SQL Injection

SQL Injection : **SQL injection** is a [code injection](https://en.wikipedia.org/wiki/Code_injection) technique used to [attack](https://en.wikipedia.org/wiki/Attack_(computing)) data-driven applications, in which malicious [SQL](https://en.wikipedia.org/wiki/SQL) statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker).[[1]](https://en.wikipedia.org/wiki/SQL_injection#cite_note-1) SQL injection must exploit a [security vulnerability](https://en.wikipedia.org/wiki/Security_vulnerability) in an application's software, for example, when user input is either incorrectly filtered for [string literal](https://en.wikipedia.org/wiki/String_literal) [escape characters](https://en.wikipedia.org/wiki/Escape_sequence) embedded in SQL statements or user input is not [strongly typed](https://en.wikipedia.org/wiki/Strongly-typed_programming_language) and unexpectedly executed. SQL injection is mostly known as an attack [vector](https://en.wikipedia.org/wiki/Vector_(malware)) for websites but can be used to attack any type of SQL database.

Steps for SQL Injection:

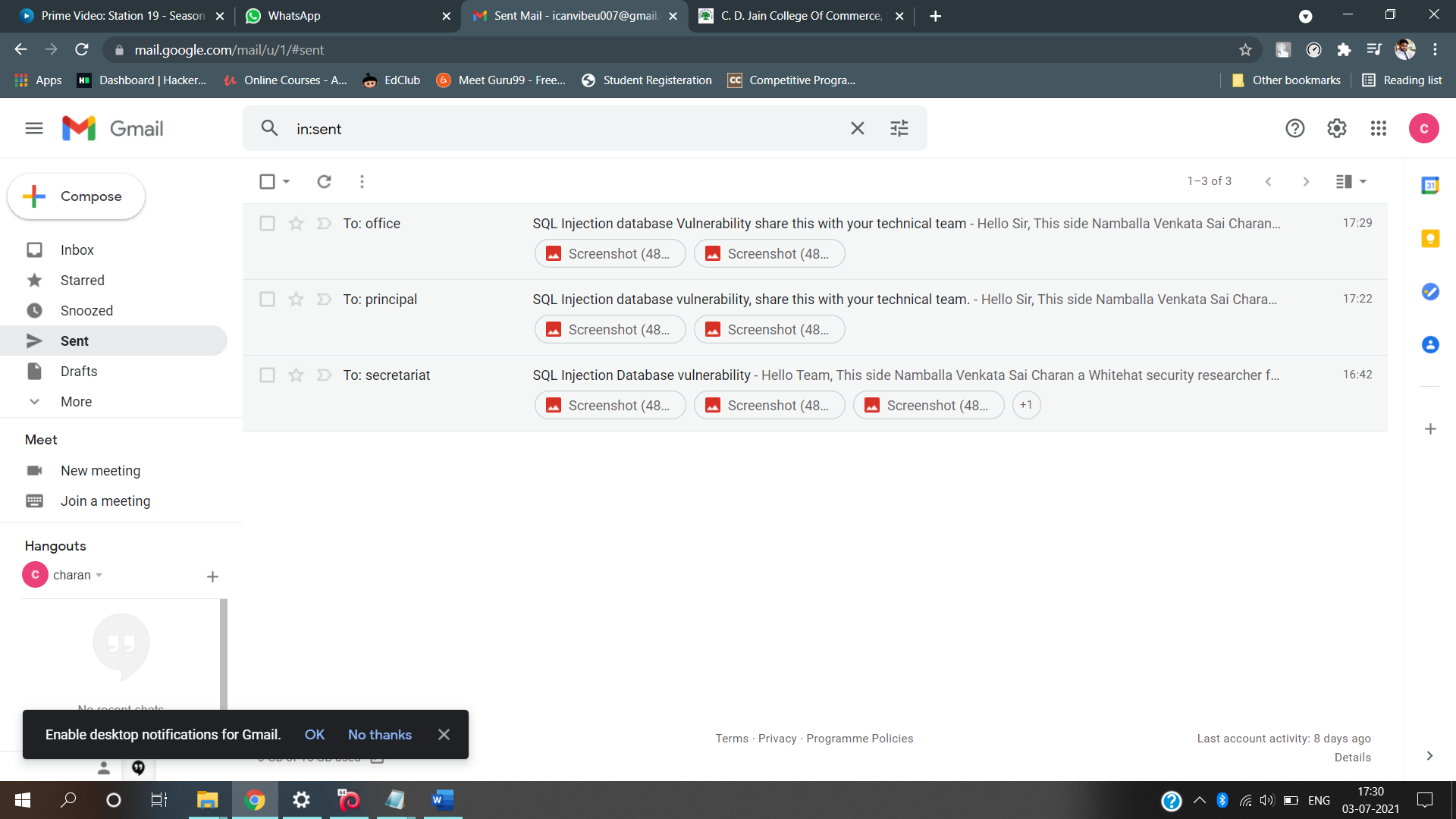
1. Check if the you are able to communicate with the database of the website using symbols like / ‘ “ % ect.
2. If you were able to create an error from database or not.
3. If your able to create an error then type the command “ sqlmap --url <website-name> --dbs”
4. If able to successfully see the names of database then type the command “ sqlmap --url <website-name> --dbs --tables”
5. Report the website to the respective mail.

Links of the websites I got sql injection database vulnerability:

<http://www.asfaa.org/members.php?id=10>

<http://jgec.ac.in/php/showfacde.php?id=23>

Mails I sent to the website contact address to report the vulnerability



Screenshots of the messages after sqlmap is done.

