

# Network and System Security – Reflection – Week 05

## Key Learning Outcomes

### Automated Vulnerability Scanning Fundamentals

Wapiti demonstrated how automated web application scanning proactively identifies vulnerabilities, helping secure applications before attackers can exploit weaknesses.

### Critical Web Vulnerabilities

Common web vulnerabilities (XSS, SQL injection, command injection, file inclusion, SSRF) highlighted how attackers exploit these flaws, providing context for real-world breaches

### Hands-On Technical Skills

- Working with Wapiti developed several practical abilities
- Installing and configuring security tools via command line (pip install wapiti3)
- Conducting structured vulnerability scans with appropriate parameters

### The Critical Importance of Ethics

Ethical and legal considerations are essential in cybersecurity, emphasising that unauthorised scanning is illegal, and practicing on sanctioned, purpose-built environments is the responsible way to develop skills.

### Scan Result Analysis and Prioritisation

Automated vulnerability scanners provide data that must be interpreted by humans, highlighting the need to assess severity, validate findings, and understand exploitability

### Best Practices

- Always obtain written authorisation before conducting security testing
- Respect scope boundaries and agreed-upon testing parameters
- Practice defence in
- Conduct continuous assessment: Security is ongoing, not one-time
- Report responsibly: Disclose vulnerabilities to affected parties before public announcement

### Moving Forward

The workshop developed practical skills in vulnerability assessment, secure coding, and interpreting security reports, while highlighting ethical responsibility, which are essential for effective cybersecurity practice.