

OAT-014 Vulnerability Scanning | OWASP Foundation

Archived: 2026-04-05 22:44:41 UTC

Vulnerability Scanning is an automated threat. The OWASP Automated Threat Handbook - Web Applications ([pdf](#), [print](#)), an output of the [OWASP Automated Threats to Web Applications Project](#), provides a fuller guide to each threat, detection methods and countermeasures. The [threat identification chart](#) helps to correctly identify the automated threat.

Definition

OWASP Automated Threat (OAT) Identity Number

OAT-014

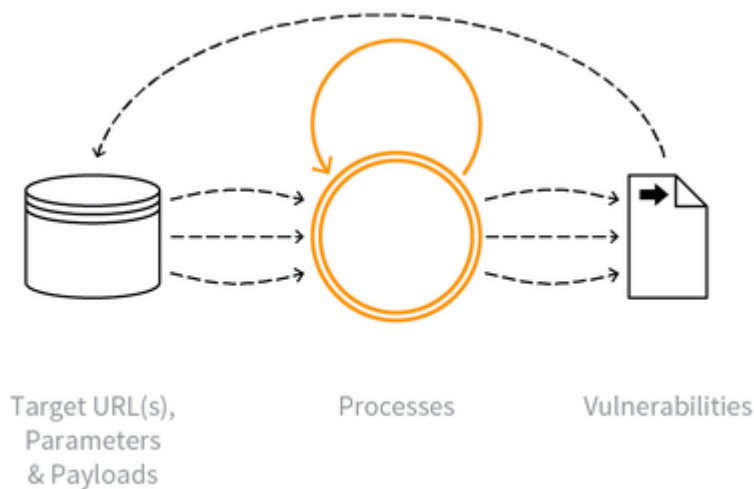
Threat Event Name

Vulnerability Scanning

Summary Defining Characteristics

Crawl and fuzz application to identify weaknesses and possible vulnerabilities.

Indicative Diagram



Description

Systematic enumeration and examination of identifiable, guessable and unknown content locations, paths, file names, parameters, in order to find weaknesses and points where a security vulnerability might exist. Vulnerability

Scanning includes both malicious scanning and friendly scanning by an authorised vulnerability scanning engine. It differs from [OAT-011 Scraping](#) in that its aim is to identify potential vulnerabilities.

The exploitation of individual vulnerabilities is not included in the scope of this ontology, but this process of scanning, along with [OAT-018 Footprinting](#), [OAT-004 Fingerprinting](#) and [OAT-011 Scraping](#) often form part of application penetration testing.

Other Names and Examples

Active/Passive scanning; Application-specific vulnerability discovery; Identifying vulnerable content management systems (CMS) and CMS components; Known vulnerability scanning; Malicious crawling; Vulnerability reconnaissance

See Also

- [OAT-004 Fingerprinting](#)
- [OAT-011 Scraping](#)
- [OAT-018 Footprinting](#)

Cross-References

CAPEC Category / Attack Pattern IDs

- —

CWE Base / Class / Variant IDs

- 799 Improper Control of Interaction Frequency
- 841 Improper Enforcement of Behavioral Workflow

WASC Threat IDs

- 21 Insufficient Anti-Automation

OWASP Attack Category / Attack IDs

- —

Source: https://owasp.org/www-project-automated-threats-to-web-applications/assets/oats/EN/OAT-014_Vulnerability_Scanning