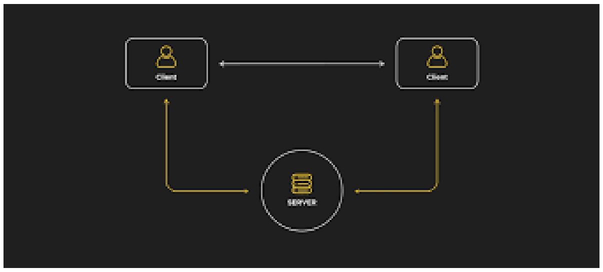
PHISHING ATTACK



What is our GOAL for this CLASS?

In this class, we performed a Phishing Attack to deploy a virus into the victim's device through the page we clone earlier.

What did we ACHIEVE in the class TODAY?

- Learning how to create python executables
- Bypassing Image Uploads in HTML

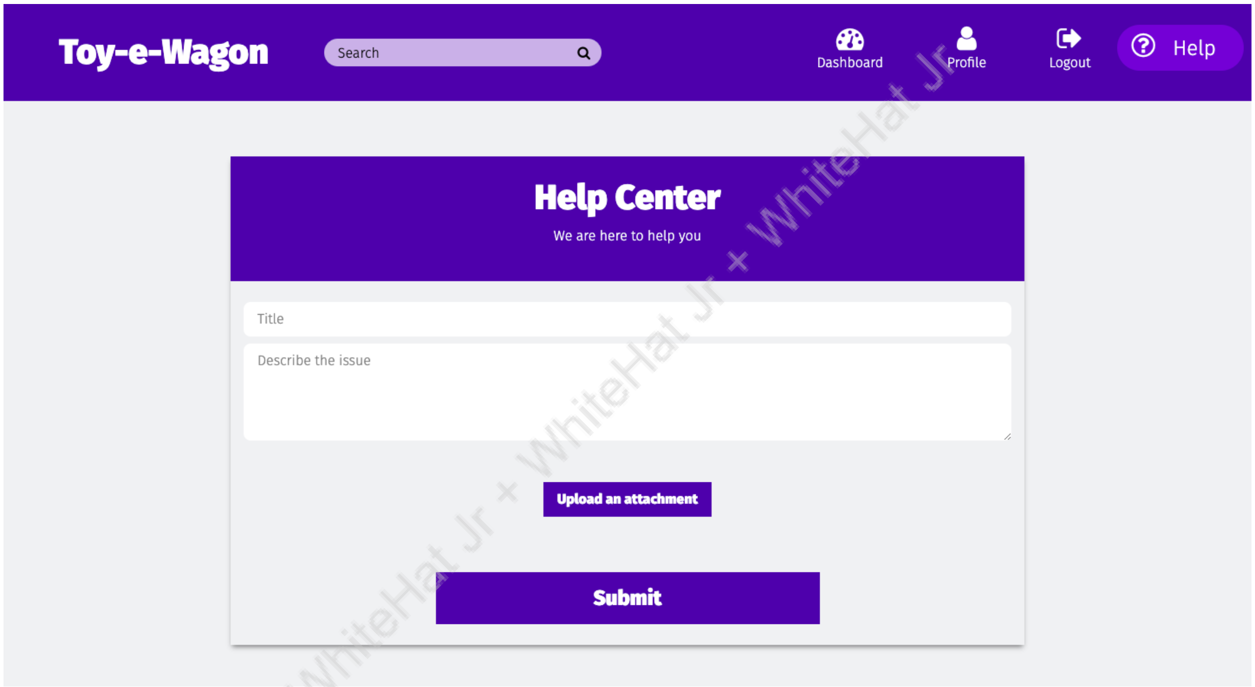
Which CONCEPTS/ CODING BLOCKS did we cover today?

- Creating Python Executables for Mac and Windows
- Bypassing Image Uploads in a website
- IDOR Attack to tweak the URL for getting the desired page.

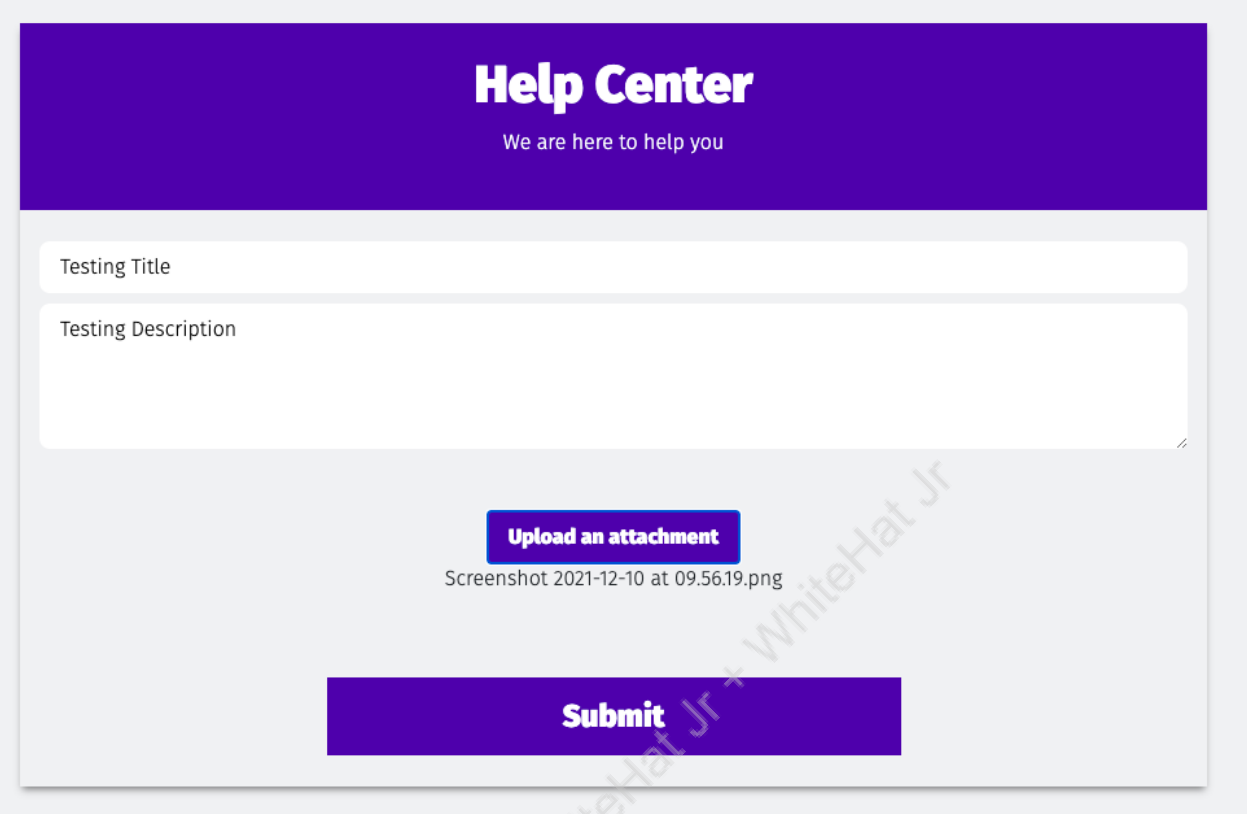
How did we DO the activities?

Activity:

1. Open the website here and login with the following credentials -
    a. Email - john.doe@gmail.com
    b. Password - hello_john
2. In the Navbar, Navigate to ***Help*** next to ***Logout*** button -



3. With the way it is designed, it should only allow uploading PDFs or Image files. For this, the backend of the application usually checks for the extension of the file uploaded and if it's an allowed extension (.jpg, .png, .pdf) then it allows the attachment to be saved into the remote server and generates a URL for it.
4. Hackers usually try to upload different file types by using 2 extension in the following way - ***file.docx.png***
5. To the backend, it looks like a PNG file but it's actually a document file. Backend would fail to detect it and save the file still, which then becomes a part of the server.
6. We create a random ticket to see how it's getting saved and then displayed in the profile page -



Help Center

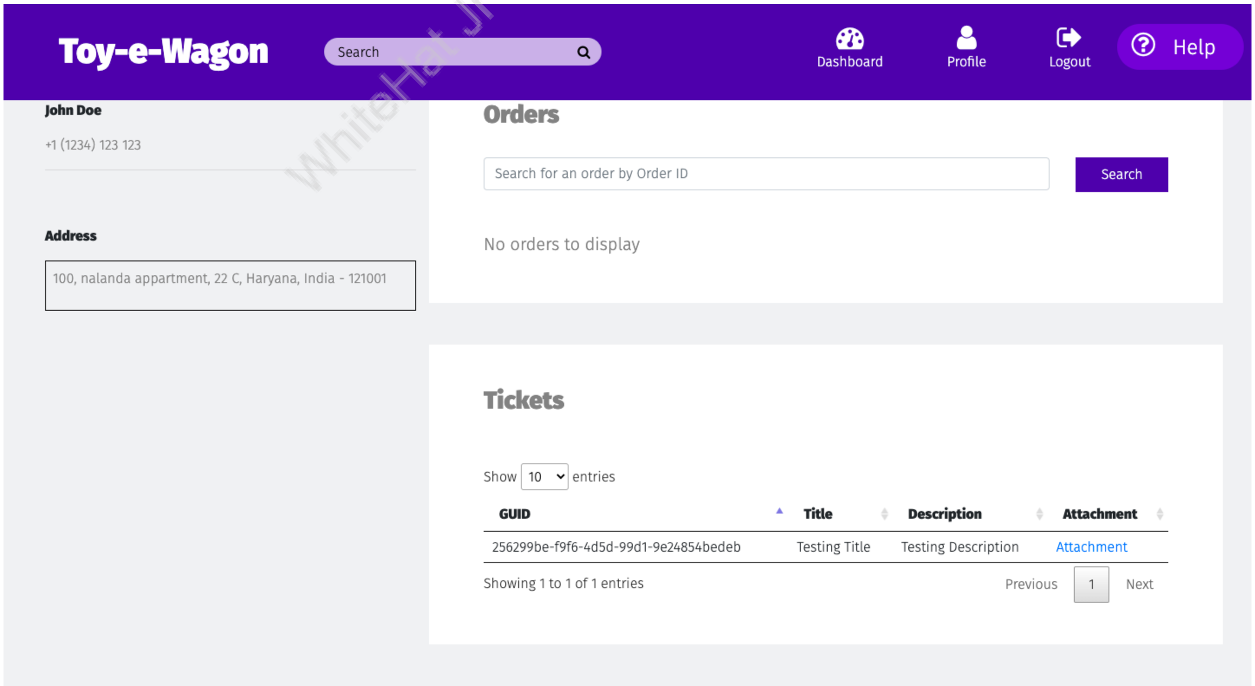
We are here to help you

Testing Title

Testing Description

Screenshot 2021-12-10 at 09.56.19.png

Profile Page -



John Doe

+1 (1234) 123 123

Address

100, nalanda appartment, 22 C, Haryana, India - 121001

Orders

Search for an order by Order ID

No orders to display

Tickets

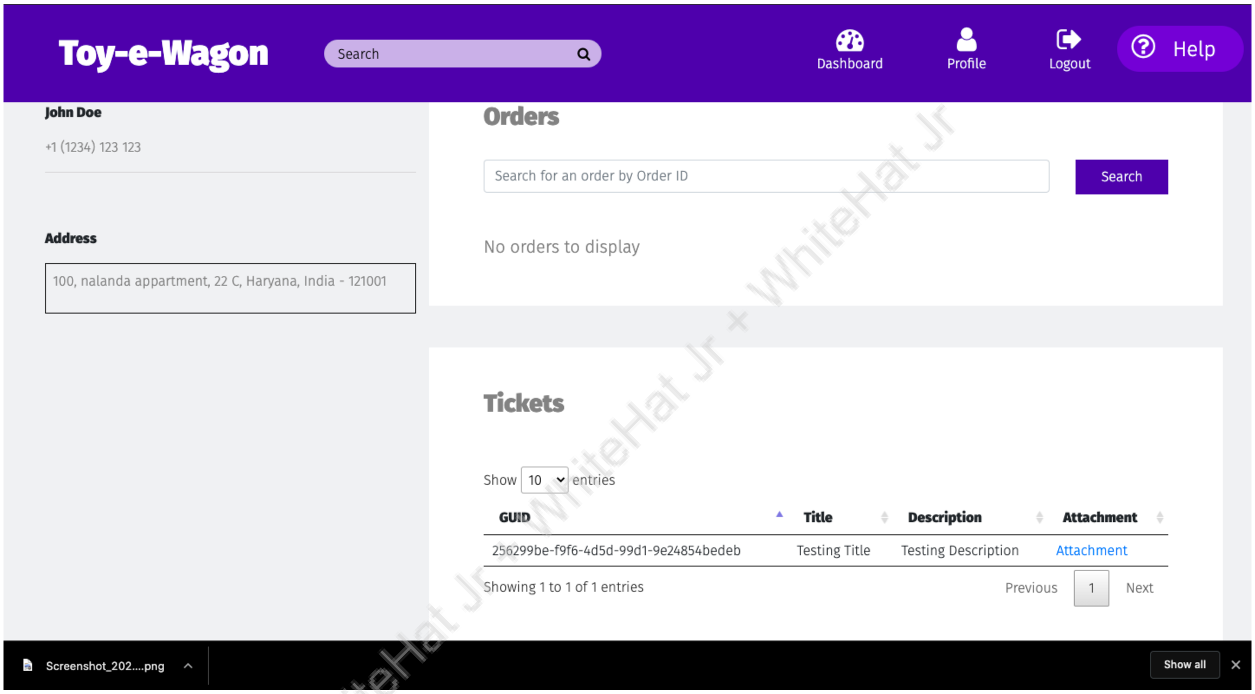
Show 10 entries

GUID	Title	Description	Attachment
256299be-f9f6-4d5d-99d1-9e24854bedeb	Testing Title	Testing Description	Attachment

Showing 1 to 1 of 1 entries

7. In the ticket section, we see the following 4 pages columns -
    a. GUID - Unique ID
    b. Title
    c. Description
    d. Attachment URL

8. If we click on the attachment, we notice that it downloads the attachment automatically for us, so that we can view it on our device.



John Doe

+1 (1234) 123 123

Address

100, nalanda appartment, 22 C, Haryana, India - 121001

Orders

Search for an order by Order ID

No orders to display

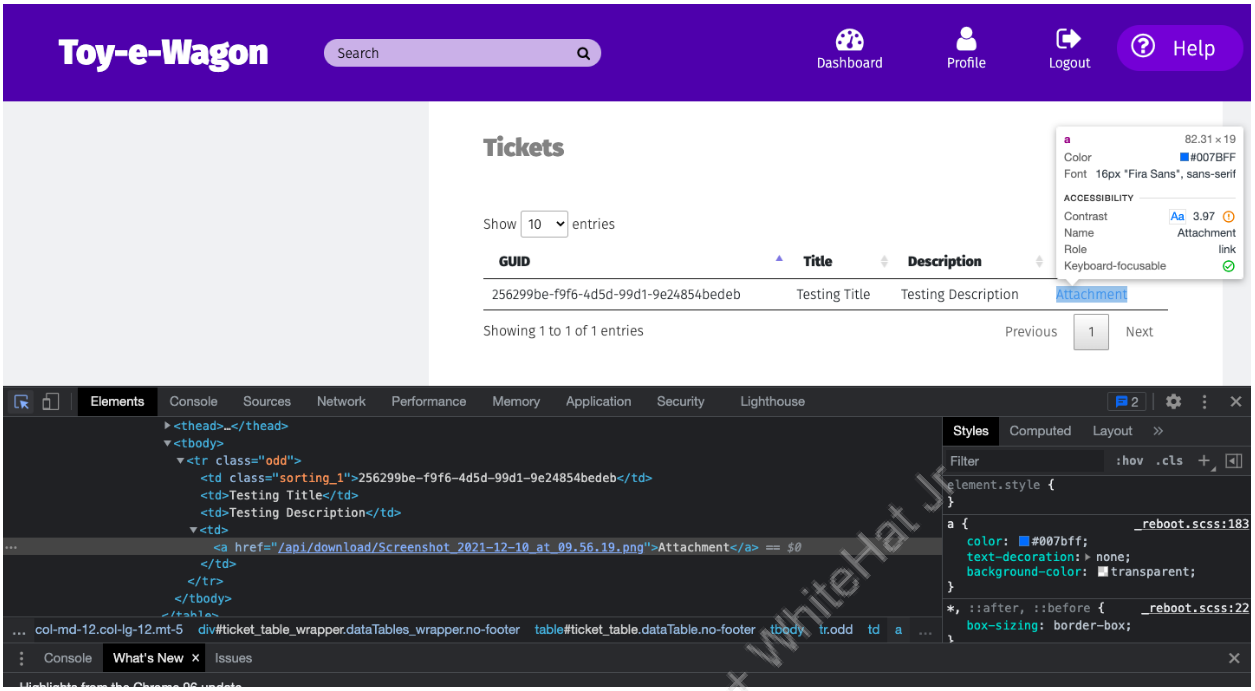
Tickets

Show 10 entries

GUID	Title	Description	Attachment
256299be-f9f6-4d5d-99d1-9e24854bedeb	Testing Title	Testing Description	Attachment

Showing 1 to 1 of 1 entries

9. We check the URL of the attachment from the Google Inspect Tool -



Tickets

Show 10 entries

GUID	Title	Description	
256299be-f9f6-4d5d-99d1-9e24854bedeb	Testing Title	Testing Description	Attachment

Showing 1 to 1 of 1 entries

Previous 1 Next

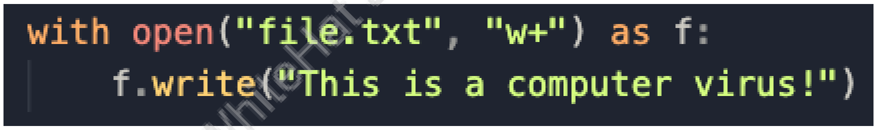
```
a                                   82.31 × 19
Color                               #007BFF
Font       16px "Fira Sans", sans-serif
ACCESSIBILITY
Contrast                            Aa 3.97
Name                                Attachment
Role                                link
Keyboard-focusable
```

```
▸<thead>…</thead>
▾<tbody>
  ▾<tr class="odd">
     <td class="sorting_1">256299be-f9f6-4d5d-99d1-9e24854bedeb</td>
     <td>Testing Title</td>
     <td>Testing Description</td>
    ▾<td>
       <a href="/api/download/Screenshot_2021-12-10_at_09.56.19.png">Attachment</a> == $0
     </td>
   </tr>
 </tbody>
</table>
```

```
element.style {
}
a {                                        _reboot.scss:183
   color: #007bff;
   text-decoration: ▸ none;
   background-color: transparent;
}
*, ::after, ::before {                     _reboot.scss:22
   box-sizing: border-box;
}
```

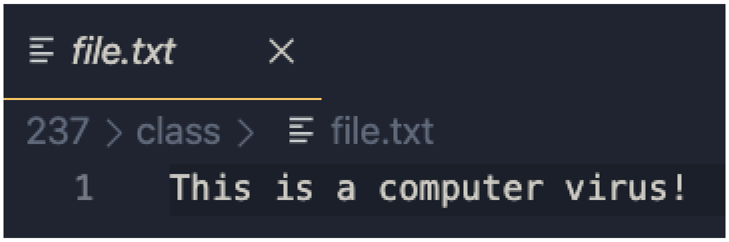
... col-md-12.col-lg-12.mt-5 div#ticket_table_wrapper.dataTables_wrapper.no-footer table#ticket_table.dataTable.no-footer tbody tr.odd td a ...

10. We notice that the following endpoint - ***/api/download/*** is being used to directly download the attachment. This URL or similar URL to this can be used to download the attached virus into a victim's device.
11. We create a simple Python program that creates a **.txt** file and writes ***"This is a computer virus"*** in it.



```
with open("file.txt", "w+") as f:
    f.write("This is a computer virus!")
```

Which creates a file like -

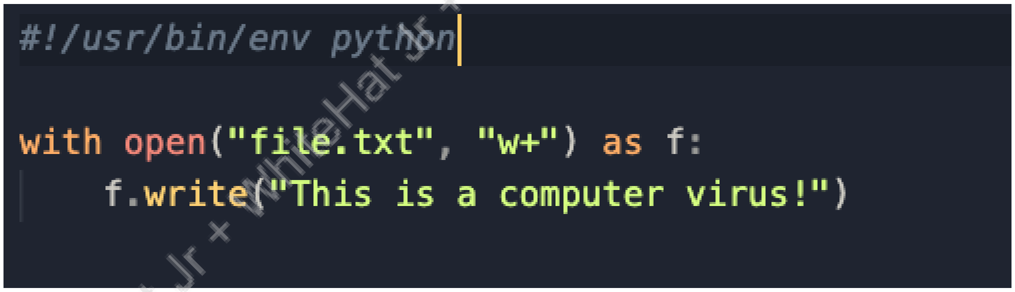


```
This is a computer virus!
```

12. An executable of a file is the **.exe** file or similar to that for other operating systems that the computer can run directly.

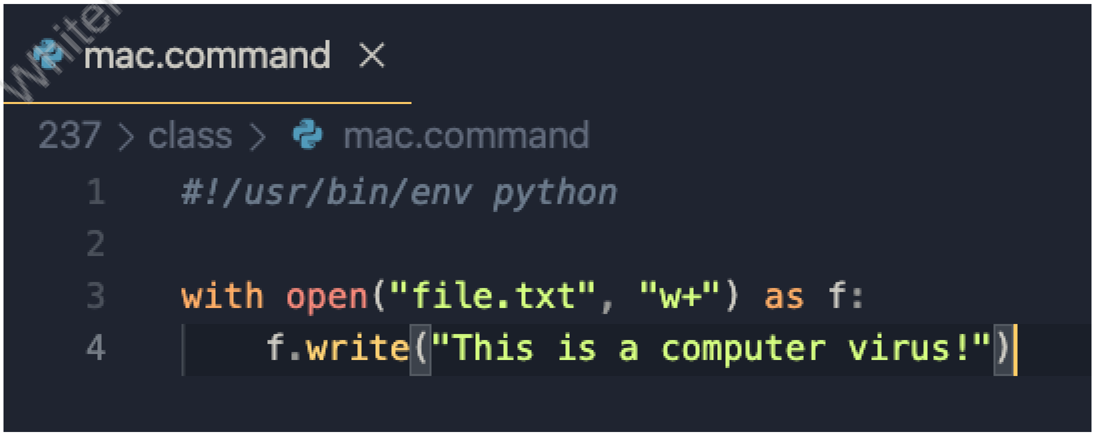
13. To create the executable for this computer program in windows, we will -
    a. Install ***pyinstaller*** into our device with the following command -
        i. ***pip install pyinstaller***
    b. Navigate to the folder in CMD and write the following command -
        i. ***pyinstaller --onefile filename***
        ii. Here the filename would be the name of the Python file you have created.
    c. It might take a couple of minutes to create the .exe file for you.
    d. The .exe file would be available once it's completed in a folder named **"dist".**

14. To create the executable for this computer program in mac or linux, we will -
    a. Create a shebang in our Python file -
        i. Shebang is the first line of the program that tells the operating system which compiler or interpreter to use while running this program.
        ii. In our case, the first line of the program would be - **"*`#!/usr/bin/env python`*"**
        iii.



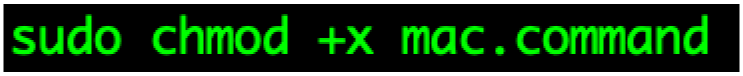
```
#!/usr/bin/env python

with open("file.txt", "w+") as f:
    f.write("This is a computer virus!")
```

    b. Change the file's extension from ***.py*** to ***.command***
        i.



```
#!/usr/bin/env python

with open("file.txt", "w+") as f:
    f.write("This is a computer virus!")
```

    c. Change the permissions of the file with the following command, to make it executable -
        i.

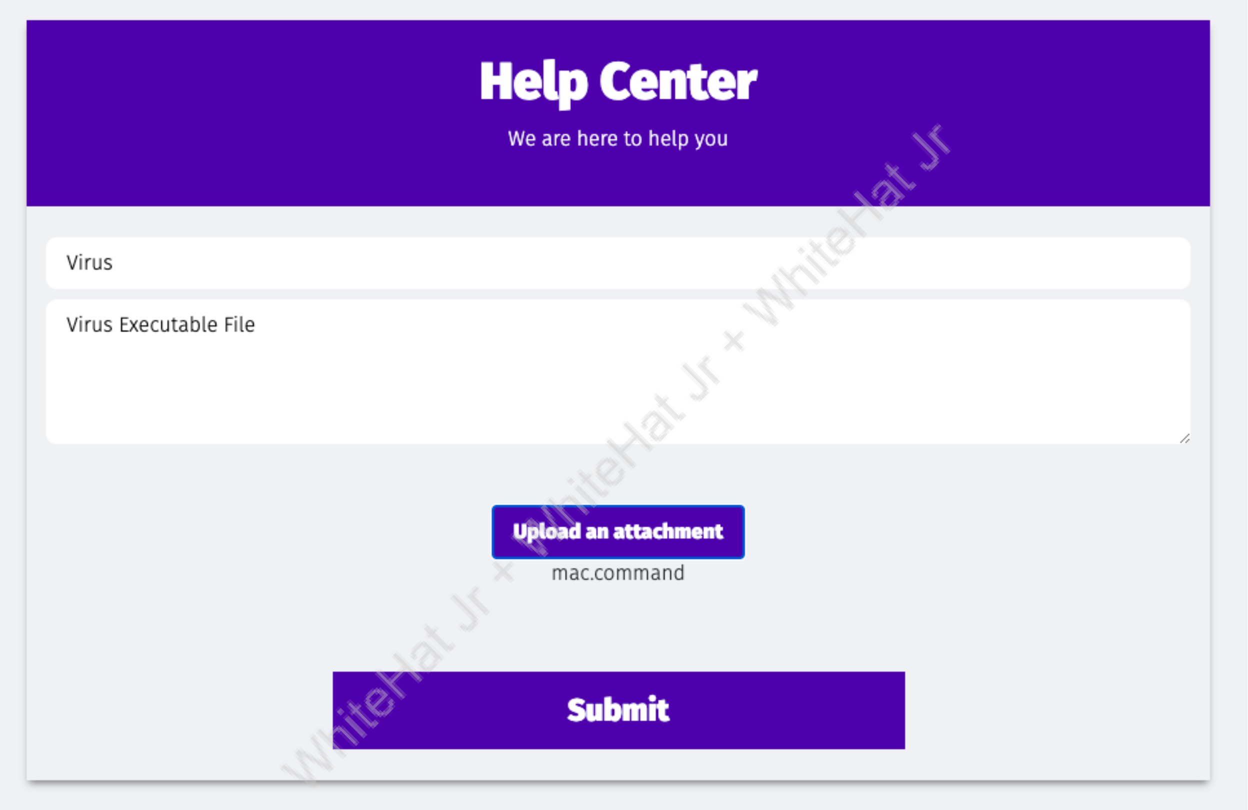


```
sudo chmod +x mac.command
```

ii. Make sure to add ***sudo*** in the command's beginning if it's giving you a permission error.

d. On double clicking on the file, you will now notice that the .txt file will get created in the system's default location. It could be the root folder of your user where folders like ***Desktop and Downloads*** also exist.

15. Now, since our temporary virus is ready to use, we can simply just upload it on the ***Help*** page to get a downloadable link for it -

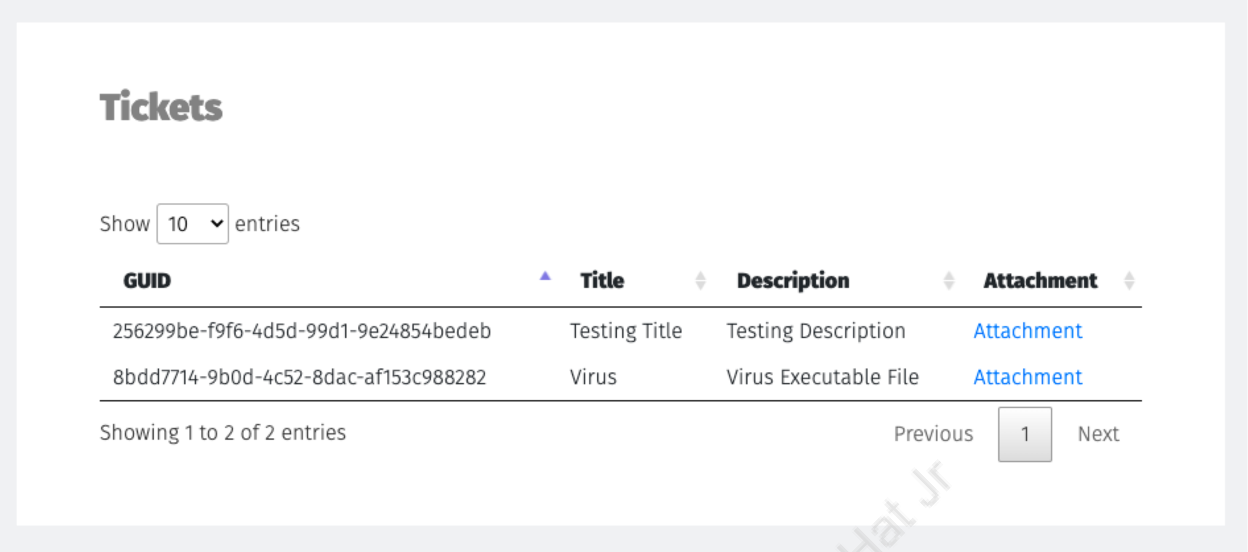


Virus

Virus Executable File

mac.command

Output on Profile Page -



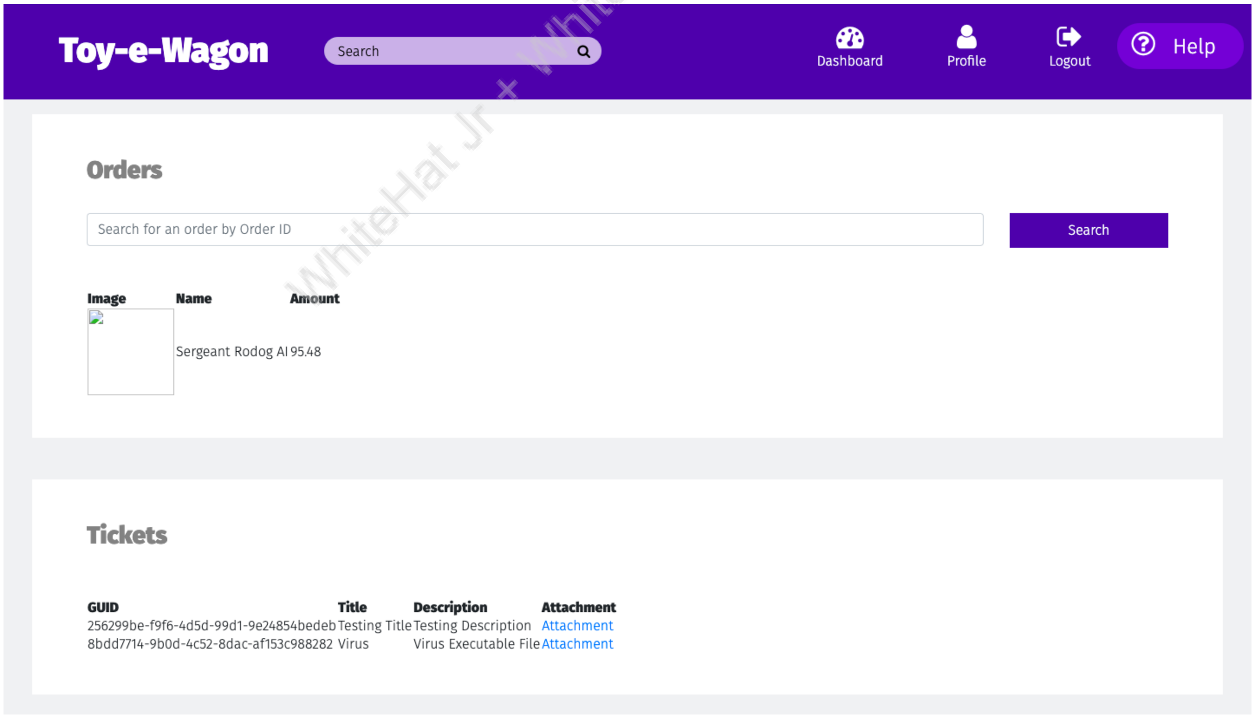
Tickets

Show 10 entries

GUID	Title	Description	Attachment
256299be-f9f6-4d5d-99d1-9e24854bedeb	Testing Title	Testing Description	Attachment
8bdd7714-9b0d-4c52-8dac-af153c988282	Virus	Virus Executable File	Attachment

Showing 1 to 2 of 2 entries

16. We will take the link of this attachment of the virus from the Google Inspect, and add it in our Phishing Page. Code for the Phishing Page exists here.
17. This cloning page now displays all the orders and tickets that the user john.doe@gmail.com has in the website. Do make sure that it has at least one order.



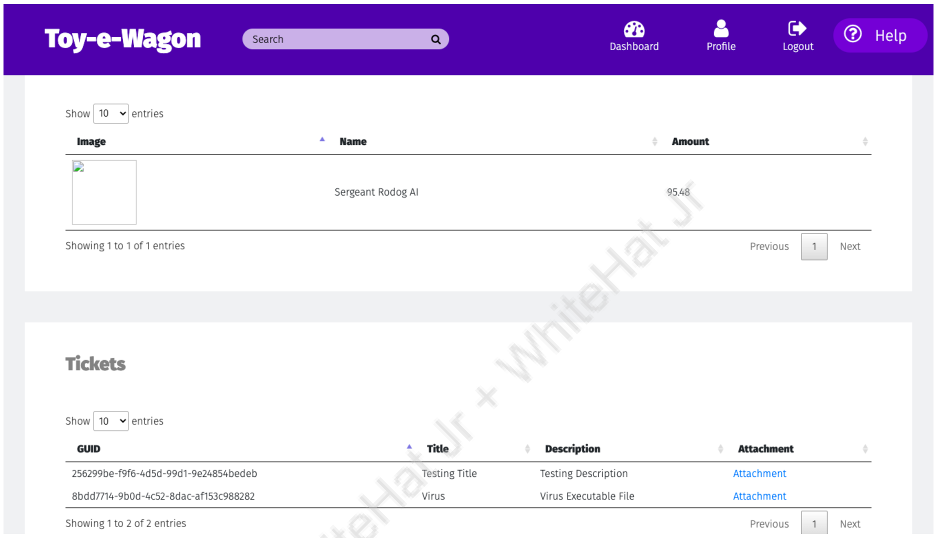
Orders

Image	Name	Amount
	Sergeant Rodog AI	95.48

Tickets

GUID	Title	Description	Attachment
256299be-f9f6-4d5d-99d1-9e24854bedeb	Testing Title	Testing Description	Attachment
8bdd7714-9b0d-4c52-8dac-af153c988282	Virus	Virus Executable File	Attachment

18. If you page looks distorted like the above, add the following links in the **<head>** tag -
    a. <link rel="stylesheet" type="text/css" href="https://cdn.datatables.net/1.11.3/css/jquery.dataTables.css">
    b. <script type="text/javascript" charset="utf8" src="https://cdn.datatables.net/1.11.3/js/jquery.dataTables.js"></script>
    c. The page would then look like -
    d.



Show 10 entries

Image	Name	Amount
	Sergeant Rodog AI	95.48

Showing 1 to 1 of 1 entries Previous 1 Next

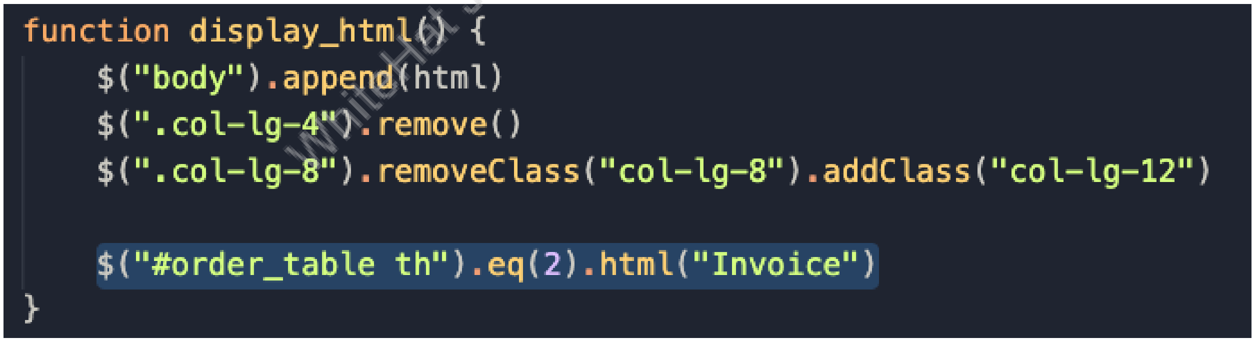
Tickets

Show 10 entries

GUID	Title	Description	Attachment
256299be-f9f6-4d5d-99d1-9e24854bedeb	Testing Title	Testing Description	Attachment
8bdd7714-9b0d-4c52-8dac-af153c988282	Virus	Virus Executable File	Attachment

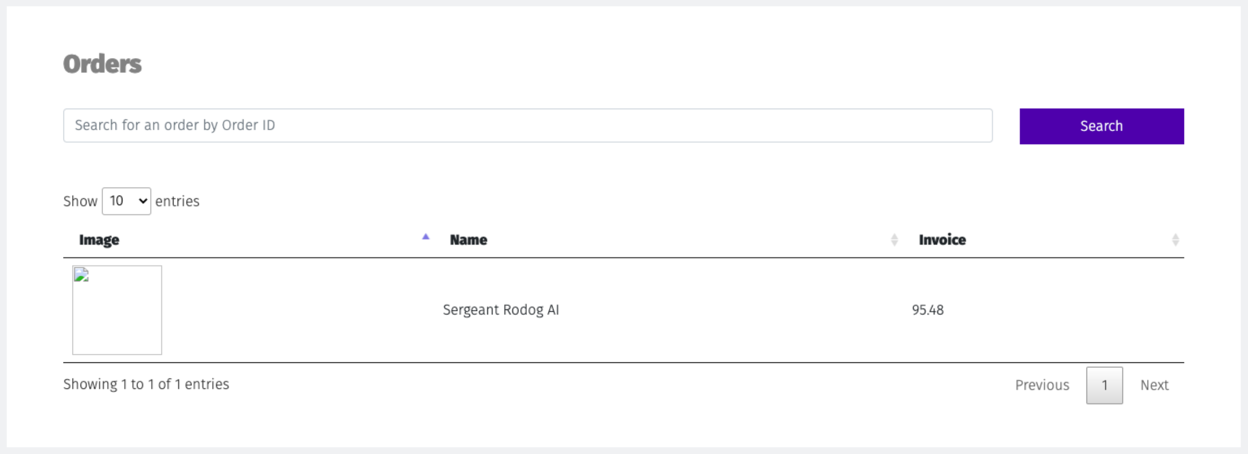
Showing 1 to 2 of 2 entries Previous 1 Next

19. We can change the ***Amount*** column when displaying the orders by using some jQuery, and instead display ***Invoice*** in its place -



```
function display_html() {
    $("body").append(html)
    $(".col-lg-4").remove()
    $(".col-lg-8").removeClass("col-lg-8").addClass("col-lg-12")

    $("#order_table th").eq(2).html("Invoice")
}
```

Output -



Orders

Search for an order by Order ID

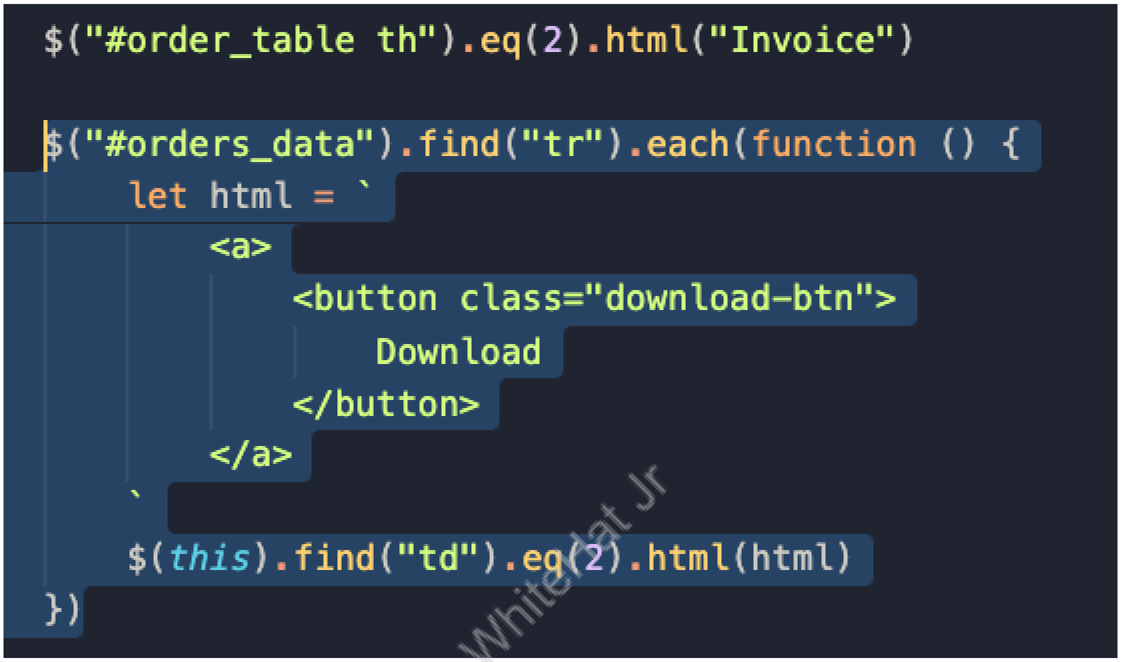
Show 10 entries

Image	Name	Invoice
	Sergeant Rodog AI	95.48

Showing 1 to 1 of 1 entries

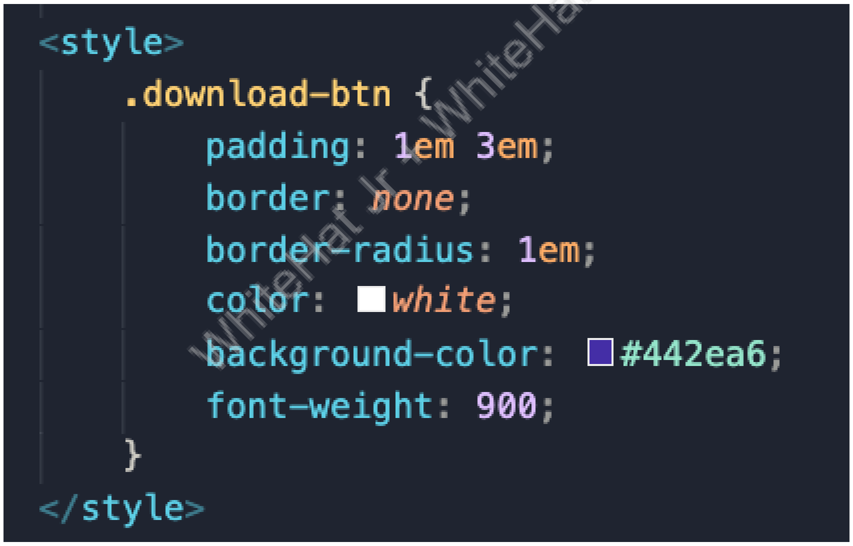
20. We wrote the above code with the following understanding -
    a. Table has an ID called **“#order_table”**
    b. It has a ***th*** tag which means table-head with 3 values -
        i. Image
        ii. Name
        iii. Invoice
    c. ***$(“#order_table th”)*** would then give us an array of ***th*** tags in the order table
    d. With the help of **eq()** function, we could traverse this array with indexes 0, 1 and 2.
    e. We use the index 2 for the last column, and with the ***html()*** function, change the HTML text of the column.
    f. Inside the same table, we have the data saved in an ID ***“#order_data”*** in which the rows are written in ***tr*** tag, or table-row.
    g. We can iterate over each of the ***tr*** tags and replace the HTML with a download button -

i.



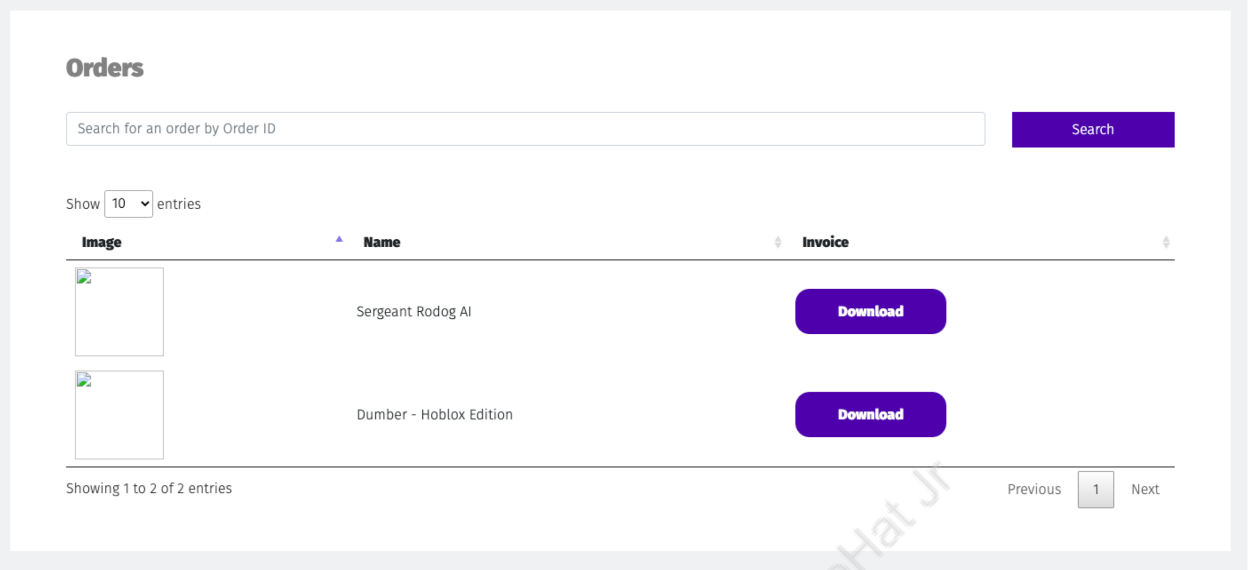
```
$("#order_table th").eq(2).html("Invoice")

$("#orders_data").find("tr").each(function () {
    let html = `
        <a>
            <button class="download-btn">
                Download
            </button>
        </a>
    `
    $(this).find("td").eq(2).html(html)
})
```

21. We add some styling for our Download button -



```
<style>
    .download-btn {
        padding: 1em 3em;
        border: none;
        border-radius: 1em;
        color: white;
        background-color: #442ea6;
        font-weight: 900;
    }
</style>
```

Output -



Orders

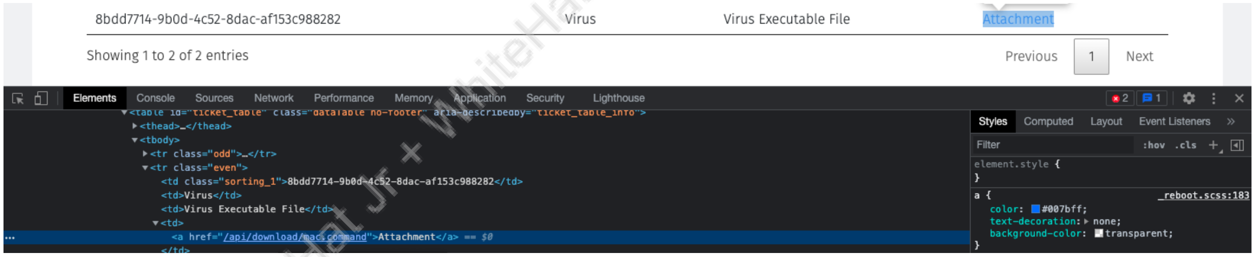
Search for an order by Order ID

Show 10 entries

Image	Name	Invoice
	Sergeant Rodog AI	Download
	Dumber - Hoblox Edition	Download

Showing 1 to 2 of 2 entries

22. We fetch the downloadable URL of our virus and add it as an ***href*** attribute to an anchor tag above the download button -

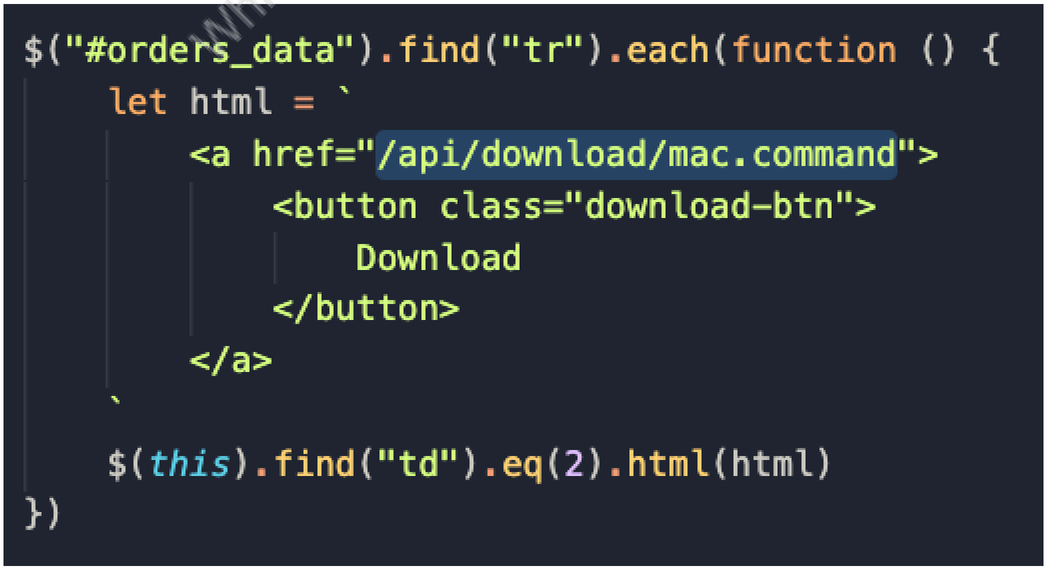


8bdd7714-9b0d-4c52-8dac-af153c988282	Virus	Virus Executable File	Attachment

Showing 1 to 2 of 2 entries

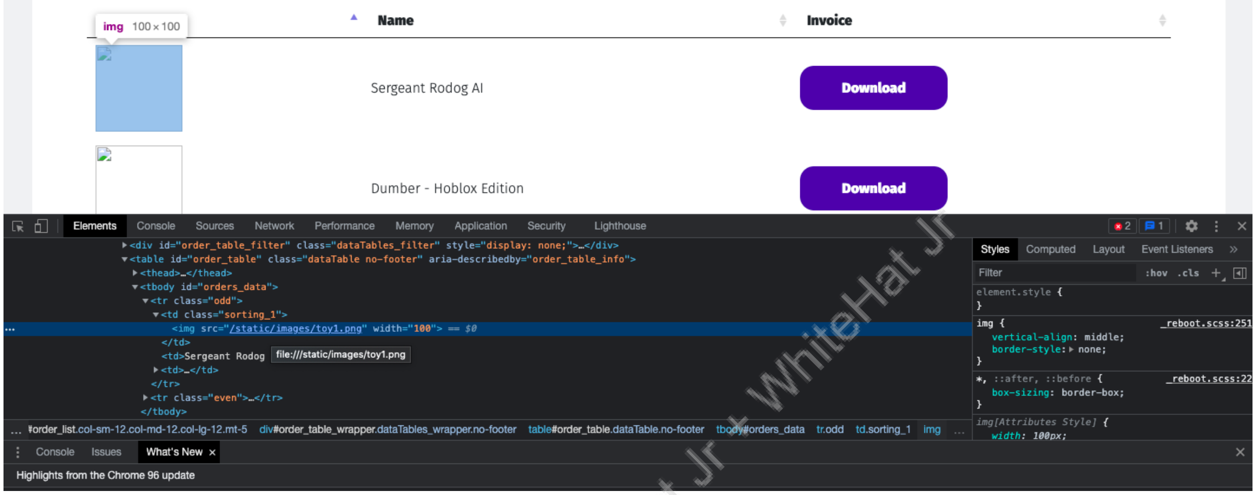
```
▼<table id="ticket_table" class="datatable no-footer" aria-describedby="ticket_table_info">
  ▶<thead>…</thead>
  ▼<tbody>
    ▶<tr class="odd">…</tr>
    ▼<tr class="even">
        <td class="sorting_1">8bdd7714-9b0d-4c52-8dac-af153c988282</td>
        <td>Virus</td>
        <td>Virus Executable File</td>
      ▼<td>
...       <a href="/api/download/mac.command">Attachment</a> == $0
        </td>
```

```
element.style {
}
a {                                     _reboot.scss:183
    color: #007bff;
    text-decoration: ▶ none;
    background-color: transparent;
}
```



```
$("#orders_data").find("tr").each(function () {
    let html = `
        <a href="/api/download/mac.command">
            <button class="download-btn">
                Download
            </button>
        </a>
    `
    $(this).find("td").eq(2).html(html)
})
```

23. We inspect the broken images coming in our cloned phishing page and realise that the images are saved in the **static** folder of the app, which means that our attachments are too getting saved in the ***static*** folder under some other URL -



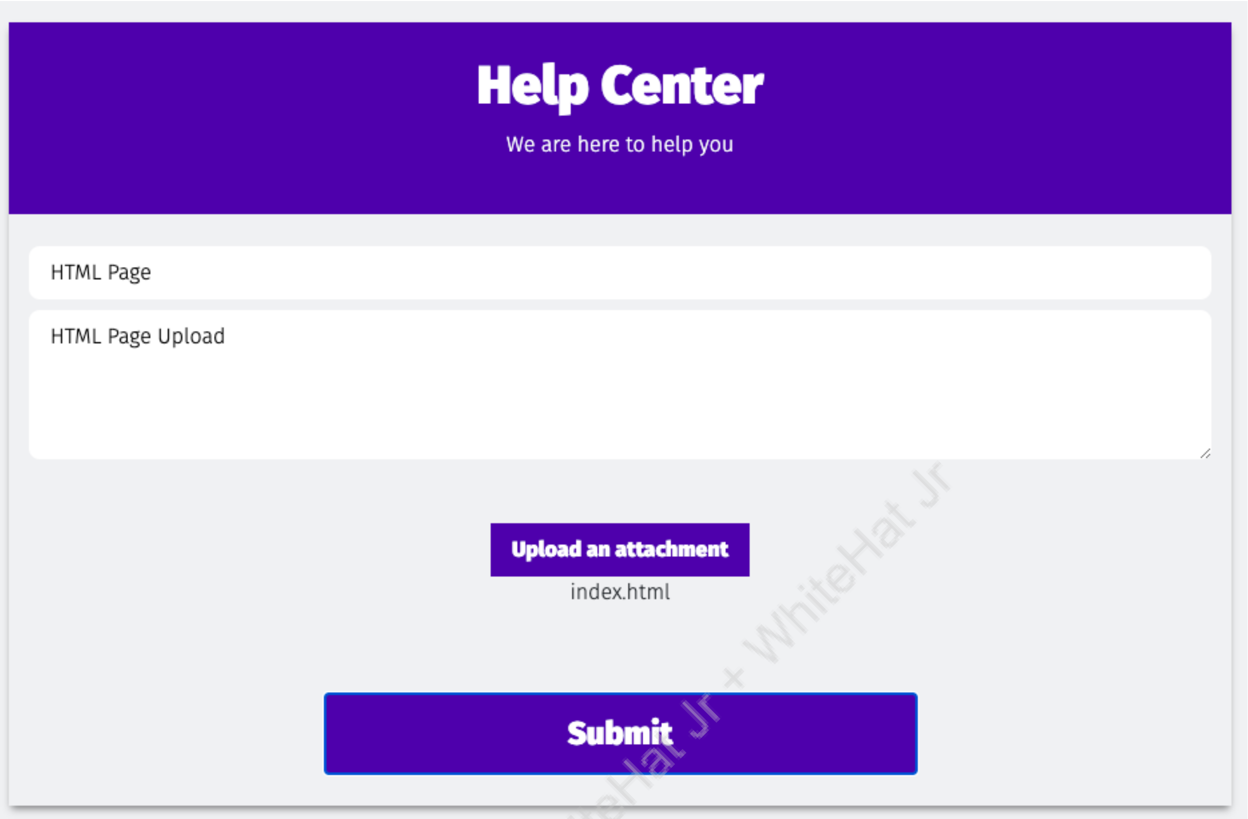
	Name	Invoice
	Sergeant Rodog AI	Download
	Dumber - Hoblox Edition	Download

```
▸<div id="order_table_filter" class="dataTables_filter" style="display: none;">…</div>
▾<table id="order_table" class="dataTable no-footer" aria-describedby="order_table_info">
  ▸<thead>…</thead>
  ▾<tbody id="orders_data">
    ▾<tr class="odd">
      ▾<td class="sorting_1">
          <img src="/static/images/toy1.png" width="100"> == $0
        </td>
        <td>Sergeant Rodog  file:///static/images/toy1.png
      ▸<td>…</td>
      </tr>
    ▸<tr class="even">…</tr>
    </tbody>
```

```
… #order_list.col-sm-12.col-md-12.col-lg-12.mt-5   div#order_table_wrapper.dataTables_wrapper.no-footer   table#order_table.dataTable.no-footer   tbody#orders_data   tr.odd   td.sorting_1   img   …
```

```
element.style {
}
img {                                  _reboot.scss:251
    vertical-align: middle;
    border-style: ▸ none;
}
*, ::after, ::before {                 _reboot.scss:22
    box-sizing: border-box;
}
img[Attributes Style] {
    width: 100px;
```

24. This brings us back to the IDOR attack we have performed earlier, which means that a similar folder-like images for attachments exists in the server too. It could be ***attachment*** or ***attachments***.
    a. For this website, we are using ***attachments***
25. By manipulating the URL again, using the structure like ***/static/attachments/filename*** we can access the file's link directly in the server and access them how we can access images.
26. We upload our cloned page's HTML into the HELP page -



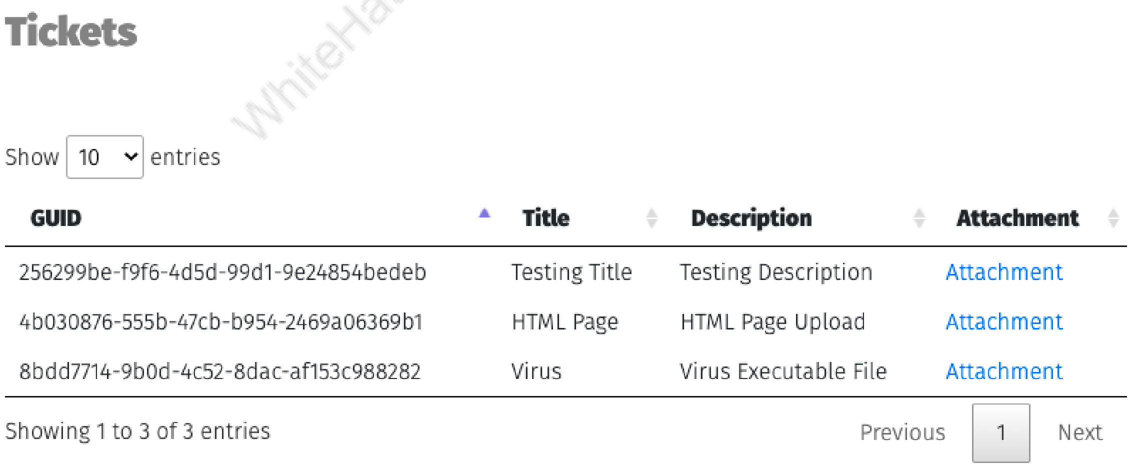
Help Center

We are here to help you

HTML Page

HTML Page Upload

Output -



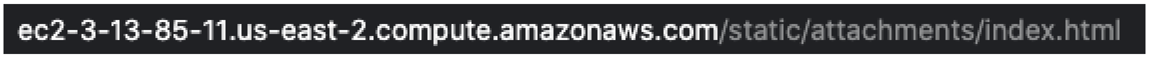
Tickets

Show 10 entries

GUID	Title	Description	Attachment
256299be-f9f6-4d5d-99d1-9e24854bedeb	Testing Title	Testing Description	Attachment
4b030876-555b-47cb-b954-2469a06369b1	HTML Page	HTML Page Upload	Attachment
8bdd7714-9b0d-4c52-8dac-af153c988282	Virus	Virus Executable File	Attachment

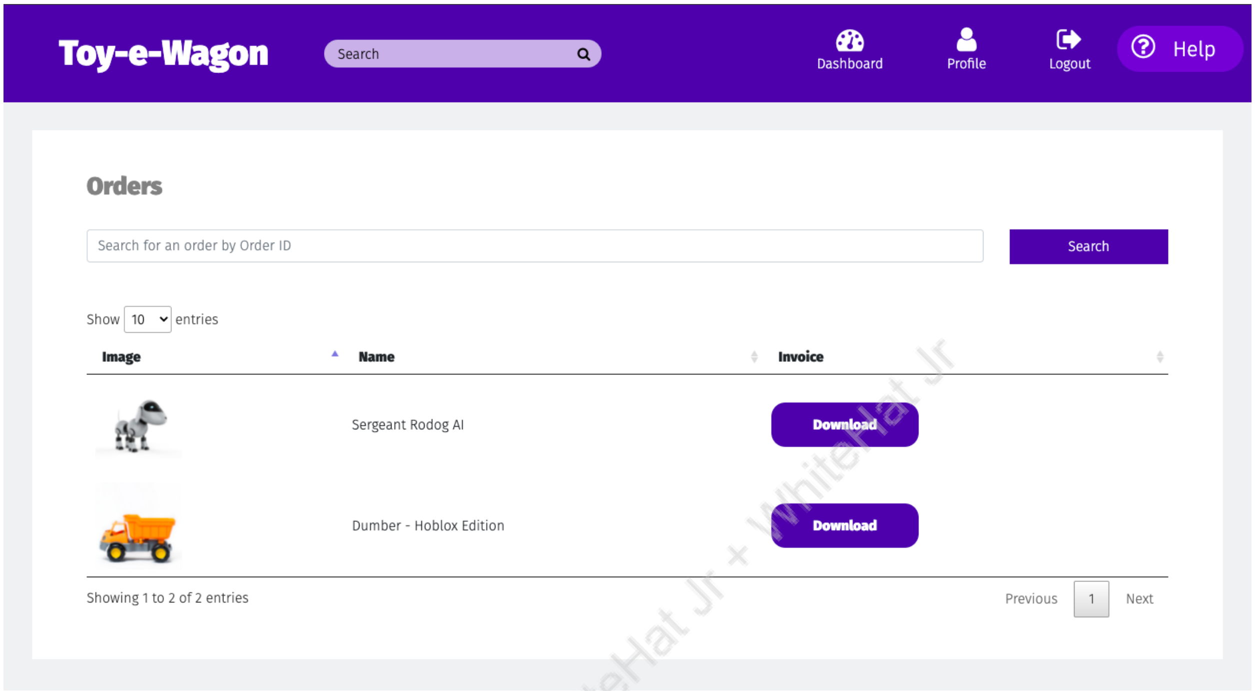
Showing 1 to 3 of 3 entries

27. We go to the URL we predicted for our Cloned HTML Page -

    a. 

    ```
    ec2-3-13-85-11.us-east-2.compute.amazonaws.com/static/attachments/index.html
    ```

28. We see it working perfectly. This page can now be used to fool other people and make them download any virus that you may want.



Orders

Search for an order by Order ID
Search

Show 10 entries

Image	Name	Invoice
	Sergeant Rodog AI	Download
	Dumber - Hoblox Edition	Download

Showing 1 to 2 of 2 entries

Previous 1 Next

What's NEXT?

In the next class, we will learn about join statements in SQL

Expand Your Knowledge:

Explore more about Python executables [here](#).