PROJECT REPORT ON CYBERSECURITY

Department of Computer Science and Engineering

National Institute of Technology Srinagar

Srinagar, 190006

March 2024

PROJECT REPORT ON CYBERSECURITY

A Report submitted

in partial fulfillment of the requirement

for the award of Degree of

Bachelor of Technology

in

Computer Science and Engineering

by

GUGULOTHU LINGANNA (2021BCSE079)

Under the Guidance of

PREETI DALELA

Managing Director

Shripriti Educational & IT Hub

Department of Computer Science and Engineering

National Institute of Technology Srinagar,

Kashmir 190006, INDIA.

March, 2024

PERMISSION

NATIONAL INSTITUTE OF TECHNOLOGY SRINAGAR
(An autonomous Institute of National Importance under the aegis of Ministry of Education, Govt. of India)
DEPARTMENT OF TRAINING & PLACEMENT
Tel/Fax: +91-194-2424809 Extn: 2130/31 Email: placements@nitsri.net
Hazratbal , Srinagar Jammu and Kashmir, 190006, INDIA

NO: NIT/T&P/INTP/2023-24/CSE/007
Date: 16-10-2023

TO WHOM IT MAY CONCERN

Subject: **Permission of Internship online/offline for student of NIT Srinagar.**

In – Plant/on–the –project internship/Practical Training is an important part of our engineering curriculum. This internship/training is regarded as a vital component of engineering education and is an indicator of extent of field experience, which is very essential for attaining excellence in the technical education. In this context, **Mr. /Ms. Gugulothu Linganna,** Enrolment No: **2021BCSE079** pursuing B. Tech in COMPUTER SCIENCE ENGINEERING DEPARTMENT (2021-2025) in this Institute has completed his/her 4th semester of the degree (pursuing in 5th semester) and is interested in 30 days internship in your esteemed organization.

It will be highly appreciated if your organization provides him/her a chance to get an exposure to some project related to him/her branch of engineering online/offline that is being carried out by your organization during winter vacation from 15th December 2023 to 15th February 2024.

We fervently hope that you will accede to our request and allow him/her to pursue him/her internship in your esteemed organization. The student has been advised to abide by the rules and regulation of your organization. Also, the student has to submit completion report and certificate in the training & placement department after completion of the internship, failing this his/her internship will be deemed incomplete.

Associate TPO (Internships)
Training and Placement
NIT Srinagar

Associate Prof. (Internships)
Training & Placement Department
National Institute of Technology
Srinagar, J&K

CERTIFICATE

STUDENT DECLARATION

I declare that this project report titled **Project report on Cybersecurity** submitted in partial fulfillment of the degree of **B. Tech in Computer Science and Engineering** is a record of original work carried out by me under the supervision of **Preeti Dalela.** The matter embodied in this project, in full or in parts, have not been submitted to any other Institution or University for the award of any degree or diploma. I also declare that the work submitted by me is entirely original, free from plagiarism, and has been diligently checked through Turnitin software to ensure its authenticity.

G. Linganna

GUGULOTHU LINGANNA
2021BCSE079

Place: Srinagar, 190006

Date:11-03-2024

ACKNOWLEDGMENTS

It is my pleasure to be indebted to various people, who directly or indirectly contributed in the development of this work and who influenced my thinking , behaviour and acts during the course of study.

I express my sincere gratitude to **"AICTE"** for providing me an opportunity to undergo winter training at **"Shripriti Educational & IT HUB".**

And also express my sincere gratitude to **Preeti Dalela** Managing Director at **"Shripriti Educational & IT HUB"** for providing me a platform to increase my technical knowledge as well as gaining practical knowledge as well as gaining practical knowledge in Cybersecurity, which will help me to achieve a better job opportunity in my field.

Lastly, I would like to thank the almighty and my parents for their moral support and my friends with whom I shared my day-to-day experience and received lots of suggestions that my quality of work.

GUGULOTHU LINGANNA

ABSTRACT

Cybersecurity is a critical field in the digital age, constantly evolving to counter emerging threats. This paper explores several key components in modern cybersecurity: steganography, port scanning, Scapy, and the OWASP Risk Calculator. Steganography, the art of concealing information within other data, provides a covert communication channel, making detection challenging for adversaries. Port scanning techniques are essential for identifying open ports and potential vulnerabilities in network systems, facilitating proactive defense measures.

Scapy, a powerful Python library, plays a crucial role in network packet manipulation, allowing for the creation, modification, and interpretation of network packets. Its versatility makes it invaluable for both offensive and defensive cybersecurity operations. Additionally, the OWASP Risk Calculator provides a structured approach to assess and prioritize security risks, aiding organizations in allocating resources effectively to mitigate potential threats.

This Project Report delves into the mechanisms, applications, and significance of these cybersecurity tools and methodologies. Through comprehensive analysis, it highlights the importance of integrating these technologies into cybersecurity strategies to enhance resilience against cyber threats. Additionally, it discusses the evolving landscape of cybersecurity, emphasizing the need for continuous adaptation and innovation to stay ahead of adversaries.

Furthermore, it examines the ethical considerations surrounding the use of these tools, emphasizing the importance of responsible and lawful utilization to uphold privacy and security standards. Overall, this paper underscores the crucial role of steganography, port scanning, Scapy, and the OWASP Risk Calculator in bolstering cybersecurity defenses and safeguarding digital assets in an increasingly interconnected world.

TABLE OF CONTENTS

LIST OF TABLES

ABBREVIATIONS/ NOTATIONS/ NOMENCLATURE

ACK	Acknowledgement
ARP	Address Resolution Protocol
BMP	Bitmap Image file
BSD	Berkeley Software Distribution
CLI	Command Line Interface
DNS	Domain Name System
DSL	Domain Specific Language
FIN	Finished
FTP	File Transfer Protocol
GIF	Graphics Interchange Format
GUI	Graphical User Interface
HTML	Hyper Text Markup Language
HTTP	Hyper Text Transfer Protocol
HTTPS	Hyper Text Transfer Protocol Secure
IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol
IP	Internet Protocol
ISP	Internet Service Provider
JPG, JPEG	Joint Photographic Experts Group
LAN	Local Area Network
MAN	Metropolitan Area Network
MFA	Multi-Factor Authentication
Nmap	Network Mapper

OS	Operating System
OSX	MacOS
OWASP	Open Web Application Security Project
PAN	Personal Area Network
PC	Personal Computer
Pcap	Packer Capture
PIL	Python Imaging Library
PNG	Portable Network Graphic
RAM	Random Access Memory
RGB	Red Green Blue
ROM	Read Only Memory
SSH	Secure Shell
SQL	Structured Query Language
SYN	Synchronize
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UTF	Unicode Transformation Format
VLAN	Virtual Local Area Network
VoIP	Voice Over Internet Protocol
WAN	Wide Area Network
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless-Fidelity
WWW	World Wide Web
XMAS	Christmas tree scan

1.CYBERSECURITY

1.1. What is Cybersecurity?

Cybersecurity refers to the practice of protecting computer systems, networks, programs, and data from digital attacks, theft, damage, or unauthorized access. With the increasing reliance on digital technologies in various aspects of life, cybersecurity has become a critical concern for individuals, businesses, governments, and organizations.

1.1 Network Security

Network security is the practice of securing a computer network from intruders or attackers targeted attackers or opportunistic malware.

1.2 Application Security

Application security focuses on keeping software and devices free of threats. A compromised application could provide access to the data its designed to protect. Successful security begins in the design stage, well before a program or device is deployed.

1.3 Information Security

Information security protects the integrity and privacy of data, both in storage and in transit

1.4 Operational Security

Operational security includes the processes and decisions for handling and protecting data assets. The permissions users have when accessing a network and the procedures that determine how and where data may be stored or shared all fall under this umbrella

1.5 Disaster Recovery and Business Continuity

Disaster recovery and business continuity define how an organization responds to a cyber-security incident or any other event that causes the loss of operations or data. Disaster recovery policies dictate how the organization restores its operations and information to return to the same operating capacity as before the event. Business continuity is the plan the organization falls back on while trying to operate without certain resources.

2.STEGANOGRAPHY

2.1 Introduction

Steganography is the art of hiding information within another file, and in this case, we'll use an image to hide text. Tkinter is a popular GUI library in Python, so we can create a simple user interface for the steganography application.

Steganography is the practice of concealing information within a message or physical object to avoid detection. The word comes from the Greek words steganos, which means “covered” or “hidden,” and graph, which means “to write”.

2.2 Characteristics of Steganography

- Conceals messages within carrier data covertly.
- Relies on security through obscurity rather than encryption.
- Offers versatility across various digital media types.
- Ensures robustness against common data manipulations.
- Complements encryption for enhanced security.

2.3 Steganography in Images

Image compression offers a solution to cover large scale image files. Two kinds of image Compression are lossless and lossy compression. Both methods save storage space but have differing in effects on any uncompressed hidden data in the image.

"Lossless" compression keeps and maintains the original image data as like exactly, it is thus more favoured by steganographic techniques or practices.

"Lossy" JPEG (Joint Photographic Experts Group) format files, offers and covers high compression, but may not maintain the original image's integrity. Hence it is called "lossy".

2.4 Image Encoding Techniques

The mostly used common approaches to information hiding in images:

- Least Significant bit insertion.
- Masking and Filtering.
- Algorithms and transformations

2.5 Code: -

```
import tkinter as tk
from tkinter import filedialog
from PIL import Image, ImageTk

def text_to_binary(text):
    binary_string = ''.join(format(ord(char), '08b') for char in text)
    return binary_string

def encode_image():
    text = entry.get("1.0",'end-1c')  # Get text from the Text widget
    binary_text = text_to_binary(text)

    image_path = filedialog.askopenfilename(title="Select an image file", filetypes=[("Image
files", "*.png;*.jpg;*.jpeg;*.bmp")])
    original_image = Image.open(image_path)

    # Encode the text into the image
    encoded_image = original_image.copy()
    binary_index = 0

    for i in range(encoded_image.width):
        for j in range(encoded_image.height):
            pixel = list(encoded_image.getpixel((i, j)))
            for k in range(3):  # Loop through RGB channels
                if binary_index < len(binary_text):
                    pixel[k] = pixel[k] & ~1 | int(binary_text[binary_index])
                    binary_index += 1

            encoded_image.putpixel((i, j), tuple(pixel))

    # Save the encoded image
```

```
    save_path = filedialog.asksaveasfilename(defaultextension=".png", filetypes=[("PNG
files", "*.png")])
    encoded_image.save(save_path)

    status_label.config(text="Image encoded successfully!")

def open_image():
    image_path = filedialog.askopenfilename(title="Select an image file", filetypes=[("Image
files", "*.png;*.jpg;*.jpeg;*.bmp")])
    img = Image.open(image_path)
    img.thumbnail((300, 300))
    img = ImageTk.PhotoImage(img)
    panel.configure(image=img)
    panel.image = img

# GUI setup
root = tk.Tk()
root.title("Steganography Encoder")

label = tk.Label(root, text="Enter text to encode:")
label.pack(pady=10)

entry = tk.Text(root, height=4, width=50)
entry.pack(pady=10)

encode_button = tk.Button(root, text="Encode Image", command=encode_image)
encode_button.pack(pady=10)

open_button = tk.Button(root, text="Open Image", command=open_image)
open_button.pack(pady=10)

panel = tk.Label(root)
panel.pack(padx=10, pady=10)

status_label = tk.Label(root, text="")
status_label.pack(pady=10)

root.mainloop()
```

2.6 Applications:

- Confidential data communication and secret data storing.
- Protecting data from alteration.
- Media Database systems.
- Access control system for digital content distribution.
- Evading detection by embedding malicious code within seemingly harmless files.
- Research and education in information security, cryptography, Cloud Computing and digital forensics.
- Detecting hidden data in digital evidence for forensic analysis captured from incidents.
- Protecting privacy by concealing sensitive information within personal photos or documents(media).
- Evading detection by embedding malicious code within looking harmless files.

2.7 Advantages and Disadvantages

2.7.1 Advantages:

- Difficult to detect and only receiver can detect.
- It can be done faster with larger number of softwares.
- Provides better security for sharing data in LAN, MAN, WAN.
- Complements encryption, enhancing overall data security.
- Offers versatility across various digital media types.
- Enhances data integrity by resisting tampering.
- Embeds large volumes of data subtly within carrier files.
- Enables authentication and copyright protection through digital watermarks.
- Incurs minimal computational overhead compared to encryption.

2.7.2 Disadvantages:

- The Confidentiality of information is covered and maintained by the algorithms, and if the algorithms are known then this technique is of no use and leads to data breach.
- Password leakage may occur and leads to unauthorized access of data and chances to theft the sensitive information.
- If this practice is goes in the wrong hands like hackers can be very much dangerous for all, especially for critical infrastructures.
- Requires both senders and receivers to share and possess knowledge of the steganographic method.
- Limited capacity for hiding large volumes of sensitive data as compared to encryption.
- May not provide absolute security, as hidden information could be compromised if the carrier file is altered or compressed.
- Raises or hikes ethical concerns when these were used for malicious purposes or privacy invasion.

3.SCAPY-

TO READ & BUILD

NETWORK

PACKETS USING

PYTHON

3.1 Introduction

In the computer security field, network scanning is essential activity which is also includes attack simulations. There are many tools like Wireshark or Nmap, but each one of them is designed for a specific purpose, such as packet sniffing or scanning.

3.2 Scapy:The Python-based network packaging tool

Scapy is a Python-based interactive packet with powerful manipulation program and library for networking operations.

Scapy's ability is to forge or decode the packets of a wide range of protocols, sends them in the wire(cables), captures them, stores them and read them using pcap files, match requests and replies, and much more to perform. It is designed to allow and make fast packet prototyping by using default values that works.

Scapy performs two main operations are sending packets and receiving continuous responses. After mentioning a packet set, the tool sends them, receives responses, matches queries with responses, and returns a list of query(ies)/response(s) packet pairs and a list of mismatched packets.

It can easily handles the most classical tasks such as scanning, tracerouting, probing, unit tests, attacks or network discovery(ies) (it can replace hping, 85% of nmap, arpspoof, arp-sk, arping, tcpdump, Wireshark, p0f, etc.). It's operational performance is very well at other specific tasks that supports most other tools can't handle, like sending invalid frames, intruding and injecting our own 802.11 frames, combining techniques together (VLAN hopping+ARP cache poisoning, VoIP decoding on WEP protected channel, ...), etc..,

Scapy supports various python versions like Python 2.7 and Python 3 (3.4 to 3.9). It's intended to be cross platform, and runs on various platforms (Linux, OSX, *BSD, and Windows).
Scapy can be used through it's command Line interface (CLI) or as a library by importing or installing it into Python programs interactively. It can be run on Linux, macOS, or Windows etc..,

Therefore, it is necessary to use a different tool for different task, and this can quickly become cumbersome as per situations. To address this issue, Philippe Biondi created Scapy: a network packet manipulation tool based on Python that allows you to create new features according to your needs.

Scapy does not have a graphical interface, it is integrated and interconnected with some visualization programs or softwares such as Wireshark, GnuPlot, Graphviz, or VPython.

3.3.Code:

```
from scapy.all import *

    # Read a packet from a pcap file
    def read_packet_from_pcap(file_path):
        packets = rdpcap(file_path)
        for packet in packets:
            print(packet.summary())

    # Build a custom packet and send it
    def build_and_send_packet(destination_ip):
        # Craft an IP packet
        ip_packet = IP(dst=destination_ip)

        # Craft a TCP packet
        tcp_packet = TCP(dport=80)

        # Combine the IP and TCP packets
        packet = ip_packet / tcp_packet

        # Send the packet
        send(packet)

    if __name__ == "__main__":
        # Read packets from a pcap file (change the file path accordingly)
        read_packet_from_pcap("datapcap.pcap")

        # Build and send a custom packet (change the destination IP accordingly)
        build_and_send_packet("192.168.56.1")
```

3.4. Features of Scapy for Complete Network Information

- Scapy simplifies identifying issues with most networking tools, which limit creativity and are rigid in purpose.

- Many tools use a shell interface, leading to complex syntax and confusion between decoding and interpretation, tasks better suited for humans.

- Some programs try to mimic this behavior, for example, by saying “this port is open” instead of “I received a SYN-ACK.” However, they frequently make mistakes.

- Such assistance can be invaluable for beginners, but experienced users know that they will spend a lot of time trying to deduce what actually happened from the program’s interpretation.

- A significant amount of information is lost along the way. Often, it is necessary to use tcpdump -xX to decode and interpret everything that escaped the program.

- Even programs that only decode do not provide all the information they received. They only offer the network view that their creator deems sufficient. Therefore, it is incomplete.

3.5. Network tools in 2 Lines of Python with Scapy

Scapy offers custom packet creation, avoiding limits with a flexible model. Users can assemble packets with any value in a field. It utilizes a Domain Specific Language (DSL) for rapid packet descriptions. Python syntax brings efficiency and simplicity, eliminating the need for separate interpreters. Packet layers can be stacked, with easily overridden default values. This reduces the need for separate tools and templates. Scapy enables concise packet description in just two lines, compared to about sixty in C. Thus, 90% of network probing tool lines can be rewritten in two lines.

3.6. A Single survey for multiple interpretations

During network probing, numerous stimuli are sent, with only a few garnering responses, aiding in information extraction for black-box testing. Scapy uniquely furnishes all data, including stimuli and responses, enabling user insight through data examination. Smaller datasets permit exploration, while interpretation depends on the perspective. Unlike most tools, Scapy retains all raw data, facilitating multiple uses and evolving perspectives. Single probes, like scans or traceroutes, can undergo multiple interpretations.

3.7. Applications

- Network packet manipulation, sniffing, and forging for cybersecurity assessments.

3.8. Advantages and Disadvantages

3.8.1 Advantages

- Packet crafting and manipulation at various network layers.
- Real-time packet sniffing and analysis.
- Extensive protocol support, including Wi-Fi (802.11), TCP/IP, and more.
- Seamless integration with Python for custom network automation and testing.
- Flexible and extensible for building custom network tools and solutions.
- Supports network reconnaissance, security testing, and forensics tasks.
- Offers a Pythonic interface for rapid development and prototyping of network applications.

3.8.2 Disadvantages

- Steeper learning curve compared to traditional network analysis tools.
- Limited support for complex protocol parsing and decoding.
- Requires Python proficiency for effective usage and customization.
- Lack of comprehensive documentation for advanced features and functionalities.
- Performance overhead when handling large-scale network traffic.
- Potential security risks if used improperly, such as for malicious network activities.
- Limited support for certain operating systems and hardware configurations.

4. OWASP-

RISK CALCULATOR

4.1. INTRODUCTION

The **Open Web Application Security Project** (**OWASP**) Risk Rating methodology is often used to assess and prioritize risks associated with software applications. It involves evaluating factors such as likelihood, impact, and remediation cost to calculate a risk rating. While OWASP provides guidelines for risk assessment, including the Risk Rating Methodology, they don't provide a specific Python code for a risk calculator.

Ideally, there would be a universal risk rating system that would accurately estimate all risks for all organizations. But a vulnerability that is critical to one organization may not be very important to another. So, a basic framework is presented here that should be ‘‘customized’’ for the particular organization.

The authors have tried hard to make this model simple to use, while keeping enough detail for accurate risk estimates to be made. Please reference the section below on customization for more information about tailoring the model for use in a specific organization.

4.2. Approach

There are many different approaches to risk analysis. See the reference section below for some of the most common ones. The OWASP approach presented here is based on these standard methodologies and is customized for application security.

Let’s start with the standard risk model:

Risk = Likelihood * Impact

In the sections below, the factors that make up “likelihood” and “impact” for application security are broken down. The tester is shown how to combine them to determine the overall severity for the risk.

4.3 . Steps to Determine Various Risk Levels:

- Step 1: Identifying a Risk.
- Step 2: Factors for Estimating Likelihood.
- Step 3: Factors for Estimating Impact.
- Step 4: Determining Severity of the Risk.
- Step 5: Deciding What to Fix.
- Step 6: Customizing Your Risk Rating Model.

4.3.1 Step 1: Identifying a Risk

The first step is:

- to identify a security risk that needs to be rated.

4.3.2 Step 2: Factors for Estimating Likelihood

There are a number of factors that can help determine the likelihood. The first set of factors are related to the threat agent involved.

- Skill level
- Motive
- Opportunity
- Size
- Ease of discovery
- Ease of exploit
- Awareness
- Intrusion detection

4.3.3 Step 3: Factors for Estimating Impact

Again, each factor has a set of options:

- Loss of confidentiality
- Loss of integrity
- Loss of availability
- Loss of accountability
- Financial damage
- Reputation damage
- Non-compliance
- Privacy violation

4.3.4 Step 4: Determining the Severity of the Risk (1)

- Informal Method

Likelihood and Impact Levels	
0 to < 3	low
3 to < 6	medium
6 to 9	high

Table 4.3.4.1 Likelihood and Impact Levels

4.3.5 Step 4: Determining the Severity of the Risk (2)

- Repeatable Method (1)

Likelihood							
Skill level	Motive	Opportunity	Size	Ease of discovery	Ease of exploit	Awareness	Intrusion detection
5	9	4	9	3	3	4	8
Overall Likelihood				**5.625**	Medium		

Table 4.3.5.1 Likelihood

Likelihood							
Skill level	Motive	Opportunity	Size	Ease of discovery	Ease of exploit	Awareness	Intrusion detection
5	9	4	9	3	3	4	8
Overall Likelihood				**5.625**	Medium		

Table 4.3.5.2 Likelihood

- Repeatable Method (2)

Impact							
Loss of confidenti-ality	Loss of integrity	Loss of availability	Loss of account-ability	Financial damage	Reputation damage	Non-compliance	Privacy violation
5	7	7	7	7	9	7	7
				Overall Impact	**7.0**	High	

Table 4.3.5.3. Impact Levels

Impact							
Loss of confidenti-ality	Loss of integrity	Loss of availability	Loss of account-ability	Financial damage	Reputation damage	Non-compliance	Privacy violation
5	7	7	7	7	9	7	7
				Overall Impact	**7.0**	High	

Table 4.3.5.4 Impact Levels

4.3.6 Step 4: Determining the Severity of the Risk (3)

- Determining Severity

Overall Risk Severity				
IMPACT	High	MEDIUM	HIGH	CRITICAL
	Medium	LOW	MEDI	HIGH
	Low	NOTE	LOW	MEDIUM
		Low		High
		LIKELIHOOD		

Table 4.3.6.1 Overall Risk Severity

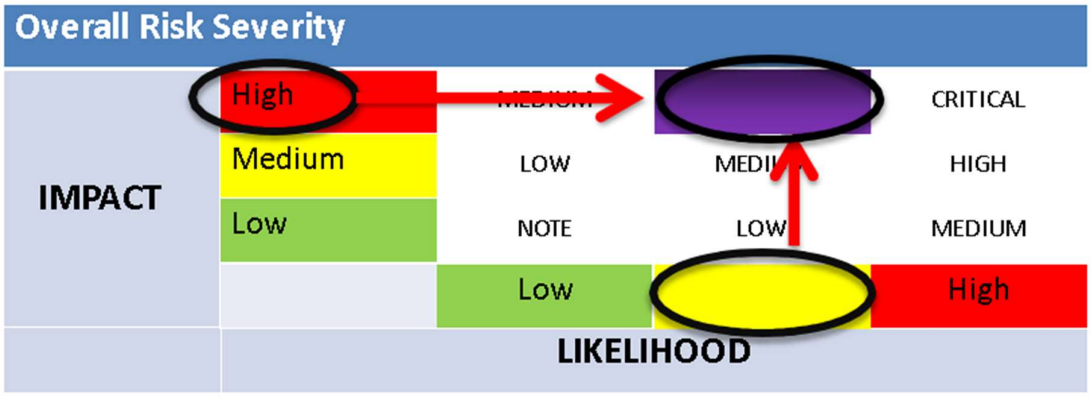

Table 4.3.6.2. Overall Risk Severity

4.3.7 Step 5: Deciding What to Fix

After the risks to the application have been classified there will **be a prioritized list of what to fix.**

As a general rule, the most severe risks should be fixed first. It simply doesn't help the overall risk profile to fix less important risks, even if they're easy or cheap to fix.

Remember that not all risks are worth fixing, and some loss is not only expected, but justifiable based upon the cost of fixing the issue.

4.3.8 Step 6: Customizing the Risk Rating Model

Having a risk ranking framework that is customizable for a business is critical for adoption.

- Adding factors.
- Customizing options.
- Weighting factors.

4.4.Code:

```
<!DOCTYPE>
<html>
        <head>
                <title>OWASP RISK CALCULATOR</title>
  <meta charset="utf-8" />
  <meta http-equiv="content-type" content="text/html" />
  <meta name="viewport" content="width=device-width, initial-scale=1">
  <meta http-equiv="X-UA-Compatible" content="IE=edge" />
                <link rel='stylesheet' href='https://stackpath.bootstrapcdn.com/bootstrap/4.5.2/css/bootstrap.min.css'>
                <script src="https://code.jquery.com/jquery-3.6.0.min.js"></script>
  <script src="https://stackpath.bootstrapcdn.com/bootstrap/4.5.2/js/bootstrap.min.js"></script>
```

```
                <script src="https://cdn.jsdelivr.net/npm/chart.js@3.4.1/dist/chart.min.js"></script>
  <link rel="stylesheet" type="text/css" href="css/owasp_risk.css">
  <script type="text/javascript" src="js/owasp_script.js"></script>
        </head>
        <body>
                <nav class="navbar navbar-expand-lg navbar-light bg-light">
      <a class="navbar-brand" href="index.html"><img src="images/Hackme.png" style="max-width: 2.5rem;margin-
left: 1rem;"></a>
      <button class="navbar-toggler" type="button" data-toggle="collapse" data-target="#navbarNavDropdown" aria-
controls="navbarNavDropdown" aria-expanded="false" aria-label="Toggle navigation">
        <span class="navbar-toggler-icon"></span>
      </button>
      <div class="collapse navbar-collapse" id="navbarNavDropdown">
        <ul class="navbar-nav">
          <li class="nav-item">
            <a class="nav-link" href="blog.html">BOOKS</a>
          </li>
          <li class="nav-item">
            <a class="nav-link" href="about.html">ABOUT ME</a>
          </li>
          <li class="nav-item">
            <a class="nav-link" href="owasp_risk_calculator.html">RISK CALCULATOR</a>
          </li>
          <li class="nav-item dropdown">
            <a class="nav-link dropdown-toggle" href="#" id="navbarDropdownMenuLink" data-toggle="dropdown" aria-
haspopup="true" aria-expanded="false">
              BLOGS
            </a>
            <div class="dropdown-menu" aria-labelledby="navbarDropdownMenuLink">
              <a class="dropdown-item" href="security.html">Security</a>
              <a class="dropdown-item" href="reversengineering.html">Reverse Engineering</a>
              <a class="dropdown-item" href="web-attacks.html">Web Attacks</a>
            </div>
          </li>
        </ul>
      </div>
    </nav>
    <canvas id="myChart" style="width: 400px;height: 400px;" class="container"></canvas>

    <!-- Begin with OWSAP RISK CALCULATOR -->
    <div class="container" style="margin-top:5rem;">
      <button id="overall_score" class="btn btn-link" style="text-align:  center;align-content: center; display:
flex;margin: auto;padding-left: 3rem;padding-right: 3rem;font-size: 2rem;"> 0</button>
    </div>
    <div class="container">
        <div class="row">
                <div class="col-sm-12 col-md-6 topics">
                        <h2>Threat Agent Factors</h2>
                        <hr>
                        <div class="row">
                                <div class="col-4">Skill Level</div>
                                <div class="col-8">
                                        <select id='sl' class="form-control" onchange="calc_score()">
                                                <option value="1">No Technical Skills </option>
                                                <option value="3">Some Technical Skills</option>
                                                <option value="5">Advanced Computer User</option>
                                                <option value="6">Network And Programming
Skills</option>
                                                <option value="9">Security Penetration Skills</option>
                                        </select>
                                </div>
                        </div>
                        <div class="row">
                                <div class="col-4">Motive</div>
                                <div class="col-8" >
                                        <select id='motive' class="form-control" onchange="calc_score()">
                                                <option value="1">Low Or No Reward</option>
                                                <option value="4">Possible Reward </option>
```

```
                                        <option value="9">High Reward </option>
                                    </select>
                                </div>
                            </div>
                            <div class="row">
                                <div class="col-4">Opportunity</div>
                                <div class="col-8">
                                    <select id='oppor' class="form-control" onchange="calc_score()">
                                        <option value="0">Full Access/Expensive Resources
Required</option>
                                        <option value="4">Special Access Or Resources
Required</option>
                                        <option value="7">Some Access Or Resources Required
</option>
                                        <option value="9">No Access Or Resources
Required</option>
                                    </select>
                                </div>
                            </div>
                            <div class="row">
                                <div class="col-4">Size</div>
                                <div class="col-8">
                                    <select id='size' class="form-control" onchange="calc_score()">
                                        <option value="2">Developers</option>
                                        <option value="2">System Administrators</option>
                                        <option value="4">Intranet Users</option>
                                        <option value="5">Partners</option>
                                        <option value="6">Authenticated Users </option>
                                        <option value="9">Anonymous Internet Users</option>
                                    </select>
                                </div>
                            </div>
                        </div>
                            <div class="col-sm-12 col-md-6 topics">
                            <h2>Vulnerability Factors</h2>
                            <hr>
                            <div class="row">
                                <div class="col-4">Ease of Discovery</div>
                                <div class="col-8">
                                    <select id='eod' class="form-control" onchange="calc_score()">
                                        <option value="1">Practically impossible</option>
                                        <option value="3">Difficult</option>
                                        <option value="7">Easy</option>
                                        <option value="9">Automated Tools available</option>
                                    </select>
                                </div>
                            </div>
                            <div class="row">
                                <div class="col-4">Ease of Exploit</div>
                                <div class="col-8">
                                    <select id='eoe' class="form-control" onchange="calc_score()">
                                        <option value="1">Theoretical</option>
                                        <option value="3">Difficult</option>
                                        <option value="5">Easy</option>
                                        <option value="9">Automated Tools available</option>
                                    </select>
                                </div>
                            </div>
                            <div class="row">
                                <div class="col-4">Awareness</div>
                                <div class="col-8">
                                    <select id='aware' class="form-control" onchange="calc_score()">
                                        <option value="1">Unknown</option>
                                        <option value="4">Hidden</option>
                                        <option value="6">Obvious</option>
                                        <option value="9">Public Knowledge</option>
                                    </select>
                                </div>
```

```
                        </div>
                        <div class="row">
                                <div class="col-4">Intrusion Detection</div>
                                <div class="col-8">
                                        <select id='intrude' class="form-control" onchange="calc_score()">
                                                <option value="1">Active Detection In Application</option>
                                                <option value="4">Logged And Reviewed</option>
                                                <option value="8">Logged Without Review</option>
                                                <option value="9">Not Logged</option>
                                        </select>
                                </div>
                        </div>
                </div>
        </div>
    </div>
    <div class="container" style="margin-top:2rem; margin-bottom:2rem;">
        <div class="row">
                <div class="col-2"></div>
                <div class="col-8" style="text-align: center;"><h4>Likelihood score</h4></div>
                <div class="col-2"></div>
        </div>
      <div>
        <button type="button" id="like_score" class="btn btn-link" style="text-align:  center;align-content: center;
display: flex;margin: auto;padding-left: 3rem;padding-right: 3rem;"> 0</button>
      </div>
     </div>
     </div>
     <!-- Impact -->
        <div class="container">
        <div class="row">
                <div class="col-sm-12 col-md-6 topics">
                        <h2>Technical Impact Factors</h2>
                        <hr>
                        <div class="row">
                                <div class="col-5">Loss Of Confidentiality </div>
                                <div class="col-7">
                                        <select id='loc' class="form-control" onchange="calc_score()">
                                                <option value="2">Minimal non-sensitive data
disclosed</option>
                                                <option value="6">minimal critical data disclosed </option>
                                                <option value="6">extensive non-sensitive data
disclosed</option>
                                                <option value="7">extensive critical data disclosed </option>
                                                <option value="9">All Data Disclosed</option>
                                        </select>
                                </div>
                        </div>
                        <div class="row">
                                <div class="col-5">Loss Of Integrity</div>
                                <div class="col-7">
                                        <select id='loi' class="form-control" onchange="calc_score()">
                                                <option value="1">Minimal Slightly Corrupt Data</option>
                                                <option value="3">Minimal Seriously Corrupt Data</option>
                                                <option value="5">Extensive Slightly Corrupt Data</option>
                                                <option value="7">Extensive Seriously Corrupt Data</option>
                                                <option value="9">All Data Totally Corrupt</option>
                                        </select>
                                </div>
                        </div>
                        <div class="row">
                                <div class="col-5">Loss Of Availability</div>
                                <div class="col-7">
                                        <select id='loa' class="form-control" onchange="calc_score()">
                                                <option value="1">Minimal Secondary Services
Interrupted</option>
                                                <option value="5">minimal Primary Services
Interrupted</option>
                                                <option value="5">Extensive Secondary Services
```

```
Interrupted</option>
                                        <option value="7">Extensive Primary Services Interrupted
</option>
                                        <option value="9">All Services Completely Lost</option>
                                    </select>
                                </div>
                            </div>
                            <div class="row">
                                <div class="col-5">Loss of Accountability</div>
                                <div class="col-7">
                                    <select id='loacc' class="form-control" onchange="calc_score()">
                                        <option value="1">Fully Traceable</option>
                                        <option value="7">Possibly Traceable</option>
                                        <option value="9">Completely Anonymous</option>
                                    </select>
                                </div>
                            </div>
                        </div>
                        <div class="col-sm-12 col-md-6 topics">
                            <h2>Businesses Impact Factors</h2>
                            <hr>
                            <div class="row">
                                <div class="col-5">Financial damage</div>
                                <div class="col-7">
                                    <select id='finan' class="form-control" onchange="calc_score()">
                                        <option value="1">Less Than The Cost To Fix The
Vulnerability</option>
                                        <option value="3">Minor Effect On Annual Profit</option>
                                        <option value="7">Significant Effect On Annual
Profit</option>
                                        <option value="9">Bankruptcy</option>
                                    </select>
                                </div>
                            </div>
                            <div class="row">
                                <div class="col-5">Reputation Damage</div>
                                <div class="col-7">
                                    <select id='reput' class="form-control" onchange="calc_score()">
                                        <option value="1">Minimal Damage</option>
                                        <option value="4">Loss Of Major Accounts</option>
                                        <option value="5">Loss Of Goodwill</option>
                                        <option value="9">Brand Damage</option>
                                    </select>
                                </div>
                            </div>
                            <div class="row">
                                <div class="col-5">Non-compliance</div>
                                <div class="col-7">
                                    <select id='comply' class="form-control" onchange="calc_score()">
                                        <option value="2">Minor Violation </option>
                                        <option value="5">Clear Violation</option>
                                        <option value="7">High Profile Violation</option>
                                    </select>
                                </div>
                            </div>
                            <div class="row">
                                <div class="col-5" >Privacy violation</div>
                                <div class="col-7">
                                    <select id='privacy' class="form-control" onchange="calc_score()">
                                        <option value="3">One Individual</option>
                                        <option value="5">Hundreds Of People </option>
                                        <option value="7">Thousands Of People</option>
                                        <option value="9">Millions Of People</option>
                                    </select>
                                </div>
                            </div>
                        </div>
                    </div>
```

```
    </div>
    <div class="container" style="margin-top:2rem; margin-bottom:2rem;">
        <div class="row">
                <div class="col-2"></div>
                <div class="col-8" style="text-align: center;"><h4>Impact score</h4></div>
                <div class="col-2"></div>
        </div>
      <div>
        <button type="button" id="impact_score" class="btn btn-link" style="align-content: center; display: flex;margin:
auto; padding-left: 3rem;padding-right: 3rem;">0</button>
      </div>
     </div>
        </body>
 <script>
    var ctx = document.getElementById('myChart').getContext('2d');
     var myChart = new Chart(ctx, {
        type: 'bar',
        data: {
           labels: ['Threat Agent', 'Vlunerability Factors', 'Technical Impact', 'Business Impact'],
           datasets: [{
              label: 'Score',
              data: [],
              backgroundColor: [
                 'rgba(255, 99, 132, 0.2)',
                 'rgba(54, 162, 235, 0.2)',
                 'rgba(255, 206, 86, 0.2)',
                 'rgba(75, 192, 192, 0.2)',
                 'rgba(153, 102, 255, 0.2)',
                 'rgba(255, 159, 64, 0.2)'
              ],
              borderColor: [
                 'rgba(255, 99, 132, 1)',
                 'rgba(54, 162, 235, 1)',
                 'rgba(255, 206, 86, 1)',
                 'rgba(75, 192, 192, 1)',
                 'rgba(153, 102, 255, 1)',
                 'rgba(255, 159, 64, 1)'
              ],
              borderWidth: 1
           }]
        },
        options: {
           scales: {
              y: {
                 beginAtZero: true,
                 suggestedMin:0,
                 suggestedMax:10
              }
           }
        }
     });

     updateChart();
   function calc_score()
   {
    var LS = 0;
    var IS = 0;
    var dataset = [];
    var TA =  parseInt(document.getElementById('sl').value)+
     parseInt(document.getElementById('motive').value)+
      parseInt(document.getElementById('oppor').value) +
      parseInt(document.getElementById('size').value);
      var VF =  parseInt(document.getElementById('eod').value) +
      parseInt(document.getElementById('eoe').value) +
      parseInt(document.getElementById('aware').value) +
      parseInt(document.getElementById('intrude').value) + 0;
      LS = TA + VF;
      TA = (TA/4).toFixed(3);
```

```
  dataset.push(TA);
  VF = (VF/4).toFixed(3);
  dataset.push(VF);
 var LS = (LS/8).toFixed(3);

var score_LS = 0;
var s1 = document.getElementById('like_score');
s1.innerHTML = LS;
if(LS < 3)
{
 s1.className = "";
 s1.classList.add('btn');
 s1.classList.add('btn-success');
 score_LS = 0;
}
else if(LS >= 3 && LS < 6 )
{
 s1.className = "";
 s1.classList.add("btn");
 s1.classList.add('btn-warning');
 score_LS = 1;
}
else
{
 s1.className = "";
 s1.classList.add('btn');
 s1.classList.add('btn-danger');
 score_LS = 2;
}


 var TI =  parseInt(document.getElementById('loc').value)+
  parseInt(document.getElementById('loi').value)+
   parseInt(document.getElementById('loa').value) +
   parseInt(document.getElementById('loacc').value);
   var BI =  parseInt(document.getElementById('finan').value) +
   parseInt(document.getElementById('reput').value) +
   parseInt(document.getElementById('comply').value) +
   parseInt(document.getElementById('privacy').value) + 0;

  IS = TI + BI;
 var IS = (IS/8).toFixed(3);
 TI = (TI/4).toFixed(3);
 dataset.push(TI);
 BI = (BI/4).toFixed(3);
 dataset.push(BI);

 var s2 = document.getElementById('impact_score');
 s2.innerHTML = IS;
 var score_IS = 0;
 if(IS < 3)
 {
 s2.className = "";
 s2.classList.add('btn');
 s2.classList.add('btn-success');
 score_IS = 2;
}
 else if(IS >= 3 && IS < 6 )
 {
 s2.className = "";
 s2.classList.add("btn");
 s2.classList.add('btn-warning');
 score_IS = 1;
 }
 else
 {
 s2.className = "";
 s2.classList.add('btn');
```

```
 s2.classList.add('btn-danger');
 score_IS = 0;
}

var matrix = [["Medium","High","Critical"],["Low","Medium","High"],["Note","Low","Medium"]]
var o_score = document.getElementById('overall_score');
var final_score = matrix[score_IS][score_LS]
o_score.innerHTML = final_score;
o_score.style.color = "black";
if(final_score == "Note")
{
 o_score.style.background = 'lightgreen';
}
else if(final_score == "Low")
{
 o_score.style.background = "Yellow";
}
else if(final_score == "Medium")
{
 o_score.style.background = "Orange"
}
else if(final_score == "High")
{
 o_score.style.background = "Red"
}
else
{
 o_score.style.background = "Pink";
}
updateChart(dataset);
}

function updateChart(dataset)
{
 myChart.data.datasets[0].data = dataset
 myChart.update();
}

</script>
</html>
```

4.5. OWASP Risk Rating Template (excel format)

Likelihood								
Threat agent factors					Vulnerability factors			
Skill level	Motive	Opportunity	Size		Ease of discovery	Ease of exploit	Awareness	Intrusion detection
4 - Advanced computer user	1 - Low or no reward	4 - Special access or resources required	5 - Partners		3 - Difficult	3 - Difficult	4 - Hidden	3 - Logged and reviewed
Overall likelihood: 3,375 MEDIUM								

Technical Impact					Business Impact			
Loss of confidentiality	Loss of integrity	Loss of availability	Loss of accountability		Financial damage	Reputation damage	Non-compliance	Privacy violation
2 - Minimal non-sensitive data disclosed	1 - Minimal slightly corrupt data	5 - Minimal primary services interrupted, extensive secondary services interrupted	9 - Completely anonymous		1 - Less than the cost to fix the vulnerability	1 - Minimal damage	5 - Clear violation	5 - Hundreds of people
Overall technical impact: 4,250 MEDIUM					Overall business impact: 3,000 MEDIUM			
Overall impact: 3,625 MEDIUM								

Overall Risk Severity = Likelihood x Impact				
Impact	HIGH	Medium	High	Critical
	MEDIUM	Low	Medium	High
	LOW	Note	Low	Medium
		LOW	MEDIUM	HIGH
	Likelihood			

Likelihood and Impact Levels	
0 to <3	LOW
3 to <6	MEDIUM
6 to 9	HIGH

Table 4.5.1. OWASP Risk Rating Template

4.6. OWASP Risk Rating Calc

Likelihood

Threat Agent Factors

Skill Level	Motive	Opportunity	Size
3 - Some technical s	4 - Possible reward	9 - No access or res	4 - Intranet users

Vulnerability Factors

Ease of Discovery	Ease of Exploit	Awareness	Intrusion Detection
7 - Easy	1 - Theoretical	4 - Hidden	8 - Logged without

Impact

Technical Impact

Loss of Confidentiality	Loss of Integrity	Loss of Availability	Loss of Accountability
9 - All data disclosed	1 - Minimal slightly	5 - Minimal primary	1 - Fully traceable

Business Impact

Financial Damage	Reputation Damage	Non-Compliance	Privacy Violation
9 - Bankruptcy	5 - Loss of goodwill	7 - High profile viola	5 - Hundreds of peo

Scores

Intermediate

Overall Likelihood	Overall Technical Impact	Overall Business Impact
5 MEDIUM	4 MEDIUM	6.5 HIGH

Final Score

Adjust score	Risk
Technical / Business	MEDIUM

Table 4.6.1. OWASP Risk Rating Calc

4.7. OWASP Risk Rating Management

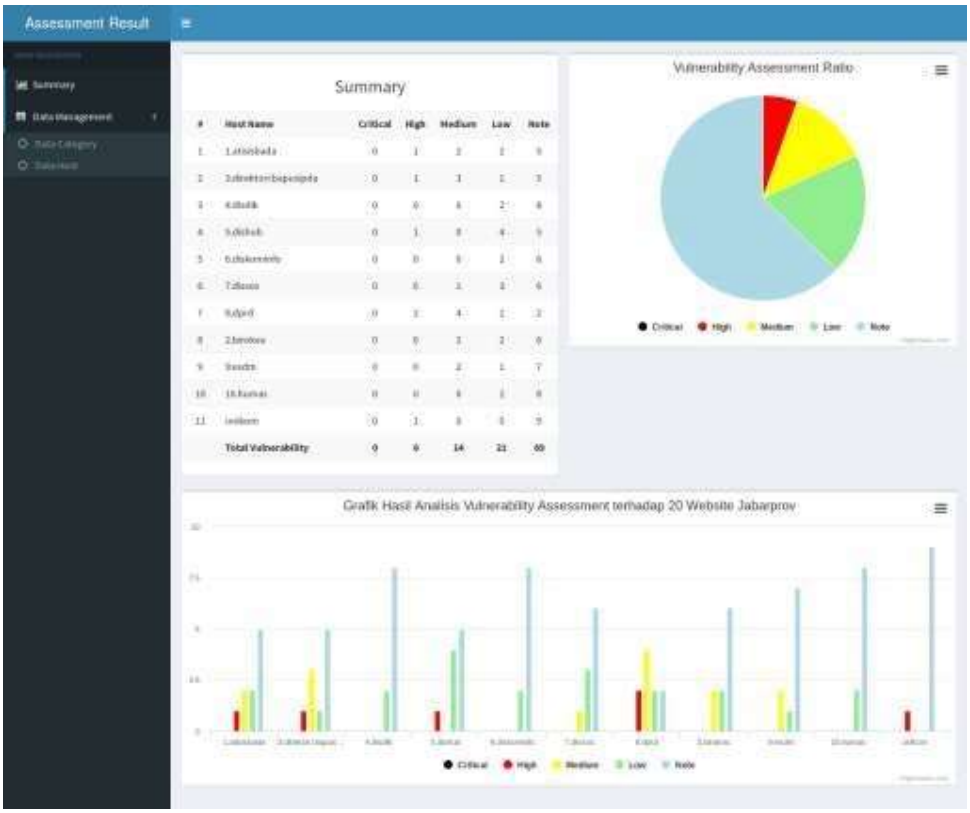

Table 4.7.1. OWASP Risk Rating Management

4.8. Category set by OWASP.

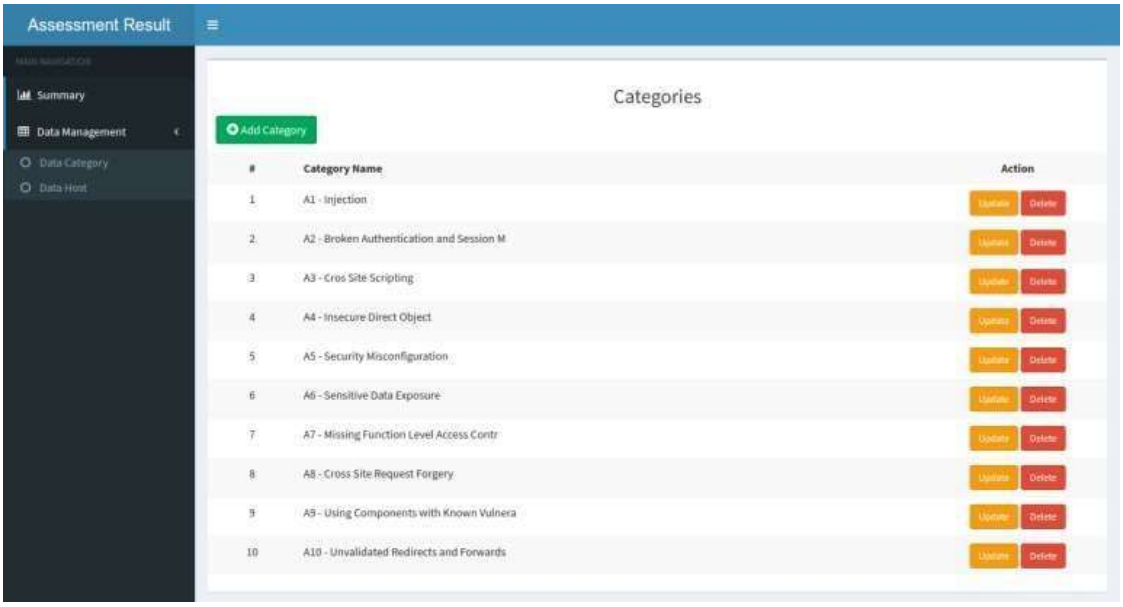

Table 4.8.1. OWASP Risk Category

4.9. Websites to assist the Risk:-

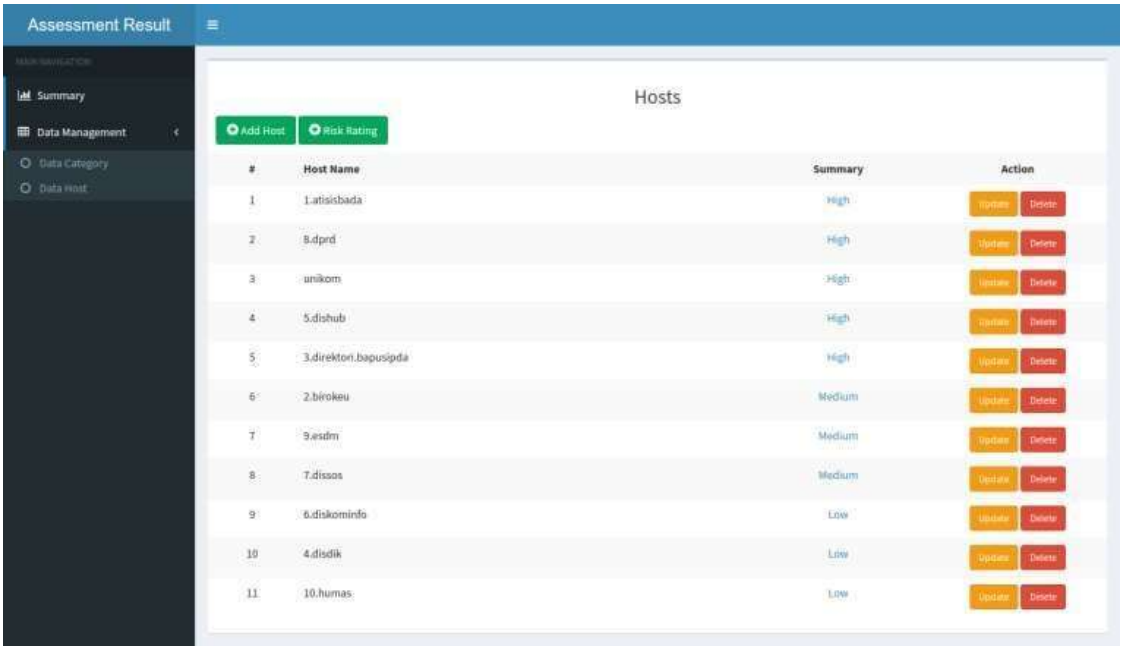

Table 4.9.1.OWASP Website to assist the Risk

5.KEYLOGGER

5.1 Introduction

A keylogger, or keystroke logger, is a type of malware or hardware that records and sends keystrokes to a hacker. Keyloggers can be software or hardware.

5.2 Types of Keyloggers

5.2.1 Software Keyloggers

A software keylogger is a form of malware that infects your device and, if programmed to do so, can spread to other devices the computer comes in contact with. While a hardware keylogger cannot spread from one device to another, like a software keylogger, it transmits information to the hacker or hacking organization, which they will then use to compromise your computer, network, or anything else that requires authentication to access.

Software keyloggers consist of applications that have to be installed on a computer to steal keystroke data. They are the most common method hackers use to access a user's keystrokes.

A software keylogger is put on a computer when the user downloads an infected application. Once installed, the keylogger monitors the keystrokes on the operating system you are using, checking the paths each keystroke goes through. In this way, a software keylogger can keep track of your keystrokes and record each one.

After the keystrokes have been recorded, they are then automatically transferred to the hacker that set up the keylogger. This is done using a remote server that both the keylogger software and the hacker are connected to. The hacker retrieves the data gathered by the keylogger and then uses it to figure out the unsuspecting user's passwords.

The passwords stolen using the key logger may include email accounts, bank or investment accounts, or those that the target uses to access websites where their personal information can be seen. Therefore, the hacker's end goal may not be to get into the account for which the password is used. Rather, gaining access to one or more accounts may pave the way for the theft of other data.

5.2.2 Hardware Keyloggers

A hardware keylogger works much like its software counterpart. The biggest difference is hardware keyloggers have to be physically connected to the target computer to record the user's keystrokes. For this reason, it is important for an organization to carefully monitor who has access to the network and the devices connected to it.

If an unauthorized individual is allowed to use a device on the network, they could install a hardware keylogger that may run undetected until it has already collected sensitive information. After hardware keystroke loggers have finished keylogging, they store the data, which the hacker has to download from the device.

The downloading has to be performed only after the keylogger has finished logging keystrokes. This is because it is not possible for the hacker to get the data while the key logger is working. In some cases, the hacker may make the keylogging device accessible via Wi-Fi. This way, they do not have to physically walk up to the hacked computer to get the device and retrieve the data.

5.3. Detecting a Keylogger:

- The simplest way to detect a keylogger is to check your task manager.
- Differentiate legitimate processes from potential threats by researching each process online.
- Access task manager in Windows by right-clicking on the taskbar and selecting "Task Manager".
- Review Background processes for suspicious activity; examine the Startup tab for unfamiliar programs and disable them if necessary.
- Check computer's internet usage report in Windows settings under "Network & Internet, Data usage".
-
- Investigate any suspicious or unrecognized programs accessing the internet, as they may be keyloggers.

5.3.1 . Extensions to Browsers for various Keyloggers

You can do the same form of investigation with browser extensions. If there are extensions you do not recall installing, disable them because they could be keyloggers. Here is how to access your extensions in some of the most common browsers:

- Safari: Choose "Preferences" in the Safari menu and click on "Extensions."
- Chrome: Go to the address field and type "chrome://extensions."
- Opera: Choose "Extensions," then select "Manage Extensions."
- Firefox: Enter "about: addons" in the address field.
- Microsoft Edge: Select "Extensions" in your browser menu.
- Internet Explorer: Go to the Tools menu and choose "Manage add-ons."

5.4. Keyloggers Attacks Devices:

To gain access to your device, a keylogger has to be installed inside it or, in the case of a hardware keylogger, physically connected to your computer. There are a few different ways keyloggers attack your device.

5.4.1 Spear Phishing

To gain access to your device, a keylogger has to be installed inside it or, in the case of a hardware keylogger, physically connected to your computer. There are a few different ways keyloggers attack your device.

5.4.2 Drive-by Download

Drive-by downloading refers to when a keylogger is installed on your computer without you knowing. This is often accomplished using a malicious website. When you visit the site, malware gets installed on your computer. It then works in the background, undetected, logging your keystrokes, then sending them to the attacker.

5.4.3 Trojan Horse

It is common for Trojan horses to have keyloggers bundled inside. A Trojan horse, similar to the one used in the Greek myth, appears to be benevolent. When the user opens it, malware containing a keylogger gets installed on their device. The malware, once installed, keeps track of the user's keystrokes and then reports them to a device accessed by the hacker.

5.5. Problems Caused by Keyloggers:

5.5.1 . Desktops and Laptops

5.5.1.1 Unknown Processes Consuming Computing Power

Like all types of software, keyloggers need to initiate a process in order to work. Each process your computer has to execute requires processing power. A keylogger's process, once initiated, can be a drain on your computing power. This may result in other applications not running the way they normally would or should. You can figure out which processes are running by pulling up the task manager, as described above in "How to Detect a Keylogger."

5.5.1.2 Delays During Typing

Because a keylogger positions itself between the keyboard and the monitor, one sign of a keylogger may be a delay when you type. If you typically see letters, numbers, or symbols appear on your screen immediately after you hit each key but then you notice a slight delay, that could be a sign that a keylogger is interrupting the process. In some cases, the delayed typing may be due to circumstances like not enough random-access memory (RAM), but if you notice this symptom, it may be a good idea to check for keyloggers.

5.5.1.3 Applications Freeze Randomly

As a keylogger does its work, it may interrupt normal application processing. This can cause the application to freeze without warning. If your applications are freezing more than usual, a keylogger could be the culprit.

5.5.2 Androids and iPhones

While there may not be any hardware keyloggers designed to attack mobile devices, Androids and iPhones can still be compromised by software keyloggers. These work by capturing where on the screen the user presses or taps, which allows the keylogger to see the virtual buttons pressed while the owner types. The data is then recorded and reported to a hacker. The threat may be even worse with these forms of keyloggers because they do more than merely monitor and record keystrokes. They can also record screenshots, things picked up by the camera, the activity of connected printers, what goes into the microphone, and network traffic. A keylogger even has the ability to prevent you from going to certain websites.To get a keylogger onto a mobile device, a hacker only needs to access it for a short period of time. You can also unintentionally install a keylogger on your device by clicking on a link or attachment.

.

5.6 Code:

```
from pynput.keyboard import Key, Listener

log_file = "keylog.txt"  # File to store the keystrokes

def on_press(key):
    try:
        with open(log_file, "a") as f:
            f.write(str(key.char))
    except AttributeError:
        # Special keys like 'Shift', 'Ctrl', etc.
        with open(log_file, "a") as f:
            f.write(str(key))

def on_release(key):
    if key == Key.esc:
        # Stop the listener
        return False

with Listener(on_press=on_press, on_release=on_release) as listener:
    listener.join()
```

5.7. Problems Caused by Keyloggers

- Keep your operating system, your applications, and web browsers up to date with the latest security patches.
- Always be skeptical about any attachments you receive, especially unexpected ones.
- Check your firewall's activity log for anything suspicious.
- Use a good antivirus/anti-malware scanner like Malwarebytes to find and remove keyloggers.
- You may use a password manager to generate highly complex passwords—in addition to enabling you to see and manage your passwords. In many cases, these programs are able to auto-fill your passwords, which allows you to bypass using the keyboard altogether.
- If you are not typing, a keylogger cannot record any strokes, and since password characters are usually replaced by asterisks, even a video surveillance system would not be able to figure out what was entered. In addition, use multi-factor authentication (MFA) when you have the option. A keylogge r may deduce your password, but the second phase of the authentication process may deter them.
- A virtual keyboard can also help prevent keyloggers from accessing your keystrokes. Even a hypervisor-based keylogger, which uses a separate operating system running underneath your main one, cannot access keystrokes performed on a virtual keyboard. On a Windows computer, you can press the Windows key and “R” at the same time

to access its virtual keyboard.

- It is also a good idea to periodically check the hardware connections on your computer. While hardware keyloggers are not as common, the back of a PC's tower may be an inviting attack surface for a keylogging hacker. This is also true when working on a public computer. The attacker may have installed a hardware keylogger days or weeks before you log in to your bank, brokerage, or email accounts.

6.PORT SCANNING

6.1 Introduction

A port scan is a common technique hackers use to discover open doors or weak points in a network. A port scan attack helps cyber criminals find open ports and figure out whether they are receiving or sending data. It can also reveal whether active security devices like firewalls are being used by an organization.

When hackers send a message to a port, the response they receive determines whether the port is being used and if there are any potential weaknesses that could be exploited.

Businesses can also use the port scanning technique to send packets to specific ports and analyze responses for any potential vulnerability. They can then use tools like IP scanning, network mapper (Nmap), and Netcat to ensure their network and systems are secure.

Port scanning can provide information such as:

- Services that are running
- Users who own services
- Whether anonymous logins are allowed
- Which network services require authentication.

6.2. Port

- A port is a point on a computer where information exchange between multiple programs and the internet to devices or other computers takes place. To ensure consistency and simplify programming processes, ports are assigned port numbers. This, in conjunction with an IP address, forms vital information that each internet service provider (ISP) uses to fulfill requests.
- Port numbers range from 0 through to 65,535 and are ranked in terms of popularity. Ports numbered 0 to 1,023 are called “well-known" ports, which are typically reserved for internet usage but can also have specialized purposes. These ports, which are assigned by the Internet Assigned Numbers Authority (IANA), are held by leading businesses and Structured Query Language (SQL) services.
- Ports are generally managed by the Transmission Control Protocol (TCP), which defines how to establish and maintain a network conversation between applications, and User Datagram Protocol (UDP), which is primarily used for establishing low-latency and loss-tolerating connections between applications.

Some of the most popular and most frequently used ports include:

- Port 20 (UDP): File Transfer Protocol (FTP) used for transferring data.
- Port 22 (TCP): Secure Shell (SSH) protocol used for FTP, port forwarding, and secure logins.
- Port 23 (TCP): The Telnet protocol used for unencrypted communication.
- Port 53 (UDP): The Domain Name System (DNS), which translates internet domain names into machine-readable IP addresses.
- Port 80 (TCP): The World Wide Web Hypertext Transfer Protocol (HTTP)

Ports numbered from 1,024 to 49,151 are considered "registered ports," and they are registered by software companies. The ports numbered from 49,152 to 65,535 are considered dynamic and private ports, which can be used by almost everyone on the internet.

6.3. Port Scanning Techniques

A port scan sees packets sent to destination port numbers using various techniques.

Several of these include:

- **Ping scans:** A ping scan is considered the simplest port scanning technique. They are also known as internet control message protocol (ICMP) requests. Ping scans send a group of several ICMP requests to various servers in an attempt to get a response. A ping scan can be used by an administrator to troubleshoot issues, and pings can be blocked and disabled by a firewall.
- **Vanilla scan:** Another basic port scanning technique, a vanilla scan attempts to connect to all of the 65,536 ports at the same time. It sends a synchronize (SYN) flag, or a connect request. When it receives a SYN-ACK response, or an acknowledgment of connection, it responds with an ACK flag. This scan is accurate but easily detectable because a full connection is always logged by firewalls.
- **FTP bounce scan:** This technique enables the sender to disguise their location by using an FTP server to bounce a packet.
- **SYN scan:** Also called a half-open scan, this sends a SYN flag to the target and waits for a SYN-ACK response. In the event of a response, the scanner does not respond back, which means the TCP connection was not completed. Therefore, the interaction is not logged, but the sender learns if the port is open. This is a quick technique that hackers use to find weaknesses.
- **XMAS and FIN scans:** Christmas tree scans (XMAS scans) and FIN scans are more discrete attack methods. XMAS scans take their name from the set of flags that are turned on within a packet which, when viewed in a protocol analyzer like

Wireshark, appear to be blinking like a Christmas tree. This type of scan sends a set of flags, which, when responded to, can disclose insights about the firewall and the state of the ports. A FIN scan sees an attacker send a FIN flag, often used to end an established session, to a specific port. The system's response to it can help the attacker understand the level of activity and provide insight into the organization's firewall usage.

- **Sweep scan:** This preliminary port scanning technique sends traffic to a port across several computers on a network to identify those that are active. It does not share any information about port activity but informs the sender whether any systems are in use.

6.4. Open Port Checker Tool Usage: -

To use the open port checker tool to run a port scan, you have to:

- Open the tool and then enter a domain or IP address.
- The tool then checks which ports are open and active and able to accept requests.
- You can also check individual ports by manually entering them to see if they are taking requests.
- The result you get from the tool is either "open," which means it is available, or "timed out," which means it is either blocked or unavailable.

6.5. Code:-

```
import socket

def port_scan(host, port):
    try:
        sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
        sock.settimeout(1)  # Adjust the timeout as needed
        result = sock.connect_ex((host, port))
        if result == 0:
            print(f"Port {port} is open")
        else:
            print(f"Port {port} is closed")
        sock.close()
    except socket.error:
        print("Failed to connect to server")

def main():
    host = input("Enter the host to scan: ")
    try:
        ip = socket.gethostbyname(host)
        print(f"Scanning host: {ip}")
    except socket.gaierror:
        print("Hostname could not be resolved. Exiting")
        return
```

```
    for port in range(1, 1025):  # Adjust the range of ports to scan
        port_scan(ip, port)

if __name__ == "__main__":
    main()
```

6.6. Preventing Port Scanning Attacks: -

- Port scanning is a popular method cyber criminals use to search for vulnerable servers. They often use it to discover organizations' security levels, determine whether businesses have effective firewalls, and detect vulnerable networks or servers. Some TCP methods also enable attackers to hide their location.

- Cyber criminals search through networks to assess how ports react, which enables them to understand the business's security levels and the systems they deploy.

- Preventing a port scan attack is reliant on having effective, updated threat intelligence that is in line with the evolving threat landscape. Businesses also require strong security software, port scanning tools, and security alerts that monitor ports and prevent malicious actors from reaching their network. Useful tools include IP scanning, Nmap, and Netcat.

6.6.1 Other Defensive Mechanisms: -

Other defense mechanisms include:

- A strong firewall: A firewall can prevent unauthorized access to a business's private network. It controls ports and their visibility, as well as detects when a port scan is in progress before shutting it down.

- TCP wrappers: These enable administrators to have the flexibility to permit or deny access to servers based on IP addresses and domain names.

- Uncover network holes: Businesses can use a port checker or port scanner to determine whether more ports are open than required. They need to regularly check their systems to report potential weak points or vulnerabilities that could be exploited by an attacker.

REFERENCES

1. "Steganography: A Review of Information Hiding Techniques" by Neil F. Johnson, Zoran Duric, and Sushil Jajodia.
2. https://www.kaspersky.com/resource-center

3. Scapy to read & write network Packets using Python : https://scapy.readthedocs.io/en/latest/
4. OWASP Risk Calculator:https://owasp.org/

5. Keylogger:"The Keyloggers Handbook: Discovering & Exploiting Keyloggers" by Preston Miller and Dan Verton,Online Security Blogs and Forums

6. Port Scanning:"Port Scanning Techniques and Countermeasures" by Michael T. Raggo and Chet Hosmer,"Understanding Port Scanning Techniques" by Prateek Gupta and Shekhar Verma.

APPENDIX 1

LIST OF RESPONDENTS TO THE SURVEY

1. IIST
1. NIT
2. JNU
3. IIT, Delhi
4. IIT, Mumby
5. IIT Chennai

Thank You