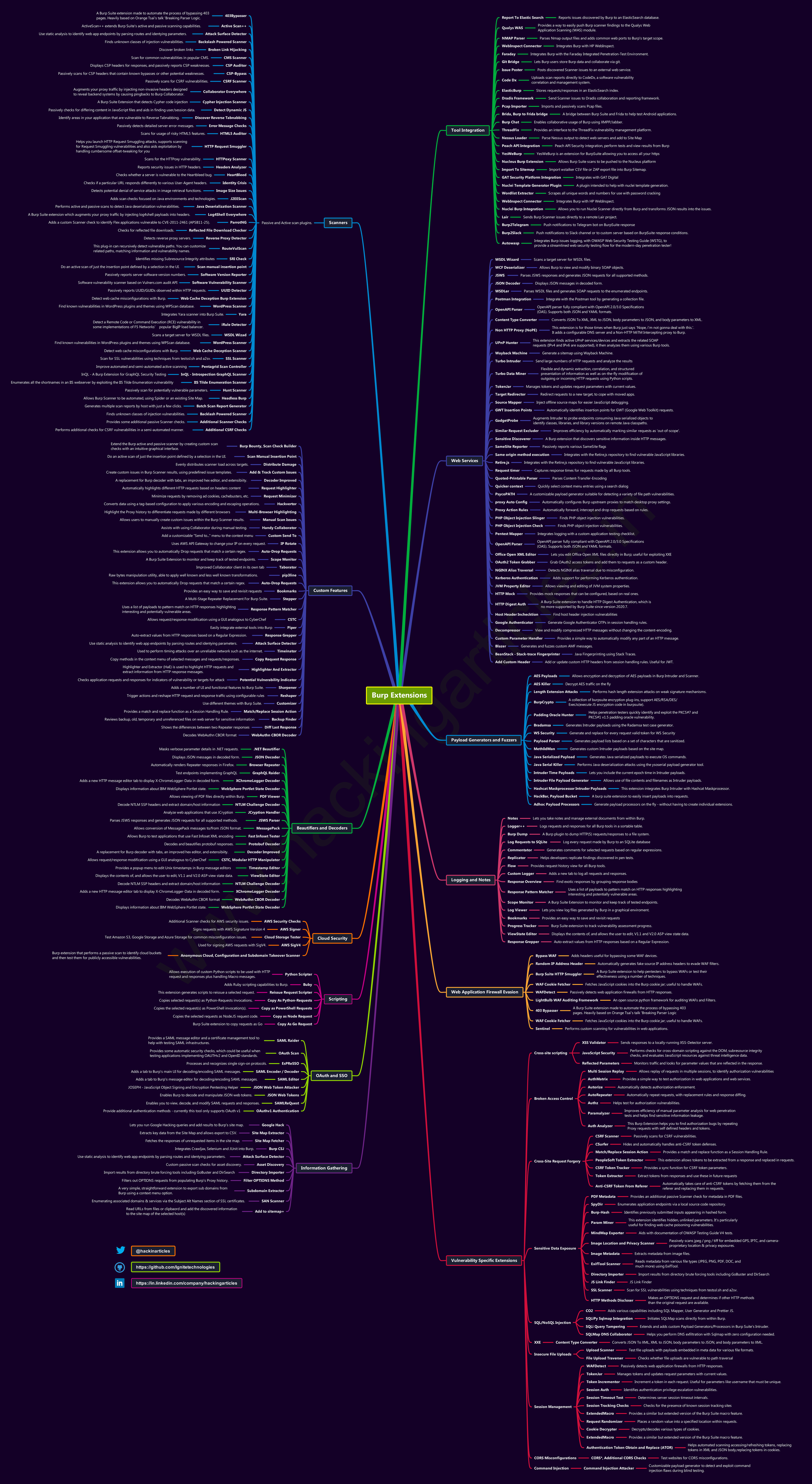
Burp Extensions
Scanners
Passive and Active scan plugins.
403Bypasser
A Burp Suite extension made to automate the process of bypassing 403 pages. Heavily based on Orange Tsai's talk 'Breaking Parser Logic.
Active Scan++
ActiveScan++ extends Burp Suite's active and passive scanning capabilities.
Attack Surface Detector
Use static analysis to identify web app endpoints by parsing routes and identying parameters.
Backslash Powered Scanner
Finds unknown classes of injection vulnerabilities.
Broken Link Hijacking
Discover broken links
CMS Scanner
Scan for common vulnerabilities in popular CMS.
CSP Auditor
Displays CSP headers for responses, and passively reports CSP weaknesses.
CSP-Bypass
Passively scans for CSP headers that contain known bypasses or other potential weaknesses.
CSRF Scanner
Passively scans for CSRF vulnerabilities.
Collaborator Everywhere
Augments your proxy traffic by injecting non-invasive headers designed to reveal backend systems by causing pingbacks to Burp Collaborator.
Cypher Injection Scanner
A Burp Suite Extension that detects Cypher code injection
Detect Dynamic JS
Passively checks for differing content in JavaScript files and aids in finding user/session data.
Discover Reverse Tabnabbing
Identify areas in your application that are vulnerable to Reverse Tabnabbing.
Error Message Checks
Passively detects detailed server error messages.
HTML5 Auditor
Scans for usage of risky HTML5 features.
HTTP Request Smuggler
Helps you launch HTTP Request Smuggling attacks, supports scanning for Request Smuggling vulnerabilities and also aids exploitation by handling cumbersome offset-tweaking for you
HTTPoxy Scanner
Scans for the HTTPoxy vulnerability.
Headers Analyzer
Reports security issues in HTTP headers.
HeartBleed
Checks whether a server is vulnerable to the Heartbleed bug.
Identity Crisis
Checks if a particular URL responds differently to various User-Agent headers.
Image Size Issues
Detects potential denial of service attacks in image retrieval functions.
J2EEScan
Adds scan checks focused on Java environments and technologies.
Java Deserialization Scanner
Performs active and passive scans to detect Java deserialization vulnerabilities.
Log4Shell Everywhere
A Burp Suite extension which augments your proxy traffic by injecting log4shell payloads into headers.
ParrotNG
Adds a custom Scanner check to identify Flex applications vulnerable to CVE-2011-2461 (APSB11-25).
Reflected File Download Checker
Checks for reflected file downloads.
Reverse Proxy Detector
Detects reverse proxy servers.
RouteVulScan
This plug-in can recursively detect vulnerable paths. You can customize related paths, matching information and vulnerability names.
SRI Check
Identifies missing Subresource Integrity attributes
Scan manual insertion point
Do an active scan of just the insertion point defined by a selection in the UI.
Software Version Reporter
Passively reports server software version numbers.
Software Vulnerability Scanner
Software vulnerability scanner based on Vulners.com audit API.
UUID Detector
Passively reports UUID/GUIDs observed within HTTP requests.
Web Cache Deception Burp Extension
Detect web cache misconfigurations with Burp.
WordPress Scanner
Find known vulnerabilities in WordPress plugins and themes using WPScan database.
Yara
Integrates Yara scanner into Burp Suite.
iRule Detector
Detect a Remote Code or Command Execution (RCE) vulnerability in some implementations of F5 Networks' popular BigIP load balancer.
WSDL Wizad
Scans a target server for WSDL files.
Wordpress Scanner
Find known vulnerabilities in WordPress plugins and themes using WPScan database.
Web Cache Deception Scanner
Detect web cache misconfigurations with Burp.
SSL Scanner
Scan for SSL vulnerabilities using techniques from testssl.sh and a2sv.
Pentagrid Scan Controller
Improve automated and semi-automated active scanning
InQL - Introspectin GraphQL Scanner
InQL - A Burp Extension for GraphQL Security Testing
IIS Tilde Enumeration Scanner
Enumerates all the shortnames in an IIS webserver by exploiting the IIS Tilde Enumeration vulnerability
Hunt Scanner
Passively scan for potentially vulnerable parameters.
Headless Burp
Allows Burp Scanner to be automated, using Spider or an existing Site Map.
Batch Scan Report Generator
Generates multiple scan reports by host with just a few clicks.
Backlash Powered Scanner
Finds unknown classes of injection vulnerabilities.
Additional Scanner Checks
Provides some additional passive Scanner checks.
Additional CSRF Checks
Performs additional checks for CSRF vulnerabilities in a semi-automated manner.
Custom Features
Burp Bounty, Scan Check Builder
Extend the Burp active and passive scanner by creating custom scan checks with an intuitive graphical interface.
Scan Manual Insertion Point
Do an active scan of just the insertion point defined by a selection in the UI.
Distribute Damage
Evenly distributes scanner load across targets.
Add & Track Custom Issues
Create custom issues in Burp Scanner results, using predefined issue templates.
Decoder Improved
A replacement for Burp decoder with tabs, an improved hex editor, and extensibility.
Request Highlighter
Automatically highlights different HTTP requests based on headers content
Request Minimizer
Minimize requests by removing ad cookies, cachebusters, etc.
Hackvertor
Converts data using a tag-based configuration to apply various encoding and escaping operations.
Multi-Browser Highlighting
Highlight the Proxy history to differentiate requests made by different browsers
Manual Scan Issues
Allows users to manually create custom issues within the Burp Scanner results.
Handy Collaborator
Assists with using Collaborator during manual testing.
Custom Send To
Add a customizable "Send to..." menu to the context menu
IP Rotate
Uses AWS API Gateway to change your IP on every request.
Auto-Drop Requests
This extension allows you to automatically Drop requests that match a certain regex.
Scope Monitor
A Burp Suite Extension to monitor and keep track of tested endpoints.
Taborator
Improved Collaborator client in its own tab
pip3line
Raw bytes manipulation utility, able to apply well known and less well known transformations.
Auto-Drop Requests
This extension allows you to automatically Drop requests that match a certain regex.
Bookmarks
Provides an easy way to save and revisit requests
Stepper
A Multi-Stage Repeater Replacement For Burp Suite.
Response Pattern Matcher
Uses a list of payloads to pattern match on HTTP responses highlighting interesting and potentially vulnerable areas.
CSTC
Allows request/response modification using a GUI analogous to CyberChef
Piper
Easily integrate external tools into Burp
Response Grepper
Auto-extract values from HTTP responses based on a Regular Expression.
Attack Surface Detector
Use static analysis to identify web app endpoints by parsing routes and identying parameters.
Timeinator
Used to perform timing attacks over an unreliable network such as the internet.
Copy Request Response
Copy methods in the context menu of selected messages and requests/responses.
Highlighter And Extractor
Highlighter and Extractor (HaE) is used to highlight HTTP requests and extract information from HTTP response messages.
Potential Vulnerability Indicator
Checks application requests and responses for indicators of vulnerability or targets for attack
Sharpener
Adds a number of UI and functional features to Burp Suite.
Reshaper
Trigger actions and reshape HTTP request and response traffic using configurable rules
Customizer
Use different themes with Burp Suite.
Match/Replace Session Action
Provides a match and replace function as a Session Handling Rule.
Backup Finder
Reviews backup, old, temporary and unreferenced files on web server for sensitive information
Diff Last Response
Shows the differences between two Repeater responses
WebAuthn CBOR Decoder
Decodes WebAuthn CBOR format
Beautifiers and Decoders
.NET Beautifier
Masks verbose parameter details in .NET requests.
JSON Decoder
Displays JSON messages in decoded form.
Browser Repeater
Automatically renders Repeater responses in Firefox.
GraphQL Raider
Test endpoints implementing GraphQL
XChromeLogger Decoder
Adds a new HTTP message editor tab to display X-ChromeLogger-Data in decoded form.
WebSphere Portlet State Decoder
Displays information about IBM WebSphere Portlet state.
PDF Viewer
Allows viewing of PDF files directly within Burp.
NTLM Challenge Decoder
Decode NTLM SSP headers and extract domain/host information
JCryption Handler
Analyze web applications that use JCryption
JSWS Parser
Parses JSWS responses and generates JSON requests for all supported methods.
MessagePack
Allows conversion of MessagePack messages to/from JSON format.
Fast Infoset Tester
Allows Burp to test applications that use Fast Infoset XML encoding
Protobuf Decoder
Decodes and beautifies protobuf responses.
Decoder Improved
A replacement for Burp decoder with tabs, an improved hex editor, and extensibility.
CSTC, Modular HTTP Manipulator
Allows request/response modification using a GUI analogous to CyberChef
Timestamp Editor
Provides a popup menu to edit Unix timestamps in Burp message editors
ViewState Editor
Displays the contents of, and allows the user to edit, V1.1 and V2.0 ASP view state data.
NTLM Challenge Decoder
Decode NTLM SSP headers and extract domain/host information
XChromeLogger Decoder
Adds a new HTTP message editor tab to display X-ChromeLogger-Data in decoded form.
WebAuthn CBOR Decoder
Decodes WebAuthn CBOR format
WebSphere Portlet State Decoder
Displays information about IBM WebSphere Portlet state.
Cloud Security
AWS Security Checks
Additional Scanner checks for AWS security issues.
AWS Signer
Signs requests with AWS Signature Version 4
Cloud Storage Tester
Test Amazon S3, Google Storage and Azure Storage for common misconfiguration issues.
AWS SigV4
Used for signing AWS requests with SigV4.
Anonymous Cloud, Configuration and Subdomain Takeover Scanner
Burp extension that performs a passive scan to identify cloud buckets and then test them for publicly accessible vulnerabilities.
Scripting
Python Scripter
Allows execution of custom Python scripts to be used with HTTP request and responses plus handling Macro messages.
Ruby
Adds Ruby scripting capabilities to Burp.
Reissue Request Scripter
This extension generates scripts to reissue a selected request.
Copy As Python-Requests
Copies selected request(s) as Python-Requests invocations.
Copy as PowerShell Requests
Copies the selected request(s) as PowerShell invocation(s).
Copy as Node Request
Copies the selected requests as NodeJS request code.
Copy As Go Request
Burp Suite extension to copy requests as Go
OAuth and SSO
SAML Raider
Provides a SAML message editor and a certificate management tool to help with testing SAML infrastructures.
OAuth Scan
Provides some automatic security checks, which could be useful when testing applications implementing OAUTH2 and OpenID standards.
ExPReSSO
Processes and recognizes single sign-on protocols.
SAML Decoder / Decoder
Adds a tab to Burp's main UI for decoding/encoding SAML messages.
SAML Editor
Adds a tab to Burp's message editor for decoding/encoding SAML messages.
JSON Web Token Attacker
JOSEPH - JavaScript Object Signing and Encryption Pentesting Helper
JSON Web Tokens
Enables Burp to decode and manipulate JSON web tokens.
SAMLReQuest
Enables you to view, decode, and modify SAML requests and responses.
OAuthv1 Authentication
Provide additional authentication methods - currently this tool only supports OAuth v1
Information Gathering
Google Hack
Lets you run Google Hacking queries and add results to Burp's site map.
Site Map Extractor
Extracts key data from the Site Map and allows export to CSV.
Site Map Fetcher
Fetches the responses of unrequested items in the site map.
Burp CSJ
Integrates Crawljax, Selenium and JUnit into Burp.
Attack Surface Detector
Use static analysis to identify web app endpoints by parsing routes and identying parameters.
Asset Discovery
Custom passive scan checks for asset discovery.
Directory Importer
Import results from directory brute forcing tools including GoBuster and DirSearch
Filter OPTIONS Method
Filters out OPTIONS requests from populating Burp's Proxy history.
Subdomain Extractor
A very simple, straightforward extension to export sub domains from Burp using a context menu option.
SAN Scanner
Enumerating associated domains & services via the Subject Alt Names section of SSL certificates.
Add to sitemap+
Read URLs from files or clipboard and add the discovered information to the site map of the selected host(s)
Tool Integration
Report To Elastic Search
Reports issues discovered by Burp to an ElasticSearch database.
Qualys WAS
Provides a way to easily push Burp scanner findings to the Qualys Web Application Scanning (WAS) module
NMAP Parser
Parses Nmap output files and adds common web ports to Burp's target scope.
WebInspect Connector
Integrates Burp with HP WebInspect.
Faraday
Integrates Burp with the Faraday Integrated Penetration-Test Environment.
Git Bridge
Lets Burp users store Burp data and collaborate via git.
Issue Poster
Posts discovered Scanner issues to an external web service.
Code Dx
Uploads scan reports directly to CodeDx, a software vulnerability correlation and management system.
ElasticBurp
Stores requests/responses in an ElasticSearch index.
Dradis Framework
Send Scanner issues to Dradis collaboration and reporting framework.
Pcap Importer
Imports and passively scans Pcap files.
Brida, Burp to Frida bridge
A bridge between Burp Suite and Frida to help test Android applications.
Burp Chat
Enables collaborative usage of Burp using XMPP/Jabber.
ThreadFix
Provides an interface to the ThreadFix vulnerability management platform.
Nessus Loader
Parse Nessus output to detect web servers and add to Site Map
Peach API Integration
Peach API Security integration, perform tests and view results from Burp
YesWeBurp
YesWeBurp is an extension for BurpSuite allowing you to access all your https
Nucleus Burp Extension
Allows Burp Suite scans to be pushed to the Nucleus platform
Import To Sitemap
Import wtsatker CSV file or ZAP export file into Burp Sitemap.
GAT Security Platform Integration
Integrates with GAT Digital
Nuclei Template Generator Plugin
A plugin intended to help with nuclei template generation.
Wordlist Extractor
Scrapes all unique words and numbers for use with password cracking
WebInspect Connector
Integrates Burp with HP WebInspect.
Nuclei Burp Integration
Allows you to run Nuclei Scanner directly from Burp and transforms JSON results into the issues.
Lair
Sends Burp Scanner issues directly to a remote Lair project.
Burp2Telegram
Push notifications to Telegram bot on BurpSuite response
Burp2Slack
Push notifications to Slack channel or to custom server based on BurpSuite response conditions.
Autowasp
Integrates Burp issues logging, with OWASP Web Security Testing Guide (WSTG), to provide a streamlined web security testing flow for the modern-day penetration tester!
Web Services
WSDL Wizard
Scans a target server for WSDL files.
WCF Deserializer
Allows Burp to view and modify binary SOAP objects.
JSWS
Parses JSWS responses and generates JSON requests for all supported methods.
JSON Decoder
Displays JSON messages in decoded form.
WSDLer
Parses WSDL files and generates SOAP requests to the enumerated endpoints.
Postman Integration
Integrate with the Postman tool by generating a collection file.
OpenAPI Parser
OpenAPI parser fully compliant with OpenAPI 2.0/3.0 Specifications (OAS). Supports both JSON and YAML formats.
Content Type Converter
Converts JSON To XML, XML to JSON, body parameters to JSON, and body parameters to XML.
Non HTTP Proxy (NoPE)
This extension is for those times when Burp just says 'Nope, i'm not gonna deal with this.'. It adds a configurable DNS server and a Non-HTTP MITM Intercepting proxy to Burp.
UPnP Hunter
This extension finds active UPnP services/devices and extracts the related SOAP requests (IPv4 and IPv6 are supported), it then analyzes them using various Burp tools.
Wayback Machine
Generate a sitemap using Wayback Machine.
Turbo Intruder
Send large numbers of HTTP requests and analyze the results
Turbo Data Miner
Flexible and dynamic extraction, correlation, and structured presentation of information as well as on-the-fly modification of outgoing or incoming HTTP requests using Python scripts.
TokenJar
Manages tokens and updates request parameters with current values.
Target Redirector
Redirect requests to a new target, to cope with moved apps.
Source Mapper
Inject offline source maps for easier JavaScript debugging.
GWT Insertion Points
Automatically identifies insertion points for GWT (Google Web Toolkit) requests.
GadgetProbe
Augments Intruder to probe endpoints consuming Java serialized objects to identify classes, libraries, and library versions on remote Java classpaths.
Similar Request Excluder
Improves efficiency by automatically marking similar requests as 'out-of-scope'.
Sensitive Discoverer
A Burp extension that discovers sensitive information inside HTTP messages.
SameSite Reporter
Passively reports various SameSite flags
Same origin method execution
Integrates with the Retire.js repository to find vulnerable JavaScript libraries.
Retire.js
Integrates with the Retire.js repository to find vulnerable JavaScript libraries.
Request timer
Captures response times for requests made by all Burp tools.
Quoted-Printable Parser
Parses Content-Transfer-Encoding
Quicker context
Quickly select context menu entries using a search dialog
PsycoPATH
A customizable payload generator suitable for detecting a variety of file path vulnerabilities.
proxy Auto Config
Automatically configures Burp upstream proxies to match desktop proxy settings.
Proxy Action Rules
Automatically forward, intercept and drop requests based on rules.
PHP Object Injection Slinger
Finds PHP object injection vulnerabilities.
PHP Object Injection Check
Finds PHP object injection vulnerabilities.
Pentest Mapper
Integrates logging with a custom application testing checklist.
OpenAPI Parser
OpenAPI parser fully compliant with OpenAPI 2.0/3.0 Specifications (OAS). Supports both JSON and YAML formats.
Office Open XML Editor
Lets you edit Office Open XML files directly in Burp; useful for exploiting XXE
OAuth2 Token Grabber
Grab OAuth2 access tokens and add them to requests as a custom header.
NGINX Alias Traversal
Detects NGINX alias traversal due to misconfiguration.
Kerberos Authentication
Adds support for performing Kerberos authentication.
JVM Property Editor
Allows viewing and editing of JVM system properties.
HTTP Mock
Provides mock responses that can be configured, based on real ones.
HTTP Digest Auth
A Burp Suite extension to handle HTTP Digest Authentication, which is no more supported by Burp Suite since version 2020.7.
Host Header Incheckition
Find host header injection vulnerabilities
Google Authenticator
Generate Google Authenticator OTPs in session handling rules.
Decompressor
View and modify compressed HTTP messages without changing the content-encoding.
Custom Parameter Handler
Provides a simple way to automatically modify any part of an HTTP message.
Blazer
Generates and fuzzes custom AMF messages.
BeanStack - Stack-trace Fingerprinter
Java Fingerprinting using Stack Traces.
Add Custom Header
Add or update custom HTTP headers from session handling rules. Useful for JWT.
Payload Generators and Fuzzers
AES Payloads
Allows encryption and decryption of AES payloads in Burp Intruder and Scanner.
AES Killer
Decrypt AES traffic on the fly
Length Extension Attacks
Performs hash length extension attacks on weak signature mechanisms.
BurpCrypto
A collection of burpsuite encryption plug-ins, support AES/RSA/DES/ Exec(s)(execute JS encryption code in burpsuite).
Padding Oracle Hunter
Helps penetration testers quickly identify and exploit the PKCS#7 and PKCS#1 v1.5 padding oracle vulnerability.
Bradamsa
Generates Intruder payloads using the Radamsa test case generator.
WS Security
Generate and replace for every request valid token for WS Security
Payload Parser
Generates payload lists based on a set of characters that are sanitized.
Meth0dMan
Generates custom Intruder payloads based on the site map.
Java Serialized Payload
Generates Java serialized payloads to execute OS commands.
Java Serial Killer
Performs Java deserialization attacks using the ysoserial payload generator tool.
Intruder Time Payloads
Lets you include the current epoch time in Intruder payloads.
Intruder File Payload Generator
Allows use of file contents and filenames as Intruder payloads.
Hashcat Maskprocessor Intruder Payloads
This extension integrates Burp Intruder with Hashcat Maskprocessor.
HackBar, Payload Bucket
A burp suite extension to easily insert payloads into requests.
Adhoc Payload Processors
Generate payload processors on the fly - without having to create individual extensions.
Logging and Notes
Notes
Lets you take notes and manage external documents from within Burp.
Logger++
Logs requests and responses for all Burp tools in a sortable table.
Burp Dump
A Burp plugin to dump HTTP(S) requests/responses to a file system.
Log Requests to SQLite
Log every request made by Burp to an SQLite database
Commentator
Generates comments for selected requests based on regular expressions.
Replicator
Helps developers replicate findings discovered in pen tests.
Flow
Provides request history view for all Burp tools.
Custom Logger
Adds a new tab to log all requests and responses.
Response Overview
Find exotic responses by grouping response bodies
Response Pattern Matcher
Uses a list of payloads to pattern match on HTTP responses highlighting interesting and potentially vulnerable areas.
Scope Monitor
A Burp Suite Extension to monitor and keep track of tested endpoints.
Log Viewer
Lets you view log files generated by Burp in a graphical enviroment.
Bookmarks
Provides an easy way to save and revisit requests
Progress Tracker
Burp Suite extension to track vulnerability assessment progress.
ViewState Editor
Displays the contents of, and allows the user to edit, V1.1 and V2.0 ASP view state data.
Response Grepper
Auto-extract values from HTTP responses based on a Regular Expression.
Web Application Firewall Evasion
Bypass WAF
Adds headers useful for bypassing some WAF devices.
Random IP Address Header
Automatically generates fake source IP address headers to evade WAF filters.
Burp Suite HTTP Smuggler
A Burp Suite extension to help pentesters to bypass WAFs or test their effectiveness using a number of techniques.
WAF Cookie Fetcher
Fetches JavaScript cookies into the Burp cookie jar; useful to handle WAFs.
WAFDetect
Passively detects web application firewalls from HTTP responses.
LightBulb WAF Auditing Framework
An open source python framework for auditing WAFs and Filters.
403 Bypasser
A Burp Suite extension made to automate the process of bypassing 403 pages. Heavily based on Orange Tsai's talk 'Breaking Parser Logic
WAF Cookie Fetcher
Fetches JavaScript cookies into the Burp cookie jar; useful to handle WAFs.
Sentinel
Performs custom scanning for vulnerabilities in web applications.
Vulnerability Specific Extensions
Cross-site scripting
XSS Validator
Sends responses to a locally-running XSS-Detector server.
JavaScript Security
Performs checks for cross-domain scripting against the DOM, subresource integrity checks, and evaluates JavaScript resources against threat intelligence data.
Reflected Parameters
Monitors traffic and looks for parameter values that are reflected in the response.
Broken Access Control
Multi Session Replay
Allows replay of requests in multiple sessions, to identify authorization vulnerabilities
AuthMatrix
Provides a simple way to test authorization in web applications and web services.
Autorize
Automatically detects authorization enforcement.
AutoRepeater
Automatically repeat requests, with replacement rules and response diffing.
Authz
Helps test for authorization vulnerabilities.
Paramalyzer
Improves efficiency of manual parameter analysis for web penetration tests and helps find sensitive information leakage.
Auth Analyzer
This Burp Extension helps you to find authorization bugs by repeating Proxy requests with self defined headers and tokens.
Cross-Site Request Forgery
CSRF Scanner
Passively scans for CSRF vulnerabilities.
CSurfer
Hides and automatically handles anti-CSRF token defenses.
Match/Replace Session Action
Provides a match and replace function as a Session Handling Rule.
PeopleSoft Token Extractor
This extension allows tokens to be extracted from a response and replaced in requests.
CSRF Token Tracker
Provides a sync function for CSRF token parameters.
Token Extractor
Extract tokens from responses and use these in future requests
Anti-CSRF Token From Referer
Automatically takes care of anti-CSRF tokens by fetching them from the referer and replacing them in requests.
Sensitive Data Exposure
PDF Metadata
Provides an additional passive Scanner check for metadata in PDF files.
SpyDir
Enumerates application endpoints via a local source code repository.
Burp-Hash
Identifies previously submitted inputs appearing in hashed form.
Param Miner
This extension identifies hidden, unlinked parameters. It's particularly useful for finding web cache poisoning vulnerabilities.
MindMap Exporter
Aids with documentation of OWASP Testing Guide V4 tests.
Image Location and Privacy Scanner
Passively scans jpeg / png / tiff for embedded GPS, IPTC, and camera-proprietary location & privacy exposures.
Image Metadata
Extracts metadata from image files.
ExifTool Scanner
Reads metadata from various file types (JPEG, PNG, PDF, DOC, and much more) using ExifTool.
Directory Importer
Import results from directory brute forcing tools including GoBuster and DirSearch
JS Link Finder
JS Link Finder
SSL Scanner
Scan for SSL vulnerabilities using techniques from testssl.sh and a2sv.
HTTP Methods Discloser
Makes an OPTIONS request and determines if other HTTP methods than the original request are available.
SQL/NoSQL Injection
CO2
Adds various capabilities including SQL Mapper, User Generator and Prettier JS.
SQLiPy Sqlmap Integration
Initiates SQLMap scans directly from within Burp.
SQLi Query Tampering
Extends and adds custom Payload Generators/Processors in Burp Suite's Intruder.
SQLMap DNS Collaborator
Helps you perform DNS exfiltration with Sqlmap with zero configuration needed.
XXE
Content Type Converter
Converts JSON To XML, XML to JSON, body parameters to JSON, and body parameters to XML.
Insecure File Uploads
Upload Scanner
Test file uploads with payloads embedded in meta data for various file formats.
File Upload Traverser
Checks whether file uploads are vulnerable to path traversal
Session Management
WAFDetect
Passively detects web application firewalls from HTTP responses.
TokenJar
Manages tokens and updates request parameters with current values.
Token Incrementor
Increment a token in each request. Useful for parameters like username that must be unique.
Session Auth
Identifies authentication privilege escalation vulnerabilities.
Session Timeout Test
Determines server session timeout intervals.
Session Tracking Checks
Checks for the presence of known session tracking sites
ExtendedMacro
Provides a similar but extended version of the Burp Suite macro feature.
Request Randomizer
Places a random value into a specified location within requests.
Cookie Decrypter
Decrypts/decodes various types of cookies.
ExtendedMacro
Provides a similar but extended version of the Burp Suite macro feature.
Authentication Token Obtain and Replace (ATOR)
Helps automated scanning accessing/refreshing tokens, replacing tokens in XML and JSON body/replacing tokens in cookies.
CORS Misconfigurations
CORS*, Additional CORS Checks
Test websites for CORS misconfigurations.
Command Injection
Command Injection Attacker
Customizable payload generator to detect and exploit command injection flaws during blind testing.
@hackinarticles
https://github.com/ignitetechnologies
https://in.linkedin.com/company/hackingarticles