

AUTOMATION TOOL FOR BUG BOUNTY

A PROJECT REPORT

Submitted by

Himanshu Singh (20BCS2142)

Himanshu Rajput (20BCS2123)

Kunal Mehra (20BCS2153)

in partial fulfillment for the award of the degree of

BACHELOR OF ENGINEERING

IN

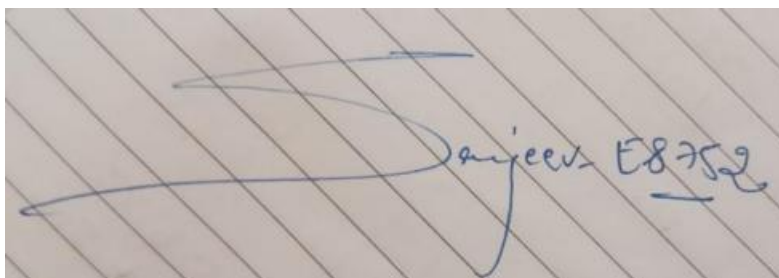
**COMPUTER SCIENCE &
ENGINEERING**



Chandigarh University
MAY 2022

BONAFIDE CERTIFICATE

Certified that this project report “**AUTOMATION TOOL FOR BUG BOUNTY**” is the bonafide work of “ Himanshu Singh, Himanshu Rajput, Kunal Mehra ” who carried out the project work under supervision.

A photograph of a handwritten signature in blue ink on lined paper. The signature is stylized and appears to read 'Sanjeev'. To the right of the signature, the alphanumeric code 'E8752' is written.

Dr. Puneet Sir
(Head of the Department)

Er. Sanjeev kumar
(Co-Supervisor)

Submitted for the project viva-voce examination held on_____

INTERNAL EXAMINER

EXTERNAL EXAMINER

ACKNOWLEDGEMENT

We especially to acknowledge incredible assistance and guidance of qualified and distinguished teachers and preachers of Chandigarh University, Kharar who always extended their helping hand to sail us smoothly through the project.

I thank the almighty for giving us the courage and perseverance in completing the project phaseII. This project itself is acknowledgements for all those people who have give us their heartfelt cooperation in making this project phase-II a grand success. I extend our sincere thanks to Supervisor- Chet Ram Sir , Co-Supervisor- Sanjeev Sir Sir, for providing sufficient infrastructure and good environment in the College to complete our Discussions. I am thankful to our secretary for providing the necessary Infrastructure, labs and also permitting to carry out this project.

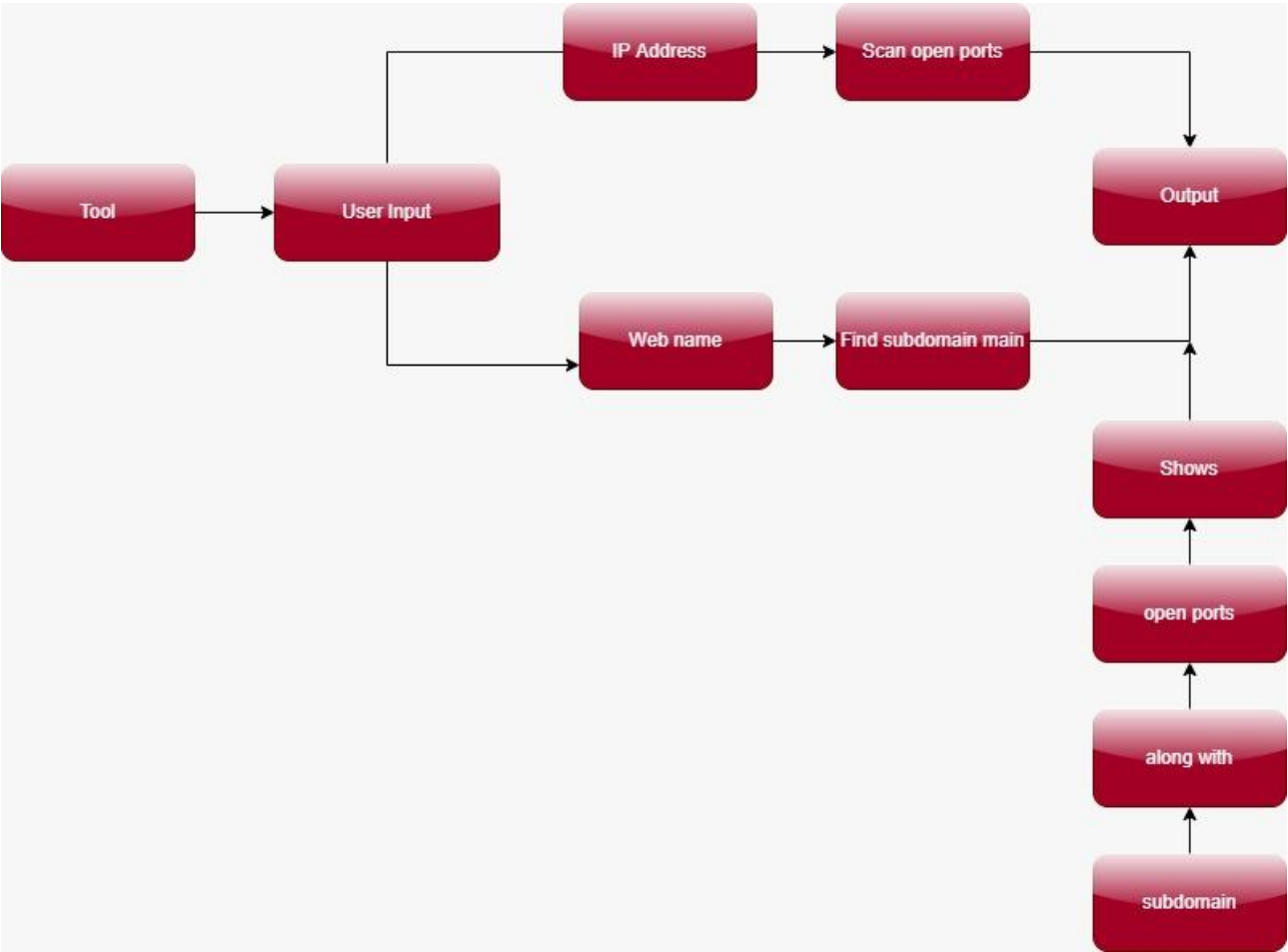
TABLE OF CONTENTS

Heading	Page No.
1. Acknowledgement	2
2. Abstract	5
3. Graphical Abstract	6
4. Abbreviations	7
5. Chapter 1: Introduction	20
6. Chapter 2: Literature Survey	23&24
7. Chapter 3: Design/Flow Process	25-27
8. Chapter 4: Result Analysis	28
9. Chapter 5: Conclusion & Future Work	32-35
10. References	36

ABSTRACT

This thesis introduces the reasoning behind the increasing popularity of the bug bounty programs and analyses, the most common, impact full bugs whose discovery can be automated at scale. As there was no suitable existing solution for similar automation identified, the thesis introduces anew framework, specifically designed for the bug bounty automation use case. We are making a bug bounty tool for finding web vulnerabilities or bug (security flaw) in any website. Bug bounty is the process of discovering vulnerabilities. Due to the advancement in technology, the Internet is gaining billions of new users every year. The Internet is accessed via Browser to browse Web applications, which mainly serve static or dynamic web pages, whose main aim is to provide the information or services to the user. The Internet consists of billions of websites that are available with minimal security features or lack secure codes which invites hackers to exploit vulnerabilities present in websites and as result data breaches occur at the organizational level which in turn harms the organization's reputation and loses its trust with users. To prevent such attacks, Cyber security Researchers and developers spend a lot of time testing their web applications before deploying in the real world or on the Internet. Automating and developing such tools which are capable of detecting the vulnerabilities would be a great contribution to Cyber security and as result, this would secure the organization from the Attackers and save ample amounts of time in the Testing phase. So, in this review paper, 5suchbrief examples are presented, wherein the researchers have performed vulnerability assessment, penetration testing and along with this the researchers have proposed a method to automate the process of finding vulnerabilities.

GRAPHICAL ABSTRACT:



ABBREVIATION:

PY- Python
Vs Code-Visual Code

PROBLEM DISCUSSION:

Bug bounty hunters have to use different tools for different attack or for finding different information related to target due to which the time increase and it is a time taken process.

So , here we come with an solution which is that we combine 2 recon tool in one which is port scanner and 2 is subdomain finder by using this tool we can find open ports and we can find subdomain of a given website so we can also save the time by using this tool.

Attainment of stated outcomes:

Attainment of stated outcomes: By using this tool we get output in which output will give you all the subdomains related to the main domains and also help in find ingo pen ports of a given target this tool is completely based on python.

Use of Modern tools in design and analysis:

Obviously, Python is a popular and necessary skill to learn. But what is the python system used for? We have already briefly touched on some of the areas where I can be used, and expand on these Python examples and others below. Python can be used:

1. AI and machine learning

Because Python is a stable, flexible, and easy-to-use programming language, it is ideal for machine learning (ML) and artificial intelligence (AI) projects. In fact, Python is one of the most popular languages among data scientists, and there are plenty of Python machine learning and AI libraries and

packages available.

If you are interested in this Python application, our Deep Learning and Python Programming AI with Microsoft Azure Expert Track can help you improve your skills in these areas. You can get Python usage and in-depth learning while improving your work on AI.

2. Data analysis

Similar to AI and machine learning, data analysis is another rapidly evolving field using the Python system. At a time when we are creating more data than ever before, there is a need for those who can collect, manage and organize information.

Python data science and analysis makes sense. Language is easy to learn, flexible, and well-supported, which means it is fast and easy to use for data analysis. When working with large amounts of information, it is useful for converting data and performing repetitive tasks.

You can learn about data analysis using Python with our Expert Track, which will help you develop effective data analysis skills.

3. Data view

Data viewing is another popular and evolving field of interest. Also, it plays on a lot of Python power. Along with its flexibility and the fact that it is open source, Python offers a variety of libraries with all sorts of features.

Whether you are looking to create a simple image representation or a collaborative layout, you can find a library that fits your needs. Examples include Pandas Visualization and Ploly . There are many possibilities, which allow you to convert data into logical data.

If Python data viewing sounds appealing, check out our 12-week Expert Track for this topic. You will learn how to use Python libraries to interpret and analyze data sets.

4. Apps

You can edit all kinds of applications using Python. Normal target language can be used to read and create file indexes, create GUI's and API's , and more. Whether you block chain apps, audio and video apps, or machine learning apps, you can build them all with Python.

Project management and Professional communication (Presentation):



Final project

Automation Tool For Bug Bounty

- ▶ Submitted by:
- ▶ Himanshu Singh(20BCS2142)
- ▶ Himanshu Rajput(20BCS2123)
- ▶ Kunar Mehra(20BCS2153)



AUTOMATION TOOL FOR BUG BOUNTY:

- Our subdomain finder tools allow you to discover the subdomains of any target domain to uncover potential attack entry points.
- Find systems that are less protected and thus more vulnerable to attacks.



INTRODUCTION:

- Automation is the latest trend in bug bounty hunting, with new frameworks being released every day. This ranges from full-fledged solutions with user interfaces and back-end databases to collections of custom-built Bash scripts. All of which have their uses depending on the level of control and depth of testing preferred by the user.

OBJECTIVES:

- Bug bounty is the process of discovering vulnerabilities. Due to the advancement in technology, the Internet is gaining billions of new users every year. The Internet is accessed via Browser to browse Web applications, which mainly serve static or dynamic web pages, whose main aim is to provide the information or services to the user.

TECHNOLOGY USED:

.Python and some libraries

.import pyfiglet

.import sys

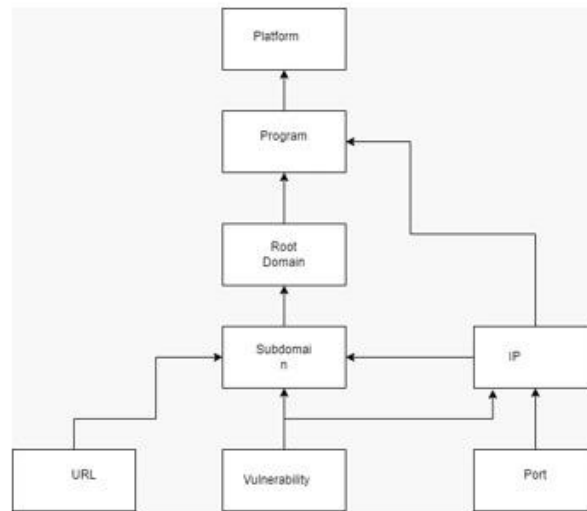
.Import socket

.from datetime import datetime

.import requests

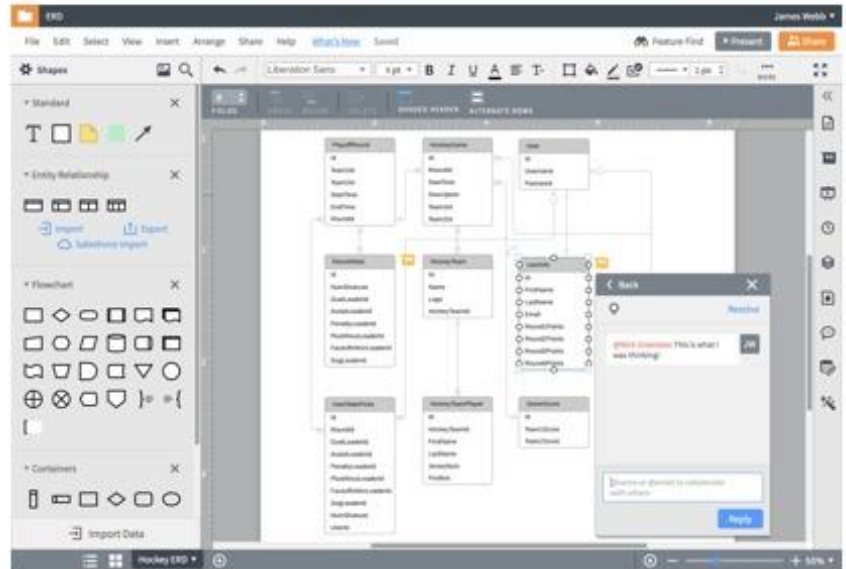
.

DFD DIAGRAM:



[illegible]

ERD DIAGRAM:



```

# Run the Scan Option Only
subprocess.run(["python3", "scan.py"], stdout=subprocess.PIPE)

for subdomain in subdomains:
    url1 = f"http://{subdomain}.example.com"
    url2 = f"https://{subdomain}.example.com"
    try:
        requests.get(url1)
        print(f"Discovered URL: {url1}")
        requests.get(url2)
        print(f"Discovered URL: {url2}")
    except requests.ConnectionError:
        pass

# Add Banner
print("\n" * 5)
print(f"Banner: {banner}")
print(f"Banner: {banner}")
print(f"Banner: {banner}")
print(f"Banner: {banner}")
print(f"Banner: {banner}")

# Scan
# Will scan ports between 1 to 65,535
for port in range(1, 65536):
    s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    socket.setdefaulttimeout(1)

    # Returns an error indicator
    result = s.connect_ex((target, port))
    if result == 0:
        print(f"Port {port} is open")
    s.close()

except KeyboardInterrupt:
    print("\nExiting Program !!!")
    sys.exit()

except socket.error:
    print("No hostname could be resolved !!!")
    sys.exit()

except socket.error:
    print("Server not responding !!!")
    sys.exit()

```



Chapter 1: Introduction

1.1) Purpose -

This tool application provides the facility to find the bugs in websites and practice, on a subject of your choice. It provides a good platform, where a person irrespective of his age not only judges their knowledge/skill but also, they can improve knowledge/skill at the same time with a small information provided to you regarding of the question.

1.2) Scope -

The Scope of this project is extremely broad in terms of gaining knowledge and sharing knowledge among world.

A few points are:

- . Automation is the latest trend in bug bounty hunting, with new frameworks being released every day.

Some obvious benefits to bug bounty automation include:

- Easily identify low-hanging vulnerabilities.
- Continuous recon to capture changing environments.
- Maximize time and profit by automating repetitive tasks.

OBJECTIVE:

The advantage of a distraction is the risk detection process. Thanks to technological advances, the Internet is gaining billions of new users every year. The Internet is accessed through a Browser to browse Web applications, which mainly provide static or dynamic web pages, the main purpose of which is to provide information or services to the user. The Internet contains billions of websites accessed with little or no security features that invite cyber criminals to take advantage of online threats and as a result data breaches occur at the organizational level which damages the organization's reputation and loses its trust with users. . To prevent such attacks, Cyber security Researchers and developers spend a lot of time testing their web applications before using them in the real world or online. Automated and developing such risk detection tools can be a major contribution to online security and as a result, this will protect the organization from attackers and save a lot of time in the Testing phase. Therefore, in this review paper, 5 such brief examples are presented, in which the researchers conducted a risk assessment, an entry test and in this case the researchers proposed an automated risk assessment process.

Single entity:

In our team, we are three members. Each member has expertise in different fields of automation tool for bug bounty like of us in python. so, we efficiently divided the work among our team members accordingly.

Life Span –

We have estimated our project's Life span to be around 3 to 4 months as per our current semester. Although the python can be further used after this time period in the upcoming future. But as our semester will end in mid of may so we have planned to make our vulnerability.

Require funds –

As this project of ours is basic and small scale project and the resources which we are using are mostly Open sourced and free of cost so, the funds required for the completion is basically zero. But in future, if we decide to add more functionality to our report handling system and host it publicly we will require around 200-300\$ excluding the cost of managing it afterward.

Life Cycle –

For our project our team has decided to go with the Waterfall Model of SDLC(Software Development Life Cycle) as it is a small-scale project and I, and my

team are examining each step of Software Development Life Cycle (SDLC) very closely.

Team Spirit –

We are three members in our team and every member is goal driven and hard-working. All of us are determined to complete our assigned work on time and each and every member of a team reviews each other work to check whether everything is up to mark or not and give the required feedback.

Directions –

We are performing this project under the guidance of our supervisor and co-supervisor. We arrange meeting with the Supervisor and Co-Supervisor of our project in certain intervals of time to show the program that we have made and take feedbacks from them and implement them accordingly.

Uniqueness –

We are planning to make a bug bounty tool using Python and some of its libraries according to the need. We are making this to help the bug bounty hunter for finding bugs /security flaw in any website so that they will earn some amount of money and can also help in improving the security of the websites. Basically, this tool is going to help you find some basic bugs in the website and improve the security of it.

Flexibility –

Throughout this project, we have aimed at making your Report Handling system as dynamic and flexible as possible, so in the further future if we decide to take our project to a high level by adding more features and hosting it publicly, we could easily do that without any fuss.

Constraints Identification

Time – Project completion or final due dates are dependent on the submission of the project's different phases. Phase I completed on 14-march-2022, phase II on 31-march-2022, and phase III will be completed on 28-April-2022. The final full-fledged project will be completed on 15-May-2022 as the tentative due dates are there.

Scope- Before carrying out the testing process, one must check for the feasibility of automation. Here are the things to consider while identifying the scope of Testing Automation: As the name suggests, in this phase, you make a plan, design the architecture, and create a strategy to achieve the goal of test automation.

Test plan: Creation of test standards and procedures, hardware, software, and test data requirements

Test design:

Design the test architecture to determine the flow of the test procedures that follow
Test strategy: Select a suitable test automation framework .

Benefits –

Advantages commonly attributed to automation include higher production rates and increased productivity, more efficient use of materials, better product quality, improved safety, shorter workweeks for labour and reduced factory lead times. Higher output and increased productivity have been two of the biggest reasons in justifying the use of automation.

Analysis of features and finalization subject to constraints: The analysis of features is done with following points in mind: Ease of access. Simple design. Convenience for the user.

Ease to use interface: The user interface integrated in the tools is made to be really easy to use for the user. The interface is really simple with almost single-click response to every feature. Open source tool for automating browser based application which is easy to get started with for simple functional testing of a web application and many companies are opting for this tool to do automated using.

Simple Design: The design of tool is made to be really simple to find vulnerability in the websites.

Convenience for the user:

Team saves time.

Higher Test coverage.

Faster time to market.

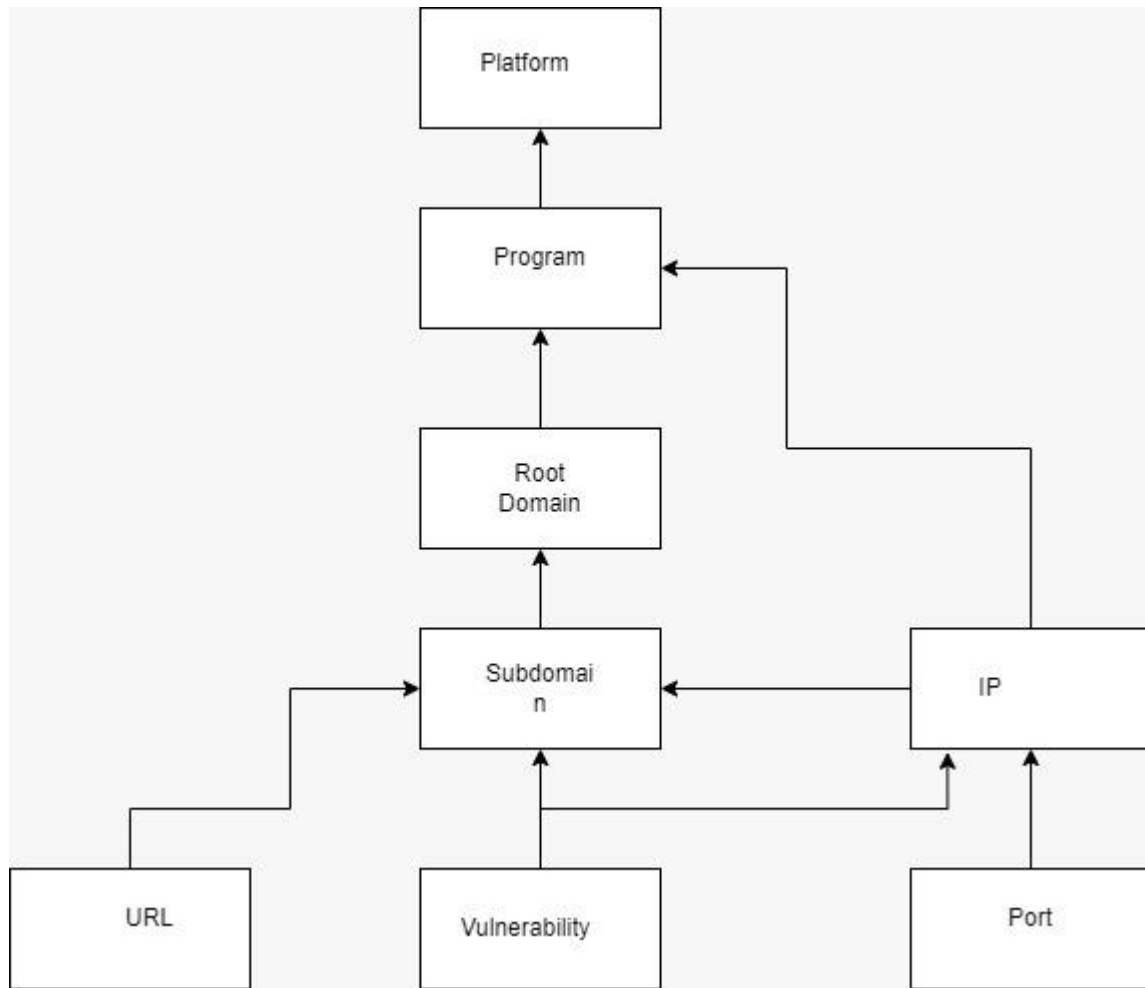
Improved accuracy

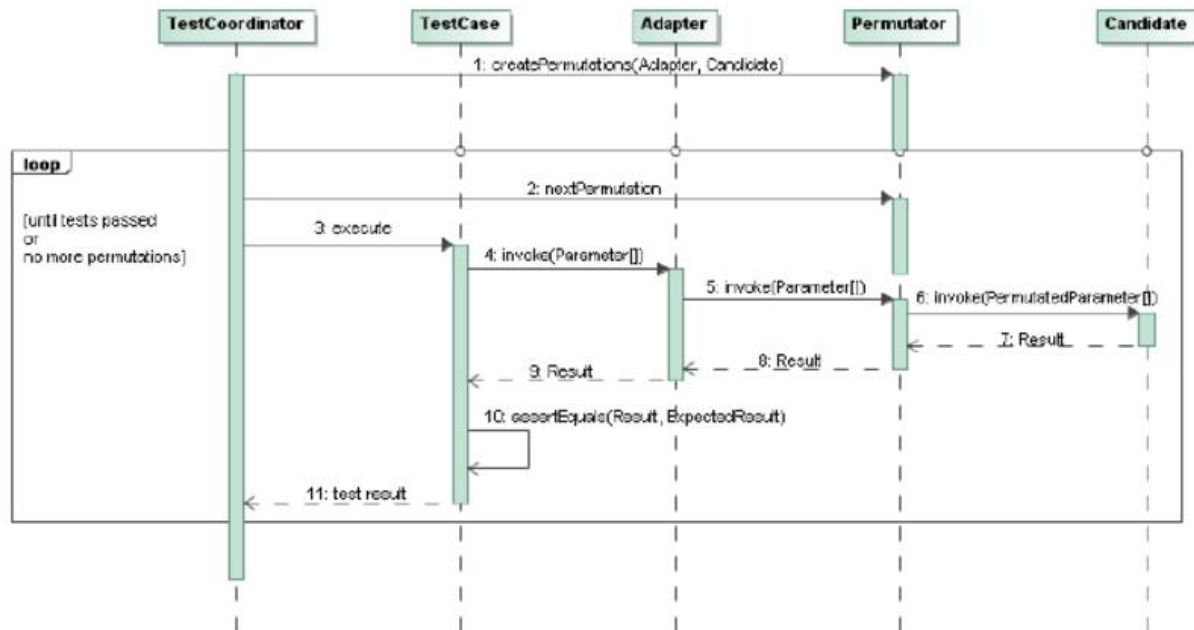
Chapter 2: Literature survey

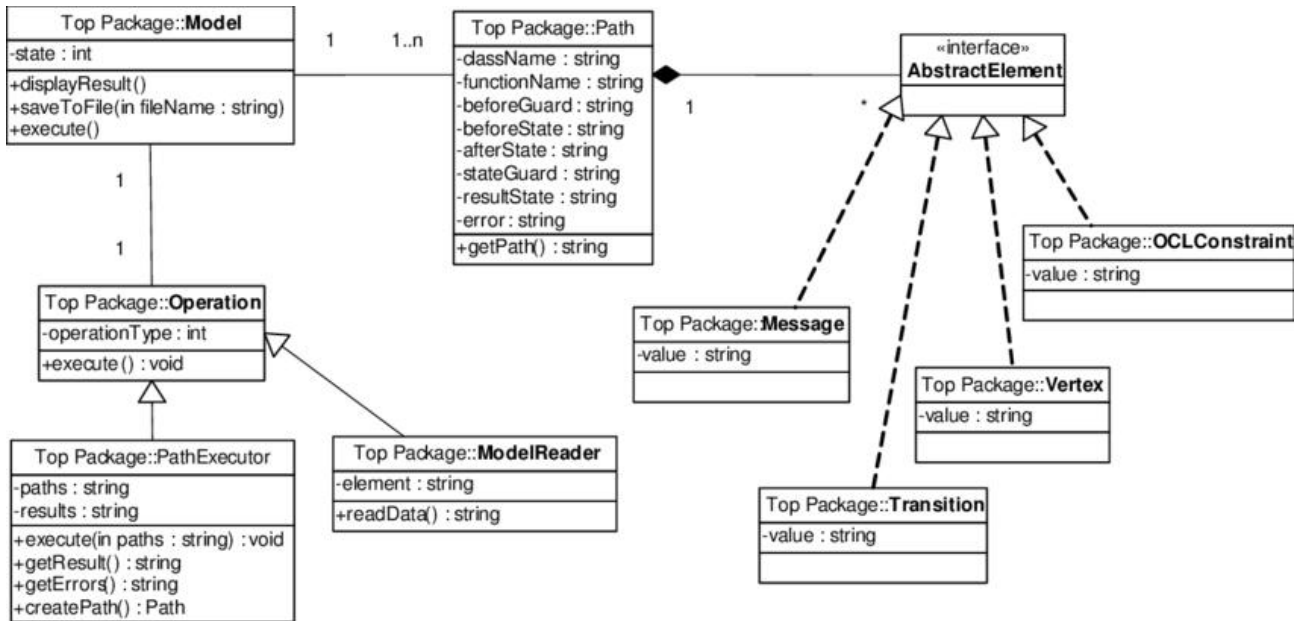
Whatever reservations there may be about ethics, efficiency or cost effectiveness, and with initial skepticism from major players, bug bounties have been embraced by many of the major technology companies as well as gaining support in other industries. Some research about the participants in the programs has started, as well as means of getting around some of the difficulties with running a bug bounty program. As indicated by, prior to the introduction of a formal mechanism for buying and selling bugs through bug bounties, obtaining a seller was challenging. Two reports by Ring illustrated this in further detail, discussing the competing opinion of whether companies should over bounties to vulnerability research - and additionally of some companies prosecuting those discovering vulnerabilities. Kuehn & Mueller, consider the changing dynamics in information security towards bug bounties being considered a norm. After case studies on Microsoft & Facebook's bug bounty they conclude that bug bounty programs exist as a way of reducing uncertainty when exchanging an information good as a reason for their development. There are currently two major operators who have had mention made in the literature who facilitate bug bounties: Bug crowd, and Hackerone, although other websites over a list of other Web applications offering a bounty. Bug crowd now publish an annual report on current trends in the bug bounty area, the most recent being in 2016 . Previously, Wooyun offered a forum for researchers to disclose bugs, and had a more coercive model - the Web applications in question were given a certain period of time to fix the -aws, before the -aw was made public. However, the website has been out of action since July 2016 when the founder Fang Xiaodun was reportedly arrested. As of March 2017, the website still displays a message indicating that it is not operational . Two of the older bounty programs, those of Mozilla and Google for their Web browsers Firefox and Chrome respectively were studied in 2013 . Both were found to be better value for the company than hiring a security researcher on a permanent basis when considering the severe security -aws they discovered relative to the cost. They found Google's bug bounty program gleaned more vulnerabilities for a comparable amount of money, which they suggested was due to the tiered reward system they operated compared to Mozilla's -at fee. In two separate papers, Zhao analysed the behaviour of white hats on the Wooyun and Hackerone platforms. In both platforms they observed the behaviour of white hats in the different systems. In, it was observed that the distribution of effort followed a power law, similar to that observed Lotka about academic publication frequency and supporting observations by, with a maximum of 291 submissions and an overall average of 4.8. Analysis of both revealed that when divided into categories of productivity each group reported a comparable amount of vulnerabilities, in addition to the severity of the vulnerability and the ranking of the website. Maillartetal. focus more on the misaligned incentives involved between the companies running a bug bounty program and the researchers themselves. The interest of the 6 company is to exhaust the amount of -aws to a residual level, whereas the interest of the researcher is the cumulative payoff they will

gain from discovering bugs. This is best served for the researchers by diversifying their efforts across different programs, since there will be bugs to discover which are easier to locate, and there should be less competition. Analysing 35 programs on Hackerone, they follow and observe a windfall effect within a few weeks of the start of the program, after which the amount of reports reduce significantly in quantity. They attribute this to timing effects, where researchers switch to a new program, or possibly stockpile vulnerabilities in advance of the program opening.

Chapter 3: Design flow/Process







Chapter 4: Results analysis and validation

In this tool we merge two basic recon tools so we get a power of 2 tools on the same side as in today's world we have single tool which work all alone. so basically here we are helping in performing two different task by using the same tool. this is the advantage of our tool.

Software Analysis Report

Libraries used Pyfiglet:

pyfiglet is a full port of FIGlet (<http://www.figlet.org/>) into pure python. It takes ASCII text and renders it in ASCII art fonts (like the title above, which is the 'block' font).

Sys:

It lets us access system-specific parameters and functions. `import sys`. First, we have to import the sys module in our program before running any functions. `sys.modules`. This function provides the name of the existing python modules which have been imported.

Socket:

In simpler terms, there is a server and a client. Socket programming is started by importing the socket library and making a simple socket. `import socket s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)` Here we made a socket instance and passed it two parameters.

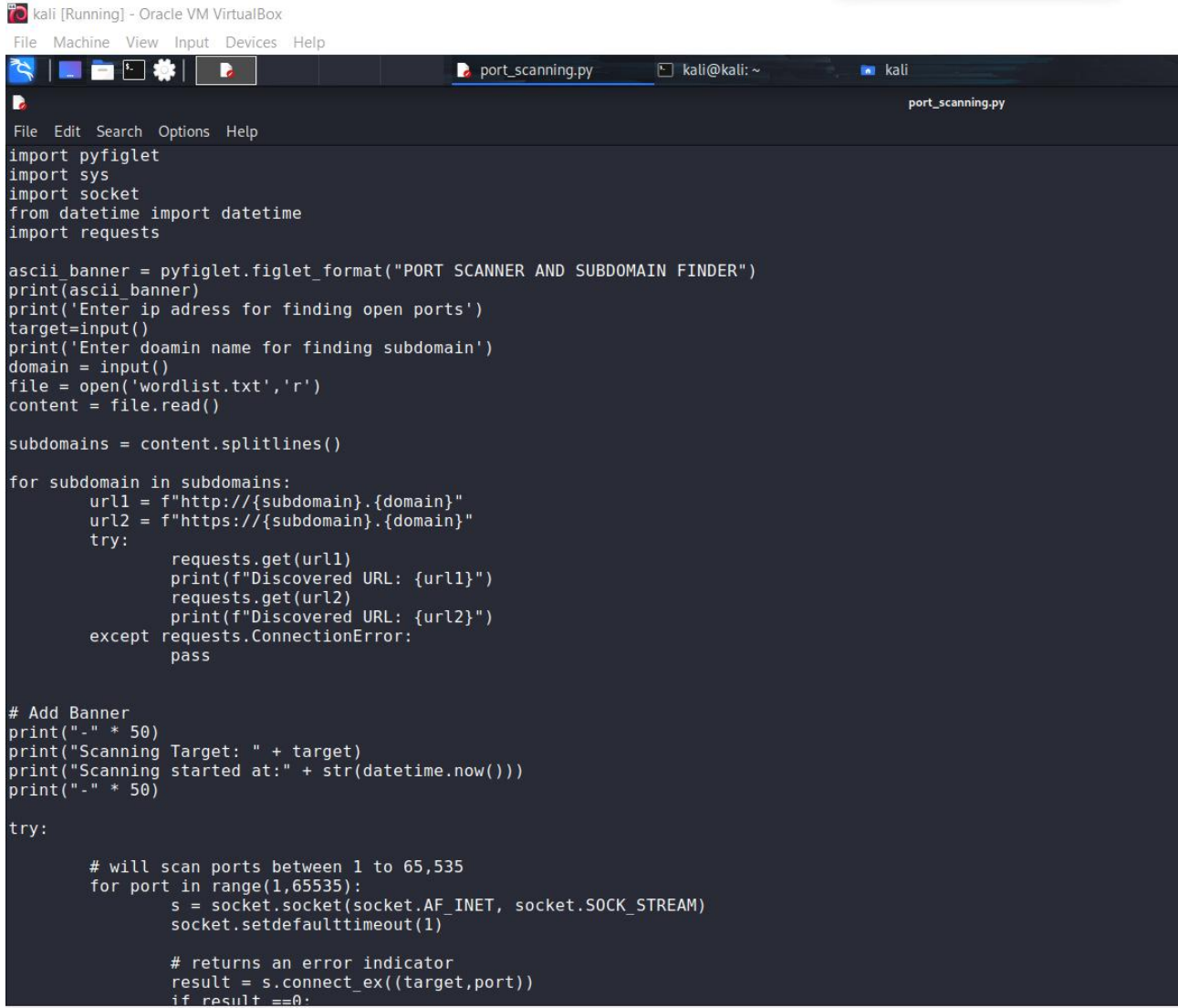
Date time:

The datetime module supplies classes for manipulating dates and times. While date and time arithmetic is supported, the focus of the implementation is on efficient attribute extraction for output formatting and manipulation. See also Module calendar. General calendar related functions.

Requests:

The requests module allows you to send HTTP requests using Python. The `HTTPrequest` returns a `Response Object` with all the response data (content, encoding, status, etc).

SCREEN LAYOUTS:



The screenshot shows a Kali Linux virtual machine running in Oracle VM VirtualBox. The terminal window displays a Python script named `port_scanning.py`. The script is designed to scan for open ports and discover subdomains. It uses `pyfiglet` for a banner, `requests` for HTTP requests, and `socket` for raw socket connections. The script prompts the user for an IP address and a domain name, then reads a wordlist to find subdomains. It scans for open ports between 1 and 65,535 and prints the results.

```
kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
port_scanning.py kali@kali: ~
port_scanning.py
File Edit Search Options Help
import pyfiglet
import sys
import socket
from datetime import datetime
import requests

ascii_banner = pyfiglet.figlet_format("PORT SCANNER AND SUBDOMAIN FINDER")
print(ascii_banner)
print('Enter ip address for finding open ports')
target=input()
print('Enter doamin name for finding subdomain')
domain = input()
file = open('wordlist.txt','r')
content = file.read()

subdomains = content.splitlines()

for subdomain in subdomains:
    url1 = f"http://{subdomain}.{domain}"
    url2 = f"https://{subdomain}.{domain}"
    try:
        requests.get(url1)
        print(f"Discovered URL: {url1}")
        requests.get(url2)
        print(f"Discovered URL: {url2}")
    except requests.ConnectionError:
        pass

# Add Banner
print("-" * 50)
print("Scanning Target: " + target)
print("Scanning started at:" + str(datetime.now()))
print("-" * 50)

try:
    # will scan ports between 1 to 65,535
    for port in range(1,65535):
        s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
        socket.setdefaulttimeout(1)

        # returns an error indicator
        result = s.connect_ex((target,port))
        if result ==0:
```

```
port_scanning.py
File Edit Search Options Help
subdomains = content.splitlines()

for subdomain in subdomains:
    url1 = f"http://{subdomain}.{domain}"
    url2 = f"https://{subdomain}.{domain}"
    try:
        requests.get(url1)
        print(f"Discovered URL: {url1}")
        requests.get(url2)
        print(f"Discovered URL: {url2}")
    except requests.ConnectionError:
        pass

# Add Banner
print("-" * 50)
print("Scanning Target: " + target)
print("Scanning started at:" + str(datetime.now()))
print("-" * 50)

try:
    # will scan ports between 1 to 65,535
    for port in range(1,65535):
        s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
        socket.setdefaulttimeout(1)

        # returns an error indicator
        result = s.connect_ex((target,port))
        if result ==0:
            print("Port {} is open".format(port))
            s.close()

except KeyboardInterrupt:
    print("\n Exiting Program !!!!")
    sys.exit()

except socket.gaierror:
    print("\n Hostname Could Not Be Resolved !!!!")
    sys.exit()

except socket.error:
    print("\n Server not responding !!!!")
    sys.exit()
```

kali [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

```
port_scanning.py kali@kali: ~
File Actions Edit View Help
conn = connection.create_connection(
File "/usr/lib/python3/dist-packages/urllib3/util/connection.py", line 86, in create_connection
sock.connect(sa)
KeyboardInterrupt
url1 = f"http://{subdomain}.{domain}"
url2 = f"https://{subdomain}.{domain}"
(kali@kali)-[~]
$ python3 port_scanning.py
PORT SCANNER
AND SUBDOMAIN
FINDER
# will scan ports between 1 to 65,535
Enter ip address for finding open ports
210.56.125.175
Enter domain name for finding subdomain
zomato.com
Discovered URL: http://www.zomato.com
Discovered URL: https://www.zomato.com
Discovered URL: http://mail.zomato.com
Discovered URL: http://m.zomato.com
Discovered URL: https://m.zomato.com
Discovered URL: http://blog.zomato.com
Discovered URL: https://blog.zomato.com
Discovered URL: http://mobile.zomato.com
Discovered URL: https://mobile.zomato.com
Discovered URL: http://api.zomato.com
Discovered URL: https://api.zomato.com
Discovered URL: http://chat.zomato.com
Discovered URL: https://chat.zomato.com
Scanning Target: 210.56.125.175
Scanning started at:2022-05-15 21:17:49.167703
Port 23 is open
Port 53 is open
Port 80 is open
```


Chapter 5: Conclusion:

The thesis was analyzed the widespread, high-risk risk that is often found in distortion profit programs and presented the novel. Attack methods that target one of the most significant risks a few years ago - malfunctioning of object storage in six different clouds providers. To illustrate the seriousness of this issue, a great deal of research has been done on it Azure Blob Storage malfunction eliminated. This was the first time major research focusing on Azure Blob Storage in the wild, and its results confirmed the idea about the durability of this issue. Large number (5,546) buckets with full community access was obtained, and after a difficult manuscript analysis, 40 buckets containing the most sensitive data were found. All companies involved be notified by email explaining the risks and recommendations reduction. In addition, the list of recommendations created in Section 6.4 has been transferred to six tested cloud providers and is now awaits their response to a possible implementation. This study has shown that although the discovery of poorly prepared buckets is an automatic process, identification The owner can be a very tedious and manual task, as there is no easy way out about how to reach the bucket holder. Because of the time-consuming nature of this process, the motivation for the same large-scale research may no doubt you have

strongly tempted the cruel characters. No bucket at risk which is part of the company with the pest community benefit program identified, but due to the small sample size and the fact that about 70% of bug bounty programs is confidential, there is no reliable conclusion to this the relationship can be drawn. The second additional thesis was the introduction of a new framework for open source automation for distraction profits. This the frame is modularly designed to allow for easy expansion, needed in the fast-growing bug bounty industry. Although the value has not been proven by many users yet, used continuously in the flow of my bug bounty, and for now repaired internally for the defense purposes of technology company Kiwi.com.

Future Scope:

The future of bug bounties is that there won't be any bug bounties at all.

Hacking without physical access to the target will probably become a thing of the past too.

The first step of this transition will be improved bug analysis tools, which will find bugs using static and dynamic analysis. We just need a few great.minds to attend to it, and perhaps some improved computer power.

The endgame will probably involve sophisticated AIs. We can go a bit more abstract and notice a higher trend : the entire world is going from flawed to flawless.

REFERENCES:

1. Geeks for geeks
2. You tube
3. Wikepedia
4. Javat point