

# RAMAIAH INSTITUTE OF TECHNOLOGY, BANGALORE -560054

(Autonomous Institute, Affiliated to VTU)

**DEPARTMENT OF**

COMPUTER SCIENCE AND ENGINEERING (ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING)

AND

COMPUTER SCIENCE AND ENGINEERING

(CYBER SECURITY)



**SUBJECT CODE: INT68 TERM:**

INTERNSHIP REPORT

**Cyber Security Internship with Keylogger Development and REC Vulnerability Exploitation**

Submitted by:

Name: Anu S M

USN: 1MS21CY010

M S RAMAIAH INSTITUTE OF TECHNOLOGY

(Autonomous Institute, Affiliated to VTU)

BANGALORE-560054

[www.msrit.edu](http://www.msrit.edu/)

# 2023-2024



# RAMAIAH INSTITUTE OF TECHNOLOGY, BANGALORE -560054

(Autonomous Institute, Affiliated to VTU)

**DEPARTMENT OF**

COMPUTER SCIENCE AND ENGINEERING (ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING)

AND

COMPUTER SCIENCE AND ENGINEERING

(CYBER SECURITY)

**CERTIFICATE**

This is to certify that the “Internship report” submitted by Anu S M (USN: 1MS21CY010) is work done by his/her and submitted during 2023 – 2024 academic year, in partial fulfillment of the requirements for the award of the degree of BACHELOR OF ENGINEERING in COMPUTER SCIENCE AND ENGINEERING (CYBER SECUITY), at Senselearner Technologies Pvt. Ltd.

**Department Internship Coordinator Head of the Department**

**INTERNSHIP COMPLETION CERTIFICATE**

****

**ACKNOWLEDGEMENT**

First, I would like to thank Ms/Mrs. Sneha Singh, Head, of Senselearner technologies Pvt. Ltd, for giving me the opportunity to do an internship within the organization.

I also would like all the people that worked along with me Senselearner technologies Pvt. Ltd with their patience and openness they created an enjoyable working environment.

It is indeed with a great sense of pleasure and immense sense of gratitude that I acknowledge the help of these individuals.

I am highly indebted to Principal Dr. N.V.R. Naidu, for the facilities provided to accomplish this internship.

I would like to thank my Head of the Department [Dr. Thippeswamy M.N](https://msrit.edu/department/faculty-detail.html?dept=cse_ai_ml&ID=1) for his constructive criticism throughout my internship.

I am extremely great full to my department staff members and friends who helped me in successful completion of this internship.

**Student Name:** Anu S M

**USN:** 1MS21CY010

**ABSTRACT**

In the realm of cybersecurity, two significant areas of concern are explored: the OWASP Top 10 report and the pervasive threat of phishing attacks. The OWASP Top 10 report provides invaluable insights into the most prevalent vulnerabilities faced by web applications, offering a comprehensive understanding of risks such as injection attacks and broken authentication. Through meticulous analysis, effective mitigation strategies are unearthed, empowering organizations to fortify their defenses against these vulnerabilities.

In parallel, phishing attacks continue to pose a formidable challenge, exploiting both technical vulnerabilities and human psychology. By dissecting the techniques employed, including email spoofing and deceptive links, alongside real-world case studies, the severity of this threat becomes apparent. These attacks not only compromise sensitive information but also erode trust and tarnish reputations.

By synthesizing the knowledge gleaned from both the OWASP Top 10 report and the exploration of phishing attacks, this abstract lays the foundation for a comprehensive internship report. It underscores the importance of acquiring skills, navigating challenges, and deepening understanding in the field of cybersecurity. Through this internship experience, the journey toward becoming a proficient cybersecurity professional is illuminated, equipped with the tools and knowledge necessary to combat evolving cyber threats effectively.

**Table of Contents**

|  |  |  |
| --- | --- | --- |
| **S.No** | **Title of the Content** | **Page No** |
| **1.** | **COMPANY PROFILE** | **1** |
| **2.** | **INTRODUCTION** | **2** |
| **3.** | **OBJECTIVES AND MODULES** | **4** |
| **4.** | **DESCRIPTION OF ROLES AND RESPONSIBILITIES**  **4.1 Roles and Responsibilities**  **4.2 Overview of Weekly Internship Activities** |  |
| **5.** | **RESOURCES DETAILS**  **5.1 System Configuration**  **5.2 Hardware Requirements**  **5.3 Software tools Requirements** |  |
| **6.** | **TECHNOLOGY** |  |
| **7.** | **IMPLEMENTATION OF MODULES**  **7.1 Coding**  **7.2 Screen Shots** |  |
| **8.** | **SKILLS LEARNED** |  |
| **9.** | **CHALLENGES FACED** |  |
| **10.** | **CONCLUSION** |  |
| **11.** | **REFERENCES** |  |

**COMPANY PROFILE**

Senselearner is a leading Global consulting and Implementation firm, proudly holding the ISO 27001:2013 certification. specialize in cybersecurity services and offer a wide range of services, including risk assessment and management, vulnerability assessment and remediation, incident response and recovery, compliance support, pen testing, training, and awareness. It is committed to providing their clients with the highest level of security and peace of mind.

Website: [http://senselearner.com](http://senselearner.com/)

Phone: 90846 58979

Industry: Computer and Network Security

Company size: 11-50 employees

Headquarters: Dehradun, Uttarakhand

Founded: 2019

**INTRODUCTION**

In an era where the digital landscape is fraught with threats and vulnerabilities, cybersecurity emerges as a paramount concern for individuals, organizations, and society at large. The proliferation of web applications, interconnected systems, and cloud-based services has ushered in unprecedented opportunities for innovation and collaboration. However, it has also exposed a myriad of security risks that threaten the integrity, confidentiality, and availability of sensitive information.

Central to my internship experience was an in-depth analysis of the OWASP Top 10 vulnerabilities, a seminal document that outlines the most critical security risks facing web applications today. Through rigorous study and practical experimentation, I gained insights into vulnerabilities such as Injection, Broken Authentication, and Cross-Site Scripting (XSS), understanding their underlying mechanisms and exploring effective mitigation strategies. This exploration not only deepened my understanding of cybersecurity principles but also equipped me with the tools and techniques needed to identify, assess, and remediate security vulnerabilities in web applications.

Furthermore, my internship journey involved an immersive exploration of phishing exploitation techniques, a pervasive threat vector that capitalizes on human psychology and trust. By dissecting real-world case studies and scrutinizing the technical intricacies of phishing attacks, I gained valuable insights into the symbiotic relationship between social engineering tactics and technological subterfuge. Through simulated phishing exercises and threat modeling, I honed my ability to anticipate and counteract evolving phishing strategies, enhancing resilience against this insidious threat.

Beyond theoretical inquiry, my internship afforded me the opportunity to engage in hands-on activities, including coding exercises, system configuration tasks, and penetration testing simulations. Collaborative projects and team-based endeavors fostered a spirit of innovation and collective problem-solving, amplifying the impact of individual contributions and reinforcing the importance of collaboration in addressing contemporary cybersecurity challenges.

As I reflect on my internship experience, I am deeply grateful for the knowledge gained, the skills acquired, and the relationships forged. This report serves as a testament to the journey undertaken, offering insights into the multifaceted nature of cybersecurity and the imperative of continuous learning and adaptation in safeguarding digital assets. As I transition from intern to cybersecurity professional, I carry with me the lessons learned and the experiences gained, ready to embark on new challenges and contribute to the ever-evolving field of cybersecurity.

**OBJECTIVES AND MODULES**

During my internship at Senselearner technologies Pvt Ltd, the journey commenced with a thorough exploration of cybersecurity fundamentals. Understanding the critical importance of cybersecurity in today's digital landscape, the primary objective was to fortify my knowledge and skills in this domain.

1. **Information Gathering:**
   * Initiated the internship journey with a thorough investigation of the company's online presence, meticulously dissecting its website architecture, and scrutinizing its network infrastructure.
   * Employed various reconnaissance techniques to map out the organization's digital footprint, including foot printing, DNS enumeration, and WHOIS analysis.
   * Leveraged tools such as Nmap, Recon-ng, and Shodan to gather valuable intelligence on the company's web servers, domain names, IP addresses, and network services.
   * Compiled a comprehensive report detailing the findings, including potential security vulnerabilities and areas for improvement in the company's cybersecurity posture.
2. **Networking Basics Badge:**
   * Embarked on a structured learning path through the Cisco Networking Academy to solidify foundational knowledge in networking principles.
   * Completed a series of online courses covering essential networking concepts, including OSI model layers, TCP/IP protocols, subnetting, and VLANs.
   * Engaged in hands-on lab exercises to reinforce theoretical concepts, configuring routers, switches, and firewalls in simulated network environments.
   * Demonstrated proficiency in networking fundamentals by earning a coveted Cisco badge, validating acquired skills and expertise.
3. **Phishing Exploitation Techniques and Nmap lab:**
   * Delved into the intricate world of phishing attacks, gaining insight into the multifaceted techniques employed by malicious actors to deceive and manipulate unsuspecting targets.
   * Participated in simulated phishing exercises to understand the psychology behind phishing tactics and the importance of user awareness and education.
   * Analyzed real-world case studies of phishing attacks, dissecting the methods used and the impact on targeted individuals and organizations.
   * Developed proficiency in detecting and mitigating phishing threats through a combination of technical controls, user training, and threat intelligence.
4. **OWASP Top 10 Labs:**
   * Immersed myself in the realm of web application security by tackling hands-on labs focused on the OWASP Top 10 vulnerabilities.
   * Utilized interactive platforms like TryHackMe to navigate through practical exercises designed to simulate real-world cybersecurity scenarios.
   * Explored a diverse range of vulnerabilities, including SQL injection, cross-site scripting (XSS), broken authentication, and insecure deserialization.
   * Applied a systematic approach to identifying, exploiting, and mitigating each vulnerability, honing skills essential for securing web applications against common threats.
5. **Cybersecurity Best Practices:**
   * Engaged in ongoing research and study to stay abreast of the latest cybersecurity trends, emerging threats, and best practices.
   * Explored topics such as security hygiene, incident response, penetration testing methodologies, and regulatory compliance.
   * Collaborated with industry professionals and peers to exchange knowledge, share insights, and contribute to the cybersecurity community.
   * Implemented cybersecurity best practices within the internship scope, applying learned principles to enhance the security posture of the organization.

Each module within the internship curriculum was meticulously designed to provide a holistic learning experience, combining theoretical knowledge with practical application to cultivate well-rounded cybersecurity professionals. Through dedication, hands-on practice, and a commitment to continuous learning, I have fortified my skills and expertise in cybersecurity, poised to tackle the dynamic challenges of the ever-evolving threat landscape.

**DESCRIPTION OF ROLES AND RESPONSIBILITIES**

**4.1 Roles and Responsibilities**

**Network Security Assistant**: Assisting the network security team, I contributed to the monitoring and maintenance of network security controls. This involved configuring firewalls, intrusion detection systems (IDS), and other network security appliances, as well as analyzing network traffic and logs for signs of unauthorized access or malicious activity.

**Report Developer:** I undertook the role of a report developer, tasked with compiling comprehensive reports documenting the findings of security assessments and penetration tests conducted during the internship. These reports served as crucial documentation of vulnerabilities discovered, their potential impact on the organization's security posture, and actionable recommendations for remediation.

**4.2 Overview of Weekly Internship Activities**

The internship activities were structured over the course of six weeks, with each week focusing on specific aspects of cybersecurity and practical skill development. The following provides a detailed overview of the weekly activities.

**Week 1: Orientation and Introduction to Cybersecurity:**

* Orientation sessions introduced me to the organization's cybersecurity policies, procedures, and infrastructure.
* Received an overview of cybersecurity concepts, including threat landscape analysis, risk assessment methodologies, and compliance frameworks.

**Week 2: Linux Fundamentals and Information Gathering:**

* Completed a Linux fundamentals course to gain essential skills in operating systems commonly used in cybersecurity.
* Participated in practical exercises to learn command-line basics, file system navigation, user management, and shell scripting.
* Engaged in information gathering and reconnaissance activities to assess the organization's digital footprint using Linux-based tools and techniques.

**Week 3: Networking Basics and Nmap Lab:**

* Completed networking basics courses provided by the Cisco Networking Academy, earning a badge in networking fundamentals.
* Participated in a lab exercise focused on Nmap, gaining hands-on experience in network scanning techniques and reconnaissance methodologies.

**Week 4: Phishing Awareness and Mitigation:**

* Studied phishing awareness strategies and mitigation techniques to combat phishing attacks effectively.
* Conducted simulated phishing exercises to assess employee susceptibility and provided training on identifying and reporting phishing attempts.

**Week 5: Introduction to OWASP Top 10 Vulnerabilities:**

* Delved into the OWASP Top 10 vulnerabilities prevalent in web applications, such as SQL injection, cross-site scripting (XSS), and broken authentication.
* Participated in practical exercises to understand how these vulnerabilities can be exploited and learned about best practices for mitigating them.

**Week 6: Final Assessment and Reporting:**

* Consolidated findings from security assessments and penetration tests into comprehensive reports.
* Presented reports to the cybersecurity team and organizational stakeholders, highlighting vulnerabilities identified, potential risks, and recommendations for improving security posture.

Top of Form

**RESOURCES DETAILS**

**5.1 System Configuration:**

During the internship, the following system configuration was utilized to facilitate various cybersecurity tasks and activities:

* **Operating System:** Kali Linux 2021.4 (64-bit)
* **Processor:** Intel Core i5 (or equivalent)
* **RAM:** 8 GB DDR4
* **Storage:** 256 GB SSD
* **Network Interface:** Ethernet (1000 Mbps)

This system configuration provided sufficient resources to run virtual machines, perform network scans, conduct penetration testing, and execute other cybersecurity-related tasks effectively.

**5.2 Hardware Requirements:**

The hardware requirements for the internship primarily consisted of standard computing equipment and peripherals, including:

* **Desktop or Laptop Computer:** Required for accessing training materials, virtual labs, and performing hands-on exercises.
* **Keyboard and Mouse:** Essential for input and navigation during practical exercises and lab sessions.
* **USB Drive:** Utilized for transferring files, virtual machine images, and other resources between systems.

**5.3 Software Tools Requirements:**

A diverse range of software tools was employed throughout the internship to facilitate learning, experimentation, and practical application of cybersecurity concepts. These included:

* **Virtualization Software:** VMware Workstation, VirtualBox
* **Network Scanning Tools:** Nmap, Wireshark
* **Penetration Testing Platforms:** Kali Linux
* **Programming Language:** Python
* **Web Application Testing Tools:** OWASP ZAP, Burp Suite
* **Remote Access Tools:** SSH
* **Documentation and Reporting Tools:** Microsoft word

**5.4 Additional Resources:**

* **TryHackMe Account:** Access to the TryHackMe platform provided access to a wide range of cybersecurity training materials, interactive labs, and real-world scenarios. This platform offered hands-on experiences covering various topics such as network security, web application security, and ethical hacking, enhancing practical skills and knowledge.

**TECHNOLOGY**

1. **Kali Linux:**

Kali Linux is a specialized Linux distribution designed for penetration testing, digital forensics, and security auditing. It includes a vast array of pre-installed tools and utilities essential for conducting cybersecurity assessments and exercises.

Kali Linux served as the primary operating system for the duration of the internship, providing a robust platform for performing various security-related tasks, such as vulnerability scanning, exploitation, and analysis.

1. **Python:**

Python emerged as a fundamental programming language for cybersecurity practitioners, offering versatility and ease of use in developing custom scripts, tools, and exploits. Interns leveraged Python for automation, tool development, and creating payloads for penetration testing, including the development of a keylogger for potential integration into phishing emails.

1. **Virtualization Software:**

Virtualization software such as VMware Workstation and VirtualBox played a crucial role in creating and managing virtualized environments for simulating real-world network configurations, deploying vulnerable machines for penetration testing, and isolating experimental setups from the host system.

1. **TryHackMe:**

TryHackMe is an online platform that offers virtual labs, challenges, and interactive learning experiences for individuals interested in cybersecurity. It provides hands-on environments for practicing penetration testing techniques, exploit development, and defensive strategies.

Interns utilized TryHackMe extensively to solve labs, participate in challenges, and gain practical experience in various cybersecurity domains, including network security, web exploitation, and digital forensics.

1. **Metasploit Framework:**

Metasploit Framework is an open-source penetration testing platform that provides a comprehensive suite of tools for exploiting vulnerabilities, managing payloads, and conducting post-exploitation activities.

During the internship, interns leveraged Metasploit Framework to simulate real-world cyber attacks, assess the security posture of target systems, and demonstrate the impact of security vulnerabilities.

1. **Wireshark:**

Wireshark is a powerful network protocol analyzer that enables users to capture, analyze, and interpret network traffic in real-time. It provides insights into network communications, protocols, and potential security threats.

Interns utilized Wireshark for network traffic analysis, packet inspection, and troubleshooting during various cybersecurity exercises, helping them understand network behavior and identify suspicious activities.

1. **Nmap:**

Nmap (Network Mapper) is a versatile network scanning tool used for host discovery, port scanning, service enumeration, and vulnerability detection. It provides valuable information about the network topology and potential security weaknesses.

Interns employed Nmap to scan network infrastructures, identify active hosts, enumerate open ports, and gather information about running services, assisting in the assessment of network security and vulnerability management.

**IMPLEMENTATION OF MODULES**

**7.1 Coding**

During the internship, significant emphasis was placed on practical coding tasks aimed at enhancing technical skills and understanding various cybersecurity concepts. The coding tasks primarily focused on developing scripts and tools to automate processes, simulate attacks, and analyse vulnerabilities. Notably, one of the key coding projects undertaken during the internship was the development of a keylogger using Python.

**Keylogger Development:**

* Objective: The objective of this project was to create a keylogger program capable of recording keystrokes on a target system covertly.
* Methodology: Python programming language was utilized due to its versatility and ease of implementation. The keylogger script was designed to run silently in the background, capturing keystrokes without the user's knowledge.
* Features: The keylogger incorporated features such as:
  + Keystroke Logging: Capturing all keystrokes typed by the user, including text input, passwords, and commands.
  + Stealth Mode: Operating discreetly to avoid detection by the user or antivirus software.
  + Persistence: Ensuring that the keylogger remains active across system reboots.
* Application: The keylogger script was integrated into simulated phishing emails as part of an exercise to demonstrate the potential risks associated with phishing attacks. When recipients interacted with the malicious email, the keylogger would silently capture their keystrokes, including sensitive information.

Additionally, another significant coding task involved the exploration of remote code execution (RCE) vulnerabilities in web applications. An RCE exploit was identified and utilized to demonstrate the severity of such vulnerabilities.

**Remote Code Execution (RCE) Exploitation:**

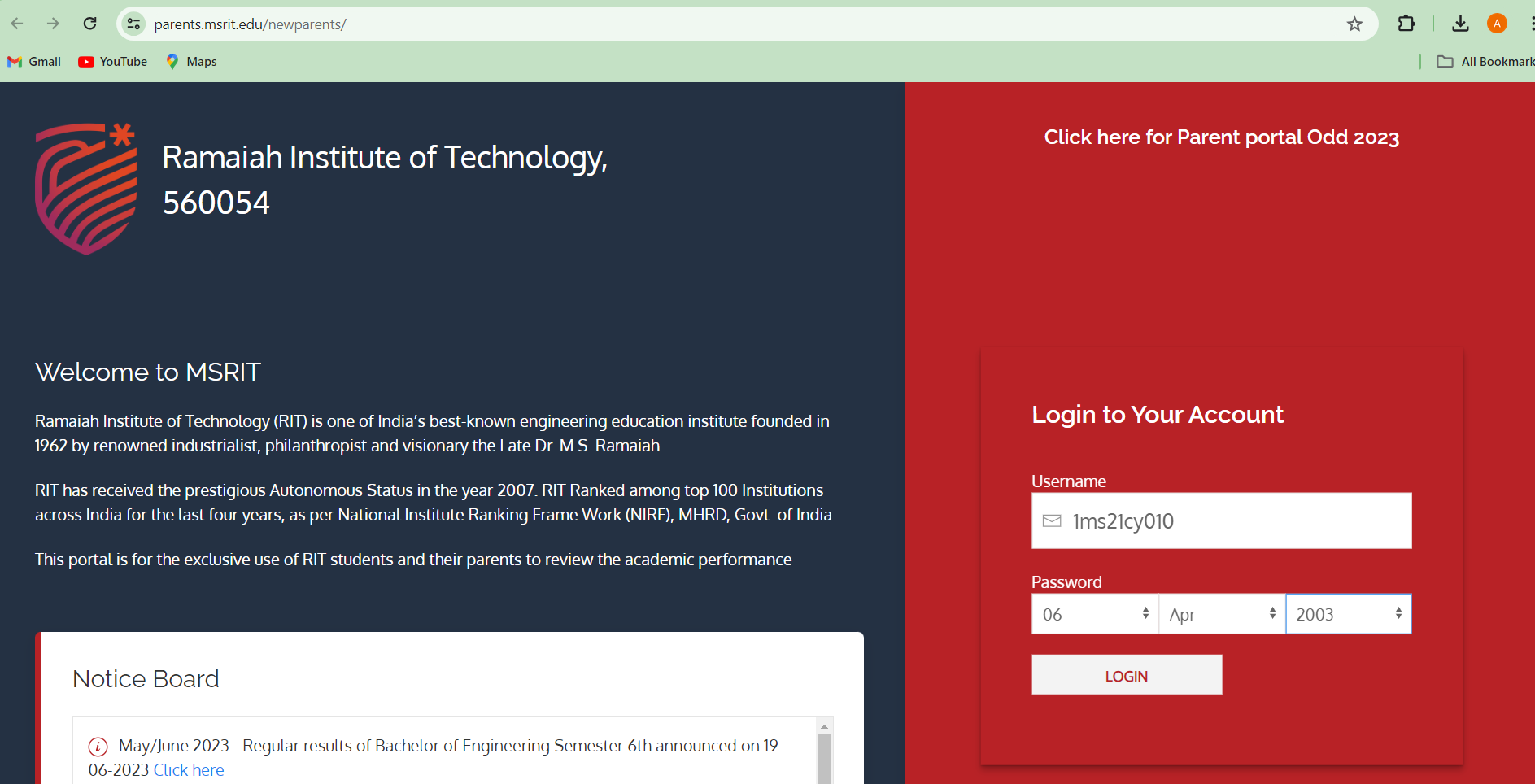
* Exploration: The task involved conducting reconnaissance on a web application to identify potential vulnerabilities. Through research and analysis, an unauthenticated RCE vulnerability was discovered in the Online Book Store application.
* Exploitation: A Python script was developed to exploit the identified RCE vulnerability. The script utilized a crafted payload to upload a PHP web shell to the target server, allowing remote command execution.
* Payload Execution: Upon successful exploitation, the web shell provided a command execution interface, enabling various commands to be executed on the target server remotely.
* Consequences: The successful exploitation of the RCE vulnerability highlighted the critical importance of secure coding practices and diligent vulnerability management in web applications.

Overall, the coding module provided valuable hands-on experience in developing cybersecurity tools and understanding the mechanisms behind various attack vectors.

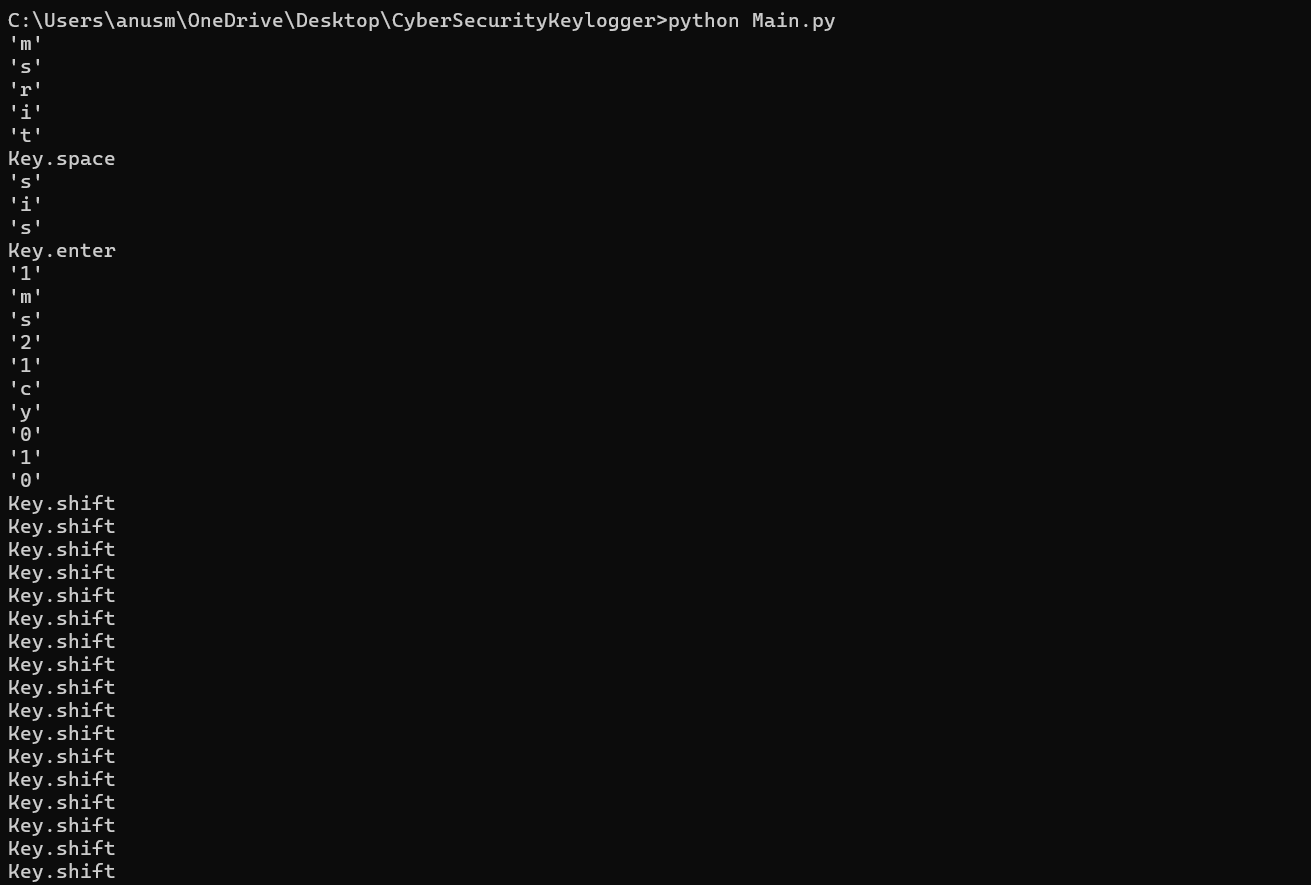
**7.2 Screenshots:**

**Keylogger**

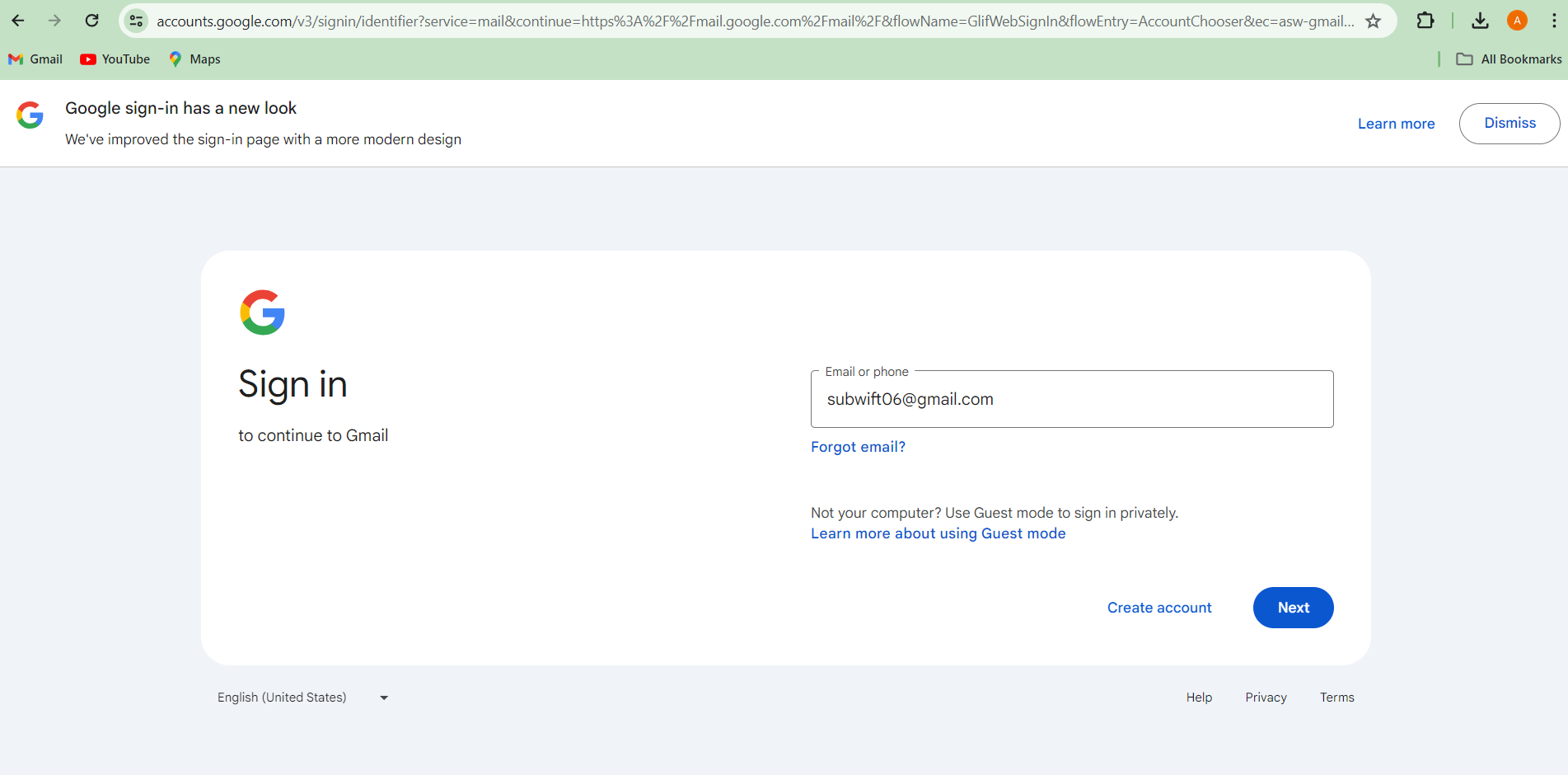
**User Authentication Process in MSRIT SIS**



**Keylogger Capturing Keystrokes**



**User authenticating in Gmail**



**Keylogger Capturing strokes**



**Remote Code Execution Process**

**Unauthenticated RCE vulnerability was discovered in the Online Book Store application**.



Payload: https://www.exploit-db.com/exploits/47887

Download the payload: w get <https://www.exploit-db.com/exploits/47887>

**Getting Number of characters present in the passwd file**



**SKILLS LEARNED**

1. **Cybersecurity Fundamentals:** Developed a solid understanding of cybersecurity principles, including threat detection, vulnerability assessment, and risk management.
2. **Network Reconnaissance:** Learned techniques for network reconnaissance, including identifying network hosts, services, and vulnerabilities using tools like Nmap.
3. **Phishing Awareness:** Gained insights into the various forms of phishing attacks, their techniques, and mitigation strategies.
4. **Exploitation Techniques:** Acquired knowledge of common exploitation techniques, including remote code execution (RCE), and their countermeasures.
5. **Web Application Security:** Explored web application security vulnerabilities such as components with known vulnerabilities and learned how to mitigate them.
6. **Linux Proficiency:** Developed proficiency in using Linux-based operating systems, particularly Kali Linux, for penetration testing and ethical hacking purposes.
7. **Python Programming:** Enhanced Python programming skills by developing scripts for tasks such as creating payloads, web scraping, and automating penetration testing tasks.
8. **Keylogger Development:** Learned to develop a keylogger using Python for capturing keystrokes, understanding its potential for monitoring and security implications.
9. **Report Writing:** Improved report writing skills by documenting findings, methodologies, and recommendations in a structured and concise manner.
10. **Critical Thinking and Problem-Solving:** Enhanced critical thinking and problem-solving abilities by analysing security issues, identifying vulnerabilities, and proposing effective solutions.

**CHALLENGES FACED**

1. **Technical Complexity:** Dealing with the technical intricacies of cybersecurity tools and techniques, such as configuring network scanners or understanding exploit payloads, posed initial challenges.
2. **Resource Limitations:** Working within the constraints of limited resources, such as access to high-end hardware or software licenses, sometimes hindered the execution of certain experiments or simulations.
3. **Time Management:** Due to the comprehensive nature of certain testing and scanning procedures, some tasks demanded considerable time investment to ensure thoroughness and accuracy.
4. **Complexity of Exploitation Techniques:** Understanding and implementing sophisticated exploitation techniques, like remote code execution or phishing attacks, demanded comprehensive research and practice.
5. **Risk of Breaking Systems:** Engaging in hands-on penetration testing activities carried the inherent risk of inadvertently disrupting systems or causing unintended damage, necessitating caution and meticulous planning

.

1. **Continuous Learning:** Keeping pace with the rapidly evolving landscape of cybersecurity, including emerging threats, tools, and techniques, necessitated a commitment to continuous learning and professional development.
2. **Cybersecurity Awareness:** Addressing the gaps in cybersecurity awareness among users or stakeholders, particularly regarding phishing or social engineering threats, required innovative educational approaches.

**CONCLUSION**

In conclusion, the internship experience provided an invaluable opportunity to delve into the dynamic and critical field of cybersecurity. Throughout the 6-week program, a diverse range of skills, knowledge, and practical experiences were acquired, contributing significantly to personal and professional development.

The journey began with an exploration of fundamental networking concepts through the Cisco Networking Academy, followed by hands-on exercises in Linux fundamentals and system administration using Kali Linux. Subsequently, the focus shifted to cybersecurity offensive techniques, including reconnaissance, exploitation, and remote code execution, through platforms like TryHackMe.

Engaging in real-world scenarios, such as phishing simulations and vulnerability exploitation labs, underscored the importance of proactive defense measures and the significance of robust cybersecurity practices. By dissecting the OWASP Top 10 vulnerabilities and exploring mitigation strategies, a deeper understanding of web application security was gained, paving the way for informed risk management and threat mitigation strategies.

The development of practical skills, including coding custom exploits and deploying keylogger payloads, highlighted the dual nature of cybersecurity as both an offensive and defensive discipline. Challenges encountered along the way, from technical complexities to ethical dilemmas, provided invaluable learning opportunities and fostered resilience and adaptability in the face of adversity.

Moreover, the internship experience emphasized the importance of continuous learning and staying abreast of emerging threats and technologies in the ever-evolving cybersecurity landscape. Through collaboration with peers, mentorship, and hands-on experimentation, a solid foundation was laid for future endeavors in cybersecurity.

In essence, the internship journey was not only about acquiring technical skills but also about cultivating a mindset of curiosity, critical thinking, and ethical responsibility. Armed with newfound knowledge and experiences, the path forward in cybersecurity is illuminated, with a commitment to safeguarding digital assets, protecting user privacy, and contributing to a safer and more secure cyberspace.

**REFERENCES**

1. Tib3rius. (2020, January 7). Online Book Store 1.0 - Unauthenticated Remote Code Execution [Exploit]. Exploit Database.

<https://www.exploit-db.com/exploits/47887>

1. Projectworlds. (n.d.). Online Book Store Project in PHP. GitHub Repository. <https://github.com/projectworlds32/online-book-store-project-in-php>
2. Cisco Networking Academy. (n.d.). Networking Basics. <https://www.cisco.com/c/en/us/solutions/small-business/resource-center/networking/networking-basics.html>
3. TryHackMe. (n.d.). Cybersecurity Training Platform.

<https://tryhackme.com/>

1. OWASP. (2022). OWASP Top Ten Web Application Security Risks. OWASP.
2. Kali Linux. (n.d.). Penetration Testing and Ethical Hacking Linux Distribution. <https://www.kali.org/>
3. Python Software Foundation. (n.d.). Python Programming Language. <https://www.python.org/>
4. Exploit-DB. (n.d.). Exploit Database.

<https://www.exploit-db.com/>

1. Linux Documentation Project. (n.d.). Linux Documentation.

<https://www.tldp.org/>

1. Stack Overflow. (n.d.). Community-Driven Question and Answer Site for Programmers. <https://stackoverflow.com/>