

PRAKTIKUM 10

Konfigurasi Keamanan Layanan Web (Secure Access)

A. TUJUAN PEMBELAJARAN

- Mengenalkan konsep .htaccess
- Melengkapi direktori dari layanan web dengan hak akses
- Melakukan redirect
- Melakukan blok terhadap alamat IP tertentu
- Mencegah hot linking dan bandwidth leeching

B. DASAR TEORI

Apache Web server memiliki beragam opsi konfigurasi bagi administrator. Masalahnya, pada saat anda hosting, anda tidak memiliki akses pada konfigurasi apache. Akibatnya anda tidak dapat melakukan perubahan setting dan terpaksa menggunakan konfigurasi default. Salah satu alternative yang dapat dilakukan untuk melakukan *overriding* konfigurasi default adalah dengan melakukan setting lewat file .htaccess.

File .htaccess berupa file ascii yang ditempatkan pada direktori www atau subdirektori www. Anda dapat membuat file ini lewat editor teks seperti notepad dan diupload dalam bentuk ASCII (bukan BINARY) di direktori mana yang anda ingin memodifikasi setting. Selain itu, hak akses file diset sebagai 644 (rw-r--r--). Fungsinya adalah memungkinkan server mengakses file, namun mencegah pengunjung untuk mengakses file lewat browser mereka karena alasan keamanan.

Perintah pada file .htaccess akan mempengaruhi semua direktori dan subdirektori dimana file tersebut diletakkan. Jika anda meletakkannya di sub direktori dari direktori www, maka file htaccess akan mempengaruhi direktori www dan semua direktori dibawahnya. Yang perlu

diperhatikan adalah semua perintah pada file .htaccess bersifat case sensitive dan didesain untuk diletakkan pada satu baris.

Beberapa fitur file .htaccess

1. Untuk memberikan pesan error

Jika anda ingin melakukan overriding pesan error dari server, anda dapat menggunakan .htaccess untuk mng-kustomisasi pesan error yang baru. Contoh konfigurasinya :

```
ErrorDocument 500 /error.html  
Override SSI Settings
```

2. Melakukan overriding setting SSI

Secara default, hanya halaman web yang memiliki ekstensi .shtml yang akan melakukan parsing server-side includes (SSI). Anda dapat melakukan overriding konfigurasi default ini agar SSI dapat bekerja dengan file .html dan .htm dengan menambahkan baris ini pada .htaccess. Contoh:

```
AddType text/html .html  
AddHandler server-parsed .html  
AddHandler server-parsed .htm
```

3. Mengganti file index.* pada homepage

Anda bisa mengganti halaman pertama web page anda yang biasanya berawal dengan index.html, index.cgi, index.shtml, dan lainnya dengan namafileku.html. Perhatikan bahwa, biasanya file pertama yang digunakan semua memiliki awal index.*. Selain itu juga, secara default, server akan mendisplay file index.* berdasarkan prioritasnya. Artinya file index.cgi memiliki keutamaan untuk ditampilkan disbanding index.html.

Misalkan anda ingin mengganti file index.* dengan nama file: filebaru.html, tambahkan baris berikut pada file .htaccess :

```
DirectoryIndex hieronymous.html
```

Jika server tidak menemukan file dengan nama filebaru.html, server akan mengeluarkan halaman pesan error: 404 Missing Page. Untuk mengubah prioritas file yang ditampilkan, anda dapat melakukan hal dibawah, dimana orde prioritas ditentukan dari yang sebelah kiri (paling tinggi) hingga paling kanan (terendah).

DirectoryIndex hieronymous.html index.cgi index.php index.html

4. Memungkinkan browsing direktori

Karena alasan sekuritas, user dilarang untuk melihat isi direktori atau disebut fasilitas directory indexing. Dengan menggunakan file .htaccess, anda dapat mengijinkan user untuk melihat index direktori web page anda. Contoh, misalnya anda memanggil <http://www.domainku.com/gambar/>, maka web server akan melisting semua file pada direktori /gambar, tanpa perlu membuat file html dengan linknya. Tinggal tambahkan baris ini pada file .htaccess untuk melakukan indexing directory.

Options +Indexes

5. Mengeblok user untuk mengakses web site

Jika anda ingin mencegah akses website pada user tertentu, asalkan anda tahu IP address atau domain name yang digunakan oleh user tersebut, anda dapat menggunakan file .htaccess untuk mengeblok user tersebut dari mengakses website anda.

```
<Limit GET>
```

```
order deny,allow
```

```
deny from 10.252.44.210
```

```
deny from 10.252.32.
```

```
deny from .domainku.com
```

```
allow from all
```

```
</Limit>
```

Pada contoh diatas, user dari nomor IP 10.252.44.210 akan di blok. Semua user dari network 10.252.32.000 s.d 10.252.32.255 akan diblok. Semua user dari domain domainku.com akan diblok. Ketika mereka mencoba mengakses website anda, mereka akan menerima pesan error 403 Forbidden ("You do not have permission to access this site")

6. Redireksi pengunjung ke halaman web baru atau direktori

Bila anda mengubah seluruh isi web site anda, memberikan nama baru bagi halaman dan direktori. Pengunjung pada halaman web lama akan menerima kode error 404, File Not Found. Anda dapat mengatasi masalah ini dengan melakukan redireksi panggilan ke halaman lama ke halaman baru. Contoh: jika halaman web lama anda adalah `../lama.html` dan anda ingin menggantinya dengan `baru.html` pada website yang lain, maka anda dapat menambahkan baris ini pada file `.htaccess`

```
Redirect permanent /lama.html http://www.domainbaru.com/baru.html
```

Dengan penambahan ini, pengunjung yang mengakses website lama pada halaman *lama.html* akan dikirim menuju website baru pada halaman *baru.html*. Selain redireksi file, anda juga bisa melakukan redireksi untuk seluruh isi direktori. Contoh: bila anda hendak meredireksi pengunjung pada seluruh directory website lama ke direktori website baru. Tambahkan baris ini pada `htaccess`.

```
Redirect permanent /direktori-lama http://www.domainbaru.com/direktori-baru/
```

Ada beberapa tipe redireksi :

- permanent – halaman web dipindah secara permanen (kode status: 301)
- temp – halaman web dipindah secara temporer (kode status: 302)
- seeother - halaman web diganti (kode status : 303)
- gone - halaman web telah dihapus secara permanen (kode status : 410)

7. Mencegah hot linking dan bandwidth leeching

Hotlinking adalah tindakan mencuri image dan bandwidth dengan melink-an image file yang dimiliki oleh suatu web server dengan web server lain secara ilegal. Hal ini dapat dicegah dengan menambahkan baris dibawah pada file `.htaccess`

Dengan cara ini, image anda hanya akan terdisplay ketika pengunjung benar-benar mengunjungi site anda. Semua image yang dilinking dengan domain lain akan nampak sebagai *broken image*.

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

Anda bahkan bisa menambahkan image lain sebagai ganti pada halaman yg terlink—dengan image yang menyindir pencurian gambar tersebut. Tambahkan baris ini untuk melakukan hal tersebut :

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

8. Mencegah pengunjung melihat file.htaccess atau file lain

Untuk mencegah pengunjung untuk melihat isi dari file .htaccess, tambahkan baris ini pada file .htaccess

```
<Files .htaccess>
    order allow,deny
    deny from all
</Files>
```

C. TUGAS PENDAHULUAN

1. Sebutkan fungsi file htaccess ? Apa hak akses .htaccess? Dimana file htaccess disimpan?
2. Apa keuntungan dan kerugian menggunakan file .htaccess ?
3. Apa yang disebut hot linking dan bandwidth leeching. Bagaimana mencegah hot linking dan bandwidth leeching ?
4. Bagaimana mencegah user dg nomor IP tertentu mengakses homepage?
5. Bagaimana caranya melakukan redireksi ?

D. PERCOBAAN

1. Melakukan virtual hosting

Pada percobaan ini, anda akan membuat dua buah website yang dihosting secara lokal di computer anda. Siapkan nama dua buah website tersebut, dan persiapkan pula halaman web untuk kedua web site tersebut. Jika halaman-halaman web tersebut telah siap, lakukan virtual hosting dengan cara dibawah.

1. Dibawah ini adalah langkah-langkah virtual hosting. Misalkan anda ingin membuat website dengan nama www.jualku.net . Sebelumnya lakukan disable terlebih dahulu terhadap website default dari apache dengan

```
$ sudo a2dissite default
```

2. Setelah ini, anda dapat mulai melakukan virtual hosting. Langkah pertama adalah menkopikan setting file default ke file website anda www.jualku.net. Ini adalah file konfigurasi apache untuk virtual hosting. Anda perlu menyetting komponen-komponen penting seperti nama website, dimana letak file html dan lain-lain

```
$ cd /etc/apache2/sites-available/
```

```
$ cp default www.jualku.net
```

3. Edit file www.webku.com dengan gedit atau pico

```
$ sudo gedit etc/apache2/sites-available/www.jualku.net
```

4. Setelah file www.jualku.net sudah terbuka.

- a. Hapus bagian AccessFileName .htaccess.
- b. Tambahkan server name dibawah baris ServerAdmin

```
ServerName www.jualku.net:80
```

5. Pada file yang sama. Ubah DocumentRoot untuk menunjuk ke web direktori dari website webku. Inilah tempat anda menyimpan halaman-halaman web anda

```
DocumentRoot /var/www/jualku
```

6. Ubah <Directory /var/www/> untuk menunjuk ke direktori jualanku

```
<Directory /var/www/jualku>
```

7. Simpan file www.jualanku.net

8. Kopi web page yang telah anda persiapkan atau web page default apache, ke direktori /var/www/jualku/ sampai semua terkopi

```
$ sudo cp /var/www/index.html /var/www/jualku/index.html
```

9. Enable-kan website www.jualku.net dengan :

```
$ sudo a2ensite www.jualku.net
```

10. Edit file /etc/hosts untuk melakukan resolusi domain www.jualku.net ke 127.0.0.1. Cari baris 127.0.0.1 , lalu tambahkan baris ini :

```
127.0.0.1 localhost
```

```
127.0.0.1 www.jualku.net.localdomain www.jualku.net
```

11. Restart web server :

```
$ sudo /etc/init.d/apache2 reload
```

```
$ sudo /etc/init.d/apache2 restart
```

12. Bukalah browser www.jualku.net. Jika berhasil, berarti virtual host anda berhasil. Selamat



13. Dengan cara yang sama, cobalah buat website www.tokobaru.com pada computer yang sama

2. Redireksi pengunjung ke halaman web baru atau direktori

Contoh kasus :

Anda mengelola website yang berisi penjualan devais jaringan, pada www.jualku.net. Setahun kemudian, anda berhasil membeli domain domain baru dengan nama www.tokobaru.com yang memiliki space lebih besar. Anda berniat memindah website www.jualku.net ke website baru, www.tokobaru.com. Anda tidak ingin kehilangan pelanggan yang biasa mengakses www.jualku.net, karena itu anda berniat melakukan redireksi dari site lama ke site baru.

1. Kita akan melakukan redireksi dari website lama (www.jualku.net) ke website baru (www.tokobaru.com). Sebelumnya cek lagi apakah virtual hosting anda telah berhasil dengan membuka browser di komputer anda

2. Edit file /etc/apache2/sites-available/www.jualku.net. Pada bagian ini :

```
<Directory /var/www/jualku>
```

```
Options Indexes FollowSymLinks MultiViews
```

```
AllowOverride None
```

```
Order allow,deny
```

```
allow from all
```

```
</Directory>
```

Gantilah AllowOverride None menjadi AllowOverride All:

3. Tambahkan baris ini pada /etc/apache2/apache.conf bila belum ada.

AccessFileName .htaccess

4. Buat file .htaccess pada directory root website www.jualku.net

\$ sudo pico /var/www/jualku/.htaccess

Kopikan baris dibawah pada file .htaccess

```
<IfPRAKTIKUMe mod_rewrite.c>
```

```
RewriteCond %{HTTP_HOST} ^www.jualku.net$
```

```
RewriteRule (.*)$ http://www.tokobaru.com/$1 [R=301,L]
```

```
</IfPRAKTIKUMe>
```

Simpan file .htaccess

5. Enablekan PRAKTIKUM rewrite.

\$ sudo a2enmod rewrite

6. Reload dan restart apache web server

\$ sudo /etc/init.d/apache2 reload

\$ sudo /etc/init.d/apache2 restart

7. Pada Firefox, sebelumnya bersihkan dulu cachanya dengan. Buka Tools -> Clear Recent History. Kemudian buka browser firefox. Arahkan ke www.jualku.net. Apa yang terjadi ?

8. Bila redireksi anda berhasil maka begitu website www.jualku.net akan langsung diredireksi ke www.tokobaru.com.

9. Tolong jelaskan syntax dari file .htaccess sebagai bagian dari laporan

3. Penggunaan file .htaccess untuk mengeblok IP tertentu

Contoh kasus:

Anda mengelola website www.jualku.net. Bekerjasamalah dengan beberapa teman anda untuk lab ini. Catat nomor IP teman anda. Siapkan no IP yang akan ditolak dan diperbolehkan. Kemudian lakukan langkah berikut :

1. Tambahkan baris berikut pada file /etc/apache2/sites-available/www.jualku.net

```
<Directory /var/www/jualku >
```

```
Options Indexes FollowSymLinks MultiViews
```

```
AllowOverride All
```

```
Order allow,deny
```

```
Allow from All
```

```
</Directory>
```

2. Coba edit /var/www/jualku/.htaccess

```
$ sudo pico /var/www/jualku/.htaccess
```

3. Misalkan nomor IP teman anda 10.0.1.5 dan 10.0.1.6. Kita mengizinkan beberapa nomor IP untuk mengakses website anda dan menolak nomor IP yang lain. Tambahkan baris ini pada /var/www/jualku/.htaccess.

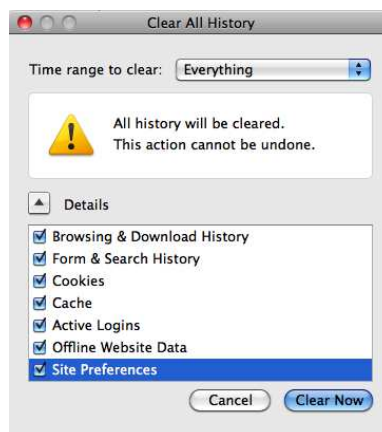
```
<IfPRAKTIKUMe mod_rewrite.c>
RewriteEngine On
Order Deny,Allow
Deny from All
Allow from 10.0.1.5 10.0.1.6
</IfPRAKTIKUMe>
```

4. Restart apache2

```
$ sudo /etc/init.d/apache2 reload
```

```
$ sudo /etc/init.d/apache2 restart
```

5. Jangan lupa untuk mengosongkan history sebelum mengarahkan browser ke halaman web. Gunanya agar browser tidak merujuk ke cache file sebelumnya. Pada menu utama, pilih Tools -> Clear Recent History untuk Firefox. Pilih Everything pada Time Range to Clear. Klik seluruh opsi yang ada yaitu Browsing&Download History, Cookies, dll. Klik Clear Now untuk membersihkan history.



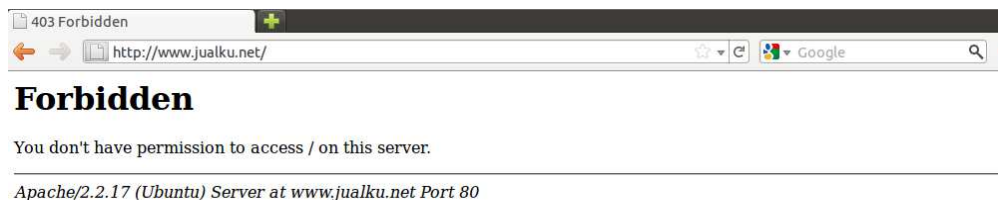
Gambar 11.1 Mengosongkan history browser Firefox.

6. Minta teman anda membuka browser dan mengarahkan ke www.jualku.net. Apakah berhasil ? Catatlah no IP yang berhasil membuka website anda dan yang gagal. Apakah sesuai dengan konfigurasi anda di file .htaccess ? Capture juga screenshotnya untuk yang gagal.

7. Cobalah untuk mendeny beberapa no IP dan meng-allow yang lain dengan mengganti file .htaccess sebagai berikut

```
<IfPRAKTIKUMe mod_rewrite.c>
RewriteEngine On
Order Deny,Allow
Allow from 10.0.1.4
Deny from 10.0.1.5 10.0.1.6
</IfPRAKTIKUMe>
```

8. Bersihkan history dengan langkah 5. Ini penting karena mungkin browser akan mengakses cache yang ada dibanding melakukan proses three way handshake dari awal. Lakukan langkah no 5 sekali lagi.



Gambar 11.2 Hasil mengeblok no IP tertentu dengan htaccess

4. Mencegah hot linking dan bandwidth leeching

Contoh kasus :

Anda mengelola web site www.jualku.net. Setelah beberapa minggu, anda mengamati bahwa trafik yang masuk ke website anda lebih besar dari jumlah user yang benar-benar mengakses website anda. Anda berpikir bahwa beberapa website melakukan hot linking dengan website anda. Anda harus mencegah hal ini dengan file htaccess.

1. Gunakan dua buah virtual host yang sudah anda buat. Misalnya www.jualku.net dan www.tokobaru.com. Website www.tokobaru.com akan melakukan hotlinking image www.jualku.net. Caranya,

- a. Buka file index.html dari www.tokobaru.com :

```
$sudo pico /var/www/tokobaru/index.html
```

- b. Serta tambahkan link berikut ke index.html. Gambar yang akan dihot-linking pada kasus ini berada pada folder /var/www/jualku/gambar/. Sesuaikan bila anda menyimpannya di tempat lain.

```

```

- c. Bukalah browser dan arahkan URL ke www.tokobaru.com di komputer lokal. Berhasilkah?
- d. Mintalah teman anda membuka browser dan arahkan URL ke www.tokobaru.com di komputer lokal. Berhasilkah? Perhatikan jangan lupa pastikan bahwa file etc/hosts teman anda sudah menyimpan entry untuk www.tokobaru.com dan www.jualku.net
2. Untuk mencegah hotlinking, buka file .htaccess di /var/www/jualku dan tambahkan baris berikut:

```
<IfPRAKTIKUMe mod_rewrite.c>
RewriteEngine On
RewriteCond %{HTTP_REFERER} !^http://(www\.)?jualku\.net [NC]
RewriteCond %{HTTP_REFERER} !^$
RewriteCond %{HTTP_REFERER} ^http://.*$
RewriteRule \.(gif|jpg|jpeg|png)$ - [F,L]
</IfPRAKTIKUMe>
```

3. Mengetes htaccess. Bukalah browser. Ketikkan url www.tokobaru.com dan lihat apa yang terjadi. Berhasilkah upaya anda mencegah hotlinking ? Simpan screenshotnya.
4. Selamat, anda telah menyelesaikan lab ☺

5. Menggunakan .htaccess untuk mengatur hak akses dari user

Contoh kasus: Anda pengelola website www.userweb.net, ada konten website pada rirektory /docs anda yang ingin anda lindungi dari ilegal user. Untuk itu anda perlu menetapkan otentikasi.

1. Konfigurasi pada apache server.
- a. Ganti dari AllowOverride none / all menjadi AuthConfig.
- \$ sudo pico /var/www/www.jualku2.net
- b. Lihat baris ini :

```
<Directory /var/www/jualku>
Options Indexes Includes FollowSymLinks MultiViews
AllowOverride AuthConfig
```

```
Order allow,deny
Allow from all
</Directory>
```

- c. Simpan konfigurasi ini dengan ctrl o. Dan keluarlah dengan ctrl x.
- d. Lakukan restart apache2

```
$ sudo /etc/init.d/apache2 reload
```

```
$ sudo /etc/init.d/apache2 restart
```

2. Buat file password dengan htpasswd tersebut. Perintah htpasswd digunakan untuk membuat text file untuk menyimpan username dan password untuk otentikasi dasar pemakai Apache.

Sintaks umum yang digunakan adalah

```
htpasswd -c <password-file> <username>
```

dimana,

- -c : digunakan untuk membuat file password. Jika file password sudah ada, maka file tersebut akan ditulis ulang. Karena itu -c digunakan bila user hanya satu. Untuk user ke dua,tiga,dst, opsi -c dihilangkan.
 - <username> : digunakan untuk membuat user name. Jika username tidak ada, maka akan dibuat baris baru berisi username tersebut. Jika username telah ada, maka passwordnya akan diganti
- a. Untuk itu, langkah pertama adalah membuat direktori dimana file password ini disimpan. Tujuannya agar hanya apache yang mampu mengakses file password tersebut. File password ini harus diletakkan di directory yang tidak dapat diakses dari web, Tujuannya agar pengunjung tidak dapat mendownload file password tersebut.

```
# mkdir -p /home/secure/
```

- b. Tambahkan user pertama , misal andri :

```
# htpasswd -c /home/secure/passwordku andri
```

- c. Tambahkan user-user berikutnya, missal shinta dan duhita

```
# htpasswd /home/secure/passwordku shinta
```

```
# htpasswd /home/secure/passwordku duhita
```

- d. Coba cek di file /home/secure/passwordku hasil pembuatan passwords anda

3. Pastikan file `/home/secure/passwordku` hanya dapat dibaca oleh apache web server. Jika apache tidak dapat membaca file ini, maka apache tidak akan dapat mengotentikasi anda. Untuk itu anda perlu mengeset permisi dengan perintah `chown`.

a. Sebelumnya, cek dulu user apache di linux anda. Letaknya di `/etc/apache/envvars`.

Envvars adalah default environment variable untuk apache2. Cari baris :

```
export APACHE_RUN_USER=  
export APACHE_RUN_GROUP=
```

b. Cek sisi sebelah kanan tanda `=`. Inilah user dan grup apache. Pada Ubuntu 10, user dan grup apache adalah `www-data`.

c. Sekarang set ownership file `/home/secure/passwordku` agar menjadi milik user dan grup: `www-data`

```
# chown www-data:www-data /home/secure/passwordku  
# chmod 0660 /home/secure/passwordku
```

4. Misalkan direktori yang ingin anda beri password user adalah `/var/www/userweb/docs`

Buatlah direktori pada `/var/www/docs` jika belum ada

```
# mkdir -p /var/www/userweb/docs
```

5. a. Buat file `.htaccess` dengan text editor:

```
# cd /var/www/userweb/docs  
# pico .htaccess
```

b. Ketikkan baris dibawah ini:

```
AuthType Basic  
AuthName "Restricted Files"  
AuthBasicProvider file  
AuthUserFile /home/secure/passwordku  
Require valid-user
```

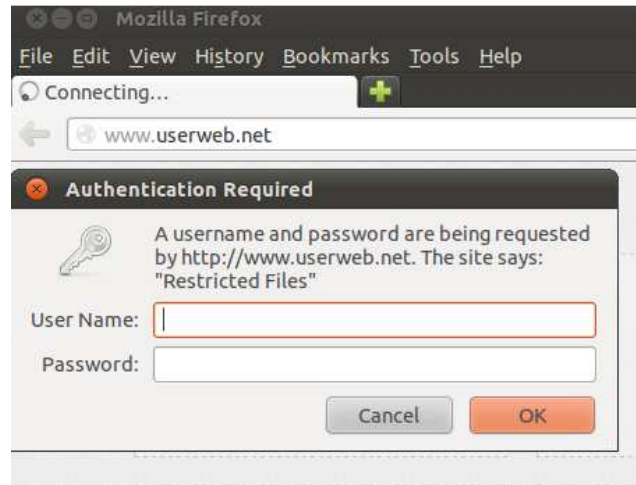
c. Simpan file dan keluarlah dari shell prompt

6. Test konfigurasi anda.

a. Bukalah browser anda. Ketik `http://www.userweb.net`. Tidak otentikasi pada halaman ini

b. Buka `http://www.userweb.net/docs`. Akan nampak lembar otentikasi sebagai berikut.

Capture hasilnya sebagai bagian dari laporan.



Gambar 11.3 Otentikasi saat browser diarahkan ke www.userweb.net/docs

- c. Masukkan user name andri dan password. Jika berhasil. Capture hasilnya
- d. Jika anda gagal dan muncul halaman error 401 yang menyatakan otentikasi salah. coba anda update lagi perintah htpasswd di langkah 2. Kemudian masukkan lagi username dan passwordnya.
- e. Setelah anda berhasil login, bersihkan dulu cache browser seperti pada percobaan sebelumnya dan coba masuk lagi dengan password yang berbeda (yang salah). Capture hasilnya.
- f. Untuk melakukan troubleshooting, lihatlah log file, baik access.log dan error.log, lihatlah

```
#tail -f file /var/log/apache2/access.log
#tail -f file /var/log/apache2/error.log
```

Apa yang anda lihat pada file log ketika user salah memasukkan password pada kedua log tersebut? Capture dan terangkan jawaban anda.



Gambar 11.4 Penolakan otorisasi (Error 401)

Daftar Pustaka

1. Apache 301 redirect – How to create htaccess redirect, <http://linuxreference.wordpress.com>
2. Apache PRAKTIKUMe mod_rewrite, http://httpd.apache.org/docs/2.2/en/mod/mod_rewrite.html