VULNERABILITY ASSESSMENT FOR EDUVOS WEB APP

Steps, Tools, and Prioritization Techniques for Identifying and Addressing Security Risks

Eduvos Midrand Campus
Security+

Table of Contents

Define Scope

Attention to detail is always important when constructing something new, this key aspect could be the difference between a hacker comprising the system and you being ahead of it before he has the chance to. We always need to know how every part in this system works not only to mitigate risk but to identify our weak points that's why defining the scope is important we have three important steps. Asset Inventory is a guide on a catalogue of your physical and digital assets, Security measures refer to the existing protections that are already in place to defend the web application and its environment and finally Targets for testing are the specific parts of the web application and its infrastructure that will be examined during the vulnerability assessment

As stated above asset inventory is a guide on a catalogue of your physical and digital assets such as (hardware software, applications, data and everything in between). Asset Inventory gives us clear break down of the digital infrastructure we have in place as an organizational and helps point out any vulnerabilities to the systems we have in place

EDUVOS Asset Inventory:

Asset ID	**Asset Type**	**Description**	**Location**	**Service**	**Owner**	**Criticality**	**Configuration Details**	**Vulnerability Scope**	**Testing Methods**	**Recovery Mechanisms**
EDUV-WEB SERVER	WEB-SERVER	handles sensitive client data	In-House	Web Application	Administrator	High	PHP/Node.js MySQL/PostgreSQL TLS (SSL) Enabled	Input validation Session management Access controls Encryption mechanisms	OWASP ZAP for automated scanning Burp Suite for interception and testing OpenVAS for web server vulnerabilities Manual inspection Authentication/authorization tests	Daily data backups DRP (Disaster Recovery Plan) Web Application Firewall to block attacks

Security Measures

Security measures refer to the existing protections that are already in place to defend the web application and its environment. The Eduvos network would need to have firewalls, encryption, user authentication, access control, and software update policies. In our assessment, we need to understand the current security measures to help identify what has already been put in place to reduce risk, and where gaps may still remain.

User Authentication Ensures: only authorized users can access the system.

Firewall: Protects the web server from unauthorized network traffic.

Data Encryption (HTTPS/TLS): secures sensitive data during transmission.

Targets for Testing

Targets for testing are the specific parts of the web application and its infrastructure that will be tested during the vulnerability assessment. Targets for testing include user interface, login systems, server configurations and how client data is handled. Defining the testing targets ensures that the assessment is focused and covers all critical components that could be vulnerable to attack.

Login Page: To check for weak authentication or brute-force vulnerabilities.

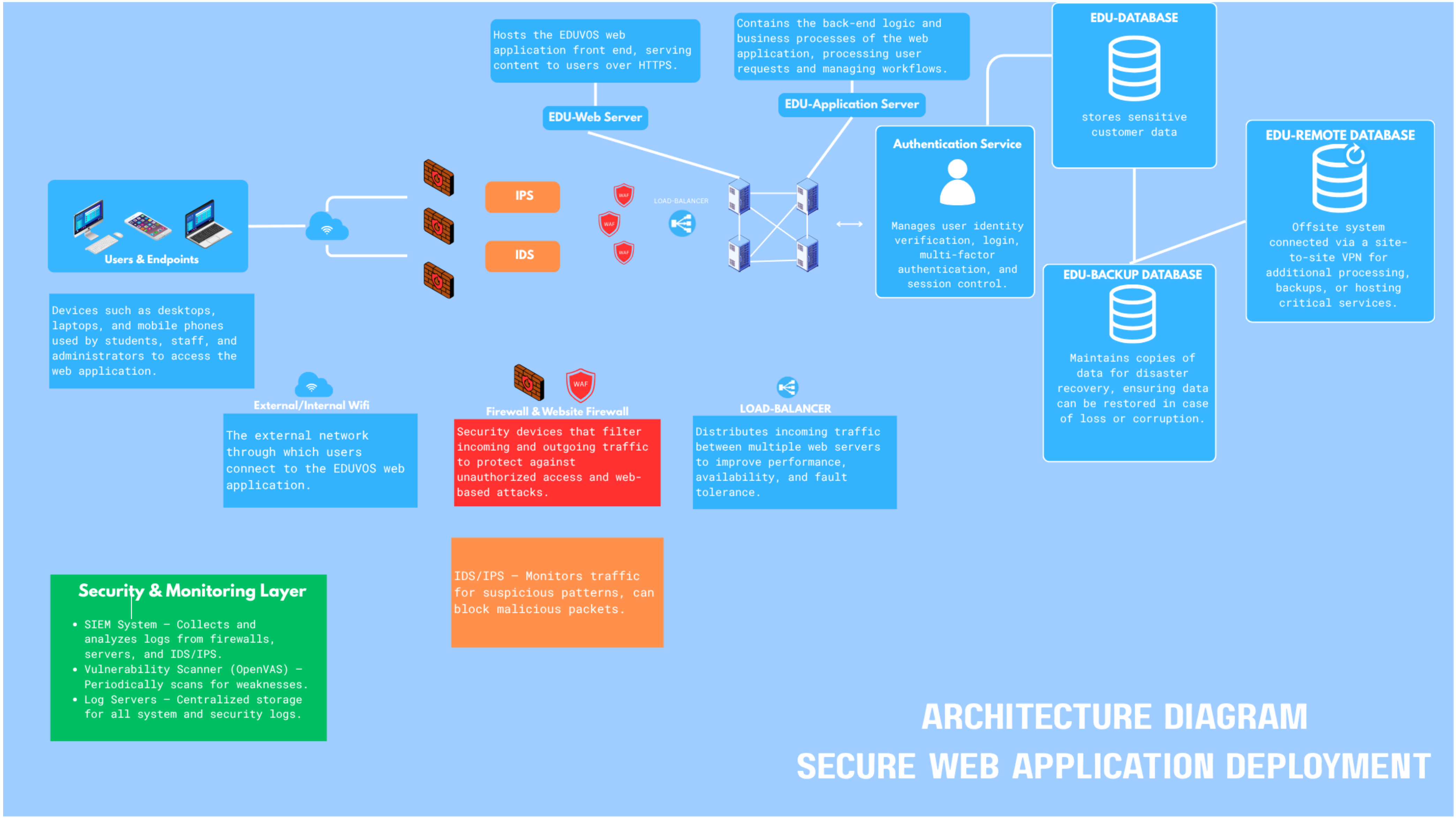
Input Fields: To test for injection flaws like SQL Injection or XSS.

Server Configuration: To identify misconfigurations or exposed services.

Gathering documentation

Architecture Diagram

Shows the EDUVOS web app's structure, including servers, databases, and supporting services, plus how data flows between them. It highlights where sensitive customer data is processed and points where vulnerabilities may appear.



Users & Endpoints

Devices such as desktops, laptops, and mobile phones used by students, staff, and administrators to access the web application.

EDU-Web Server

Hosts the EDUVOS web application front end, serving content to users over HTTPS.

EDU-Application Server

Contains the back-end logic and business processes of the web application, processing user requests and managing workflows.

Authentication Service

Manages user identity verification, login, multi-factor authentication, and session control.

EDU-DATABASE

stores sensitive customer data

EDU-REMOTE DATABASE

Offsite system connected via a site-to-site VPN for additional processing, backups, or hosting critical services.

EDU-BACKUP DATABASE

Maintains copies of data for disaster recovery, ensuring data can be restored in case of loss or corruption.

External/Internal Wifi

The external network through which users connect to the EDUVOS web application.

Firewall & Website Firewall

Security devices that filter incoming and outgoing traffic to protect against unauthorized access and web-based attacks.

LOAD-BALANCER

Distributes incoming traffic between multiple web servers to improve performance, availability, and fault tolerance.

IDS/IPS – Monitors traffic for suspicious patterns, can block malicious packets.

Security & Monitoring Layer

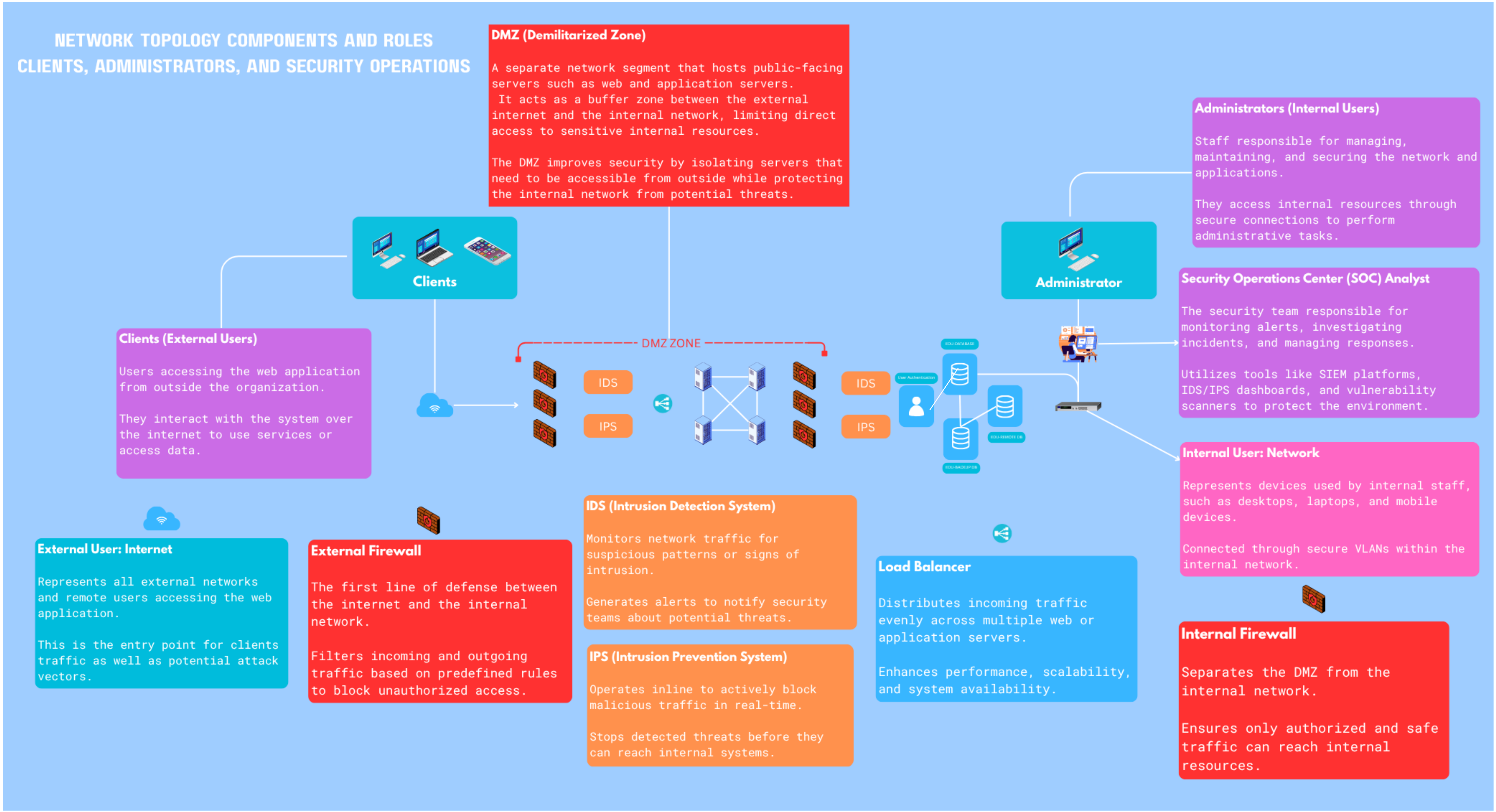
- SIEM System – Collects and analyzes logs from firewalls, servers, and IDS/IPS.
- Vulnerability Scanner (OpenVAS) – Periodically scans for weaknesses.
- Log Servers – Centralized storage for all system and security logs.

ARCHITECTURE DIAGRAM

SECURE WEB APPLICATION DEPLOYMENT

Network Topology

Shows how EDUVOS's network is arranged, including firewalls, DMZ, SOC monitoring points, and links to the web app. It helps identify attack paths and confirms that security controls are in the right places.



NETWORK TOPOLOGY COMPONENTS AND ROLES
CLIENTS, ADMINISTRATORS, AND SECURITY OPERATIONS

DMZ (Demilitarized Zone)

A separate network segment that hosts public-facing servers such as web and application servers. It acts as a buffer zone between the external internet and the internal network, limiting direct access to sensitive internal resources.

The DMZ improves security by isolating servers that need to be accessible from outside while protecting the internal network from potential threats.

Administrators (Internal Users)

Staff responsible for managing, maintaining, and securing the network and applications.

They access internal resources through secure connections to perform administrative tasks.

Security Operations Center (SOC) Analyst

The security team responsible for monitoring alerts, investigating incidents, and managing responses.

Utilizes tools like SIEM platforms, IDS/IPS dashboards, and vulnerability scanners to protect the environment.

Clients (External Users)

Users accessing the web application from outside the organization.

They interact with the system over the internet to use services or access data.

Internal User: Network

Represents devices used by internal staff, such as desktops, laptops, and mobile devices.

Connected through secure VLANs within the internal network.

External User: Internet

Represents all external networks and remote users accessing the web application.

This is the entry point for clients traffic as well as potential attack vectors.

External Firewall

The first line of defense between the internet and the internal network.

Filters incoming and outgoing traffic based on predefined rules to block unauthorized access.

IDS (Intrusion Detection System)

Monitors network traffic for suspicious patterns or signs of intrusion.

Generates alerts to notify security teams about potential threats.

IPS (Intrusion Prevention System)

Operates inline to actively block malicious traffic in real-time.

Stops detected threats before they can reach internal systems.

Load Balancer

Distributes incoming traffic evenly across multiple web or application servers.

Enhances performance, scalability, and system availability.

Internal Firewall

Separates the DMZ from the internal network.

Ensures only authorized and safe traffic can reach internal resources.

Set Objectives

The main goal of this vulnerability assessment is to find any weaknesses in the web application that could let attackers access or damage sensitive customer information. By spotting these issues early, we can help protect the application from cyberattacks and keep customer data safe. This is especially important because of South Africa’s data protection law, POPIA, which requires businesses to handle personal data responsibly.

Compliance - Check that the web application follows important rules and standards, including POPIA and any other relevant regulations. Find any areas where the application’s security might not meet these rules and provide proof to support future audits.

Bounded

Clearly state which parts of the web application and related systems will be tested.

Make sure testing is done only on approved systems to avoid causing problems in live environments.

Focus on the most important parts of the system that deal with sensitive data to make the assessment efficient.

Tools

The tools section lists the software and utilities that will be used to identify vulnerabilities during testing.

Burp Suite Scanner – Used for scanning and intercepting web application traffic to detect issues like injection flaws, broken authentication, and insecure configurations.

Nmap – A network mapping and scanning tool used to identify active hosts, open ports, and running services.

OWASP ZAP – An open-source security tool that analyses web traffic to detect vulnerabilities such as cross-site scripting and SQL injection.

OpenVAS – is primarily used for vulnerability scanning and management.

Prioritising Vulnerabilities

Vulnerabilities are ranked based on severity, impact, and likelihood of exploitation. A table like the one below ensures remediation efforts focus on the most critical risks first.

Severity	**Example Vulnerability**	**Impact**	**Likelihood**	**Priority**
Critical	SQL injection exposing student/customer data	Full database compromise	High	1
High	Insecure admin panel without MFA	Unauthorized admin access	Medium	2
Low	Outdated JavaScript library with known exploits	Potential XSS or data leak	Medium	3
Medium	Missing security headers on non-sensitive pages	Minor security hardening required	Low	4

Conclusion Summary of the Assessment

This vulnerability assessment covered several critical areas to ensure the EDUVOS web application is secure and compliant. We began by defining the scope, including creating an asset inventory to understand all physical and digital resources, reviewing existing security measures like firewalls, encryption, and authentication, and identifying targets for testing such as login systems, input fields, and server configurations.

We documented the system through an architecture diagram and network topology, which highlighted data flow and potential attack paths. The assessment objectives focused on detecting weaknesses that could expose sensitive customer information, ensuring POPIA compliance, and clearly defining testing boundaries to protect live systems.

Using tools such as Burp Suite, Nmap, OWASP ZAP, and OpenVAS, vulnerabilities were identified and prioritized according to severity, impact, and likelihood of exploitation. By following this structured approach, we not only identified critical risks but also established a clear roadmap for remediation, strengthening security and safeguarding sensitive data.

References

Cisco Systems, Inc, 2025. *Cisco Cyber Threat Trends Report.* [Online]
Available at: https://www.cisco.com/c/en/us/products/security/cyber-threat-trends-report.html
[Accessed 18 August 2025].

Imperva, 2025. *What is Vulnerability Assessment.* [Online]
Available at: https://www.imperva.com/learn/application-security/vulnerability-assessment/
[Accessed 18 August 2025].

OWASP Foundation, 2020. *OWASP Web Security Testing Guide v4.2..* [Online]
Available at: https://owasp.org/www-project-web-security-testing-guide/
[Accessed 18 August 2025].

Wiz, 2025. *Vulnerability Assessments: Tips, Tools, and Templates.* [Online]
Available at: https://www.wiz.io/academy/vulnerability-assessments
[Accessed 18 August 2025].