Virtchual’s Flag Quest 2024(Official Write-up)

virtchual · Follow

10 min read · Just now

--

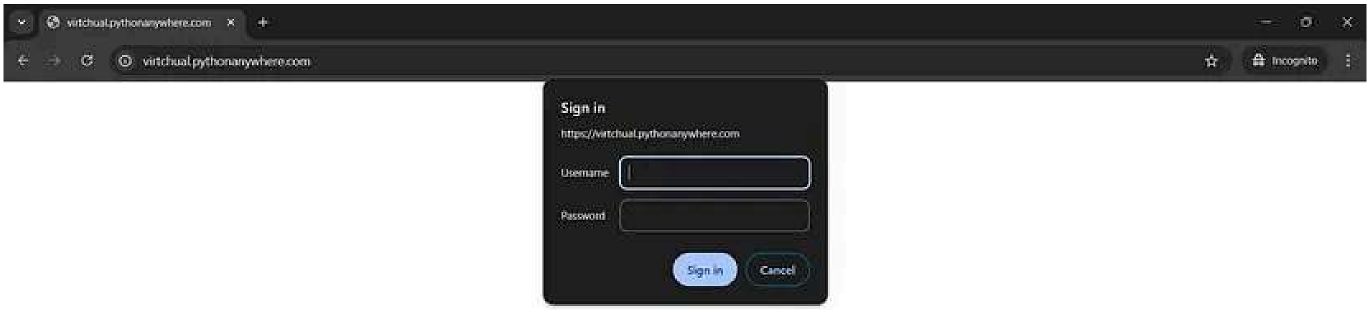
Start

After Clicking ‘Start’ above , u get navigated to the below the URL

“https://virtchual.pythonanywhere.com/”

Do not worry, its safe.

As Safe as an Anaconda 😋


virtchual.pythonanywhere.com
virtchual.pythonanywhere.com
Incognito
Sign in
https://virtchual.pythonanywhere.com
Username
Password
Sign in
Cancel

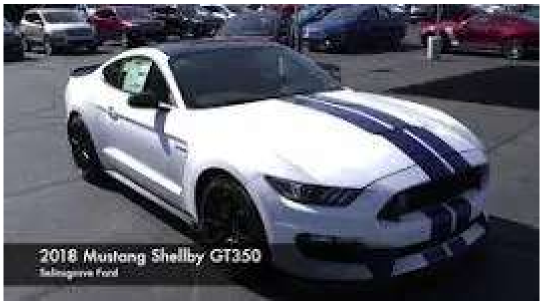
‘Sign in’ Prompt

Now the first hurdle.

As u can see in the above image ,u get prompted with a ‘Sign in’ window for ‘Username’ and ‘Password’, which obviously u don’t know.

Even i don’t know.

Lol, just kidding.



Password.jpeg

The above image is very crucial for solving this hurdle.

I'll let u guys guess the 'Username'.

Hint: Its strictly alphabetic.

Lets focus on the 'Password'.

Hmmmmm

Hmm

……

……

……

Ahh! Yes, 'Password'.

I would've downloaded the image, if i were u.

You just need one Linux tool to solve this.

Some people would've already guessed it.

Yes, its 'ExifTool'

Naaaah, i'm just messing around.

It's actually 'Steghide'.

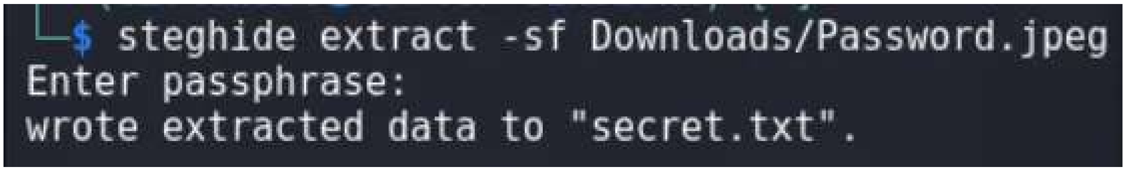
No joke this time.

Well, if u've the tool that's fine. 'Tool junkies' can skip the next part and do what u'r supposed to do.

And for the rest of them,

Type this command:

steghide extract -sf Password.jpeg



```
└─$ steghide extract -sf Downloads/Password.jpeg
Enter passphrase:
wrote extracted data to "secret.txt".
```

steghide

I know, I know. 'Password.jpeg' is usually located in Downloads/Password.jpeg.

When prompted for a passphrase, **press Enter** to proceed .

```
$ steghide extract -sf Downloads/Password.jpeg
```

```
Enter passphrase: Press Enter⏎
```

```
wrote extracted data to "secret.txt".
```

```
$ cat secret.txt
[redacted]
```

If u don't have 'Steghide' or u don't run linux then get some life.

Just jesting. 😅

or am I? 🗿🗿🗿

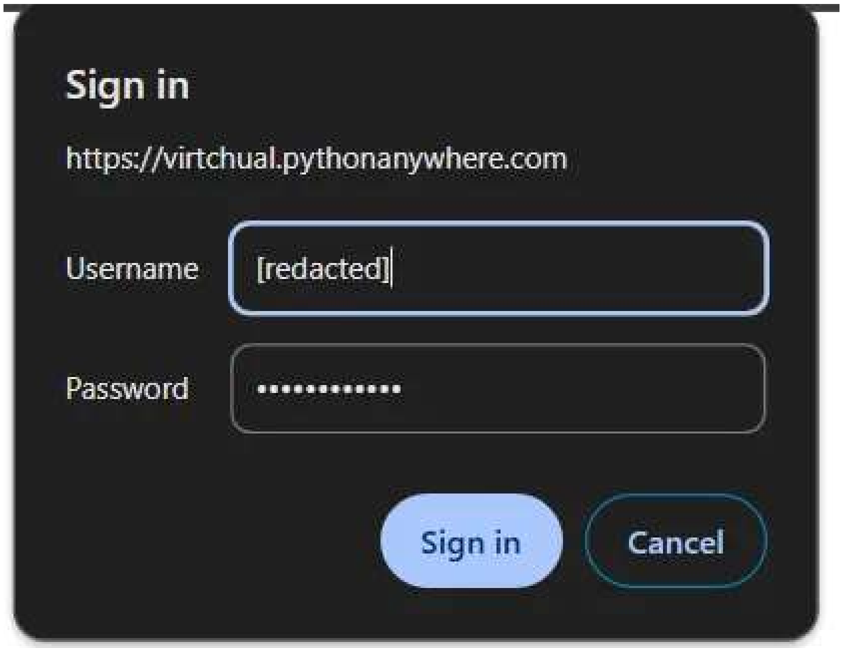
Ok ! Back to 'Steghide' alterantive.

Just go here 👇 👇 👇 👇

https://futureboy.us/stegano/decinput.html

Upload the image and submit.

By now, u should've guessed the 'Username'



Sign in

https://virtchual.pythonanywhere.com

Username [redacted]

Password •••••••••••••

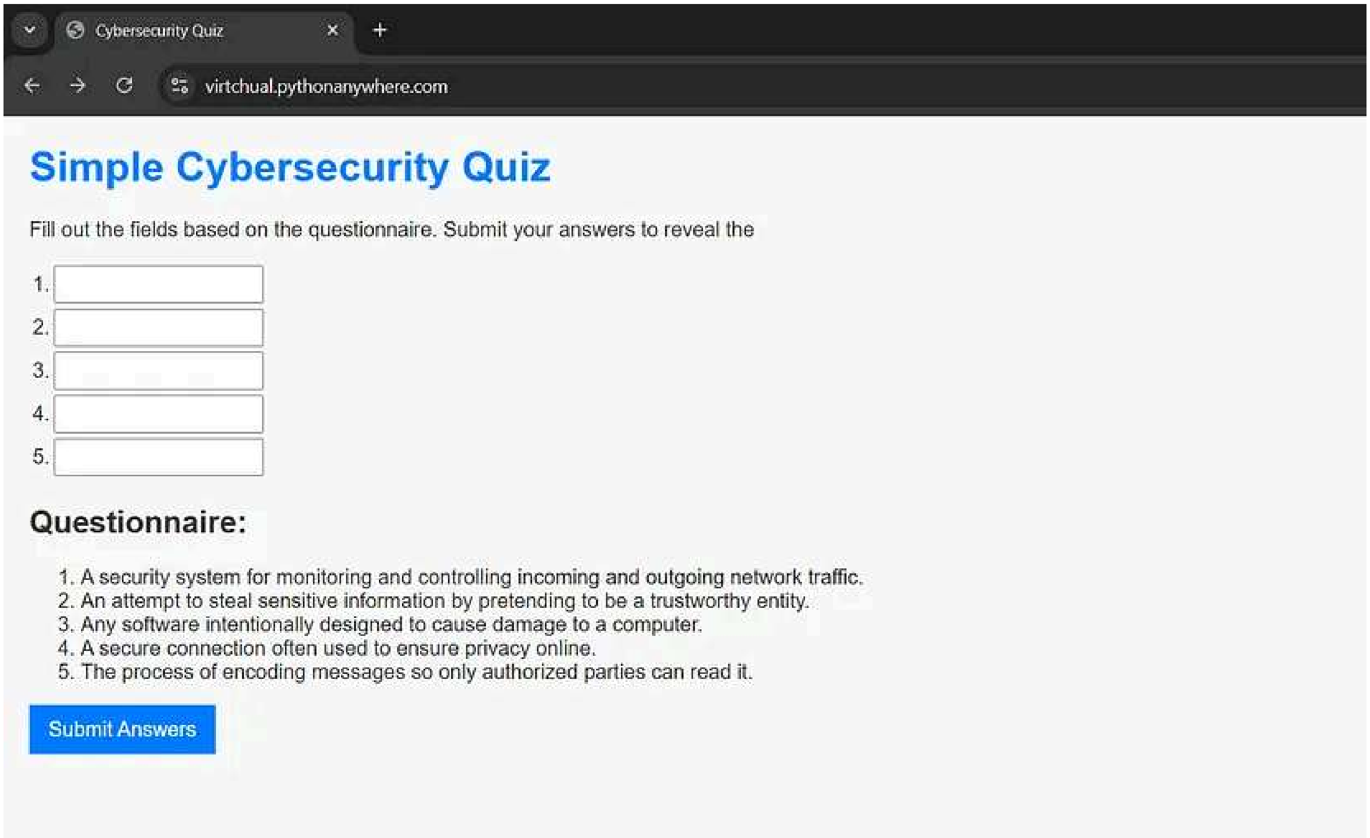
Sign in

No, its not "[redacted]" 😭 😭

Its 👇 👇

'Starts with s and ends with y'

Now click on 'Sign in'



Simple Cybersecurity Quiz

Fill out the fields based on the questionnaire. Submit your answers to reveal the

1.
2.
3.
4.
5.

Questionnaire:

1. A security system for monitoring and controlling incoming and outgoing network traffic.
2. An attempt to steal sensitive information by pretending to be a trustworthy entity.
3. Any software intentionally designed to cause damage to a computer.
4. A secure connection often used to ensure privacy online.
5. The process of encoding messages so only authorized parties can read it.

Cybersecurity Quiz

Fill the fields with right answers and submit them.

Got ur first flag?

5 more to go.

Yes, there are totally 6 flags.(5 flags + 1 Bonus flag)

Recon time!!!

If i were u ,i would do the directory enumeration.

Yes ,i suggest u either use nikto or dirsearch.

```
nikto -h https://virtchual.pythonanywhere.com/ -id username:password -output sca
```

```
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          35.173.69.207
+ Target Hostname:    virtchual.pythonanywhere.com
+ Target Port:        443
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /CN=*.pythonanywhere.com
                   Altnames: *.pythonanywhere.com
                   Ciphers:  TLS_AES_256_GCM_SHA384
                   Issuer:   /C=US/O=Let's Encrypt/CN=E5
+ Start Time:         2024-12-29 21:16:51 (GMT5.5)
---------------------------------------------------------------------------
+ Server: PythonAnywhere
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://d
+ /: The site uses TLS and the Strict-Transport-Security HTTP header is not defi
+ /: The X-Content-Type-Options header is not set. This could allow the user age
+ / - Requires Authentication for realm 'Default Realm'
+ Successfully authenticated to realm 'Default Realm' with user-supplied credent
+ /cgi-bin/: There appears to be Clacks Overhead on the server and the message i
+ /robots.txt: Entry '/static/styles.css' is returned a non-forbidden or redirec
+ /robots.txt: Entry '/admin/' is returned a non-forbidden or redirect HTTP code
+ /robots.txt: contains 2 entries which should be manually viewed. See: https://
+ /: The Content-Encoding header is set to "deflate" which may mean that the ser
+ Server is using a wildcard certificate: *.pythonanywhere.com. See: https://en.
+ OPTIONS: Allowed HTTP Methods: GET .
+ /admin/: This might be interesting.
```

```
dirsearch -u https://virtchual.pythonanywhere.com/ --auth username:password --au
```

```
  _|. _ _  _  _  _ _|_    v0.4.3
 (_||| _) (/_(_|| (_| )
Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 | Wordlist

Output File: /home/virtchual/reports/https_virtchual.pythonanywhere.com/__24-12-

Target: https://virtchual.pythonanywhere.com/

[12:14:33] Starting:
[12:15:06] 200 -  600B  - /admin/
[12:15:32] 200 -    2KB - /cgi-bin/
[12:15:33] 405 -  753B  - /check
[12:16:26] 200 -  391B  - /robots.txt
[12:16:34] 404 -  754B  - /static/api/swagger.yaml
[12:16:34] 404 -  754B  - /static/api/swagger.json
[12:16:34] 404 -  746B  - /static/dump.sql

Task Completed
```

Now u only need to traverse these 3 paths :

1. /admin/

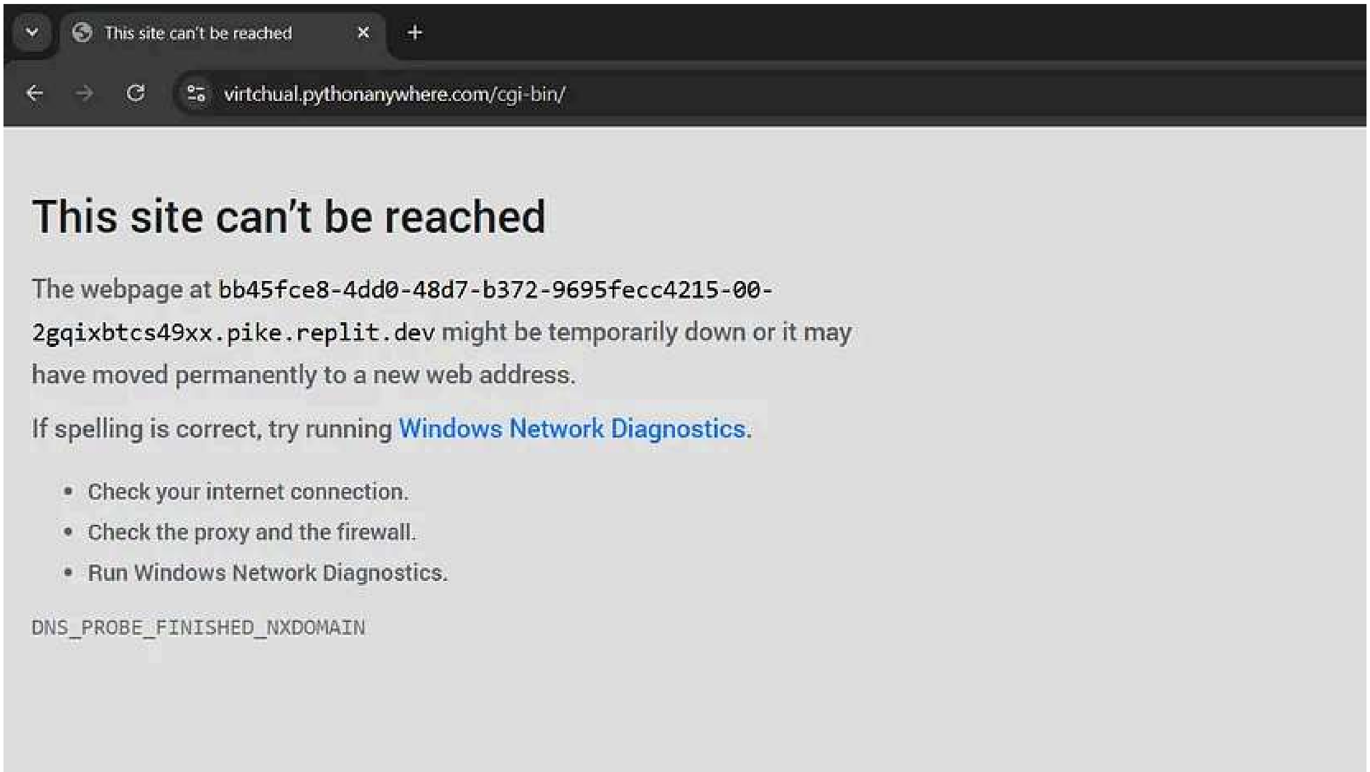
2. /cgi-bin/

3. /robots.txt

I’ll start with /cgi-bin/

2. /cgi-bin/

i.e https://virtchual.pythonanywhere.com/cgi-bin/


This site can't be reached
virtchual.pythonanywhere.com/cgi-bin/

This site can't be reached

The webpage at bb45fce8-4dd0-48d7-b372-9695fecc4215-00-2gqixbtcs49xx.pike.replit.dev might be temporarily down or it may have moved permanently to a new web address.

If spelling is correct, try running Windows Network Diagnostics.

- Check your internet connection.
- Check the proxy and the firewall.
- Run Windows Network Diagnostics.

DNS_PROBE_FINISHED_NXDOMAIN

Do not panic.

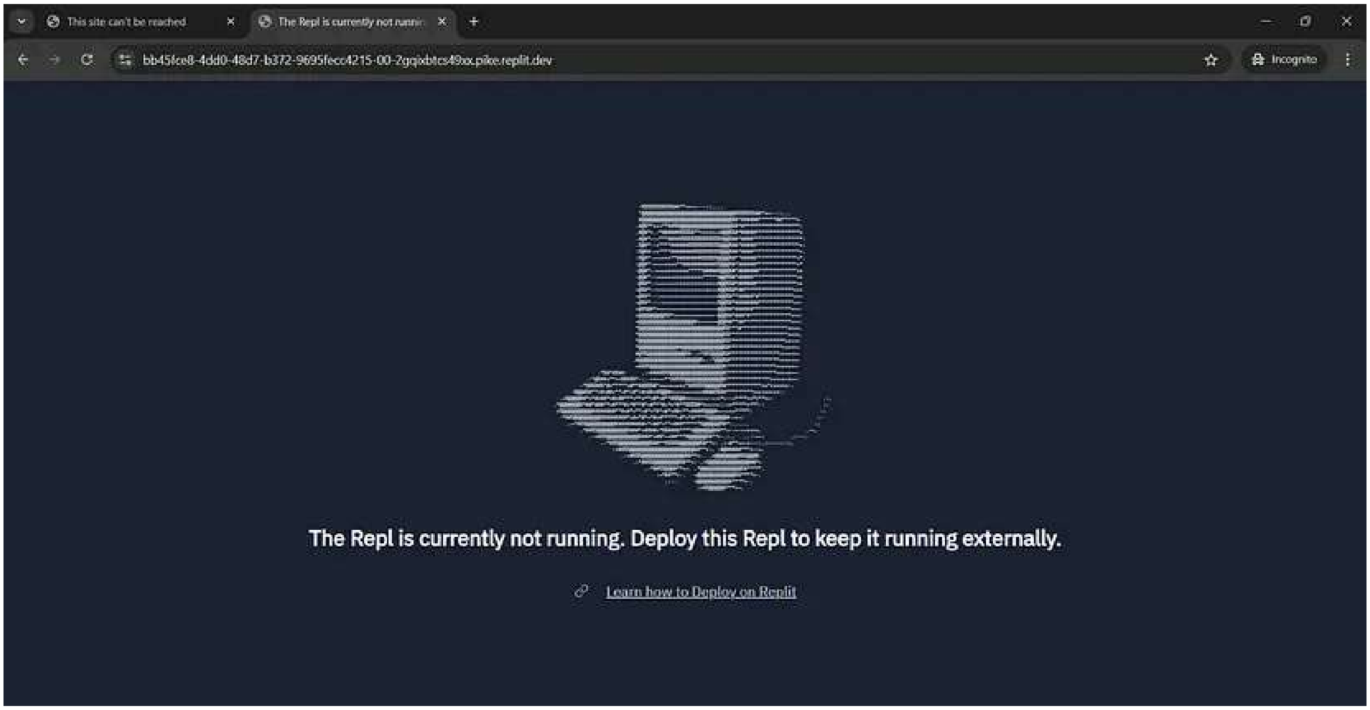
This is just a mimic page of the actual 'This site can't be reached'.

But there is something very wrong with this page if u've noticed it.

‘bb45fce8–4dd0–48d7-b372–9695fecc4215–00–2gqixbtcs49xx.pike.replit.dev’

Yes, it was supposed to be ‘https://virtchual.pythonanywhere.com/cgi-bin/’

Lets head there then.

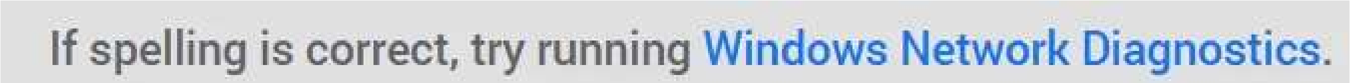

This site can't be reached
The Repl is currently not runnin
bb45fce8-4dd0-48d7-b372-9695fecc4215-00-2gqixbtcs49xx.pike.replit.dev
Incognito

The Repl is currently not running. Deploy this Repl to keep it running externally.

Learn how to Deploy on Replit

Relax, even I know this page is a dead end.

Lets head back to our "https://virtchual.pythonanywhere.com/cgi-bin/" because there is something else we can try.

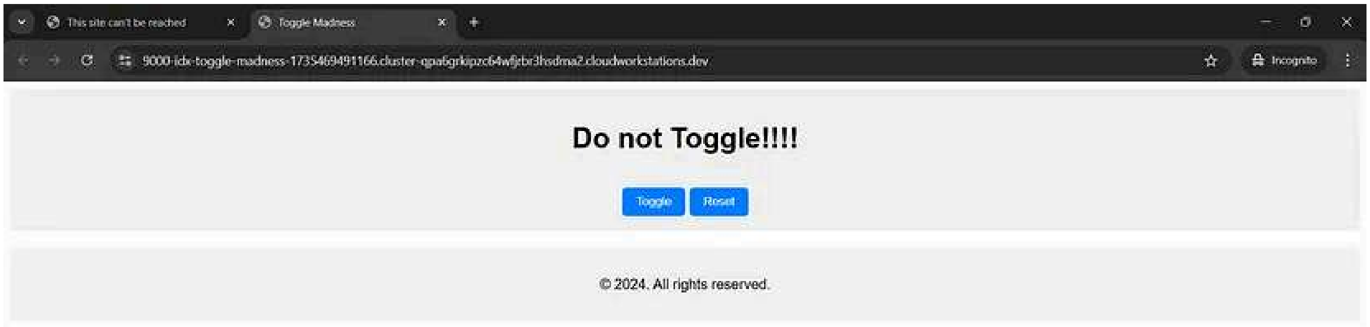


If spelling is correct, try running Windows Network Diagnostics.

Troubleshooting

What's this?

Lets run it


This site can't be reached
Toggle Madness
9000-idx-toggle-madness-1735469491166.cluster-qpa6grkipzc64wfjrbr3hsdma2.cloudworkstations.dev
Incognito
Toggle
Reset

Do not Toggle!!!!

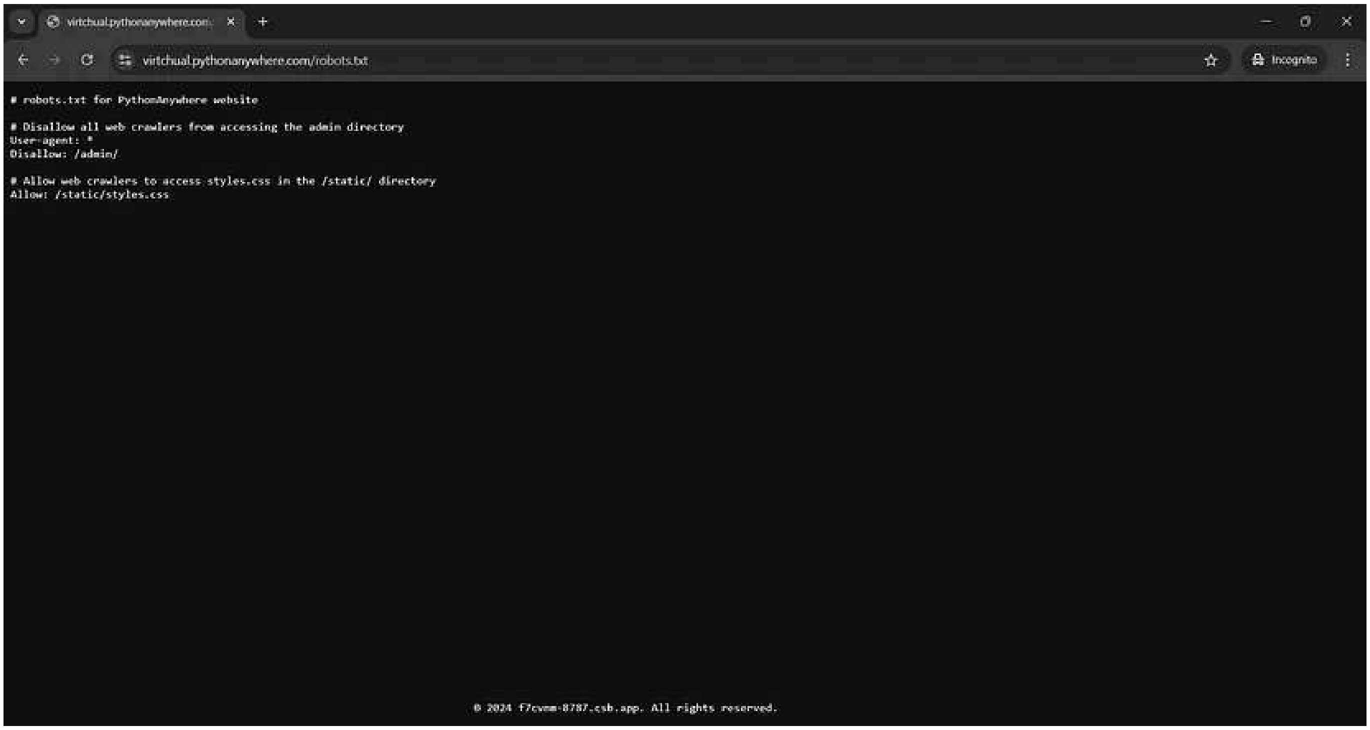
© 2024. All rights reserved.

I’ll let ur *impostor instincts* decide what to do next. 👀

Now that /cgi-bin/ is either complete or left to be completed, let’s head over to our next path.

3. /robots.txt

i.e https://virtchual.pythonanywhere.com/robots.txt


virtchual.pythonanywhere.com/
virtchual.pythonanywhere.com/robots.txt
Incognito

```
# robots.txt for PythonAnywhere website

# Disallow all web crawlers from accessing the admin directory
User-agent: *
Disallow: /admin/

# Allow web crawlers to access styles.css in the /static/ directory
Allow: /static/styles.css
```

© 2024 f7cvmm-8787.csb.app. All rights reserved.

“Once again, there’s something here that shouldn’t be here.”

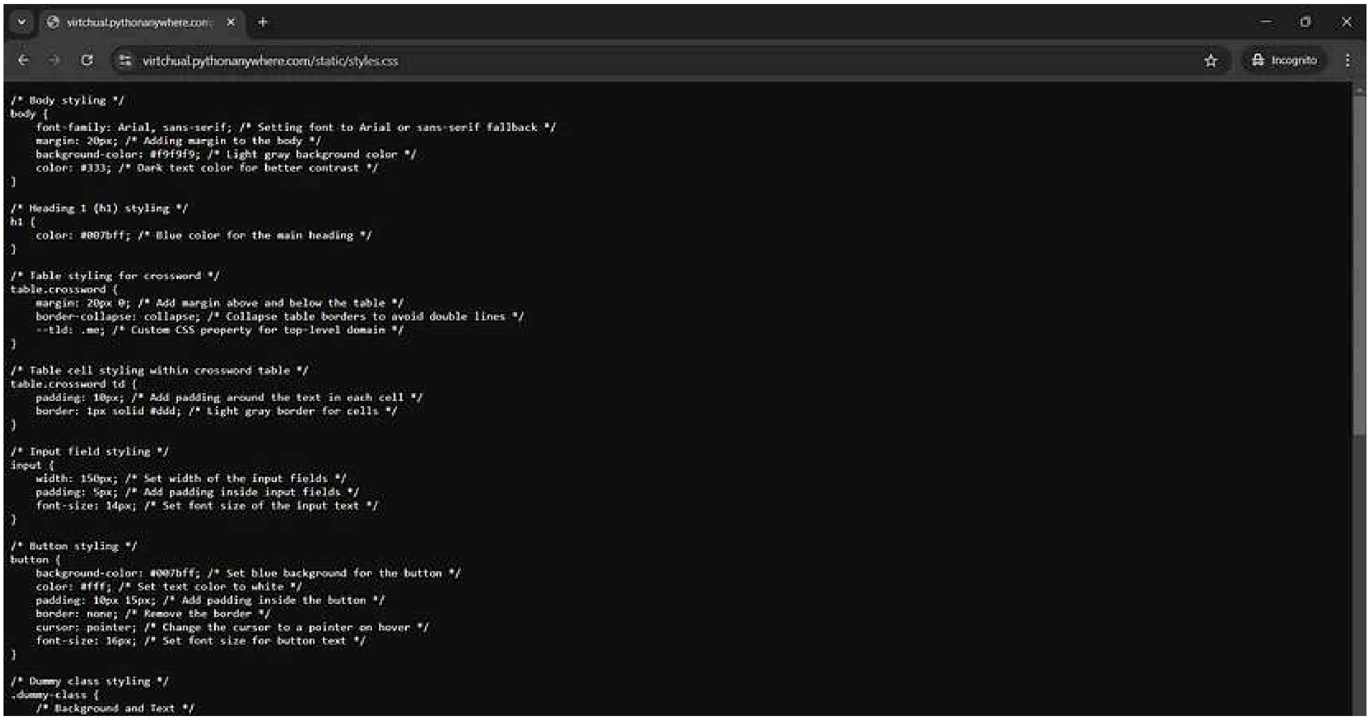
But before going there , lets read the robots.txt.

```
# robots.txt for PythonAnywhere website

# Disallow all web crawlers from accessing the admin directory
User-agent: *
Disallow: /admin/

# Allow web crawlers to access styles.css in the /static/ directory
Allow: /static/styles.css
```

Well something is allowed.

Then we are definitely exploring it.

https://virtchual.pythonanywhere.com/static/styles.css


virtchual.pythonanywhere.com
virtchual.pythonanywhere.com/static/styles.css
Incognito

```
/* Body styling */
body {
    font-family: Arial, sans-serif; /* Setting font to Arial or sans-serif fallback */
    margin: 20px; /* Adding margin to the body */
    background-color: #f9f9f9; /* Light gray background color */
    color: #333; /* Dark text color for better contrast */
}

/* Heading 1 (h1) styling */
h1 {
    color: #007bff; /* Blue color for the main heading */
}

/* Table styling for crossword */
table.crossword {
    margin: 20px 0; /* Add margin above and below the table */
    border-collapse: collapse; /* Collapse table borders to avoid double lines */
    --tld: .me; /* Custom CSS property for top-level domain */
}

/* Table cell styling within crossword table */
table.crossword td {
    padding: 10px; /* Add padding around the text in each cell */
    border: 1px solid #ddd; /* Light gray border for cells */
}

/* Input field styling */
input {
    width: 150px; /* Set width of the input fields */
    padding: 5px; /* Add padding inside input fields */
    font-size: 14px; /* Set font size of the input text */
}

/* Button styling */
button {
    background-color: #007bff; /* Set blue background for the button */
    color: #fff; /* Set text color to white */
    padding: 10px 15px; /* Add padding inside the button */
    border: none; /* Remove the border */
    cursor: pointer; /* Change the cursor to a pointer on hover */
    font-size: 16px; /* Set font size for button text */
}

/* Dummy class styling */
.dummy-class {
    /* Background and Text */
```

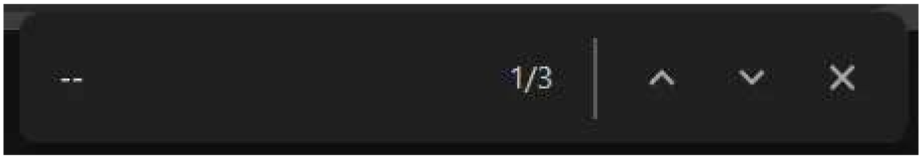
styles.css

```
/* Body styling */
body {
    font-family: Arial, sans-serif; /* Setting font to Arial or sans-serif fallb
    margin: 20px; /* Adding margin to the body */
    background-color: #f9f9f9; /* Light gray background color */
    color: #333; /* Dark text color for better contrast */
}

/* Heading 1 (h1) styling */
h1 {
    color: #007bff; /* Blue color for the main heading */
}

/* Table styling for quiz */
table.quiz {
    margin: 20px 0; /* Add margin above and below the table */
    border-collapse: collapse; /* Collapse table borders to avoid double lines *
    --tld: .me; /* Custom CSS property for top-level domain */
}

/* Table cell styling within quiz table */
table.quiz td {
    padding: 10px; /* Add padding around the text in each cell */
    border: 1px solid #ddd; /* Light gray border for cells */
}
```

```
    /* Input field styling */
    input {
        width: 150px; /* Set width of the input fields */
        padding: 5px; /* Add padding inside input fields */
        font-size: 14px; /* Set font size of the input text */
    }

    /* Button styling */
    button {
        background-color: #007bff; /* Set blue background for the button */
        color: #fff; /* Set text color to white */
        padding: 10px 15px; /* Add padding inside the button */
        border: none; /* Remove the border */
        cursor: pointer; /* Change the cursor to a pointer on hover */
        font-size: 16px; /* Set font size for button text */
    }

    /* Dummy class styling */
    .dummy-class {
        /* Background and Text */
        background-color: #f0f0f0; /* Light gray background */
        color: #333; /* Dark text color for contrast */
        --bare-domain: glitch.me; /* Custom CSS property for domain */

        /* Dimensions */
        width: 300px; /* Set width */
        height: 150px; /* Set height */

        /* Border and Shadow */
        border: 1px solid #ccc; /* Light border color */
        border-radius: 10px; /* Round corners */
        box-shadow: 0px 4px 6px rgba(0, 0, 0, 0.1); /* Apply subtle shadow */

        /* Font */
        font-family: 'Arial', sans-serif; /* Use Arial font for text */
        font-size: 16px; /* Set font size */

        /* Layout */
        display: flex; /* Enable Flexbox for layout */
        justify-content: center; /* Center content horizontally */
        align-items: center; /* Center content vertically */

        /* Hover Effects */
        transition: background-color 0.3s, transform 0.3s; /* Smooth transition for
        --prefix-domain: pattern-wave-trail; /* Custom CSS property for subdomain */
    }

    /* Dummy class hover effect */
    .dummy-class:hover {
        background-color: #007bff; /* Change background color to blue on hover */
        color: white; /* Change text color to white */
        transform: scale(1.05); /* Slightly increase the size on hover */
    }

    /* Button hover effect */
    button:hover {
        background-color: #0056b3; /* Change background to a darker blue on hover */


    }
```

I'm gonna be direct and on to the point from now on and no more yapping.

Press Ctrl + F and search ' --'

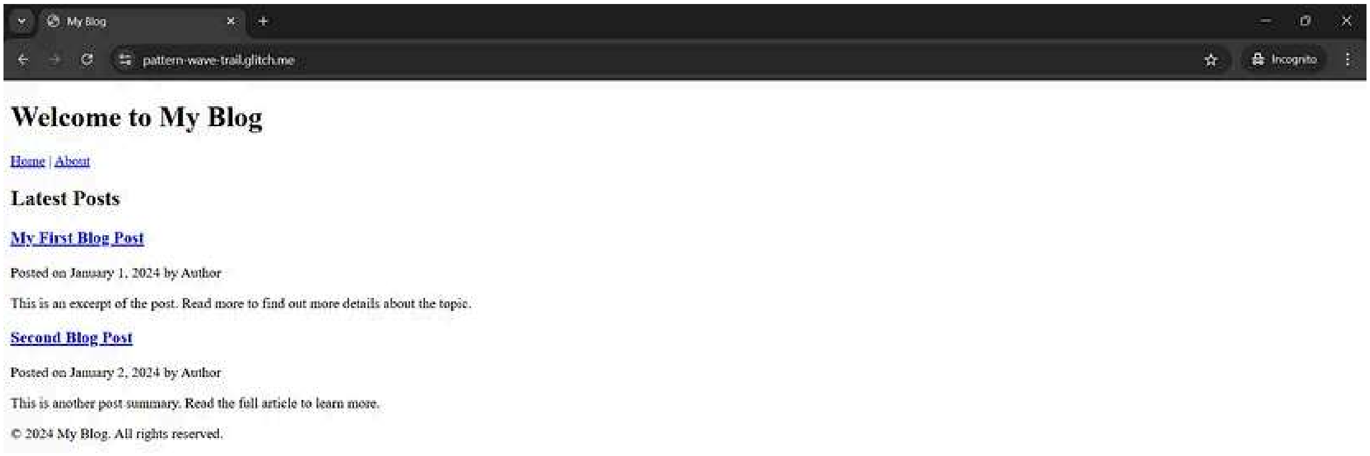


--

```
    --tld: .me; /* Custom CSS property for top-level domain */
    --bare-domain: glitch.me; /* Custom CSS property for domain */
    --prefix-domain: pattern-wave-trail; /* Custom CSS property for subdomain */
```

Combine them and u get this 👇

Go to https://pattern-wave-trail.glitch.me/



Welcome to My Blog

Home | About

Latest Posts

My First Blog Post

Posted on January 1, 2024 by Author

This is an excerpt of the post. Read more to find out more details about the topic.

Second Blog Post

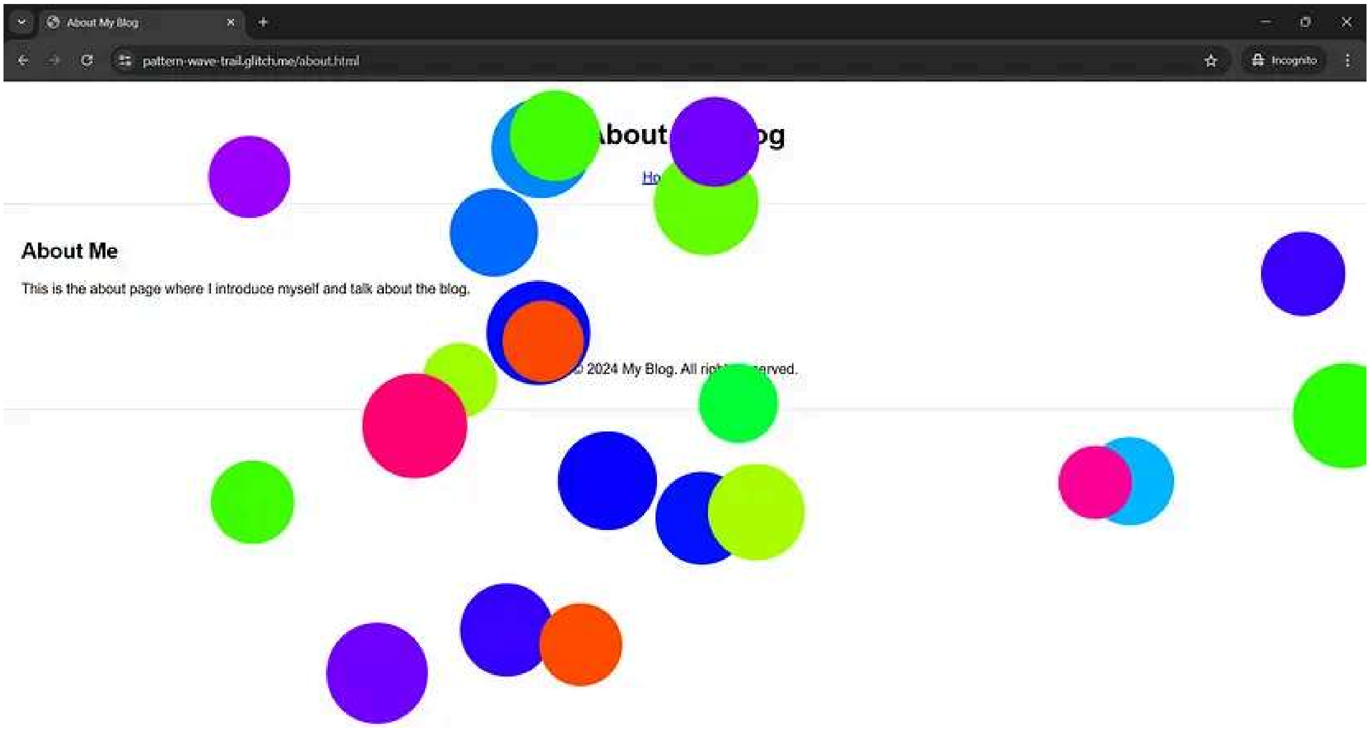
Posted on January 2, 2024 by Author

This is another post summary. Read the full article to learn more.

© 2024 My Blog. All rights reserved.

Blog

Go to 'About' section.



About Me

This is the about page where I introduce myself and talk about the blog.

© 2024 My Blog. All righ erved.

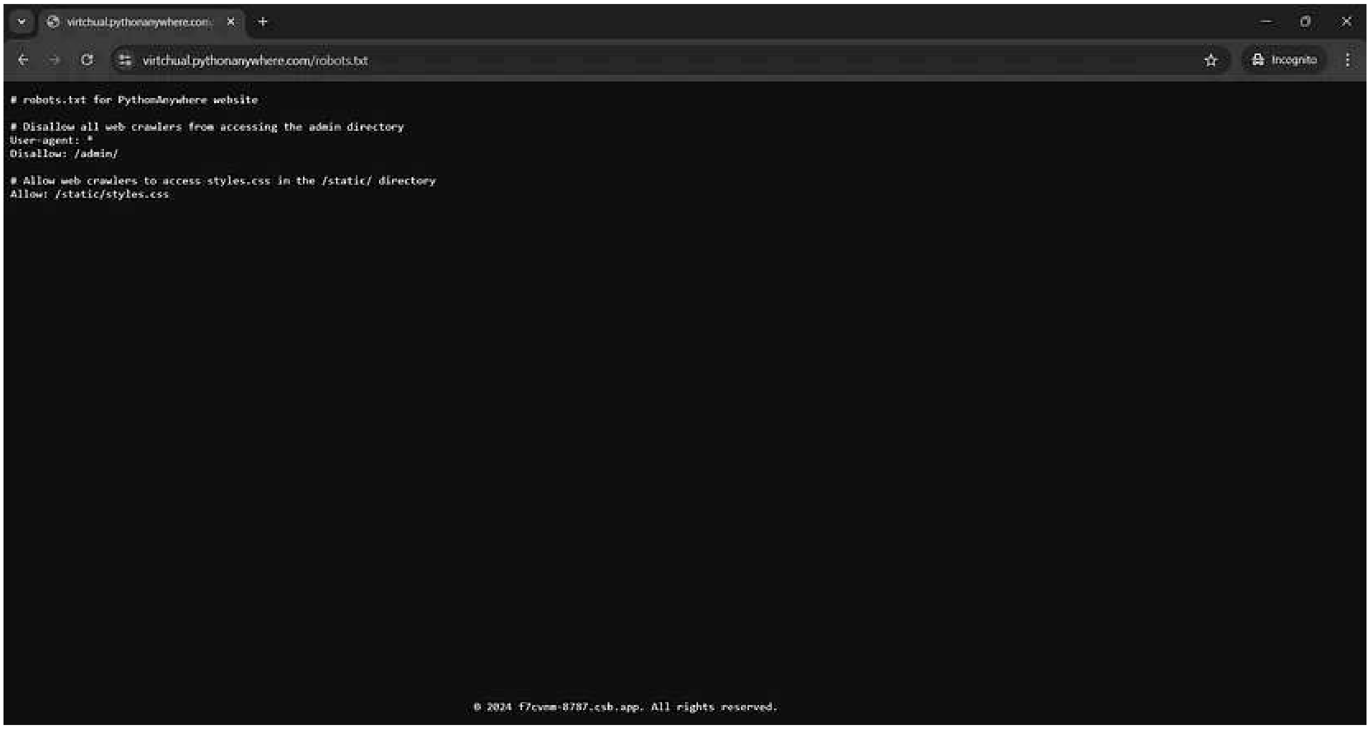
Bubbles Burster

Now u need to click on each colored bubble or whatever u call it to burst /pop them.

After bursting all those bubbles u get a flag.

Now lets head back to robots.txt.

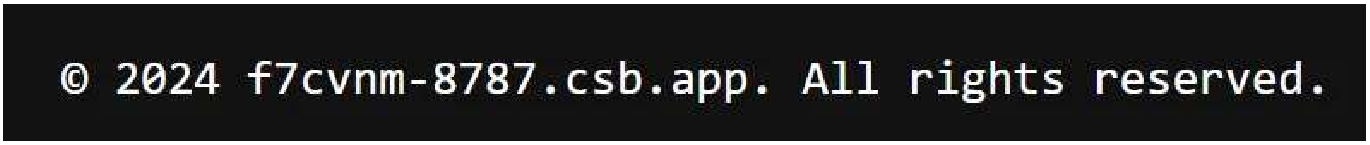
https://virtchual.pythonanywhere.com/robots.txt


virtchual.pythonanywhere.com
virtchual.pythonanywhere.com/robots.txt
Incognito

```
# robots.txt for PythonAnywhere website

# Disallow all web crawlers from accessing the admin directory
User-agent: *
Disallow: /admin/

# Allow web crawlers to access styles.css in the /static/ directory
Allow: /static/styles.css
```

```
© 2024 f7cvnm-8787.csb.app. All rights reserved.
```

At the bottom u see 👇 👇 which is very uncommon.

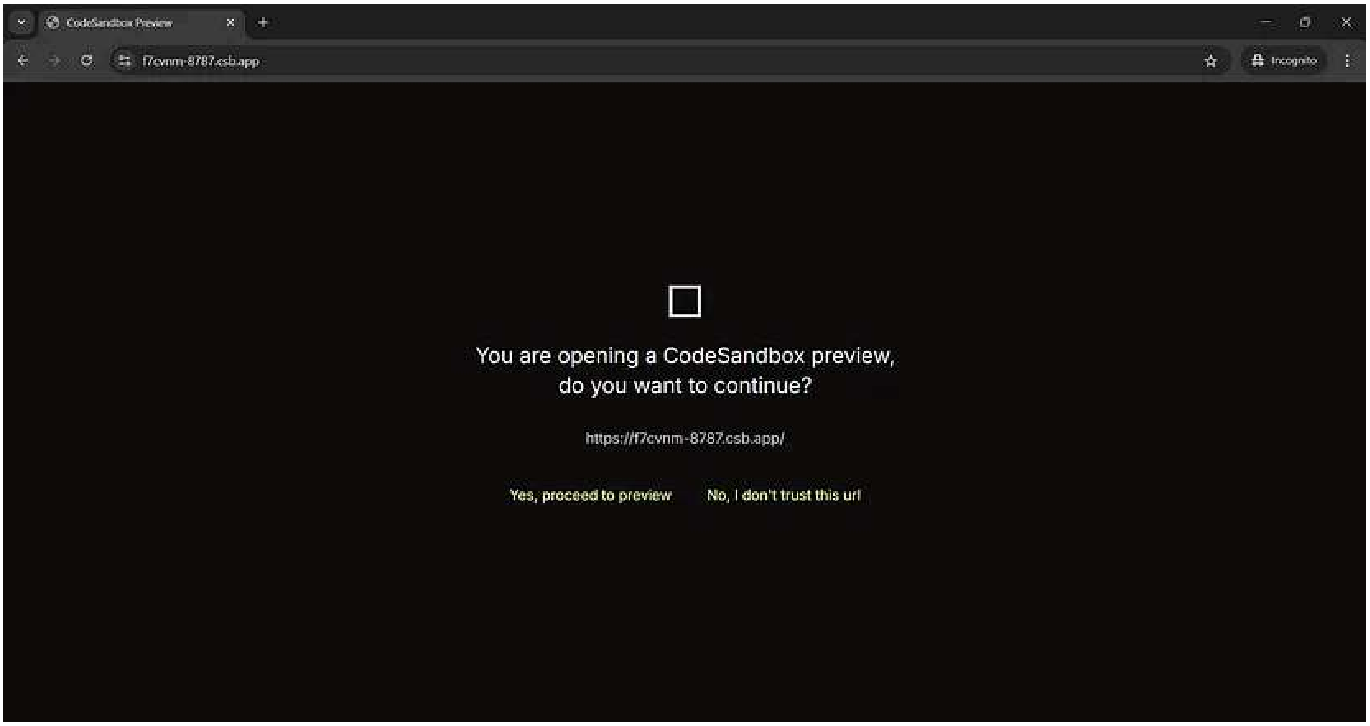


```
© 2024 f7cvnm-8787.csb.app. All rights reserved.
```

Footer

f7cvnm-8787.csb.app

Go to https://f7cvnm-8787.csb.app/

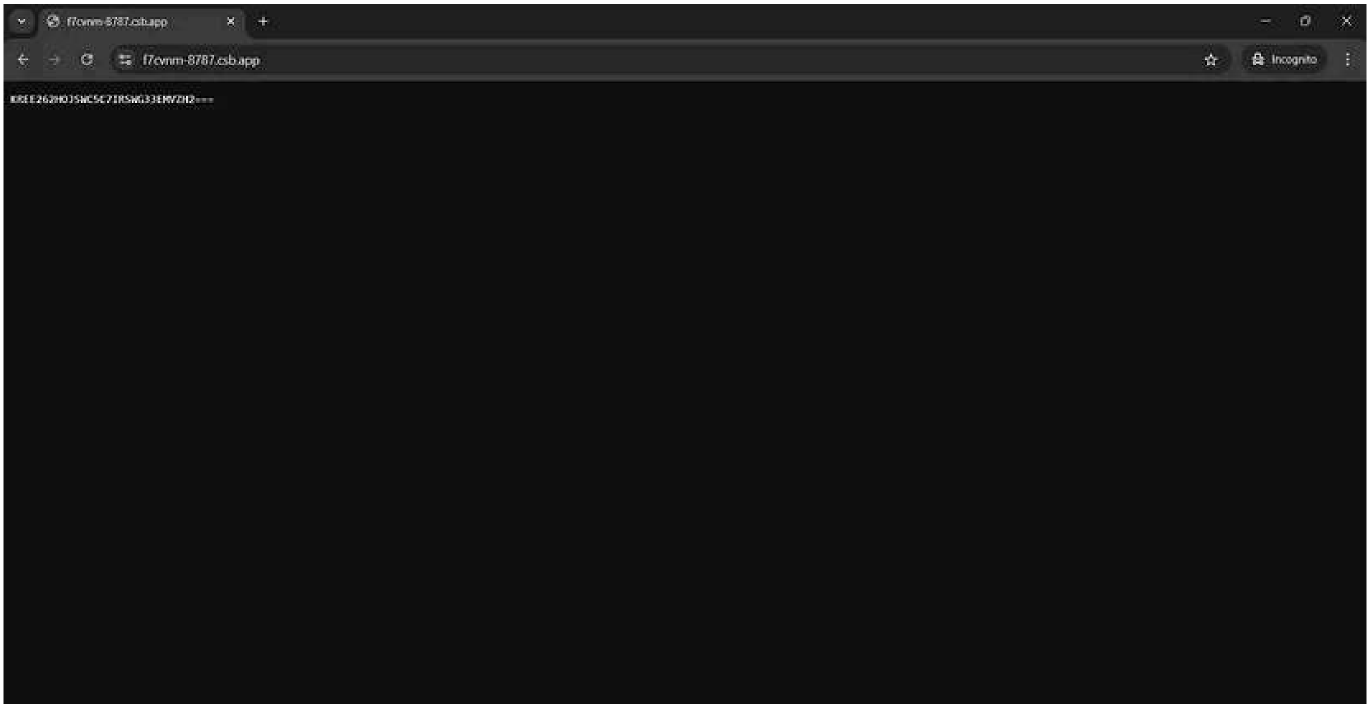


You are opening a CodeSandbox preview,
do you want to continue?

https://f7cvnm-8787.csb.app/

CodeSanbox

Click on ‘Yes, proceed to preview’



```
KREE262HOJSWCSC7IRSWG33EMVZH2===
```

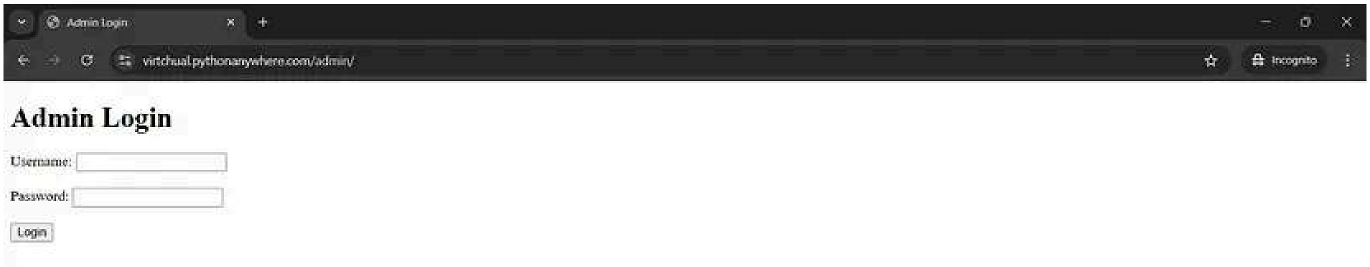
Base32

U obviously know what to do next.

Hint: CyberChef

Now that /cgi-bin/ and /robots.txt paths are completed , lets head over to the final path i.e '/admin/'.

1. /admin/



Admin Login

Username:

Password:

Login

Admin Login

NO! NO! NO! NO!

This is not related to SQLi.

Just Bruteforce it manually.

Else write a code to automate the bruteforcing.

For instance, lets take this curl command 👇

```
curl -u *username:*password  https://virtchual.pythonanywhere.com/admin/  -d "**
```

where

- *username:*password is for Basic Sign in @https://virtchual.pythonanywhere.com
- **username=admin_username&**password=admin_password is for login form @https://virtchual.pythonanywhere.com/admin/

To automate the above process with custom usernames and passwords file u can use the following bash script :

```
#!/bin/bash

# Define the target URL for login
URL="https://virtchual.pythonanywhere.com/admin/"

# Check if both username and password files are provided
if [ $# -ne 4 ]; then
    echo "Usage: $0 <username> <password> <usernames_file> <passwords_file>"
    exit 1
fi

# Assign the provided username and password files to variables
uname="$1"
pass="$2"
USERNAMES_FILE="$3"
PASSWORDS_FILE="$4"

# Check if the username and password files exist
if [ ! -f "$USERNAMES_FILE" ]; then
    echo "Error: The file '$USERNAMES_FILE' does not exist."
    exit 1
fi
```

```
    if [ ! -f "$PASSWORDS_FILE" ]; then
        echo "Error: The file '$PASSWORDS_FILE' does not exist."
        exit 1
    fi

    # Loop through usernames and passwords
    for username in $(cat "$USERNAMES_FILE"); do
        for password in $(cat "$PASSWORDS_FILE"); do
            echo "Trying username: $username with password: $password"

            # Send login attempt using curl and capture HTTP status code
            response=$(curl -u "$uname":"$pass"  https://virtchual.pythonanywhere.co

            # Check if the response indicates success (e.g., 200 status or a known s
            if [[ "$response" == "200" ]]; then
                echo "Login successful with username: $username and password: $passw
                break 2
            else
                echo "Login failed for username: $username and password: $password"
            fi
        done
    done
```

```
nano filename.sh
#Paste the above given bash script code here
```

```
chmod +x filename.sh
```

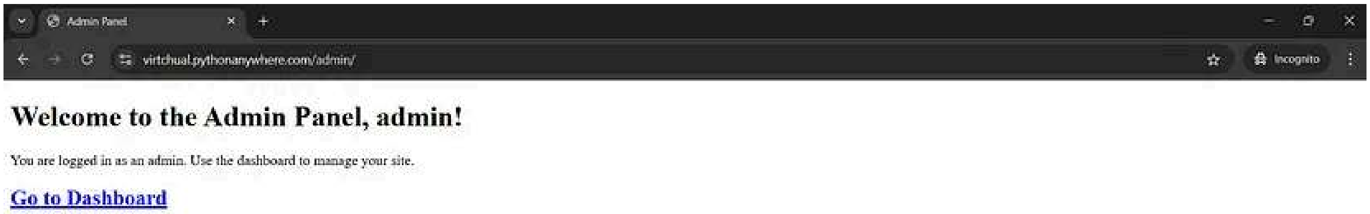
```
./filename *username *password usernames.txt passwords.txt
```

```
Usage: ./filename.sh <username> <password> <usernames_file> <passwords_file>
```

where

- *username and *password is for Basic Sign in @https://virtchual.pythonanywhere.com
- usernames.txt and passwords.txt are the custom username and password lists file for login form @https://virtchual.pythonanywhere.com/admin/

After logging in u see this admin page below

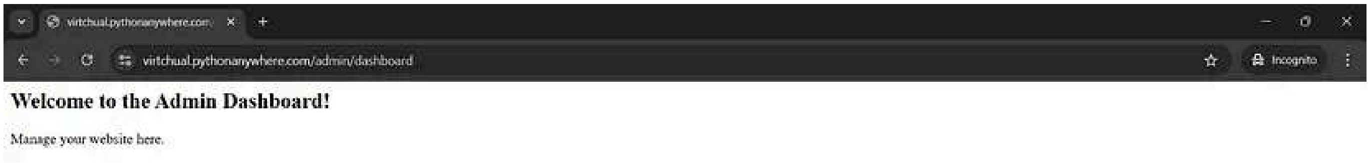


Welcome to the Admin Panel, admin!

You are logged in as an admin. Use the dashboard to manage your site.

Go to Dashboard

Click on 'Go to Dashboard'


virtchual.pythonanywhere.com/
virtchual.pythonanywhere.com/admin/dashboard
Incognito

Welcome to the Admin Dashboard!

Manage your website here.

If u've followed me till here then u should have all the flags except the bonus flag.

I'm gonna leave some hints here 👇 👇 👇 to find it.

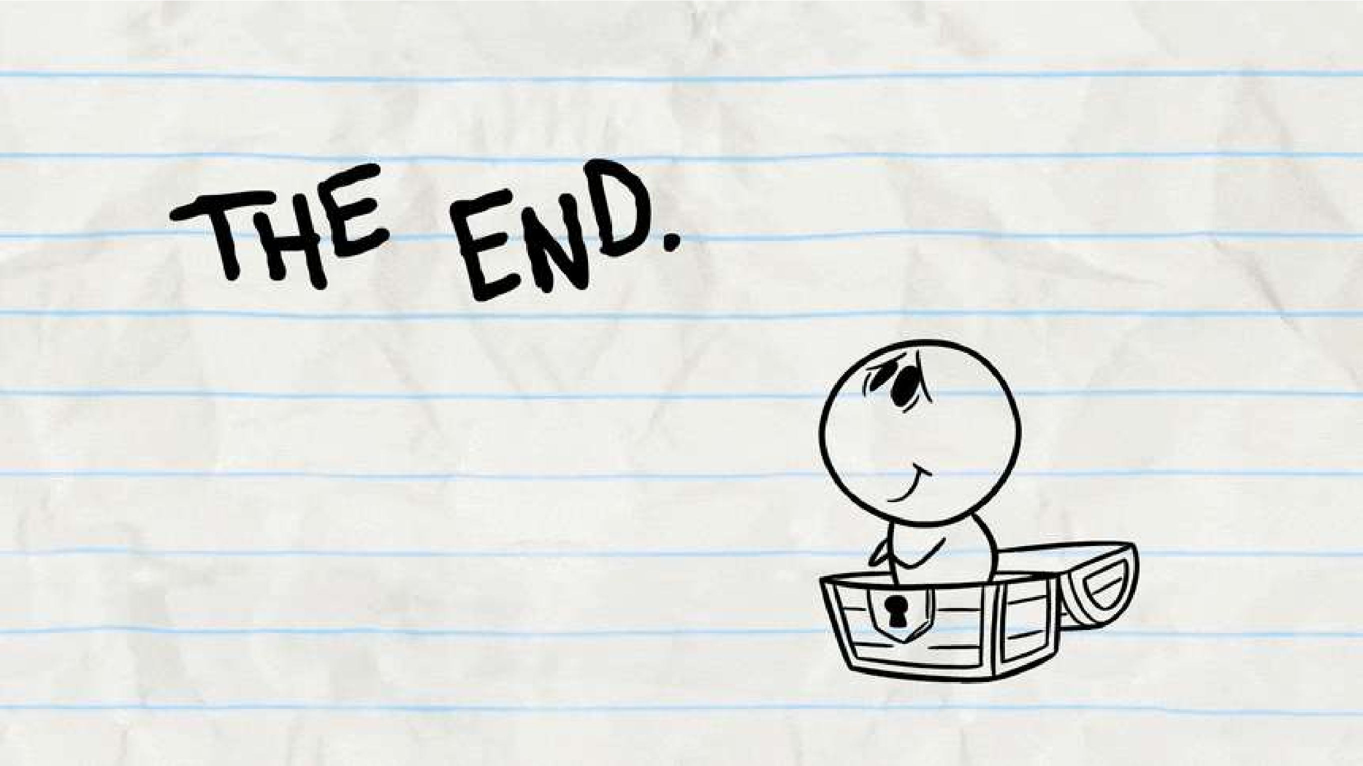
Hint:

- Think out of the box.
- View source codes.
- It is something do to with math.

— —

— — — — — — — — — — — — — — —END — — — — — — — — — — — — — — — — —

— —



1. Username : shellby ; 2. Password : 1h4t3d43m0n5 ; 3. Admin Username : admin ; 4. Admin Password : password123 ; 5. Flag 1 : THM{this_was_easy} ; 6. Flag 2 : THM{Welcome_to_Dark_Mode} ; 7. Flag 3 : THM{end_of_toggling} ; 8. Flag 4 : THM{Great_Decoder} ; 8. Flag 4 : THM{BUBBLES_ARE_COOL} ; 9. Bonus Flag : THM{OBFUSCATION}

Tryhackme Writeup Tryhackme Walkthrough Tryhackme Tryhackme Room Tryhackme Ctf

Written by virtchual

0 Followers · 1 Following

Follow

Timeless Nocturnal Adventurer

No responses yet