
[Cyber Webinar]

SQL injection + SQLmap

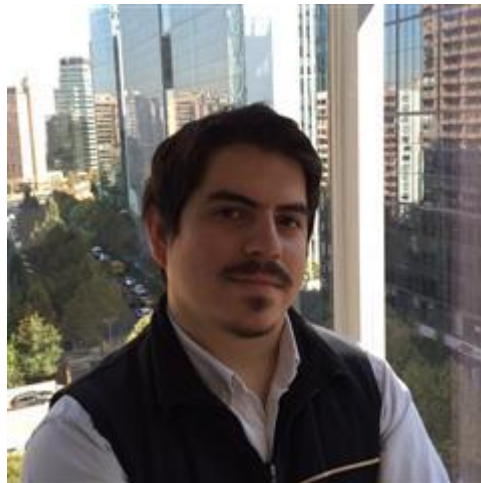
The logo for SQLmap is centered on the slide. It consists of a blue rectangular box with a fine grid pattern. Inside the box, the word "sqlmap" is written in a white, lowercase, monospaced font. Below the name, the text "Automatic SQL injection and database takeover tool" is written in a smaller, white, lowercase, monospaced font. The box is flanked by two short, horizontal, olive-green bars.

sqlmap

Automatic SQL injection and database
takeover tool

Presentación

- Miguel Díaz
- Especialista en Seguridad informática
- Trabajo en CSIRT
- **Especialidad:** ~~Romper sitios~~
Seguridad en sitios web



www.linkedin.com/in/mdiazcl

¿Qué es una SQL injection?

- Inyectar código en un sitio web, específicamente en sus consultas SQL.

Por qué ocurre?

- Por una falta o incorrecta de validación.

Cómo funciona?

- Es lo que vamos a ver en esta presentación



SQL Injection

Conceptos básicos

- Protocolo HTTP
- Consultas SQL (Programación)
- Procesamiento HTTP del Servidor

Protocolo HTTP

Paso 1

```
GET /Index.html HTTP/1.1\r\n
Connection: Keep-Alive\r\n
Accept: */*\r\n
User-Agent: Sample Application\r\n
Host: www.microsoft.com\r\n\r\n
```

Paso 2,3



HTTP Server

```
HTTP/1.1 200 OK
Server: Microsoft-IIS/5.0\r\n
Content-Location: http://
www.microsoft.com/default.htm\r\n
Date: Tue, 25 Jun 2002 19:33:18 GMT\r\n
Content-Type: text/html\r\n
Accept-Ranges: bytes\r\n
Last-Modified: Mon, 24 Jun 2002 20:27:23
GMT\r\n
Content-Length: 26812\r\n
\r\n
<html>
.
.
.
</html>
```

Paso 4



Pocket PC
Device

Fuente: etutorials.org

- **Paso 1:** Petición HTTP por parte del Cliente
- **Paso 2:** Servidor procesa la petición
- **Paso 3:** Servidor procesa un HTML
- **Paso 4:** Servidor entrega al servidor (con código 200)

- Métodos HTTP:

- GET
- POST

Consultas SQL

SQL: Structured Query Language

Sintaxis de una consulta:

SELECT <columnas> FROM <tabla>
<condiciones>

La consulta es procesada por una base de datos y entrega un resultado.

Tabla: usuarios

A	B	C	D	E
ID	USUARIO	PASSWORD	RUT	NIVEL
1	admin	4dm1n	1-9	99
2	John	doe_123	21789291-0	5
3	Ana	q1w2e3r4	10669662-4	4
4	Bob	alfiler_1	8852209-5	3
5	Charlie	brown_147	19522809-4	2
6	Dayton	dan!47	18446209-5	1

Ejemplo:

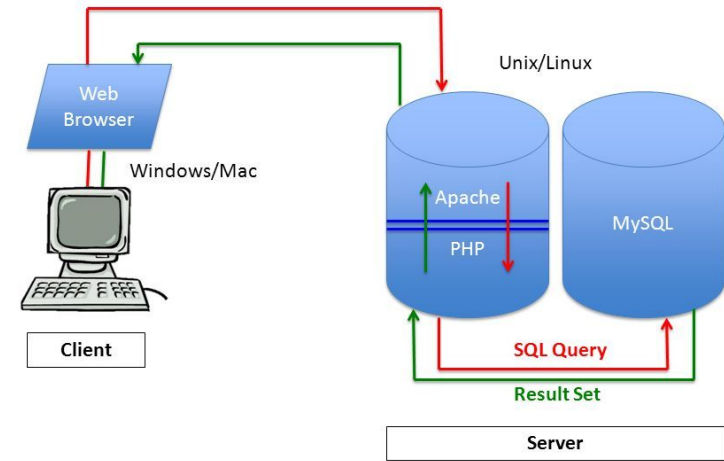
SELECT usuario,password FROM usuarios
WHERE nivel = 99;

Resultado:

USUARIO	PASSWORD	NIVEL
admin	4dm1n	99

Procesamiento HTTP del Servidor

1. Servidor recibe la petición
2. Procesador PHP procesa el archivo (ej: index.php)
3. Realiza la consulta (SQL Query)
4. Servidor de base de datos devuelve registros
5. PHP Proceso lo recibido
6. Servidor crea el HTML y lo envía al cliente



Fuente: <http://slideplayer.com/slide/8396823/>

Como es en código PHP?

```
# Define POST variables
```

```
uname = request.POST['username']
```

```
passwd = request.POST['password']
```

Recibe variables por parte del navegador cliente

```
# SQL query vulnerable to SQLi
```

```
sql = "SELECT id FROM users WHERE username=''" + uname + "'" AND password=''" + passwd + "'"
```

Genera la consulta SQL

```
# Execute the SQL statement
```

```
database.execute(sql)
```

Ejecuta la consulta

Vamos a inyectar código en una aplicación vulnerable