

22/04/2022

Thanushree NG

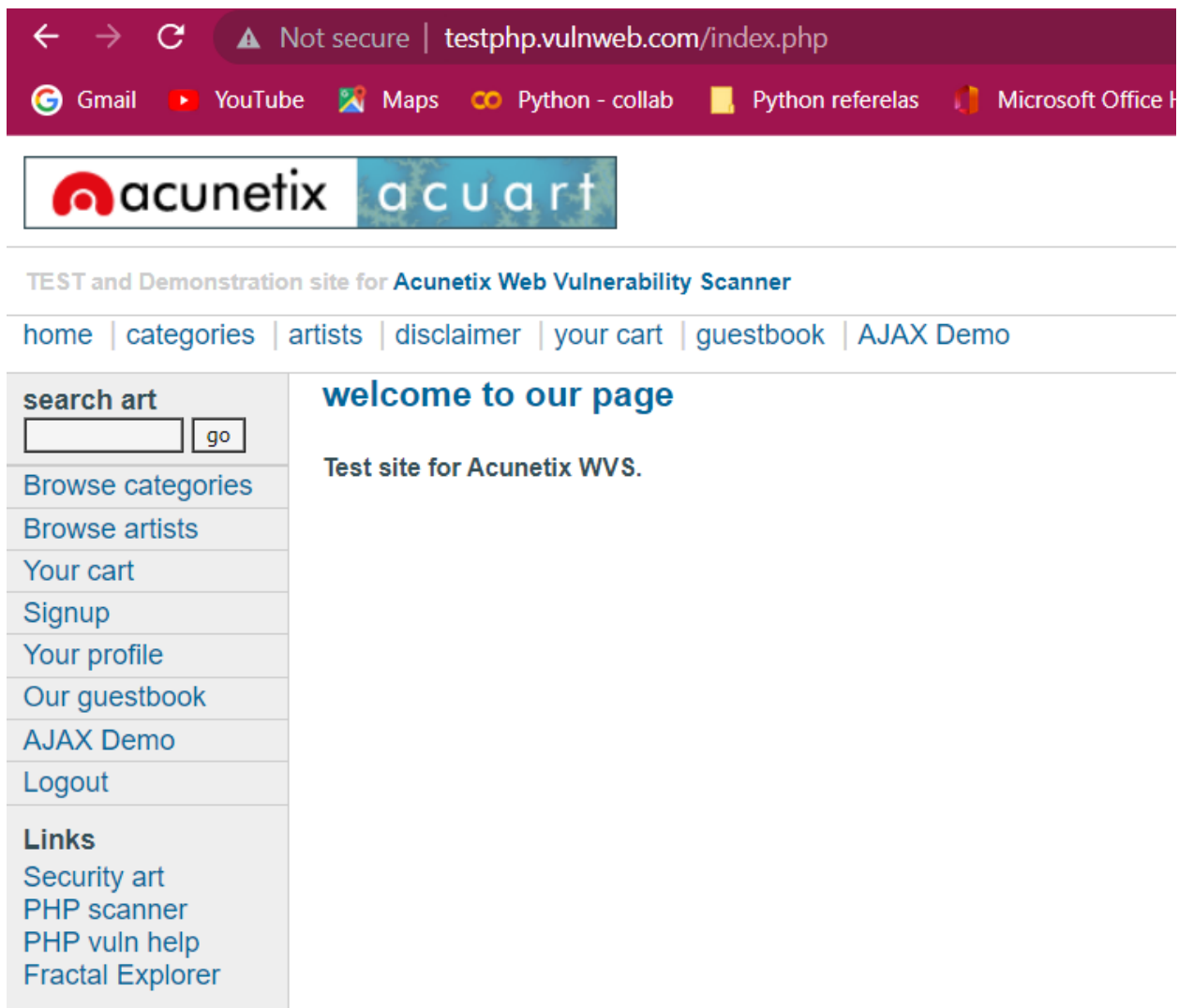
Lab 6:

Explore SQL Injection attacks using vulnerable webpages as per your choice.

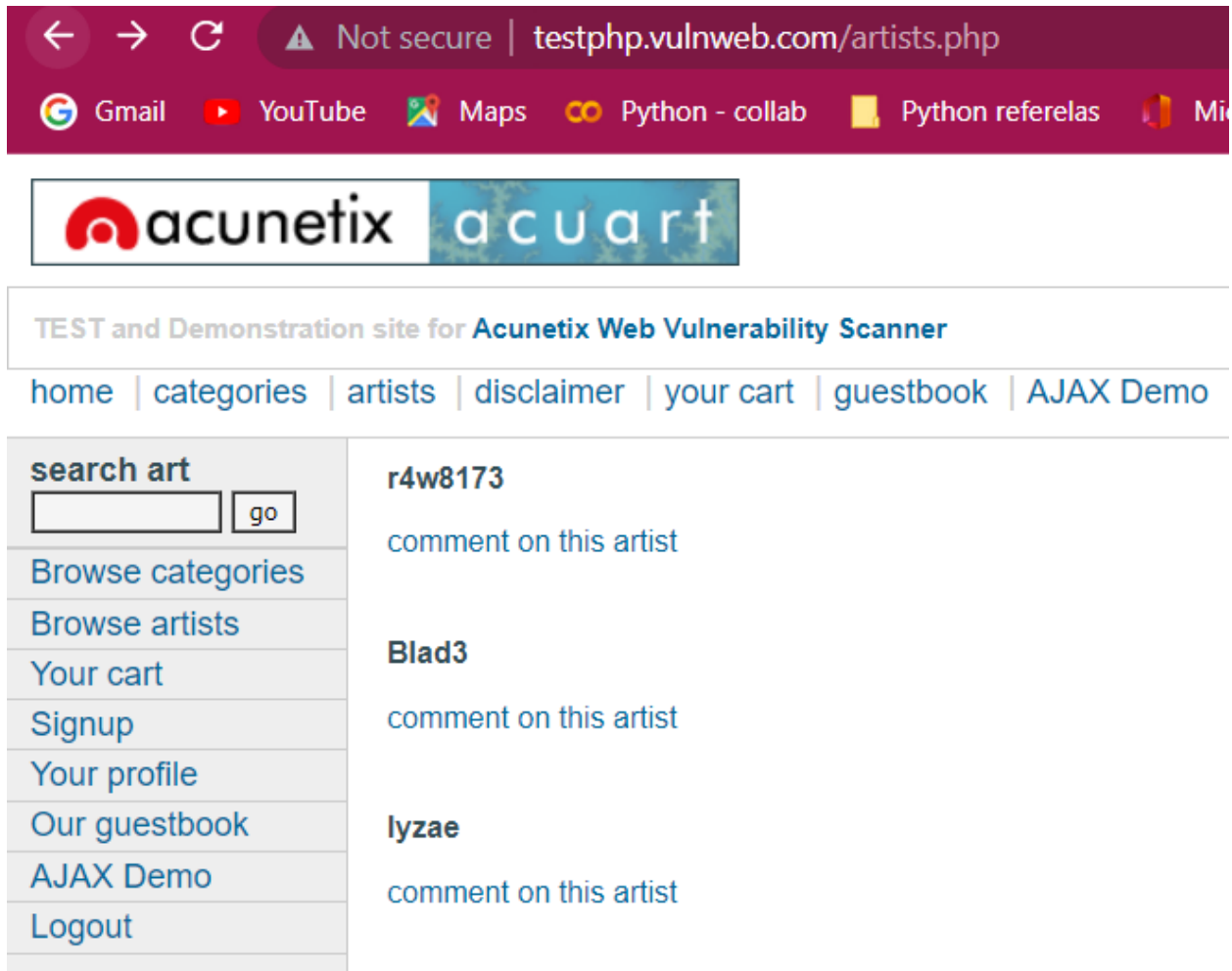
Create report with screenshots.

Task:

1. Selected the website **vulnweb** to explore vulnerability.



2. Browse Artists to check the database usage



The screenshot shows a web browser window with the address bar displaying "testphp.vulnweb.com/artists.php". The browser's address bar also shows "Not secure". The page features a navigation bar with links: home, categories, artists, disclaimer, your cart, guestbook, and AJAX Demo. A search bar is present with the text "search art" and a "go" button. The main content area displays a list of artists: r4w8173, Blad3, and lyzae, each with a "comment on this artist" link. The left sidebar contains a menu with links: Browse categories, Browse artists, Your cart, Signup, Your profile, Our guestbook, AJAX Demo, and Logout.

← → ↻ ⚠ Not secure | testphp.vulnweb.com/artists.php

Gmail YouTube Maps Python - collab Python referelas Mi

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

Logout

r4w8173

comment on this artist

Blad3

comment on this artist

lyzae

comment on this artist

- Checking artist=3 'lyzae'

← → ↻ Not secure | testphp.vulnweb.com/artists.php?artist=3

Gmail YouTube Maps Python - collab Python referelas Microsoft Office Ho... Online learning

acunetix **acuart**

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

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

search art
 go

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

Links
Security art
PHP scanner
PHP vuln help
Fractal Explorer

artist: lyzae

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.

3. To check if the site is vulnerable to SQL injection, add ' at the end of URL:

<http://testphp.vulnweb.com/artists.php?artist=3'>

← → ↻ Not secure | testphp.vulnweb.com/artists.php?artist=3%27

Gmail YouTube Maps Python - collab Python referelas Microsoft Office Ho... Online learning

acunetix **acuart**

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

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

search art
 go

Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook

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

4. The returned response from database is a query which indicates that the site is vulnerable to SQL injection.

Give username as 1' or '1' = '1 so as to bypass authentication.

The condition 1' or '1' = '1 always returns true and hence allowing successful bypass login without actual credentials.



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](#)

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**.

5. Login successful with sql injection:

← → ↻

Not secure | testphp.vulnweb.com/userinfo.php

Gmail

YouTube

Maps

Python - collab

Python referelas

Microsoft Office Ho...

Online learning

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

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

Logout test

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

You have 0 items in your cart. You visualize you cart [here](#).

(test)

On this page you can visualize or edit you user information.

Name:

<h1><marquee>1}}acx{{98991*97996

Credit card number:

if(now())=sysdate(),sleep(15),0)

E-Mail:

1}

Phone number:

555-666-0606

Address:

1acx__\$98991*97996}__:::x

update

1}}acx{{98991*97996