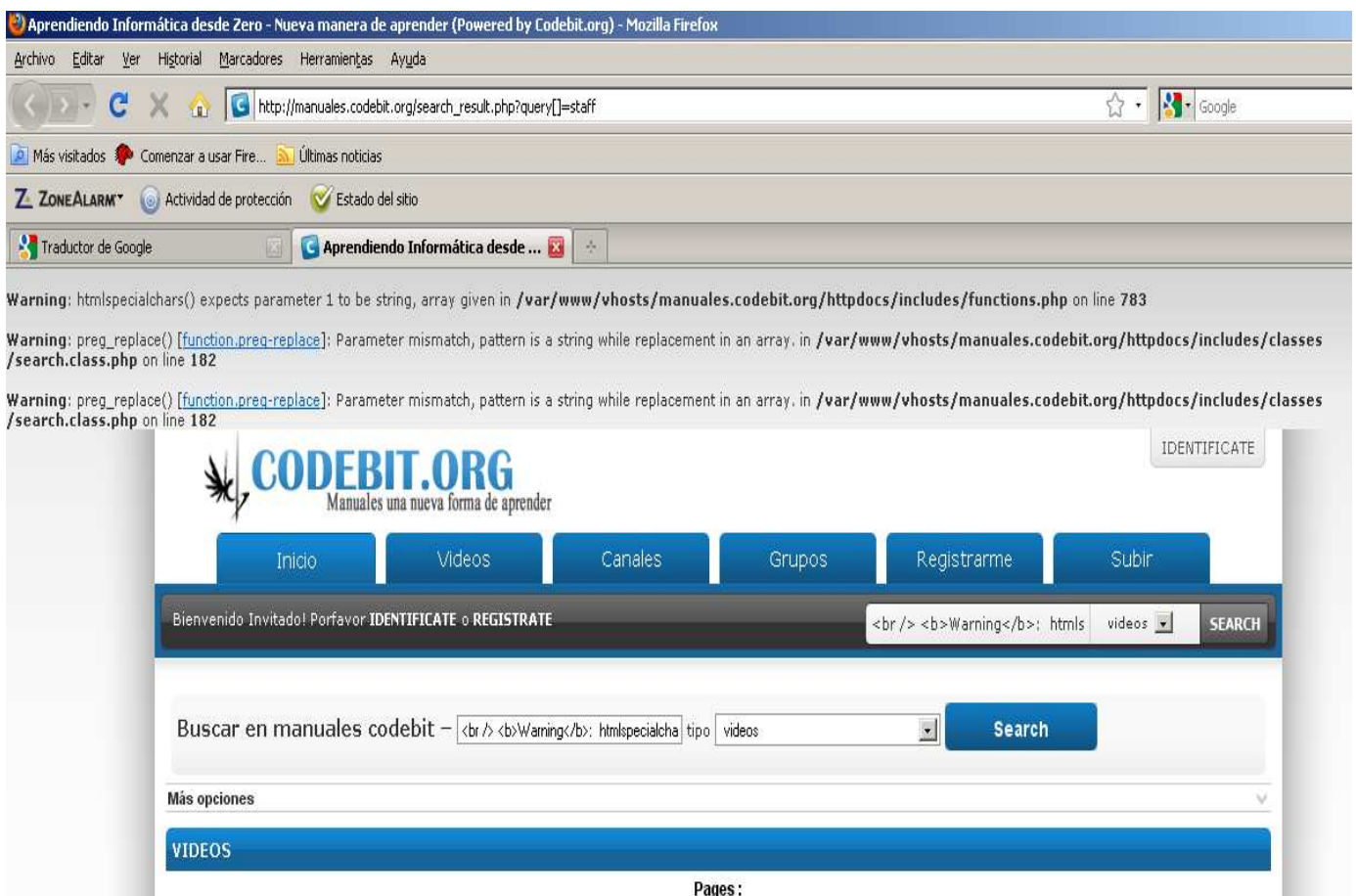


PFD (Partial Function Disclosure)

El PFD consiste en que tras introducir valores malformados podamos obtener errores de los cuales extraer la ruta y parcialmente algunas funciones usadas por la web. Cómo podemos observar el concepto es parecido al del FPD (Full Path Disclosure) y su explotación será casi la misma que el FPD pero la diferencia radica en que a la hora de explotar el bug se mostraran algunas de las funciones que son usadas por la aplicación web como se muestra a continuación en la figura.



Como vemos el bug lo estamos explotando asiendo a la variable query= en un array como se muestra en la imagen (query[]=) lo cual aparte de mostrarnos la ruta con lo cual vendría a ser un FPD (Full Path Disclosure). Aparte se mostrarían algunas de las funciones que usa la web y la línea de código en la cual están siendo usadas lo cual vendría a ser el PFD (Partial Function Disclosure) que es el tema de este paper.

Algunos tendrán la pregunta diciendo de que sirve poder ver algunas de la funciones usadas en la aplicación web pues bueno todo nos podría ser útil para saber a que tipo de filtros pro ejemplo nos estamos enfrenta y a la vez nos vamos asiendo una idea de cómo esta programa la aplicación web y que tipo de seguridad se esta empleando.

¿Forma de Repararlo?

La forma de repararlos es muy fácil solo tenemos que desactivar `display_error` en el archivo `php.ini`

Bueno con esto termino esta explicación de PFD (Partial Function Disclosure)

PFD (Partial Function Disclosure) escrito y Termino inventado por Jbyte (jbyte@hotmail.es)

30 de Enero del 2010