Hybrid Spidering Your Web Application

Sunny Wear
SECURITY ARCHITECT AND PENETRATION TESTER
@SunnyWear www.sunnywear.org

Gray Box Testing

Authenticated Accounts

“Bob”
non-admin user

“Admin”
administrator

Demo

Validate our accounts

- Login as Bob
- Login as Admin
- Logout prior to scoping

Scoping Our Target

Target Sitemap -> Juice Shop

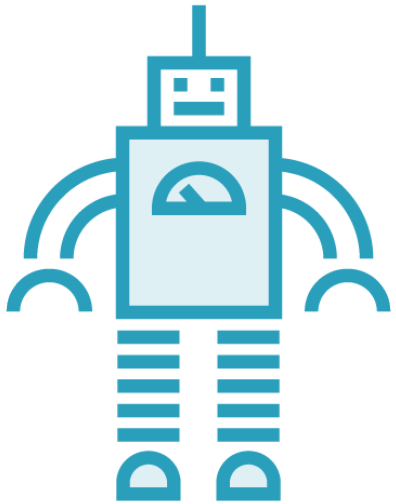
Demo

Set target/scope

Filter URL

Spidering Your Scoped Target

Types of Spidering

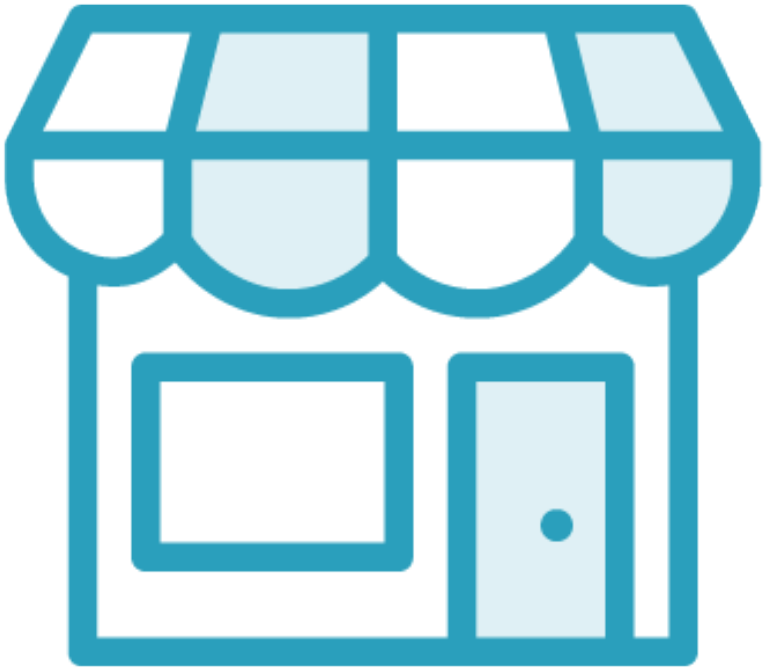


Automated

Manual

Hybrid

OWASP Juice Shop



Technology stack

- HTML5
- AngularJS
- bootstrap
- Nodejs

Event triggers

- Manually click

Spidering Bob's Account

1. Login as Bob
2. Set scope
3. Spider scope
4. Save as session state file

Spidering Admin's Account

1. Login as Admin
2. Set scope
3. Spider scope
4. Leave as current sitemap

Demo

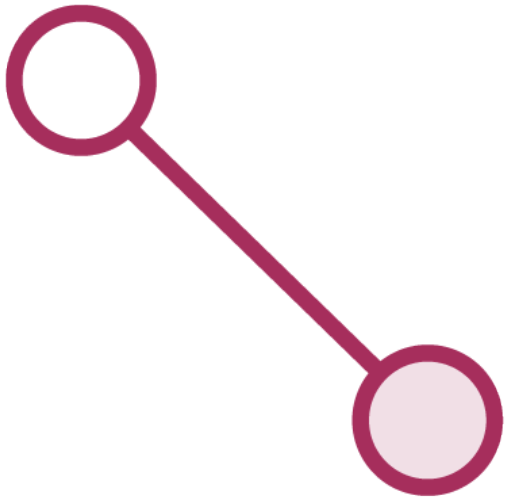
Hybrid spidering of Juice Shop

Spider Bob's account

Spider admin's account

Privilege Escalation Discovery

Clean Demarcation



Non-admin boundaries

Administrator

Compare Site Maps Functionality

Allows a visual display of differences between two target site maps.

Each site map is loaded into the Comparer module.

Sitemap Comparison Feature

Sitemap 1

Sitemap 2

Comparison

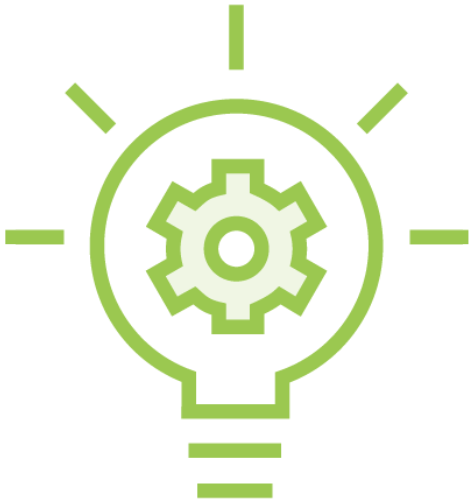
Demo

Sitemap Comparison

- Uses current sitemap
- Compare to saved session sitemap
- Identify privilege escalation opportunities

Directory Brute-forcing

Discover Using Custom Wordlists



Unlinked folders

Unmapped admin consoles

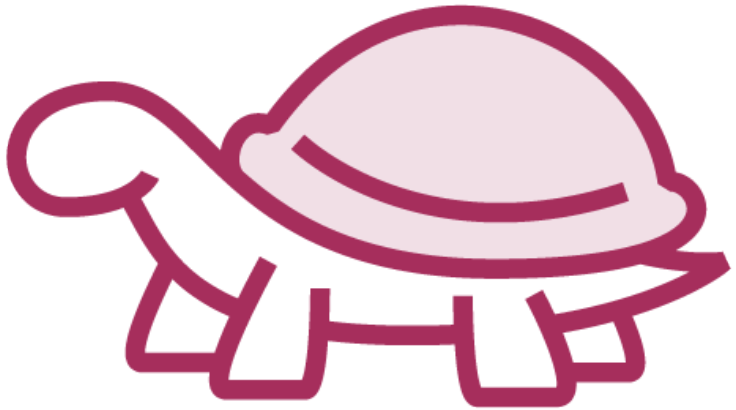
Demo

Use a custom wordlist

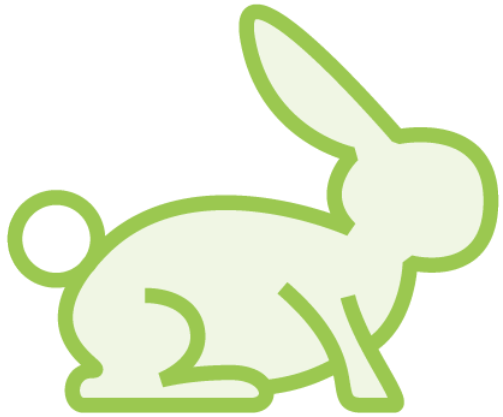
Perform discover content attack

Scanning our Target

Scanner Options



Passive



Active

Demo

Scanning against the Juice Shop

Summary

Hybrid spidering

Site map comparison

Directory brute-forcing

Scanner findings