Inxección MySQL

Exemplo de inxección MySQL:

```
<!DOCTYPE html>
<html lang="es">
<head>
        <meta charset="UTF-8" />
        <title>Prueba de inyección MySQL</title>
</head>
<body>
<br/>Para chequear si es vulnerable la página añadimos un ' al final de alguna variable
<br/>Por ejemplo: inyeccion.php?nombre=&password='
<br/>Si obtenemos algún mensaje de error:<b>You have an error in your SQL syntax</b>,
 entonces es vulnerable a inyección.
<br/>
<br/>Si usted teclea en Nombre: usuario' --
<br/>Si usted teclea en Password: xxxx' or 1='1
<br/>O bien teclean en Password: xxxx' or '1=1
<br/>
<br/>O bien: usuario'; delete from pruebas --
<hr/>

<?php
// Ejemplo de inyección MySQL
// Más info: http://www.go4expert.com/forums/showthread.php?t=20438
if (isset($_GET['nombre']))
{
// Nos conectamos a la base de datos.
// Datos configuración de la conexión al MySQL.
$nombrebase="xxxxxx";
$usuario="xxxxxx";
$servidor="localhost";
$password="xxxxx";
//////////////////////////////////////
// Hacemos la conexión al servidor de MySQL.
$conexion=mysql_connect($servidor,$usuario,$password) or die("Error conectando a BD: ".mysql_error());

// Seleccionamos la base de datos en esa conexión.
mysql_select_db($nombrebase,$conexion) or die("Error seleccionando base de datos");

// Consulta a ejecutar para acceder al sistema.
$sql=sprintf("select * from pruebas where nombre='%s' and password='%s'",$_GET['nombre'],$_GET['password']);


// Corrección de la inyección MySQL
/* $sql=sprintf("select * from pruebas where nombre='%s'  and password='%s'",
$mysqli->real_escape_string($_POST['nombre']),$mysqli->real_escape_string($_POST['password']));
*/
// Imprimimos la instrucción MySQL
echo "Consulta ejecutada: <b>".$sql."</b><br/>";

// Ejecutamos la consulta.
$resultados=mysql_query($sql,$conexion) or die(mysql_error());

// Mostramos los registros encontrados.
echo "<br/>Registros encontrados: ".mysql_num_rows($resultados);

// Número de registros en la consulta.
if (mysql_num_rows($resultados)!=0)
echo "<br/><font color=red><h2>Acceso concedido al sistema.</h2></font>";

//      Para probar la inyección.
//      Metemos en el campo usuario: xxxx' or 1='1
//      xxxx'; delete from usuarios or '1=1

}
?>
<h2>Formulario de acceso</h2>
<form name="formulario" method="get">
Nombre: <input name="nombre" type="text" />
```

```
<br/>Password: <input name="password" type="password" />
<br/>
<input type="submit" value="Consultar"/>
</form>
<br/><br/>
</body>
</html>
```

Video Youtube demostrando inyección MySQL.