**Vulnerable Web Creator**

**14-08-2023**

**Version 0.0.1**

**1.  Overview**

**1.1    Purpose**

**2.  Requirements**

**2.1    Assets**

**2.1.2 Software**

**3.  Deployment Tutorial**

**3.1    Windows**

**4. Adding vulnerability Tutorial**

1. **Introduction**
   1. **Purpose**

The presented tool is a python-based interactive tool which helps in designing a web application which not only gives the ability to pick and choose various vulnerabilities with multiple severities but also gives the ability to modify how the application will look & feel. In an educational environment, an Admin or a host can create easy-to-deploy websites within couple of minutes by having these multiple variations to choose from.

1. **Requirements**

Basic minimum requirements for Windows can be found below.

**Note:** We **highly** recommend to use Windows.

* 1. **Assets**
     1. **Windows OS:**

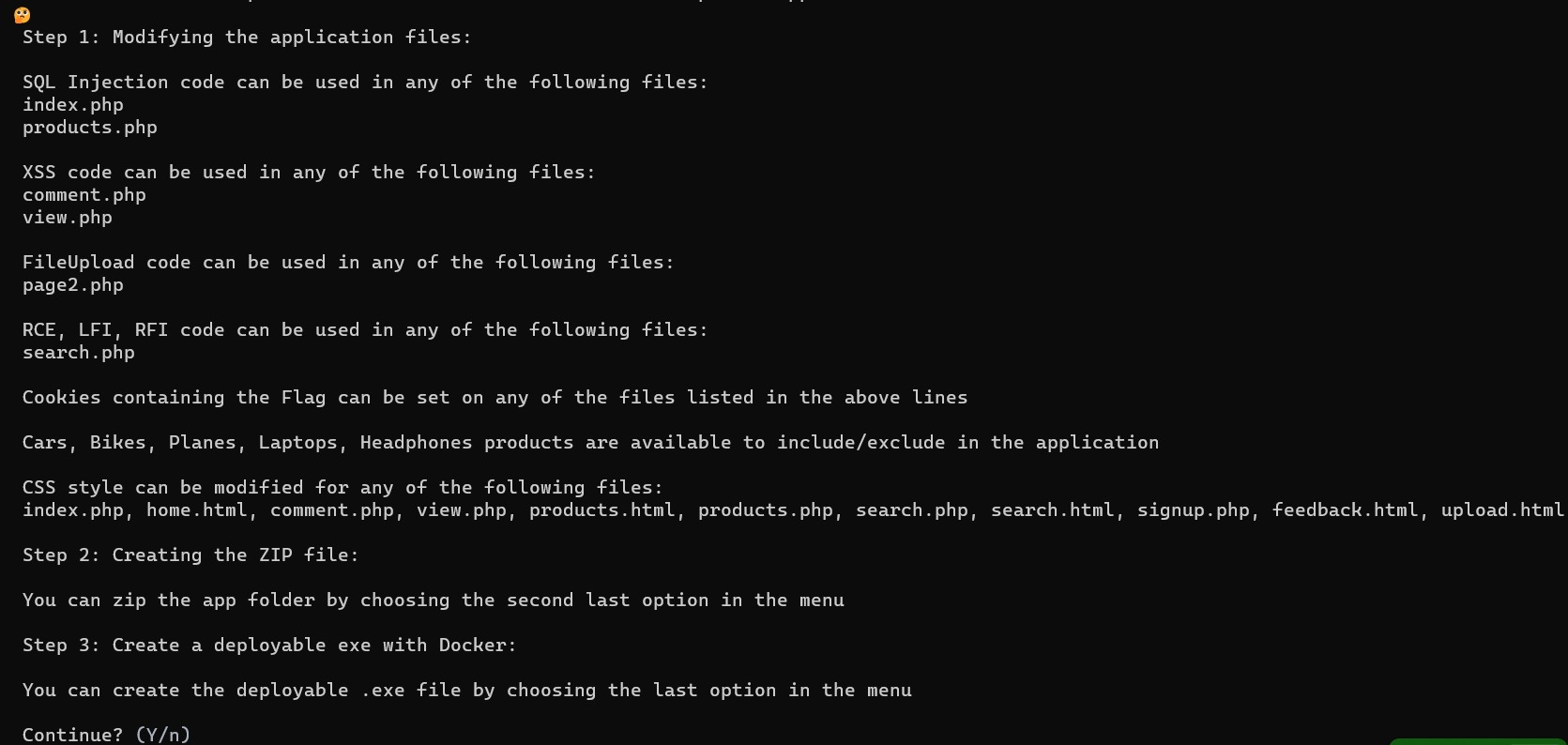
1. Software

* Python 3.9 or above (latest version installed)
* Requirements for the tool installed (provided in *requirements.txt)*

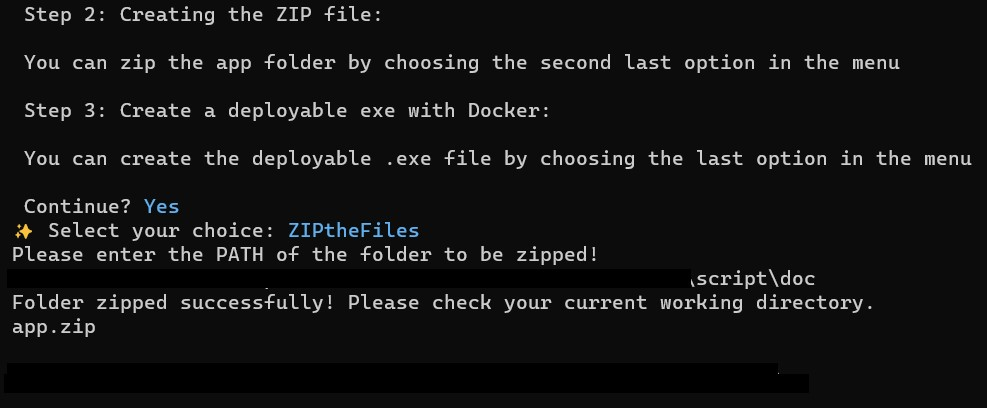
(Can be used via pip install -r requirements.txt)

1. **Deployment Tutorial**
   1. **Windows**

* Make sure that the requirements are installed successfully
* Read the user information carefully before proceeding ahead

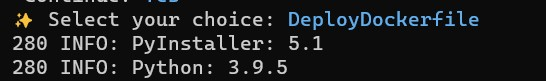


* If needed, to zip the app folder, please choose the appropriate option and proceed as shown below:

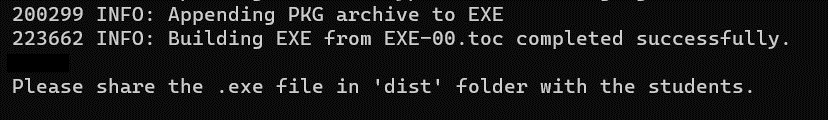


* Continue and choose the last option (**deploydockerfile**). This option will create an *.exe* file which can be shared with Students for their assignment.





* Please give it 3-5 minutes to create the exe file. Once the file is created, you will see the notification as shown below



1. **Adding vulnerability tutorial**

If needed, you can add your own vulnerable code into the application.

Once you have created a .py file containing the vulnerability in the default template. It is recommended to follow the next steps to ensure that the tool works properly (In the below example, we will add the phpinfo vulnerability:

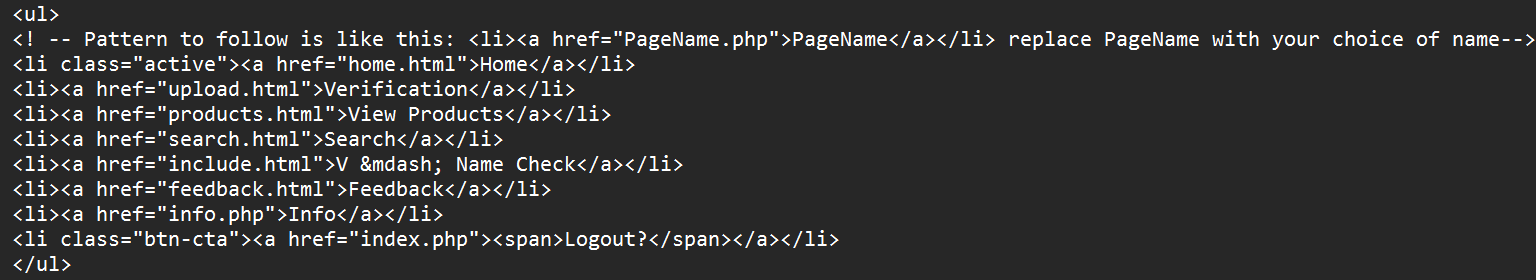
1. Import the module



1. Add the if-else loop as shown below



1. Now you can proceed with adding the vulnerability into the web application
2. Once done, we will need to edit the *headers.html* file in the web app:



**Note:** If the newly created vulnerability requires a new table within the existing database, then that table needs to manually created as per the vulnerability requirements.