SQL Injection

Essa é uma técnica bastante simples.

Para aprender como se proteger, primeiro vamos aprender como atacar.

Para demonstrar na prática a técnica de SQL Injection faremos o seguinte:

1. Vamos criar uma pequena aplicação usando a tecnologia MySQL, PHP e HTML
2. Vamos usar o Xampp para criar a aplicação
3. A aplicação deverá conter:
    a. uma página inicial com um formulário de login
    b. uma página de boas vindas com um botão de logoff para sair da aplicação
4. No caso de um login com sucesso levaremos o usuário a uma página com uma mensagem de boas vindas e daremos início ao controle de seção de uso para o usuário logado
5. Inicialmente essa pequena aplicação não terá qualquer tipo de verificação contra SQL Injection

- Abra o Xampp,
- Ligue os serviços Apache e o MySQL
- Crie os arquivos abaixo na pasta c:\xampp\htdocs\exemplo
- Execute a aplicação e teste se o usuário admin entra com a senha correta
- Depois, execute a aplicação novamente e teste com um usuário ou senha incorretos

Seguem os códigos fonte:

conexao.php

```
<?php
$servername = "localhost";
$username = "root";
$password = "";
$dbname = "sqlinjection";

// Criar conexão
$conn = new mysqli($servername, $username, $password, $dbname);

// Verificar conexão
if ($conn->connect_error) {
    die("Conexão falhou: " . $conn->connect_error);
}
?>
```

index.php

```
<!DOCTYPE html>
<html>
<head>
    <title>Login</title>
</head>
<body>
    <h2>Login</h2>
    <form action="login.php" method="post">
        <label for="username">Usuário:</label><br>
        <input type="text" id="username" name="username"><br>
        <label for="password">Senha:</label><br>
        <input type="password" id="password" name="password"><br><br>
        <input type="submit" value="Entrar">
    </form>
</body>
</html>
```

login.php

```
<?php
session_start();
require_once('conexao.php');

if ($_SERVER["REQUEST_METHOD"] == "POST") {
    $username = $_POST['username'];
    $password = $_POST['password'];

    $sql = "SELECT * FROM usuarios WHERE username = '$username' AND senha =
'$password'";
    $result = $conn->query($sql);

    if ($result->num_rows > 0) {
        $_SESSION['username'] = $username;
        header("Location: welcome.php");
    } else {
        echo "Usuário ou senha incorretos.";
    }
}

$conn->close();
?>
```

welcome.php

```php
<?php
session_start();
if (!isset($_SESSION['username'])) {
    header("Location: index.php");
    exit();
}
?>

<!DOCTYPE html>
<html>
<head>
    <title>Boas Vindas</title>
</head>
<body>
    <h2>Bem-vindo, <?php echo $_SESSION['username']; ?>!</h2>
    <a href="logout.php">Sair</a>
</body>
</html>
```

logout.php

```php
<?php
session_start();
session_destroy();
header("Location: index.php");
?>
```

SQL para criar o banco, a tabela e inserir um usuário

```sql
-- Criar o banco de dados
CREATE DATABASE IF NOT EXISTS sqlinjection;

-- Selecionar o banco de dados
USE sqlinjection;

-- Criar a tabela "usuarios"
CREATE TABLE IF NOT EXISTS usuarios (
    id INT AUTO_INCREMENT PRIMARY KEY,
    username VARCHAR(50) NOT NULL,
    senha VARCHAR(50) NOT NULL
);

-- Inserir um registro de exemplo na tabela "usuarios"
INSERT INTO usuarios (username, senha) VALUES ('admin', '123');
```