

Seguridad Web



Medellín, 8 de Octubre de 2011

Matias Katz

Mail: matias@matiaskatz.com

Blog: www.matiaskatz.com

Twitter: [@matiaskatz](https://twitter.com/matiaskatz)



www.mkit.com.ar

- ✓ Proceso de Hacking a través de aplicaciones web públicamente visibles en Internet
- ✓ Es el método preferido por muchos atacantes
- ✓ Permite un alto impacto de una manera simple y transparente
- ✓ Respeto un anonimato casi completo
- ✓ Es muy difícil de detectar por parte de la víctima

- ✓ SQL Injection
 - ✓ Inyección de comandos SQL hacia el servidor a través de interacciones con la App
 - ✓ Permite manipular las actividades que la App realiza hacia el servidor SQL
 - ✓ Nos da la posibilidad de obtener información, así como también ingresarla
- ✓ Cross-Site Scripting (XSS)
 - ✓ Llamado XSS para no confundirlo con CSS (Cascading Style Sheets)
 - ✓ Manipula la lectura de código HTML que el navegador realizará al cargar el site
 - ✓ Nos permite interactuar directamente con el usuario, el sistema y sus archivos
- ✓ Ambos métodos pueden llegar a obtener resultados **altamente peligrosos**

- ✓ Toma provecho de los comandos típicos a utilizar en un servidor SQL:
 - ✓ SELECT: Selecciona registros dentro de una tabla
 - ✓ FROM: Establece la tabla de origen de la información
 - ✓ WHERE: Filtra los resultados según un parámetro específico
 - ✓ ORDER BY: Ordena los resultados según una columna en particular
 - ✓ UNION: Une consultas y las concatena en un único resultado

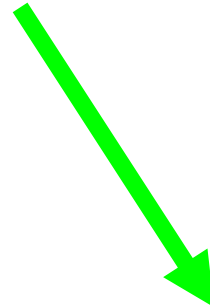
- ✓ Utiliza los parámetros típicos en un servidor SQL:
 - ✓ ' (comilla simple): Sirve para establecer cadenas del tipo *STRING*
 - ✓ ; (punto y coma): Sirve para indicar la finalización de una sentencia
 - ✓ -- (doble signo negativo): Sirve para comentar el resto de texto en la sentencia
 - ✓ <, >, = (menor que, mayor que, igual que): Operadores comparativos de datos



La siguiente consulta nos dará todos los registros en la tabla *'usuarios'*



```
SELECT * FROM usuarios;
```



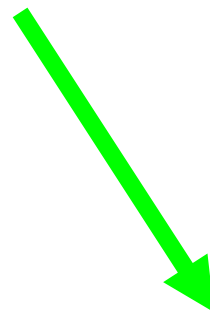
id	usuario	password
1	Juan	juan123
2	Pedro	pedro456
3	Carlos	carlos789



La siguiente consulta nos dará el registro que corresponda al nombre *'juan'*



```
SELECT * FROM usuarios WHERE usuario='juan';
```




id	usuario	password
1	Juan	juan123

✓ Esta consulta se genera a raíz de la información proveída por la aplicación:

✓ *<http://www.host.com/consulta?usuario=juan>*

✓ `SELECT * FROM usuarios WHERE usuario='juan';`





id	usuario	password
1	Juan	juan123

✓ En base a esto, podemos alterar la consulta:

✓ *..consulta?usuario=juan;select * from admins;*

✓ **SELECT * FROM usuarios WHERE usuario='juan';**
SELECT * FROM admins;



id	usuario	password
1	Juan	juan123
id	admin	password
1	admin1	4dm1n
2	admin2	#\$%GFD

✓ Algunos de los ataques de Inyección SQL más comunes son:

✓ 'OR '1'='1

✓ ORDER BY x

✓ UNION ALL SELECT x,y,z FROM

✓ UNION ALL SELECT group_concat(table_name) FROM information_schema.tables

✓ SELECT group_concat(user) FROM mysql.user

✓ SELECT password FROM mysql.user WHERE user='root'

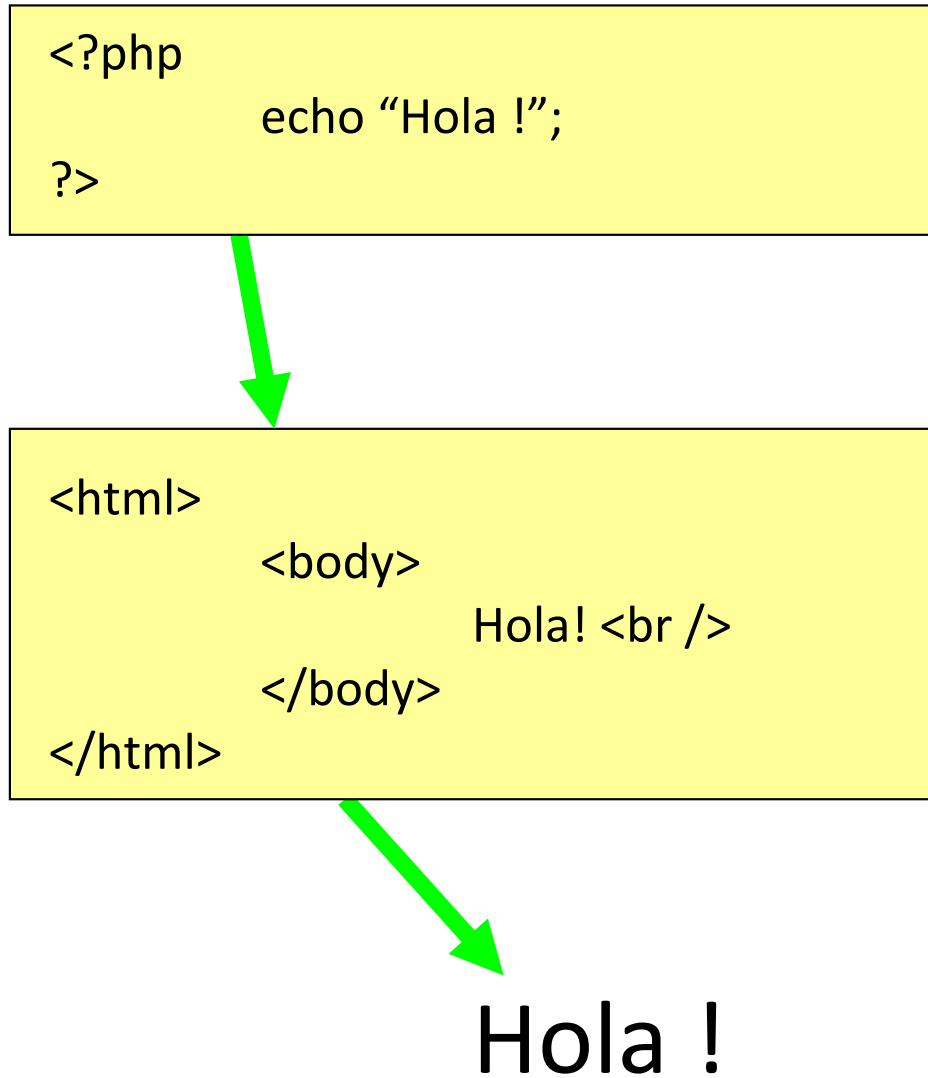
✓ load_file('x')

DEMO

- ✓ Toma provecho de la forma que el navegador procesa los tags HTML
 - ✓ : Permite incorporar y mostrar una imagen en pantalla
 - ✓ <script>: Permite declarar un script en Javascript
 - ✓ <iframe>: Permite incluir un marco con un origen de datos diferente
 - ✓ Scripts de descarga de archivos
 - ✓ Scripts de subida de archivos



La lectura de un texto es lineal y sin revisión previa:



HTML puede tomar información de una variable:



`http://www.host.com/consulta.php?nombre=Pedro`




```
<?php
    $nombre=$_POST['nombre']
    echo "Hola $nombre !";
?>
```



Hola Pedro!

✓ De esta forma, podemos modificar lo mostrado en pantalla:

✓ ...consulta.php?nombre=



```
<?php
    $nombre=$_POST['nombre']
    echo "Hola $nombre !";
?>
```




Hola  !

 Los ataques de Cross-Site Scripting (XSS) más comunes son:

 ``

 `<iframe src="xx">`

 `<script>alert('XSS');</script>`

 `<script>alert(document.cookie);</script>`

DEMO

Preguntas ?



Medellín, 8 de Octubre de 2011

Matias Katz

Mail: matias@matiaskatz.com

Blog: www.matiaskatz.com

Twitter: [@matiaskatz](https://twitter.com/matiaskatz)

