- Customize burp behavior using your own or third party code
  - Burp Extensions
    - Extensions
      - .NET Beautifier
      - 403 Bypasser
      - 5GC API Parser
      - Active Scan++
      - Add & Track Custom Issues
      - Add Custom Header
      - Add to SiteMap+
      - Additional CSRF Checks
      - Additional Scanner Checks
      - Adhoc Payload Processors
      - AES Killer, decrypt AES traffic on the fly
      - AES Payloads
      - Anti-CSRF Token From Referer
      - Asset Discovery
      - Attack Surface Detector
      - Auth Analyzer
      - Authentication Token Obtain and Replace
      - AuthMatrix
      - Authz
      - Auto-Drop Requests
      - AutoRepeater
      - Autorize
      - Autowasp
      - AWS Security Checks
      - AWS Signer
      - AWS Sigv4
      - Backslash Powered Scanner
      - Backup Finder
      - Batch Scan Report Generator
      - BeanStack - Stack-trace Fingerprinter
      - Professional
      - Blazer
      - Bookmarks
      - Bradamsa
      - Brida, Burp to Frida bridge
      - Broken Link Hijacking
      - Professional
      - Browser Repeater
      - Buby
      - Professional
      - BugPoC
      - Burp Bounty, Scan Check Builder
      - Professional
      - Burp Chat
      - Burp CSJ
      - Burp Share Requests
      - Burp2Slack
      - Burp2Telegram
      - BurpCrypto, Encryption Payload Processor
      - BurpelFish
      - Burp-hash
      - Professional
      - BurpSmartBuster
      - Bypass WAF
      - Carbonator
      - Clipboard Repeater
      - Cloud Storage Tester
      - CMS Scanner
      - CO2
      - Code Dx
      - Collabfiltrator
      - Professional

Collaborator Everywhere
Professional
Command Injection Attacker
Commentator
Content Type Converter
Cookie Decrypter
Professional
Copy As Go Request
Copy as Node Request
Copy as PowerShell Requests
Copy As Python-Requests
Copy Request Response
CORS*, Additional CORS Checks
Professional
Crypto Messages Handler
Cryptojacking Mine Sweeper
Professional
CSP Auditor
CSP-Bypass
Professional
CSRF Scanner
Professional
CSRF Token Tracker
CSTC, Modular HTTP Manipulator
CSurfer
Custom Logger
Custom Parameter Handler
Custom Send To
CustomDeserializer
Customizer
CVSS Calculator
Cypher Injection Scanner
Decoder Improved
Decompressor
Detect Dynamic JS
Professional
Diff Last Response
Directory Importer
Discover Reverse Tabnabbing
Distribute Damage
Dradis Framework
Professional
ElasticBurp
Error Message Checks
Professional
EsPReSSO
ExifTool Scanner
ExtendedMacro
Faraday
Fast Infoset Tester
File Upload Traverser
Professional
Filter Options Method
Flow
Freddy, Deserialization Bug Finder
Professional
GadgetProbe
GAT Security Platform Integration
Professional
Git Bridge
Google Authenticator
Google Hack
GraphQL Raider
Professional
GWT Insertion Points
HackBar, Payload Bucket

Contents
Request/Response
Issues
Advisory
Site Map
define in scope targets for your current work.This configuration affects the behavior of tool through out the suite
Target Scope
Scope
OS command injection
SQL injection
SQL injection (second order)
ASP.NET tracing enabled
File path traversal
XML external entity injection
LDAP injection
XPath injection
XML injection
ASP.NET debugging enabled
HTTP PUT method is enabled
Out-of-band resource load (HTTP)
File path manipulation
PHP code injection
Server-side JavaScript code injection
Perl code injection
Ruby code injection
Python code injection
Expression Language injection
Unidentified code injection
Server-side template injection
SSI injection

Hackvertor
Handy Collaborator
Hashcat Maskprocessor Intruder Payloads
Headers Analyzer
Professional
Headless Burp
HeartBleed
Highlighter And Extractor
HTML5 Auditor
HTTP Digest Auth
HTTP Methods Discloser
HTTP Mock
HTTP Request Smuggler
HTTPoxy Scanner
Hunt Scanner
Identity Crisis
Professional
IIS Tilde Enumeration Scanner
Professional
Image Location and Privacy Scanner
Professional
Image Metadata
Image Size Issues
Import To Sitemap
InQL - Introspection GraphQL Scanner
Intruder Time Payloads
IP Rotate
iRule Detector
Professional
Issue Poster
Professional
J2EEScan
Java Deserialization Scanner
Java Serial Killer
Java Serialized Payloads
JavaScript Security
Professional
JCryption Handler
JQ
JS Link Finder
Professional
JS Miner
Professional
JSON Decoder
JSON Query
JSON Web Token Attacker
JSON Web Tokens
JSWS Parser
JVM Property Editor
JWT Editor
Kerberos Authentication
Lair
Professional
Length Extension Attacks
LightBulb WAF Auditing Framework
Log Requests to SQLite
Log Viewer
Log4Shell Everywhere
Professional
Logger++
Manual Scan Issues
Professional
Match/Replace Session Action
MessagePack
Meth0dMan

Cross-site scripting (stored)
HTTP request smuggling
Client-side desync
Web cache poisoning
HTTP response header injection
Cross-site scripting (reflected)
Client-side template injection
Cross-site scripting (DOM-based)
Cross-site scripting (reflected DOM-based)
Cross-site scripting (stored DOM-based)
Client-side prototype pollution
JavaScript injection (DOM-based)
JavaScript injection (reflected DOM-based)
JavaScript injection (stored DOM-based)
Path-relative style sheet import
Client-side SQL injection (DOM-based)
Client-side SQL injection (reflected DOM-based)
Client-side SQL injection (stored DOM-based)
WebSocket URL poisoning (DOM-based)
WebSocket URL poisoning (reflected DOM-based)
WebSocket URL poisoning (stored DOM-based)
Local file path manipulation (DOM-based)
Local file path manipulation (reflected DOM-based)
Local file path manipulation (stored DOM-based)
Client-side XPath injection (DOM-based)
Client-side XPath injection (reflected DOM-based)
Client-side XPath injection (stored DOM-based)
Client-side JSON injection (DOM-based)
Client-side JSON injection (reflected DOM-based)
Client-side JSON injection (stored DOM-based)
Flash cross-domain policy
Silverlight cross-domain policy
Cross-origin resource sharing
Cross-origin resource sharing: arbitrary origin trusted
Cross-origin resource sharing: unencrypted origin trusted
Cross-origin resource sharing: all subdomains trusted
Cross-site request forgery
SMTP header injection
JWT signature not verified
JWT none algorithm supported
JWT self-signed JWK header supported
JWT weak HMAC secret
JWT arbitrary jku header supported
JWT arbitrary x5u header supported
Cleartext submission of password
External service interaction (DNS)
External service interaction (HTTP)
External service interaction (SMTP)
Referer-dependent response
Spoofable client IP address
User agent-dependent response
Password returned in later response
Password submitted using GET method
Password returned in URL query string
SQL statement in request parameter
Cross-domain POST
ASP.NET ViewState without MAC enabled
XML entity expansion
Long redirection response
Serialized object in HTTP message
Duplicate cookies set
Input returned in response (stored)
Input returned in response (reflected)
Suspicious input transformation (reflected)
Suspicious input transformation (stored)

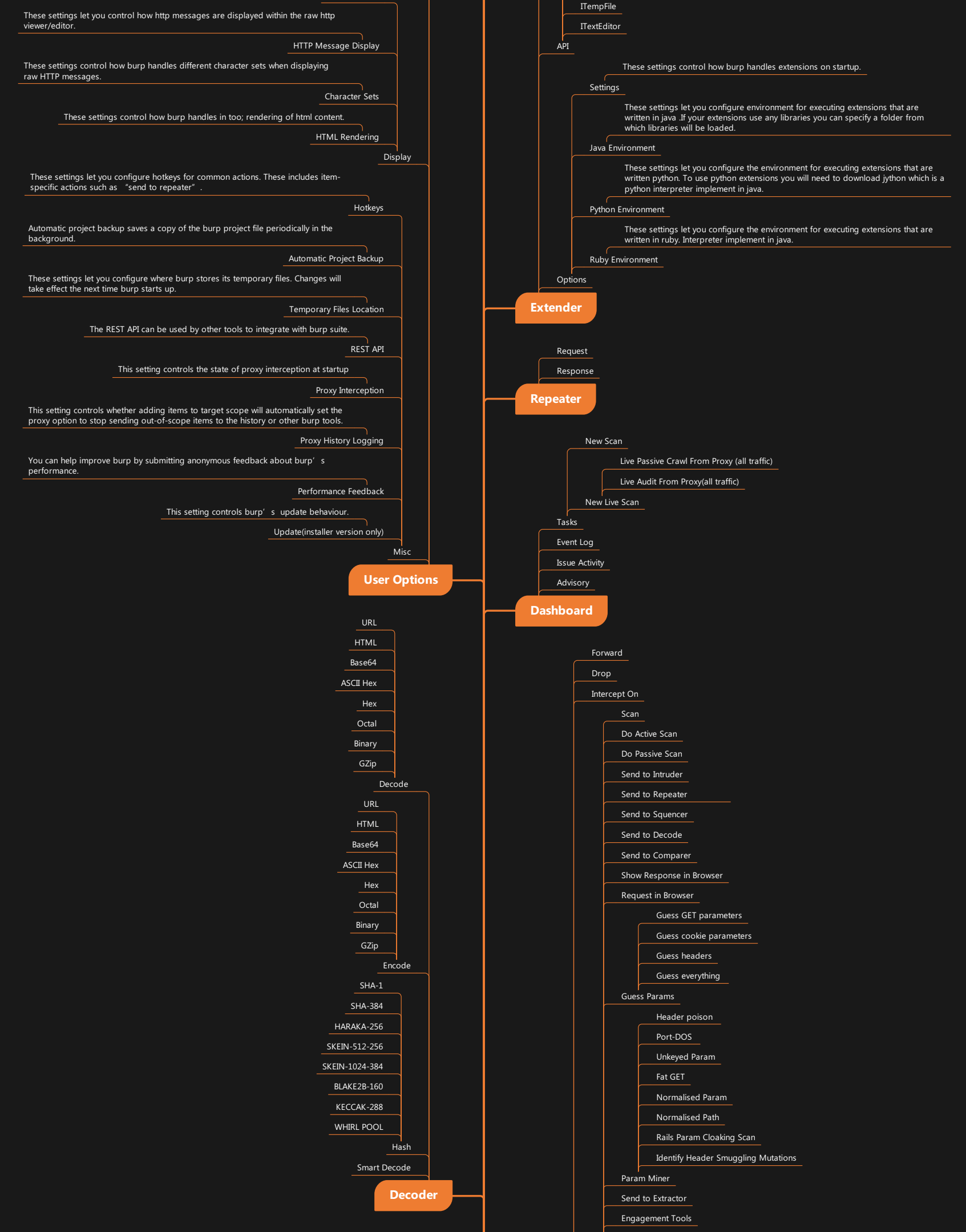
MindMap Exporter
Multi Session Replay
Multi-Browser Highlighting
Nessus Loader
NGINX Alias Traversal
Professional
NMAP Parser
Non HTTP Proxy (NoPE)
NoSQLi Scanner
Professional
Notes
NTLM Challenge Decoder
Nuclei Burp Integration
Nuclei Template Generator Plugin
Nucleus Burp Extension
Professional
OAUTH Scan
OAuth2 Token Grabber
OAuthv1 Authentication
Office Open XML Editor
OpenAPI Parser
Padding Oracle Hunter
Param Miner
Paramalyzer
ParrotNG
Payload Parser
Pcap Importer
Professional
PDF Metadata
Professional
PDF Viewer
Peach API Integration
Pentagrid Scan Controller
Professional
Pentest Mapper
PeopleSoft Token Extractor
PHP Object Injection Check
PHP Object Injection Slinger
pip3line
Piper
Postman Integration
Potential Vulnerability Indicator
Progress Tracker
Protobuf Decoder
Proxy Action Rules
Proxy Auto Config
PsychoPATH
Python Scripter
Qualys WAS
Professional
Quicker Context
Quoted-Printable Parser
Professional
Random IP Address Header
Reflected File Download Checker
Reflected Parameters
Professional
Reissue Request Scripter
Replicator
Report To Elastic Search
Professional
Request Highlighter
Request Randomizer
Request Timer
Reshaper

www.hackingarticles.in

Request URL override
Vulnerable JavaScript dependency
Open redirection (reflected)
Open redirection (stored)
Open redirection (DOM-based)
Open redirection (reflected DOM-based)
Open redirection (stored DOM-based)
TLS cookie without secure flag set
Cookie scoped to parent domain
Cross-domain Referer leakage
Cross-domain script include
Cookie without HttpOnly flag set
Session token in URL
Password field with autocomplete enabled
Password value set in cookie
File upload functionality
Frameable response (potential Clickjacking)
Browser cross-site scripting filter disabled
HTTP TRACE method is enabled
Cookie manipulation (DOM-based)
Cookie manipulation (reflected DOM-based)
Cookie manipulation (stored DOM-based)
Ajax request header manipulation (DOM-based)
Ajax request header manipulation (reflected DOM-based)
Ajax request header manipulation (stored DOM-based)
Denial of service (DOM-based)
Denial of service (reflected DOM-based)
Denial of service (stored DOM-based)
HTML5 web message manipulation (DOM-based)
HTML5 web message manipulation (reflected DOM-based)
HTML5 web message manipulation (stored DOM-based)
HTML5 storage manipulation (DOM-based)
HTML5 storage manipulation (reflected DOM-based)
HTML5 storage manipulation (stored DOM-based)
Link manipulation (DOM-based)
Link manipulation (reflected DOM-based)
Link manipulation (stored DOM-based)
Link manipulation (reflected)
Link manipulation (stored)
Document domain manipulation (DOM-based)
Document domain manipulation (reflected DOM-based)
Document domain manipulation (stored DOM-based)
DOM data manipulation (DOM-based)
DOM data manipulation (reflected DOM-based)
DOM data manipulation (stored DOM-based)
CSS injection (reflected)
CSS injection (stored)
Client-side HTTP parameter pollution (reflected)
Client-side HTTP parameter pollution (stored)
Form action hijacking (reflected)
Form action hijacking (stored)
Database connection string disclosed
Source code disclosure
Backup file
Directory listing
Email addresses disclosed
Private IP addresses disclosed
Social security numbers disclosed
Credit card numbers disclosed
Private key disclosed
Robots.txt file
Json Web Key Set disclosed
JWT private key disclosed

Response Grepper
Response Overview
Response Pattern Matcher
Retire.js
Professional
Reverse Proxy Detector
RouteVulScan
Professional
Same Origin Method Execution
SameSite Reporter
Professional
SAML Editor
SAML Encoder / Decoder
SAML Raider
SAMLReQuest
San Scanner
Scan manual insertion point
Scope Monitor
Sensitive Discoverer
Professional
Sentinel
Professional
Session Auth
Professional
Session Timeout Test
Session Tracking Checks
Professional
Sharpener
Similar Request Excluder
Site Map Extractor
Site Map Fetcher
Software Version Reporter
Professional
Software Vulnerability Scanner
Professional
Source Mapper
SpyDir
SQLi Query Tampering
SQLiPy Sqlmap Integration
SQLMap DNS Collaborator
Professional
SRI Check
Professional
SSL Scanner
Stepper
Subdomain Extractor
Taborator
Professional
Target Redirector
ThreadFix
Professional
Timeinator, Time Based Attacker
Timestamp Editor
Token Extractor
Token Incrementor
TokenJar
Turbo Data Miner
Turbo Intruder
Upload Scanner
Professional
UPnP Hunter
UUID Detector
ViewState Editor

- Target
  - Issue Definations
    - Extension generated issue
    - Hidden HTTP 2
    - Mixed content
    - Strict transport security not enforced
    - Unencrypted communications
    - TLS certificate
    - Content type is not specified
    - Content type incorrectly stated
    - HTML uses unrecognized charset
    - HTML does not specify charset
    - Multiple content types specified
    - Base64-encoded data in parameter
    - Cacheable HTTPS response
- Comparer
  - This function lets you do a word or byte level comparison between different data. You can load ,paste or send data here from other tools and then select the comparison you want to perform
- Sequencer
  - Live Capture
    - Live capture options
      - These setting control the engine used for making http request and harvesting tokens
    - Token location within response
      - Select the location in the response where token appear.
    - Select live capture request
      - Send requests here from other tools to configure a live capture . select a request to use, configure the other options below, then click "start live capture"
  - Manual Load
    - This function allows you to load sequencer with a sample of tokens that you already obtained and then perform the statistical analysis on the sample.
  - Analysis Options
    - Token Analysis
      - Bit level analysis
      - Character level analysis
    - Token Handling
      - These settings control how tokens are handled during analysis
- Connections
  - Socks Proxy
    - These settings burp to use a socks proxy. This settings is applied at the tcp level and all outbound requests will be send via this proxy. If you configured rules for upstream http proxy servers , then requests to upstream proxies will be sent via the socks proxy configured here.
  - Upstream Proxy Servers
    - The following whether burp sends each outgoing request to a proxy server, or directly to the destination web server. The first rule that matches each destination host will be used. To send all traffic to a single proxy server. Create a rule with * as the destination host.
  - Platform Authentication
    - These settings let you configure burp to automatically carry out platform authentication to destination web servers.
  - TLS
    - Client TLS Certificates
      - These settings let you configure the client TLS certificates that burp will use when a destination host requests one. Burp will use the first certificate in the list whose list host configuration matches the name of the host being contacted.
    - Java TLS Options
      - These settings can be used to enable certain TLS features that might be needed to successfully connect to some servers.
  - User Interface
    - These settings let you control the appearance of burp’ s user interface.
- Bapp Store
  - YesWeBurp
  - Yara
  - XSS Validator
  - XChromeLogger Decoder
  - Wsdler
  - WSDL Wizard
  - WS Security
  - WordPress Scanner
  - Wordlist Extractor
  - WebInspect Connector
  - WebSphere Portlet State Decoder
  - WebAuthn CBOR Decoder
  - Web Cache Deception Scanner
  - WCF Deserializer
  - Wayback Machine
  - WAFDetect
  - WAF Cookie Fetcher
- IBurpCollaboratorClientContext
- IBurpCollaboratorInteraction
- IBurpExtender
- IBurpExtenderCallbacks
- IContextMenuFactory
- IContextMenuInvocation
- ICookie
- IExtensionHelpers
- IExtensionStateListener
- IHttpHeader
- IHttpListener
- IHttpRequestResponse
- IHttpRequestResponsePersisted
- IHttpRequestResponseWithMarkers
- IHttpService
- IInterceptedProxyMessage
- IIntruderAttack
- IIntruderPayloadGenerator
- IIntruderPayloadGeneratorFactory
- IIntruderPayloadProcessor
- IMenuItemHandler
- IMessageEditor
- IMessageEditorController
- IMessageEditorTab
- IMessageEditorTabFactory
- IParameter
- IProxyListener
- IRequestInfo
- IResponseInfo
- IResponseKeywords
- IResponseVariations
- IScanIssue
- IScannerCheck
- IScannerInsertionPoint
- IScannerInsertionPointProvider
- IScannerListener
- IScanQueueItem
- IScopeChangeListener
- ISessionHandlingAction
- ITab


These settings let you control how http messages are displayed within the raw http viewer/editor.
HTTP Message Display
These settings control how burp handles different character sets when displaying raw HTTP messages.
Character Sets
These settings control how burp handles in too; rendering of html content.
HTML Rendering
Display
These settings let you configure hotkeys for common actions. These includes item-specific actions such as "send to repeater".
Hotkeys
Automatic project backup saves a copy of the burp project file periodically in the background.
Automatic Project Backup
These settings let you configure where burp stores its temporary files. Changes will take effect the next time burp starts up.
Temporary Files Location
The REST API can be used by other tools to integrate with burp suite.
REST API
This setting controls the state of proxy interception at startup
Proxy Interception
This setting controls whether adding items to target scope will automatically set the proxy option to stop sending out-of-scope items to the history or other burp tools.
Proxy History Logging
You can help improve burp by submitting anonymous feedback about burp's performance.
Performance Feedback
This setting controls burp's update behaviour.
Update(installer version only)
Misc
User Options
URL
HTML
Base64
ASCII Hex
Hex
Octal
Binary
GZip
Decode
URL
HTML
Base64
ASCII Hex
Hex
Octal
Binary
GZip
Encode
SHA-1
SHA-384
HARAKA-256
SKEIN-512-256
SKEIN-1024-384
BLAKE2B-160
KECCAK-288
WHIRL POOL
Hash
Smart Decode
Decoder
ITempFile
ITextEditor
API
These settings control how burp handles extensions on startup.
Settings
These settings let you configure environment for executing extensions that are written in java .If your extensions use any libraries you can specify a folder from which libraries will be loaded.
Java Environment
These settings let you configure the environment for executing extensions that are written python. To use python extensions you will need to download jython which is a python interpreter implement in java.
Python Environment
These settings let you configure the environment for executing extensions that are written in ruby. Interpreter implement in java.
Ruby Environment
Options
Extender
Request
Response
Repeater
New Scan
Live Passive Crawl From Proxy (all traffic)
Live Audit From Proxy(all traffic)
New Live Scan
Tasks
Event Log
Issue Activity
Advisory
Dashboard
Forward
Drop
Intercept On
Scan
Do Active Scan
Do Passive Scan
Send to Intruder
Send to Repeater
Send to Squencer
Send to Decode
Send to Comparer
Show Response in Browser
Request in Browser
Guess GET parameters
Guess cookie parameters
Guess headers
Guess everything
Guess Params
Header poison
Port-DOS
Unkeyed Param
Fat GET
Normalised Param
Normalised Path
Rails Param Cloaking Scan
Identify Header Smuggling Mutations
Param Miner
Send to Extractor
Engagement Tools

Burp Suite

Intruder

- Target
  - Attack Target
    - Configure the details of the target for the attack
- Positions
  - Attack Type
    - Sniper
    - Cluster Bomb
    - Pitchfork
    - Battering Ram
- Payloads
  - Payload Sets
    - You can define one or more payload sets. The number of payload sets depends on the attacks types defined in the positions tab. Various payload types are available for each payload set and each payload type can be customized in different ways.
  - Payload Options
    - This payload type lets you configure simple list of strings that are used as Payloads.
  - Payload Processing
    - You can define rules to perform various processing tasks on each payload before it is used.
  - Payload Encoding
    - This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.
- Options
  - Request Headers
    - These settings control whether intruder updates the configured request headers during attacks.
  - Request Engine
    - These setting control the engine used by making http request when performing attacks.
  - Attack Result
    - These settings control what information is captured in attack results.
  - Grep-Match
    - These settings can used to flag result item containing specified expressions.
  - Grep-Extract
    - These settings can be useful information from responses into the attack results table.
  - Grep-Payloads
    - These setting can be used to flag result items containing reflections of the submitted payload
  - Redirections
    - These setting control how burp handles redirections when performing attacks.

Proxy

- Intercept
  - Action
    - Copy Url
    - Copy as Curl Command
    - Copy to File
    - Save Item
    - Save Entire History
    - Paste URL as Request
    - Add to Site Map
    - Cut
    - Copy
    - Paste
    - Message Editor Document
    - Burp Repeater Document
  - Open Browser
- HTTP History
- WebSocket History
- Options
  - Proxy Listners
    - Burp proxy uses listeners to receive incoming HTTP requests from your browser.
  - Intercept Client Requests
    - Use these settings to control which requests are stalled for viewing and editing in the intercept tab.
  - Intercept Server Responses
    - Use these to control which responses are stalled for viewing and editing in the intercept tab.
  - Intercepts WebSockets Messages
    - Use these settings to control which websockets messages are stalled for viewing and editing in the intercept tab
  - Response Modification
    - These settings are used to perform automatic of responses.
  - Match & Replace
    - These settings are used to automatically replace parts of requests and responses passing through the proxy.
  - TLS Pass Through
    - These settings are used to specify destination web servers for which burp will directly pass through TLS connections.
  - Miscellaneous
    - These settings control some specific details of burp proxy' s behaviour.

@hackinarticles
https://github.com/Ignitetechnologies
https://in.linkedin.com/company/hackingarticles