@Generalzodx28

SCANNING AND THREAT MODELING
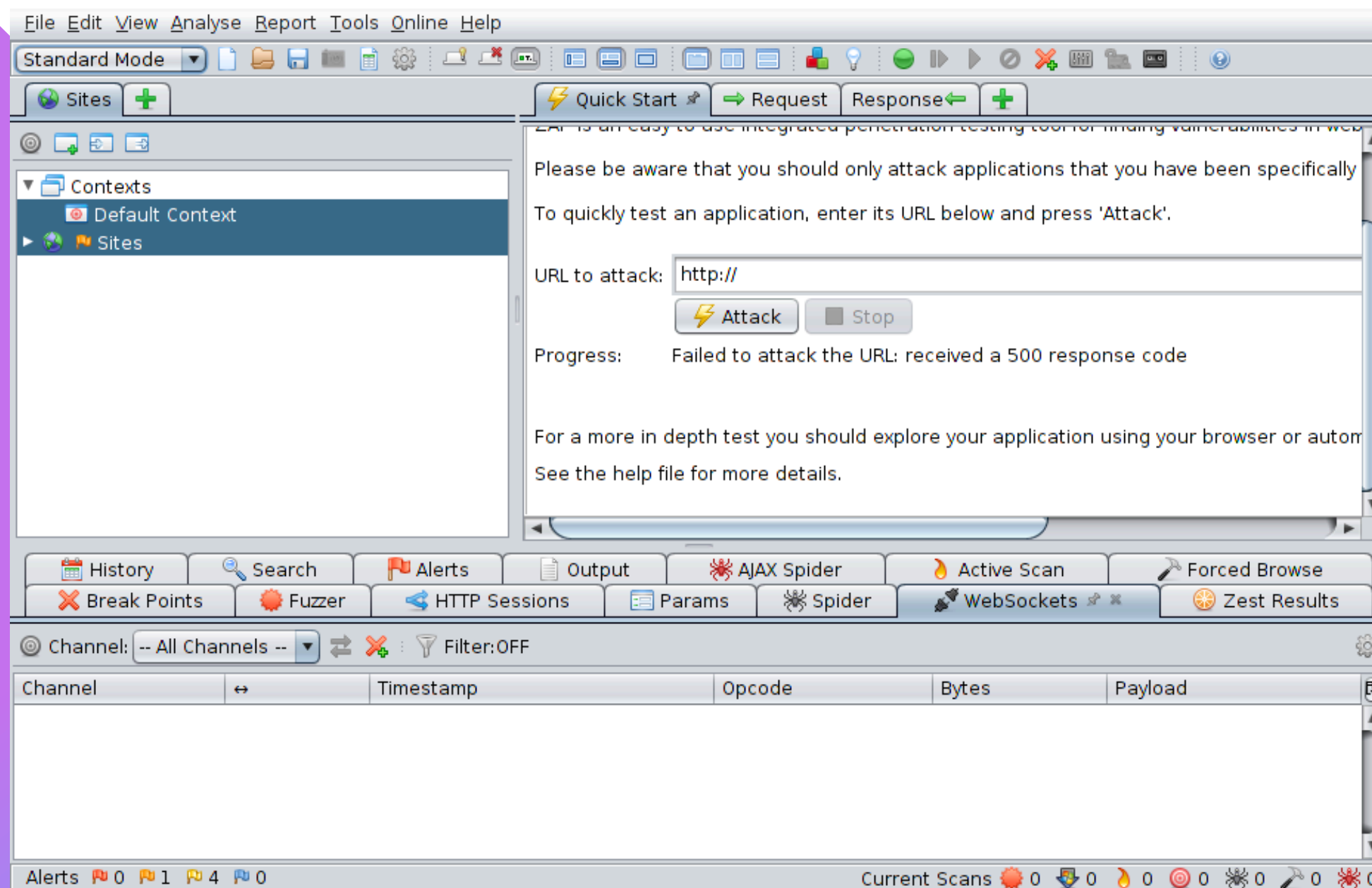
REPORT

AUGUST 2024

SUBMITTED BY: @GENERAL_ZODX28
SUBMITTED TO: @.VIPER_11
DATED: AUG 8, 2024

Owasp Zap

OWASP ZAP (Zed Attack Proxy) is an open-source web application security testing tool developed by the Open Web Application Security Project (OWASP). It is designed to help find security vulnerabilities in web applications during the development and testing phases.

OWASP ZAP is highly regarded in the security community due to its comprehensive feature set, ease of use, and active development.

Snyk

Snyk is a developer-first security platform that helps developers find, fix, and monitor vulnerabilities in their code, dependencies, container images, and infrastructure as code (IaC). It integrates into the development process, allowing teams to identify and remediate security issues early in the software development lifecycle (SDLC).

Types of backups

- A **Full Backup** involves copying all the data from a system to the backup storage. This backup contains everything—files, databases, system settings, etc.—so it represents the complete state of the system at the time of the backup.

- An **Incremental Backup** only saves the data that has changed since the last backup of any type (whether that was a full or another incremental backup). For example, if a full backup is done on Monday and an incremental backup is done on Tuesday, the Tuesday backup will only include the files that were added or changed since Monday.

- A **Differential Backup** saves the data that has changed since the last full backup. Unlike incremental backups, which only record changes since the last backup of any kind, differential backups accumulate changes over time until the next full backup. For example, if a full backup is done on Monday, a differential backup on Tuesday will include all changes since Monday, and a differential backup on Wednesday will also include all changes since Monday.

Scanning for Insider Threats

Implement SIEMs like:
- **Wazuh**
- **Security Onion**

THANK YOU