



How Boolean-Based Blind SQL Injection Works



Yousef Alotaibi

Follow

7 min read · Apr 20, 2025



25



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. What is Boolean-Based Blind SQL Injection?

Boolean-Based Blind SQL Injection is a type of SQL injection where the application doesn't return visible data but responds differently to true or false SQL conditions, allowing attackers to infer information bit by bit by observing changes in the application's behavior (like page content or status code).

2. How It Starts

It begins when an attacker identifies a user input field (such as a URL parameter or form field) that is passed to a SQL query without proper sanitization. Instead of returning database output directly, the application responds differently to true and false conditions in the query.

By injecting Boolean expressions (like `AND 1=1` or `AND 1=2`), the attacker

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

Email address does not match in our records!

E-Mail Address

Send Password Reset Link

And when you send a correct email address, you should see a different message:

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

To inject the payload, you usually try to break the SQL syntax by adding a single quote ' or a double quote " into the parameter.

Since we don't have access to the application's source code to create a custom payload, we can use common ones like:

```
' OR 1=1 -- //
```

This breaks the SQL query and forces it to return a true condition.

If the payload works correctly, we should see a true response message like this:

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

While Testing this vulnerability via Burp-Suite you can notice that the request is redirected and does not presented the message of send email:

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

So, we have to update the session each time we test a new payload, which takes time and effort.

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

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

- proxy=http://127.0.0.1:8080 Sends traffic through a proxy (e.g., Burp Suite) so you can inspect the full HTTP requests and responses to review it.
- batch Runs in non-interactive mode, automatically answering all prompts.

The tool detected the asterisk (*) in the request and started processing the marked parameter.

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

```
ELSE (SELECT [RANDNUM1] UNION SELECT [RANDNUM2])
```

```
END)
```

```
)
```

A deep dive into the payload:

The tool used the following payload to fetching the databases names:

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

This checks whether the following logic (inside the SELECT CASE) returns 3379. If true the injection is successful. If false the application behaves differently.

4.3 SELECT CASE WHEN (...) THEN 3379 ELSE (SELECT 7129 UNION SELECT 3547):

This is the main Boolean condition:

If the condition is true, return 3379

If false, return multiple values (which causes an error or different behavior)

4.4 MID(...):

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

4.6 SELECT DISTINCT(IFNULL(...)) FROM INFORMATION_SCHEMA.SCHEMATA LIMIT 2,1:

Gets the third schema name (index starts at 0)

CAST(... AS NCHAR) makes sure it's in text format

IFNULL(..., 0x20) replaces NULL with a space character

Final results:

- If the 10th character of the 3rd schema name has ASCII 103, the full condition is true the query returns 3379 the application behaves normally.

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 Yousef Alotaibi

31 followers · 1 following

Follow

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

See all from Yousef Alotaibi

Recommended from Medium

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

A Step-by-Step Guide to Docker Image Optimisation: Reduce Size...

When I first deployed a Node.js app to production using Docker, I was stunned, The...

 6d ago

 710

 18



This new IDE from Google is an absolute game changer

This new IDE from Google is seriously revolutionary.

 Mar 12

 5.3K

 310



☐ Mohsin khan

☐ Cfir Aguston

Bypassing 2FA in a Public Bug

The Forbidden Intel Opcode That

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