PennState
College of Information
Sciences and Technology

Lab Assignment Report

COURSE:	**IST 894**
ASSIGNMENT:	**LAB ASSIGNMENT REPORT 4**
SUBMITTED BY:	**BRANTLEY PRICE**
DUE DATE:	**JUNE 29TH, 2025**
INSTRUCTOR:	**DR. BARTOLACCI**

Contents

General Context

This lab assignment covered a cyber range exercise, “Common Attack Types,” and a course, Recon and Footprinting. This exercise and course, although not directly correlated, provide complementary learning to help the student identify, analyze, and execute the kinds of techniques they may see adversaries use to compromise systems they are entrusted to protect. There is practical information to be learned here, and although this lab was more focused on the offensive side of things, this perspective equips the student with vital information to prepare for these attack vectors.

In the Recon and Footprinting course, the student was introduced to a variety of open-source intelligence (OSINT) and enumeration tools. For the uninitiated, OSINT is defined as the act of gathering and analyzing publicly available data for intelligence purposes (Baker, 2025). Some of the tools identified were WHOIS, Netcraft, Google Hacking, Maltego, and dnsrecon. Together, these tools were demonstrated to be highly effective in gathering information about domains, public infrastructure, and system configurations. At one point, the instructor was able to pull username and password information from a website from a simple Google search.

The cyber range lab on Common Attack Types took some of the same types of information but allowed the student solid, albeit brief, hands-on experience to transition from theory to practical action. Using a simulated vulnerable web app, the lab demonstrated common web app vulnerabilities like HTML injection, SQL injection, and OS command injection. SQL Injections are still responsible for some of the most common vulnerabilities, accounting for 1,727 of the 16,950 (>10%) vulnerabilities and exploits in MITRE’s CVE database in the first six full months of 2025 (MITRE, 2025). Seeing the attacks in action provided the student with important context that they would not otherwise have.

Technical Context

The Recon and Footprinting course provided student with the opportunity to experience a structured course that covered both passive and active OSINT. Tools used during this course covered several different facets of OSINT and DNS enumeration. WHOIS and NSLookup, for example, provide domain registration data that can help an attacker identify key administrative and technical contact information. Hacking techniques were explored by using a method called “Google Dorking” within the Google Hacking Database (GHDB). Dorking is a technique that uses advanced search operators to uncover information on the internet that may not be readily available through a normal search query (Wright, 2023). Maltego was also used to help visualize the relationship between people, domains, and emails. Maltego is an extremely powerful tool that can extract data from various sources, including social media platforms, public records, email addresses, and websites (Vaishnavi, 2024). All of the information gathered by these tools is publicly available, provided you know the correct search parameters and tools to use.

The Common Attack Types cyber range exercise was hands-on and provided the student with the chance to apply some of the most common offensive techniques against a vulnerable web app. Three major vulnerabilities were covered: stored and reflected HTML injections, OS command injections, and SQL injections. The student was able to interact with server-side components to simulate an environment wherein they had already gained access to the system. The attacks were effective in simulating the vulnerabilities when the requisite misconfigurations exist. The student was able to see the success of these vulnerabilities just as they would in a real-world environment, e.g., delayed responses in blind HTML injections.

The cyber range exercise and the course work together to provide a strong simulation of adversarial actions, as well as a course that showcases some pretty startling OSINT capabilities, much of

which is available for the use of the general public. Both are highly relevant to modern penetration testing and red-teaming and can help the student form a technical foundational understanding of advanced tactics, techniques, and procedures (TTPs) that adversaries use daily to attack and exploit vulnerabilities on their systems.

Screenshots

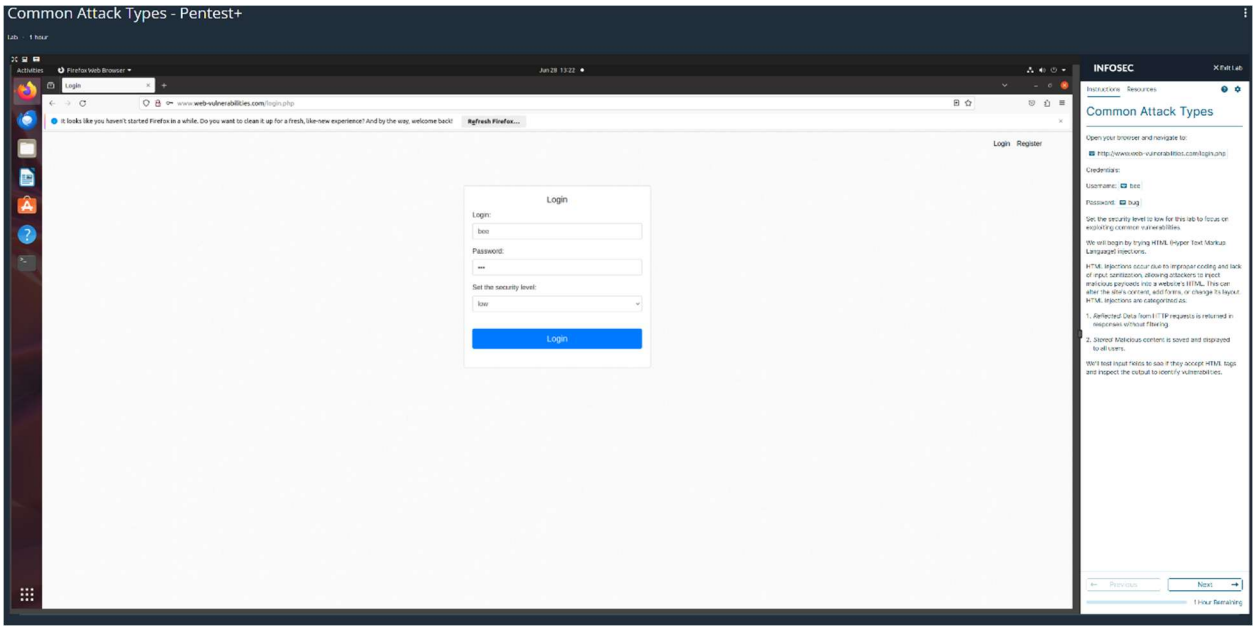

Figure 1: Logging In

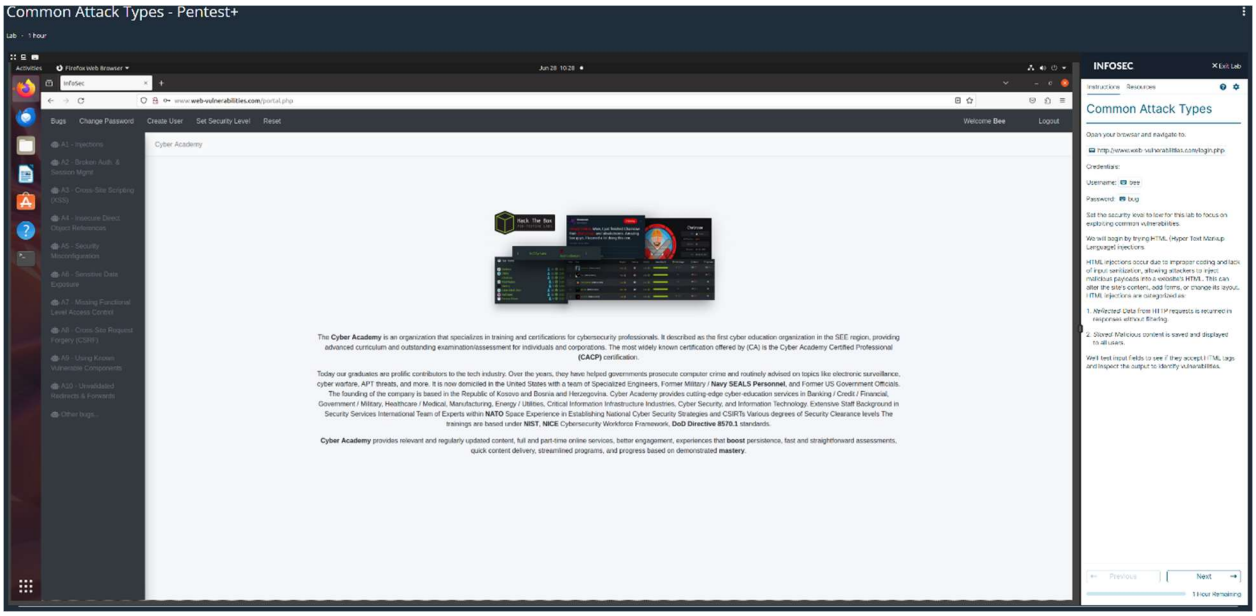

Figure 2: Logged into the App

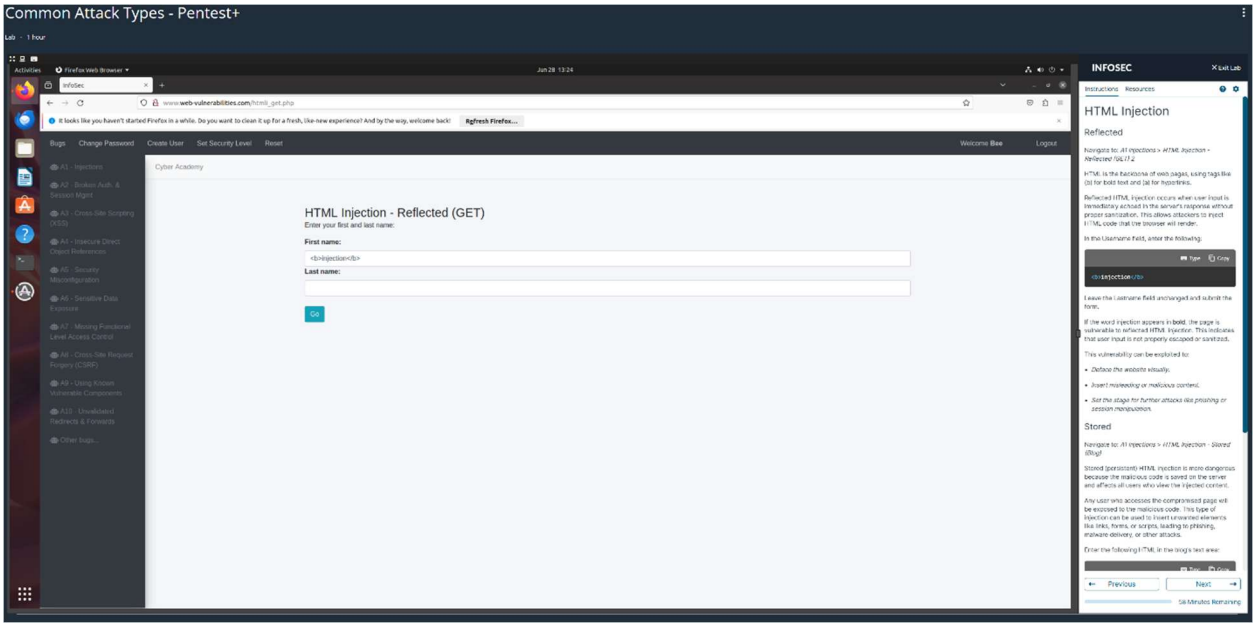

Figure 3: HTML Injection Input

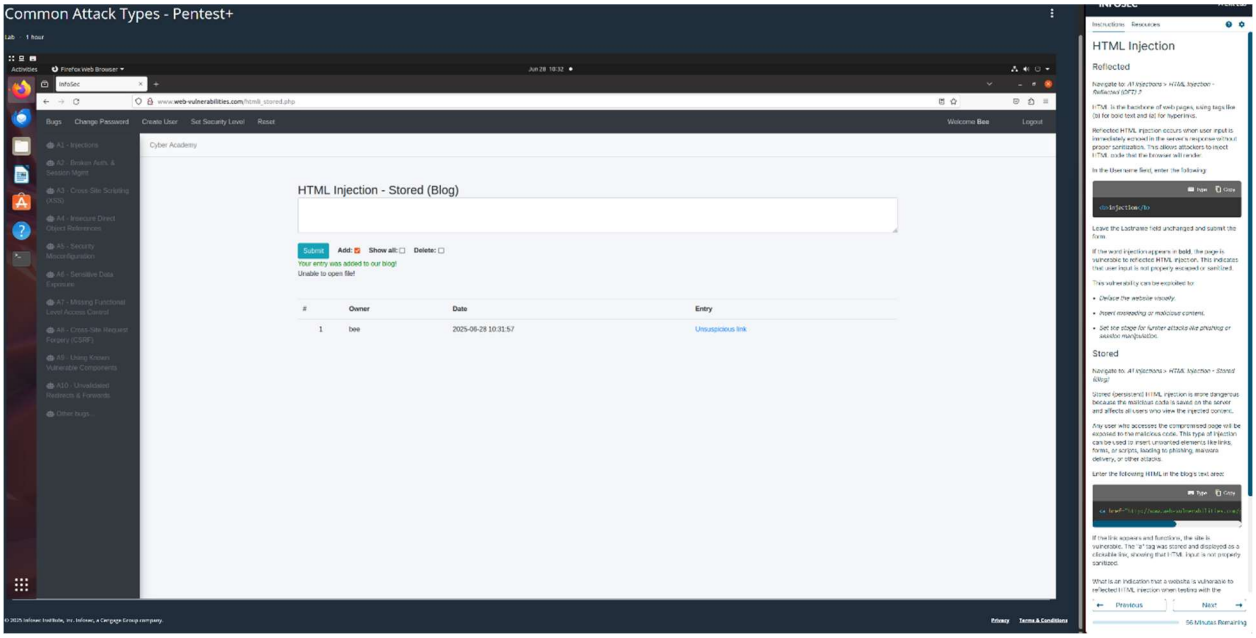

Figure 4: HTML Injection

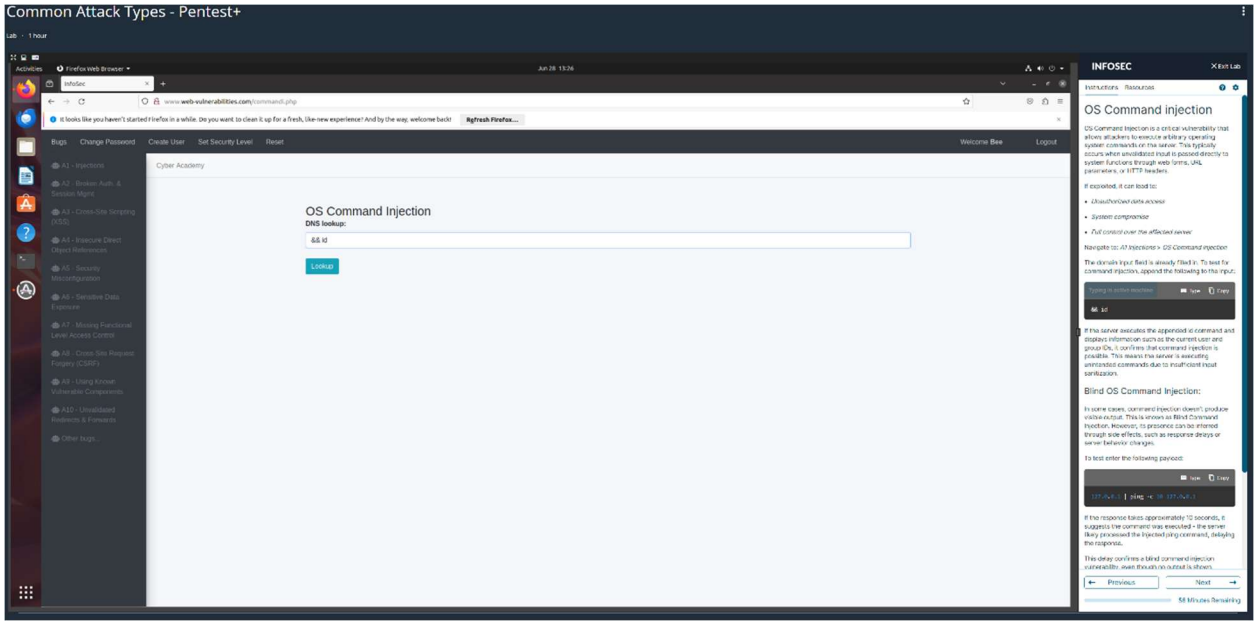

Figure 5: OS Command Injection Input

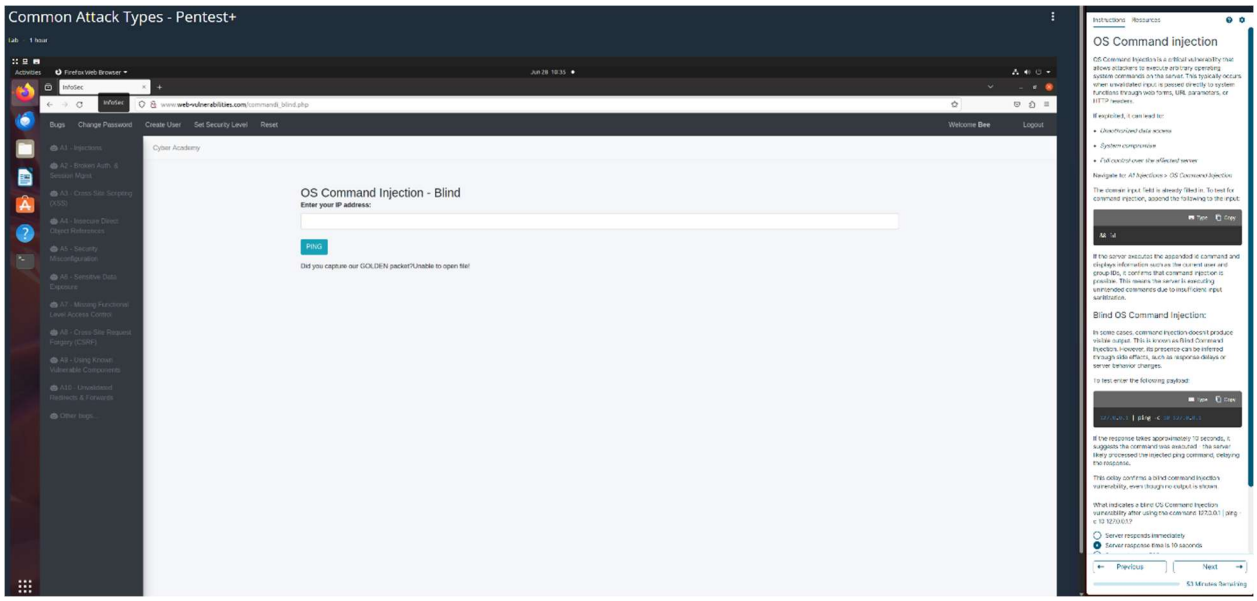

Figure 6: OS Command Injection

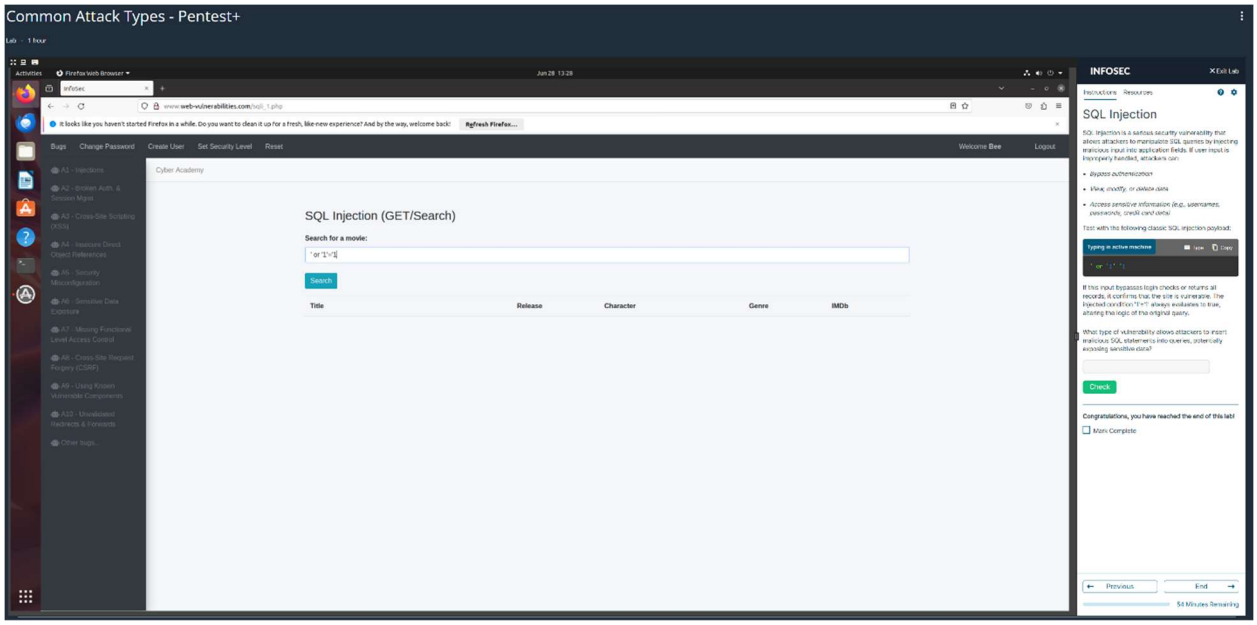

Figure 7: SQL Injection Input

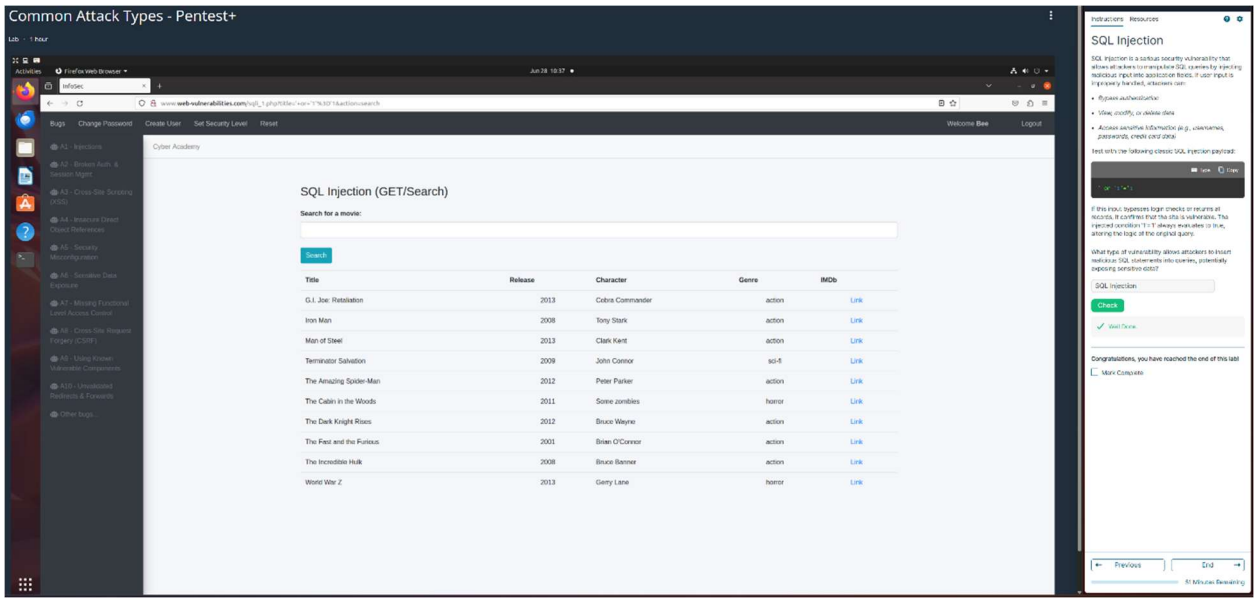

Figure 8: SQL Injection

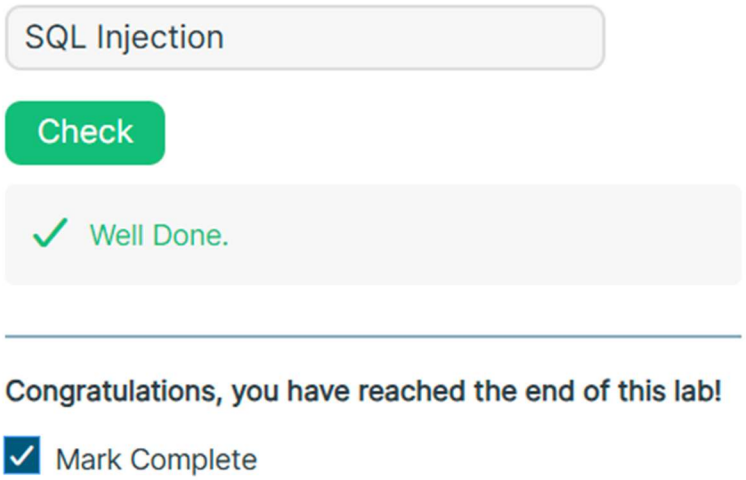

Figure 9: Cyber Range Complete

Figure 10: Recon and Footprinting Completion Certificate

References

Baker, K. (2025, January 17). *What is OSINT Open Source Intelligence?* Crowdstrike. Retrieved June 28, 2025, from https://www.crowdstrike.com/en-us/cybersecurity-101/threat-intelligence/open-source-intelligence-osint/

MITRE. (2025). *Common Vulnerabilities and Exposures*. CVE.org. Retrieved June 28, 2025, from https://www.cve.org

Vaishnavi. (2024, December 23). What makes Maltego the best tool for cyber intelligence | Overview, features, and why ethical hackers should use it. *WebAsha Technologies*. https://www.webasha.com/blog/what-makes-maltego-the-best-tool-for-cyber-intelligence-overview-features-and-why-ethical-hackers-should-use-it

Wright, M. (2023, December 20). *What is Google Dorking/Hacking | Techniques & Examples | Imperva*. Learning Center. https://www.imperva.com/learn/application-security/google-dorking-hacking/