

Web Application Penetration Testing with Burp Suite

SPIDERING YOUR WEB APPLICATION



Sunny Wear

SECURITY ARCHITECT AND PENETRATION TESTER

@SunnyWear www.sunnywear.org

Why Spider

Spidering



Mapping your
application

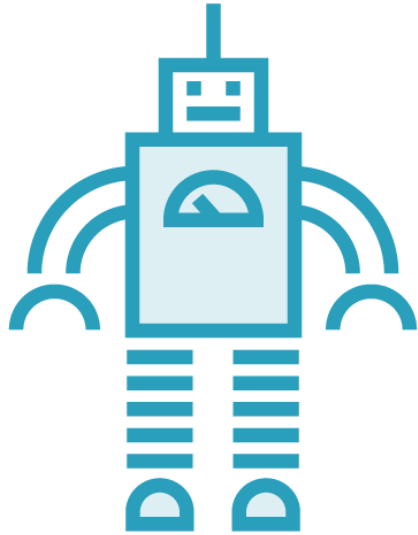


Links

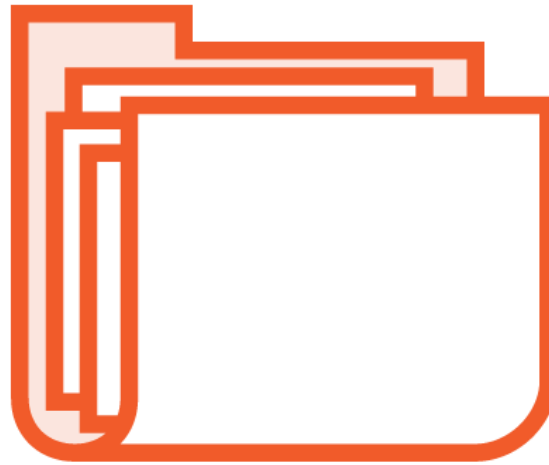


Forms

Automated Spidering



Automated



Files, Folders, Forms



Parsed Response

Manual Spidering

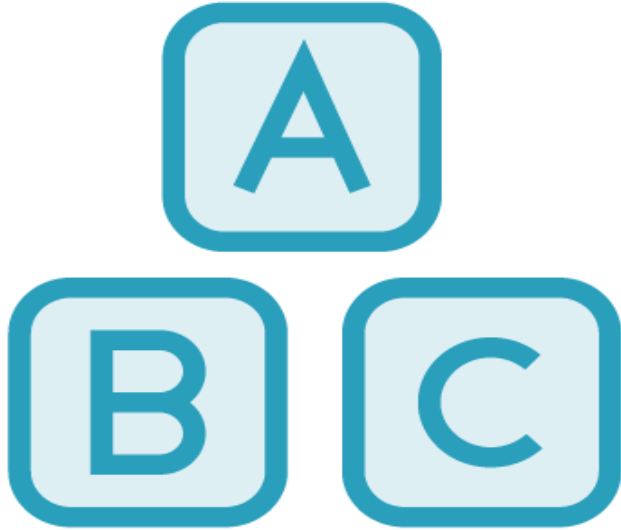


Flash, Silverlight



Client-side
Technologies

Timing

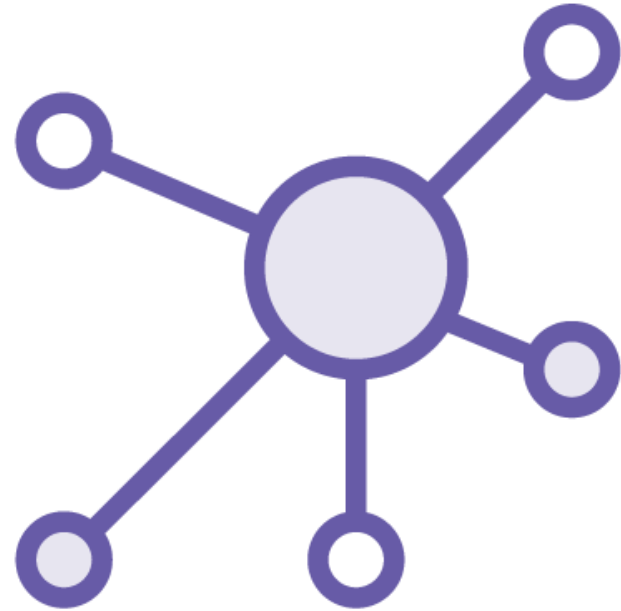
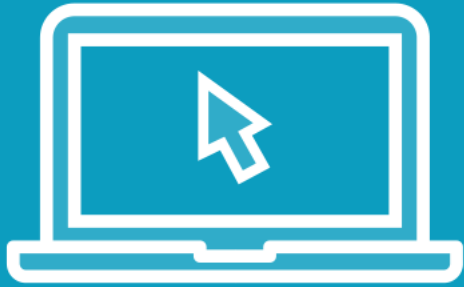


Sequence



On-going

Demo



Spidering Options

Spider “tabs”

A solid orange rectangular block.

Control

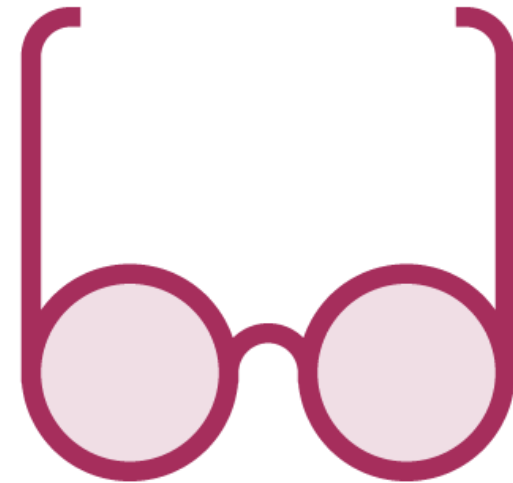
A solid green rectangular block.

Options

Spider Control Tab



Spider Status

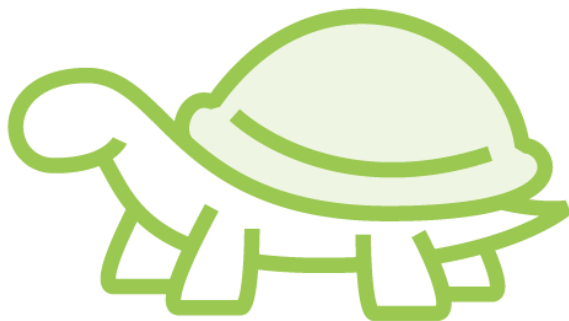


Spider Scope

Spider Options Tab



Crawler Settings



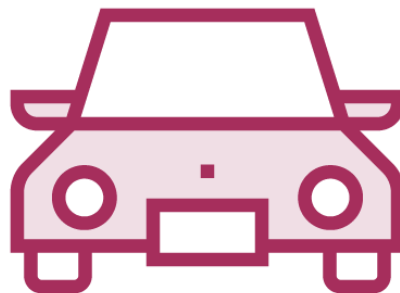
Passive Spidering



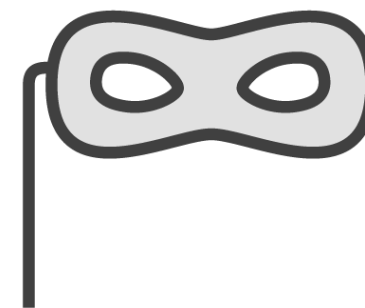
Form Submission



Application Login

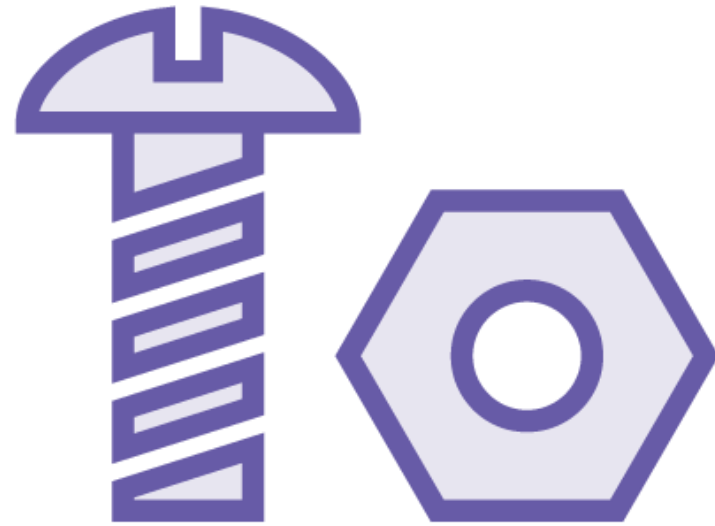


Spider Engine



Request Headers

Demo



Spidering your Web Forms

Spider Options Tab - Forms

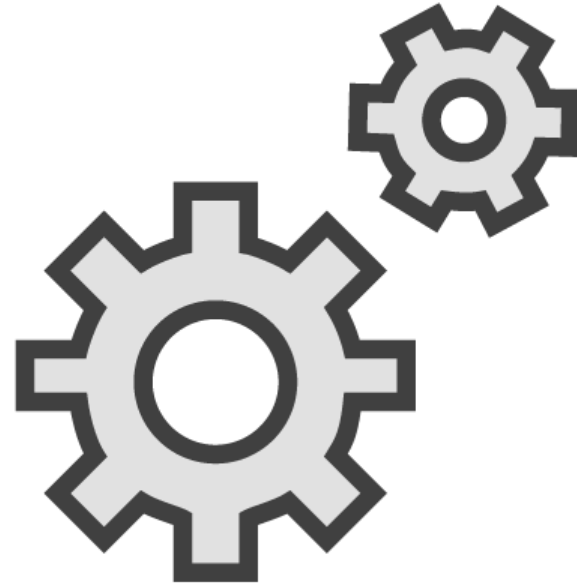
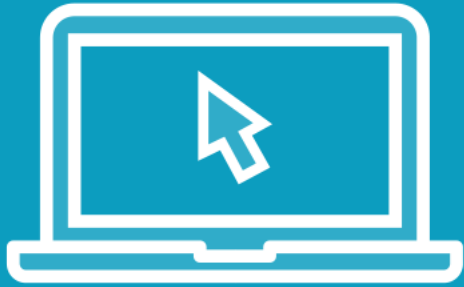


Form Submission



Application Login

Demo



Identifying your Target

Target “tabs”

Scope

Sitemap

Target Scope



Scope settings

In-scope Targets

**Out-of-scope
Targets**

Target Sitemap



Sitemap settings

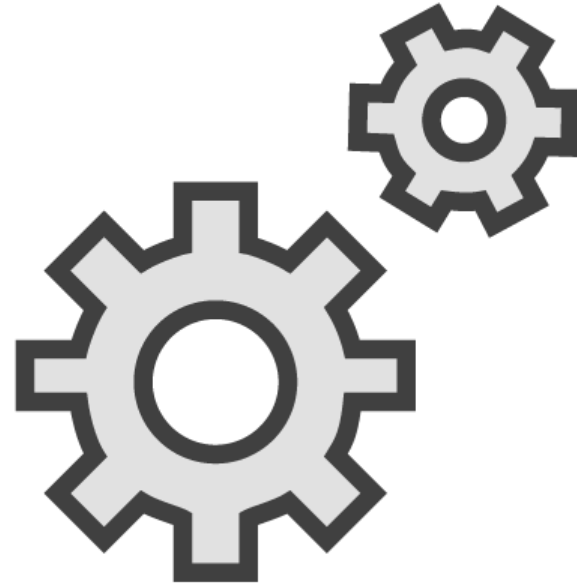
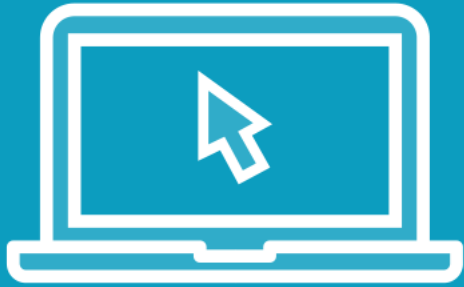
Filter

Contents

Issues

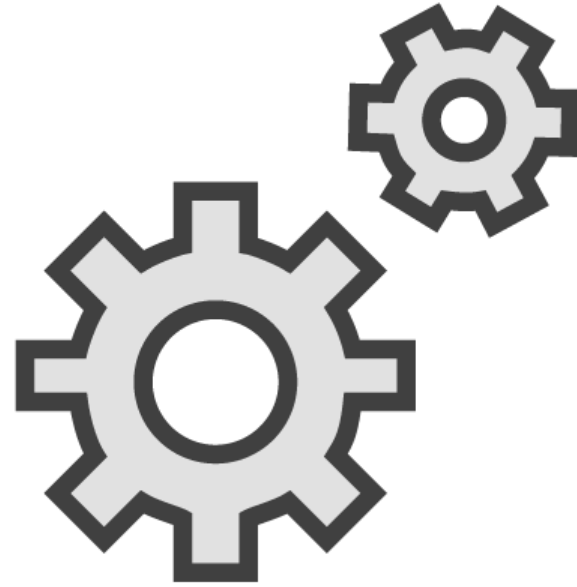
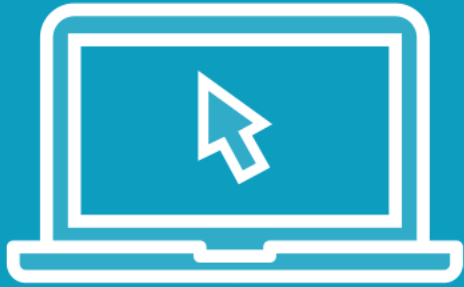
Advisory

Demo



Spidering against your Target

Demo



Examining Your Results

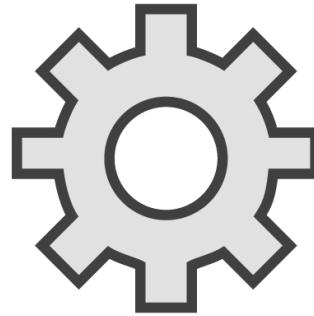
Icons



Highest
domain



Branch



Identified
scope

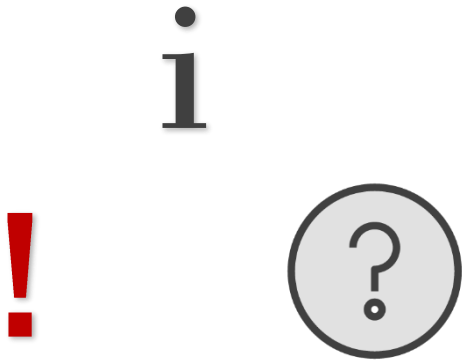


Issue
Identified

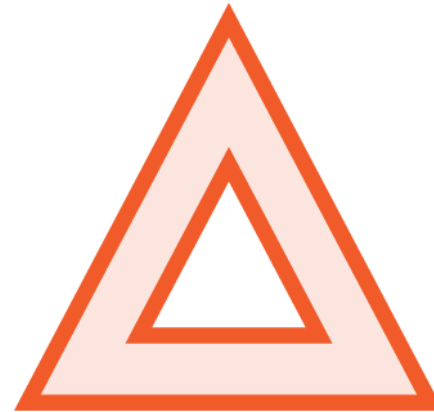


Message
(Request,
Response)

Issues and Advisory



Issues Icons



Severity and
Confidence
Ratings

Colors

Red (High)

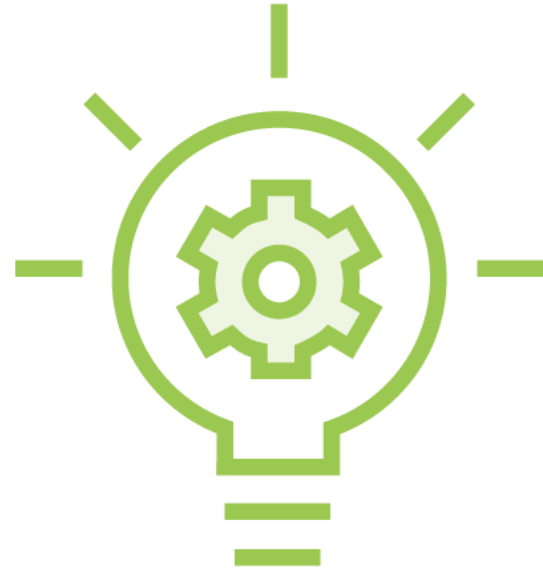
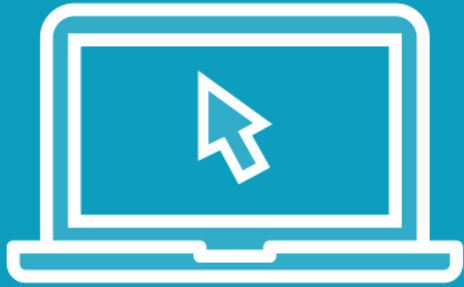
Orange (Medium)

Yellow (Low)

Gray (Information)

White (Information)

Demo



Summary



Spidering complete

Commence attack