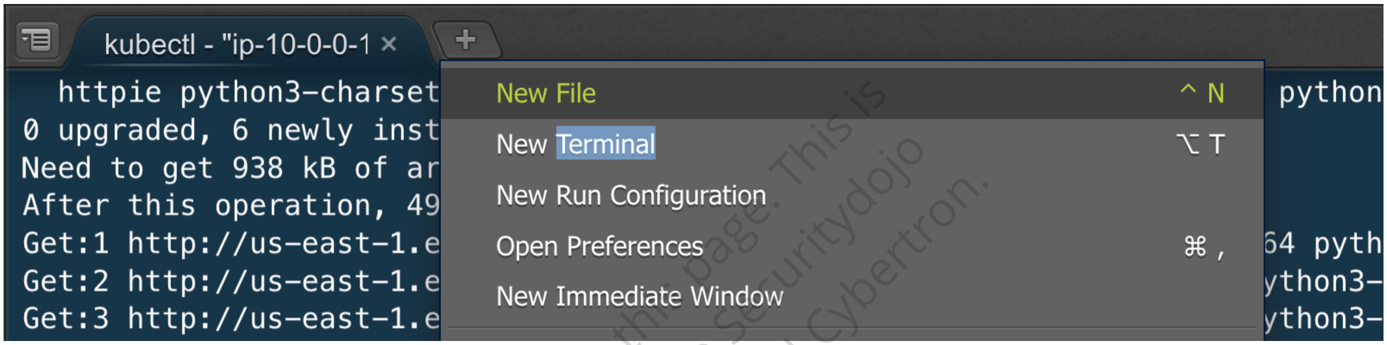
Lab: Validation of Sample Application

> For this demo replace the `http://<subdomain>.securitydojo.co.in` with your domain name, do not copy paste.

Open New Terminal

- Click on `+` icon, then select `new terminal` to open new terminal.

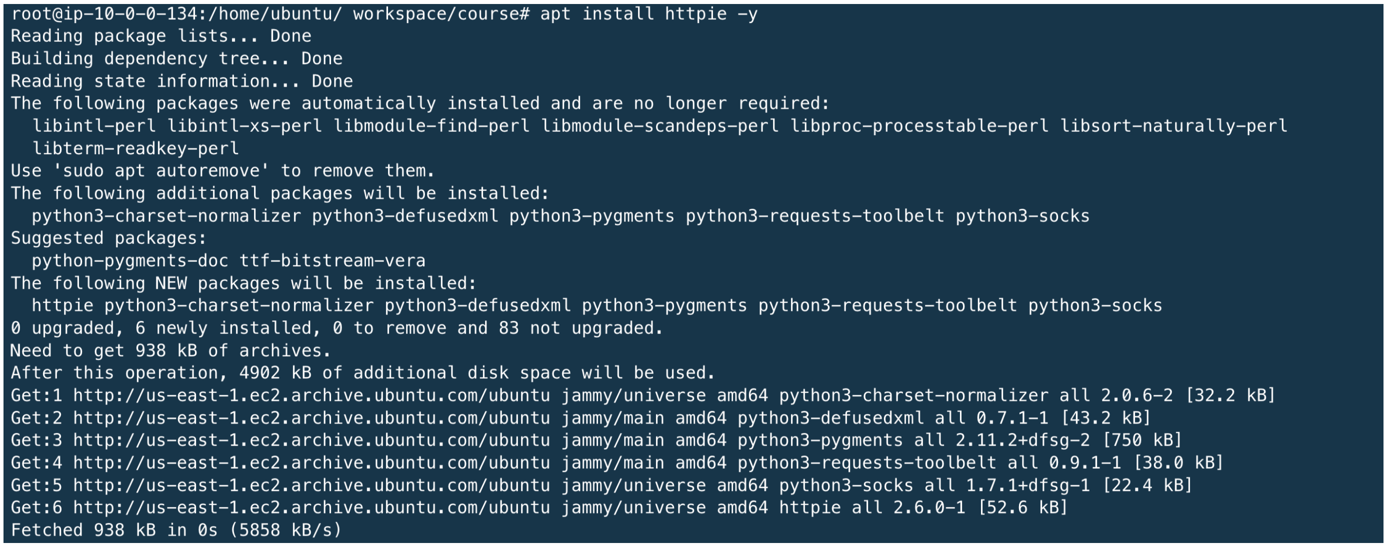


```
  httpie python3-charset                                               python
0 upgraded, 6 newly inst
Need to get 938 kB of ar
After this operation, 49
Get:1 http://us-east-1.e                                               64 pyth
Get:2 http://us-east-1.e                                               ython3-
Get:3 http://us-east-1.e                                               ython3-
```

Application Walkthrough

- Install `httpie` for testing the application flow via cli.

```
cd course
apt install httpie -y
```



```
root@ip-10-0-0-134:/home/ubuntu/ workspace/course# apt install httpie -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libintl-perl libintl-xs-perl libmodule-find-perl libmodule-scandeps-perl libproc-processtable-perl libsort-naturally-perl
  libterm-readkey-perl
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  python3-charset-normalizer python3-defusedxml python3-pygments python3-requests-toolbelt python3-socks
Suggested packages:
  python-pygments-doc ttf-bitstream-vera
The following NEW packages will be installed:
  httpie python3-charset-normalizer python3-defusedxml python3-pygments python3-requests-toolbelt python3-socks
0 upgraded, 6 newly installed, 0 to remove and 83 not upgraded.
Need to get 938 kB of archives.
After this operation, 4902 kB of additional disk space will be used.
Get:1 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/universe amd64 python3-charset-normalizer all 2.0.6-2 [32.2 kB]
Get:2 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/main amd64 python3-defusedxml all 0.7.1-1 [43.2 kB]
Get:3 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/main amd64 python3-pygments all 2.11.2+dfsg-2 [750 kB]
Get:4 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/main amd64 python3-requests-toolbelt all 0.9.1-1 [38.0 kB]
Get:5 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/universe amd64 python3-socks all 1.7.1+dfsg-1 [22.4 kB]
Get:6 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/universe amd64 httpie all 2.6.0-1 [52.6 kB]
Fetched 938 kB in 0s (5858 kB/s)
```

Open new file by clicking `+` icon & select `new file`.

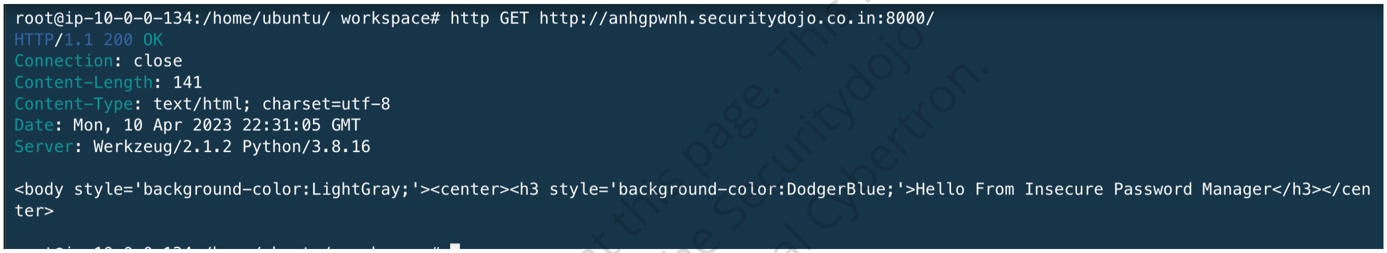
Refer: HTTPie – API testing client

Replace <subdomain> with your domain name

- Copy the http://<subdomain>.securitydojo.co.in:8000 URL from the browser and run the below command.

The response should be the homepage of the Insecure Password Manager application.

```
http GET http://<subdomain>.securitydojo.co.in:8000/
```

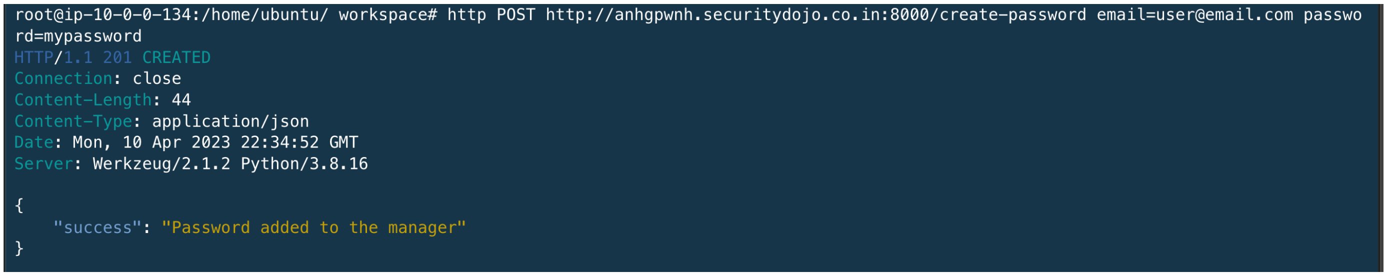


```
root@ip-10-0-0-134:/home/ubuntu/ workspace# http GET http://anhgpwnh.securitydojo.co.in:8000/
HTTP/1.1 200 OK
Connection: close
Content-Length: 141
Content-Type: text/html; charset=utf-8
Date: Mon, 10 Apr 2023 22:31:05 GMT
Server: Werkzeug/2.1.2 Python/3.8.16

<body style='background-color:LightGray;'><center><h3 style='background-color:DodgerBlue;'>Hello From Insecure Password Manager</h3></cen
ter>
```

- To save email and password in the password manager, make an HTTP POST request to the /create-password endpoint with email and password parameters.

```
http POST http://<subdomain>.securitydojo.co.in:8000/create-password
email=user@email.com password=mypassword
```

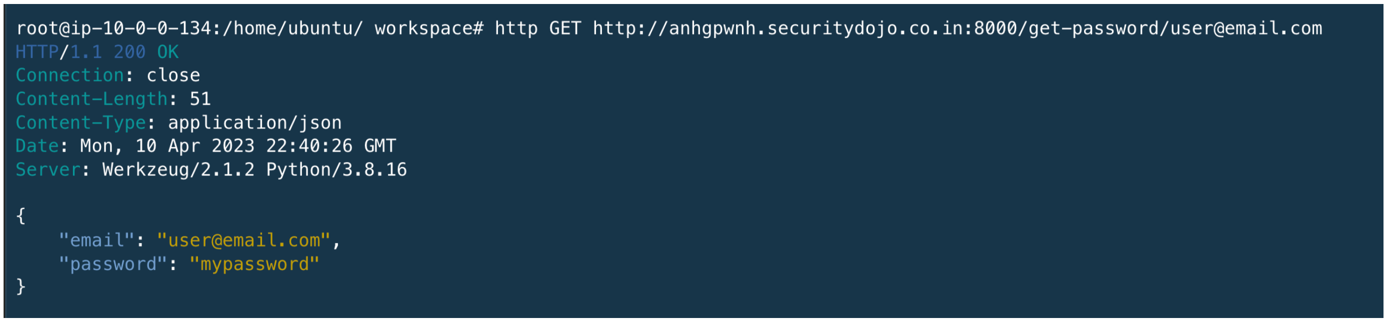


```
root@ip-10-0-0-134:/home/ubuntu/ workspace# http POST http://anhgpwnh.securitydojo.co.in:8000/create-password email=user@email.com passwo
rd=mypassword
HTTP/1.1 201 CREATED
Connection: close
Content-Length: 44
Content-Type: application/json
Date: Mon, 10 Apr 2023 22:34:52 GMT
Server: Werkzeug/2.1.2 Python/3.8.16

{
    "success": "Password added to the manager"
}
```

- To get the password and email via email address, make an HTTP GET request to the /get-password/ endpoint with email parameter.

```
http GET http://<subdomain>.securitydojo.co.in:8000/get-password/user@email.com
```



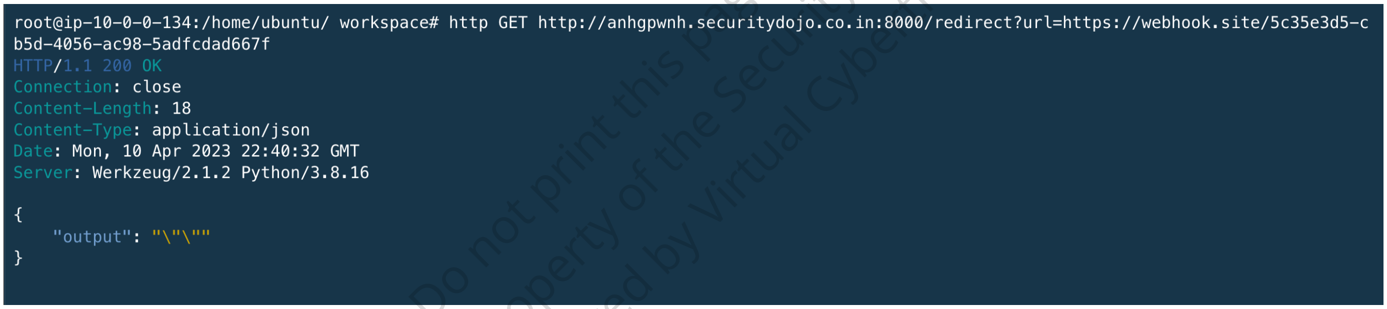
```
root@ip-10-0-0-134:/home/ubuntu/ workspace# http GET http://anhgpwnh.securitydojo.co.in:8000/get-password/user@email.com
HTTP/1.1 200 OK
Connection: close
Content-Length: 51
Content-Type: application/json
Date: Mon, 10 Apr 2023 22:40:26 GMT
Server: Werkzeug/2.1.2 Python/3.8.16

{
    "email": "user@email.com",
    "password": "mypassword"
}
```

- To test the SSRF vulnerability, make an HTTP GET request to the /redirect endpoint with a URL parameter.

> Using https://webhook.site, use any domain for testing, to get the URL visit the webhook.site and use the endpoint provided.

```
http GET http://<subdomain>.securitydojo.co.in:8000/redirect?url=https:
//webhook.site/5c35e3d5-cb5d-4056-ac98-5adfcdad667f
```



```
root@ip-10-0-0-134:/home/ubuntu/ workspace# http GET http://anhgpwnh.securitydojo.co.in:8000/redirect?url=https://webhook.site/5c35e3d5-c
b5d-4056-ac98-5adfcdad667f
HTTP/1.1 200 OK
Connection: close
Content-Length: 18
Content-Type: application/json
Date: Mon, 10 Apr 2023 22:40:32 GMT
Server: Werkzeug/2.1.2 Python/3.8.16

{
    "output": "\"\""
}
```

Conclusion

In this tutorial, we have covered the endpoints of the Insecure Password Manager application, which is a sample application created for educational purposes only. This tutorial has demonstrated how to interact with the application using HTTPie CLI, but other tools such as cURL can also be used.

Do not close the lab

> This lab will be used to learn attacks & enumeration in kubernetes cluster via external attack surface.