


# Lighthouse VPN User Guide:



## Use our lighthouse VPN to perform necessary testing

---

|                |                                                                                                                                                                    |           |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|
| <b>Step 1:</b> | <b>Download and Configure the Cyberbay VPN Profile with OpenVPN Connect</b>                                                                                        | <b>01</b> |
| <b>Step 2:</b> | <b>Enroll in the mission to activate the VPN URL: (for first-time enrollment)</b>                                                                                  | <b>03</b> |
| <b>Step 3:</b> | <b>Access the VPN URL link on the "My Lighthouse" page</b>                                                                                                         | <b>04</b> |
| <b>Step 4:</b> | <b>To set up upstream proxy servers in your selected tool (e.g., Burp Suite) using the information obtained from the VPN URL link.</b>                             | <b>04</b> |
|                |  <b>How to setup the Upstream Proxy Servers in Burp Suite Community Edition</b> | <b>05</b> |
| <b>Step 5:</b> | <b>Start using the VPN to perform testing</b>                                                                                                                      | <b>04</b> |



## FAQs

---

|          |                                                                                                 |           |
|----------|-------------------------------------------------------------------------------------------------|-----------|
| <b>1</b> | <b>How to ensure you are using the Cyberbay VPN Profile every time you start a new mission?</b> | <b>11</b> |
| <b>2</b> | <b>How to Manage URL Link on " My Lighthouse page"?</b>                                         | <b>11</b> |
|          | Handling Expired VPN URL                                                                        | <b>11</b> |
|          | Managing Active Lighthouse Sessions: Handling Maximum Connections                               | <b>12</b> |
| <b>3</b> | <b>How to reconnect to our VPN URL If you have already enrolled in the mission?</b>             | <b>13</b> |

If you have any questions or are uncertain of how this instruction operates, please do not hesitate to contact us and our customer service representatives will give you an answer as soon as possible.

[hello@cyberbay.tech](mailto:hello@cyberbay.tech)

# Use our lighthouse VPN to perform necessary testing

**Step 1: Download and Configure the Cyberbay VPN Profile with OpenVPN Connect and establish a secure VPN connection.**

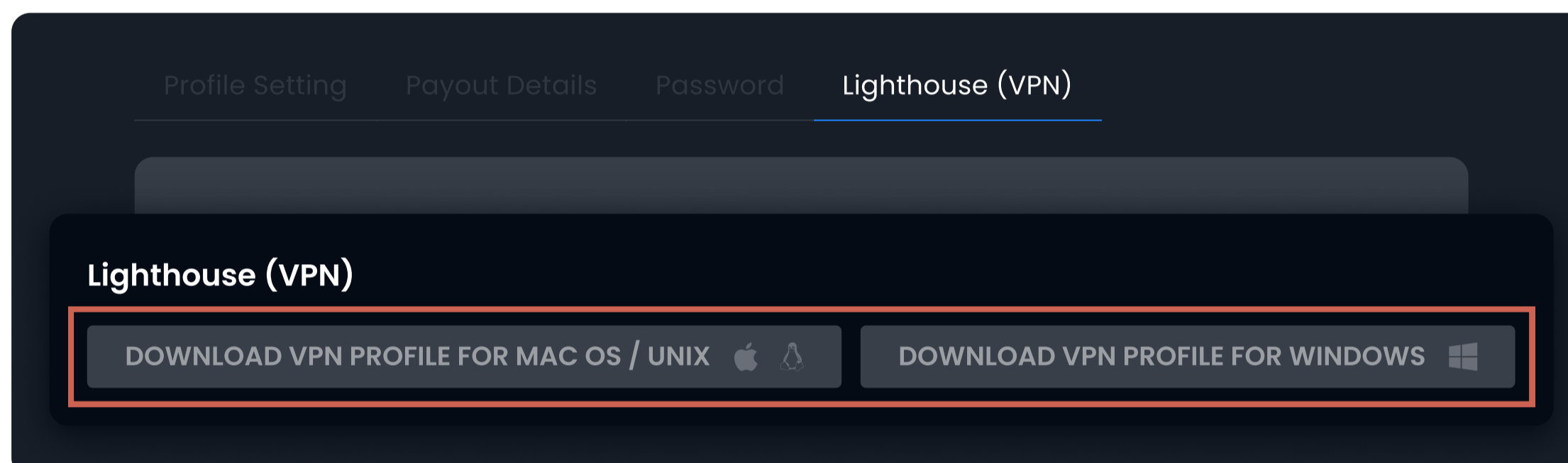
**ⓘ Important Note:**

Download and activate the Cyberbay VPN Profile before connecting to the Lighthouse VPN. Failure to do so will prevent you from establishing a connection.

CONNECTED

OpenVPN Profile  
cyberbay vpn profile

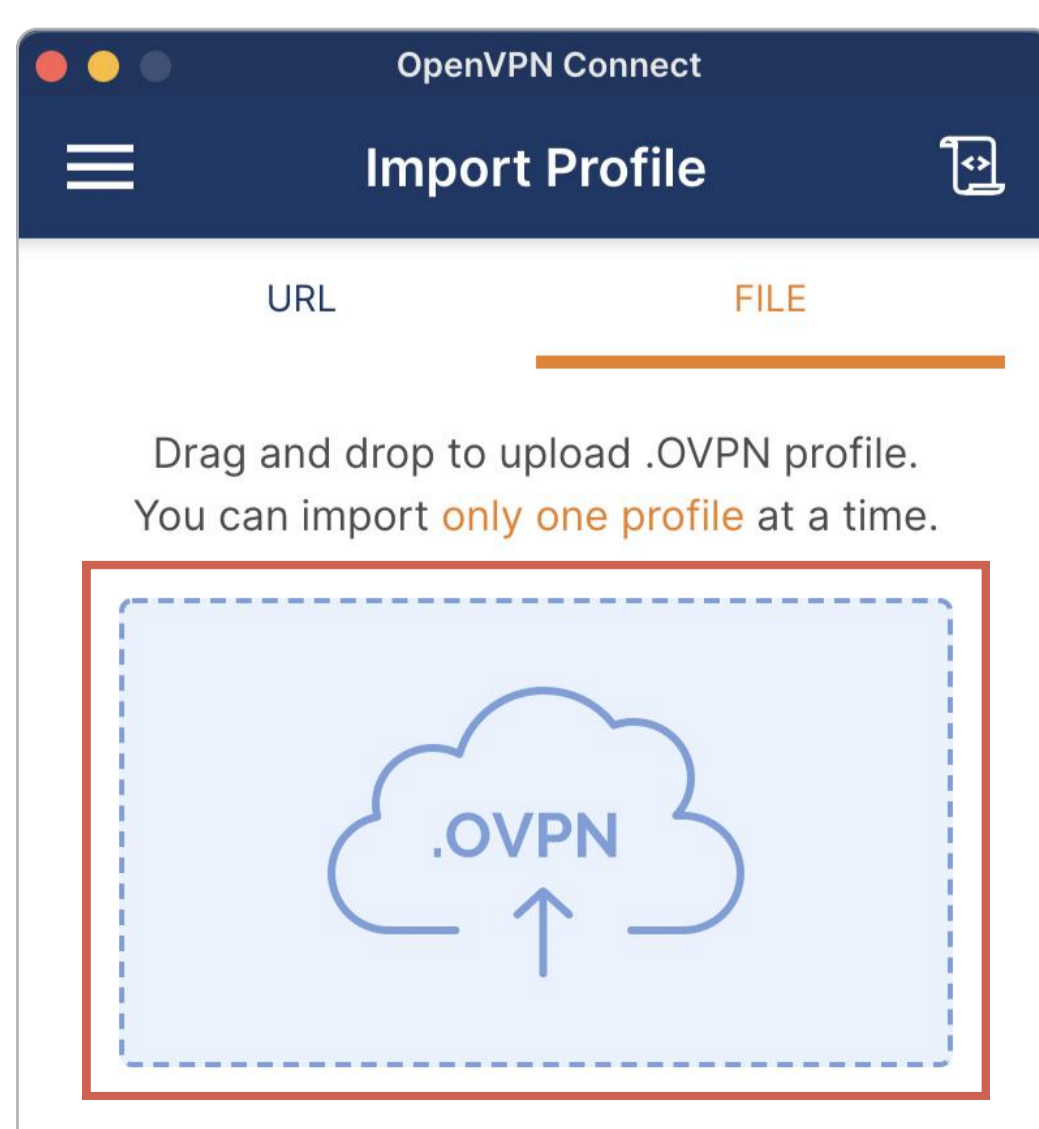
- 1 Find your unique security.txt template from your Cyberbay account. Click "Edit" of your bounty mission and download the template at "Ownership Verification" section.



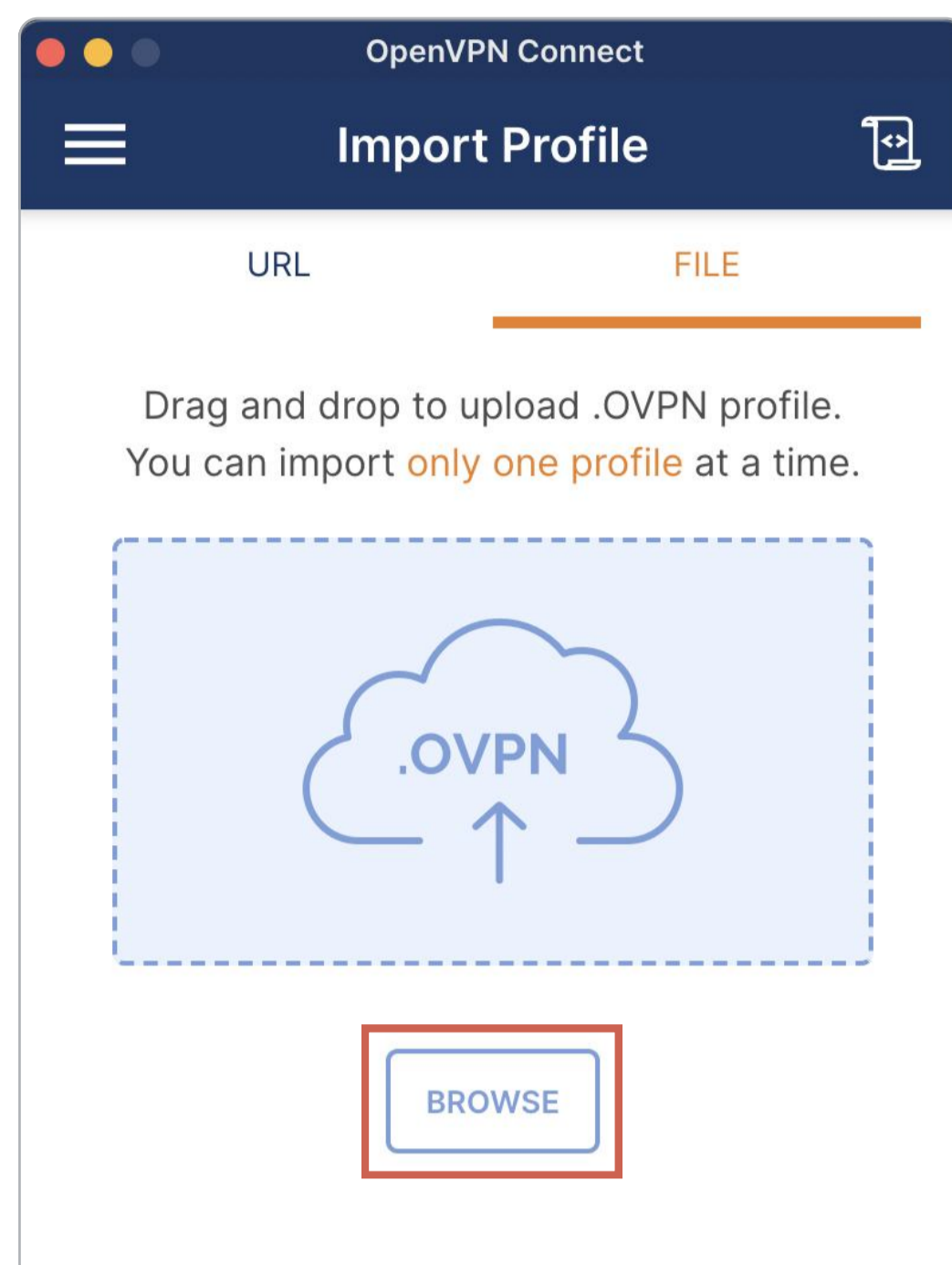
- 2 Open the OpenVPN Connect app on your device. If you don't have it installed, you can download it from your device's app store.



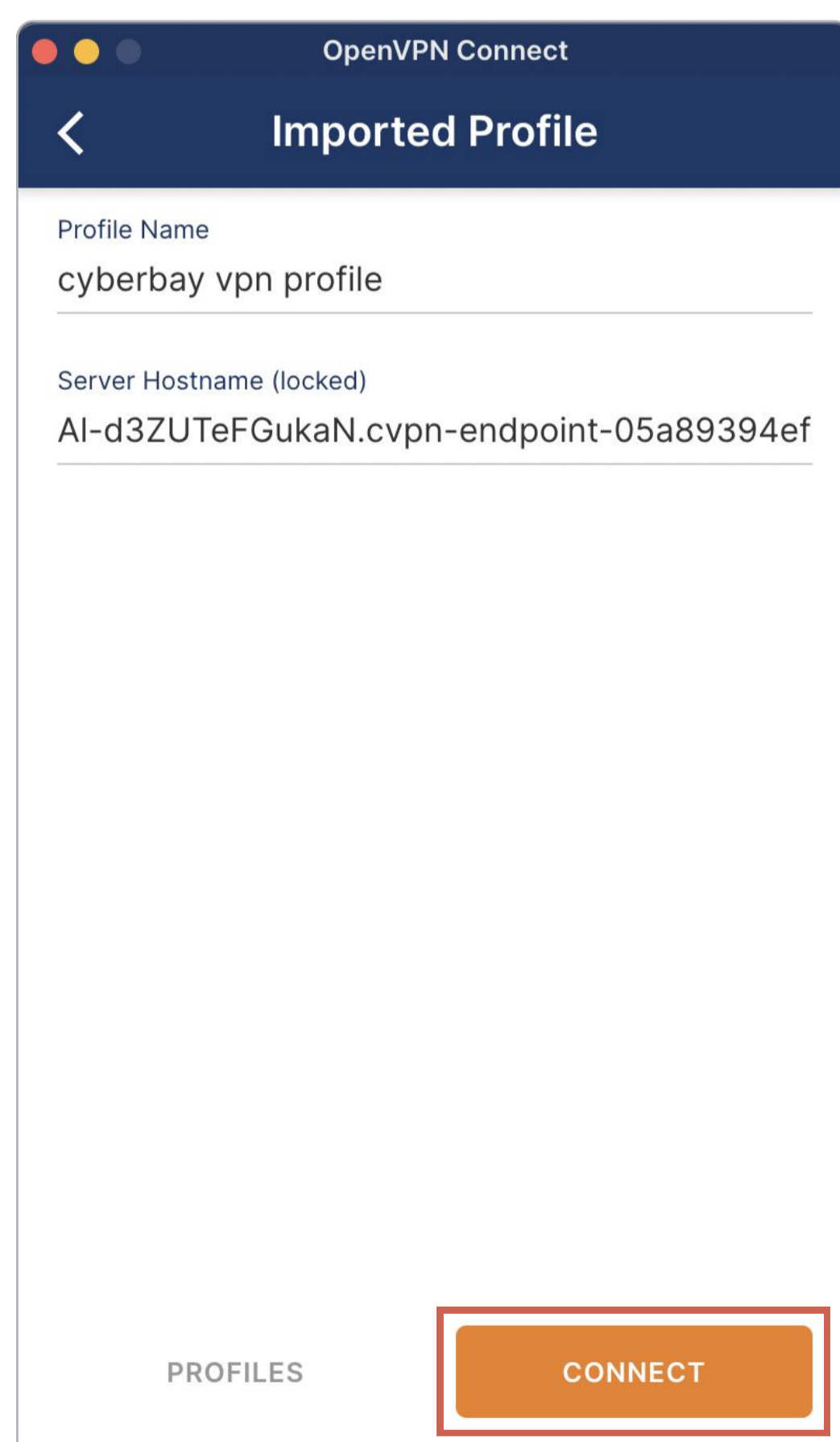
- 3 Once you have the OpenVPN Connect app open, you have two options:
  - Option 1: Drag and drop the downloaded VPN Profile file directly into the OpenVPN Connect app. The app will automatically import the configuration from the file.



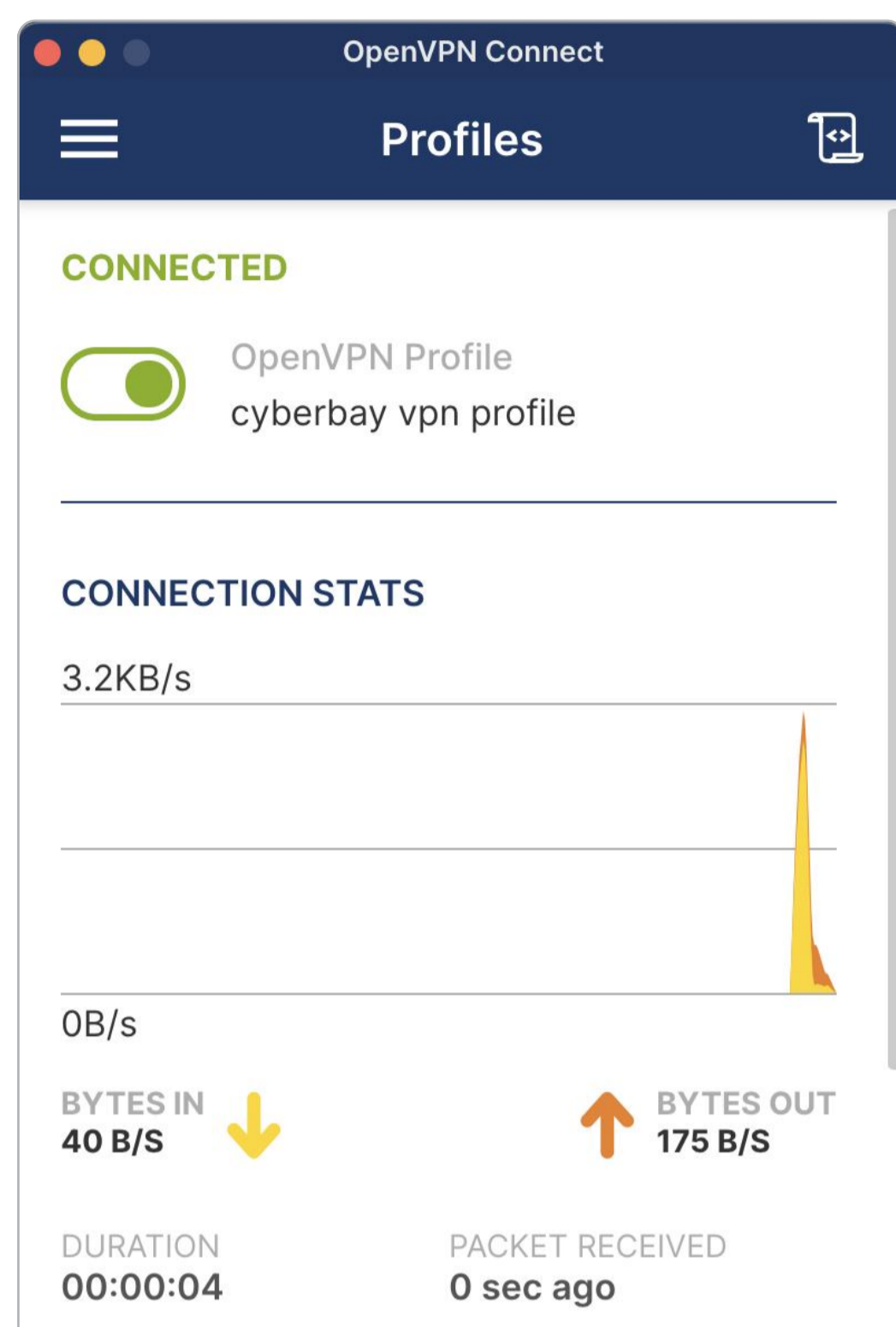
- Option 2: Within the OpenVPN Connect app, browse your device to select the downloaded VPN Profile file. Confirm the import to add the configuration to the app.



- After the configuration is added, you can customize the settings according to your preferences. This includes changing the profile name and adding any necessary credentials.
- Once you have finalized your configuration settings, click on the **connect** button within the OpenVPN Connect app to establish a secure VPN connection.



- 6 Congratulations! You have successfully established a secure VPN connection using the Cyberbay VPN Profile.

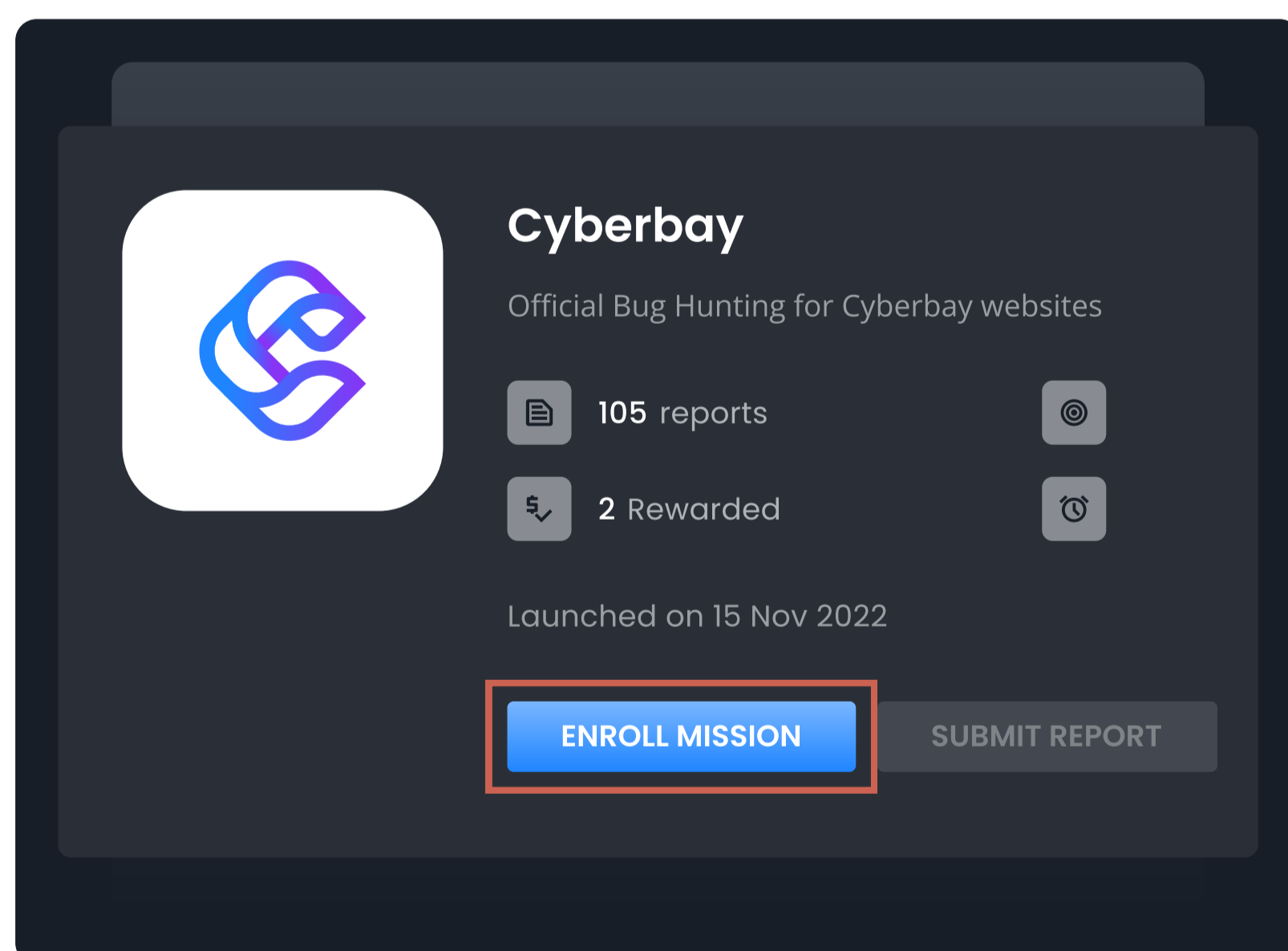


\*If needed, you can further customize the profile name and credentials within the OpenVPN Connect app.

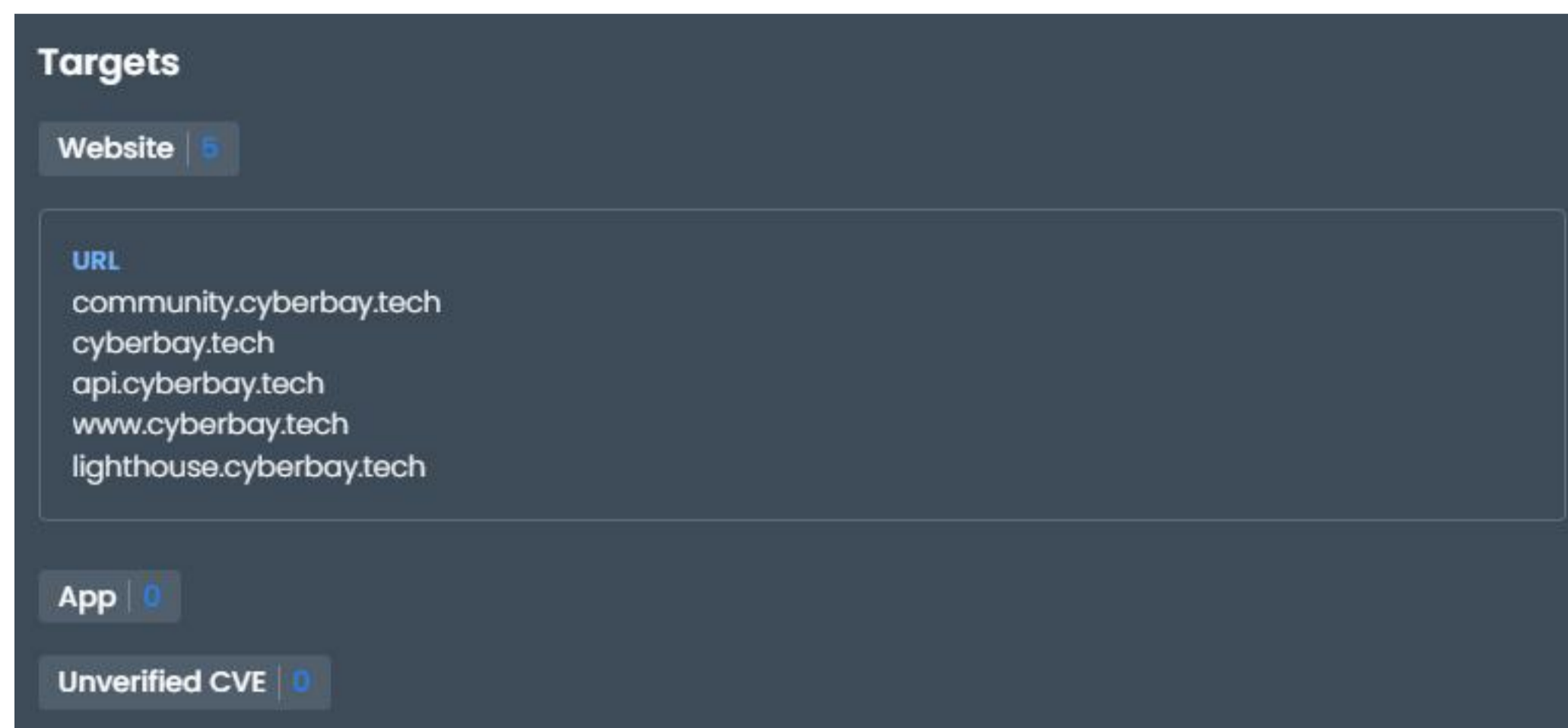
**Step 2: Enroll in the mission to activate the VPN URL: (for first-time enrollment)**

Go to the mission details page and enroll in the mission to activate the VPN URL.

\* This step is necessary to gain access to the VPN connection.

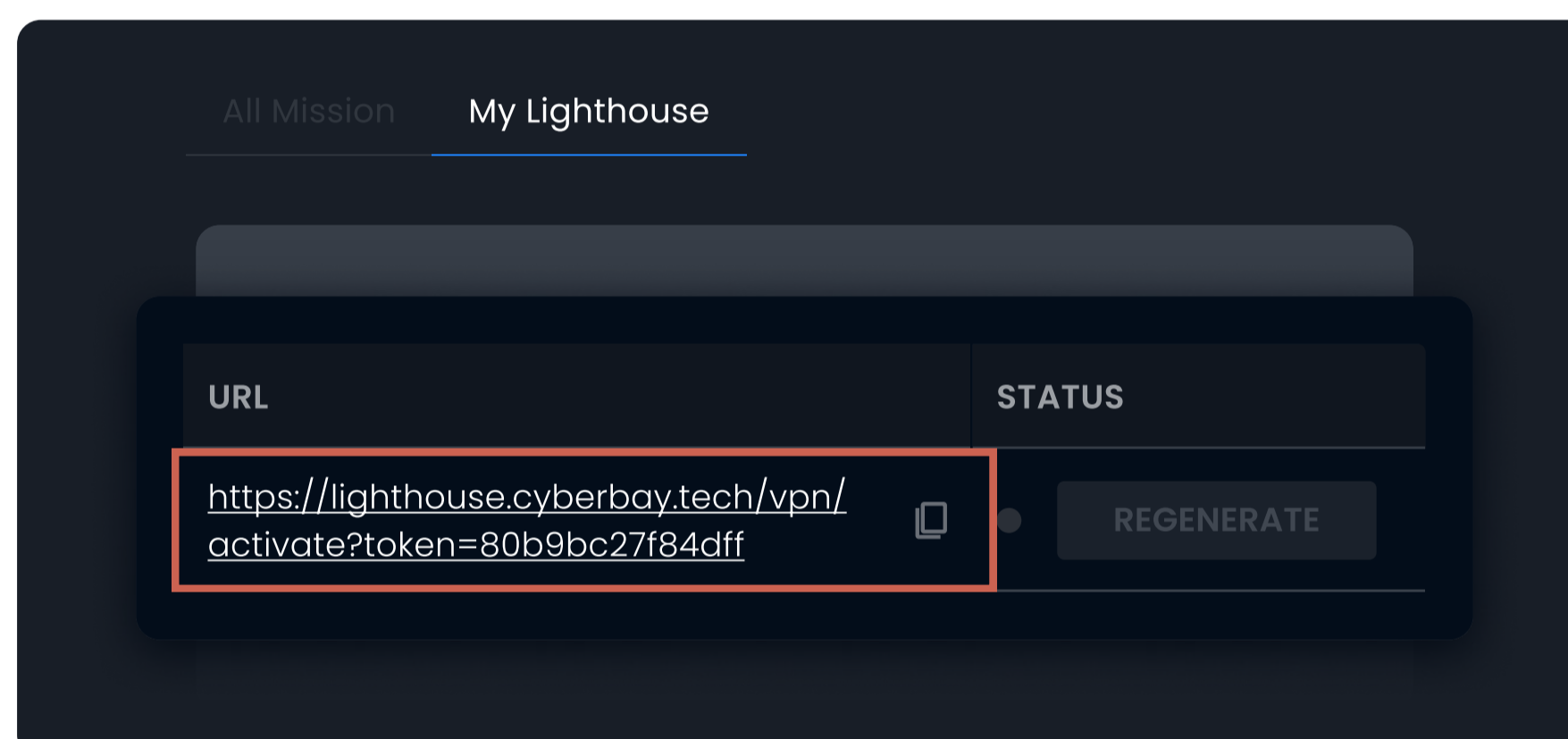


**Step 3:** Review the Target URLs and locate the "Targets" section to view the available URLs for testing.



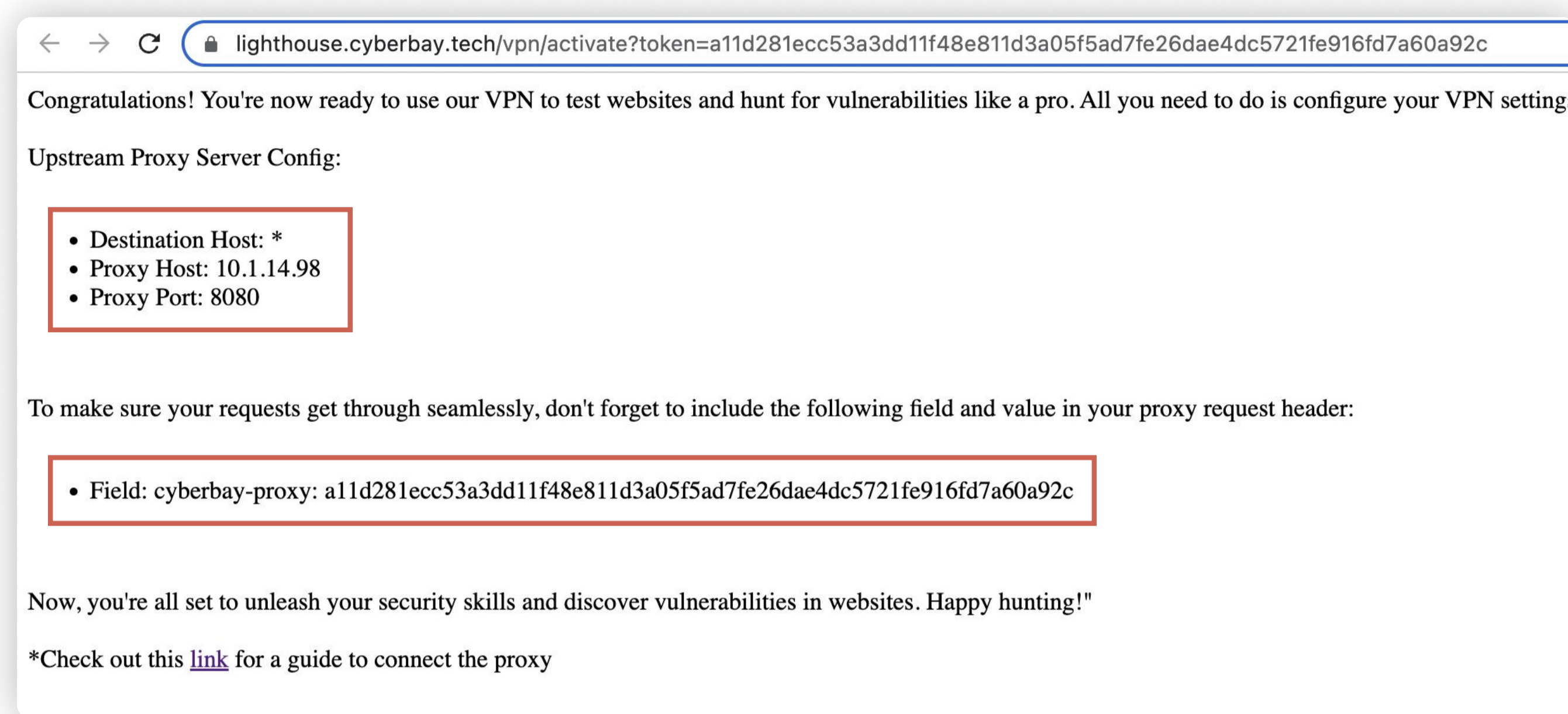
**Step 4:** Retrieve the VPN URL from the "My Lighthouse" Page

Navigate to the "My Lighthouse" page and locate the VPN URL linked to your mission. Click on the URL to activate it.



**Step 5: To set up upstream proxy servers in your selected tool (e.g. [Burp Suite Community Edition](#))**

Connect to the VPN: Using a selected tool of your choice (e.g Burp Suite Community Edition etc.), configure the **provided VPN information** in the VPN link to establish a connection to the VPN server.



The screenshot shows a web browser window with the URL `lighthouse.cyberbay.tech/vpn/activate?token=a11d281ecc53a3dd11f48e811d3a05f5ad7fe26dae4dc5721fe916fd7a60a92c`. The page content includes a congratulatory message, a section for 'Upstream Proxy Server Config' with a red-bordered box containing the following list:

- Destination Host: \*
- Proxy Host: 10.1.14.98
- Proxy Port: 8080

Below this, it instructs the user to include a specific field in their proxy request header, with a red-bordered box containing:

- Field: cyberbay-proxy: a11d281ecc53a3dd11f48e811d3a05f5ad7fe26dae4dc5721fe916fd7a60a92c

The page concludes with a 'Happy hunting!' message and a link to a proxy connection guide.

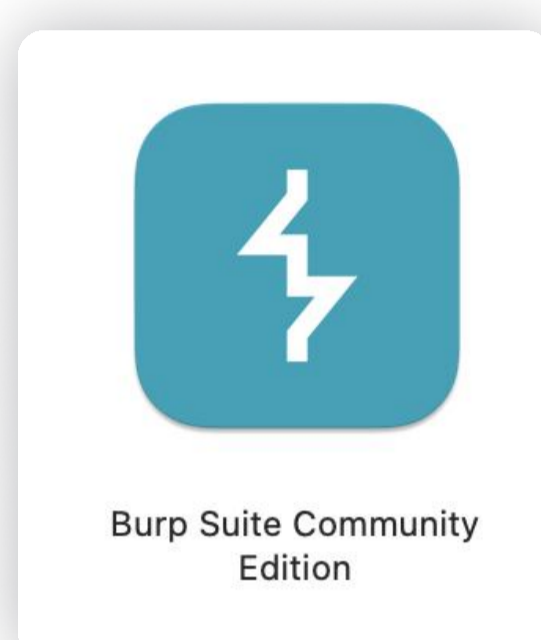
\*Follow the instructions specific to your VPN client for setting up the connection.

**[How to setup the Upstream Proxy Servers in Burp Suite Community Edition](#)****Step 6: Start using the VPN to perform testing:**

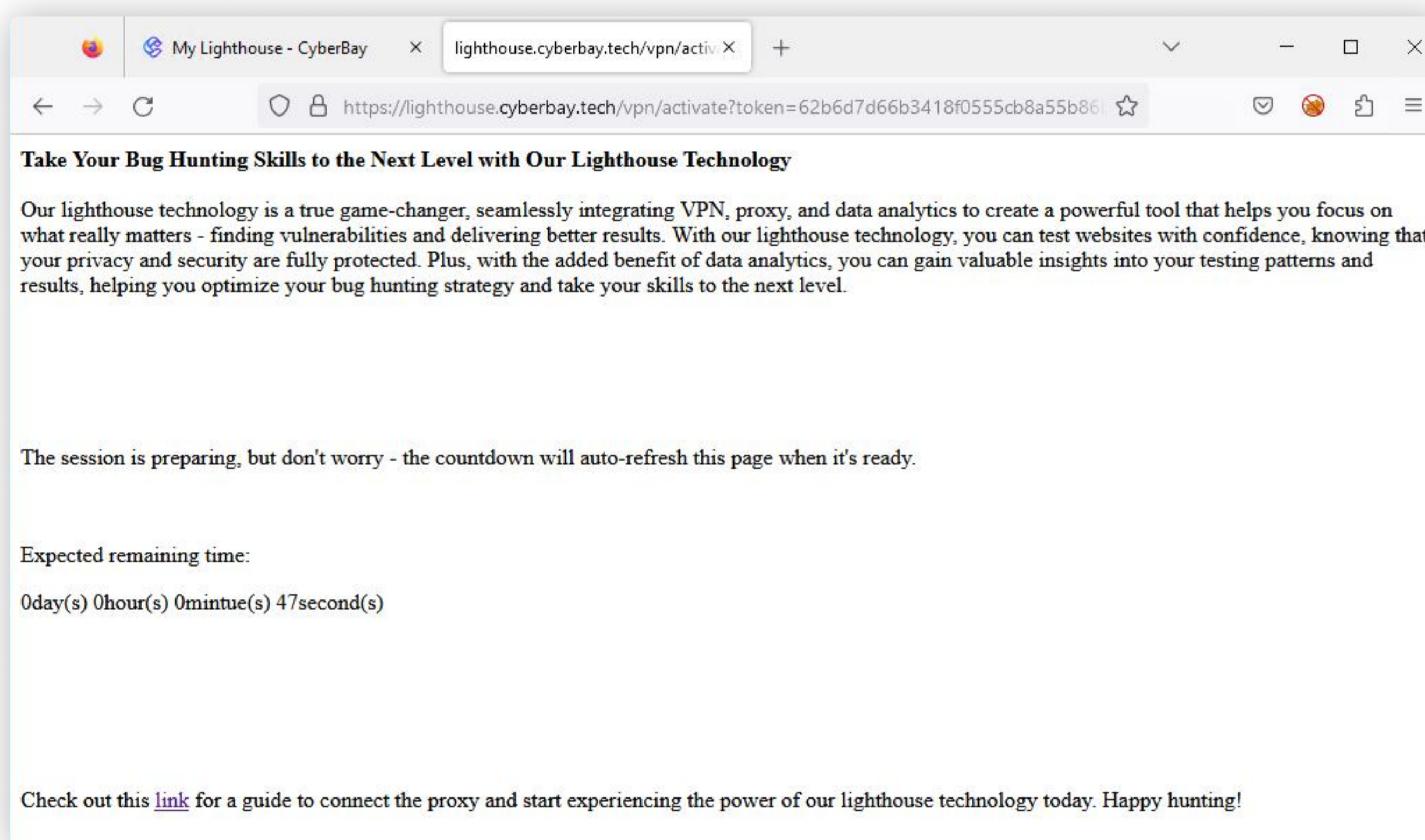
Once you have set up the proxy settings in in your selected tool (e.g Burp Suite Community), you should be connected to the VPN. You can now perform the necessary testing or access the resources as required for the bounty mission.

# How to setup the Upstream Proxy Servers in Burp Suite Community Edition v2023.5.1

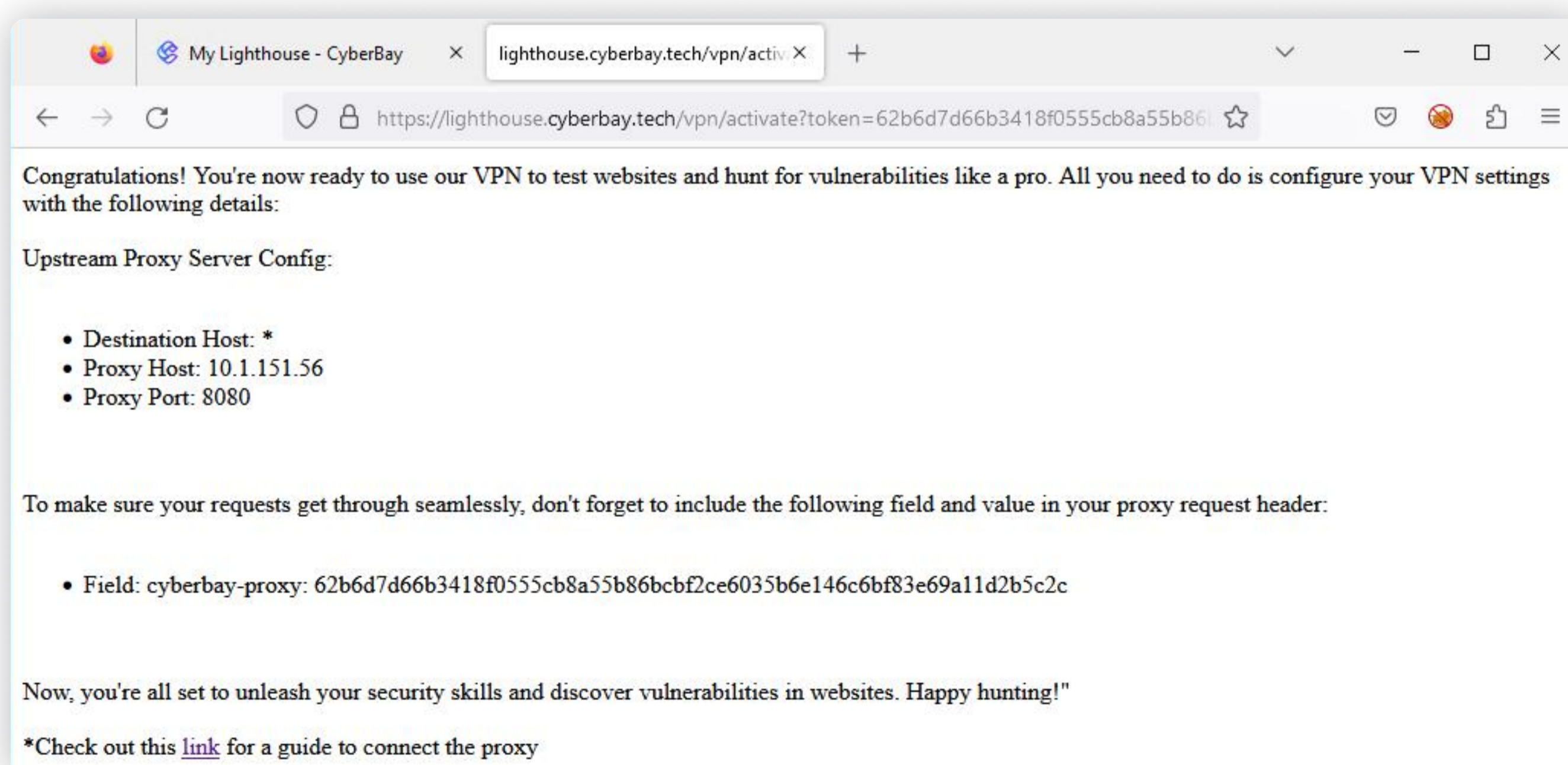
- 1 Burp Suite is pre-installed in kali linux or you can download and install it from [here](#).



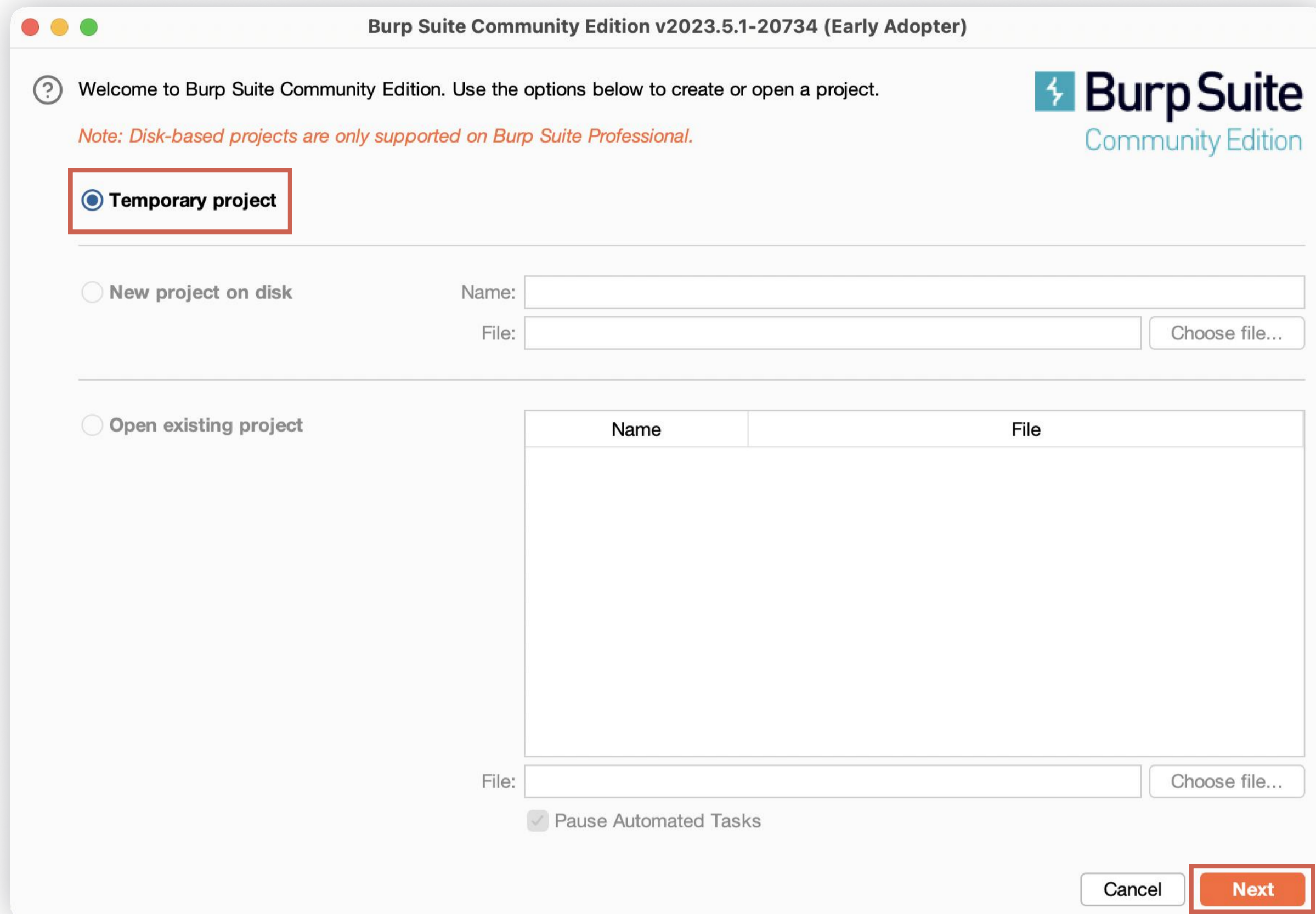
- 2 Please wait for the session preparation. The page will auto refresh automatically in **60** seconds.



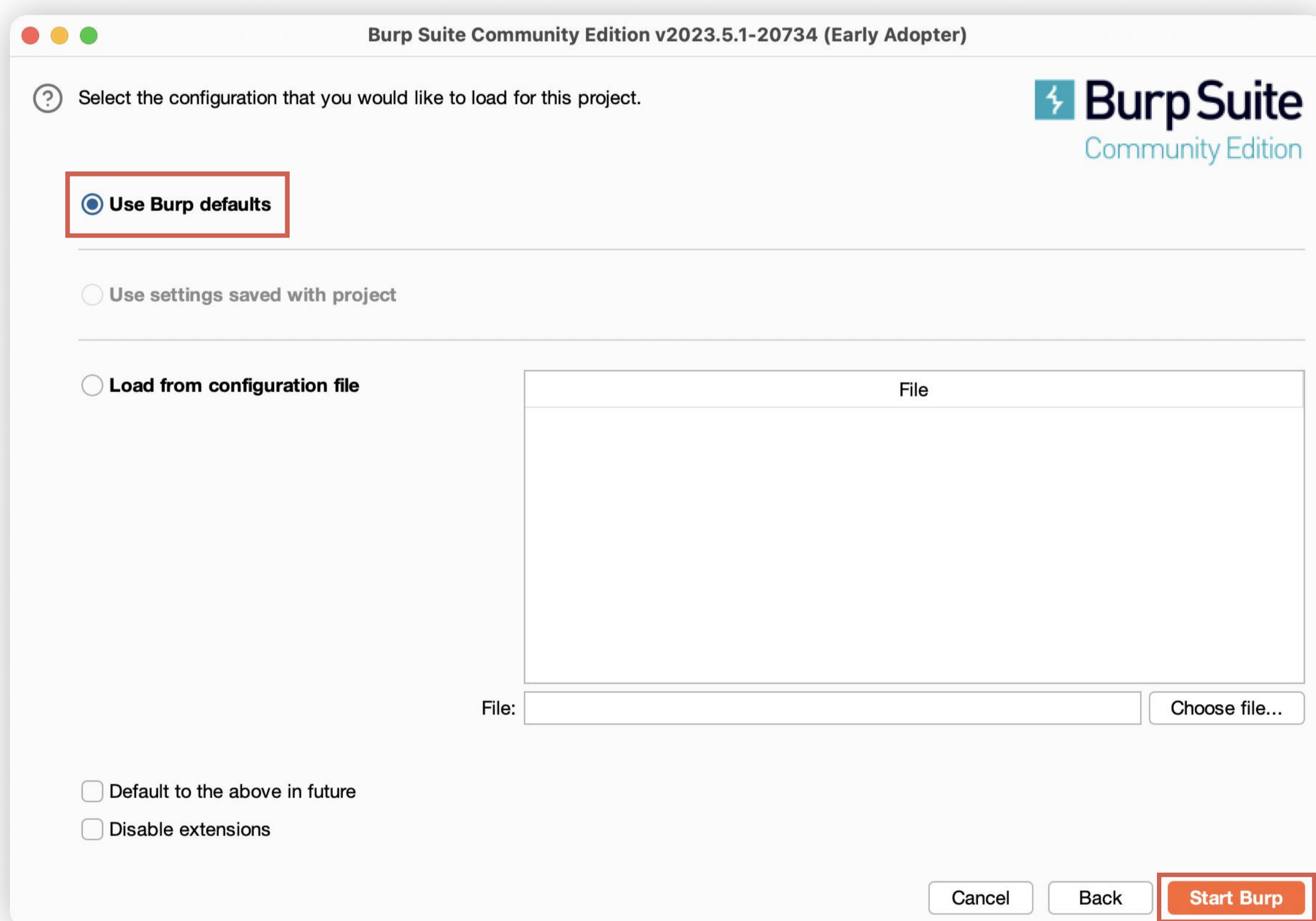
- 3 Please mark down the resources.



- 4 Once the resource is ready. Open Burp Suite and select **Temporary project**. Then click **Next**.

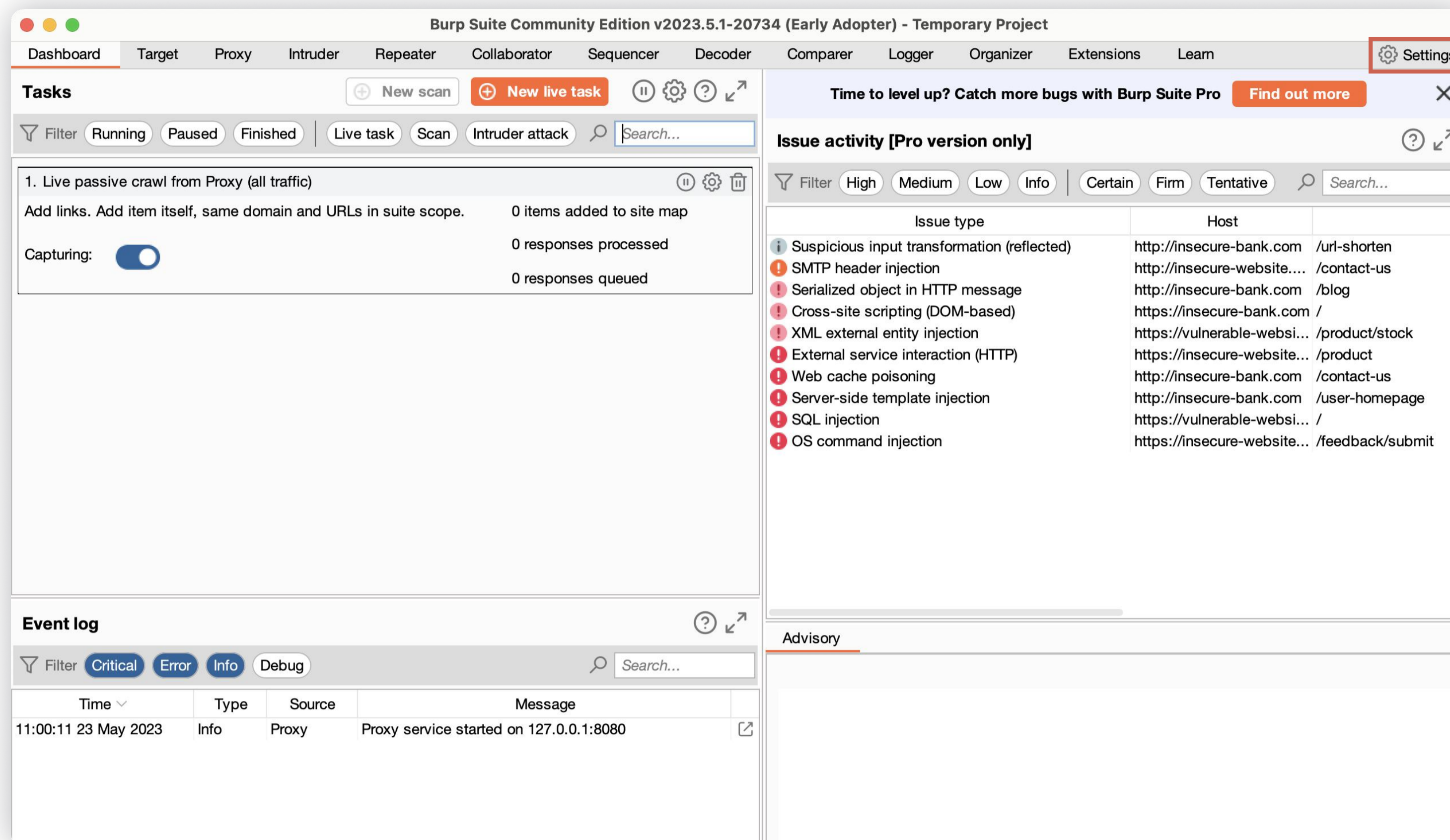


- 5 Please choose **Use Burp Defaults**. Then click **Start Burp**.

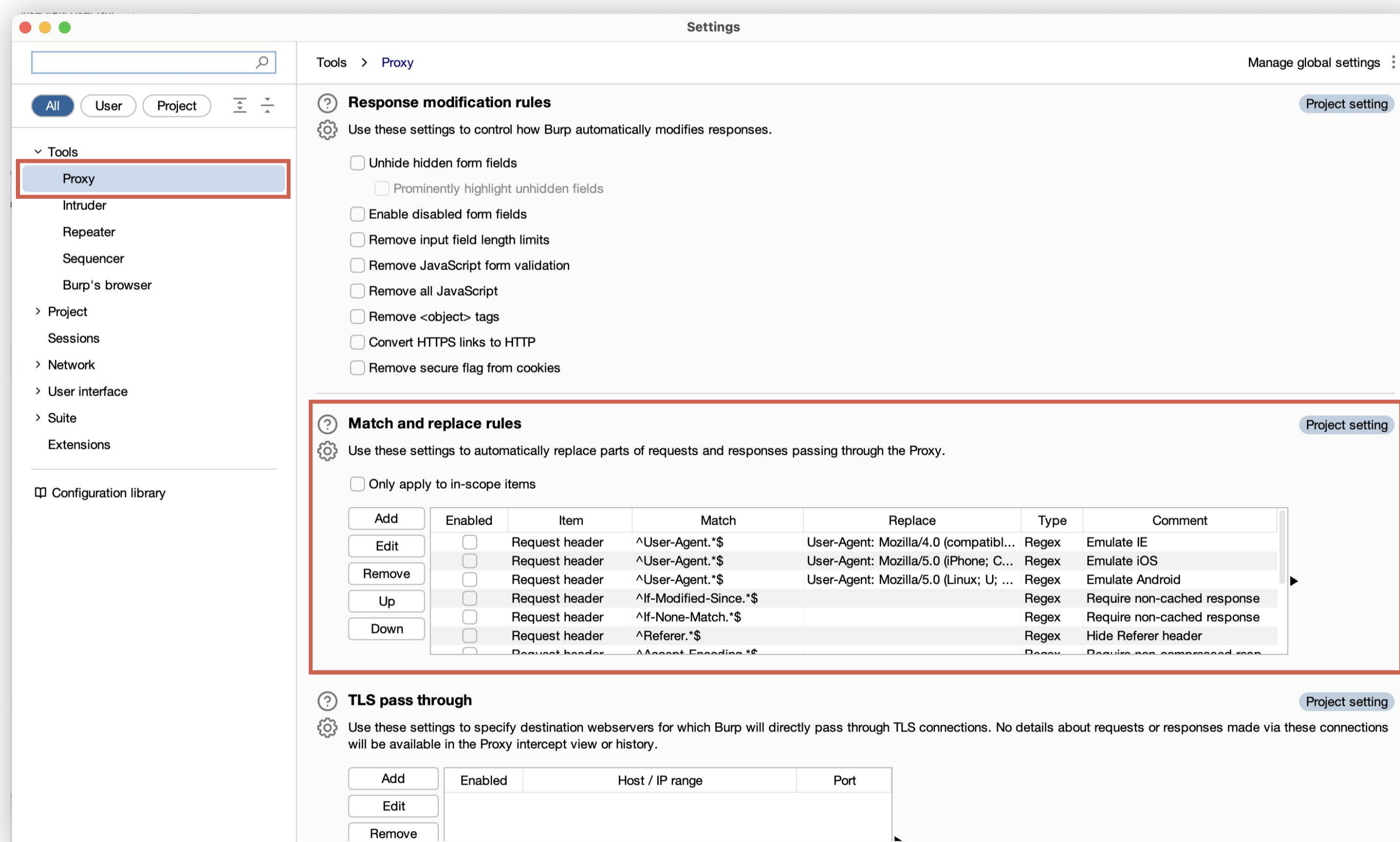




6 Click on **Settings** in the navigation bar on the right side.



7 Please select **Proxy**. Scroll down to **Match and replace rules** and click **Add**.



## 8 Please specify the details of the Match and Replace as shown in Notes.

lighthouse.cyberbay.tech/vpn/activate?token=a11d281ecc53a3dd11f48e811d3a05f5ad7fe26dae4dc5721fe916fd7a60a92c

Congratulations! You're now ready to use our VPN to test websites and hunt for vulnerabilities like a pro. All you need to do is configure your VPN settings

Upstream Proxy Server Config:

- Destination Host: \*
- Proxy Host: 10.1.14.98
- Proxy Port: 8080

To make sure your requests get through seamlessly, don't forget to include the following field and value in your proxy

- Field: cyberbay-proxy: a11d281ecc53a3dd11f48e811d3a05f5ad7fe26dae4dc5721fe916fd7a60a92c

Now, you're all set to unleash your security skills and discover vulnerabilities in websites. Happy hunting!"

\*Check out this [link](#) for a guide to connect the proxy

**Add match/replace rule**

Specify the details of the match/replace rule.

Type: Request header

Match: *Regex condition to match - leave blank to add a new header*

Replace: *Literal string to replace - leave blank to remove a matched header*

Comment:

Regex match

OK Cancel

### Note:

Type: Request Header

Replace: cyberbay-proxy: {YOUR ACTIVATION TOKEN}

## 9 Select **User** at the top of the left sidebar. Under Network options, choose **Connections**. Find or search **Upstream proxy servers** and click on the **Add** button.

Settings

Network > Connections

Manage global settings

Prompt for credentials on platform authentication failure

**Upstream proxy servers** User setting Project setting

Use these settings to control whether Burp sends outgoing requests to an upstream proxy server, or directly to the destination web server. The first rule that matches each destination host is used. To send all traffic to a single proxy server, create a rule with \* as the destination host.

Override options for this project only

|        | Enabled                             | Destination host | Proxy host  | Proxy port | Auth type | Username |
|--------|-------------------------------------|------------------|-------------|------------|-----------|----------|
| Add    | <input type="checkbox"/>            | *                | 10.1.132.65 | 8080       |           |          |
| Edit   | <input type="checkbox"/>            | *                | 10.1.56.146 | 8080       |           |          |
| Remove | <input type="checkbox"/>            | *                | 10.1.14.152 | 8080       |           |          |
| Up     | <input type="checkbox"/>            | *                | 10.1.17.184 | 8080       |           |          |
| Down   | <input checked="" type="checkbox"/> | *                | 10.1.143.83 | 8080       |           |          |

**SOCKS proxy** User setting Project setting

Use these settings to configure Burp to use a SOCKS proxy for all outgoing communications. This setting is applied at the TCP level, and all outbound requests will be sent via this proxy. If you have configured rules for upstream HTTP proxy servers, then requests to upstream proxies will be sent via the SOCKS proxy configured here.

Override options for this project only

Use SOCKS proxy

SOCKS proxy host:

SOCKS proxy port:

Username:

Password:

Do DNS lookups over SOCKS proxy

## 10 Please specify the details of the Match and Replace as shown in Notes.

lighthouse.cyberbay.tech/vpn/activate?token=a11d281ecc53a3dd11f48e811d3a05f5ad7fe26dae4dc5721fe916fd7a60a92c

Congratulations! You're now ready to use our VPN to test websites and hunt for vulnerabilities like a pro. All you need to do is configure your VPN settings

Upstream Proxy Server Config:

- Destination Host: \*
- Proxy Host: 10.1.14.98
- Proxy Port: 8080

To make sure your requests get through seamlessly, don't forget to include the following field and value in your proxy

- Field: cyberbay-proxy: a11d281ecc53a3dd11f48e811d3a05f5ad7fe26dae4dc5721fe916fd7a60a92c

Now, you're all set to unleash your security skills and discover vulnerabilities in websites. Happy hunting!"

\*Check out this [link](#) for a guide to connect the proxy

**Add upstream proxy rule**

Enter the details of the upstream proxy rule. You can use wildcards to specify destination hosts (\* matches zero or more characters, ? matches any character except a dot). Leave the proxy host blank to connect directly for the specified destination host.

Destination host: \*

Proxy host: 10.1.15.129

Proxy port: 8080

Authentication type: None

Username:

Password:

Domain:

Domain hostname:

OK Cancel

### ⓘ Important Note:

\*The information is provided during the account registration. Destination host should always input as " \* ".

## 11 Please be ensure to click the right proxy by clicking the box.

**Upstream proxy servers** User setting Project setting

Use these settings to control whether Burp sends outgoing requests to an upstream proxy server, or directly to the destination web server. The first rule that matches each destination host is used. To send all traffic to a single proxy server, create a rule with \* as the destination host.

Override options for this project only

|                          | Enabled                             | Destination host | Proxy host  | Proxy port | Auth type | Username |
|--------------------------|-------------------------------------|------------------|-------------|------------|-----------|----------|
| <input type="checkbox"/> | <input checked="" type="checkbox"/> | *                | 10.1.15.129 | 8080       |           |          |

Add Edit Remove Up Down

## 12 On the left sidebar, click **Proxy**. Please ensure that the correct listener is enabled.

Tools > Proxy Manage global settings

**Proxy listeners** Project setting

Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser to use one of the listeners as its proxy server.

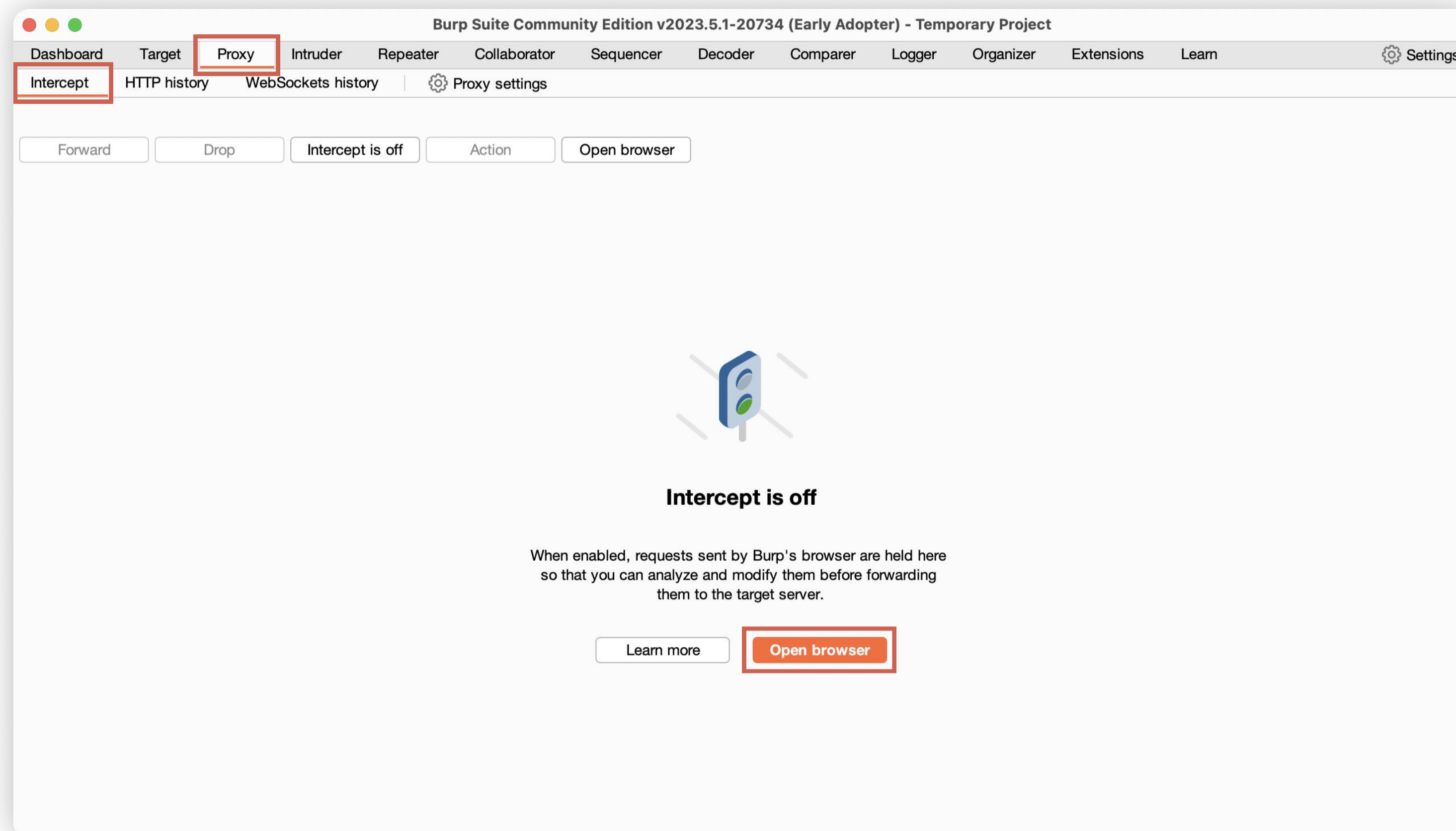
|                          | Running                             | Interface      | Invisible | Redirect | Certificate | TLS Protocols | Support HTTP/2                      |
|--------------------------|-------------------------------------|----------------|-----------|----------|-------------|---------------|-------------------------------------|
| <input type="checkbox"/> | <input checked="" type="checkbox"/> | 127.0.0.1:8080 |           |          | Per-host    | Default       | <input checked="" type="checkbox"/> |

Add Edit Remove

Each installation of Burp generates its own CA certificate that Proxy listeners can use when negotiating TLS connections. You can import or export this certificate for use in other tools or another installation of Burp.

Import / export CA certificate Regenerate CA certificate

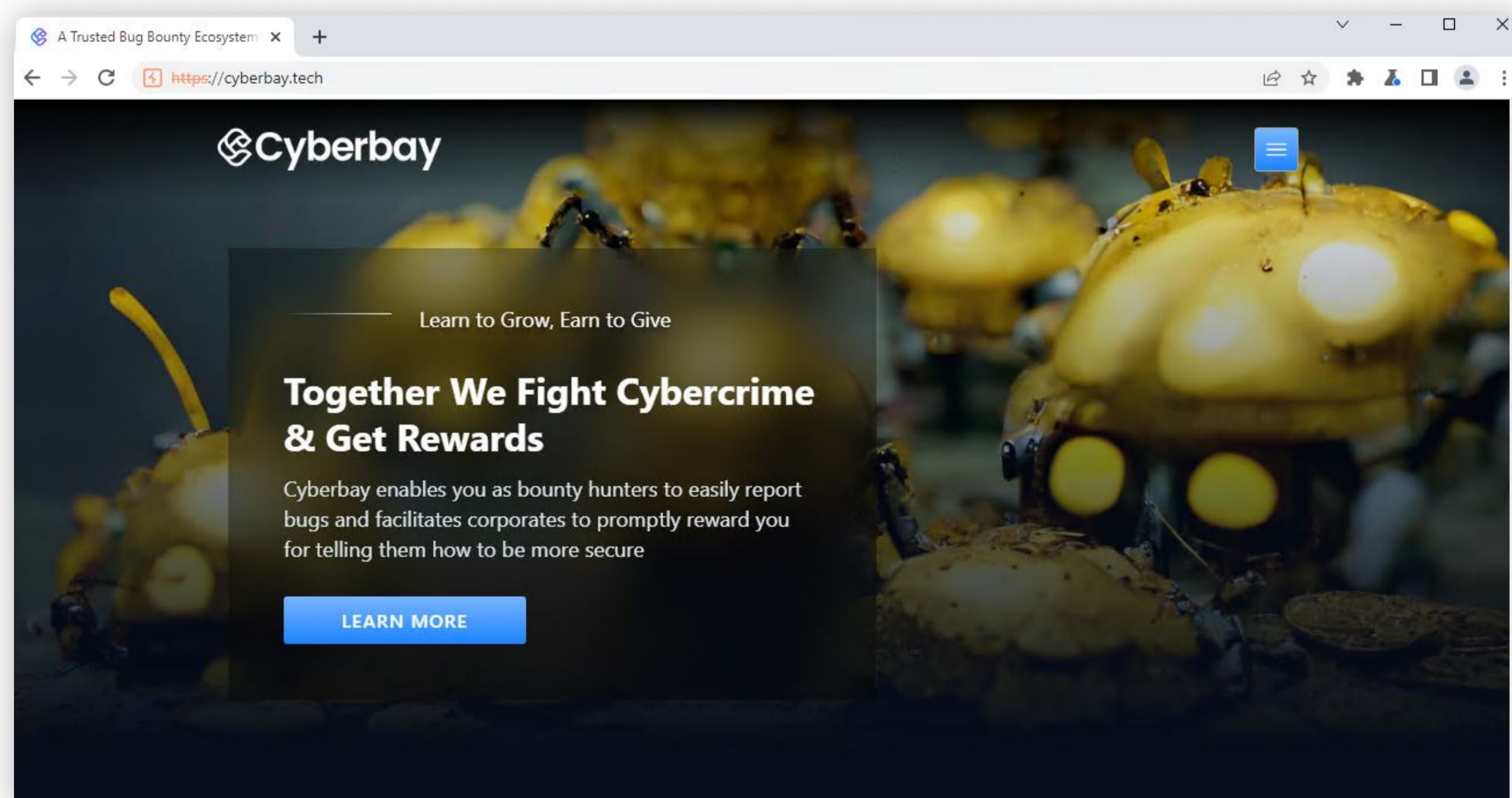
13 Click **Intercept** in the navigation bar. Then click on the **Open Browser**.



#### Note

It might take a few minutes to open the browser.

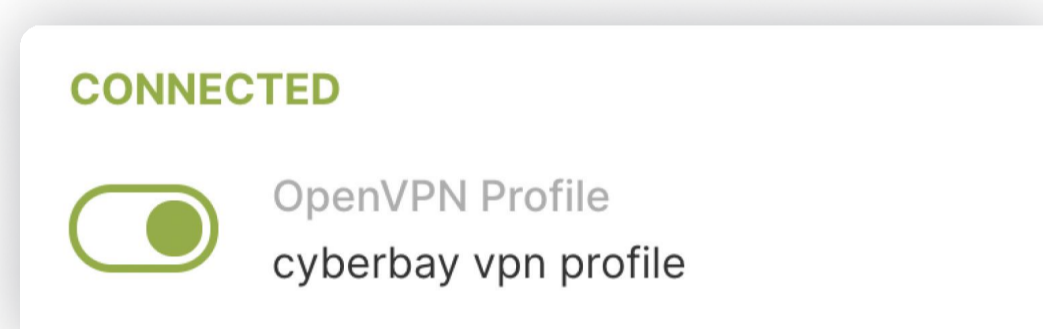
14 Proxy the list of "Targets" URLs identified in Step 3. Begin testing once the URLs have been proxied.



## FAQs

### 1 How to **ensure** you are using the Cyberbay VPN Profile with OpenVPN Connect every time you start a new mission?

- After downloading the VPN Profile and establishing a secure VPN connection following the previous instructions, make sure to **keep the OpenVPN Connect app open** on your device.
- Whenever you start a new mission, before accessing any relevant platforms or websites, ensure that the OpenVPN Connect app is **running** in the background.
- If the OpenVPN Connect app is closed or the VPN connection is disconnected, open the app again and tap on the "**Connect**" button to re-establish the secure VPN connection using the Cyberbay VPN Profile.
- It's important to verify that the VPN connection is active before proceeding with any activities related to the mission. You can usually check the status of the VPN connection within the OpenVPN Connect app, which typically shows a connected status.



- Keep in mind that for each new mission, it's crucial to activate the Cyberbay VPN Profile before connecting to the Lighthouse VPN. Failure to do so will prevent you from establishing a connection.

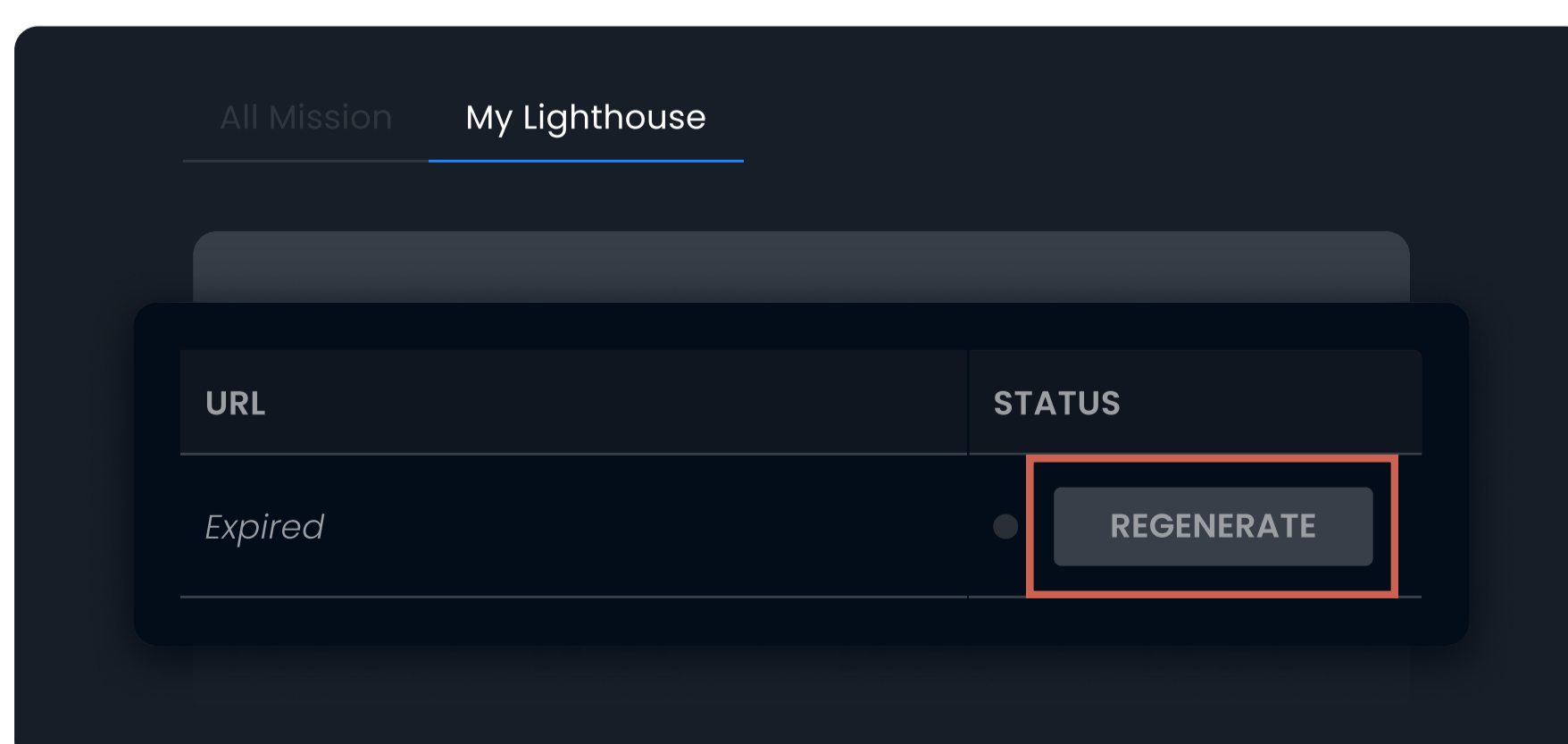
### 2 How to manage URL link on "My Lighthouse page"?

#### Handling Expired VPN URL

If your VPN URL is marked as expired, it indicates that the validity period for the URL has ended. To address this, follow these steps:

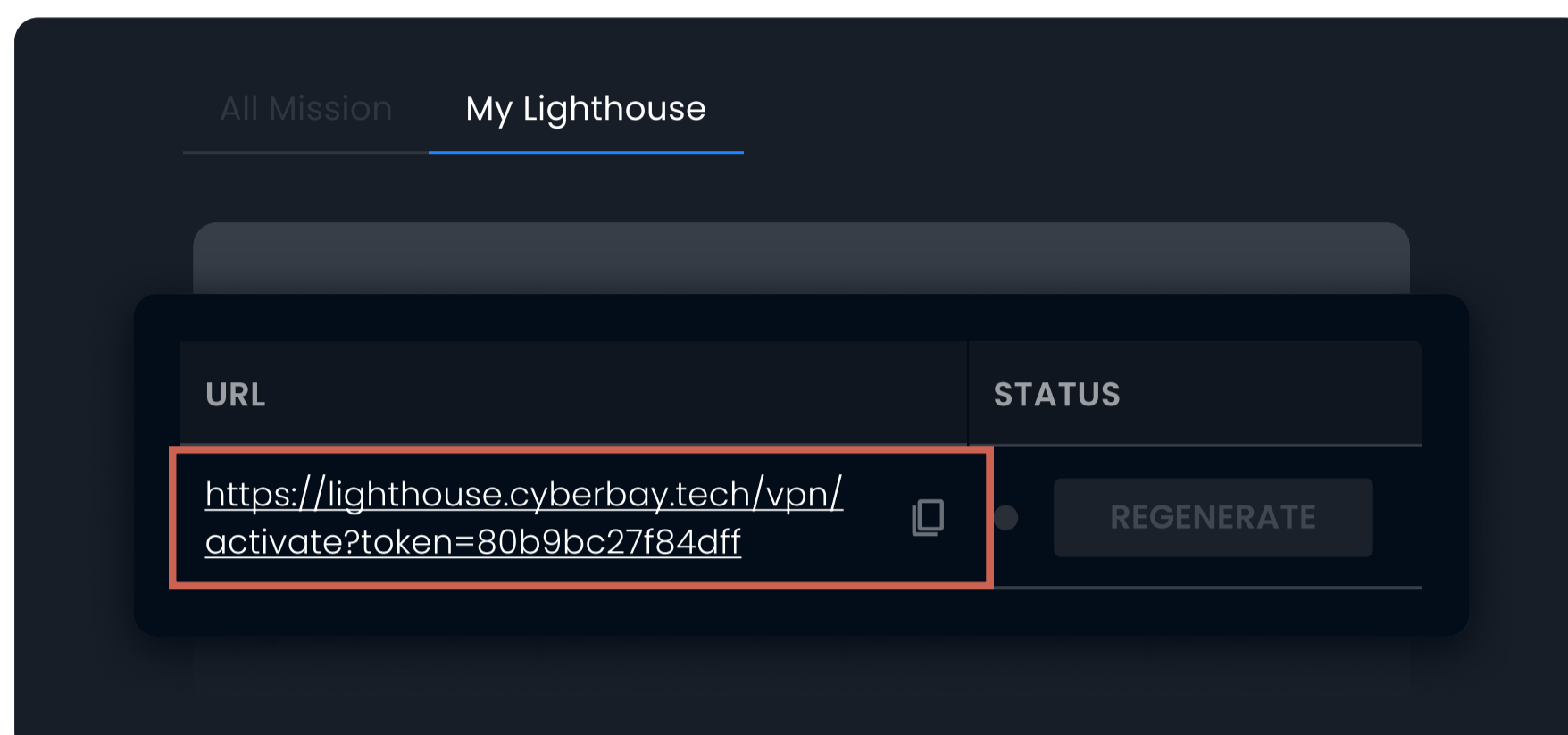
#### 1 Click on a "Regenerate" button, to generate a fresh URL.

This step ensures that you have an updated and valid URL to access the desired resources. It's especially helpful when you have reached the maximum limit of active URLs.



## 2 A fresh and valid VPN URL has been generated for you.

You can configure the provided VPN information within the VPN link to establish a connection to the VPN server.



## 2

### Managing Active Lighthouse Sessions: Handling Maximum Connections

We allow a maximum of **three** active Lighthouse sessions at a time. If you have already connected to three sessions and want to activate another VPN token, you have two options:

#### OPTION 1

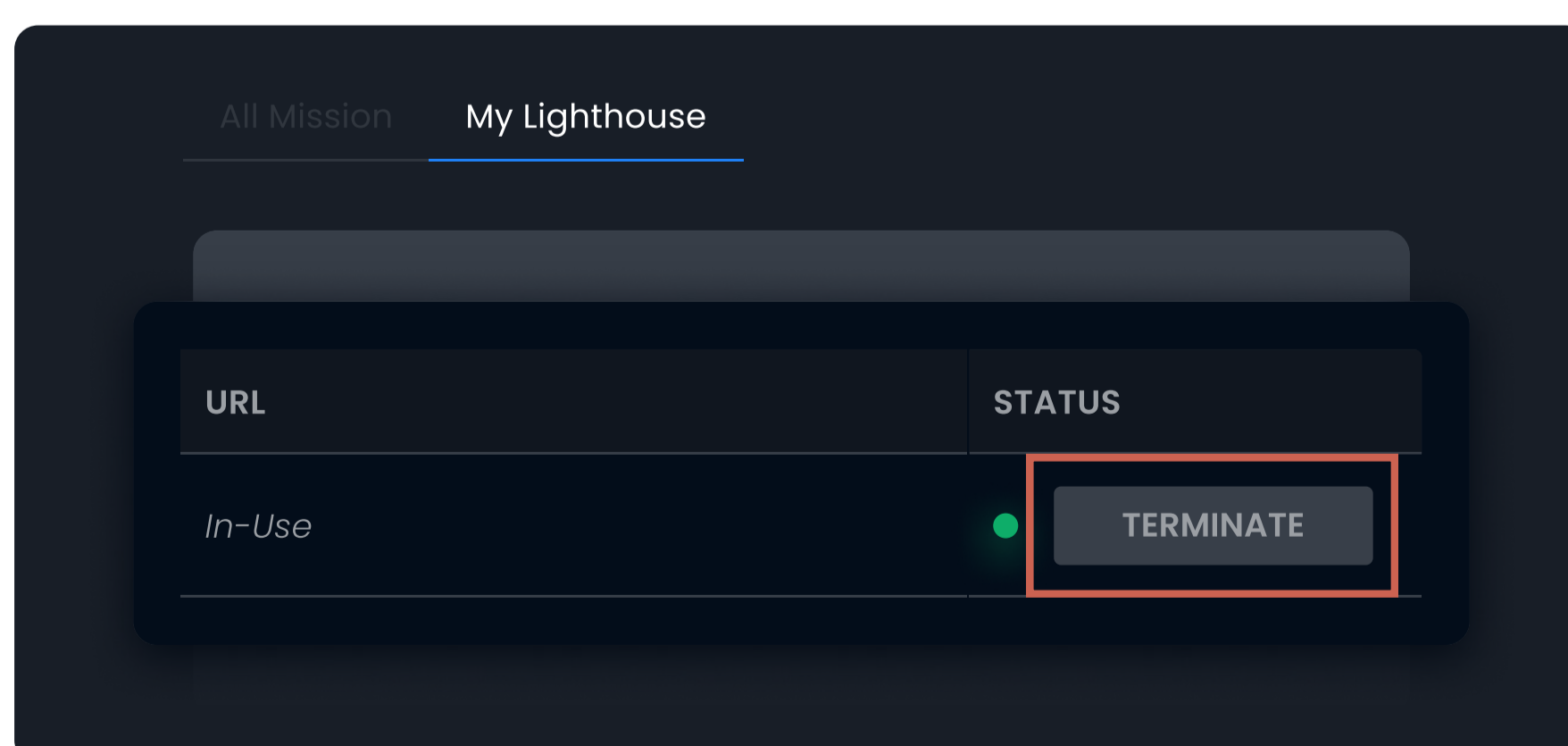
Wait for the natural idle timeout of one of the existing sessions: Once a session becomes idle or disconnected, you can activate a new VPN token.

#### OPTION 2

Manually shut down one of the existing sessions: If you need to activate a new VPN token immediately, manually disconnect one of the active sessions from your "My Lighthouse Page." This will free up a slot for a new session. To address this, follow these steps:

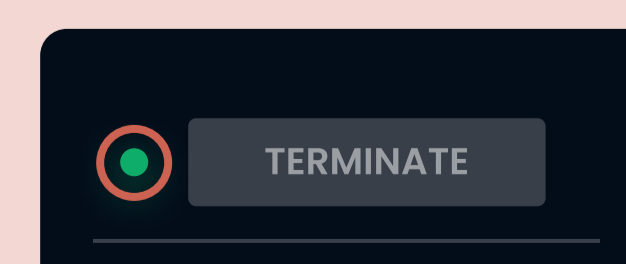
### 1 Click the "Terminate" button to disconnect or terminate a specific URL link.

This step is useful when you no longer need to access or interact with the URL link, especially when you have reached the maximum limit of active URLs.



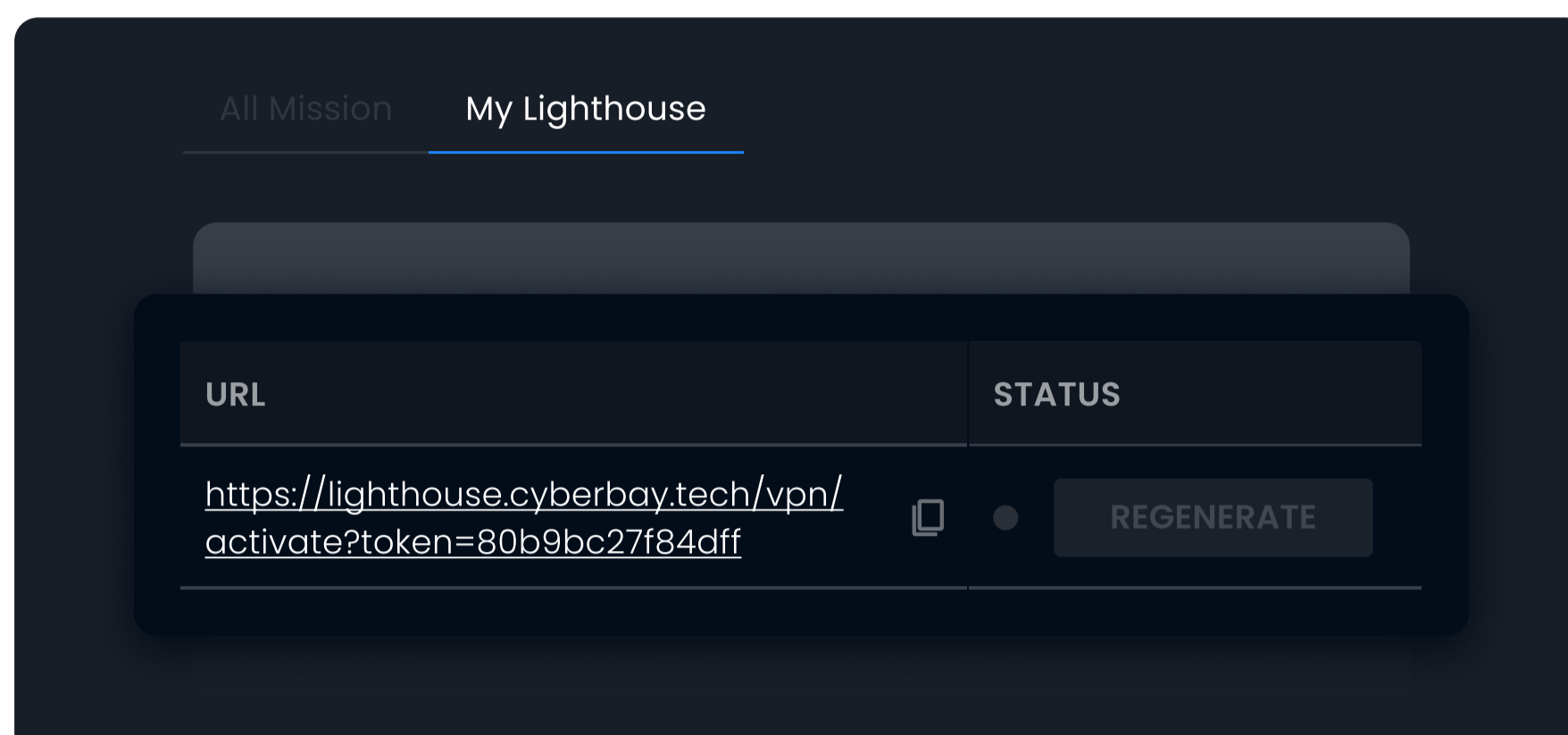
#### ⓘ Important Note:

The presence of the green light indicator does not necessarily mean that you are already connected to the VPN server. It serves as a status indication that the VPN is active and ready for use.



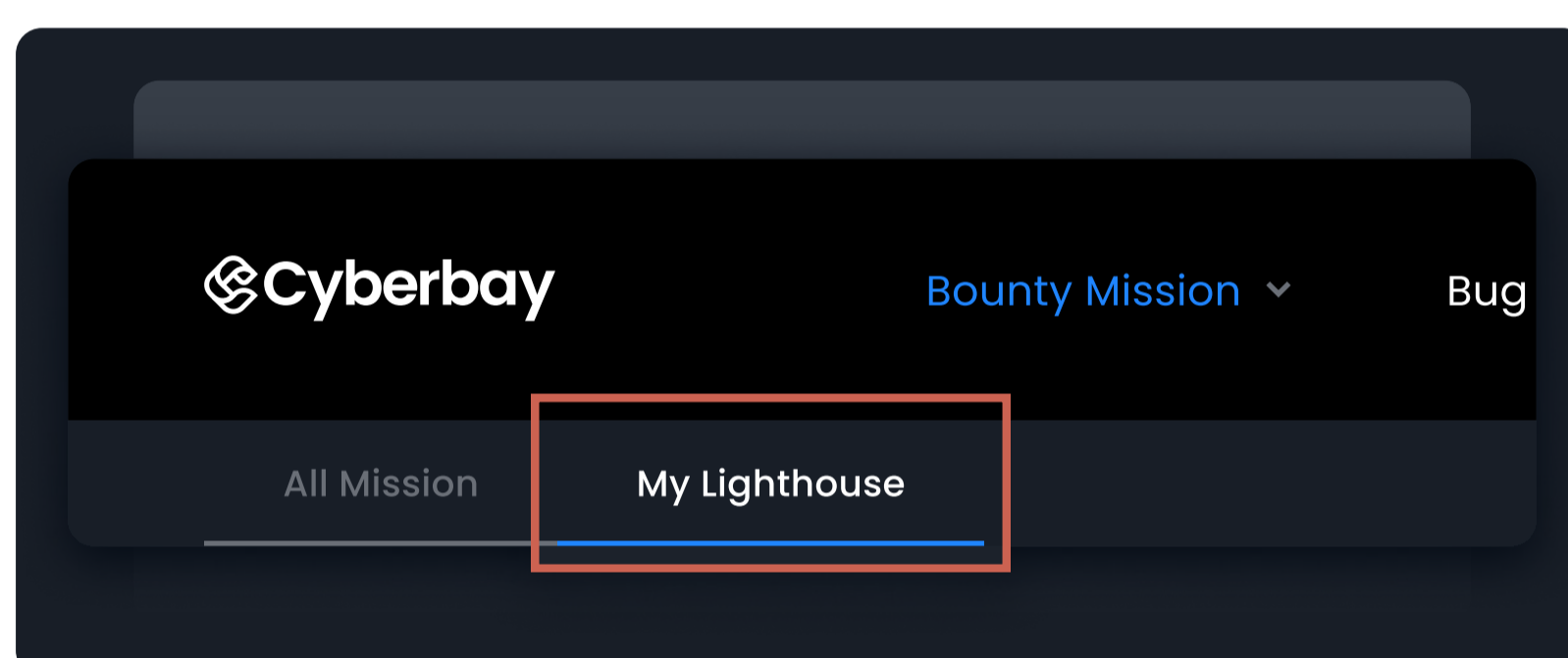
## 2 After terminating the previous VPN session, a fresh and valid VPN URL is generated.

You can configure the provided VPN information within the VPN link to establish a connection to the VPN server.



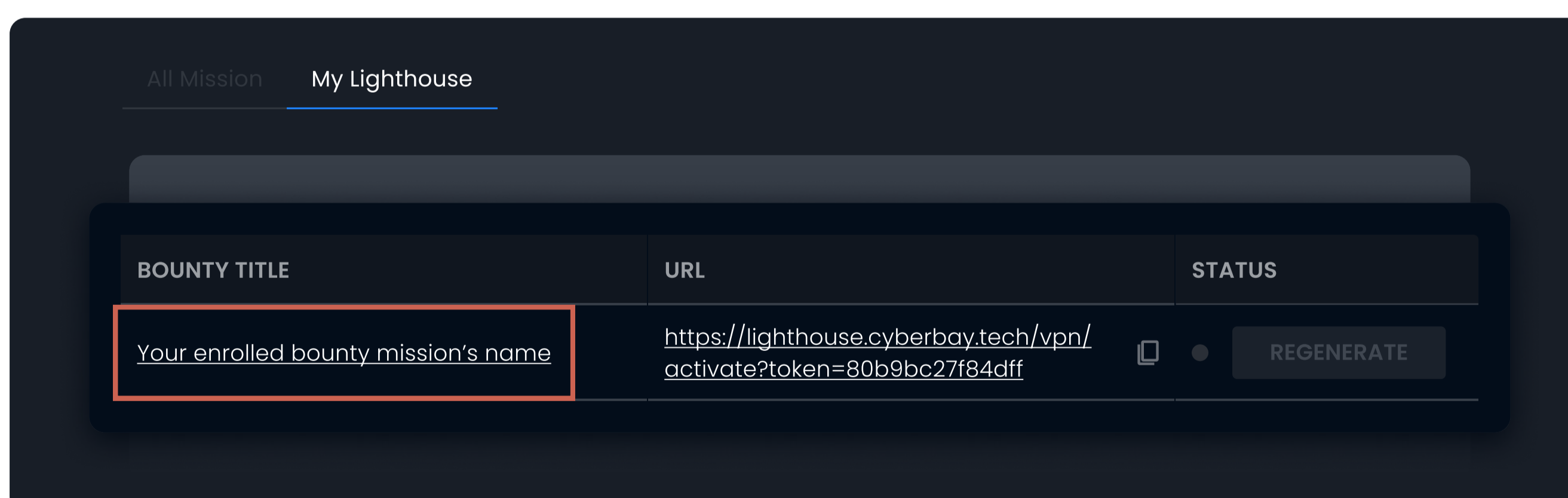
## 3 How to reconnect to our VPN URL If you have already enrolled in the mission?

### 1 Go to the "My Lighthouse" page:



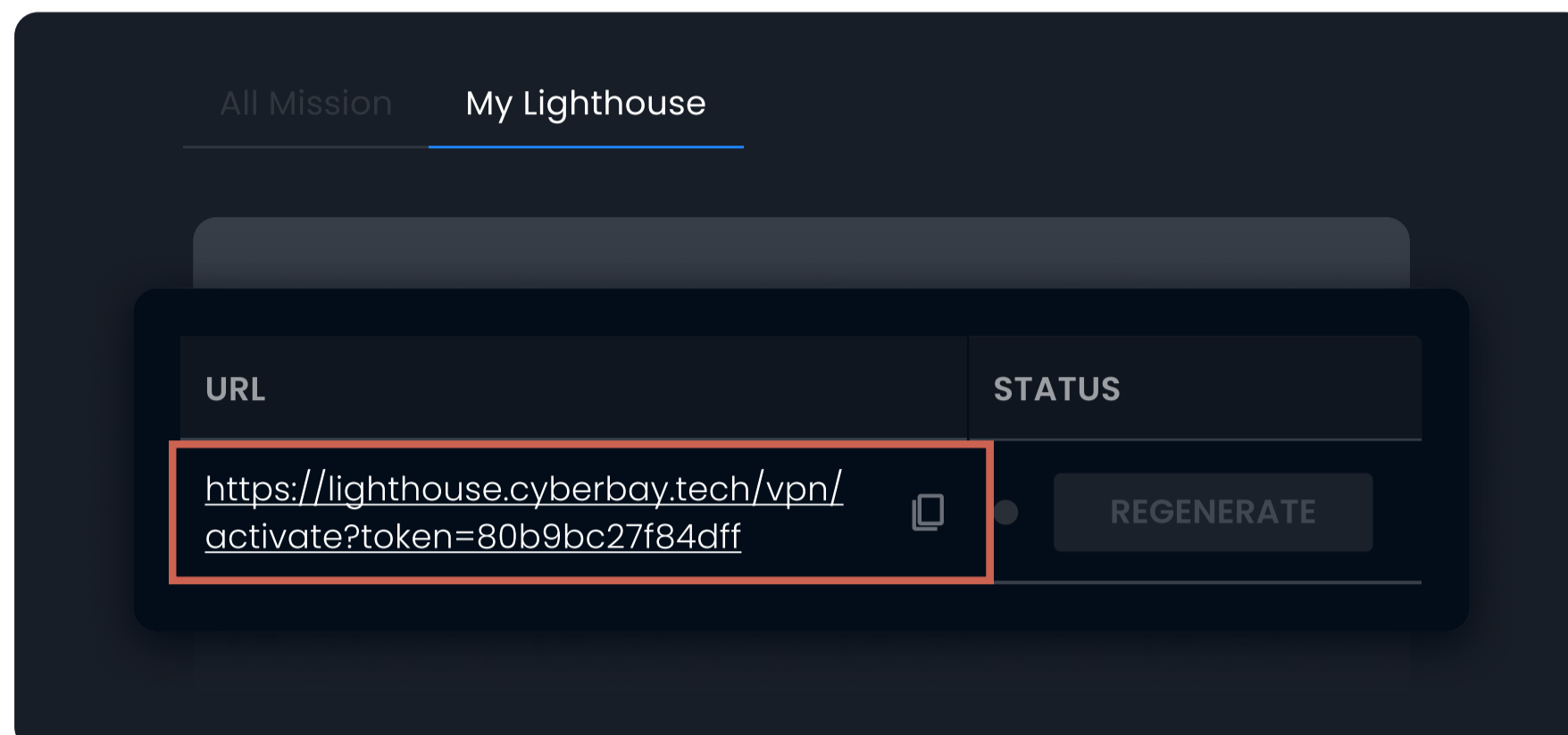
### 2 Locate the mission:

- Look for the specific mission you have enrolled in. The missions you have joined should be listed on the "My Lighthouse" page.



### 3 Find the associated URL:

- Once you have identified the mission, you should find the associated URL for that mission. The URL will likely be displayed alongside the mission details.



### 4 Regenerate the URL (if required):

- If there is an option to regenerate the URL, click on the "Regenerate" button or link to obtain a new URL. This step may be necessary if the previous URL has expired

