



SQL injection to RCE exploitation



Bijay Kumar

Follow

3 min read · Sep 13, 2024



51



Hello Hackers!



Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for \$5/month

1. Conditions Required for Escalation from SQLi to RCE:

- **Database Privileges:** The database user must have sufficient privileges to execute operating system-level commands (e.g., `xp_cmdshell` in SQL Server, `COPY ... PROGRAM` in PostgreSQL).
- **Database-Specific Features:** Some databases have built-in functions or stored procedures that allow the execution of shell commands.

Techniques for Exploiting SQLi to Achieve RCE:

Here are a few methods attackers may use to escalate SQL Injection to Remote Code Execution:

• ~~Using Database-Specific Functions to Execute System Commands: Some~~

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

- PostgreSQL (`COPY ... PROGRAM`): PostgreSQL allows execution of system commands using the `COPY` command with the `PROGRAM` option:

```
' ; COPY (SELECT '') TO PROGRAM 'whoami'; --
```

Preconditions:

- The attacker needs sufficient privileges to execute `COPY` with `PROGRAM`.
- The PostgreSQL server must run on an environment that allows this.

Reading and Writing Files: SQL injection may allow the attacker to read or

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

- Find an entry point (such as a form, query string, etc.) vulnerable to SQL injection.
- Test and confirm that the input can be manipulated to change the SQL query.

2. Determine Database Type and Version:

- Use the SQL injection to extract information about the database type (MySQL, SQL Server, PostgreSQL, Oracle, etc.) and its version. This helps in understanding which specific commands or techniques can be used.

3. Check for Available Privileges and Features:

- Enumerate the current user's privileges and the available database

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

- Use the RCE to escalate privileges, pivot to other systems, or exfiltrate data.

Mitigation Techniques

To prevent SQL injection from escalating to RCE:

1. **Use Least Privilege Principles:** Ensure that the database user only has the minimum permissions required. Avoid giving permissions to execute OS-level commands unless absolutely necessary.
2. **Disable Dangerous Functions:** Disable or restrict database functions that can execute system-level commands (e.g., `xp_cmdshell` in SQL Server, `LOAD DATA INFILE` in MySQL).

3. **Regular Patching:** Keep the database and associated software up to date.

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

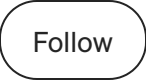
✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app



Written by Bijay Kumar

8 followers · 1 following



No responses yet



Write a response

What are your thoughts?

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

 Bijay Kumar

DOM-based Cross-Site Scripting (DOM XSS)—Detailed explanation

Hi Hackers !

Sep 13, 2024  2



 Bijay Kumar

Secure code review : Part -2

Hi Hackers !

Sep 13, 2024



Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app



6d ago



204



4



Long Vu

SQL Injection prevention

What SQL Injection is

Nov 15, 2024



Rahul M S

No Sleep, All SQLi, A Hot Chennai Night, Random Browsing, and a...

Apr 6



Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

See more recommendations

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app