

Scanning Your Web Application



Sunny Wear

SECURITY ARCHITECT AND PENETRATION TESTER

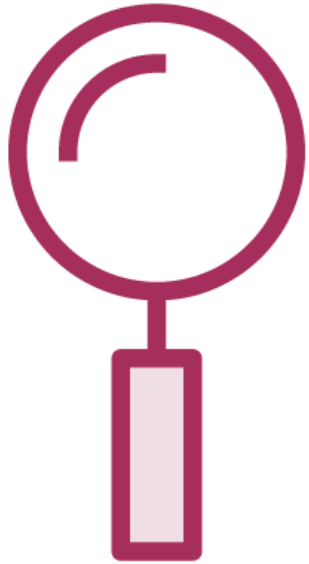
@SunnyWear www.sunnywear.org



Why Scan



Scanner



Findings

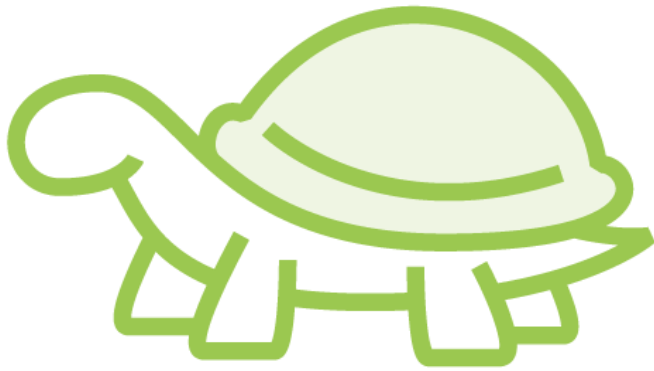


Indicators

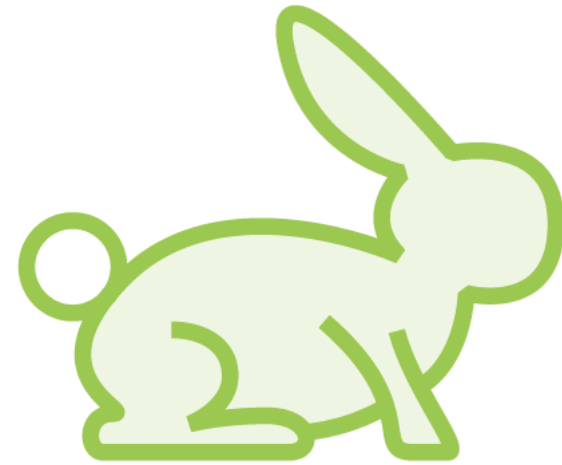


Vulnerability
Identification

Scanning Modes

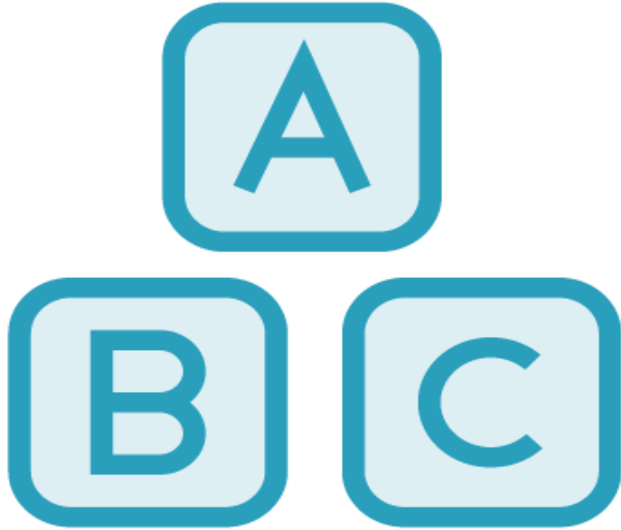


Passive

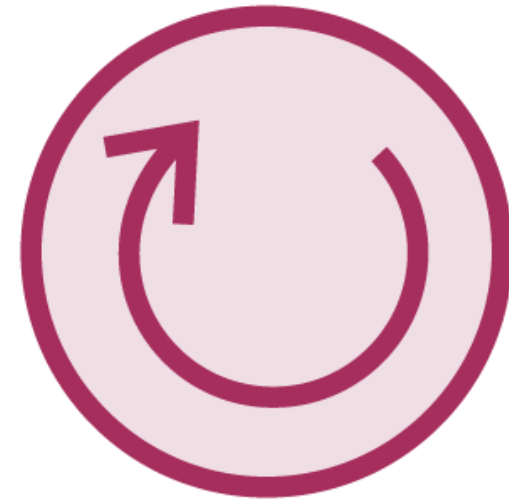


Active

Timing



Sequence



Passive Scanning is
On-going

Vulnerability vs False Positive

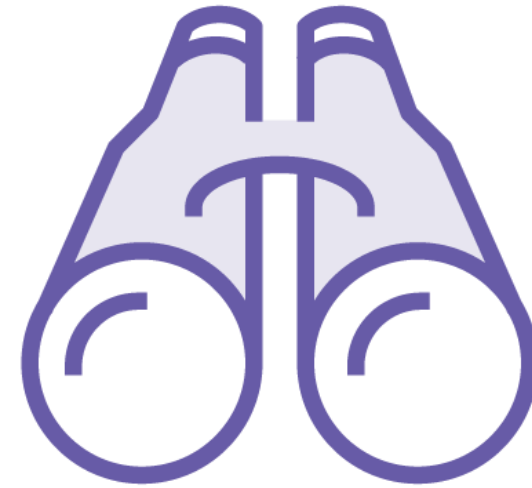


Verification



Practice

Demo



Scanner Functions



Scanner Tabs

Issue Activity

Scan Queue

Live Scanning

Issue Definitions

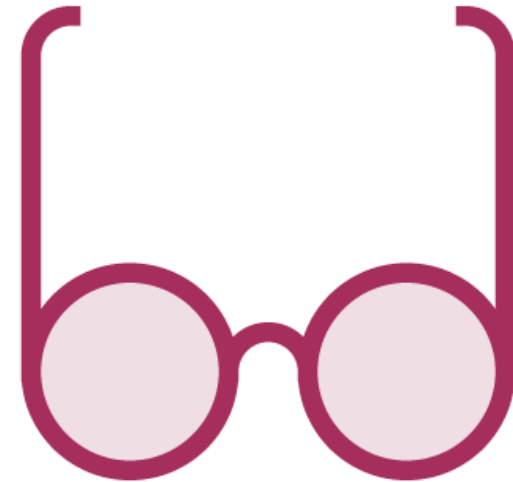
Options



Scanner Issue Activity Tab

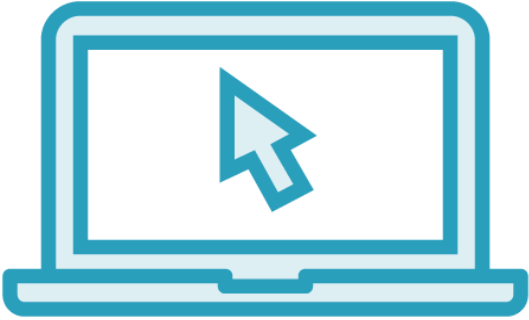


Issues Identified



Message Editor Details
(Advisory, Request, Response)

Scanner Scan Queue Tab



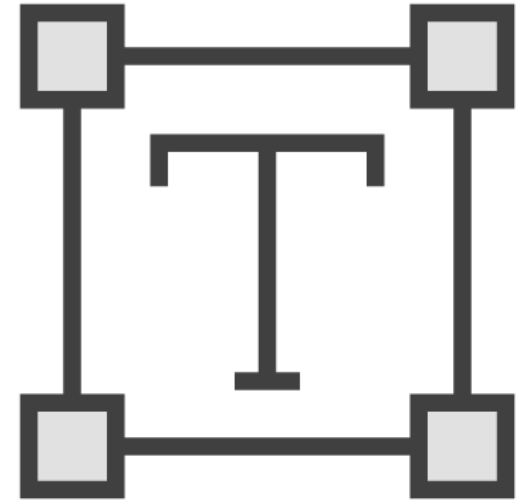
Host, URL,
Status



Issues, Requests



Insertion Points



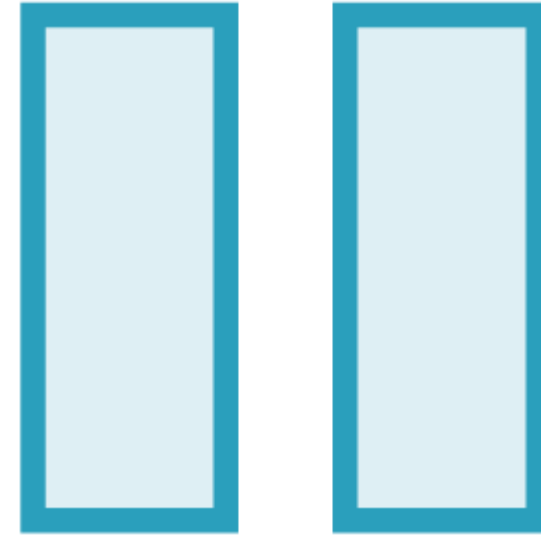
Timings,
Comment



Scanner Live Scanning Tab



Live Active Scanning



Live Passive Scanning



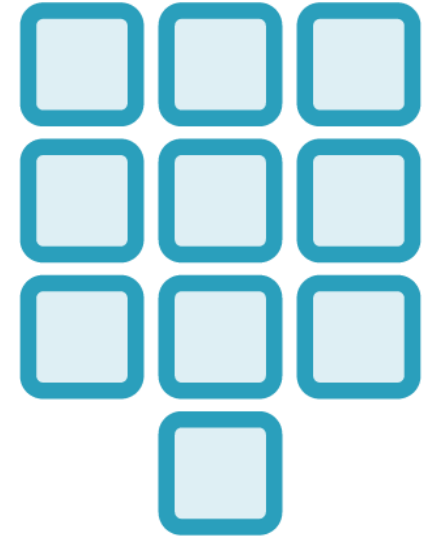
Scanner Issue Definitions Tab



Issue Name



Severity

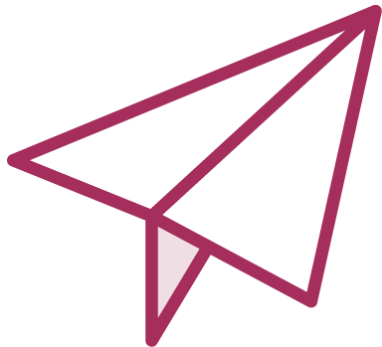


Index Number

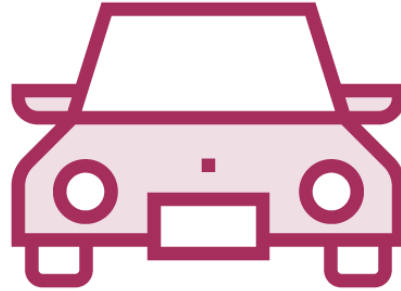
Scanner Options Tab



Attack Insertion Points



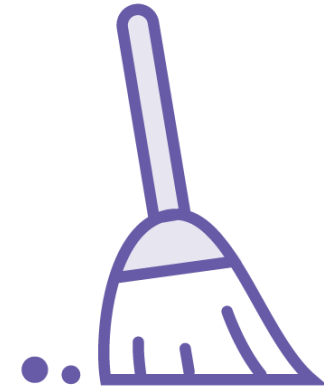
Active Scanning Areas



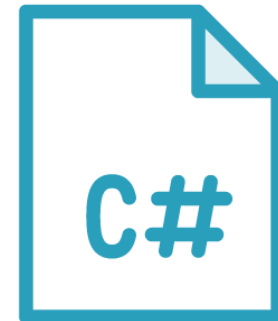
Active Scanning
Engine



Passive Scanning
Areas



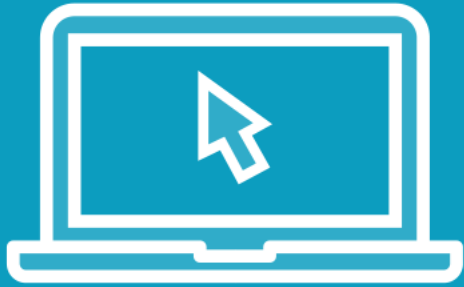
Active Scanning
Optimization



Static Code Analysis



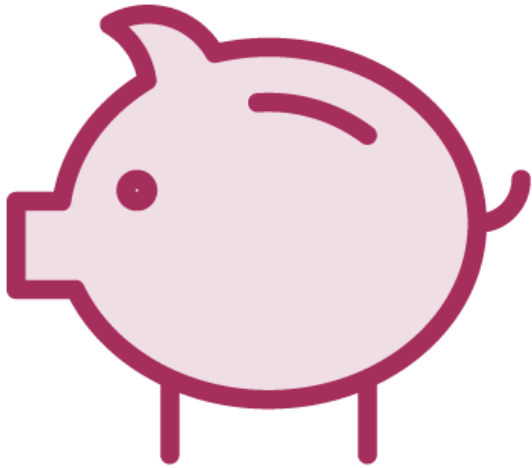
Demo



Passive Scanner



Live Passive Scanning



No New Requests

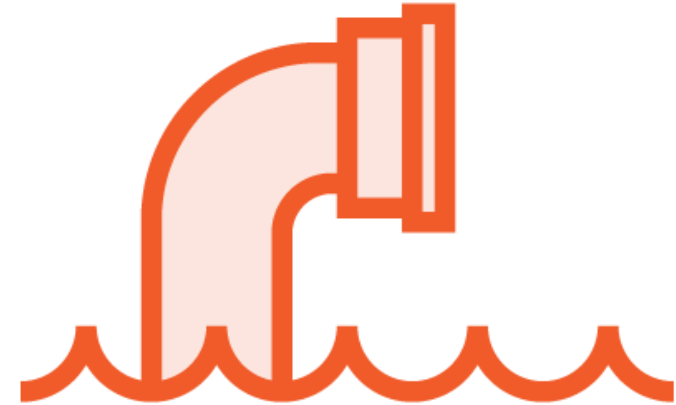


Deduce Vulnerabilities

Live Scanning Tab



Passive Scan Behavior



Scope

Scanner Options Tab



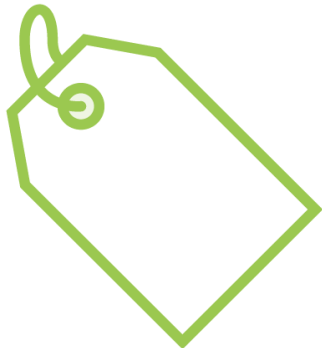
Headers



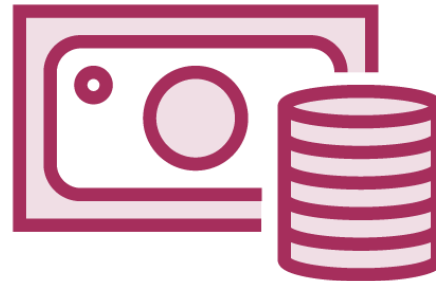
Forms



Parameters



Cookies



Caching



ASP .NET View State

Demo



Active Scanner



Live Active Scanning



New Modified Requests



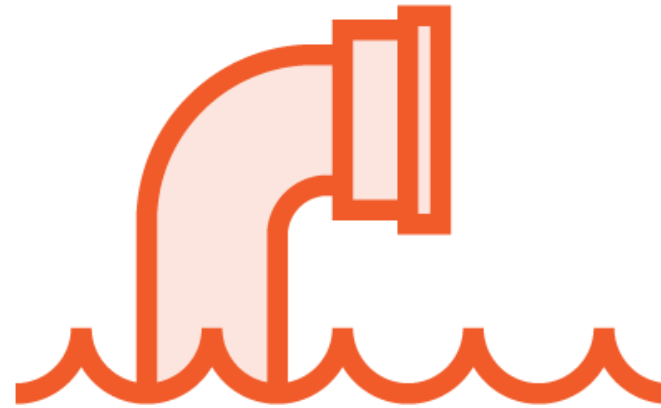
Identify Vulnerabilities



Live Scanning Tab



Auto Behavior



Scope

Active Scanning Wizard



Fine-tune Scope



Scanner Options Tab



SQL Injection



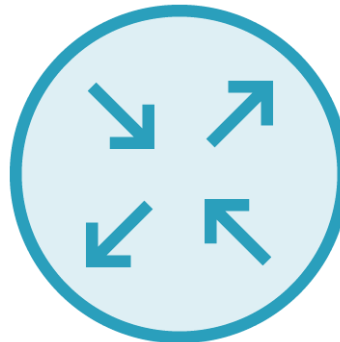
XSS



DOM Issues



HTTP Header
Injection



Open Redirection

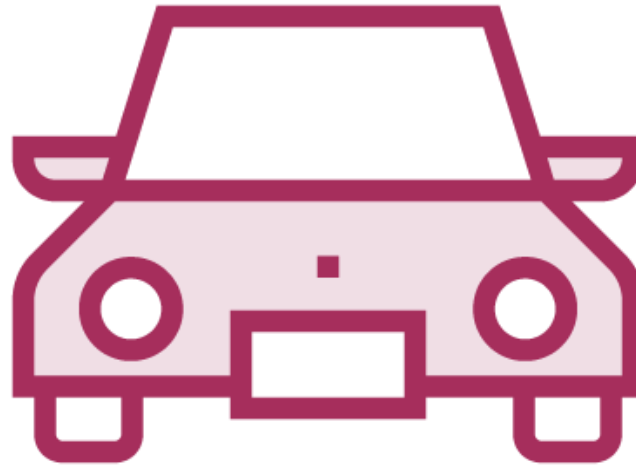


SOAP Injection

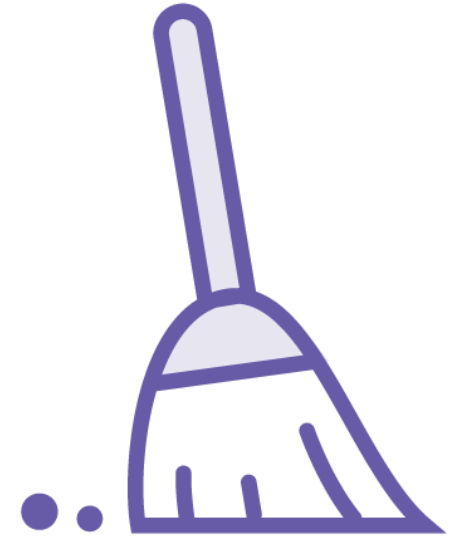
Scanner Options Tab Continued



Attack Insertion Points

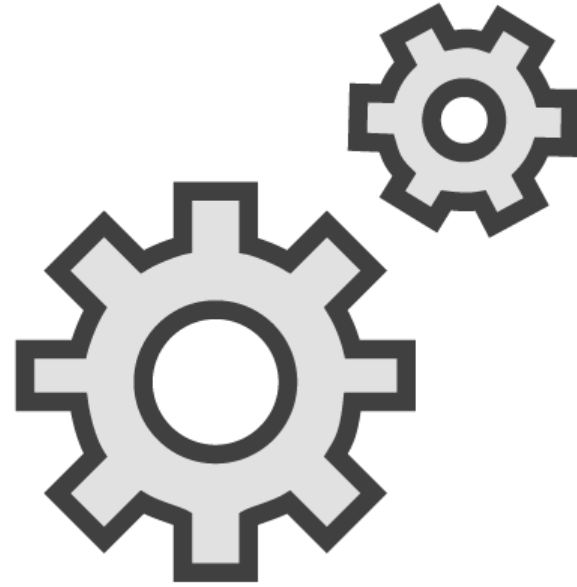
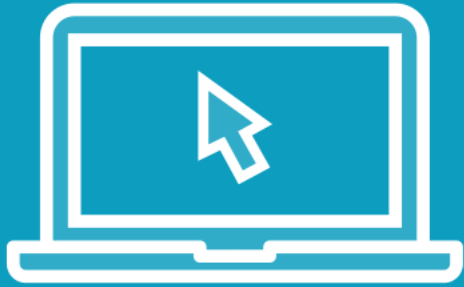


**Active Scanning
Engine**



**Active Scanning
Optimization**

Demo



Scanning Against Your Target



Active Scanning of Target

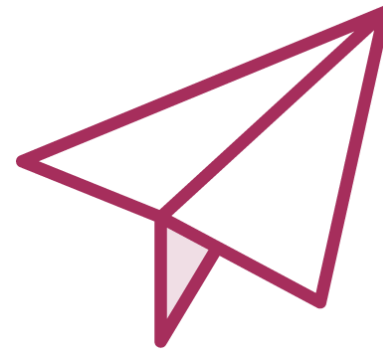


Commence Attack!



Monitor Scan

Demo



Summary



Scanning Complete

Digging into Your Results

