COURSE CODE: PRAC3301 Section: BSIT

COURSE TITLE: OJT/PRACTICUM 1

TERM: 1st Semester, SY 2024-2025

PROFESSOR: MR. VINCENT CARLO T. GARADOS

DATE: Nov, 16, 2024

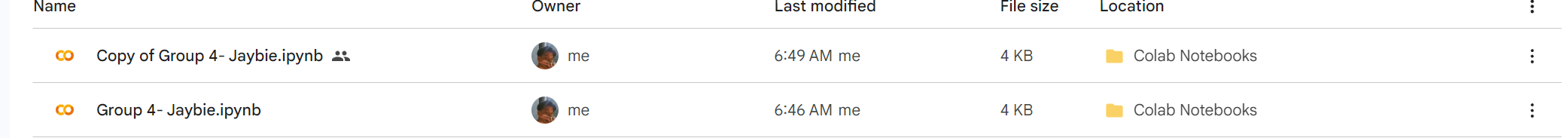
NAME OF STUDENT: Jaybie E. Sosmeña

SPEAKERS NAME: Sir. Marc Anthony Tonido

TITLE: Fundamentals of Web App Security

**OJT NARRATIVE REPORT**

1. SCREENSHOT OF DUTY



1. NARRATIVE REPORT

I recently attended a webinar titled "Fundamentals of Web Application Security," which provided an insightful overview of the principles, challenges, and best practices involved in securing web applications. As someone eager to deepen my understanding of cybersecurity, this session was particularly enlightening, as it covered key aspects of web app security in a clear and structured manner.The webinar began with an **introduction to web application security**, explaining it as the practice of protecting websites and online services from unauthorized access, attacks, and breaches. The presenter highlighted the significance of ensuring the **Confidentiality, Integrity, and Availability (CIA)** of web applications and data. What stood out to me was the emphasis on the widespread usage of web applications across industries, making them prime targets for attackers. The session underscored the business impacts of poor security, such as financial losses, reputational damage, and legal consequences.The next segment delved into the **core security services for web applications**, focusing on three critical areas **Data Protection:** The importance of safeguarding sensitive information, such as user credentials and financial data, from unauthorized access was emphasized. **Access Control:** Ensuring only authorized users have access to specific parts of an application or can perform certain actions was presented as a foundational principle. **Secure Communication:** The role of encryption protocols like HTTPS in protecting data as it travels over the internet was explained in detail. A significant portion of the webinar explored **common threats to web applications**, many of which I had heard about but had not fully understood. These included:**SQL Injection (SQLi):** A technique where attackers inject malicious SQL queries to manipulate databases, leading to data theft or deletion.**Cross-Site Scripting (XSS):** Malicious scripts are injected into web pages to steal user data or hijack sessions.**Cross-Site Request Forgery (CSRF):** This threat tricks users into executing unwanted actions while authenticated on a web application.**Insecure Deserialization:** A lesser-known but critical vulnerability, where serialized data is exploited to execute malicious code.**Broken Authentication and Session Management:** Weak or poorly implemented authentication systems can lead to account takeovers or unauthorized access. I found the explanations for these threats particularly eye-opening, as they demonstrated how attackers exploit common vulnerabilities in web applications.The final part of the session focused on the **OWASP Top 10 Vulnerabilities**, a widely recognized framework for identifying critical security risks in web applications. OWASP, or the Open Web Application Security Project, is a non-profit organization that provides valuable resources for improving web security. The presenter explained several key vulnerabilities from the list, such as **Injection Attacks:** Including SQL and OS Command Injection.**Broken Authentication:** Risks from weak or compromised credentials.**Sensitive Data Exposure:** Insecure handling of personal or financial information.**Cross-Site Scripting (XSS):** The dangers of script injection vulnerabilities.**Security Misconfiguration:** Problems arising from default passwords or incomplete updates.The session also introduced tools and resources available on the OWASP website, which I plan to explore further to deepen my understanding.Overall, this webinar provided a comprehensive overview of web application security and its importance in today’s digital landscape. It highlighted not only the technical aspects of protecting web applications but also the broader implications of neglecting security. This session has motivated me to learn more about identifying and mitigating web app vulnerabilities, especially those outlined in the OWASP Top 10. I am grateful for this learning opportunity, which has enhanced my awareness and inspired me to prioritize secure practices in any future web development projects.