**Fundamentos de Seguridad**

***Práctica Footprinting***

**Dora Angélica Ávila Galván**

**angelica.avila.galvan@outlook.com**

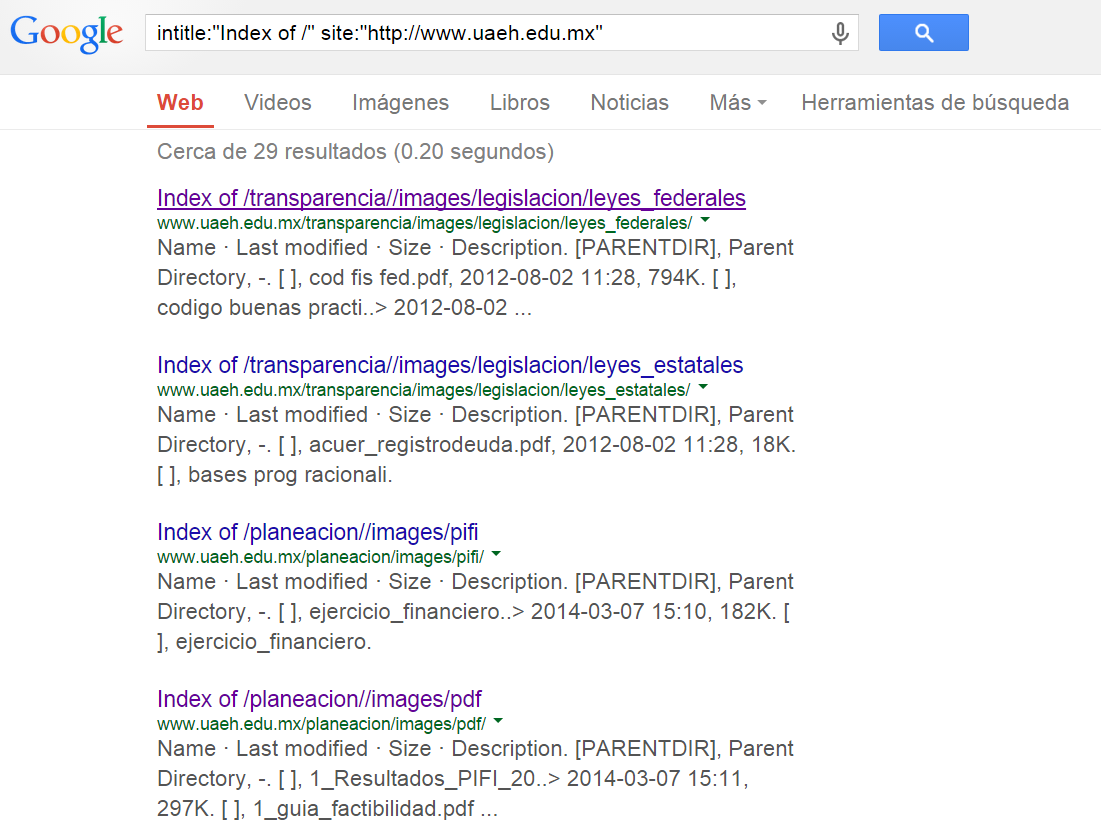
El footprinting es considerado un pre-ataque, pues es el primer paso para obtener información sobre una red y es posible encontrar varias formas de entrar a una organización.

Para esta práctica, se utiliza el footprinting para encontrar información y vulnerabilidades del sitio Web <http://www.uaeh.edu.mx/> perteneciente a la Universidad Autónoma del Estado de Hidalgo.

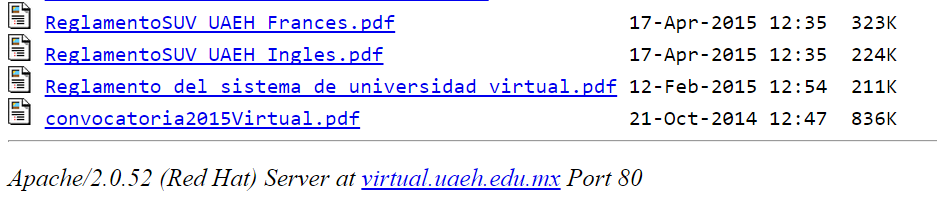
1.- Se recolectó información del sitio Web a atacar, a través de whois.net, de esta forma podemos saber las fechas de creación y expiración, la última fecha de actualización, el nombre de la persona del contacto administrativo, el lugar e inclusive el DNS:

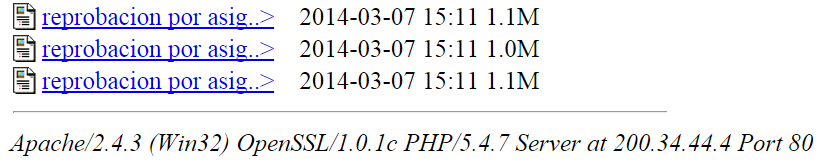


2.- Se utilizó el dork ***intitle*** de Google para buscar páginas con ese título:

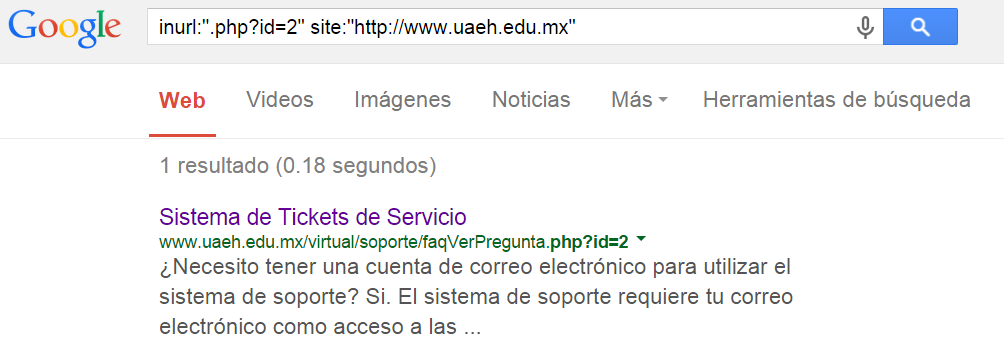


Como resultado, se obtuvo una lista de directorios a los que se puede acceder de manera directa, proporcionando información del servidor, el sistema operativo, la IP y el puerto:





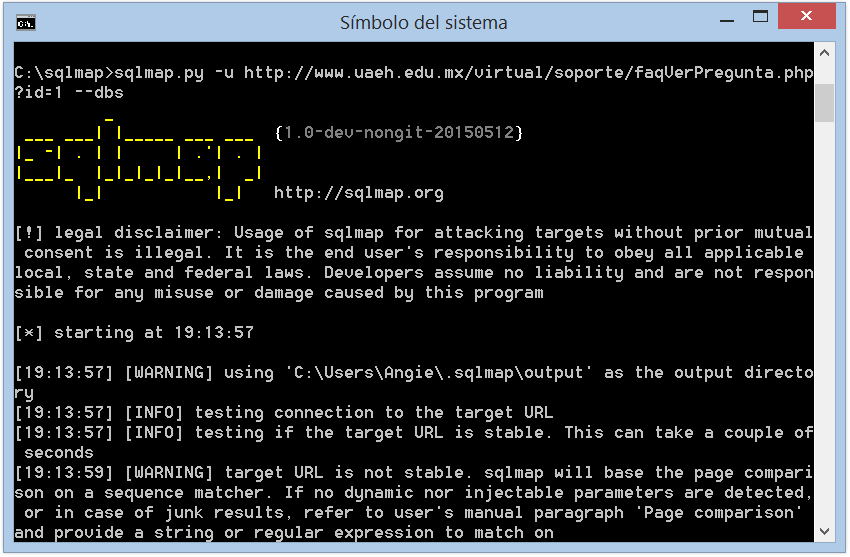
3.- Se comprobó si el sitio Web era vulnerable a sql injection, para ello, primero se utilizó el dork:



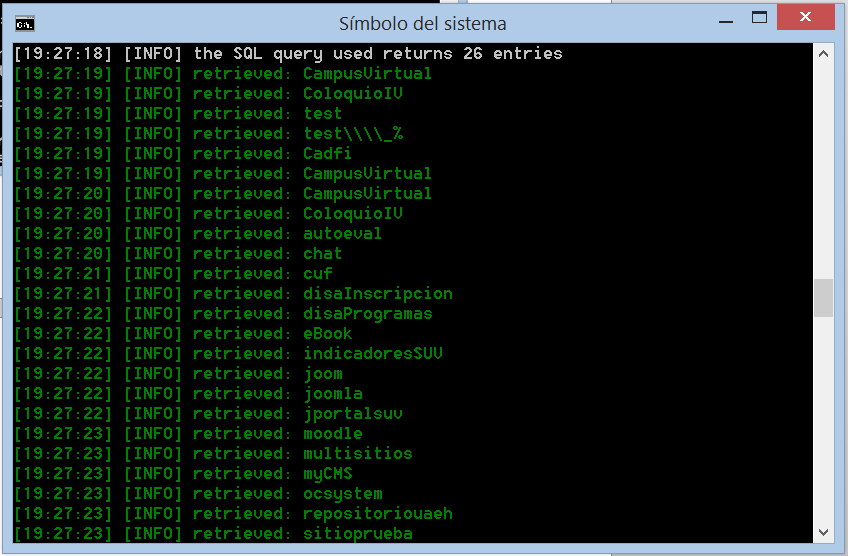
Al entrar en la página se le agregó una comilla en la URL, obteniendo el siguiente resultado, mostrando que la página si es vulnerable a un ataque de sql injection:

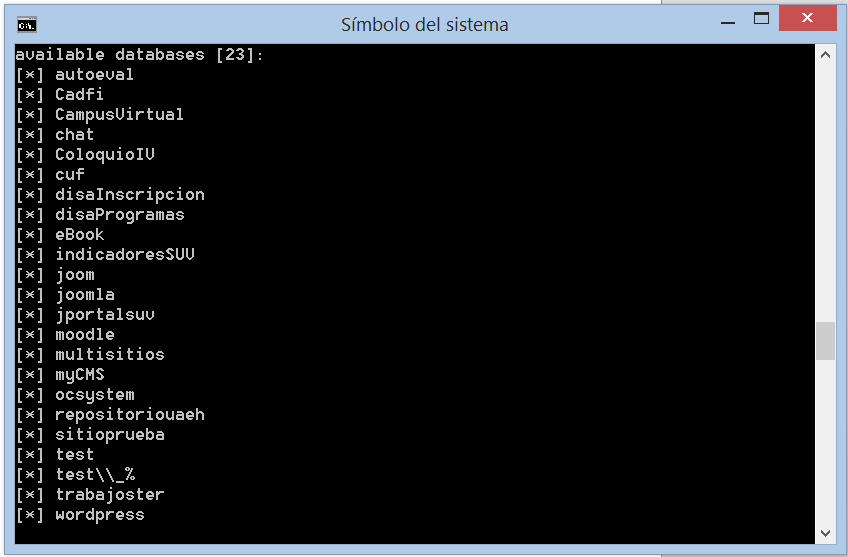


4.- Se utilizó ***sqlmap***,una herramienta dedicada a realizar ataques de SQLi (sql injection) a través de realización de peticiones a los parámetros de una URL mediante peticiones GET y POST, para obtener información sobre las bases de datos que utiliza el sitio:



Proporcionó los siguientes resultados, mostrando las bases de datos disponibles en el sitio:





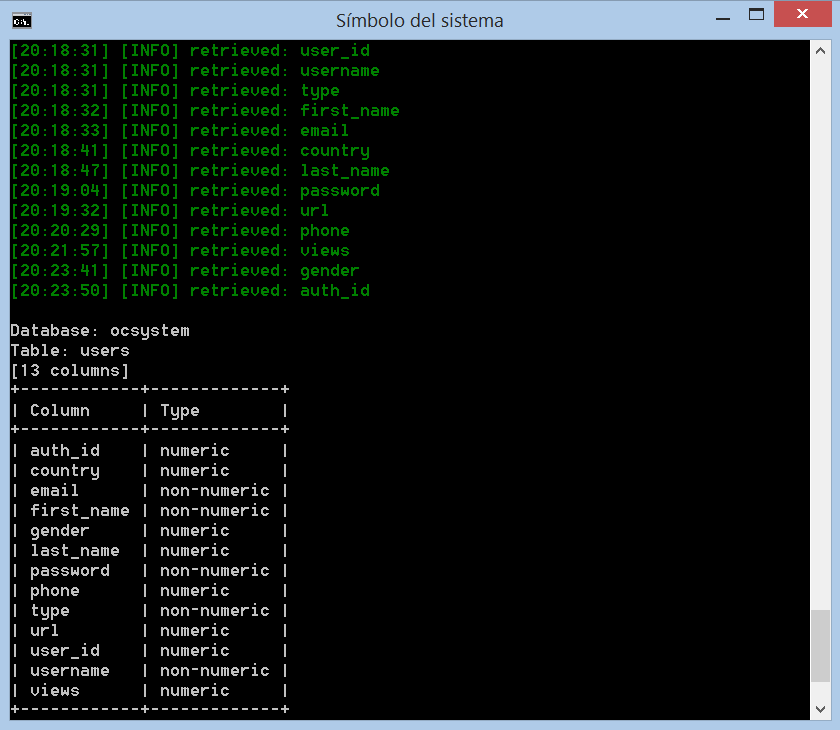
Al conocer las bases de datos del sitio, se puede acceder a las tablas e inclusive a los datos de éstas, a través de ***sqlmap***.



En este caso, elegí la BD ocsystem y posteriormente seleccione la tabla de users, y sqlmap me muestra la información de las columnas:

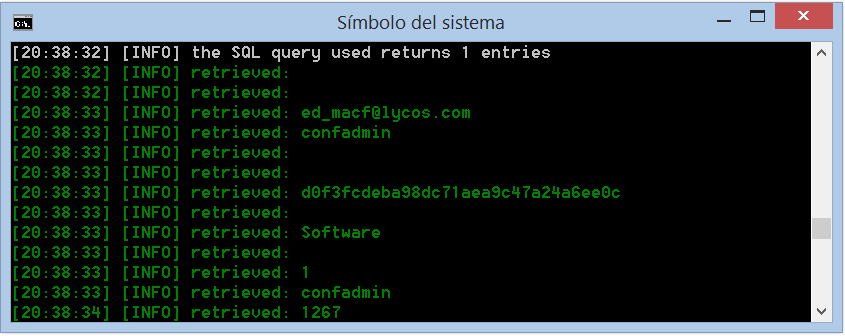




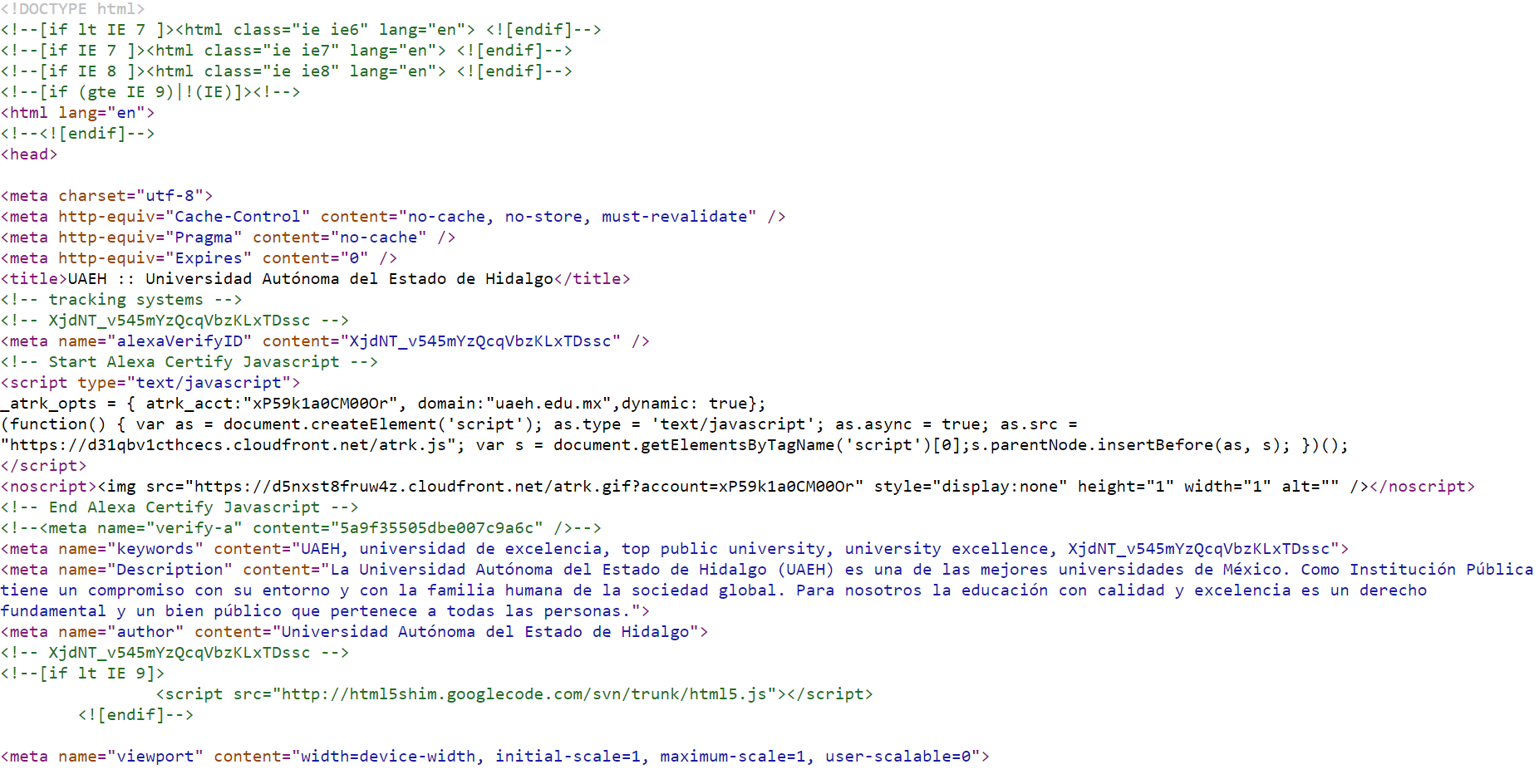


Finalmente, para obtener el *username* y el *password* de la tabla, se ejecuta el siguiente comando:



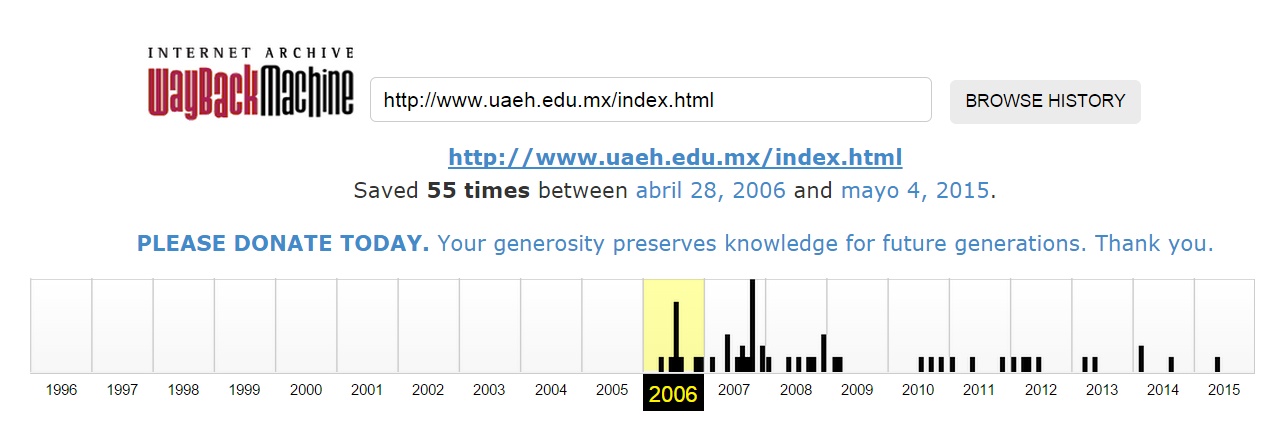


5.- Se analizó el código fuente del sitio Web con el fin de verificar si existen campos ocultos y explorar las cabeceras, los directorios de imágenes, las hojas de estilo, observar los scripts, etc.



La página Web principal incluye varios scripts y hace uso de referencias y de hojas de estilo, así mismo a lo largo del sitio, funciona de manera similar.

6.- Finalmente, busqué más información del sitio a través de web.archive.org:





En esta página se puede encontrar el historial del sitio, cualquier modificación o actualización, lo cual es útil por si se requiere información publicada anteriormente.