Vidyalankar Polytechnic
Wadala, Mumbai-37

Internship Report
(2024-2025)

Department of Computer Engineering

Institute

Vision

To achieve excellence in imparting technical education so as to meet the professional and societal needs.

Mission

- Developing technical skills by imparting knowledge and providing hands on experience.
- Creating an environment that nurtures ethics, leadership and team building.
- Providing industrial exposure for minimizing the gap between academics & industry.

Program

Vision:

To empower students with domain knowledge of Computer Engineering and interpersonal skills to cater to the industrial and societal needs.

Mission:

M1: Developing technical skills byexplaining the rationale behind learning.

M2: Developing interpersonal skills to serve the society in the best possible manner.

M3: Creating awareness about the ever-changing professional practices to build industrial adaptability.

Diploma Programme in Computer Engineering

I – Scheme

Programme Structure

Programme Educational Objectives (PEO)

PEO 1 Provide socially responsible, environment friendly solutions to Computer engineering related broad-based problems adapting professional ethics.

PEO 2 Adapt state-of-the-art Computer engineering broad-based technologies to work in multidisciplinary work environments.

PEO 3 Solve broad-based problems individually and as a team member communicating effectively in the world of work.

Program Outcomes (PO)

Basic and Discipline specific knowledge: Apply knowledge of basic mathematics, science and engineering fundamentals and engineering specialization to solve engineering problems.

Problem analysis: Identify and analyze well-defined engineering problems using codified standard methods.

Design/ development of solutions: Design solutions for well-defined technical problems and assist with the design of systems components or processes to meet specified needs.

Engineering Tools, Experimentation and Testing: Apply modern engineering tools and appropriate technique to conduct standard tests and measurements.

Engineering practices for society, sustainability, and environment: Apply appropriate technology in context of society, sustainability, environment, and ethical practices.

Project Management: Use engineering management principles individually, as a team member or a leader to manage projects and effectively communicate about well-defined engineering activities.
Life-long learning Ability to analyze individual needs and engage in updating in the context of technological changes.

Program Specific Outcomes (PSO)

Computer Software and Hardware Usage: Use state-of-the-art technologies for operation andapplication of computer software and hardware.

Computer Engineering Maintenance: Maintain computer engineering related software and hardware systems.

SUMMER INTERNSHIP REPORT

AT

Secure Cyber Future

Submitted in partial fulfillment of the requirement for the award of Diploma in Computer Engineering

JUNE 2024 - JULY 2024

SUBMITTED BY

Vaishnavi Parulekar-22203A0048

SUBMITTED TO

Department of Computer Engineering

VIDYALANKAR POLYTECHNIC
WADALA(E), MUMBAI-400037

ROLL NO. & NAME OF THE STUDENT: **22203A0048 -Vaishnavi Parulekar**

STARTING DATE: **03/06/2024**

COMPLETION DATE: **13/07/2024**

TOTAL WORKING DAYS: **45**

NAME OF THE INDUSTRY: **Secure Cyber Future**

ADDRESS OF THE INDUSTRY WITH PINCODE: **Mumbai , Maharashtra**

DOMAIN: **Cyber Security**

Maharashtra State Board of Technical Education, Mumbai

Certificate

This is to certify that Ms. **Vaishnavi Parulekar**

With Enrollment No**. 2205680048** has successfully completed Industrial Training (22049) in **Secure Cyber Future** from 5th June_2024 to 13th July 2024 for partial fulfillment towards completion of Diploma in Computer Engineering from **Vidyalankar Polytechnic** (0568)

External Examiner

Name of the Mentor
Prof.Pradeep Shirke

(Head of Department)
Prof. Vijay Patil

(Principal)
Prof. Ashish Ukidve

Abstract

I am thrilled to have completed my internship at Secure Cyber Future Company, where I gained invaluable hands-on experience in the field of cyber security. During my tenure, I had the opportunity to delve into the world of web security and vulnerability assessment, developing a comprehensive understanding of the importance of identifying and mitigating potential threats.

One of the highlights of my internship was working with Burp Suite, a cutting-edge application used for modern security assessment and penetration testing of web applications. Additionally, I utilized SQLmap, a powerful tool for detecting and exploiting SQL injection vulnerabilities.

Under the guidance of our Industry Mentor, I was assigned a range of tasks that challenged me to think critically and apply my knowledge in practical scenarios. These tasks not only deepened my understanding of the cyber security domain but also instilled in me the importance of effective time management, allowing me to meet deadlines and deliver high-quality results.

Throughout my internship, I maintained a detailed record of my progress, compiling a comprehensive report for each task and submitting them to the company before the assigned deadlines. This experience has not only honed my technical skills but also taught me the value of discipline, organization, and attention to detail.

ACKNOWLEDGEMENT

I would like to extend my sincere gratitude to Secure Cyber Future Company for providing me with the opportunity to intern with their esteemed organization.

I am deeply thankful to my Industry Mentor Aditya Jadhav Sir, who guided me throughout my internship and provided me with valuable insights and expertise in the field of cyber security.

Pradeep Shirke Sir, our college mentor, who has guided us with his wisdomand expertise.
I appreciate the trust placed in me to work on various tasks and projects, which helped me develop my skills and knowledge in vulnerability assessment, web security, and time management.

Thank you to the entire Secure Cyber Future Company team for their support, encouragement, and collaboration during my internship. I am proud to have been a part of a team dedicated to making the cyber world a safer place.

This internship has been a significant milestone in my academic and professional journey, and I will always cherish the learnings and experiences gained during my time atSecure Cyber Future Company

INDEX

CHAPTER EIGHT

8.0 Particulars of Practical experiences in Industry/ Organization if any in Production/ Assembly/ Testing/ Maintenance.

CHAPTER NINE

9.0 Short report/ Description of the project

CHAPTER TEN

10.0 Special/ Challenging experiences encountered during training.

11.0 REFERENCES/ BIBILIOGRAPHY

CHAPTER 1

1. Introduction

I am pleased to share my internship experience at Secure Cyber Future, a renowned Cyber Security company, where I spent 43 days from 05/06/24 to 13/07/24. During my internship my Company mentor and college mentor were auxiliary. During my time at this company, I was assigned various tasks related to Cyber Security by my Industry Mentor and his team, which helped me gain in-depth knowledge and hands-on experience in the domain. These tasks not only challenged me but also allowed me to apply theoretical concepts to real-world problems. I successfully completed each task and submitted detailed reports to the company before the designated deadlines.

Our Mission

- The company provides end-to-end Cyber Security Services.
- The mission of the company is to protect the web application from cyber-attacks and report it to the company.

Our Values

- Agility
- Honesty
- Excellence
- Trust

CHAPTER 2

1. Introduction to industry

Secure Cyber Future is a cutting-edge cybersecurity company founded in June 2017 by Aditya Jadhav. The company headquarter is in Mumbai. With a mission to identify and address IT infrastructure weaknesses before they can be exploited by malicious hackers, the company is dedicated to providing swift and effective solutions to ensure the security and integrity ofits clients' web applications

2. Services

We provide end-to-end Cyber Security Services covering the following areas:

1. Vulnerability Assessment.
2. Advanced Malware Protection.
3. Datacenter & Perimeter Security.
4. Network Risk Assessment.
5. Security-Monitoring-Services (SIEM &SOC).
6. Host & End Point Security.
7. Cloud & Virtualization Security.
8. Security Device Management. (And many More Related to Cyber Space).

CHAPTER 3

3. Types of major equipment/Instruments/ Machine used in industry with Specification and approximate cost of equipment/Instruments.

3.0. Software tools

1. Burp Suite:- A comprehensive toolkit for web application security testing. Used for vulnerability scanning, penetration testing, and security research.

2. SQLmap:- An open-source tool for automating SQL injection attacks and exploitation. Used for detecting and exploiting SQL injection vulnerabilities

3. Firefox:- A popular web browser with built-in developer tool Used for web development, testing, and debugging

4. Chrome:- A popular web browser with built-in developer tools. Used for web development, testing, and debugging

5. TempMail:- A temporary email service for receiving disposable emails. Used for testing email-based functionality or avoiding spam.

3.1 Routine Maintenance.

1. Everyweek the company used to provide us task.
2. The company even gave us the videos and articles to read
3. To submit the report before the deadline the report should include
    a) Detailed descriptions of the steps taken to perform the test.
    b) The results of your testing, including any identified vulnerabilities.
    c) Potential impacts ofthe identified issues.
    d) Recommendations for mitigation if any vulnerabilities are found.

CHAPTER 4

4.0 Manufacturing Process/ Product Development Process.

1. Research on the task given on google hacking database website.
2. Click on the link of GHDB and search the link on google
3. Click on the website of which the google shows
4. Find vulnerability on the website such as XSS, SQL, CORS, Email rate limiting and GHDB vulnerable website
5. Search for every vulnerability on this GHDB
6. Make a report for it.

4.1 Planning and control methods.

1. Time Management: Prioritize tasks based on importance and deadlines. Allocate specific time slots for each task. Use calendars, planners, or apps to stay organized Avoid multitasking and minimize distractions.

2. Note Taking: Record important information during meetings, calls, or discussions.Organize notes using headings, bullet points, or tags. Review and summarize notes regularly.

3. Tool Usage: Familiarize yourself with tools and software relevant to your work. Utilize tools for task management, communication, and collaboration. Automate repetitive tasks where possible. Stay updated with new tool features and best practices

4. Verification: Check and confirm the accuracy of information. Validate data and results through testing or review. Ensure compliance with standards and regulations.Verify user identities and access permissions

5. Reporting: Prepare regular reports on progress, results, or metrics.

CHAPTER 5

5.0 Testing Procedures.

In our company we were told to do Manual testing.

Manual testing procedure:

1. Test Planning:
   - Review software requirements and specifications
   - Identify test objectives and scope
   - Develop test cases and test scripts
   - Create test data and test environment
2. Test Execution:
   - Execute test cases and test scripts
   - Observe and record test results
   - Take screenshots and log errors
3. Test Reporting:
   - Document test results and defects found
   - Create test summary reports
   - Provide recommendations for defect fixing and improvement

.

CHAPTER 6

6.1 Trouble shooting procedures, debugging, work handled.

Troubleshooting Procedures:

1. Identify the problem: Clearly define the issue or error.
2. Gather information: Collect relevant data, logs, and screenshots.
3. Analyze the issue: Review the information and identify potential causes.
4. Develop a plan: Create a step-by-step plan to troubleshoot and resolve the issue.
5. Implement the plan: Execute the plan, testing and verifying each step.
6. Verify the fix: Confirmthe issue is resolved and the fix is effective.

Debugging:

Debug: Use manual debugging techniques to identify the root cause.

Work Handled:

1. Manual testing of software applications.
2. Identifying and reporting defects.
3. Documenting testing activities and results.

CHAPTER 7

7.0 Safety Procedures

1.XSS (Cross-Site Scripting) Security

XSS attacks inject malicious scripts into websites, compromising user data and security.

Input validation and sanitization. Output encoding

2.Password Security

Passwords are vulnerable to attacks like phishing, brute force, and password cracking.

Use strong, unique passwords. Implement password hashing and salting

3.API Security

APIs are vulnerable to attacks like unauthorized access, data breaches, and injection attacks.

Authentication and authorization. Input validation and sanitization

4.Database Security

Databases contain sensitive data, making them a prime target for attacks.

Access control and authentication. Data encryption and masking. Regular backups

5.Website Security

Websites are vulnerable to various attacks, including XSS, SQL injection, and malware.

Security measures:

Regular security updates and patches. Web application firewall (WAF)

Secure protocols (HTTPS)

CHAPTER 8

8.0 Particulars of Practical experiences in Industry/ Organization if any in Production/ Assembly/ Testing/ Maintenance.

1. Conducted manual testing of software applications to identify defects and ensure Quality. User interface testing: Checking for intuitive and user-friendly interfaces. Usability defects: Difficulties with user experience.

2.Provided feedback on software quality and usability to improve overall product. Offered constructive feedback to developers and product teams to enhance software quality and usability.

3. Documented testing activities and results to maintain accurate records. Maintain detailed records of testing activities, including: Test cases executed. Defects found and reported. Test results and outcomes.

4. Successfully identified and reported defects, leading to improved software quality. Identified defects that impacted software quality and usability. Reported defects clearly and concisely, including: Defect description. Steps to reproduce. Expected vs. actual results. Collaborated with developers to ensure defects were addressed and resolved.

CHAPTER 9

Week 1: From: 03/06/2024 **To:** 12/06/2024

1. Install the Burp Suite
2. Learned about howto use the Burp Suite
3. Learned about XSS vulnerability
4. Did Testing of XSS vulnerability for adidad.cvicte.sk website https://adidas.cvicte.sk/ by injecting the script "/><script>alert (1) </script>
5. Made the report for this adidad.cvicte.sk website

Week 2: From: 13/06/2024 To:17/06/2024

1. Downloaded SQL Map and installed the latest version of Python.
2. Learned how to use SQL Map with the help of the commands
3. Did a penetration testing task on the website, sistemas.pedagogica.edu.sv using SQL Map and Burp Suite
4. Learned about CORS (Cross-Origin Resource Sharing) vulnerability

Week 3: From:18/06/2024 To: 22/06/2024

1. Received task 3 regarding CORS vulnerability
2. To test the website [demandbase.com](https://www.demandbase.com) with a focus on its origin domain
3. Used Curl command.
    - curl https://www.demandbase.com /H "Origin: https://api.demandbase.com" -I
4. Learned about email Rate limiting

Week 4: From: 25/06/2024 To: 28/06/2024

1. Learned about email rate limiting from You tube
2. Received the task 4 of email rate limiting. To verify the "Forgot Password" functionality of
   invoicer.ai.
3. Made the Report
4. Learnt about Google Dorks -Google hacking database.

Week 5: From 01/07/2024 **To** 4/07/2024

1. Learnt about Google Dorks
2. Received task 5 regarding Google dorks on google hacking database.
   -The task was to find 5 vulnerable websites using google dorks.(https://www.exploit-db.com/google-hacking-database).
3. Made the report

Week 6: From 10/07/2024 To 13/07/2024

1. Received the task 6
2. In this task I had to find all the 5 vulnerabilities on (https://www.exploit-db.com/google-hacking-database). They were
   XSS
   SQL
   CORS vulnerability
   Email rate limiting
   Google Dorks vulnerable sites
3. Searched for these vulnerabilities in the provided website
4. Made the Report

CHAPTER 10

10.0 Special/ Challenging experiences encountered during training.

We did our internship at SECURE CYBER FUTURE. It was overall a great experience, but where there is experience, there is also challenges coming along. So here are some of the challenges that we faced during our internship.

1) The challenging part of my internship was to submit the report in the given time that is before the deadline

2) For me to use the Burp Suite in the professional way was difficult in the initial days as it was completely new application to us

3) The google hacking database was used to find the vulnerabilities in the given links it was difficult to visit each and every website in the google hacking database

CHAPTER 11

11.0 References

• SANS Information Security White Paper

[1] https://www.sans.org/white-papers/

• Port Swigger

[2] https://portswigger.net/

• CERT Division at Carnegie Mellon University

[3] https://cert.europa.eu/publications

• European Union Agency for Cybersecurity (ENISA). Cloud Security Guidelines. ENISA, 2023.

[4] https://www.enisa.europa.eu/publications/cloud-security-%20guidelines

• The Hacker News

[5] https://www.hackerone.com/