Home | Introduction | Attacks | Advanced | Defense | Resources | About

sqlinjection

GET THE BOOK!

Recent Articles

- Time-Based Blind SQL Injection using Heavy Query
- Estimating MySQL Table Size using SQL Injection
- Time-Based Blind SQL Injection Attacks
- Analysing Server Response and Page Source
- Database Fingerprinting for SQL Injection

SQL Injection and Database Errors

Understand and identify database errors

Information leaked by errors, especially database errors, can help an attacker **to achieve a successful SQL injection attack**. They basically give hints to help crafting an SQL segment that will be correcly integrated in the query. It can also reveal precious details about the system, the database and the main query. For these reasons, a good security tester must be able to **identify errors** and take advantage of the information they provide.

Database Errors Causes

Database errors are mostly generated when the attacker is testing for SQL injection vulnerabilities without knowing the query's structure. They are also frequently seen when the first SQL segments are injected in attempt to take over the main query.

Errors are thrown by the database engine for one main reason; an invalid SQL statement. Basically any incorrect SQL instruction identified when parsing or executing the SQL will generate an error. To name a few : unexpected quote, invalid table name, misspelled operator, mismatching data types (for example when using UNION), missing parenthesis, insufficient permissions, etc.

It must also be mentionned that **some powerful SQL injection techniques** completely rely on database errors. In those cases, the attacker intentionally crafts an invalid SQL segment and analyses information returned in the error message. It is a fast and efficient way to extract specific information.

Database Error Examples

In order to help you identify database errors a few examples are presented below.

MySQL Errors

MySQL Errors starts with the error number (4 digits) followed by a dot and the error description.

EXAMPLE OF MYSQL ERROR MESSAGE.

```
1064 - You have an error in your SQL syntax; check the manual that corresponds to your
MySQL server version for the right syntax to use near ''' at line 1.
```

For more information about MySQL errors visit MySQL's official error codes and messages documentation.

SQL Server Errors

Error messages from SQL Server contain the error number, the level, the state and the line number followed by the error description.

EXAMPLE OF SQL SERVER ERROR.

```
Msg 105, Level 15, State 1, Line 1
Unclosed quotation mark after the character string ''.
```

For more information consult this detailed list of SQL Server errors and the official documentation about error severity.

Oracle Errors

Oracle errors are particularly easy to identify since all error code is prefix with "ORA-". The error message contains prefix and the error code; a 5 digit number. It is followed by the error description.

EXAMPLE OF ORACLE ERROR.

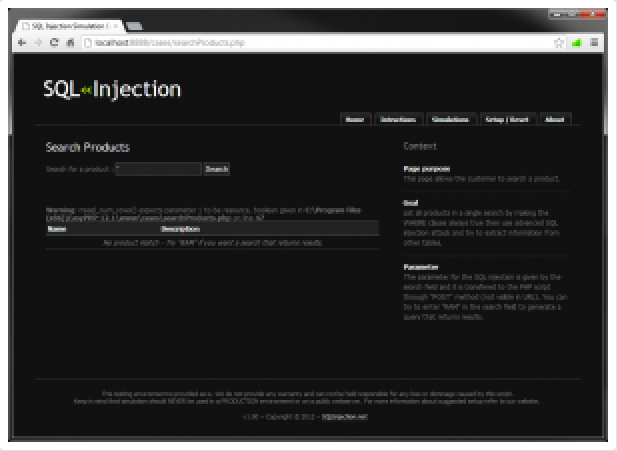
```
ORA-01756: quoted string not properly terminated.
```

For more information visit Oracle errors documentation.

Finding Errors

You need to know that error messages can be presented to the user in different ways. If **error reporting** is enabled, database errors can be sent directly to the end user. Most of the time, they will be embedded in the webpage with some partial stack trace. You may also face a custom or generic error page presenting the information.

Some API only show the error returned by the function that executed the invalid query or tried fetching its results. It does not provide as much details as database errors, however it indicates that something unexpected happened and this is enough to help the attacker. The screen capture illustrates this situation in a PHP page.



PHP Error from Invalid Query

It is still possible you see the error message if error reporting is disabled but this is quite rare in real scenarios. It would require that the application code handles the error and displays it to the end user.

Posted in : Anomalies

Tagged: Database Error | Error | Error Reporting | Test | Valid Query

Do you want to try the simulation?

You can download a secure simulation environment to try every techniques explained on this website. It's totally free!

Take the tour →

This article was helpful?

Then please share it via these links.

Related Articles

Check out the related articles below to find more of the same content.

Extracting Information from Custom Errors

Understanding information provided by application errors

Detecting SQL Injection Vulnerabilities from HTTP Errors

Understanding HTTP errors generated by SQL injection attacks

Database Fingerprinting for SQL Injection

Identifying the underlying DBMS

About

Sqlinjection.net was developed to provide information about SQL injection to students, IT professionals and computer security enthusiasts. It intends to be a reference about this security flaw.

Read more

Main Sections

- Introduction to SQL Injection
- SQL injection Tutorial
- Advanced SQL Injection
- Securing Against SQL Injection
- Resources for SQL Injection

Disclamer

This website and/or it's owner is a participant in the Amazon Services LLC Associates Program, an affiliate advertising program designed to provide a means for sites to earn advertising fees by advertising and linking to sqlinjection.net.

sqlinjection.net

Copyright · Disclaimer · Terms of Use · Privacy Policy · **Back to Top ↑**