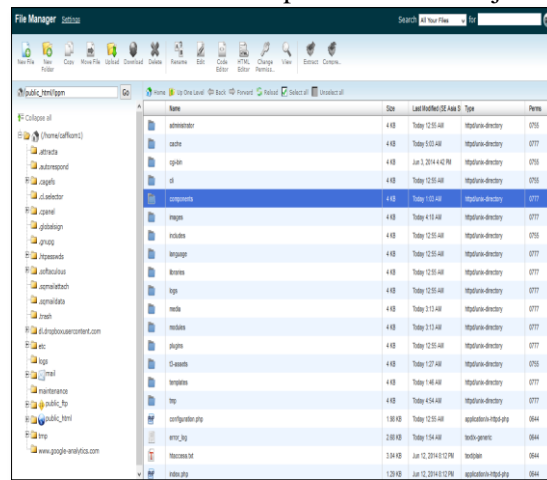
2. Masukan username dan password

Username : riko
 Password : teknikinformatika12

3. Setelah sukses login dan masuk ke *cpanel*, masuk ke menu *file manager* untuk melihat direktori website objek

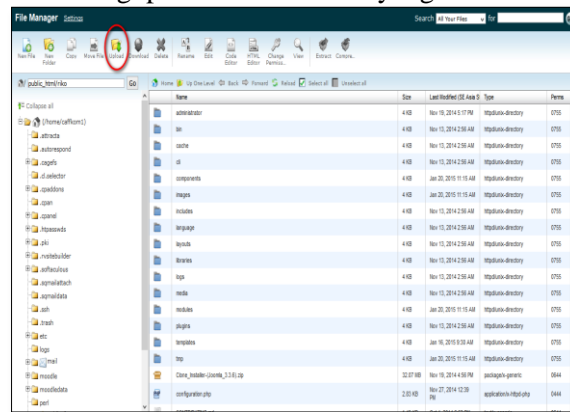


Gambar 23 Home Cpanel Website Objek



Gambar 24 File Manager Website Objek

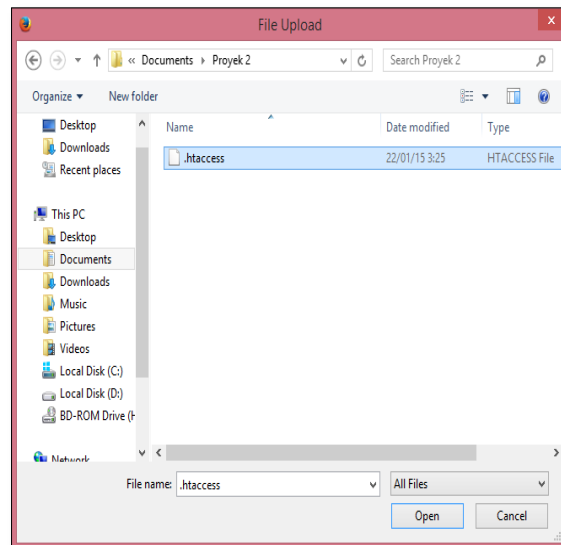
4. Pilih menu upload untuk mengupload file .htaccess yang telah diedit.



Gambar 25 Proses 1 Upload File .htaccess



Gambar 26 Proses 2 Upload File .htaccess

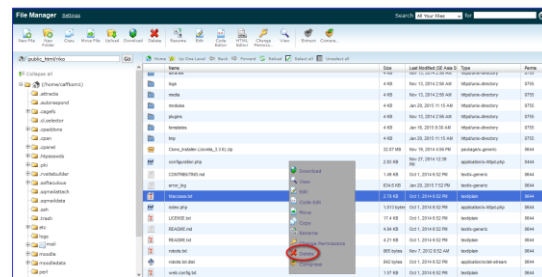


Gambar 27 Proses 1 Upload File .htaccess



Gambar 28 Upload File .htaccess Selesai

5. Lalu hapus file Htaccess



Gambar 29 File Htaccess di Hapus

4.KESIMPULAN DAN SARAN

4.1. Simpulan

Sistem keamanan website yang dibangun menggunakan file.htaccess dapat melindungi website dari pencurian informasi dan dari serangan cracker yang sering terjadi pada saat ini.

4.2. Saran

Dalam pengaman website menggunakan file .htaccess ini masih banyak kekurangan. Oleh sebab itu penulis mengharapkan untuk kedepannya dapat dikembangkan lebih baik lagi agar bisa menjadi sistem keamanan yang sempurna.

DAFTAR PUSTAKA

- [1]. Slamet Riyanto. 2014. Web Dinamis dengan PHP dan MySQL. Penerbit Selamat Riyanto
- [2]. Tim EMS. 2011. Proyek Membuat Website dengan Joomla. Jakarta: Penerbit PT. Elex Media Komputindo.
- [3]. Sugiri, 2012. Desain Web menggunakan HTML + CSS. Jogjakarta: Penerbit Andi Offset Jogjakarta.
- [4]. Th0R. 2008. Hacker's Biggest Secret Zero-knowledge Password. Jakarta: Penerbit PT. Elex Media Komputindo.
- [5]. Fritz Gamaliel. 2014. Super Web Programming 10 Bahasa 10 Proyek Web. Yogyakarta: Penerbit Loko Medi
- [6]. Jamie Cameron. 2004. Managing Linux Systems with Webmin System Administration and Module Development. Penerbit Prentice Hall Professional