

## FUNDAMENTOS DE SEGURIDAD

(Práctica Footprinting)

María Delia Sánchez Carmona

deliaschz@gmail.com

Footprinting es el primer paso para obtener información sobre una organización la información puede ser pública o privada y muchas veces se tiene acceso a la información privada por una mala configuración.

El sitio seleccionado para esta práctica es: [www.partidodeltrabajo.org.mx/](http://www.partidodeltrabajo.org.mx/), perteneciente al partido del trabajo. Los pasos que se siguieron fueron los siguientes:

1. Se obtuvo información sobre fecha de creación, última actualización, datos de contacto administrativo, etc., a través de whois.net.

Domain Name: partidodeltrabajo.org.mx

Created On: 2005-01-12

Expiration Date: 2016-01-11

Last Updated On: 2015-01-20

Registrar: Akky (Una division de NIC Mexico)

URL: <http://www.akky.mx>

Whois TCP URI: [whois.akky.mx](http://whois.akky.mx)

Whois Web URL: <http://www.akky.mx/jsf/whois/whois.jsf>

Registrant:

Name: PARTIDO DEL TRABAJO

City: Mexico

State: Distrito Federal

Country: Mexico

Administrative Contact:

Name: Javier Marquez Garcia

City: Mexico

State: Distrito Federal

Country: Mexico

Technical Contact:

Name: Javier Marquez Garcia

City: Mexico

State: Distrito Federal

Country: Mexico

Billing Contact:

Name: Javier Marquez Garcia

City: Mexico

State: Distrito Federal

Country: Mexico

Name Servers:

DNS: ns1.sedetechosting.com

DNS: ns2.sedetechosting.com

DNSSEC DS Records:

## 2. Se comprobó si el sitio era vulnerable a inyección sql

Al responder una encuesta que esta en el sitio de forma errónea se muestra el siguiente mensaje que brinda información suficiente para detectar que es vulnerable a inyección de código sql.

**Warning:** mysql\_fetch\_assoc(): supplied argument is not a valid MySQL result resource in /home/partidod/public\_html/2011/enq/vota.php on line 11

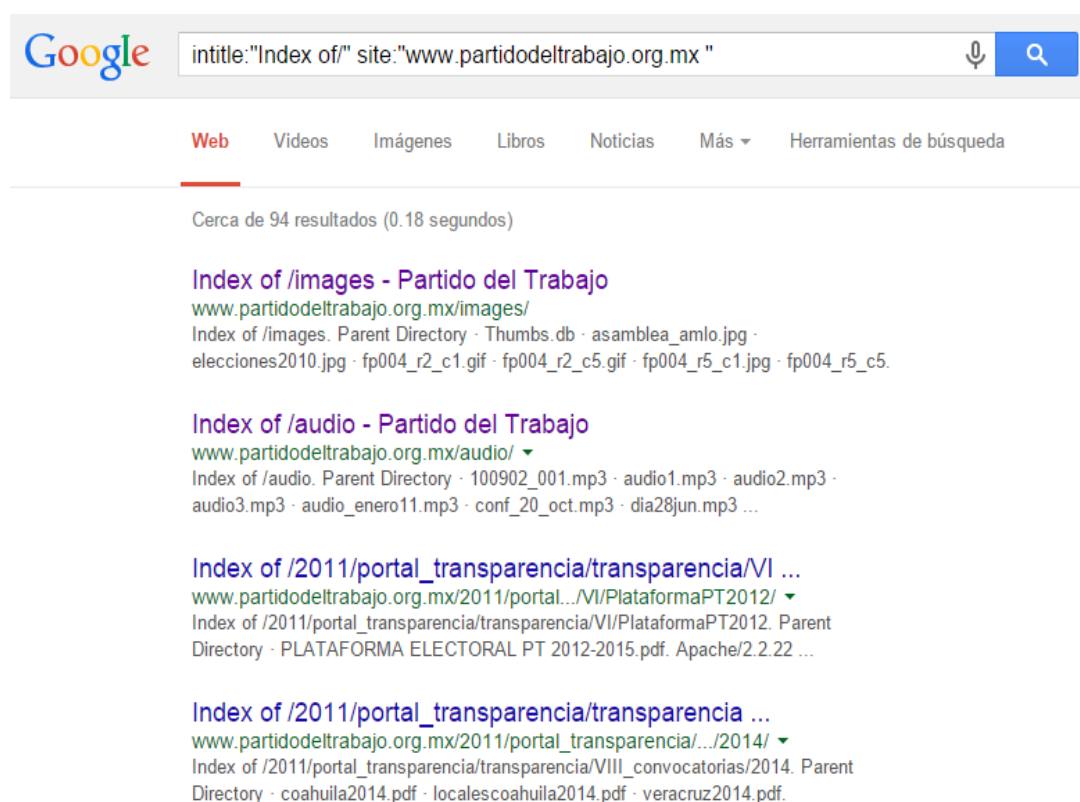
Query Error: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near " at line 1

SQL:select votos from respuestas WHERE idresp=

Query Error: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near " at line 1

SQL:update respuestas set `votos`=1 WHERE idresp=

## 3. Se utilizó el dork *intitle* de Google para buscar páginas relacionadas.



The screenshot shows a Google search interface with the query "intitle:\"Index of/\" site:\"www.partidodeltrabajo.org.mx \"". Below the search bar, there are tabs for "Web", "Videos", "Imágenes", "Libros", "Noticias", "Más", and "Herramientas de búsqueda". The search results are displayed below the tabs, showing "Cerca de 94 resultados (0.18 segundos)". The first result is "Index of /images - Partido del Trabajo" with the URL "www.partidodeltrabajo.org.mx/images/". The second result is "Index of /audio - Partido del Trabajo" with the URL "www.partidodeltrabajo.org.mx/audio/". The third result is "Index of /2011/portal\_transparencia/transparencia/VI ..." with the URL "www.partidodeltrabajo.org.mx/2011/portal.../VI/PlataformaPT2012/". The fourth result is "Index of /2011/portal\_transparencia/transparencia ..." with the URL "www.partidodeltrabajo.org.mx/2011/portal\_transparencia/.../2014/".

De manera que se tuvo a acceso a material de audio que no es accesible desde la página

## Index of /audio

- [Parent Directory](#)
- [100902\\_001.mp3](#)
- [audio1.mp3](#)
- [audio2.mp3](#)
- [audio3.mp3](#)
- [audio\\_enero11.mp3](#)
- [conf\\_20\\_oct.mp3](#)
- [dia28jun.mp3](#)
- [player\\_mp3\\_maxi.swf](#)

Apache/2.2.22 (Unix) mod\_ssl/2.2.22 OpenSSL/0.9.7a mod\_auth\_passthrough/2.1 mod\_bwlimited/1.4 FrontPage/5.0.2.2635 Server at www.partidodeltrabajo.org.mx Port 80

4. por último se obtuvo más información a través de *web.archive.org* que permite explorar en las versiones pasadas del sitio, recabando así más información.



En cuanto al análisis del código html no se encontraron script en la página principal que pudiera incrementar la vulnerabilidad.