



# Burp suite: Top 5 Community edition extensions

[Introduction](#)

[Add custom headers](#)

[Authorize](#)

[Bypass WAF](#)

[Headless mode](#)

[IP Rotate](#)

## Introduction

When you use Burp Suite Community edition, there are several possibilities in terms of extensions we can use, however we are more limited. Some of the Professional edition extensions can be extremely useful for both bug bounty hunters and pentesters alike but the community edition certainly has some useful extensions as well.

## Add custom headers

Sometimes our targets require us to add custom headers, this useful extension allows us to do that easily.

## Authorize

This amazing extension allows us to easily test for BAC and IDOR. We have a separate chapter on this extension.

## Bypass WAF

This extension add headers to all Burp requests to bypass some WAF products. The following headers are automatically added to all requests:

```
X-Originating-IP: 127.0.0.1
X-Forwarded-For: 127.0.0.1
X-Remote-IP: 127.0.0.1
X-Remote-Addr: 127.0.0.1
```

## Headless mode

This extension allows you to run Burp Suite's Spider and Scanner tools in headless mode via the command-line. It can:

- Run burp scan in headless or GUI mode.
- Specify target sitemap and add URL(s) to Burp's target scope.
- Use the seed request/response data saved in a project file, generated by any integration, functional or manual testing.
- Mark issues as false positives, these will not be reported in the scan report anymore.
- Spider the target scope.
- Actively scan the target scope.
- Generate a scan report in JUnit, HTML, or XML format. The JUnit report can be used to instruct the CI server to fail the build when vulnerabilities are found.
- Shut down Burp

## IP Rotate

This extension allows you to easily spin up API Gateways across multiple regions. All the Burp Suite traffic for the targeted host is then routed through the API Gateway endpoints which causes the IP to be different on each request. (There is

a chance for recycling of IPs but this is pretty low and the more regions you use the less of a chance).

This is useful to bypass different kinds of IP blocking like bruteforce protection that blocks based on IP, API rate limiting based on IP or WAF blocking based on IP etc.

For more information see [Bypassing\\_  
\\_\\_\\_\\_IP Based Blocking Using AWS](#)