# Module 10: Investigating Web Attacks Report

Lara Alofi

2110886

Y

Computer Hacking Forensic Investigator (CHFI)

Lab Session Identifiers

1. <https://labclient.labondemand.com/LabClient/993f8857-e6ac-4714-b472-25e638b74c48>

Username on EC-Council System

1. 2110886@uj.edu.sa

A white screen with black text

Description automatically generated

**Lab 01:**

This lab focuses on analyzing log files from Apache, IIS servers, and ModSecurity to identify and investigate web application attacks using Splunk Enterprise. Key attacks examined include Cross-Site Scripting (XSS), SQL Injection, Directory Traversal, Command Injection, XML External Entity (XXE), and Brute-Force Attacks. Participants use filters to uncover malicious activities, analyze attack patterns (timestamps, IPs, and HTTP responses), and gain insights into system vulnerabilities to enhance forensic investigation and improve security.

**Lab 02:**

This lab focuses on using Python scripts to analyze Apache server logs for web application attacks, including SQL Injection, Command Injection, Directory Traversal, and Cross-Site Scripting (XSS). Participants write and execute scripts to parse logs, identify malicious patterns, and gather evidence of attacks such as unauthorized database access, injected shell commands, file traversal, and embedded scripts. The lab demonstrates Python's effectiveness in automating forensic analysis and detecting vulnerabilities.