Xavier Institute of Engineering
A SISTER INSTITUTE OF ST XAVIER'S COLLEGE, MUMBAI

XAVIER INSTITUTE OF ENGINEERING
Mahim Causeway, Mahim, Mumbai – 400 016 ☎24455937 / 24460359 / 24451961
Fax: +91(22) 24462267 Email : office@xavier.ac.in
Riya Kamble: +91 8355852392 / 202103028.riyakpp@student.xavier.ac.in
Bhanavi Pandey: +91 93264 12652 / 202204042.bhanavipkm@student.xavier.ac.in

Value Added Course On CyberSentinel : ISO Certification on Vulnerability Assessment and Penetration Testing

Event Coordinator(s):

1. **Dr. Vaishali Gaikwad**
2. **Prof. Stella J.**

Date: December 27th to December 31st 2024

Time: 9:00 AM to 4:00 PM

Location: Computer Centre (CC Lab), Xavier Institute of Engineering, Mumbai.

Platform: Offline

No. of participants: 10

Day 1: 27th December 2024

On 27th December 2024, Allyn Girls organized an **Value Added course on CyberSentinel : ISO Certification on Vulnerability Assessment and Penetration Testing**. The session was hosted by **Dr. Vaishali Gaikwad** and **Prof. Stella J.** and featured three distinguished speakers:

- **Dr. Rohit Gautam**, CISO, Hacktify
- **Dr. Shifa Cyclewala**, CEO, Hacktify
- **Uddesh Vaidya ,** Security Analyst, Hacktify

The lecture offered a **practical and theoretical blend**, covering the following key areas:

1. **Cybersecurity Basics:**
   - Definition and importance of cybersecurity.
   - Common threats like phishing, greed-based scams, and oversharing information.
2. **Reconnaissance and Tools:**
   - Introduction to **Reconnaissance** for gathering target information.
   - Tools such as:
     - **Harvester:** For collecting email, domain, and other public information.
     - **Subfinder:** For finding subdomains.
     - **Burp Suite:** For testing web application vulnerabilities.
     - **Nmap:** For network scanning and identifying open ports.
3. **Bug Bounty Practices:**
   - Learning methods for identifying and reporting vulnerabilities in live systems.
4. **OWASP Top 10 Risks:**
   - Including Insecure Design, Security Misconfigurations, and SSRF (Server-Side Request Forgery).
5. **Practical Insights on VAPT:**
   - Hands-on exercises in Vulnerability Assessment and Penetration Testing.

Day 2: 28th December 2024

Session Overview

- **Instructor:** Uddesh Vaidya
- **Focus Areas:** Web Application Attack Techniques (Theory and Practical)
- **Key Highlights:**

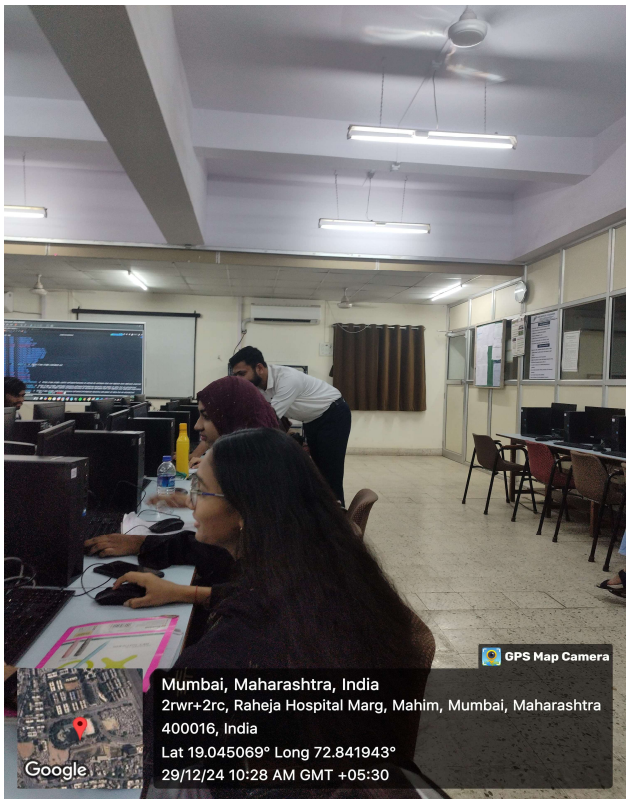
  - Uddesh Vaidya provided practical demonstrations along with theoretical explanations.
  - Individual attention was given, and all students' doubts were cleared in detail.

- **Topics Covered**

1. **Web Application Attacks:**
   - **Cross-Site Scripting (XSS):**
     - Types:
       - Stored XSS
       - Reflected XSS
       - Blind XS
     - Example Payloads:
       - `<script>alert(1)</script>`
       - `document.cookie`
   - **HTML Injection & SQL Injection:**
     - SQL Attack Example:
       - `admin' OR '1' = '1`
     - Structured Query Language basics discussed.
2. **Authentication Vulnerabilities:**
   - **Broken Authentication:**
     - Prevention:
       - Implementing secure logout mechanisms.
     - Examples of bypass techniques:
       - OTP bypass
       - Login bypass
3. **Content Security Policy (CSP):**
   - CSP introduction for mitigating vulnerabilities.
4. **Cookie Manipulation:**
   - Example:
     - Changing `user=user` to `user=admin`
5. **HTTP Response Status Codes:**
   - Categories discussed:
     - Informational (100–199)
     - Successful (200–299)
     - Redirection (300–399)
     - Client Error (400–499)
     - Server Error (500–599)
6. **Local File Inclusion (LFI):**
   - Exploit examples:
     - Accessing sensitive files like passwords.
7. **Denial of Service (DoS) Attack:**
   - Practical command examples:
     - Navigating to Go file directory: `cd doser.go`
     - Building the Go file: `go build doser.go`
8. **SQL Injection Testing :**
     - Exploiting login forms.

Practical Activities

- Practicals covered theoretical aspects hands-on:
  - **XSS Demonstration:**
    - Running payloads in a controlled environment.
  - **SQL Injection Testing:**
    - Exploiting login forms.
  - **Cookie Poisoning:**
    - Observing and modifying cookies.
  - **DoS Attack Simulation:**
    - Building and running scripts to understand attack effects



Day 3: 29th December:

1. **CORS Attack (Cross-Origin Resource Sharing):**
   - Exploiting misconfigured CORS policies to access sensitive data from another domain.
   - **Practical Execution:**
     - Using Burp Suite to intercept and manipulate requests.
     - Observing how unauthorized data can be accessed.

2. **IDOR (Insecure Direct Object Reference):**
   - A vulnerability where attackers directly access unauthorized objects by modifying references.
   - Example:
     - Changing URL parameters to access someone else's data.
     - URL: `example.com/profile?id=101` → `example.com/profile?id=102`
   - **Mitigation:**
     - Implement proper access control and validation checks.

3. **Price Tampering:**
   - Exploiting vulnerabilities in e-commerce platforms to manipulate product prices.
   - **Practical Execution:**
     - Using developer tools or Burp Suite to modify form data (e.g., reducing price values before submission).
   - **Mitigation:**
     - Server-side validation of prices and quantities.

4.Host Header Injection:

- Injecting malicious host headers to trick servers into serving unintended responses.
- **Example:**
  - Injecting `Host: malicious-site.com` in HTTP headers.
- **Mitigation:**
  - Validate host headers on the server side.

5. **HTML Injection:**
   - Injecting unauthorized HTML elements into web pages to manipulate content.
   - Practical examples included adding forms or scripts.

Day 4: 30th December

1. **CSI (Client-Side Injection):**
   - Overview of how attackers exploit vulnerabilities on the client side to manipulate or compromise application behavior.
   - Practical examples included modifying client-side scripts or parameters to bypass application logic.

2. **CSRF (Cross-Site Request Forgery):**
   - **CSRF Vulnerability with No Defenses:**
     - Demonstrated how attackers can exploit the absence of CSRF protections to perform unauthorized actions on behalf of authenticated users.
     - Example: Exploiting forms or requests that lack CSRF tokens.
   - **CSRF Vulnerability with Weak Defenses:**
     - Highlighted vulnerabilities where token-based defenses are implemented incorrectly or bypassable.
     - Discussed common mistakes in CSRF protection mechanisms and their consequence.

     - Using payloads to demonstrate how RCE vulnerabilities can compromise server security.
     - Example: Injecting malicious code into vulnerable endpoints to gain server access.

RCE (Remote Code Execution):

- Explained how attackers exploit vulnerabilities to execute arbitrary code on a target server.
- **Practical Demonstration:**
  - Using payloads to demonstrate how RCE vulnerabilities can compromise server security.
  - Example: Injecting malicious code into vulnerable endpoints to gain server access.
- **Mitigation Strategies:**
  - Input validation and sanitization.
  - Restricting user access to sensitive execution environments.

CE (RCE (Remote Code Execution):

- Explained how attackers exploit vulnerabilities to execute arbitrary code on a target server.
- **Practical Demonstration:**
  - Using payloads to demonstrate how RCE vulnerabilities can compromise server security.
  - Example: Injecting malicious code into vulnerable endpoints to gain server access.
- **Mitigation Strategies:**
  - Input validation and sanitization.
  - Restricting user access to sensitive execution environments.

Code Execution):

- Explained how attackers exploit vulnerabilities to execute arbitrary code on a target server.
- **Practical Demonstration:**
  - Using payloads to demonstrate how RCE vulnerabilities can compromise server security.
  - Example: Injecting malicious code into vulnerable endpoints to gain server access.
- **Mitigation Strategies:**
  - Input validation and sanitization.
  - Restricting user access to sensitive execution environments.

Day 5: 31st December

Session Overview

- **Instructor:** Uddesh Vaidya
- **Focus:** Final Practical Exam, MCQ Assessment, and Certificate Ceremony

Exam Details

1. **Practical Exam:**
    - Students were tasked to find and report multiple vulnerabilities on a provided website.
    - Objective: Test the practical application of vulnerabilities such as XSS, SQL Injection, CSRF, RCE, IDOR, and others.
    - Reports were evaluated based on accuracy and detail.
2. **MCQ Exam:**
    - Covered theoretical and practical concepts learned over the past five days.
    - Topics included: Vulnerabilities, attack techniques, and mitigation strategies.

Certificate Ceremony

- After the exam, a **Certificate Ceremony** was held to recognize the efforts of all participants and the contributions of the instructor.
- **Highlights of the Ceremony:**
    - **Special Acknowledgment:**
        - Our college principal, **Dr. Y. D. Venkatesh Sir**, presented Uddesh Vaidya with a certificate of appreciation and a token of gratitude in the form of a cheque.
    - **Student Certificates:**
        - Certificates were distributed to all participating students, acknowledging their successful completion of the course.
    - The ceremony marked the culmination of an enriching and rewarding five-day learning experience.

Overall Feedback

1. **Knowledge and Skills Gained:**
    - Students gained in-depth knowledge of various vulnerabilities and learned ethical hacking techniques.
    - Practical and theoretical understanding of cybersecurity concepts was significantly enhanced.
2. **Mentorship:**
    - Uddesh Vaidya provided exceptional guidance throughout the course, resolving doubts and ensuring individual attention to each student.
3. **Confidence Building:**
    - The course equipped students with the confidence to identify and exploit vulnerabilities responsibly.
    - Real-world practice prepared students for challenges in the cybersecurity field.

The CyberSentinel Course was a well-structured and impactful program that combined learning, practice, and recognition. The certificate ceremony, graced by **Dr. Y. D. Venkatesh Sir**, celebrated the achievements of both the instructor and the students. The program not only enhanced technical skills but also fostered a deep interest in ethical hacking and cybersecurity.

Special thanks to the Allyn Girls for arranging the "CyberSentinel" course.
Your effort and dedication in organizing this course are deeply appreciated. Thank you for making it a valuable and enriching experience for all participants!