University of Dhaka
Dept. of Computer Science and Engineering
Professional Masters in Information and Cyber Security (PMICS) Program

---

CSE 808 - Information Infrastructure Protection

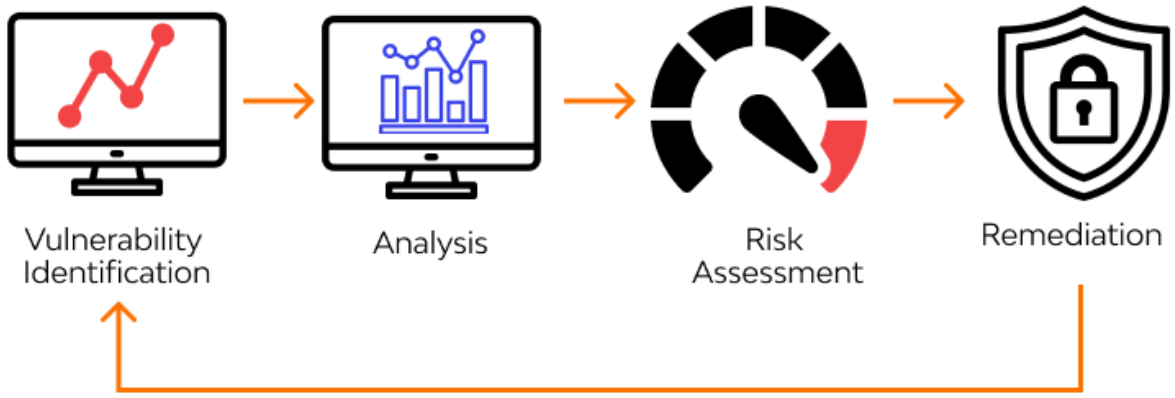
"Vulnerability Assessment & Vulnerability Scanning Tools"

Lab Class 4 – Manual

Conducted by: Md. Shakhawat Hossain Robin

What is vulnerability assessment?

- Vulnerability assessment in cybersecurity refers to the process of identifying risks and vulnerabilities in computer networks, systems, hardware, applications, and other parts of the IT ecosystem.
- A vulnerability assessment is the process of defining, identifying, classifying and prioritizing vulnerabilities in computer systems, applications and network infrastructures.



Types of vulnerability assessments

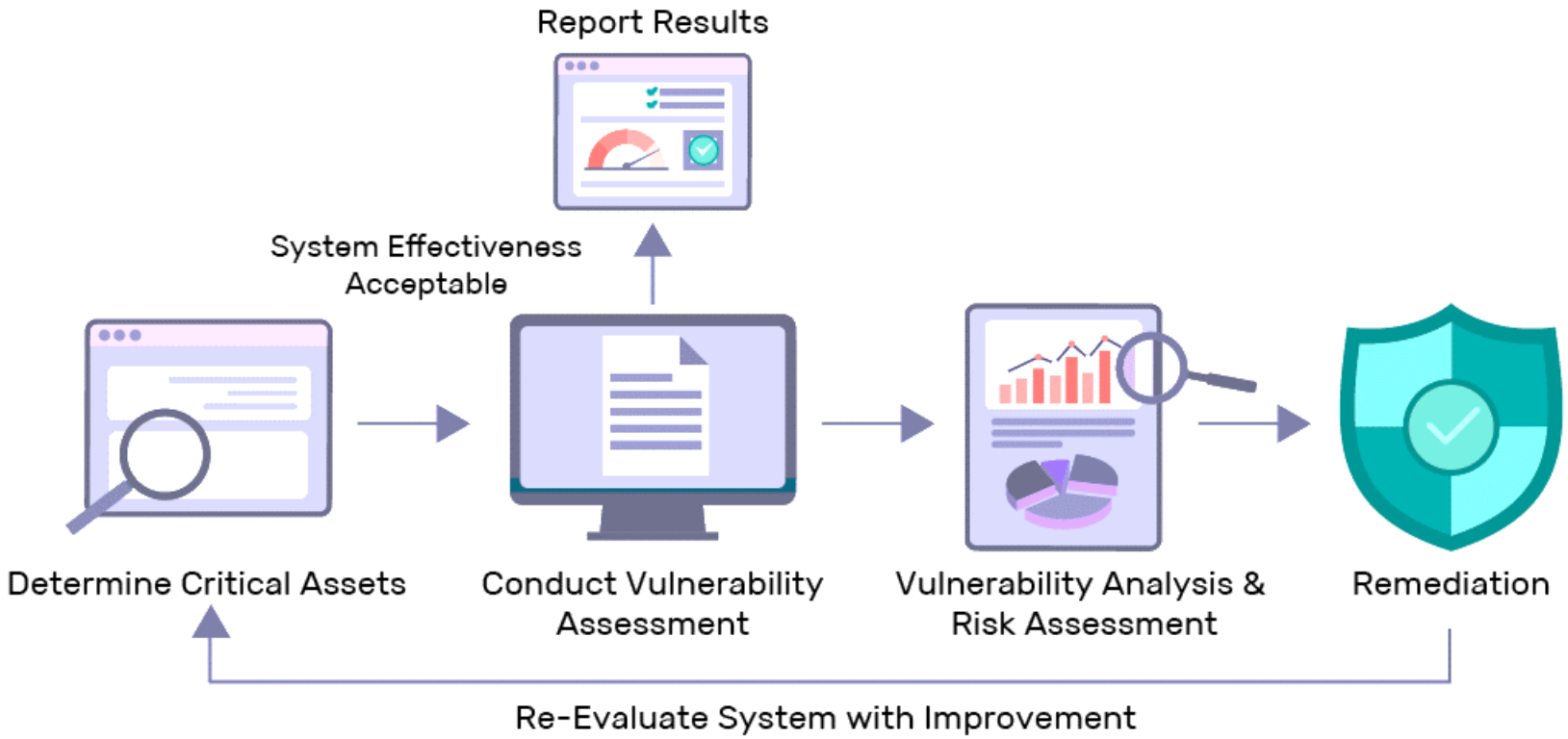
There are several types of vulnerability assessments including:

- **Host assessment –** The assessment of critical servers, which may be vulnerable to attacks if not adequately tested or not generated from a tested machine image.
- **Network and wireless assessment –** The assessment of policies and practices to prevent unauthorized access to private or public networks and network-accessible resources.
- **Database assessment –** The assessment of databases or big data systems for vulnerabilities and misconfigurations, identifying rogue databases or insecure dev/test environments, and classifying sensitive data across an organization's infrastructure.
- **Application based –** The identifying of security vulnerabilities in web applications and their source code by automated scans on the front-end or static/dynamic analysis of source code.

Types of vulnerability assessments.

- **API-Based Vulnerability Assessment** – API vulnerability assessment is conducted to identify and mitigate potential security risks in APIs. This process identifies vulnerabilities and weaknesses in the API's design, implementation, and deployment.
- **Physical Vulnerability Assessment** – A physical vulnerability assessment identifies vulnerabilities in physical security measures, such as locks, surveillance cameras, and access control systems. These assessments typically involve physical inspections of the facility and its security measures.
- **Cloud-Based Vulnerability Assessment** – A cloud-based vulnerability assessment identifies vulnerabilities in cloud infrastructure and services, such as Amazon Web Services (AWS) and Microsoft Azure.
- **Social Engineering Vulnerability Assessment** – A social engineering vulnerability assessment identifies vulnerabilities in human behavior, such as phishing attacks and other social engineering techniques.

Vulnerability Assessment Process



Vulnerability Assessment vs. Penetration Testing

Vulnerability Assessment:

- **Scanning:** Automated tools are used to scan the target system for known vulnerabilities.
- **Identifying Weaknesses:** The assessment identifies security weaknesses and provides a prioritized list of vulnerabilities.
- **No Exploitation:** Vulnerability assessment does not involve actively exploiting vulnerabilities; it focuses on identification and reporting.
- **Remediation Recommendations:** The assessment results typically include recommendations for remediation and mitigation.

Penetration Testing:

- **Active Exploitation:** Penetration testing involves actively attempting to exploit vulnerabilities to assess their impact.
- **Realistic Scenarios:** Testers simulate real-world attack scenarios to identify potential entry points and the extent of damage that could occur.
- **Manual and Automated Testing:** Both manual techniques and automated tools are used to identify and exploit vulnerabilities.
- **Limited Scope:** Penetration testing usually focuses on specific target systems or components.
- **Actionable Insights:** Penetration testing provides actionable insights into the effectiveness of security measures and the potential impact of successful attacks

Vulnerability Assessment (Scanning)

Authenticated Scan

Authenticated scans are those that use valid credentials to log in to the target system or network and perform a deeper analysis of its configuration, patches, and software.

Unauthenticated scans?

Unauthenticated scans are those that do not use any credentials and rely on external information and probes to detect vulnerabilities.

Vulnerability Assessment Methods

Authenticated Scan

Authenticated scans are those that use valid credentials to log in to the target system or network and perform a deeper analysis of its configuration, patches, and software.

Unauthenticated scans?

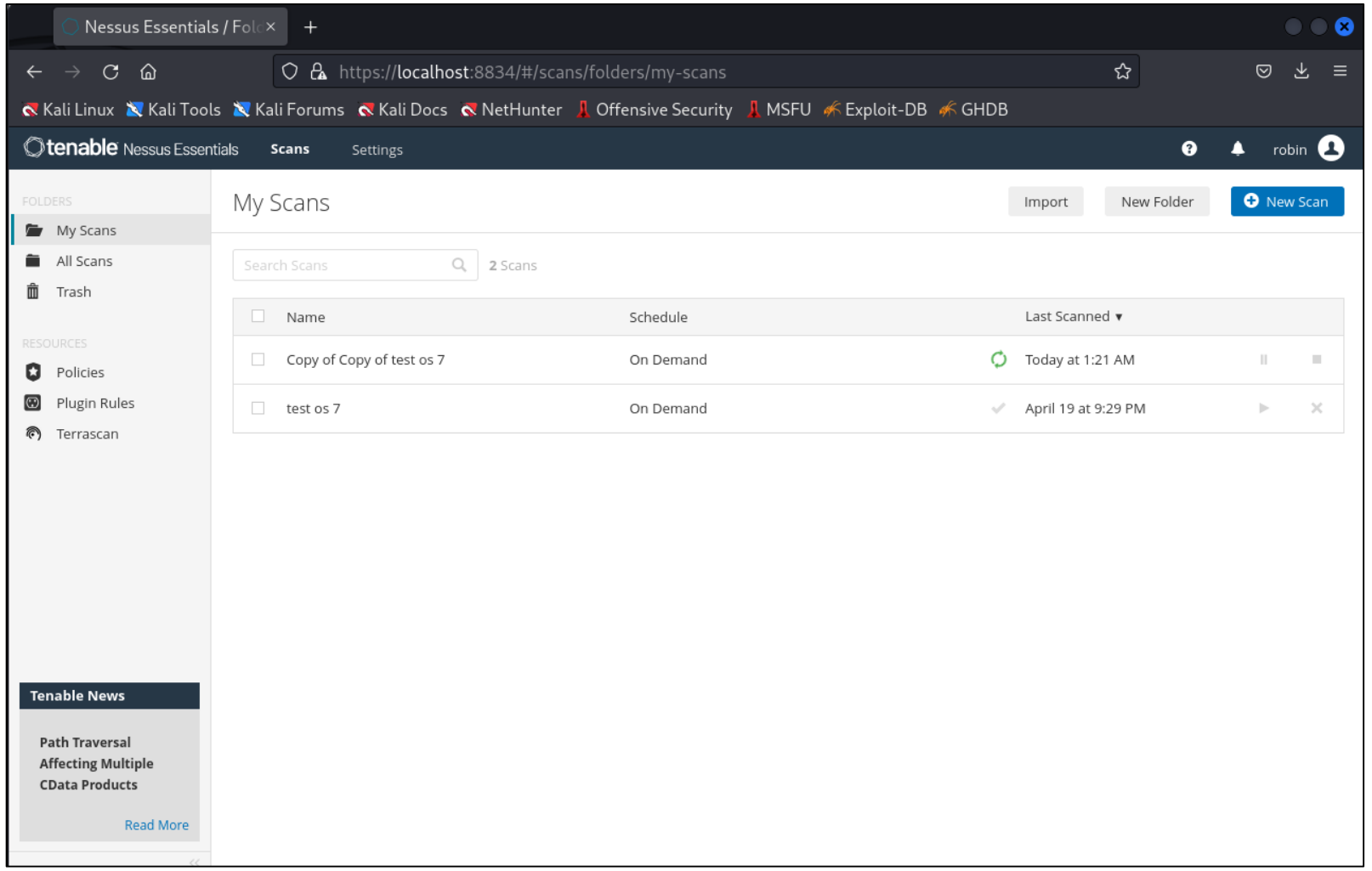
Unauthenticated scans are those that do not use any credentials and rely on external information and probes to detect vulnerabilities.

Penetration Testing Methods

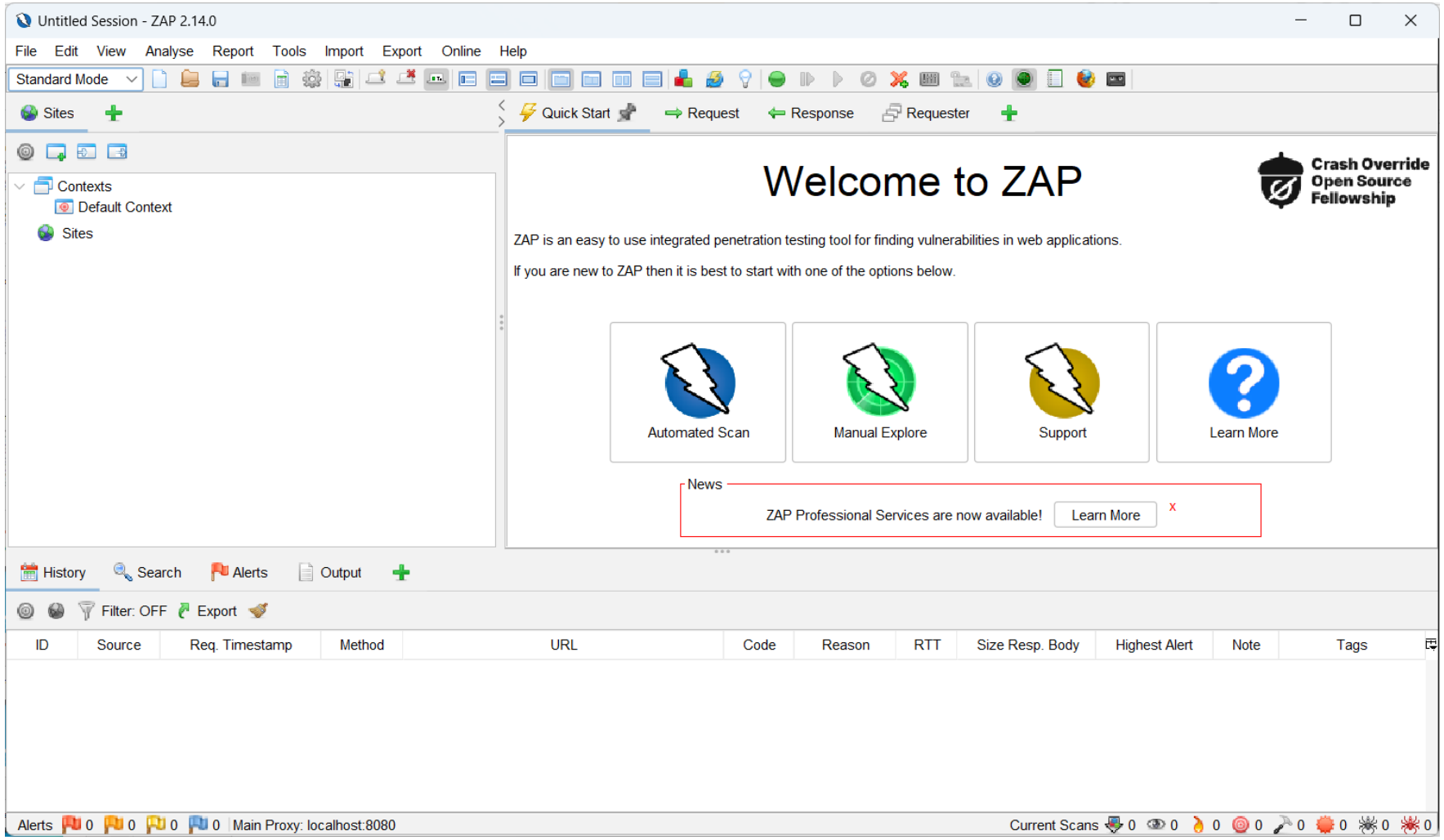
- **White box:** In a white box assessment, the tester has full knowledge of the system or network being tested, including the source code, network diagrams, and configuration files. This allows the tester to perform a more comprehensive assessment, as they can understand how the system works and how vulnerabilities could be exploited.
- **Grey box:** In a grey box assessment, the tester has some knowledge of the system or network being tested, but not as much as in a white box assessment. This might include information such as the network architecture, the operating system, and the web application framework.
- **Black box:** In a black box assessment, the tester has no knowledge of the system or network being tested. This means that the tester must rely on their own skills and knowledge to identify vulnerabilities.


Vulnerability
Scanner Tools

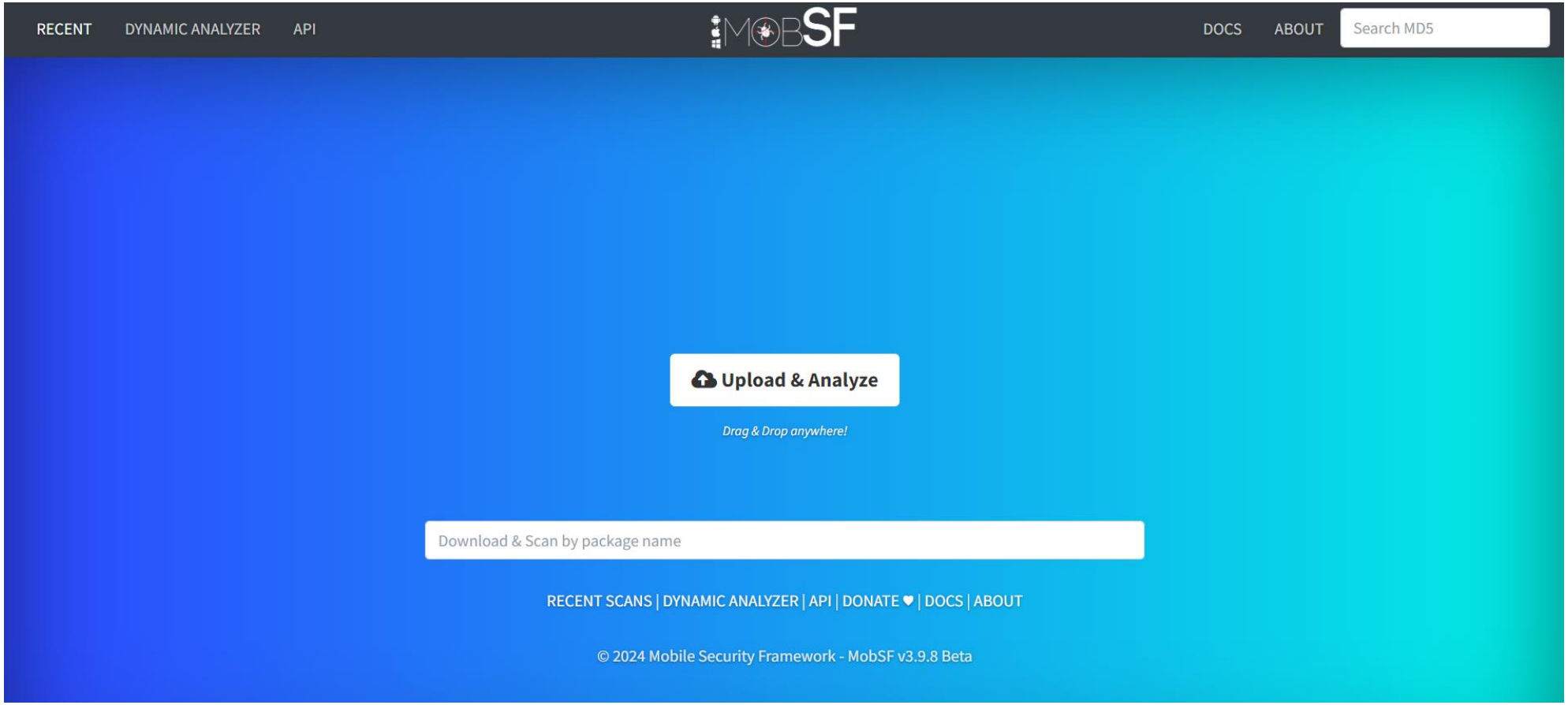
Nessus Essentials (Host Based Assessment Tool)



OWASP Zap / Zaproxy (Web App Assessment Tool)



MobSF (Mobile App Assessment Tool)



Vulnerability Assessment Best Practices

- **Know Your Assets –** Identify and categorize all assets in your environment. Understanding what you need to protect is crucial for an effective assessment.
- **Automation –** Leverage automated tools for scanning and identifying vulnerabilities. Automation speeds up the assessment process and ensures consistent results.
- **Formulate KPIs –** Define Key Performance Indicators (KPIs) to measure the success and effectiveness of your vulnerability assessment program. KPIs provide valuable insights into the program's impact.
- **Build a Vulnerability Management Database –** Maintain a centralized database to track and manage identified vulnerabilities. This database aids in tracking remediation efforts and monitoring progress.
- **Prioritization –** Rank vulnerabilities based on severity, potential impact, and exploitability to focus on the most critical issues.
- **False Positive Verification –** Verify identified vulnerabilities to eliminate false positives and ensure accuracy.
- **Documentation –** Thoroughly document the findings, including vulnerabilities, evidence, and potential risks.
- **Remediation Recommendations –** Provide clear and actionable recommendations for addressing identified vulnerabilities.
- **Collaboration –** Involve different teams, such as IT, security, and development, to ensure a holistic assessment.
- **Integration with Other Security Protocols –**Integrate vulnerability assessment into your broader security strategy. Coordinate with intrusion detection, incident response, and other security practices for a cohesive defense.
- **Share Executive Reports** – Prepare summarized reports for organizational leadership, providing an overview of assessment findings, risks, and recommended actions. This promotes informed decision-making.

Thanks to all