

# Burp Suite: The Basics

An introduction to using Burp Suite for Web Application pentesting

## Task 2 : Getting Started What is Burp Suite?

Question	Answer
Which edition of Burp Suite will we be using in this module?	Burp Suite Community
Which edition of Burp Suite runs on a server and provides constant scanning for target web apps?	Burp Suite Enterprise
Burp Suite is frequently used when attacking web applications and _____ applications.	mobile

## Task 3 Getting Started Features of Burp Community

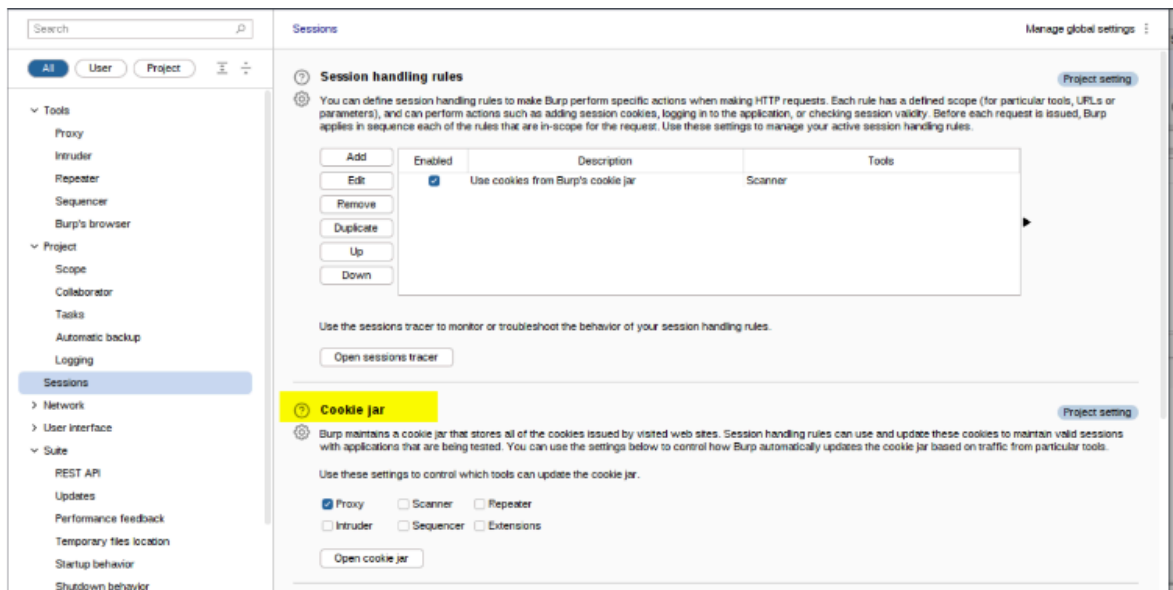
Question	Answer
Which Burp Suite feature allows us to intercept requests between ourselves and the target?	proxy
Which Burp tool would we use if we wanted to bruteforce a login form?	Intruder

## Task 7 Options

In which category can you find reference to a "Cookie jar"?

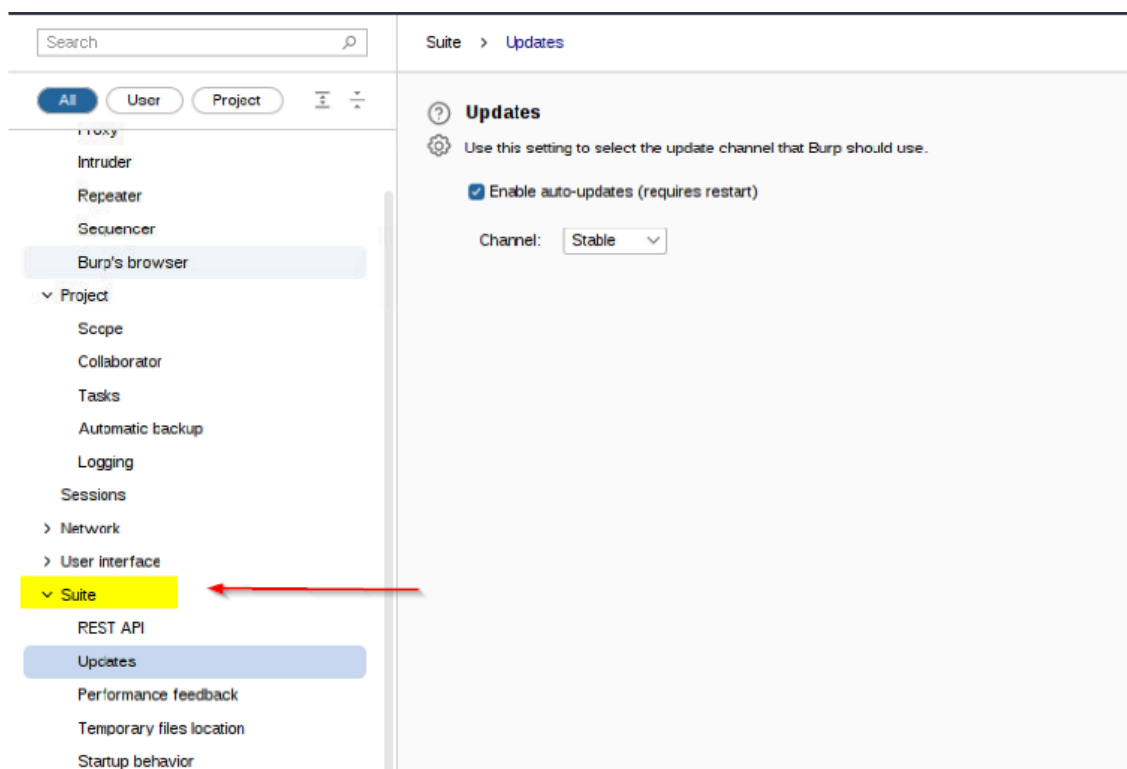
→ I clicked on settings, Under categories

Answer: **sessions**



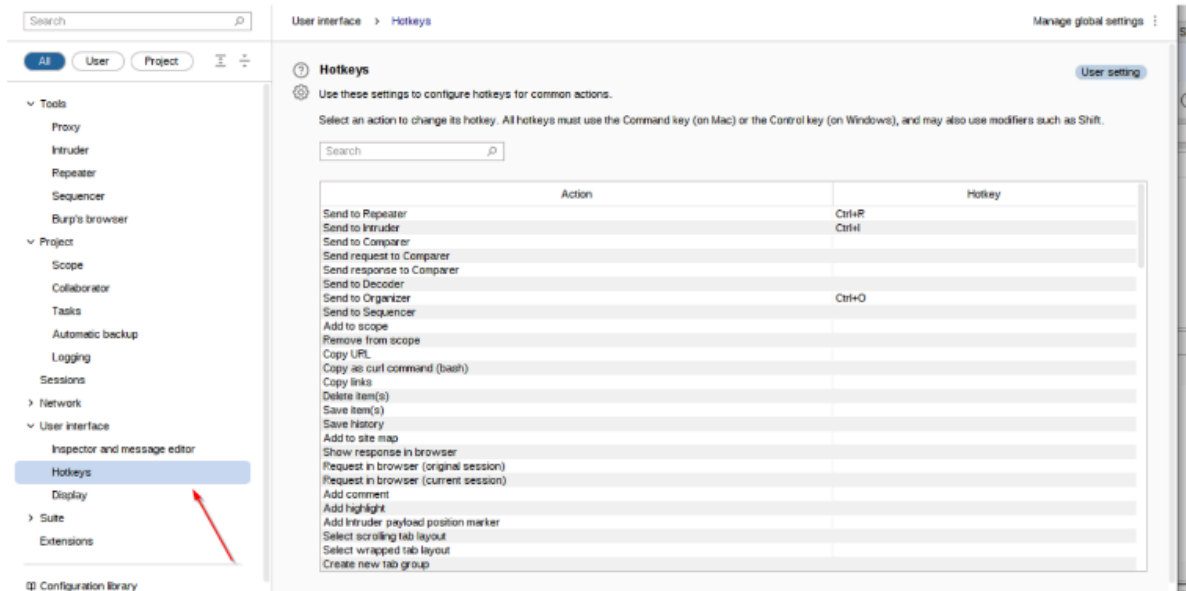
In which base category can you find the "Updates" sub-category, which controls the Burp Suite update behaviour?

Answer: **suite**



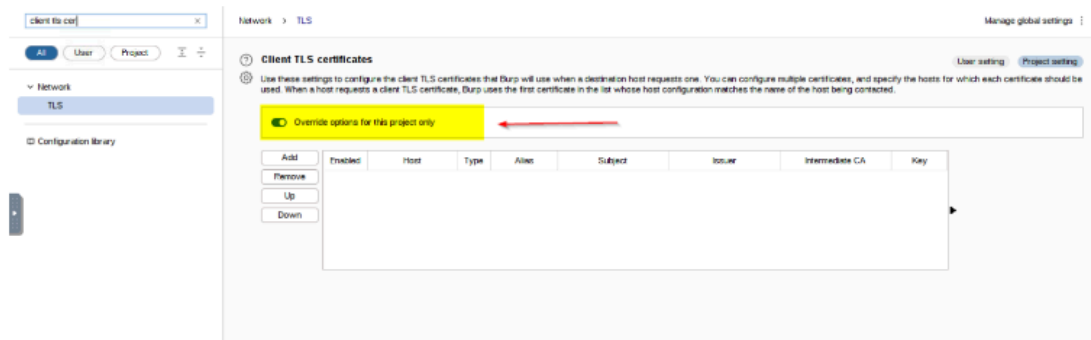
What is the name of the sub-category which allows you to change the keybindings for shortcuts in Burp Suite ?

Answer: **hotkeys**



If we have uploaded Client-Side TLS certificates, can we override these on a per-project basis (Aye/Nay)?

Answer: **Aye**



## Task 8 Proxy Introduction to the Burp Proxy

Question	Answer
Which button would we choose to send an intercepted request to the target in Burp Proxy?	forward
[Research] What is the default keybind for this?  <i>Note: Assume you are using Windows or Linux (i.e. swap Cmd for Ctrl).</i>	Ctrl+F

## Task 9 Proxy Connecting through the Proxy (FoxyProxy)

Read through the options in the right-click menu.

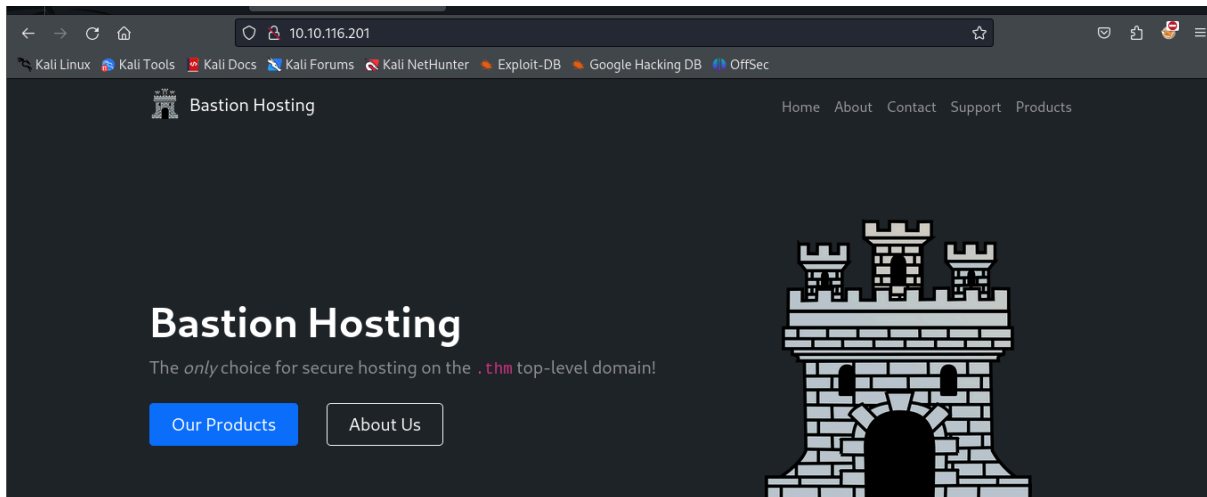
There is one particularly useful option that allows you to intercept and modify the response to your request.

What is this option?

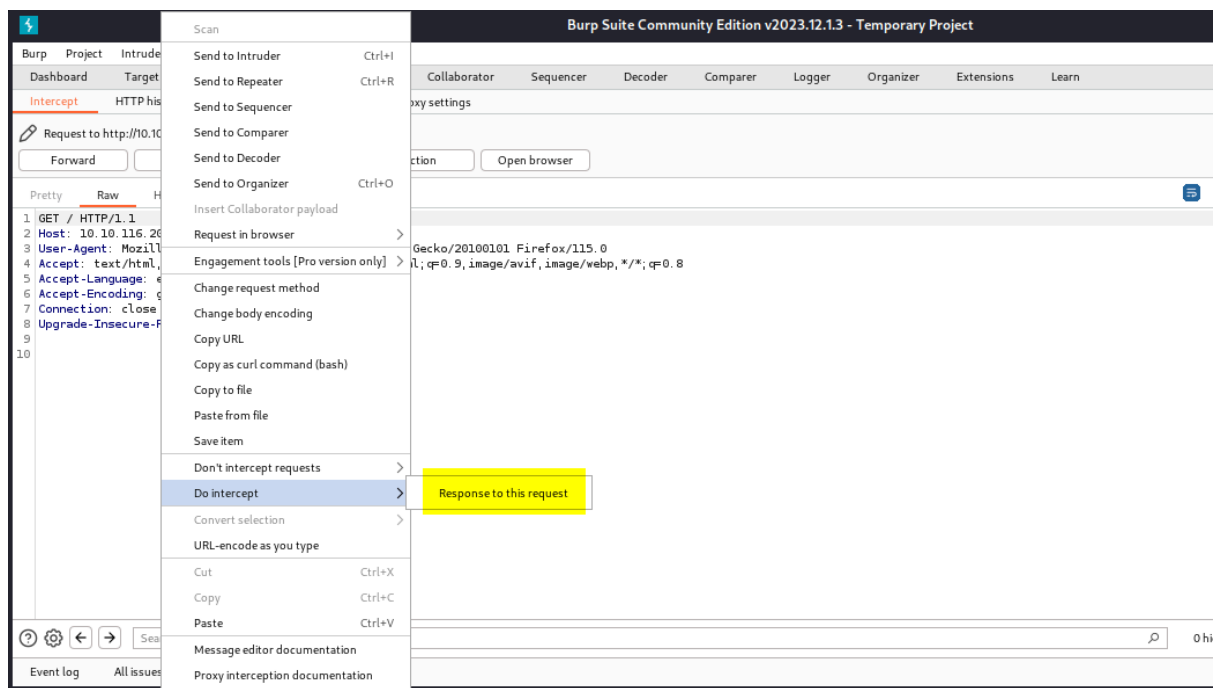
*Note: The option is in a dropdown sub-menu.*

**Answer: Response to this request**

→ Checking the target website



- ➔ And intercepting the request by making sure my proxy is enabled and intercept is on
- ➔ Right clicked on the request



## Task 13 Proxy Site Map and Issue Definitions

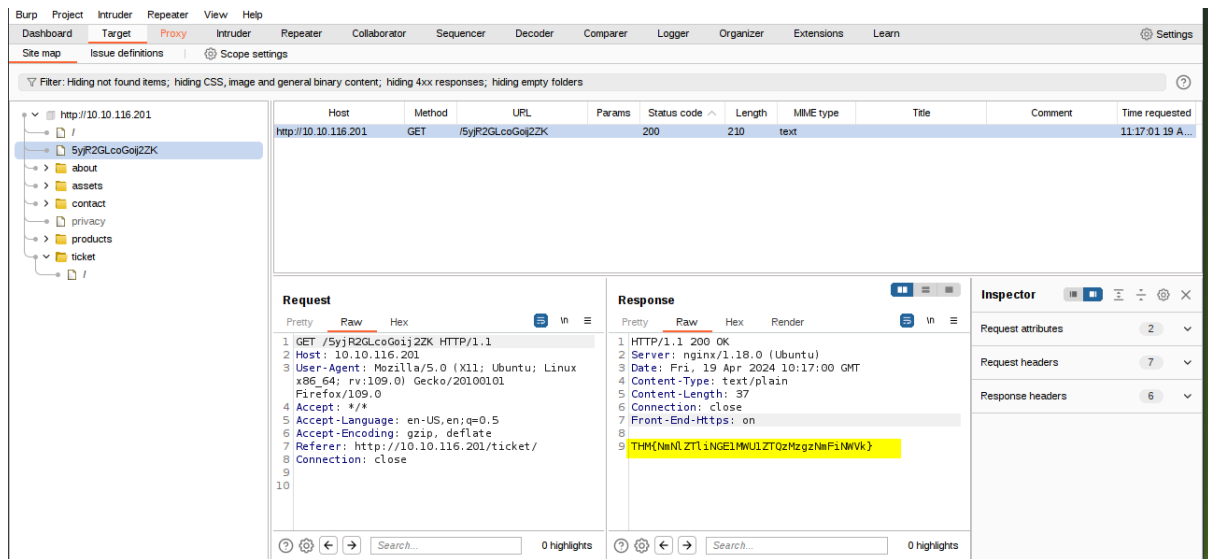
Take a look around the site on <http://10.10.116.201/> -- we will be using this a lot throughout the module. Visit every page linked to from the homepage, then check your sitemap -- one endpoint should stand out as being very unusual!

Visit this in your browser (or use the "Response" section of the site map entry for that endpoint)

What is the flag you receive?

- I enabled interception in the proxy tab, forwarded the website request, and examined the "Response" section of the site map entry. While looking through for suspicious content, I discovered the flag.

**Answer/Flag:** `THM{NmNIZTliNGE1MWU1ZTQzMzgZnmFiNWVk}`



Look through the Issue Definitions list.

What is the typical severity of a Vulnerable JavaScript dependency?

**Answer:** Low

Burp

Project

Intruder

Repeater

View

Help

Dashboard

Target

Proxy

Intruder


Repeater

Collaborator

Sequencer

Site map

Issue definitions

 Scope settings

Issue definitions

This listing contains the definitions of all issues that can be detected by Burp Scanner.

Name	Typical severity	Type index
Referer-dependent response	Information	0x00400100
Spoofable client IP address	Information	0x00400110
User agent-dependent response	Information	0x00400120
Password returned in later response	Medium	0x00400200
Password submitted using GET method	Low	0x00400300
Password returned in URL query string	Low	0x00400400
SQL statement in request parameter	Medium	0x00400480
Cross-domain POST	Information	0x00400500
ASP.NET ViewState without MAC enabled	High	0x00400600
XML entity expansion	Medium	0x00400700
Long redirection response	Information	0x00400800
Serialized object in HTTP message	High	0x00400900
Duplicate cookies set	Information	0x00400a00
Input returned in response (stored)	Information	0x00400b00
Input returned in response (reflected)	Information	0x00400c00
Suspicious input transformation (reflected)	Information	0x00400d00
Suspicious input transformation (stored)	Information	0x00400e00
Request URL override	Information	0x00400f00
Vulnerable JavaScript dependency	Low	0x00500080
Open redirection (reflected)	Low	0x00500100
Open redirection (stored)	Medium	0x00500101
Open redirection (DOM-based)	Low	0x00500110
Open redirection (reflected DOM-based)	Low	0x00500111
Open redirection (stored DOM-based)	Medium	0x00500112
TLS cookie without secure flag set	Medium	0x00500200
Cookie scoped to parent domain	Low	0x00500300
Cross-domain Referer leakage	Information	0x00500400
Cross-domain script include	Information	0x00500500
Cookie without HttpOnly flag set	Low	0x00500600
Session token in URL	Medium	0x00500700
Password field with autocomplete enabled	Low	0x00500800

END!!!