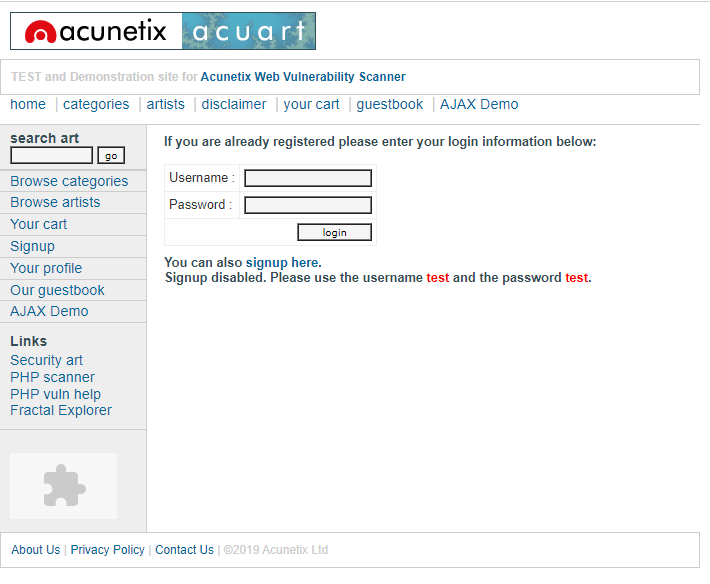
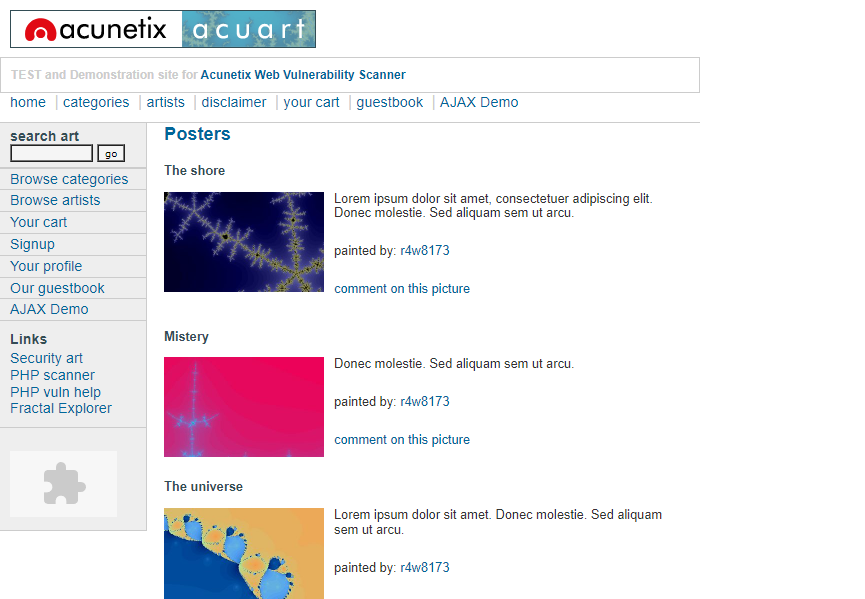
**Sql injection:**

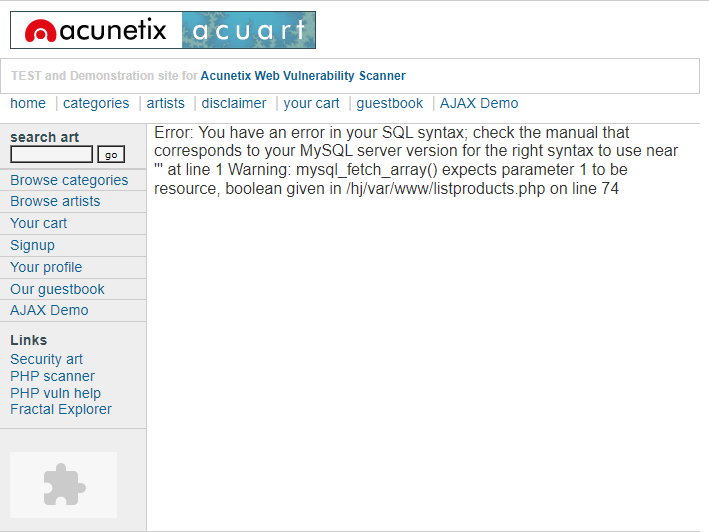
Target: http://testphp.vulnweb.com



I first went to browse categories on the websites and clicked on posters to find the error in the url.



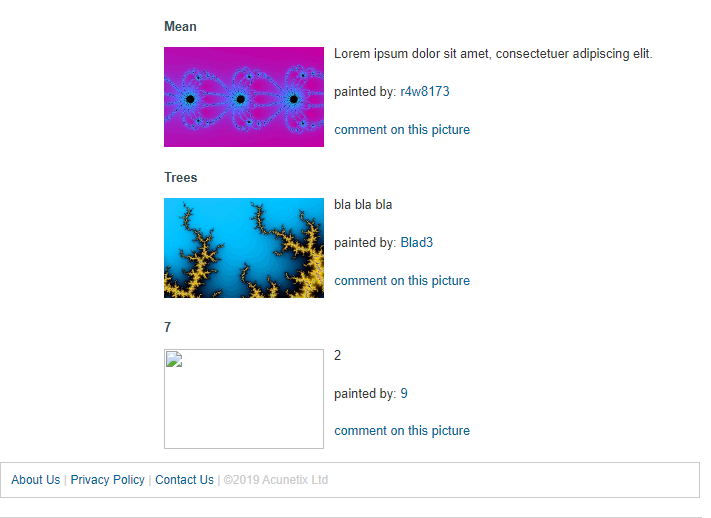
First I tried to add a special character (‘) in the url but it gave error.

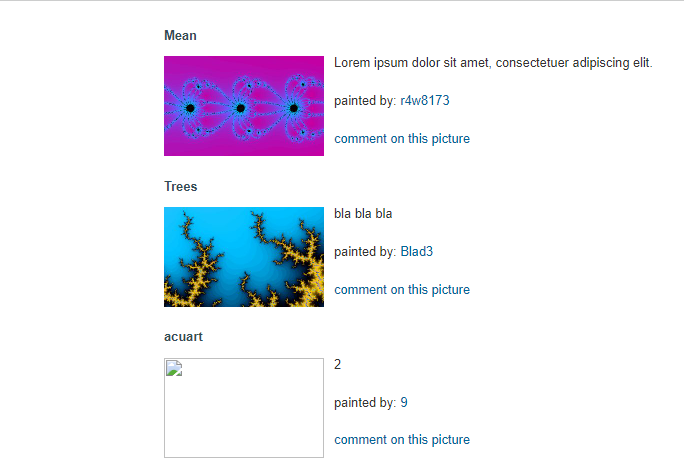


Then I added the command order by in the url with different numbers like 12,15,16,20 but all of them gave error except 11 which means 11 columns are available in public.



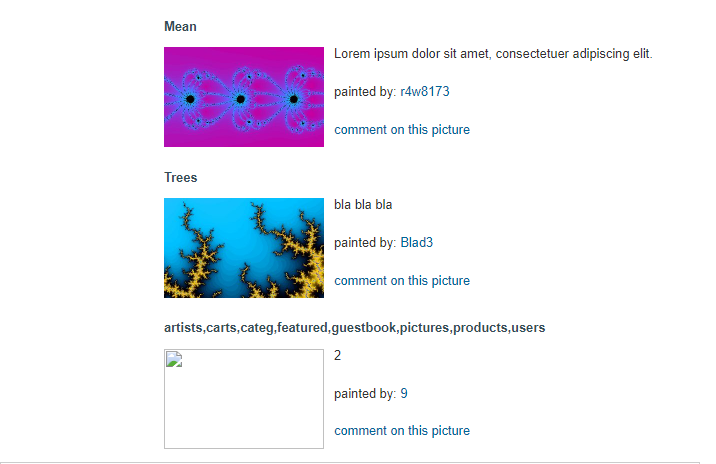
Then I executed the command union select 1,2,3,4,5,6,7,8,9,10,11 in the url . It gave me an extra column at the last with the numbers 7,2 and 9 which means the columns 7,2 and 9 are vulnerable.



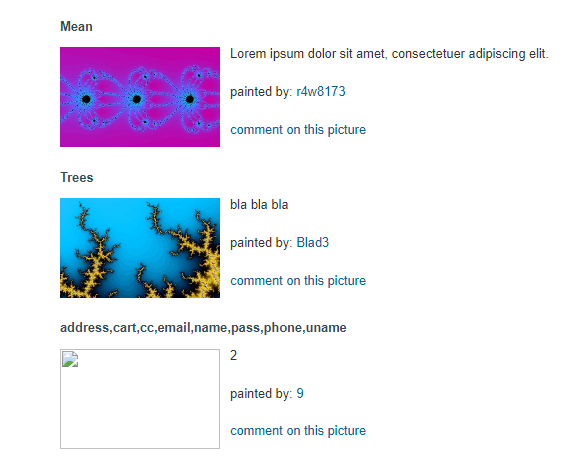
Then to know the database name I replaced 7 with the command database() in the url.

I got the database name as acuart.

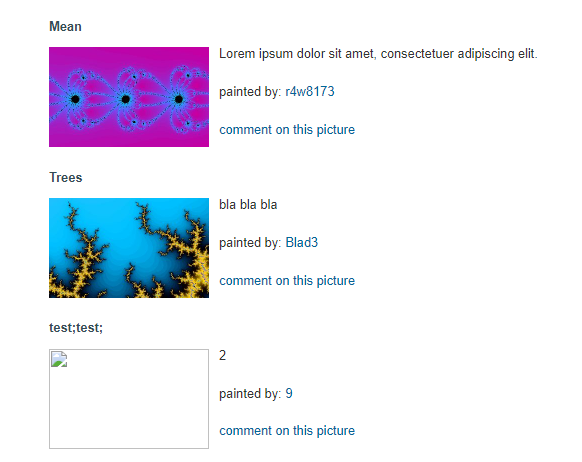
Then I replaced 7 with group\_concat(table\_name) and added from information\_schema.tables where table\_schema=database(). After exceuting this command we got the table names as artists,carts,carteg,featured,guestbook,pictures,products,users.



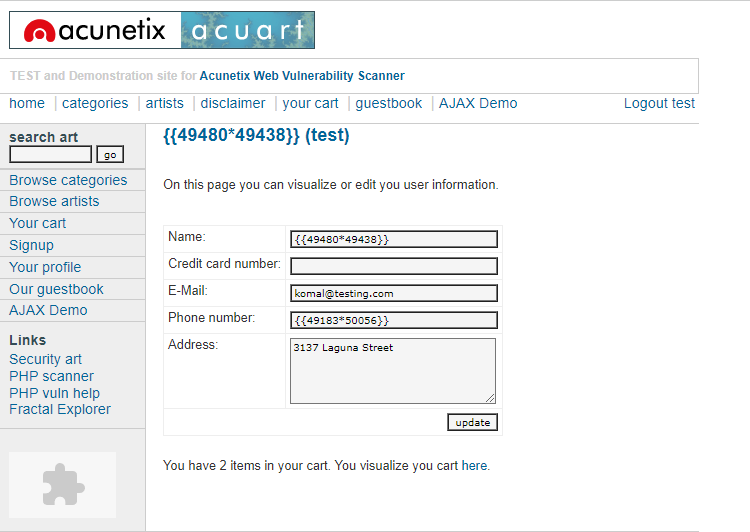
Then I changed table to columns in the url except the last part where i added table\_name=0x7573657273 . By executing this command I got the column names of the users table which are address,cart,cc,email,name,pass,phone,uname.



Then I replaced 7 by group\_concat(uname,pass,email) in the url and added from users at the end of url.



I finally got the username and password as test. I tried to enter the credentials in the website and it worked . This ends our sql injection process.



Threat : if this sql injection was performed by black hat hacker he could have easily used these credentials for the wrong purpose and the website might have been compromised. . All in all , no client’s credentials should be accessible to any unknown person which could compromise the privacy of the client as well as the website.

Solution : the database admin should make sure that the sql commands are not accepted by the users. The network admin should secure the firewall. They may also hire a cyber security analyst to fully secure the website.