Project Proposal of

"WebVuln Tool"

By

MOMIN NAOFIL AHMAD NEHAL AHMAD

(Elective-II PSCSP6 Cyber and Information Security)

SUBMITTED IN PARTIAL FULFILLMENT

OF THE REQUIREMENTS FOR THE M.SC. COMPUTER SCIENCE

IN

B.N.N. COLLEGE OF ARTS, SCIENCE AND COMMERCE, BHIWANDI

AND

MUMBAI UNIVERSITY

DECLARATION BY THE STUDENT

I, Momin **Naofil Ahmad Nehal Ahmad** student of M.Sc. Computer Science hereby declare that the project proposal work being presented in this report entitled "**WebVuln Tool**" submitted in the department of Master's in Computer Science by me, in B.N.N. College during the academic year 2020-21, is based on actual work carried out by me under the guidance and supervision of Prof. _____.

I further state that this work is original and not submitted anywhere else for any examination.

_____

MOMIN NAOFIL AHMAD

M.Sc. Computer Science III Semester

B.N.N. College Bhiwandi

EVALUATION CERTIFICATE

This is to certify that this report represent the original work done by **MOMIN NAOFIL AHMAD NEHAL AHMAD** during this project proposal submission as a partial fulfillment of the requirement for the Master's of Computer Science , Semester III of the B.N.N. College of Arts, Science and Commerce, Bhiwandi.

This Project proposal is original to the best of our knowledge and has accepted for Assessment.

Date: 13/12/2021 EXTERNAL EXAMINAR

SYNOPSIS OF PROJECT

TITLE OF THE PROJECT

“WebVuln Tool”

LANGUAGE AND SOFTWARE USED:

This project is build using Python language into the Linux Firmware because of its open source characteristic.
Software requirement for this software is Python, installed on Linux Server Machine or Virtual Machine. Although lots of Python module requires that are covered in Methodology.

INTRODUCTION:

WebVuln, as name indicates Websites Vulnerabilities. It is an open source intelligence gathering includes: Searching for information about a competitor's employees or services, Law enforcement agencies gathering intelligence using online public resources to prevent crimes, Identifying vulnerabilities to exploit at a later stage on a target system or network. This project contains different modules like searching information on social media about specific individual, checking URL redirection any many more. All modules are covered in methodology. After AT&T had dropped out of the Multics project, the Unix operating system was conceived and implemented by Ken Thompson and Dennis Ritchie (both of AT&T Bell Laboratories) in 1969 and first released in 1970. Later they rewrote it in a new programming language, C, to make it portable. The availability and portability of UNIX caused it to be widely adopted, copied and modified by academic institutions and businesses.

Before Google became synonymous with looking things up on the Internet, Yahoo, which first indexed the web, was the number two most popular site online. Today, it still (somehow) attracts a ton of traffic, coming in at the number one spot just a smidge above Google, according to Comscore numbers from this August. Back then, Yahoo was considered "good," to quote this 1998 article usability by Jakob Nielsen. After-all it had a page load time of three seconds. "This is one of the fastest download times among major websites," noted Jakob Nielsen. (Today, those three seconds would be a little slower than average.) He also praised Yahoo for its "minimalist" design, "links, links, and more links everywhere you turn," and the "structured navigation system."

And In 1991, Python first arrived in the world by Guido van Rossum; Python is a multi-paradigm programming language. Object-oriented programming and structured programming are fully supported, and many of its features support functional programming and aspect-oriented programming (including by met programming and

metaobjects (magic methods)).Many other paradigms are supported via extensions, including design by contract and logic programming.

With the Google Search Engine we all know that the Google is a Mountain, we can just climb on it, not move it, so thinking about the correlation between Google Searching using Python becomes more attractive as a tool. We are able to search what we want but somehow lots of people are not aware of deep learning in Google Search like Dorking in Google. Google dorking is a hacking technique that makes use of Google's advanced search services to locate valuable data or hard-to-find content. At the surface level, Google dorking involves using specific modifiers to search data. Although benign types of Google dorking simply use the resources that are available from Google, some forms of it are concerning to regulators and security specialists because they could indicate hacking or cyber attack reconnaissance. Hackers and other cyber-criminals can use these types of Google dorking to obtain unauthorized data or to exploit security vulnerabilities in websites, which is why this term is gaining a negative connotation from the security community. Any futurist attempting to create accurate and useful scenarios of the future would be much more successful serving a nonprofit who has clear numbers to indicate past performance. As in the private sector, these indications work better when more data points over a larger period of time are available. Any given nonprofit using social service software would likely be aware of which methods presently maximize efficiency. But would that same nonprofit be slowed by a sudden change in population within the area it serves? Such a change might require time to adjust, reassess, and test out newer strategies before returning to a satisfactory state of efficiency. These are the problems I believe futurists could help solve while working in tandem with preexisting data provided by new technology.

FIRST MODULE OF THE PROJECT

- Social media has a huge impact on individuals and their lives. While some impacts can be positive, social media has been shown to negatively affect things like our moods and stress levels. Addiction is caused by social media too. The negative impact of social media is seen by us on YouTube by getting scammed by another fraudster. More like Cyber Attacks, Hacker are using our social media information as their powerful tool to exploit our privacy.
- Almost everyone have their cell phone on their hand, there is an IP addresses assigned to you devices which are most needed thing to sending and receiving information from internet route. An internet protocol (IP) address allows computers to send and receive information. In IP spoofing, a hacker uses tools to modify the source address in the packet header to make the receiving computer system think the packet is from a trusted source, such as another computer on a legitimate network, and accept it. Because this occurs at the network level, there are no external signs of tampering.
- "A telephone number is not considered Personally Identifiable Information under the law, so technically there's not a legal obligation to protect that information." Companies use your cell phone to track your spending habits and also use it as your mobile identity. But your social media account, your e-mails are attached to your Phone Numbers.
- URL Redirection is a vulnerability which allows an attacker to force users of your application to an untrusted external site. The attack is most often performed by delivering a link to the victim, who then clicks the link and is unknowingly redirected to the malicious website. This vulnerability exploits the inherent trust that a user has in the legitimate domain. Since the victim is generally unaware of URL redirections; they are considerably more susceptible to phishing and social engineering attacks. For penetration testers, most instances of URL redirection will be fairly obvious. A smaller number, on the other hand, are a little more complex. Below are three common types of URL redirection pentesters should look out for.
- Students, Businessman, Organizations or any individual have their habit to read books; with the help of their cell it is possible because of Portable Document Format. PDF stands for "portable document format". Essentially, the format is used when you need to save files that cannot be modified but still need to be easily shared and printed. Today almost everyone has a version of Adobe Reader or other program on their computer that can read a PDF file. PDFs can have viruses that come embedded with a code that makes documents sign able and (somewhat) editable. The mechanics are very similar to virus-infected Microsoft

Word files. While their malware hides inside macros scripts, an infected PDF file will contain malicious JavaScript code. If I say that you can see the pdf metadata without opening pdf file so.

SECOND MODULE OF THE PROJECT

- ClickJacking attack is an attack that fools users into thinking they are clicking on one thing when they are actually clicking on another. Its other name, user interface (UI) redressing, better describes what is going on. Users think they are using a web page's normal UI, but in fact there is a hidden UI in control; in other words, the UI has been redressed. When users click something they think is safe, the hidden UI performs a different action.

  The attack is possible thanks to HTML frames (iframes), the ability to display web pages within other web pages through frames. If a web page allows itself to be displayed within a frame, an attacker can cover the original web page with a hidden, transparent layer with its own JavaScript and UI elements. The attacker then tricks users into visiting the malicious page, which looks just like a site users know and trust. There is no indication there is a hidden UI layered over the original site. Users click a link or a button, expecting a particular action from the original site, and the attacker's script runs instead. But the attacker's script can also execute the expected action to make it appear nothing has gone wrong.

  Clickjacking itself is not the end goal of the attack; it is simply a means of launching some other attack by making users think they are doing something safe. The actual attack can be virtually anything possible via web pages. This ranges from malicious actions, such as installing malware or stealing credentials, to more innocuous things, such as boosting click stats on unrelated sites, boosting ad revenues on sites, gaining likes on Facebook, or increasing views of YouTube videos.

- Host header injection attack, The purpose of the HTTP Host header is to help identify which back-end component the client wants to communicate with. If requests didn't contain Host headers, or if the Host header was malformed in some way, this could lead to issues when routing incoming requests to the intended application. Historically, this ambiguity didn't exist because each IP address would only host content for a single domain. Nowadays, largely due

to the ever-growing trend for cloud-based solutions and outsourcing much of the related architecture, it is common for multiple websites and applications to be accessible at the same IP address. This approach has also increased in popularity partly as a result of IPv4 address exhaustion.

The HTTP Host header is a mandatory request header as of HTTP/1.1. It specifies the domain name that the client wants to access. For example, when a user visits https://portswigger.net/web-security, their browser will compose a request containing a Host header as follows:

GET /web-security HTTP/1.1
Host: portswigger.net

In some cases, such as when the request has been forwarded by an intermediary system, the Host value may be altered before it reaches the intended back-end component.

- Subdomain Enumeration attack , is the process of finding valid (resolvable) sub domains for one or more domain(s). Unless the DNS server exposes a full DNS zone (via AFXR), it is really hard to obtain a list of existing sub domains. The common practice is to use a dictionary of common names, trying to resolve them. While this method is effective in some cases, it doesn't include sub domains that have strange names. Another approach is to crawl the second-level domain in order to find links to sub domains (faster approach is to use a search engine directly). After completing the sub domain enumeration process, the attacker finds blog.example.com as one of the sub domains in the target's DNS zone. The attacker is enriching this finding up to the web application layer and finds out that the blog is using Word press as a content management system. The attacker then runs wpscan in order to find Word press vulnerabilities. Fortunately, the target's Word press instance uses a vulnerable plug-in which an attacker is able to exploit, gain access to the environment and pivot further into the network. This example might seem a bit exaggerated, however, this is exactly what happened in the Panama Papers Case.

- Reverse IP attack

  The technique known as Reverse IP Lookup is a way to identify hostnames that have DNS (A) records associated with an IP address. A web server can be configured to serve multiple virtual hosts from a single IP address. This is a common technique in shared hosting environments. It is also common in many organizations and can be an excellent way to expand the attack surface during reconnaissance of a web server. If for example, your primary target

web site appears to be secure, you may be able to gain access to the underlying operating system by attacking a less secure site on the same server. Potentially bypassing the security controls of the target site. Reverse IP Lookup returns up to 1,000 domains hosted on a single IP, including all the common gTLD (generic Top Level Domain) and any ccTLD (Country Code Top Level Domain) domains. For more popular IPs with more than 1,000 domains, order a Reverse IP report and we'll deliver it to you in minutes. Reverse IP reports are a useful tool to sort, parse and review large lists of domains. Reverse IP Lookup is an incredibly powerful tool with many high-value business applications. Retrieve a list of all domains using the same IP address as you, and sharing the same resources Track down malicious behavior of phishing or scamming websites that reside on the same host. Perform research on hosting or parking companies before you decide to make a switch.

Here in our project titled WebVuln, introducing some relatable tools that can be used by a security consultant and a penetration tester to find and test the vulnerabilities of any website or can find the information about specific individuals. I am working on another module that could be integrate with this, that will for the Instagram reconnaissance which will be useful to searching the Instagram Account. Having these following options.

FILE=y/n Enable/disable output in a '<target username>_<command>.txt' file'

JSON=y/n Enable/disable export in a '<target username>_<command>.json' file'

addrs Get all registered addressed by target photos

cache Clear cache of the tool

captions Get target's photos captions

commentdata Get a list of all the comments on the target's posts

comments Get total comments of target's posts

followers Get target followers

followings Get users followed by target

fwersemail Get email of target followers

fwingsemail Get email of users followed by target

fwersnumber Get phone number of target followers

fwingsnumber Get phone number of users followed by target

hashtags Get hashtags used by target

info Get target info

likes Get total likes of target's posts

mediatype Get target's posts type (photo or video)

photodes Get description of target's photos

photos Download target's photos in output folder

propic Download target's profile picture

stories Download target's stories

tagged Get list of users tagged by target

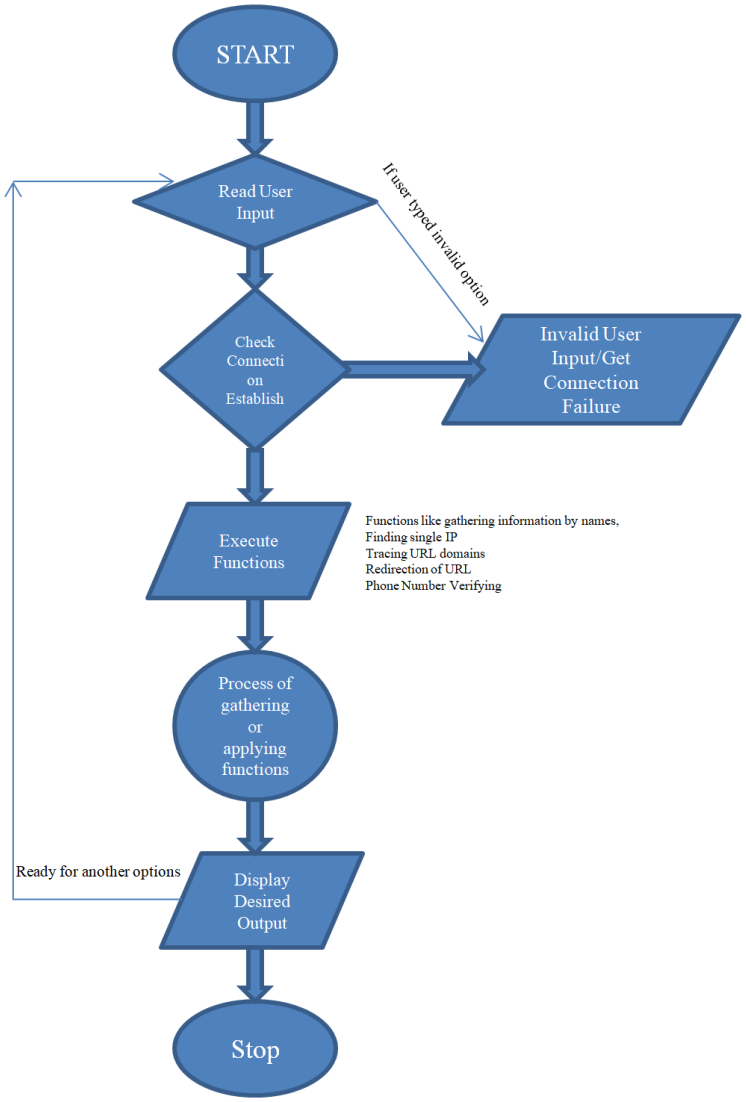
target Set new target

wcommented Get a list of user who commented target's photos

wtagged Get a list of user who tagged target

These script also be useful to trace somebody Instagram, download profile and photos and save whole information as TXT or JSON file.

Simple Flow Chart:



RELATED WORK:

1) Research Paper G.NIKHITA REDDY, G.J. UGANDER REDDY

A STUDY OF CYBER SECURITY CHALLENGES AND ITS EMERGNING TRENDS ON LATEST TECHNOLOGIES

Cyber Security plays an important role in the field of information technology .Securing the information have become one of the biggest challenges in the present day. Whenever we think about the cyber security the first thing that comes to our mind is cyber crimes which are increasing immensely day by day. Various Governments and companies are taking many measures in order to prevent these cyber crimes. Besides various measures cyber security is still a very big concern to many. This paper mainly focuses on challenges faced by cyber security on the latest technologies .It also focuses on latest about the cyber security techniques, ethics and the trends changing the face of cyber security.

Keywords: cyber security, cyber crime, cyber ethics, social media

Today we are able to connect to anyone in any part of the world. But for these mobile networks security is a very big concern. These days firewalls and other security measures are becoming porous as people are using devices such as tablets, phones, PC's etc all of which again require extra securities apart from those present in the applications used. We must always think about the security issues of these mobile networks. Further mobile networks are highly prone to these cyber crimes a lot of care must be taken in case of their security issues. As we become more social in an increasingly connected world, companies must find new ways to protect personal information. Social media plays a huge role in cyber security and will contribute a lot to personal cyber threats. Social media adoption among personnel is skyrocketing and so is the threat of attack. Since social media or social networking sites are almost used by most of them every day it has become a huge platform for the cyber criminals for hacking private information and stealing valuable data.

2) Research paper by Azeez Nureni Ayofe, Berry Irwin

CYBER SECURITY: CHALLENGES AND THE WAY FORWARD

The high level of insecurity on the internet is becoming worrisome so much so that transaction on the web has become a thing of doubt. Cybercrime is becoming ever more serious and prevalent. Findings from 2002 Computer Crime and Security Survey show an upward trend that demonstrates a need for a timely review of existing approaches to fighting this new phenomenon in the information age. In this paper, we provide an overview of Cybercrime and present an international perspective on fighting Cybercrime. This work seeks to define the concept of cyber-crime, explain tools being used by the criminals to perpetrate their evil handiworks, identify reasons for cyber-crime, how it can be eradicated, look at those involved and the reasons for their involvement, we would look at how best to detect a criminal mail and in conclusion, proffer recommendations that would help in checking the increasing rate of cyber-crimes and criminals.

Cybercrimes committed against persons include various crimes like transmission of child-pornography, harassment of any one with the use of a computer such as e-mail. The trafficking, distribution, posting, and dissemination of obscene material including pornography and indecent exposure, constitutes one of the most important Cybercrimes known today. The potential harm of such a crime to humanity can hardly be amplified . This is one Cybercrime which threatens to undermine the growth of the younger generation as also leave irreparable scars and injury on the younger generation, if not controlled. The third category of Cyber-crimes relate to Cybercrimes against Government. Cyber terrorism is one distinct kind of crime in this category. The growth of internet has shown that the medium of Cyberspace is being used by individuals and groups to threaten the international governments as also to terrorize the citizens of a country. This crime manifests itself into terrorism when an individual "cracks" into a government or military maintained website.

CAUSES OF CYBER – CRIME

There are many reasons why cyber-criminals commit cyber-crime, chief among them are these three listed below: ⌵ Cyber crimes can be committed for the sake of recognition. This is basically committed by youngsters who want to be noticed and feel among the group of the big and tough guys in the society. They do not mean to hurt anyone in particular; they fall into the category of the Idealists; who just want to be in spotlight. ⌵ Another cause of cyber-crime is to make quick money. This group is greed motivated and is career criminals, who tamper with data on the net or system especially,

e-commerce, e-banking data information with the sole aim of committing fraud and swindling money off unsuspecting customers. ⌵ Thirdly, cyber-crime can be committed to fight a cause one thinks he believes in; to cause threat and most often damages that affect the recipients adversely. This is the most dangerous of all the causes of cyber-crime. Those involve believe that they are fighting a just cause and so do not mind who or what they destroy in their quest to get their goals achieved. These are the cyber-terrorists.

Some of Powerful Open Source Project based on this Domain

1) **Metasploit** was created by H. D. Moore in 2003 as a portable network tool using Perl. By 2007, the Metasploit Framework had been completely rewritten in Ruby. It consists of an excellent collection containing different tools for carrying out penetration testing exercises. IT experts and cyber security professionals use Metasploit to accomplish varying security objectives. These include identifying vulnerabilities in network or system, formulating strategies for strengthening cyber security defense and managing the completed security evaluations. Metasploit can test the security of different systems, including online-based or web-based applications, networks, servers, among others. Metasploit identifies all new security vulnerabilities as they emerge, thus ensuring round-the-clock security. Also, security professionals often use the tool to evaluate IT infrastructure security against vulnerabilities reported earlier.
2) **Aircrack-ng** was developed by Thomas d'Otreppe de Bouvette. It contains a comprehensive set of utilities used to analyze the weaknesses of Wi-Fi network security. Cyber security professionals use it to capture data packets communicated through a network for continuous monitoring. Also, Aircrack-ng provides functionalities for exporting captured data packets to text files to be subjected to more security assessments. Besides, it permits capture and injection, which is essential in assessing the performance of network cards. These instructions illustrate all major features of Beautiful Soup 4, with examples. I show you what the library is good for, how it works, how to use it, how to make it do what you want, and what to do when it violates your expectations.
3) **Reconnaissance**

   The adversary is trying to gather information they can use to plan future operations. Reconnaissance consists of techniques that involve adversaries actively or passively gathering information that can be used to support targeting. Such information may include details of the victim organization, infrastructure, or staff/personnel. This information can be leveraged by the adversary to aid in other phases of the adversary lifecycle, such as using gathered information to plan and execute Initial Access, to

scope and prioritize post-compromise objectives, or to drive and lead further Reconnaissance efforts. Reconnaissance generally follows seven steps:

Collect initial information
Determine the network range
Identify active machines
Find access points and open ports
Fingerprint the operating system
Discover services on ports
Map the network
Using these steps, an attacker will aim to gain the following information about a network:

File permissions
Running network services
OS platform
Trust relationships
User account information
One of the most common techniques involved with reconnaissance is port scanning, which sends data to various TCP and UDP (user datagram protocol) ports on a device and evaluates the response.

OBJECTIVES OF THE PROJECT

This main objective of the project to create a open source tool in python for the searching, testing the websites and gathering the information of specific individual and understating how cyber securities work against crime and law enforcements.

We are living in a modern era that every person needs their privacy on the internet but somehow Social Engineering attacks are becoming more common. Hackers are stealing our privacy and attacking our device remotely and play scamming cards emotionally with us. Social recognition can be defined as an employee reward and recognition methodology. Specific tools are used to provide a "communal forum" where workers of every level can come together, share their experiences, and assign rewards to or recognize their peers for their accomplishments. Every one using device having their IP attached with it, IP geolocation is the mapping of an IP address to the geographic location of the internet from the connected device. By geographically mapping the IP address, it provides you with location information such as the country, state, city, zip code, latitude/longitude, ISP, area code, and other information. More often those people are creating their blogs or a websites for their goal or a startups they are also aware about phishing attacks on their own devices, their website are vulnerable to exploits.

A Penetration testers, or pen testers for short, perform simulated cyber attacks on a company's computer systems and networks. These authorized tests help identify security vulnerabilities and weaknesses before malicious hackers have the chance to exploit them. We use penetration testing to determine what their network would reveal in the event of a reconnaissance attack. During testing, organizations can deploy port scanning tools (which scan large networks and determine which hosts are up) and vulnerability scanners (which find known vulnerabilities in the network).

SIEM solutions can also detect source IPs that are running a port scanning tool in your network.

Other reconnaissance prevention techniques are highlighted in the MITRE ATT&CK Framework.

In this project Processes of given input are efficiently handled by python interpreter by create class files every time when execution. This project build in CLI form that is not more attractive when opens in editor and console but System that automate decision such as its algorithm gather report on inputs. This project based on social activity scanning that can be useful to understand how attackers gain and gather the user's information and attack them next to it. Checking the exploitation on websites by using modules of Clickjacking and Host header injection. These tools are specially used by penetration tester or cyber crime investigator to find out weakness in a system or a websites.

METHODOLOGY:

Credential Access consists of techniques for stealing credentials like account names and passwords. Techniques used to get credentials include keylogging or credential dumping. Using legitimate credentials can give adversaries access to systems, make them harder to detect, and provide the opportunity to create more accounts to help achieve their goals. Learners will acquire the technical skills needs to develop custom Python scripts to automate cyber security tasks. The challenges in this project involve developing or modifying Python code to address cyber security use cases drawn from MITRE ATT&CK and Shield. Python is an interpreted, high-level, general-purpose programming language. The Python standard library contains well over 200 modules, although the exact number varies between distributions. High-level because of the amount of abstraction, it is very abstract and uses natural language elements, which are easier to use and understand. It makes the whole process simpler and more automated than lower-level languages.

A general-purpose programming language is designed to be used for writing software in the widest variety of application domains. A general-purpose programming language has this status because it does not include language constructs designed to be used within a specific application domain. Highly Efficient (Python's clean object-oriented design provides enhanced process control, and the language is equipped with excellent text processing and integration capabilities, as well as its own unit testing framework

Linux makes it easier to use python because you don't go through many installation steps unlike in Windows. And it's easy to switch between versions of python when you work in Linux. Learning python wouldn't depend upon the OS. On Linux. Python comes preinstalled on most Linux distributions, and is available as a package on all others. However there are certain features you might want to use that are not available on your distro's package. You can easily compile the latest version of Python from source.

Another element of Python’s excellence comes not from the language itself, but from the community. In the Python community, there is much consensus about the way to accomplish certain tasks and the idioms that you should (and should not) use. While the language itself may support certain phrasings for accomplishing something, the consensus of the community may steer you away from that phrasing. For example, from module import * at the top of a module is valid Python. However, the community frowns upon this and recommends that you use either: import module or: from module import resource. Importing all the contents of a module into another module’s namespace can cause serious annoyance when you try to figure out how a module works, what functions it is calling, and where those functions come from. This particular

convention will help you write code that is clearer and will allow people who work on your code after you to have a more pleasant maintenance experience. Following common conventions for writing your code will put you on the path of best practices. We consider this a good thing.

The Python Standard Library is another excellent attribute of Python. If you ever hear the phrase “batteries included” in reference to Python, it simply means that the standard library allows you to perform all sorts of tasks without having to go elsewhere for modules to help you get it done. For example, though it isn’t built-in to the language directly, Python includes regular expression functionality; sockets; threads; date/time functionality; XML parsers; config file parser; file and directory functionality; data persistence; unit test capabilities; and http, ftp, imap, smpt, and nntp client libraries; and much more. So once Python is installed, modules to support all of these functions will be imported by your scripts as they are needed. You have all the functionality we just listed here. It is impressive that all of this comes with Python without requiring anything else. All of this functionality will help you out immensely as you write Python programs to do work for you.

Easy access to numerous third-party packages is another real advantage of Python. In addition to the many libraries in the Python Standard Library, there are a number of libraries and utilities that are easily accessible on the internet that you can install with a single shell command. The Python Package Index, PyPI (http://pypi.python.org), is a place where anyone who has written a Python package can upload it for others to use.Python is a valuable programming language since it can be used in detecting malware, penetration testing, scanning, and analyzing cyber threats.

Below the Python Modules presented, those are used in this project.

- Python requests module has several built-in methods to make Http requests to specified URI using GET, POST, PUT, PATCH or HEAD requests. A Http request is meant to either retrieve data from a specified URI or to push data to a server. It works as a request-response protocol between a client and a server.
- The webbrowser module provides a high-level interface to allow displaying web-based documents to users. Under most circumstances, simply calling the open() function from this module will do the right thing. Under Unix, graphical browsers are preferred under X11, but text-mode browsers will be used if graphical browsers are not available or an X11 display isn’t available. If text-mode browsers are used, the calling process will block until the user exits the browser.
- gTTS (Google Text-to-Speech)is a Python library and CLI tool to interface with Google Translate text-to-speech API. We will import the gTTS library from the gtts

module which can be used for speech translation. The text variable is a string used to store the user's input.

- urllib.request is a Python module for fetching URLs (Uniform Resource Locators). It offers a very simple interface, in the form of the urlopen function. This is capable of fetching URLs using a variety of different protocols. It also offers a slightly more complex interface for handling common situations - like basic authentication, cookies, proxies and so on. These are provided by objects called handlers and openers.
- Beautiful Soup is a Python library for pulling data out of HTML and XML files. It works with your favorite parser to provide idiomatic ways of navigating, searching, and modifying the parse tree. It commonly saves programmers hours or days of work.
- Python is used for a wide variety of purposes & is adorned with libraries & classes for all kinds of activities. Out of these purposes, one is to read text from PDF in Python. PdfFileReader in Python offers functions that help in reading & viewing the pdf file. It offers various functions using which you can filter the pdf on the basis of the page number, content, page mode, etc
- gmplot is a matplotlib-like interface to generate the HTML and JavaScript to render all the data user would like on top of Google Maps.
- Reverse IP/DNS API client library in Python language. Reverse IP API allows users to get a list of all domains using the same IP address with a single API.
- Using these all module different python files are create and emerged in a single file and all are build in Linux Environment so maybe it is not work perfectly in Windows Environment especially with their ASCII and Coloring format of Linux Environment.
- JSON Module, It’s pretty easy to load a JSON object in Python. Python has a built-in package called json, which can be used to work with JSON data. It’s done by using the JSON module, which provides us with a lot of methods which among loads() and load() methods are gonna help us to read the JSON file.
- With the Instagram API, you can get a list of recent comments on a media object, get information about a user, get media published by a user, get information about a location, get information about a tag object, and more. Price: The API is offered for free
- VMware Workstation is a line of Desktop Hypervisor products which lets users run virtual machines, containers and Kubernetes clusters. This project created in Kali Linux(a Linux Distro) Environment on virtual machine (VMware 16 version)

Screenshot of WebVuln in Linux Terminal

1)Information gathering

2) Module: Web Vulnerability scanning.

3) Module: grabinsta