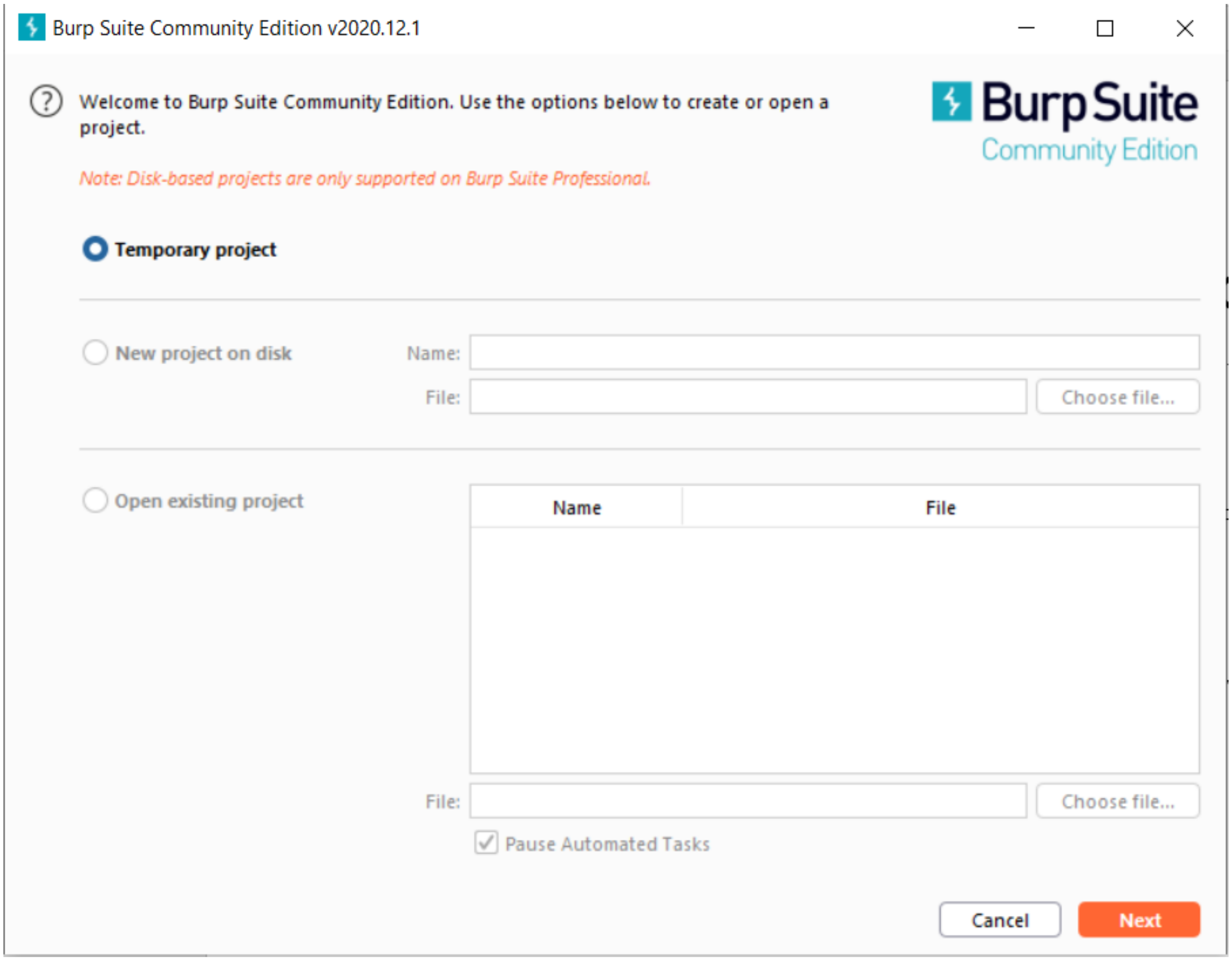
Installing and Using Burp

We're going to use Burp as our interception proxy to monitor and change our traffic for the BodgeIt challenge.

Below are the steps to get it to work

1. Go to [Download Burp Suite Community Edition - PortSwigger](). We're going to download the Community Edition (which is free). There's a professional version that costs about $300/year. For this challenge and in the beginning the community edition will work.
2. Download the Community Edition for your operating system
3. Once the software is downloaded, install the software
4. After installing the software, open Burp Community. You should see the following:



Burp Suite Community Edition v2020.12.1

Welcome to Burp Suite Community Edition. Use the options below to create or open a project.

Note: Disk-based projects are only supported on Burp Suite Professional.

● Temporary project

○ New project on disk

Name:

File:

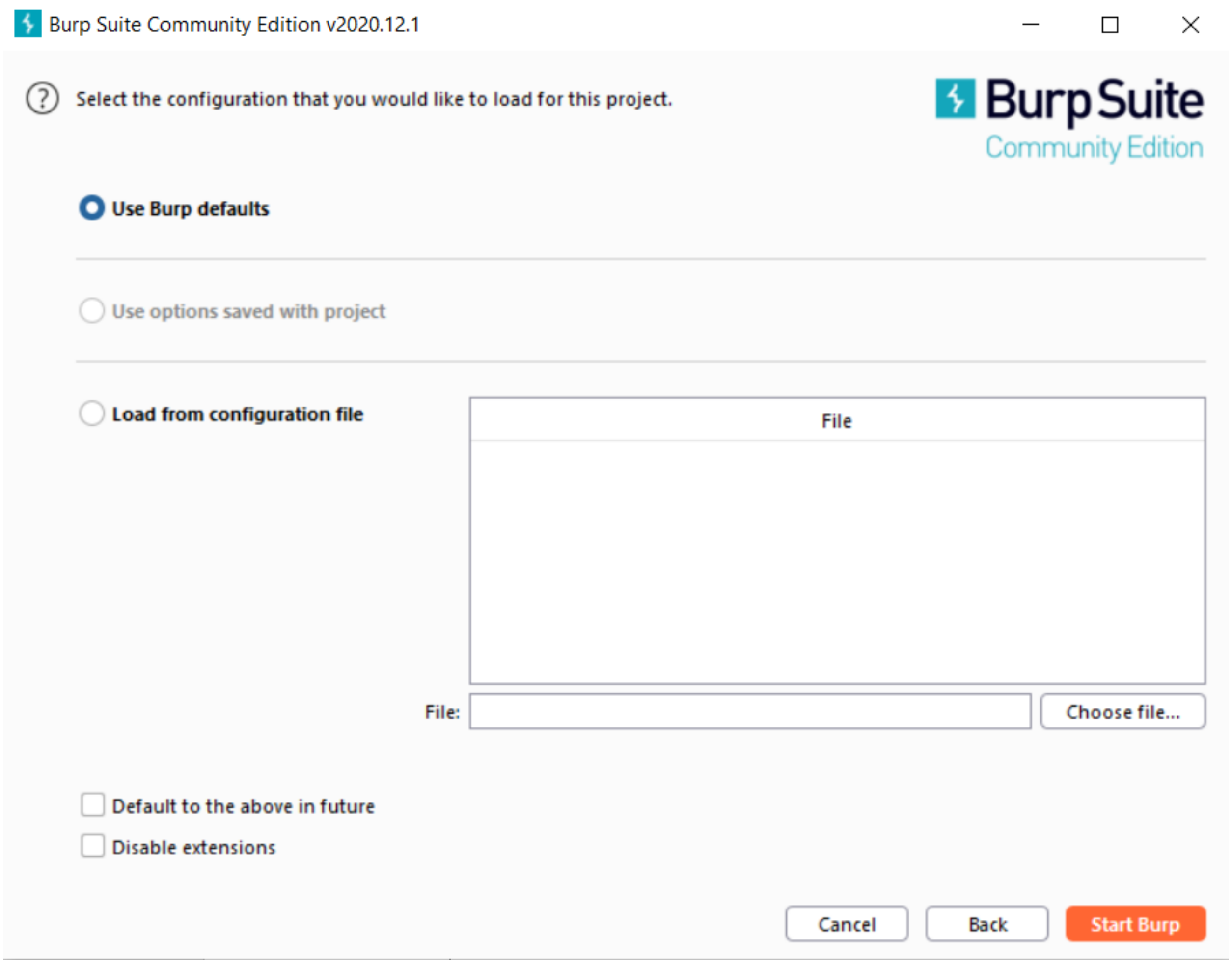
○ Open existing project

Name	File

File:

☑ Pause Automated Tasks

5. We're going to click Next


Burp Suite Community Edition v2020.12.1

Select the configuration that you would like to load for this project.

● Use Burp defaults

○ Use options saved with project

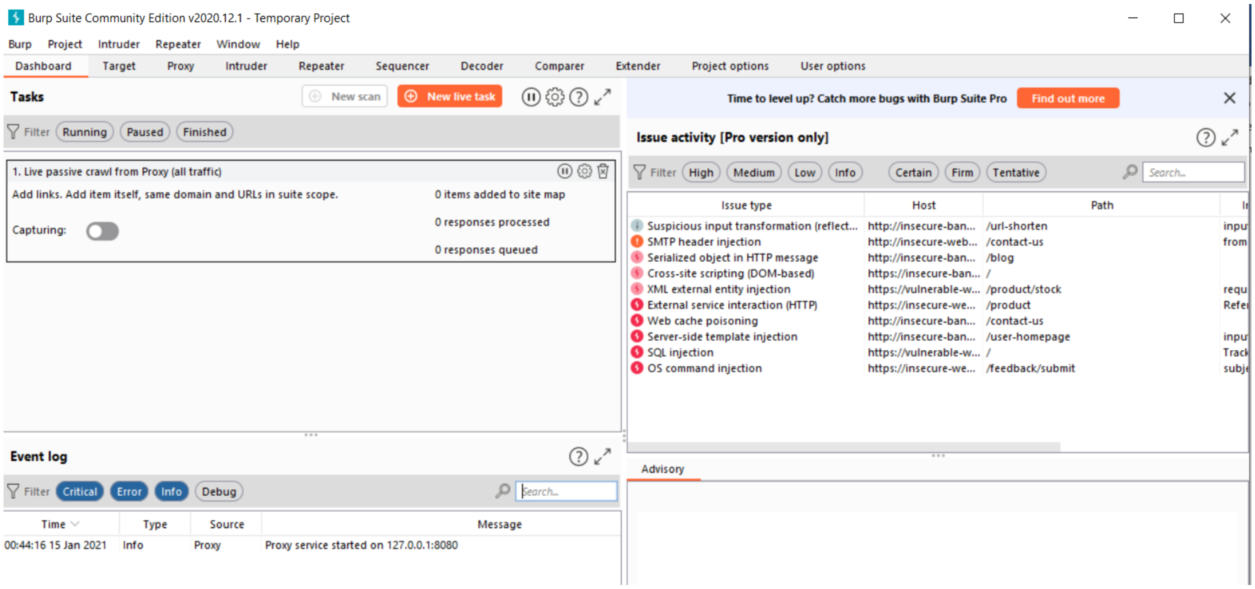
○ Load from configuration file

File:

□ Default to the above in future

□ Disable extensions

6. Click Start Burp button
7. First thing we’re going to do is disable capturing. Move the toggle button from right to left. The reason we’re disabling the capturing feature is we do not want to inspect traffic of web pages that we’re not going to exploit. Your screen should look like this:


Burp Suite Community Edition v2020.12.1 - Temporary Project

1. Live passive crawl from Proxy (all traffic)

Add links. Add item itself, same domain and URLs in suite scope.

Capturing: ○

0 items added to site map

0 responses processed

0 responses queued

Time to level up? Catch more bugs with Burp Suite Pro

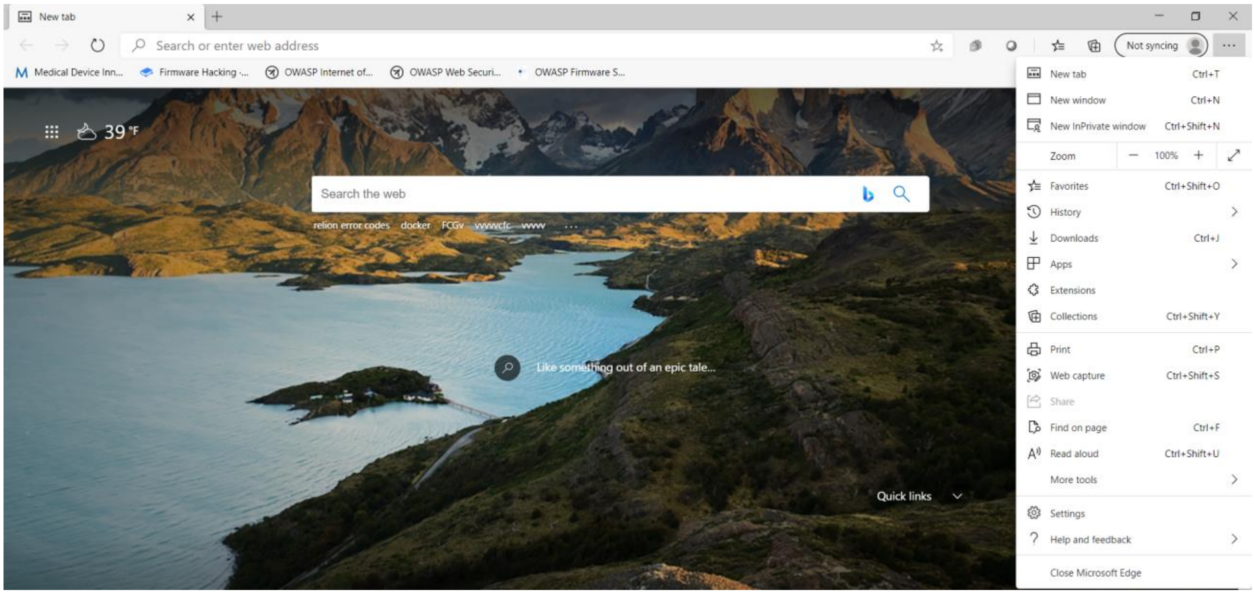
Issue activity [Pro version only]

Issue type	Host	Path	I
Suspicious input transformation (reflect...	http://insecure-ban...	/url-shorten	inpu
SMTP header injection	http://insecure-web...	/contact-us	from
Serialized object in HTTP message	http://insecure-ban...	/blog	
Cross-site scripting (DOM-based)	https://insecure-ban...	/	
XML external entity injection	https://vulnerable-w...	/product/stock	requ
External service interaction (HTTP)	https://insecure-we...	/product	Refe
Web cache poisoning	http://insecure-ban...	/contact-us	
Server-side template injection	http://insecure-ban...	/user-homepage	inpu
SQL injection	https://vulnerable-w...	/	Track
OS command injection	https://insecure-we...	/feedback/submit	subj

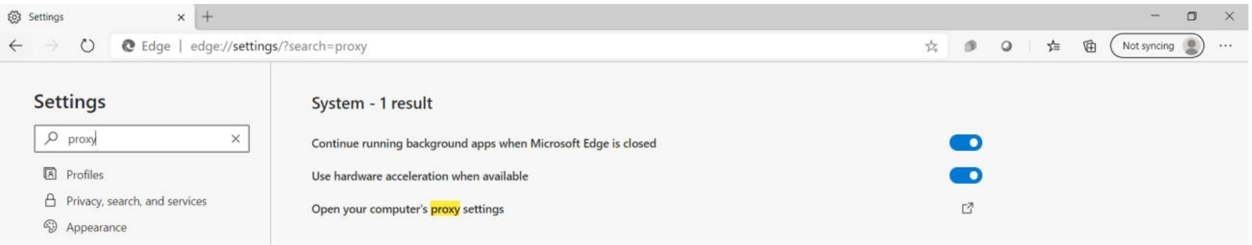
Event log

Time	Type	Source	Message
00:44:16 15 Jan 2021	Info	Proxy	Proxy service started on 127.0.0.1:8080

8. Looking at the event log at the bottom we see that the proxy has started at 127.0.0.1 (loopback/home address) on port 8080. We're going to need this in the next step
9. Open your browser of choice. In my case I am going to use Edge
10. Once the browser is open, go to Settings
11. It should look like this



12. In the search button type, proxy


Settings
Edge | edge://settings/?search=proxy
Not syncing
Settings
proxy
Profiles
Privacy, search, and services
Appearance

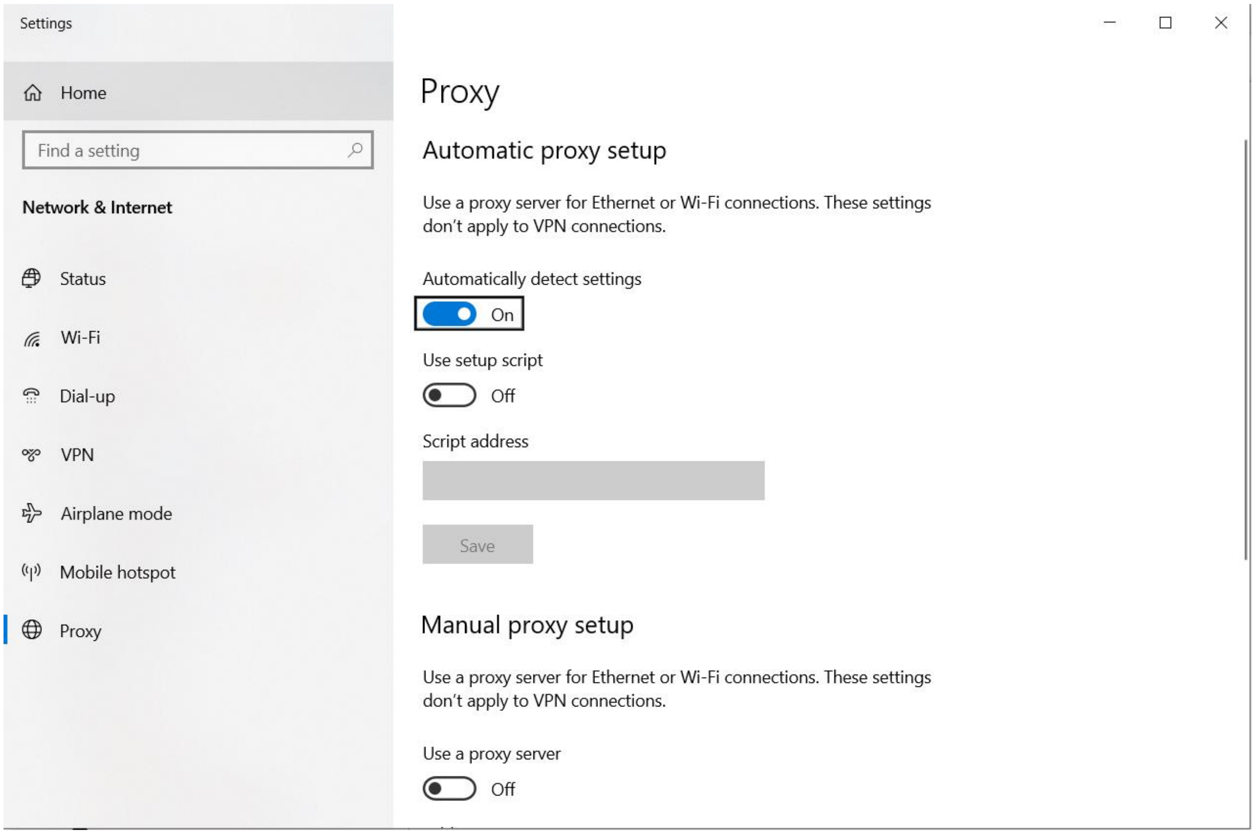
System - 1 result

Continue running background apps when Microsoft Edge is closed

Use hardware acceleration when available

Open your computer's proxy settings

13. Click on "Open your computer's proxy settings"
14. The screen you will see is this



Proxy

Automatic proxy setup

Use a proxy server for Ethernet or Wi-Fi connections. These settings don't apply to VPN connections.

Automatically detect settings

On

Use setup script

Off

Script address

Manual proxy setup

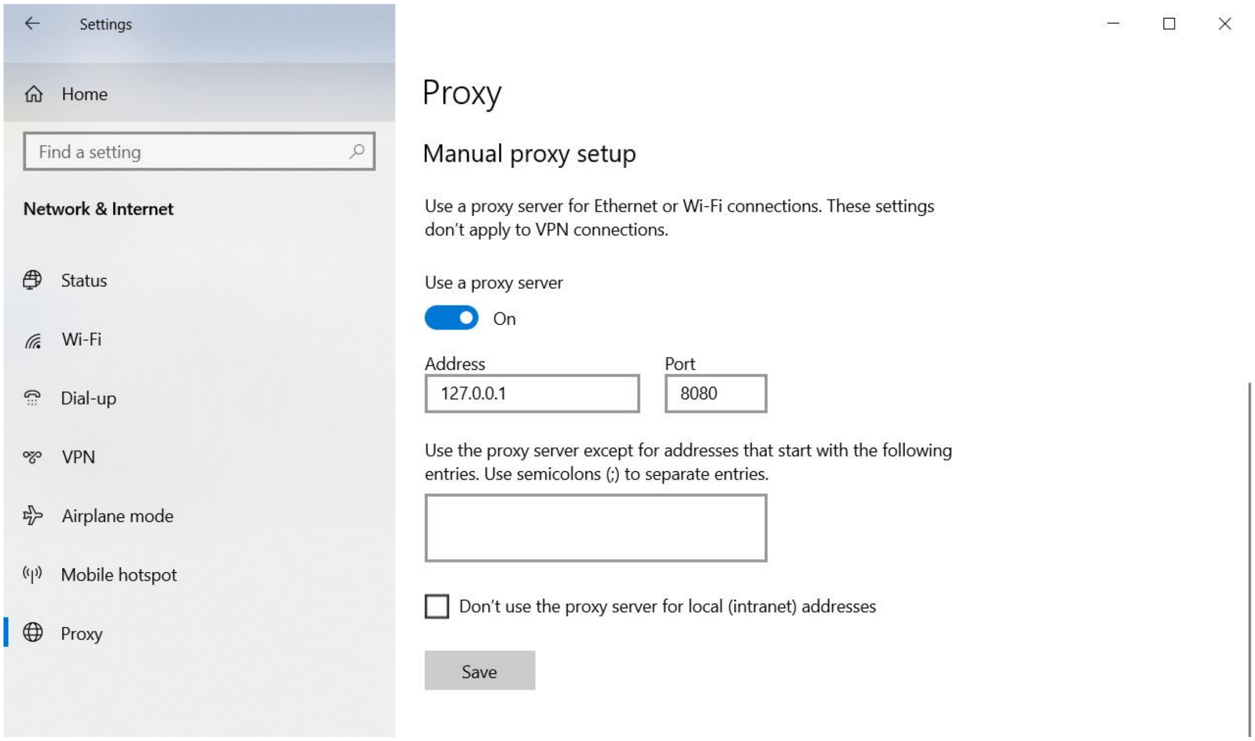
Use a proxy server for Ethernet or Wi-Fi connections. These settings don't apply to VPN connections.

Use a proxy server

Off

Scroll down to the manual proxy setup

15. In the "Use a proxy server" we're going to turn that on, and enter the address, port we have before (127.0.0.1, 8080). The screen should look like the following:



Settings

Home

Find a setting

Network & Internet

Status

Wi-Fi

Dial-up

VPN

Airplane mode

Mobile hotspot

Proxy

Proxy

Manual proxy setup

Use a proxy server for Ethernet or Wi-Fi connections. These settings don't apply to VPN connections.

Use a proxy server

On

Address: 127.0.0.1

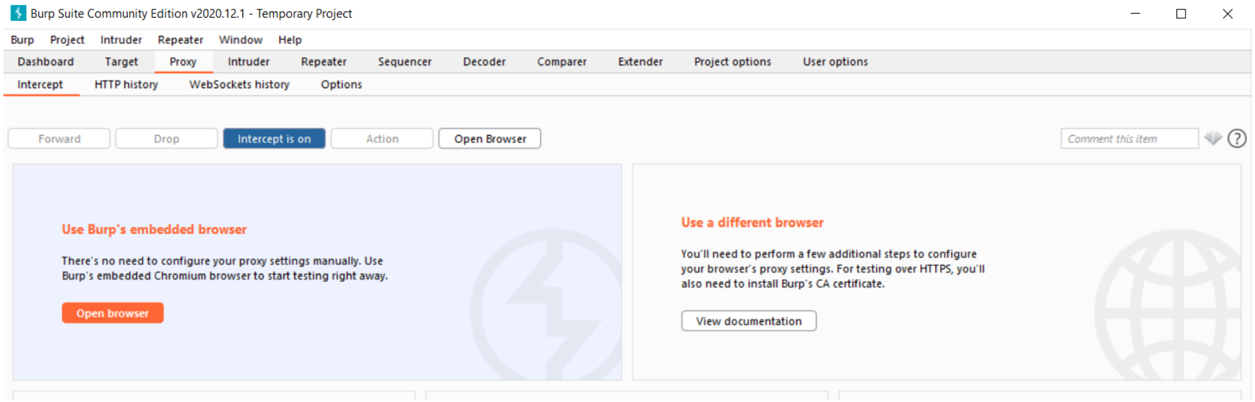
Port: 8080

Use the proxy server except for addresses that start with the following entries. Use semicolons (;) to separate entries.

□ Don't use the proxy server for local (intranet) addresses

Save

16. Click the Save button
17. Going back to Burp let's go to the Proxy Tab



Burp Suite Community Edition v2020.12.1 - Temporary Project

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

Intercept HTTP history WebSockets history Options

Forward Drop Intercept is on Action Open Browser Comment this item

Use Burp's embedded browser

There's no need to configure your proxy settings manually. Use Burp's embedded Chromium browser to start testing right away.

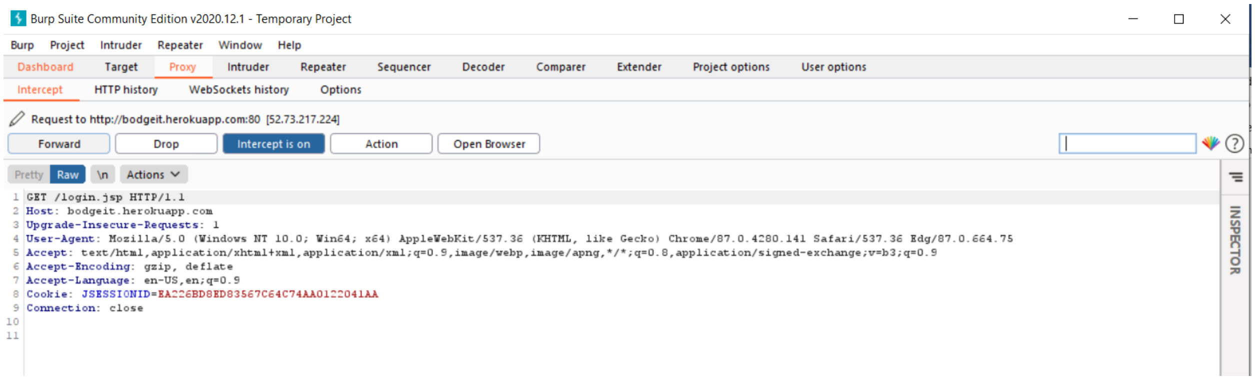
Open browser

Use a different browser

You'll need to perform a few additional steps to configure your browser's proxy settings. For testing over HTTPS, you'll also need to install Burp's CA certificate.

View documentation

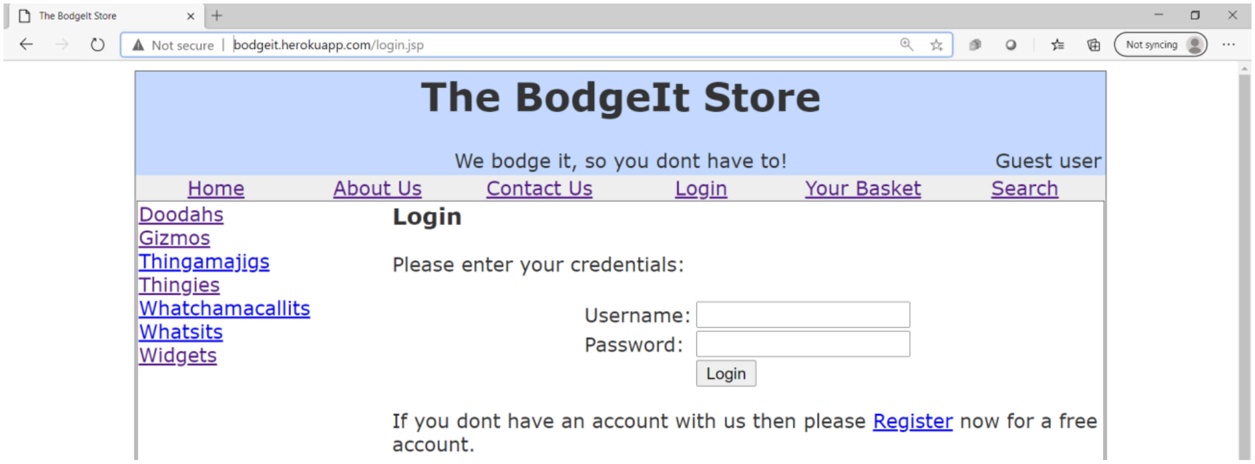
18. As you can see the intercept is on. This is what we want, as any traffic we have will be intercepted to Burp. Let's try it
19. Let's enter the link to the BodgeIt store in the URL bar, Settings (bodgeit.herokuapp.com).
20. Going back to Burp, Proxy we see the following:


Burp Suite Community Edition v2020.12.1 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Intercept HTTP history WebSockets history Options
Forward
Drop
Intercept is on
Action
Open Browser
Pretty Raw \n Actions
INSPECTOR

Request to http://bodgeit.herokuapp.com:80 [52.73.217.224]

```
GET /login.jsp HTTP/1.1
Host: bodgeit.herokuapp.com
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.141 Safari/537.36 Edg/87.0.664.75
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: JSESSIONID=EA226BD8ED83567C64C74AA0122041AA
Connection: close
```

21. Sweet! The traffic is being captured. As you can see the Dashboard, Proxy, and Intercept tabs are highlighted. Click the Forward button to have the traffic continue
22. Going back to the browser we see:



The BodgeIt Store

We bodge it, so you dont have to! Guest user

Home About Us Contact Us Login Your Basket Search

Doodahs
Gizmos
Thingamajigs
Thingies
Whatchamacallits
Whatsits
Widgets

Login

Please enter your credentials:

Username:
Password:
Login

If you dont have an account with us then please Register now for a free account.

23. The page rendered properly. Now we’re ready to exploit the BodgeIt Store!