

Digging Deeper into Your Results



Sunny Wear

SECURITY ARCHITECT AND PENETRATION TESTER

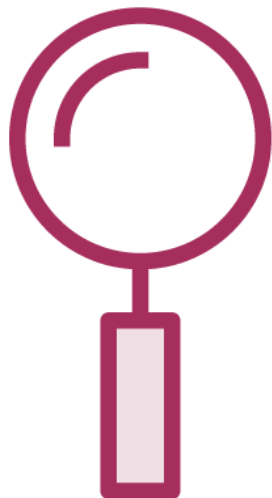
@SunnyWear www.sunnywear.org



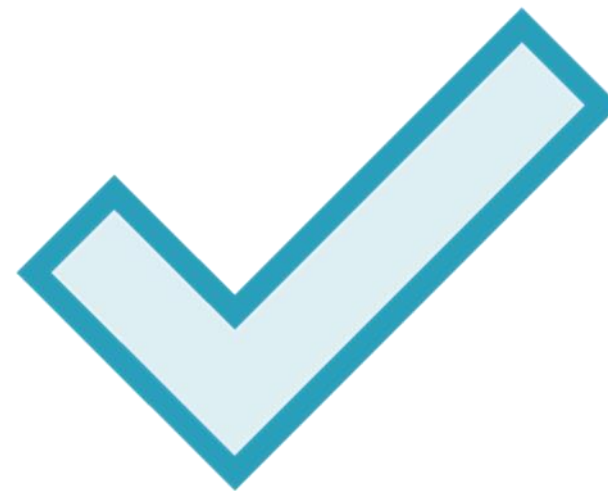
Analyzing Scan Results



Scan Results



Findings



Validation



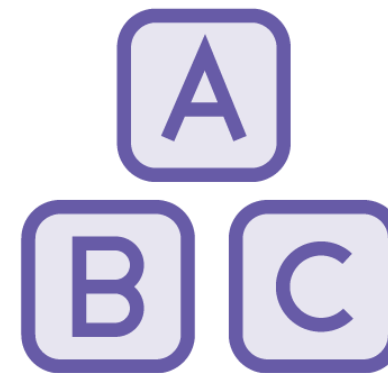
Burp Suite of Modules



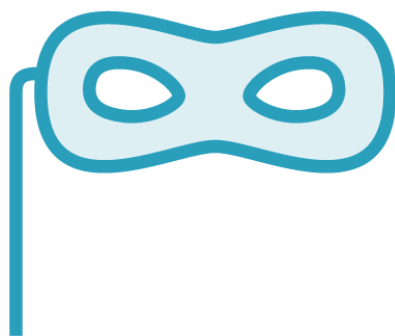
Repeater



Intruder



Sequencer



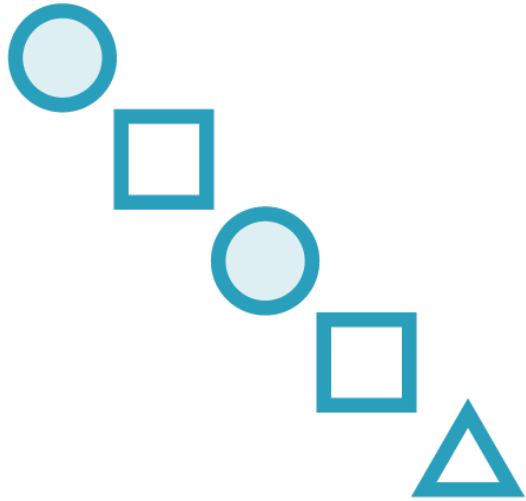
Decoder



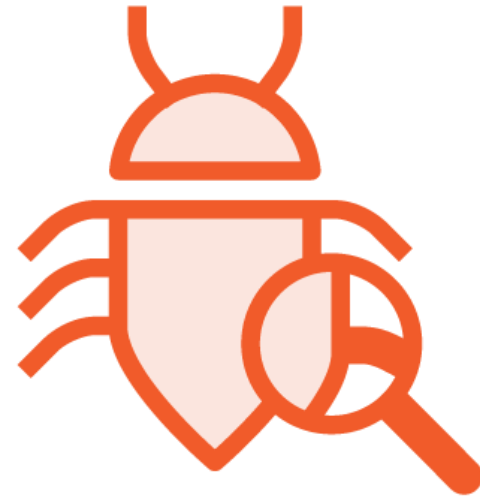
Comparer



Repeater

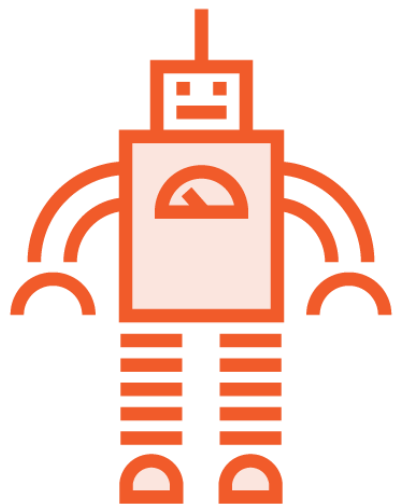


Modify and reissue

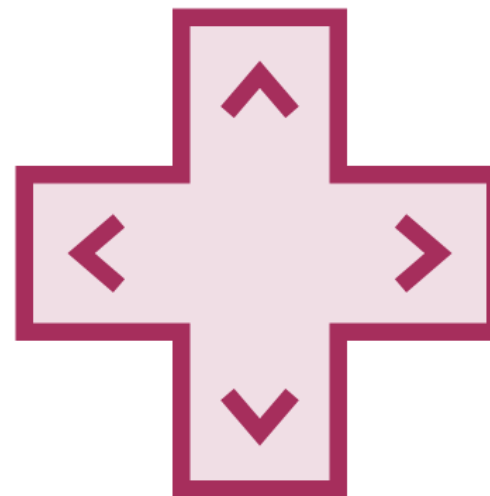


Analyze response

Intruder



Automate attacks



Fine-grained control



Sequencer



Degree of randomness

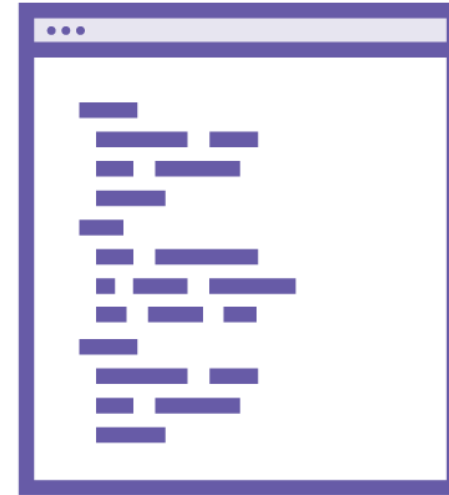


Tokens

Decoder

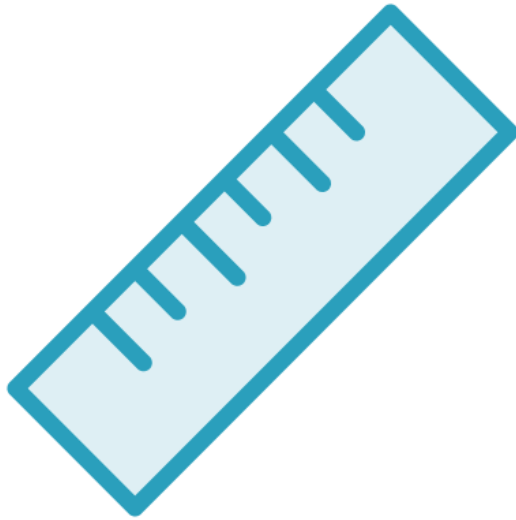


Convert raw into encoded data

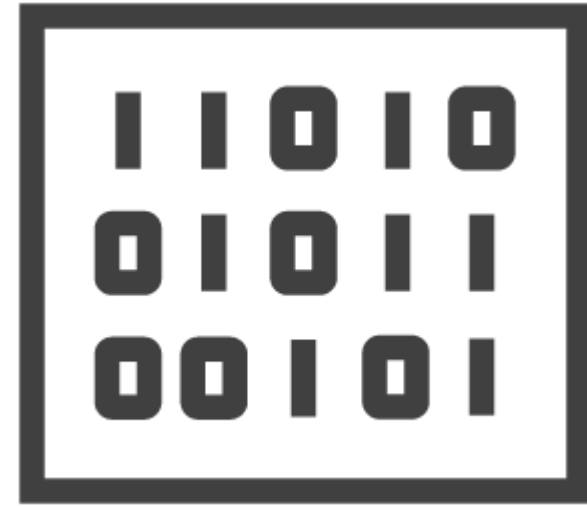


URL, HTML, Base64

Comparer

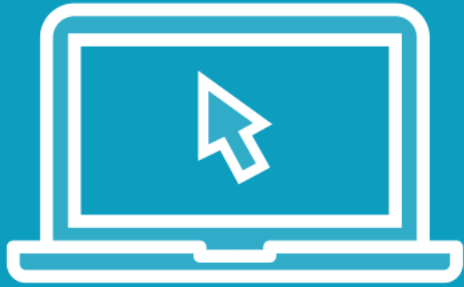


Visual diff



Words or bytes

Demo



Repeater to Your Rescue



Repeater Panels

Request

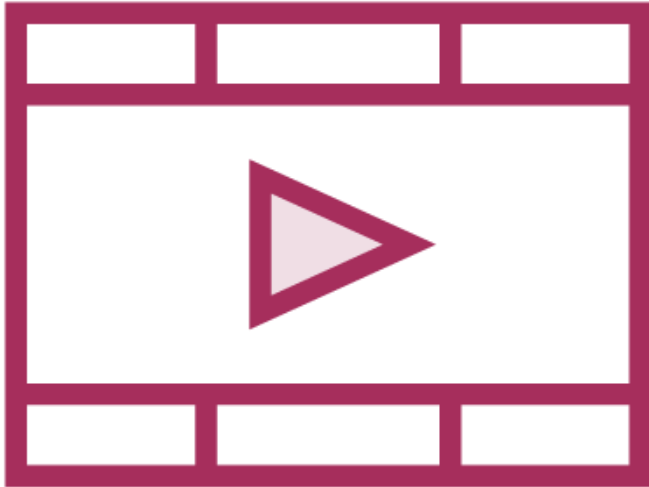
Response



Go



Repeater Panel Details



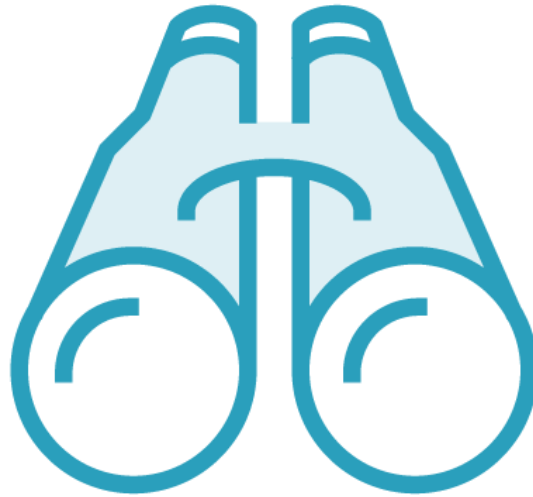
Message Editor **Request** details
(Raw, Params, Headers, Hex)



Message Editor **Response** details
(Raw, Headers, Hex, HTML, Render)



Repeater Search Box



Search



Demo



Intruder for the Win



Intruder Tabs

Target

Positions

Payloads

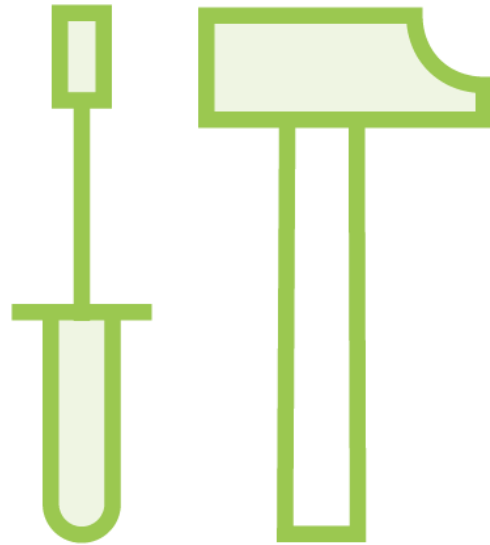
Options



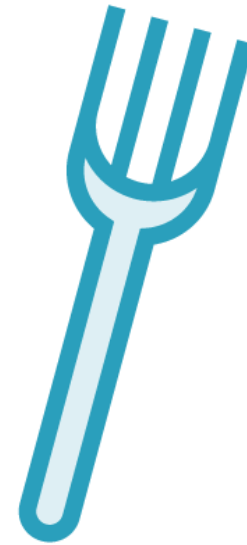
Payload Attack Types



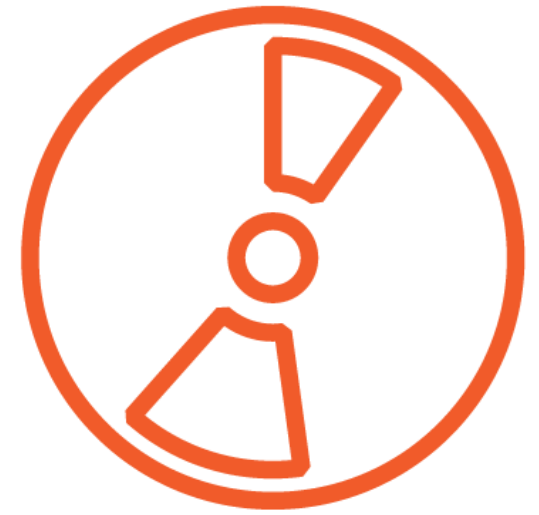
Sniper



Battering Ram

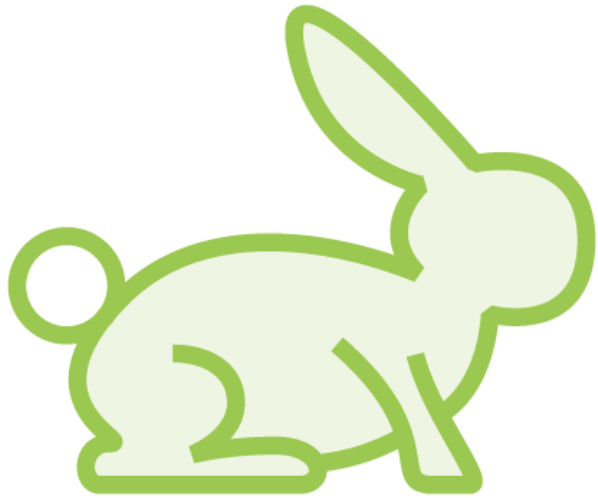


Pitchfork



Cluster Bomb

Actively Scan your Intruder Positions

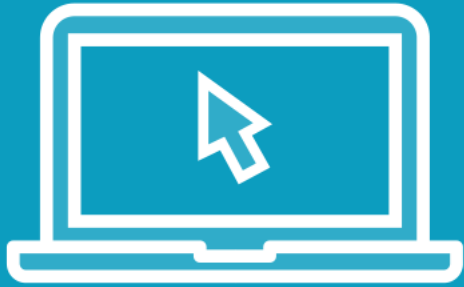


Active Scanner



Insertion Points

Demo



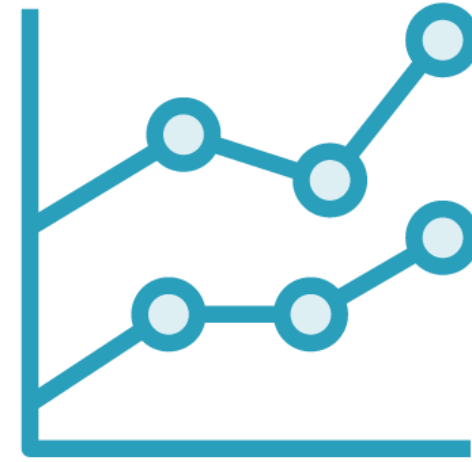
Sequencer for Your Tokens



Purpose of Sequencer



Degree of randomness



Large sample of tokens

Sequencer Sub-tabs



Live capture



Manual load



Analysis options



Demo



Decoder is Delightful



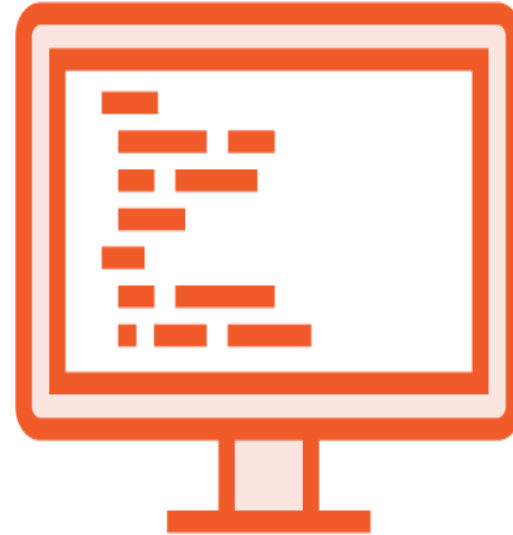
Encode/Decode



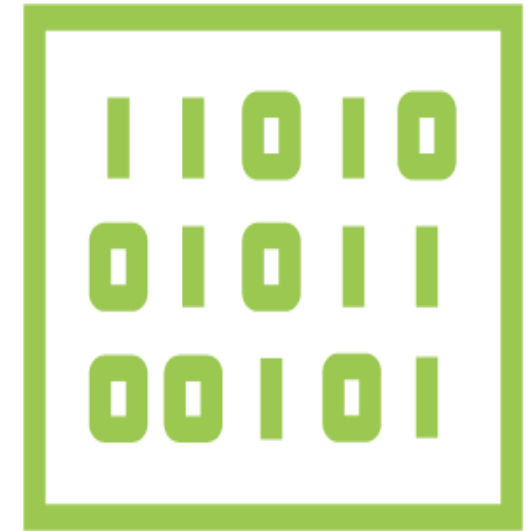
URL



HTML

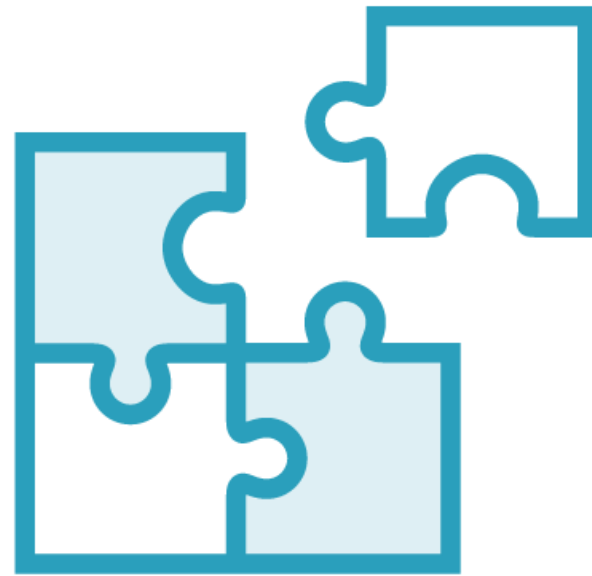


Base64



Binary

Demo



Comparer Assist



Why Compare?

Message changes

Username enumeration

Privilege escalation

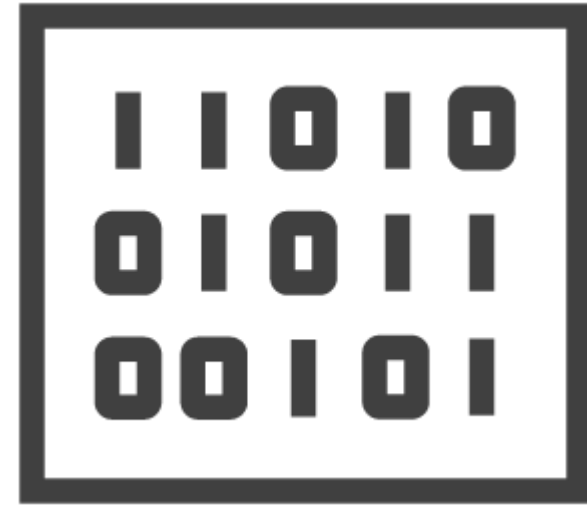
Injection attack responses



Compare Messages



Word compare



Byte compare

How to Compare



Contextual

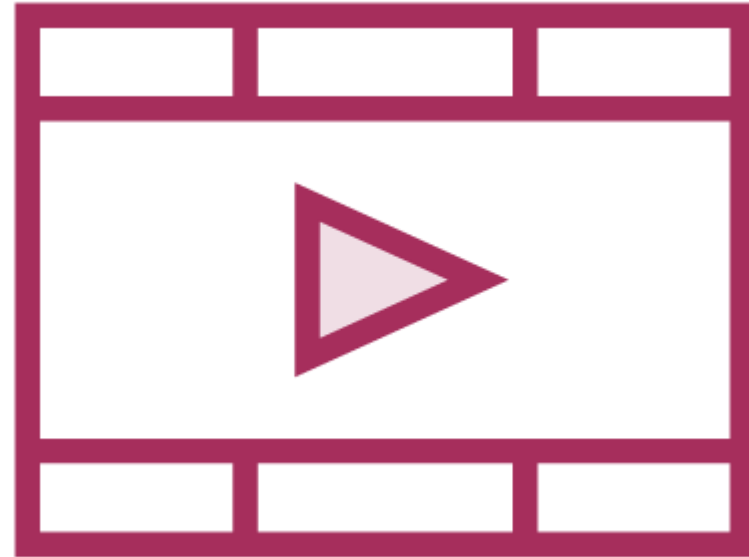
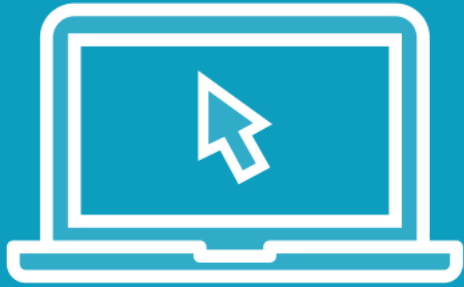


File load



Copy/paste

Demo



Summary



Analysis of results complete

Build your report

