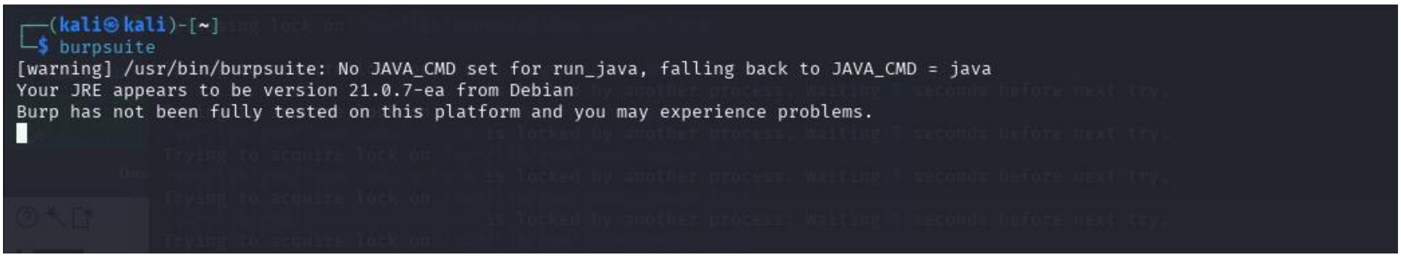
# What is Burp Suite?

Burp Suite is a comprehensive tool used in web application security testing that allows users to identify and exploit vulnerabilities. Put simply, it’s a tool that helps people find weaknesses in websites.

Burp Suite has many functions: web scraping, penetration testing, and vulnerability scanning. But at its core, Burp Suite acts as a web proxy that sits between the user’s browser and the web application. It will intercept the user’s HTTP requests, giving you the ability to modify specific parts of a request.

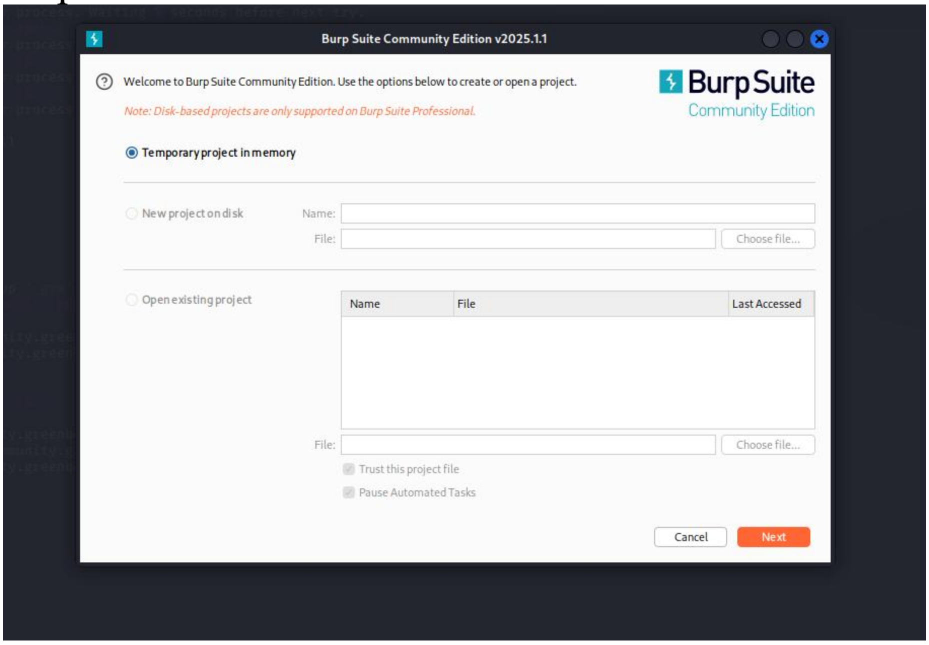
1. This guide is my attempt to provide a high level overview that will help you learn Burp Suite the way I wish someone had taught me.

Step1 : burpsuite



```
┌──(kali㉿kali)-[~]
└─$ burpsuite
[warning] /usr/bin/burpsuite: No JAVA_CMD set for run_java, falling back to JAVA_CMD = java
Your JRE appears to be version 21.0.7-ea from Debian
Burp has not been fully tested on this platform and you may experience problems.
```

Step2:



Burp Suite Community Edition v2025.1.1

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 in memory

○ New project on disk — Name: — File:

○ Open existing project

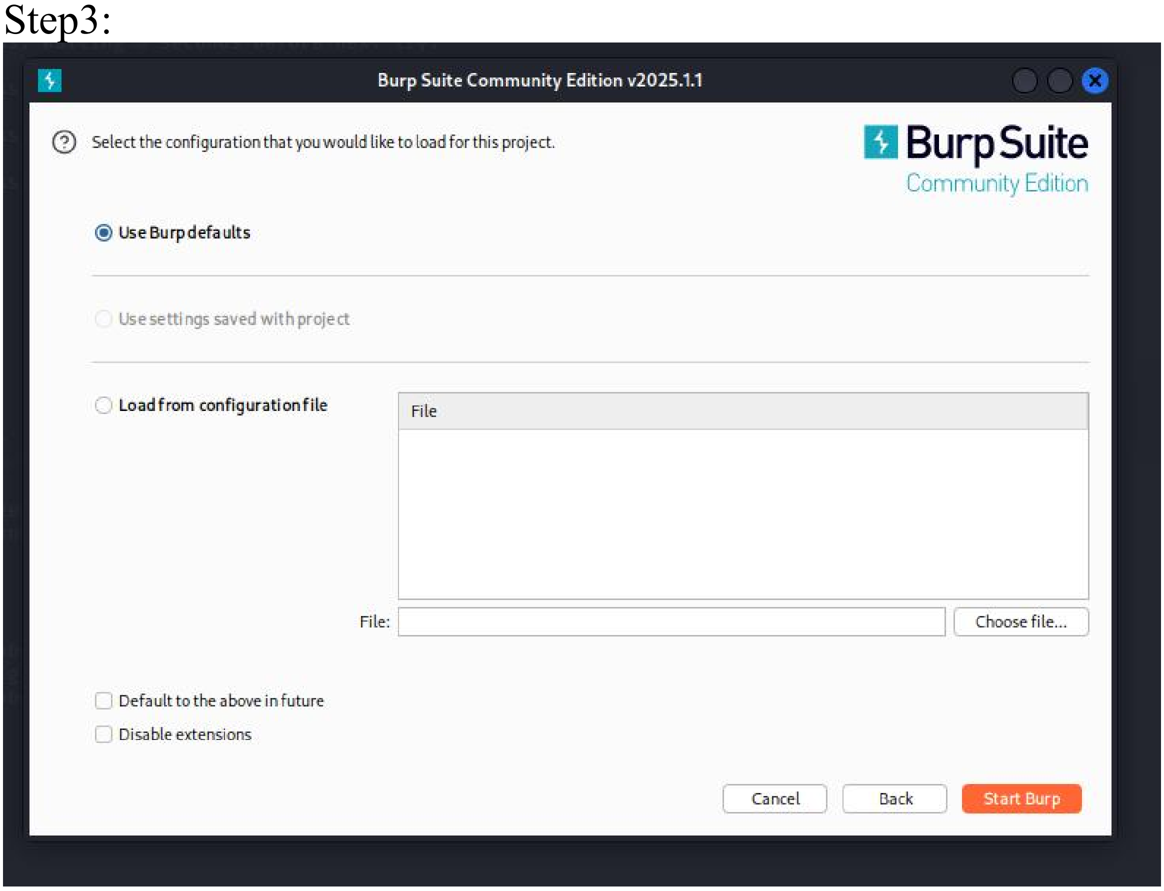
| Name | File | Last Accessed |
|---|---|---|

File:

☑ Trust this project file

☑ Pause Automated Tasks

Step3:



Burp Suite Community Edition v2025.1.1

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

● Use Burp defaults

○ Use settings saved with project

○ Load from configuration file

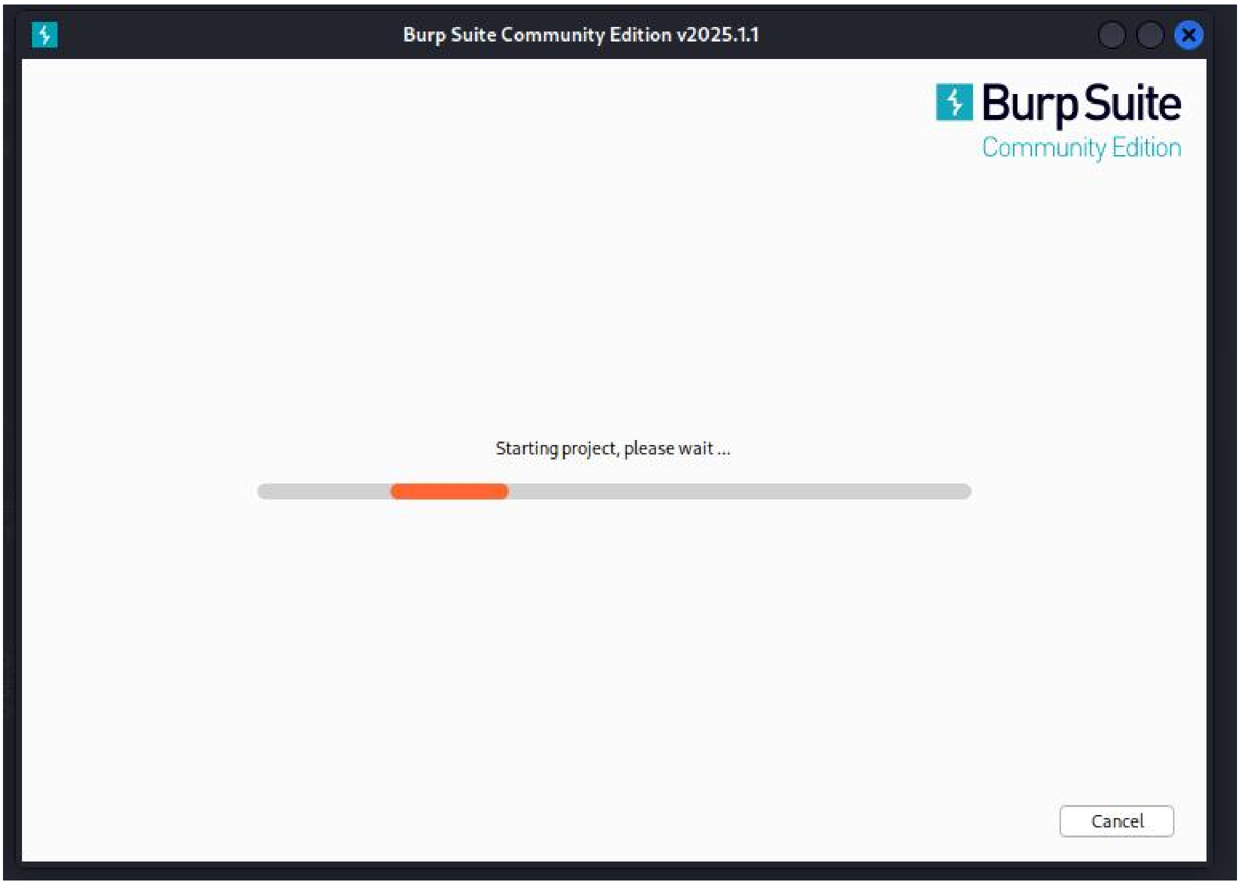
| File |
|---|

File:

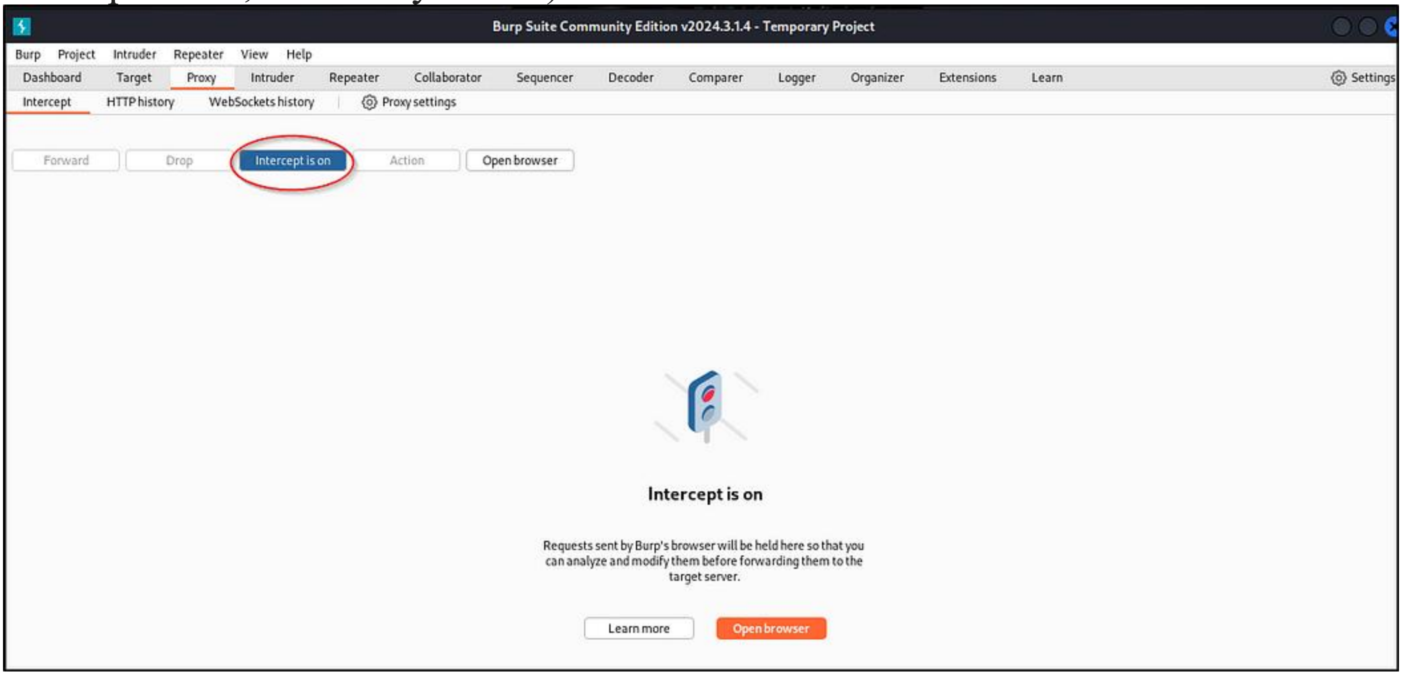
□ Default to the above in future

□ Disable extensions

Step4:
Press the start button


Burp Suite Community Edition v2025.1.1
Burp Suite
Community Edition
Starting project, please wait ...
Cancel

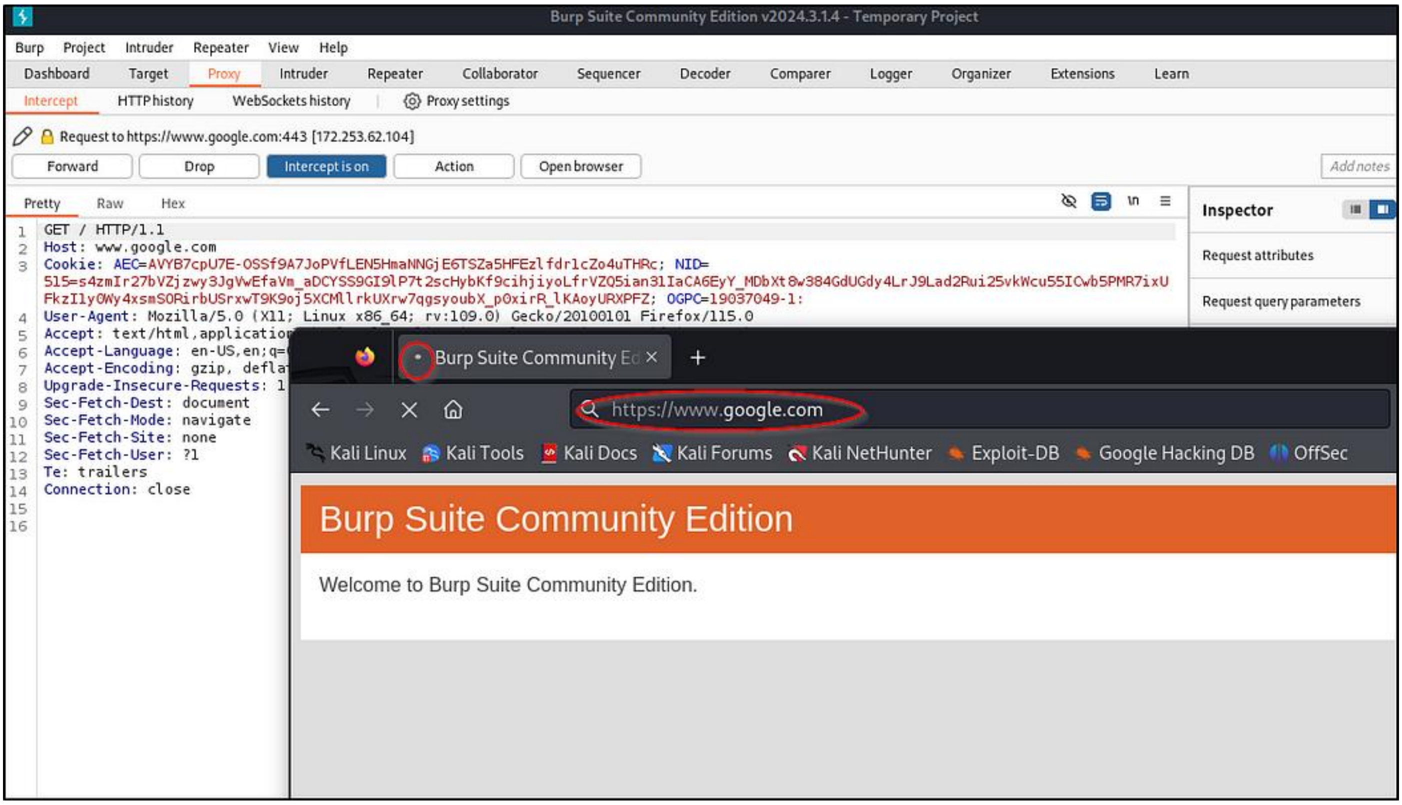
Once you hit OK, the certificate should be installed. To check, go to a website like Google and, in Burp Suite within the proxy tab, turn Intercept on. Refresh the webpage of your choice, and it should hang. You should see the webpage spinning and waiting. It's waiting because we're pushing all this traffic through the Burp Suite proxy. It's all in Burp Suite, intercepted. We now have the ability to manipulate it (forward traffic, drop traffic, or modify traffic).


Burp Suite Community Edition v2024.3.1.4 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Intercept HTTP history WebSockets history Proxy settings
Forward Drop Intercept is on Action Open browser
Learn more Open browser

Intercept is on

Requests sent by Burp's browser will be held here so that you can analyze and modify them before forwarding them to the target server.

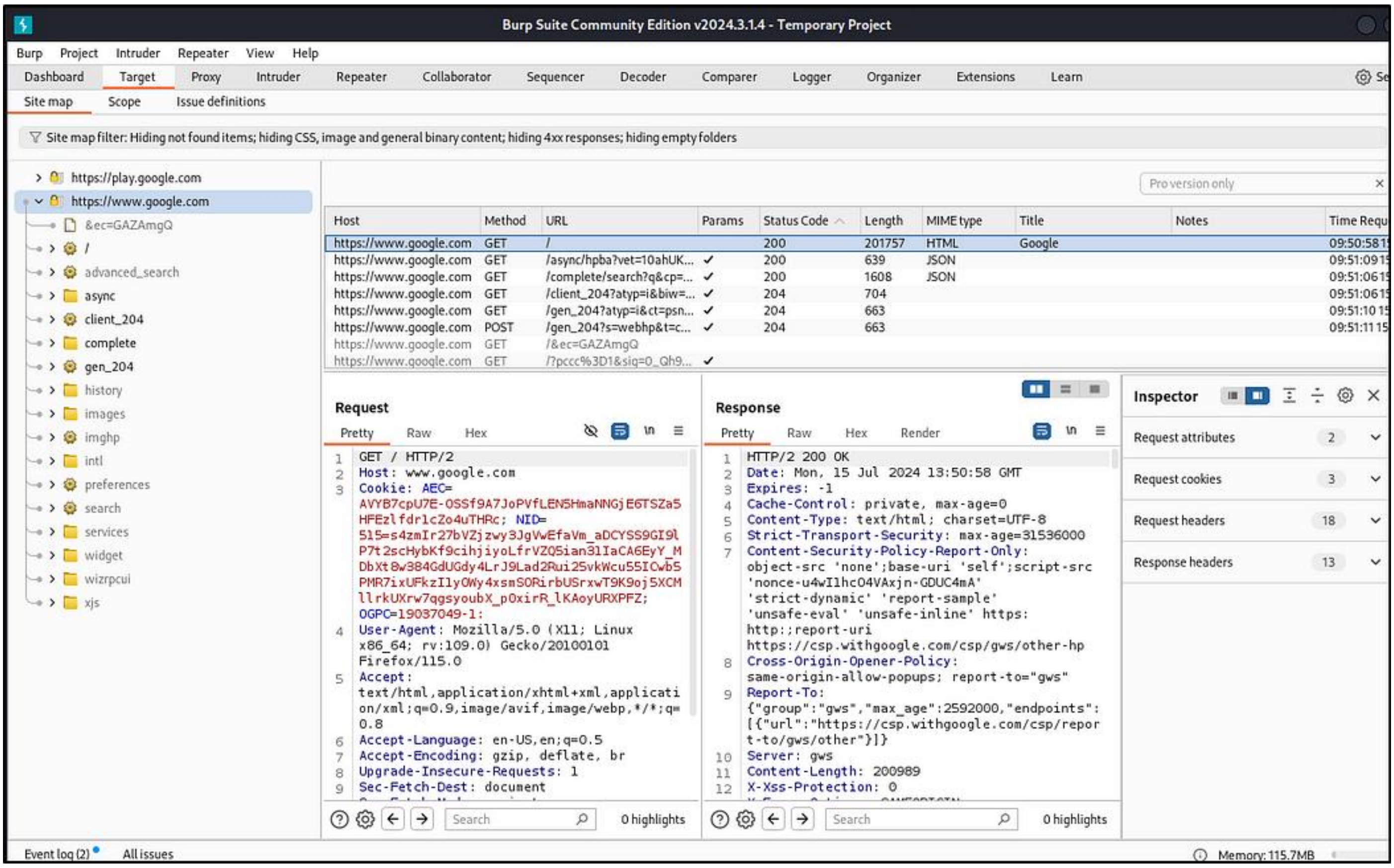
**Made by Moeez Javed**


Burp Suite Community Edition v2024.3.1.4 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Intercept HTTP history WebSockets history Proxy settings
Forward Drop Intercept is on Action Open browser
Add notes
Pretty Raw Hex
Inspector
Request attributes
Request query parameters
Burp Suite Community Ed
https://www.google.com
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Burp Suite Community Edition
Welcome to Burp Suite Community Edition.

Request to https://www.google.com:443 [172.253.62.104]

```
GET / HTTP/1.1
Host: www.google.com
Cookie: AEC=AVYB7cpU7E-OSSf9A7JoPVfLEN5HmaNNGjE6TSZa5HFEzlfdrlcZo4uTHRc; NID=
515=s4zmIr27bVZjzwy3JgVwEfaVm_aDCYSS9GI9lP7t2scHybKf9cihjiyoLfrVZQ5ian31IaCA6EyY_MDbXt8w384GdUGdy4LrJ9Lad2Rui25vkWcu55ICwb5PMR7ixU
FkzIly0Wy4xsmSORirbUSrxwT9K9oj5XCMllrkUXrw7qgsyoubX_p0xirR_lKAoyURXPFZ; OGPC=19037049-1:
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,applicatio
Accept-Language: en-US,en;q=
Accept-Encoding: gzip, defla
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Te: trailers
Connection: close
```

Let’s take a look at what’s happening when we navigate to a website.



Site map filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

| Host | Method | URL | Params | Status Code | Length | MIME type | Title | Notes | Time Requ |
|---|---|---|---|---|---|---|---|---|---|
| https://www.google.com | GET | / | | 200 | 201757 | HTML | Google | | 09:50:58 1 |
| https://www.google.com | GET | /async/hpba?vet=10ahUK... | ✓ | 200 | 639 | JSON | | | 09:51:09 1 |
| https://www.google.com | GET | /complete/search?q&cp=... | ✓ | 200 | 1608 | JSON | | | 09:51:06 1 |
| https://www.google.com | GET | /client_204?atyp=i&biw=... | ✓ | 204 | 704 | | | | 09:51:06 1 |
| https://www.google.com | GET | /gen_204?atyp=i&ct=psn... | ✓ | 204 | 663 | | | | 09:51:10 1 |
| https://www.google.com | POST | /gen_204?s=webhp&t=c... | ✓ | 204 | 663 | | | | 09:51:11 1 |
| https://www.google.com | GET | /&ec=GAZAmgQ | | | | | | | |
| https://www.google.com | GET | /?pccc%3D1&siq=0_Qh9... | ✓ | | | | | | |

Request

Pretty Raw Hex

```
GET / HTTP/2
Host: www.google.com
Cookie: AEC=
AVYB7cpU7E-OSSf9A7JoPVfLEN5HmaNNGjE6TSZa5
HFEzlfdrlcZo4uTHRc; NID=
515=s4zmIr27bVZjzwy3JgVwEfaVm_aDCYSS9GI9l
P7t2scHybKf9cihjiyoLfrVZQ5ian31IaCA6EyY_M
DbXt8w384GdUGdy4LrJ9Lad2Rui25vkWcu55ICwb5
PMR7ixUFkzIly0Wy4xsmSORirbUSrxwT9K9oj5XCM
llrkUXrw7qgsyoubX_p0xirR_lKAoyURXPFZ;
OGPC=19037049-1:
User-Agent: Mozilla/5.0 (X11; Linux
x86_64; rv:109.0) Gecko/20100101
Firefox/115.0
Accept:
text/html,application/xhtml+xml,applicati
on/xml;q=0.9,image/avif,image/webp,*/*;q=
0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
```

Response

Pretty Raw Hex Render

```
HTTP/2 200 OK
Date: Mon, 15 Jul 2024 13:50:58 GMT
Expires: -1
Cache-Control: private, max-age=0
Content-Type: text/html; charset=UTF-8
Strict-Transport-Security: max-age=31536000
Content-Security-Policy-Report-Only:
object-src 'none';base-uri 'self';script-src
'nonce-u4wIlhcO4VAxjn-GDUC4mA'
'strict-dynamic' 'report-sample'
'unsafe-eval' 'unsafe-inline' https:
http:;report-uri
https://csp.withgoogle.com/csp/gws/other-hp
Cross-Origin-Opener-Policy:
same-origin-allow-popups; report-to="gws"
Report-To:
{"group":"gws","max_age":2592000,"endpoints":
[{"url":"https://csp.withgoogle.com/csp/repor
t-to/gws/other"}]}
Server: gws
Content-Length: 200989
X-Xss-Protection: 0
```

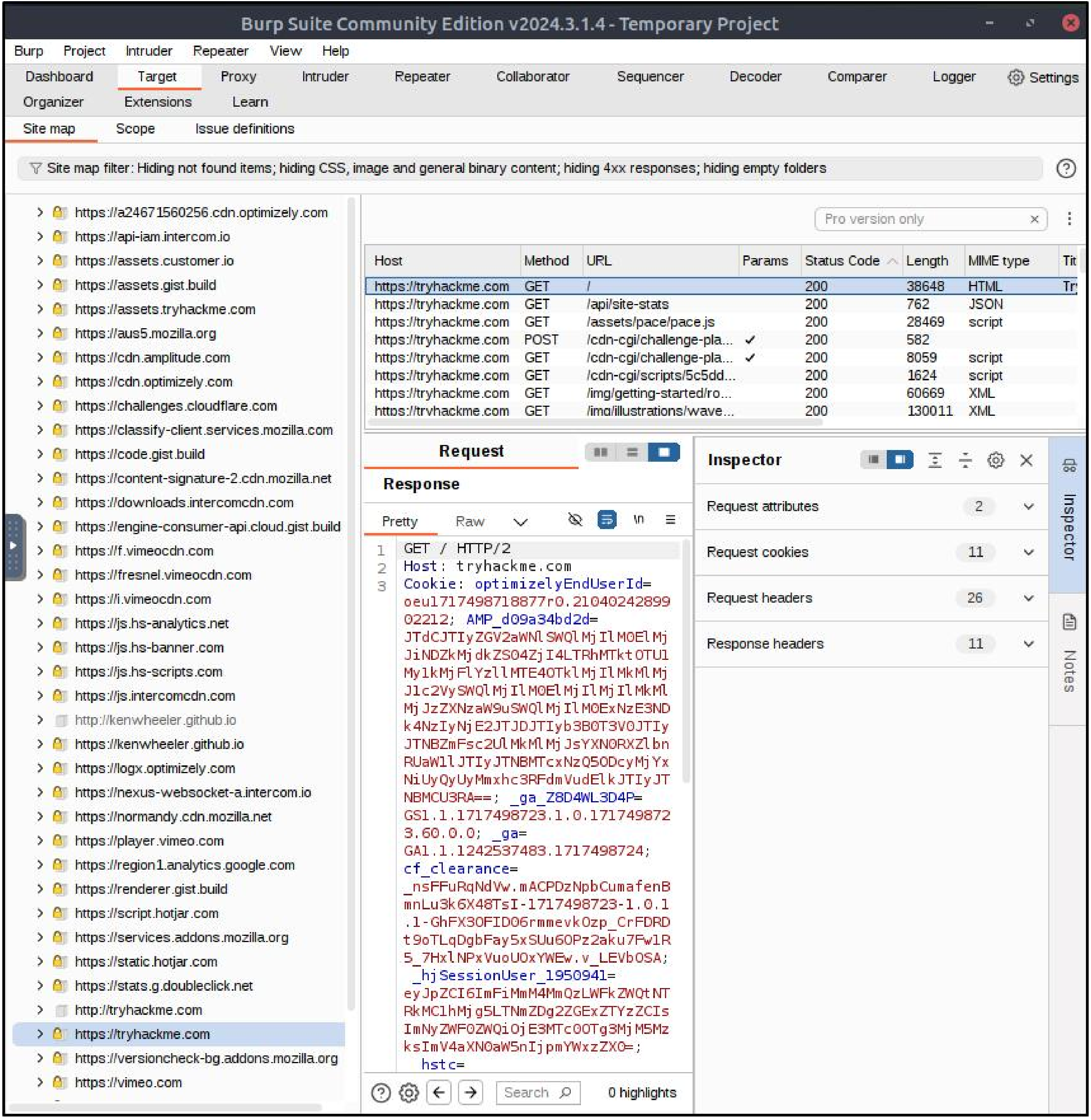
Every page that we visit while the Burp proxy is running will be displayed in the Site map. Burp begins site mapping or crawling the website. In the “Target” tab, you’ll see a tree structure on the left that represents the site’s various resources. Some text will appear in dark black, indicating links that have been accessed, while other text will be greyed out, signifying links identified by Burp Suite that haven’t yet been visited. This process of site mapping helps you visualize the structure and discover hidden resources.

### Setting the Scope

As you can imagine, capturing and logging all the traffic can quickly become overwhelming, especially when you are trying to stay in scope for one specific target. Luckily, we can set the scope for the project, telling Burp to only log the traffic you are interested in.

Just take a look at all the sites and resources that come up when simply visiting *tryhackme.com*.

Made by Moeez Javed


Burp Suite Community Edition v2024.3.1.4 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Settings
Organizer Extensions Learn
Site map Scope Issue definitions
Pro version only
Request
Response
Pretty Raw \n
Inspector
Inspector
Notes
Search
0 highlights

Site map filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

- https://a24671560256.cdn.optimizely.com
- https://api-iam.intercom.io
- https://assets.customer.io
- https://assets.gist.build
- https://assets.tryhackme.com
- https://aus5.mozilla.org
- https://cdn.amplitude.com
- https://cdn.optimizely.com
- https://challenges.cloudflare.com
- https://classify-client.services.mozilla.com
- https://code.gist.build
- https://content-signature-2.cdn.mozilla.net
- https://downloads.intercomcdn.com
- https://engine-consumer-api.cloud.gist.build
- https://f.vimeocdn.com
- https://fresnel.vimeocdn.com
- https://i.vimeocdn.com
- https://js.hs-analytics.net
- https://js.hs-banner.com
- https://js.hs-scripts.com
- https://js.intercomcdn.com
- http://kenwheeler.github.io
- https://kenwheeler.github.io
- https://logx.optimizely.com
- https://nexus-websocket-a.intercom.io
- https://normandy.cdn.mozilla.net
- https://player.vimeo.com
- https://region1.analytics.google.com
- https://renderer.gist.build
- https://script.hotjar.com
- https://services.addons.mozilla.org
- https://static.hotjar.com
- https://stats.g.doubleclick.net
- http://tryhackme.com
- https://tryhackme.com
- https://versioncheck-bg.addons.mozilla.org
- https://vimeo.com

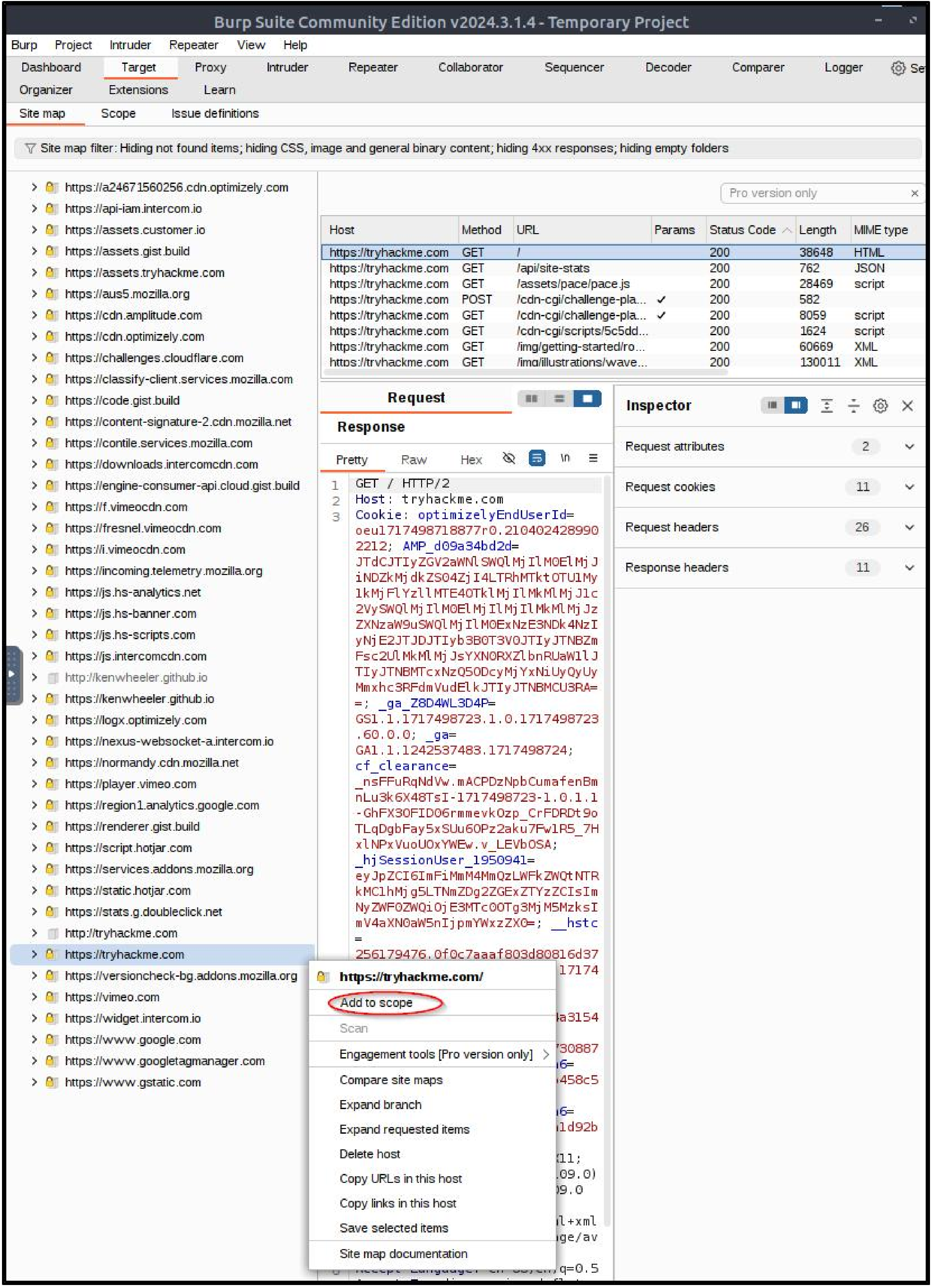
| Host | Method | URL | Params | Status Code | Length | MIME type | Tit |
|---|---|---|---|---|---|---|---|
| https://tryhackme.com | GET | / | | 200 | 38648 | HTML | Tr |
| https://tryhackme.com | GET | /api/site-stats | | 200 | 762 | JSON | |
| https://tryhackme.com | GET | /assets/pace/pace.js | | 200 | 28469 | script | |
| https://tryhackme.com | POST | /cdn-cgi/challenge-pla... | ✓ | 200 | 582 | | |
| https://tryhackme.com | GET | /cdn-cgi/challenge-pla... | ✓ | 200 | 8059 | script | |
| https://tryhackme.com | GET | /cdn-cgi/scripts/5c5dd... | | 200 | 1624 | script | |
| https://tryhackme.com | GET | /img/getting-started/ro... | | 200 | 60669 | XML | |
| https://tryhackme.com | GET | /img/illustrations/wave... | | 200 | 130011 | XML | |

```
GET / HTTP/2
Host: tryhackme.com
Cookie: optimizelyEndUserId=
oeu1717498718877r0.21040242899
02212; AMP_d09a34bd2d=
JTdCJTIyZGV2aWNlSWQlMjIlM0ElMj
JiNDZkMjdkZS04ZjI4LTRhMTkt0TU1
My1kMjFlYzllMTE4OTklMjIlMkMlMj
J1c2VySWQlMjIlM0ElMjIlMjIlMkMl
MjJzZXNzaW9uSWQlMjIlM0ExNzE3ND
k4NzIyNjE2JTJDJTIyb3B0T3V0JTIy
JTNBZmFsc2UlMkMlMjJsYXN0RXZlbn
RUaW1lJTIyJTNBMTcxNzQ5ODcyMjYx
NiUyQyUyMmxhc3RFdmVudElkJTIyJT
NBMCU3RA==; _ga_Z8D4WL3D4P=
GS1.1.1717498723.1.0.171749872
3.60.0.0; _ga=
GA1.1.1242537483.1717498724;
cf_clearance=
_nsFFuRqNdVw.mACPDzNpbCumafenB
mnLu3k6X48TsI-1717498723-1.0.1
.1-GhFX3OFID06rmmevk0zp_CrFDRD
t9oTLqDgbFay5xSUu6OPz2aku7Fw1R
5_7HxlNPxVuoUOxYWEw.v_LEVbOSA;
 _hjSessionUser_1950941=
eyJpZCI6ImFiMmM4MmQzLWFkZWQtNT
RkMC1hMjg5LTNmZDg2ZGExZTYzZCIs
ImNyZWF0ZWQiOjE3MTc0OTg3MjM5Mz
ksImV4aXN0aW5nIjpmYWxzZX0=;
  hstc=
```

| | | |
|---|---|---|
| Request attributes | 2 | ⌄ |
| Request cookies | 11 | ⌄ |
| Request headers | 26 | ⌄ |
| Response headers | 11 | ⌄ |

We can clean this up by right clicking on the tryhackme request and selecting *Add to scope*.

**Made by Moeez Javed**


Burp Suite Community Edition v2024.3.1.4 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Se
Organizer Extensions Learn
Site map Scope Issue definitions
Pro version only
Request
Response
Pretty Raw Hex \n
Inspector
https://tryhackme.com/
Add to scope
Scan
Engagement tools [Pro version only]
Compare site maps
Expand branch
Expand requested items
Delete host
Copy URLs in this host
Copy links in this host
Save selected items
Site map documentation

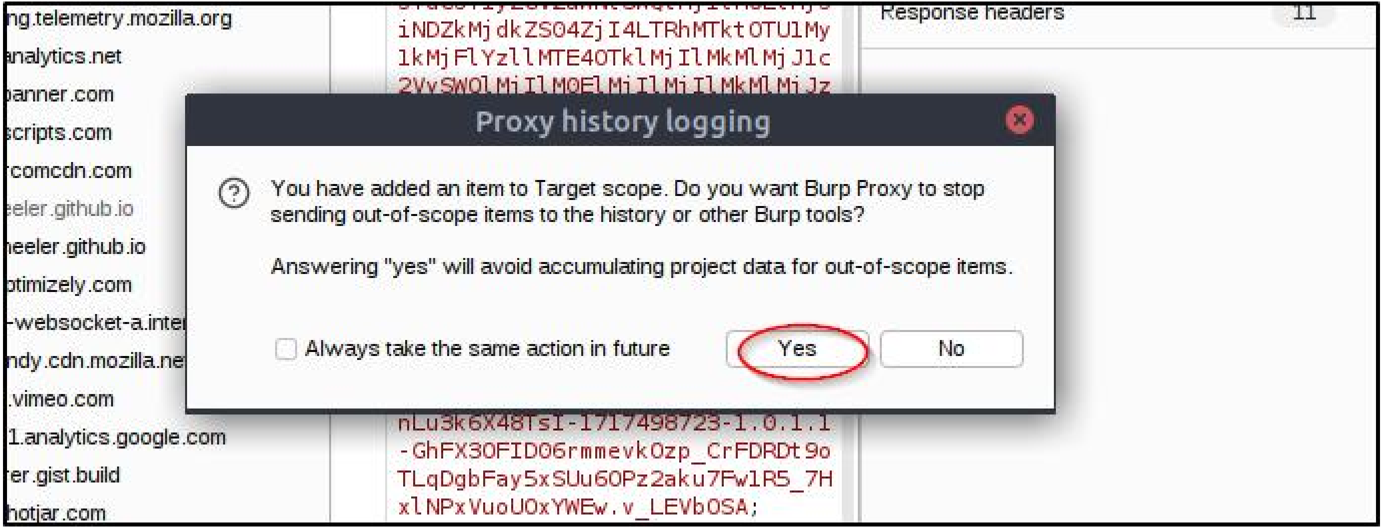
Site map filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

- https://a24671560256.cdn.optimizely.com
- https://api-iam.intercom.io
- https://assets.customer.io
- https://assets.gist.build
- https://assets.tryhackme.com
- https://aus5.mozilla.org
- https://cdn.amplitude.com
- https://cdn.optimizely.com
- https://challenges.cloudflare.com
- https://classify-client.services.mozilla.com
- https://code.gist.build
- https://content-signature-2.cdn.mozilla.net
- https://contile.services.mozilla.com
- https://downloads.intercomcdn.com
- https://engine-consumer-api.cloud.gist.build
- https://f.vimeocdn.com
- https://fresnel.vimeocdn.com
- https://i.vimeocdn.com
- https://incoming.telemetry.mozilla.org
- https://js.hs-analytics.net
- https://js.hs-banner.com
- https://js.hs-scripts.com
- https://js.intercomcdn.com
- http://kenwheeler.github.io
- https://kenwheeler.github.io
- https://logx.optimizely.com
- https://nexus-websocket-a.intercom.io
- https://normandy.cdn.mozilla.net
- https://player.vimeo.com
- https://region1.analytics.google.com
- https://renderer.gist.build
- https://script.hotjar.com
- https://services.addons.mozilla.org
- https://static.hotjar.com
- https://stats.g.doubleclick.net
- http://tryhackme.com
- https://tryhackme.com
- https://versioncheck-bg.addons.mozilla.org
- https://vimeo.com
- https://widget.intercom.io
- https://www.google.com
- https://www.googletagmanager.com
- https://www.gstatic.com

| Host | Method | URL | Params | Status Code | Length | MIME type |
|---|---|---|---|---|---|---|
| https://tryhackme.com | GET | / | | 200 | 38648 | HTML |
| https://tryhackme.com | GET | /api/site-stats | | 200 | 762 | JSON |
| https://tryhackme.com | GET | /assets/pace/pace.js | | 200 | 28469 | script |
| https://tryhackme.com | POST | /cdn-cgi/challenge-pla... | ✓ | 200 | 582 | |
| https://tryhackme.com | GET | /cdn-cgi/challenge-pla... | ✓ | 200 | 8059 | script |
| https://tryhackme.com | GET | /cdn-cgi/scripts/5c5dd... | | 200 | 1624 | script |
| https://tryhackme.com | GET | /img/getting-started/ro... | | 200 | 60669 | XML |
| https://tryhackme.com | GET | /img/illustrations/wave... | | 200 | 130011 | XML |

```
GET / HTTP/2
Host: tryhackme.com
Cookie: optimizelyEndUserId=
oeu1717498718877r0.21040242899022
12; AMP_d09a34bd2d=
JTdCJTIyZGV2aWNlSWQlMjIlM0ElMjJ
iNDZkMjdkZS04ZjI4LTRhMTktOTU1My
1kMjFlYzllMTE4OTklMjIlMkMlMjJ1c
2VySWQlMjIlM0ElMjIlMjIlMkMlMjJz
ZXNzaW9uSWQlMjIlM0ExNzE3NDk4NzI
yNjE2JTJDJTIyb3B0T3V0JTIyJTNBZm
Fsc2UlMkMlMjJsYXN0RXZlbnRUaW1lJ
TIyJTNBMTcxNzQ5ODcyMjYxNiUyQyUy
Mmxhc3RFdmVudElkJTIyJTNBMCU3RA=
=; _ga_Z8D4WL3D4P=
GS1.1.1717498723.1.0.1717498723
.60.0.0; _ga=
GA1.1.1242537483.1717498724;
cf_clearance=
_nsFFuRqNdVw.mACPDzNpbCumafenBm
nLu3k6X48TsI-1717498723-1.0.1.1
-GhFX3OFID06rmmevkOzp_CrFDRDt9o
TLqDgbFay5xSUu60Pz2aku7Fw1R5_7H
xlNPxVuoUOxYWEw.v_LEVbOSA;
_hjSessionUser_1950941=
eyJpZCI6ImFiMmM4MmQzLWFkZWQtNTR
kMC1hMjg5LTNmZDg2ZGExZTYzZCIsIm
NyZWF0ZWQiOjE3MTc0OTg3MjM5MzksI
mV4aXN0aW5nIjpmYWxzZX0=; __hstc
=
256179476.0f0c7aaaf803d80816d37
17174
a3154
30887
6=
458c5
6=
1d92b
11;
.09.0)
9.0
l+xml
ge/av
q=0.5
```

| Inspector | |
|---|---|
| Request attributes | 2 |
| Request cookies | 11 |
| Request headers | 26 |
| Response headers | 11 |



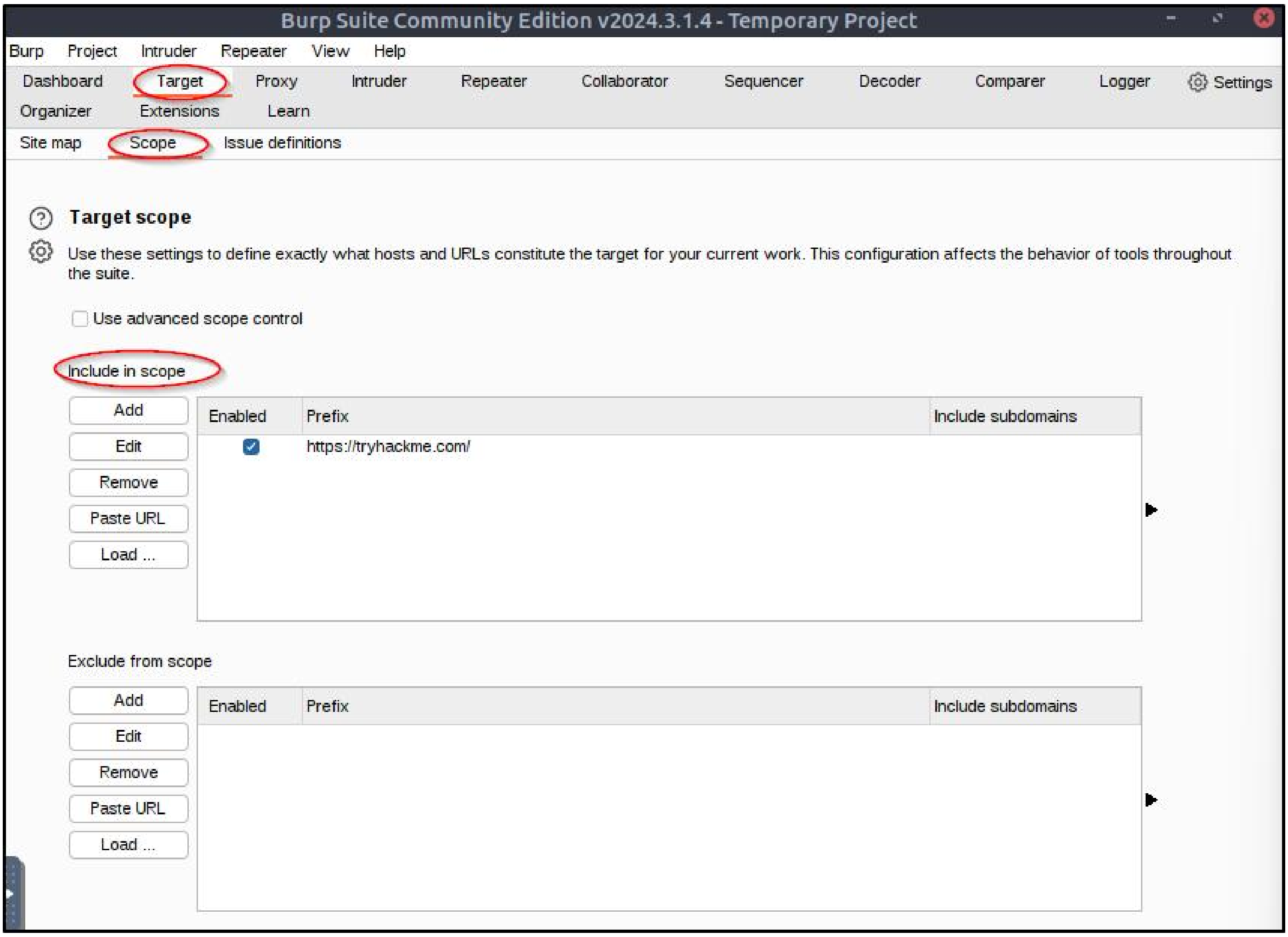
**Proxy history logging**

You have added an item to Target scope. Do you want Burp Proxy to stop sending out-of-scope items to the history or other Burp tools?

Answering "yes" will avoid accumulating project data for out-of-scope items.

☐ Always take the same action in future

You can also edit your scope in the Target Scope tab.



Burp Suite Community Edition v2024.3.1.4 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Settings
Organizer Extensions Learn
Site map Scope Issue definitions

**Target scope**

Use these settings to define exactly what hosts and URLs constitute the target for your current work. This configuration affects the behavior of tools throughout the suite.

☐ Use advanced scope control

Include in scope

Add
Edit
Remove
Paste URL
Load ...

| Enabled | Prefix | Include subdomains |
|---|---|---|
| ☑ | https://tryhackme.com/ | |

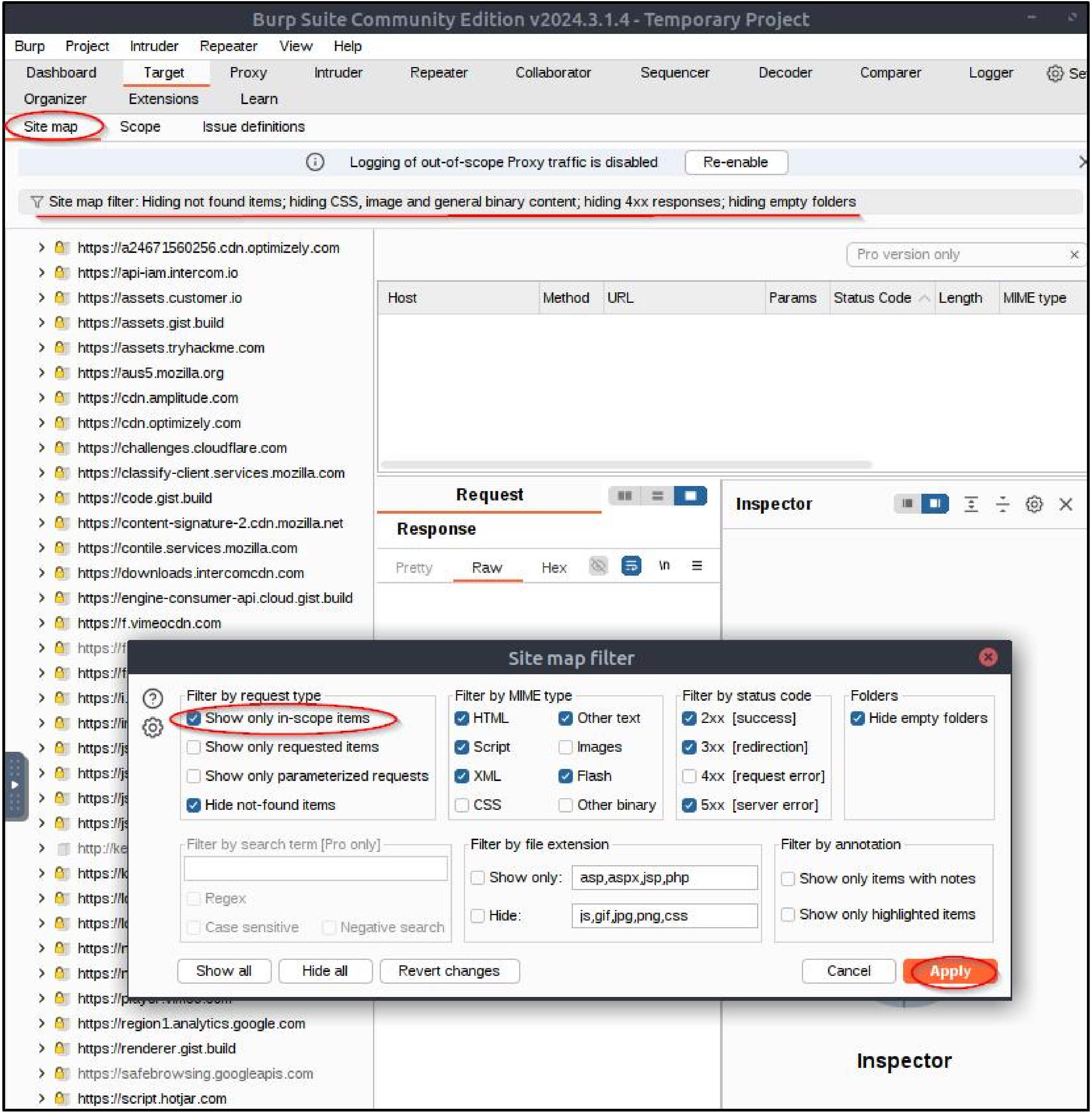
Exclude from scope

Add
Edit
Remove
Paste URL
Load ...

| Enabled | Prefix | Include subdomains |
|---|---|---|

Target > Scope > Include in scope

Next, return to the Site map tab, click on the Site map filter towards the top, and we want to tell Burp to show only in-scope items.



Burp Suite Community Edition v2024.3.1.4 - Temporary Project

Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Se
Organizer Extensions Learn
Site map Scope Issue definitions

Logging of out-of-scope Proxy traffic is disabled Re-enable

Site map filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

- https://a24671560256.cdn.optimizely.com
- https://api-iam.intercom.io
- https://assets.customer.io
- https://assets.gist.build
- https://assets.tryhackme.com
- https://aus5.mozilla.org
- https://cdn.amplitude.com
- https://cdn.optimizely.com
- https://challenges.cloudflare.com
- https://classify-client.services.mozilla.com
- https://code.gist.build
- https://content-signature-2.cdn.mozilla.net
- https://contile.services.mozilla.com
- https://downloads.intercomcdn.com
- https://engine-consumer-api.cloud.gist.build
- https://f.vimeocdn.com
- https://region1.analytics.google.com
- https://renderer.gist.build
- https://safebrowsing.googleapis.com
- https://script.hotjar.com

Site map filter

Filter by request type
- ☑ Show only in-scope items
- □ Show only requested items
- □ Show only parameterized requests
- ☑ Hide not-found items

Filter by MIME type
- ☑ HTML ☑ Other text
- ☑ Script □ Images
- ☑ XML ☑ Flash
- □ CSS □ Other binary

Filter by status code
- ☑ 2xx [success]
- ☑ 3xx [redirection]
- □ 4xx [request error]
- ☑ 5xx [server error]

Folders
- ☑ Hide empty folders

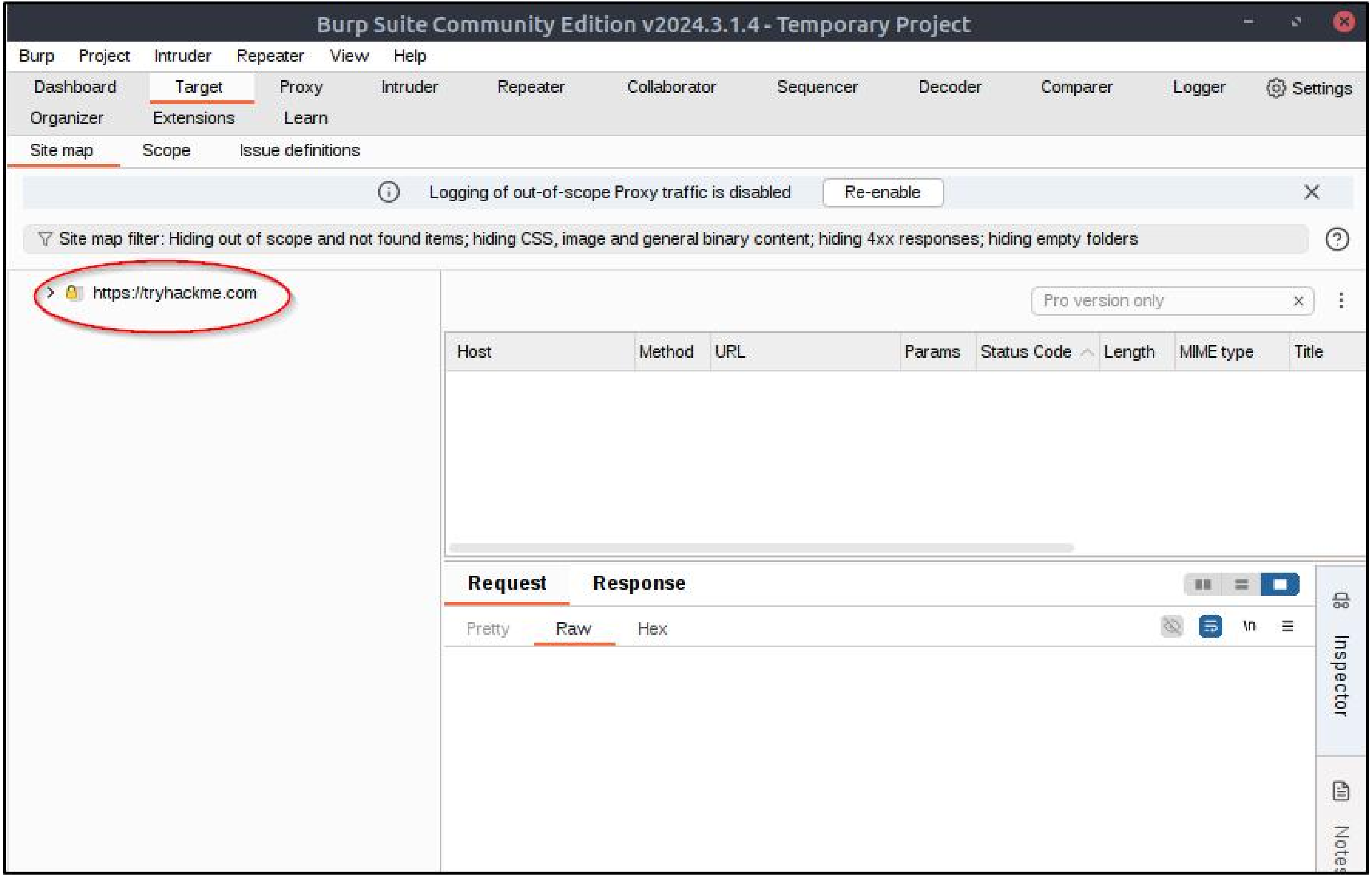
Filter by search term [Pro only]
- □ Regex
- □ Case sensitive □ Negative search

Filter by file extension
- □ Show only: asp,aspx,jsp,php
- □ Hide: js,gif,jpg,png,css

Filter by annotation
- □ Show only items with notes
- □ Show only highlighted items

Target > Site map > Site map filter > Show only in-scope items > Apply

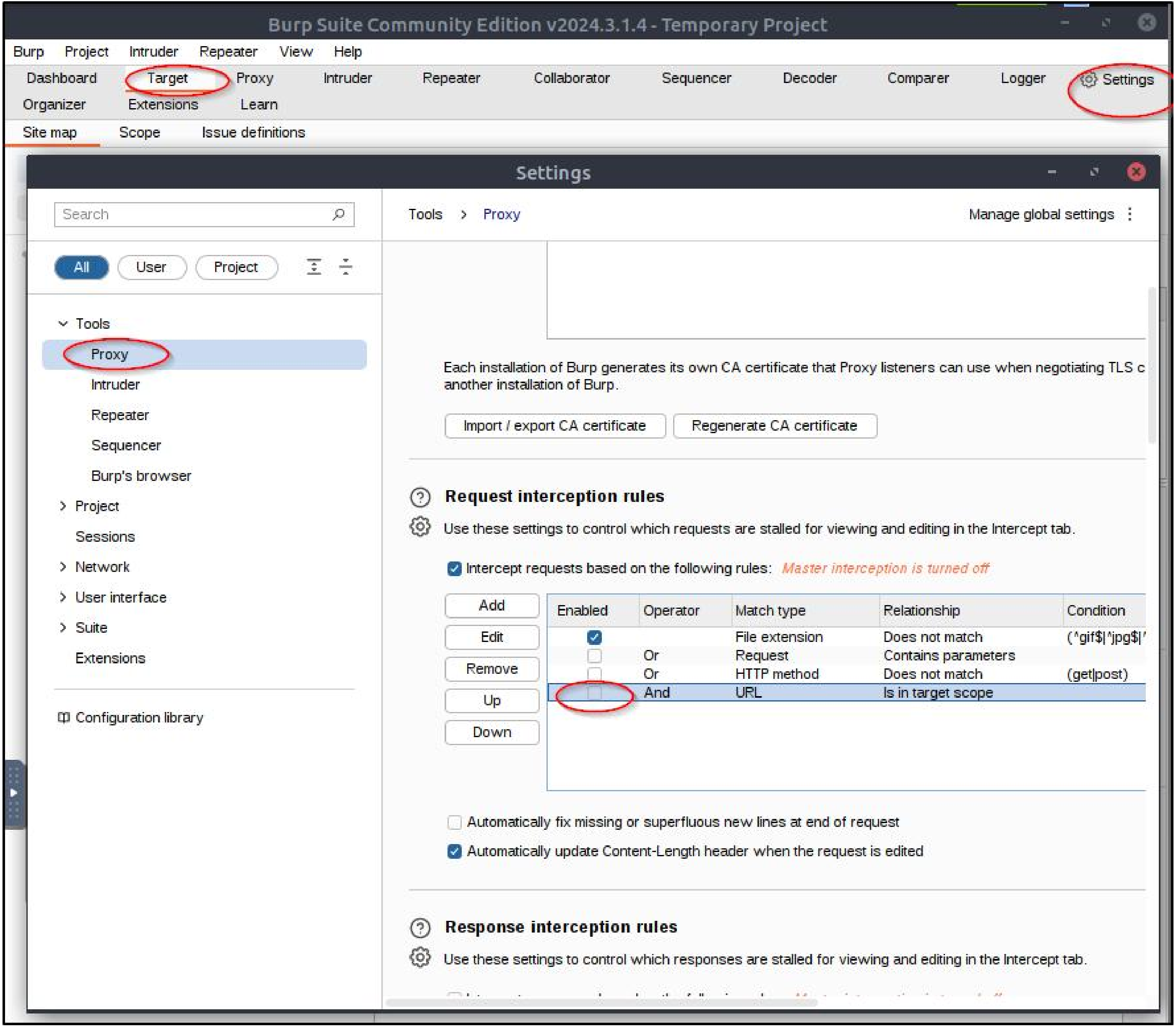
Now we have cleaned it up, and the tree structure shows only our target scope: https://tryhackme.com



Logging of out-of-scope Proxy traffic is disabled

Site map filter: Hiding out of scope and not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

Even though we are only focusing on the target scope, the proxy is still intercepting everything. We can disable this by going to the proxy settings tab and selecting *And URL Is in target scope*.


Burp Suite Community Edition v2024.3.1.4 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Settings
Organizer Extensions Learn
Site map Scope Issue definitions
Settings
Search
All User Project
Tools
Proxy
Intruder
Repeater
Sequencer
Burp's browser
Project
Sessions
Network
User interface
Suite
Extensions
Configuration library
Tools > Proxy
Manage global settings

Each installation of Burp generates its own CA certificate that Proxy listeners can use when negotiating TLS c
another installation of Burp.

Import / export CA certificate
Regenerate CA certificate

**Request interception rules**

Use these settings to control which requests are stalled for viewing and editing in the Intercept tab.

☑ Intercept requests based on the following rules: *Master interception is turned off*

| Enabled | Operator | Match type | Relationship | Condition |
|---|---|---|---|---|
| ☑ | | File extension | Does not match | (^gif$\|^jpg$\|' |
| ☐ | Or | Request | Contains parameters | |
| ☐ | Or | HTTP method | Does not match | (get\|post) |
| ☐ | And | URL | Is in target scope | |

☐ Automatically fix missing or superfluous new lines at end of request

☑ Automatically update Content-Length header when the request is edited

**Response interception rules**

Use these settings to control which responses are stalled for viewing and editing in the Intercept tab.

Settings > Proxy > Request interception rules

When this option is enabled, the proxy will ignore any traffic that is not in scope.

## Burp Suite Proxy: Endpoint Validation

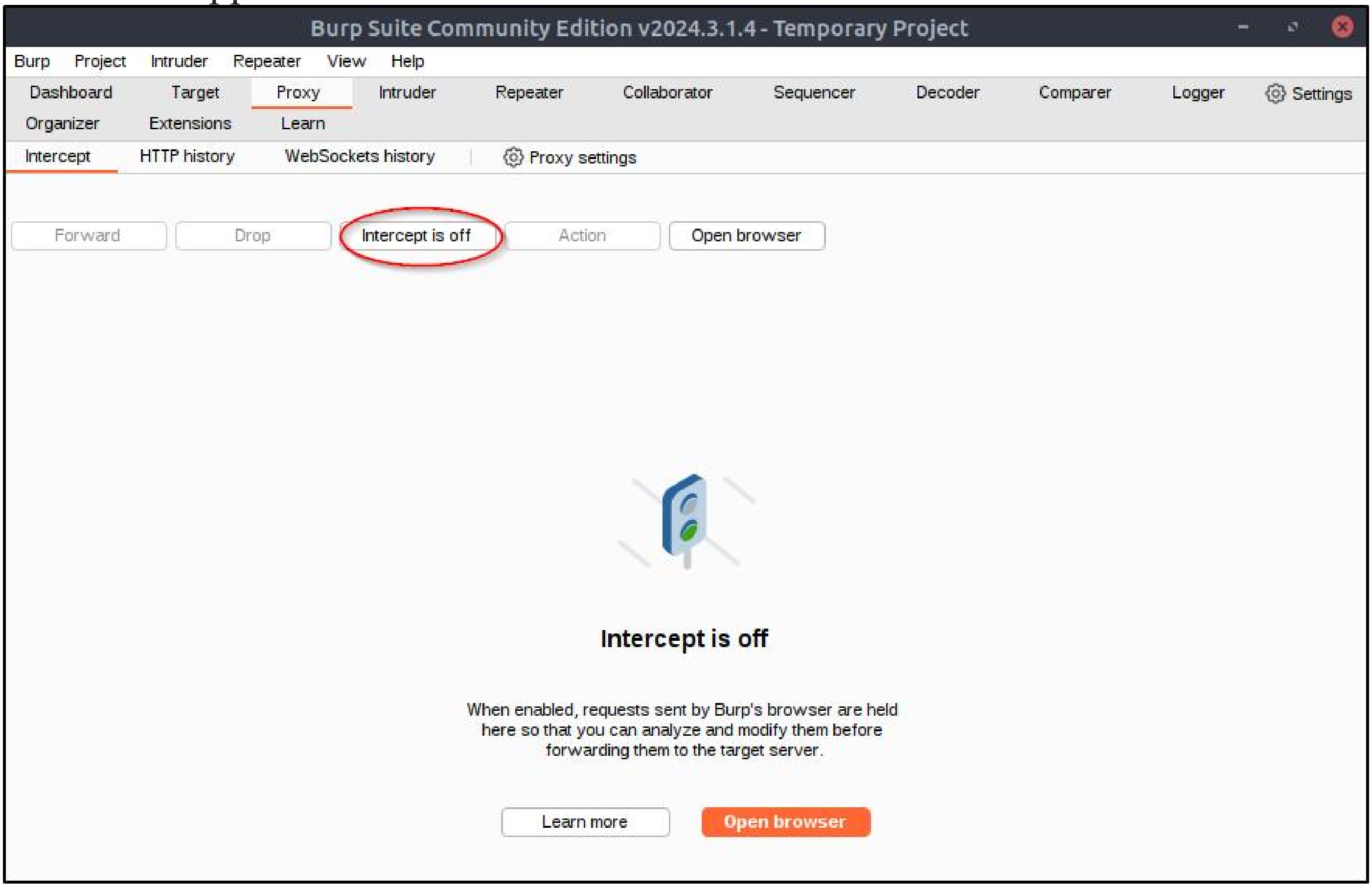
Now that you understand how Burp Suite captures and logs traffic, let’s explore how to intercept a web request and modify its contents before sending it to the web application.

This exercise demonstrates how to test a web application’s endpoint validation. Proper input validation is crucial for security, and endpoints that accept numeric values should ensure that the input is indeed a positive integer within an acceptable range to prevent potential vulnerabilities.

This example involves altering the HTTP Request data to see how the application responds. Obviously, I cannot demonstrate a test on a real system, so I am utilizing a target web application from tryhackme.com.

## STEP 1: Initial Setup

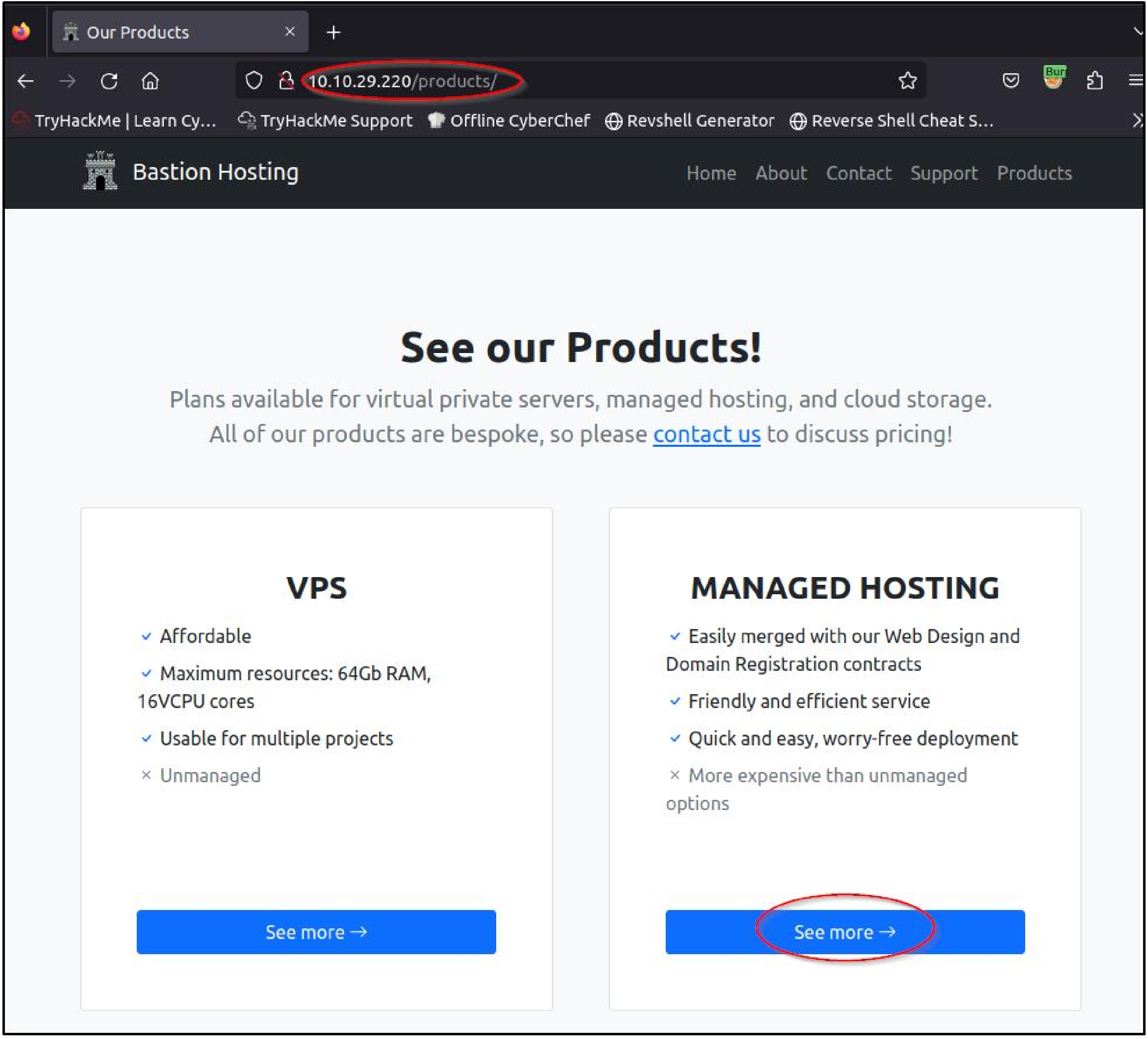
- Disable Burp Intercept and navigate to the target at *http://10.10.29.220/products*.
- Click on "See More" links to view different products and observe the URL pattern (e.g., */products/3*). The purpose is to identify and understand the web application structure



Intercept is off

When enabled, requests sent by Burp's browser are held here so that you can analyze and modify them before forwarding them to the target server.

**Made by Moeez Javed**



# See our Products!

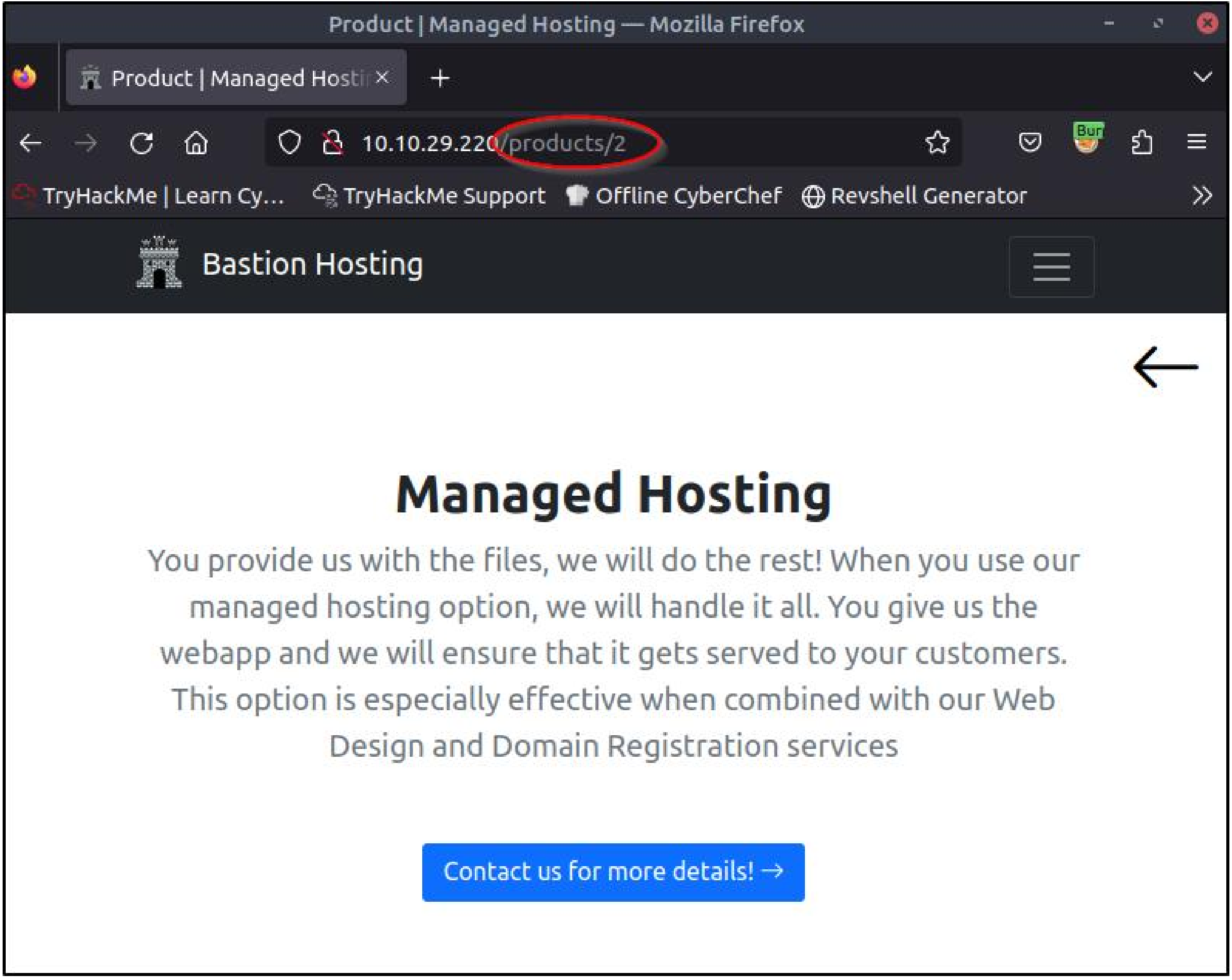
Plans available for virtual private servers, managed hosting, and cloud storage.
All of our products are bespoke, so please contact us to discuss pricing!

## VPS

- ✓ Affordable
- ✓ Maximum resources: 64Gb RAM, 16VCPU cores
- ✓ Usable for multiple projects
- × Unmanaged

## MANAGED HOSTING

- ✓ Easily merged with our Web Design and Domain Registration contracts
- ✓ Friendly and efficient service
- ✓ Quick and easy, worry-free deployment
- × More expensive than unmanaged options



Product | Managed Hosting — Mozilla Firefox

10.10.29.220/products/2

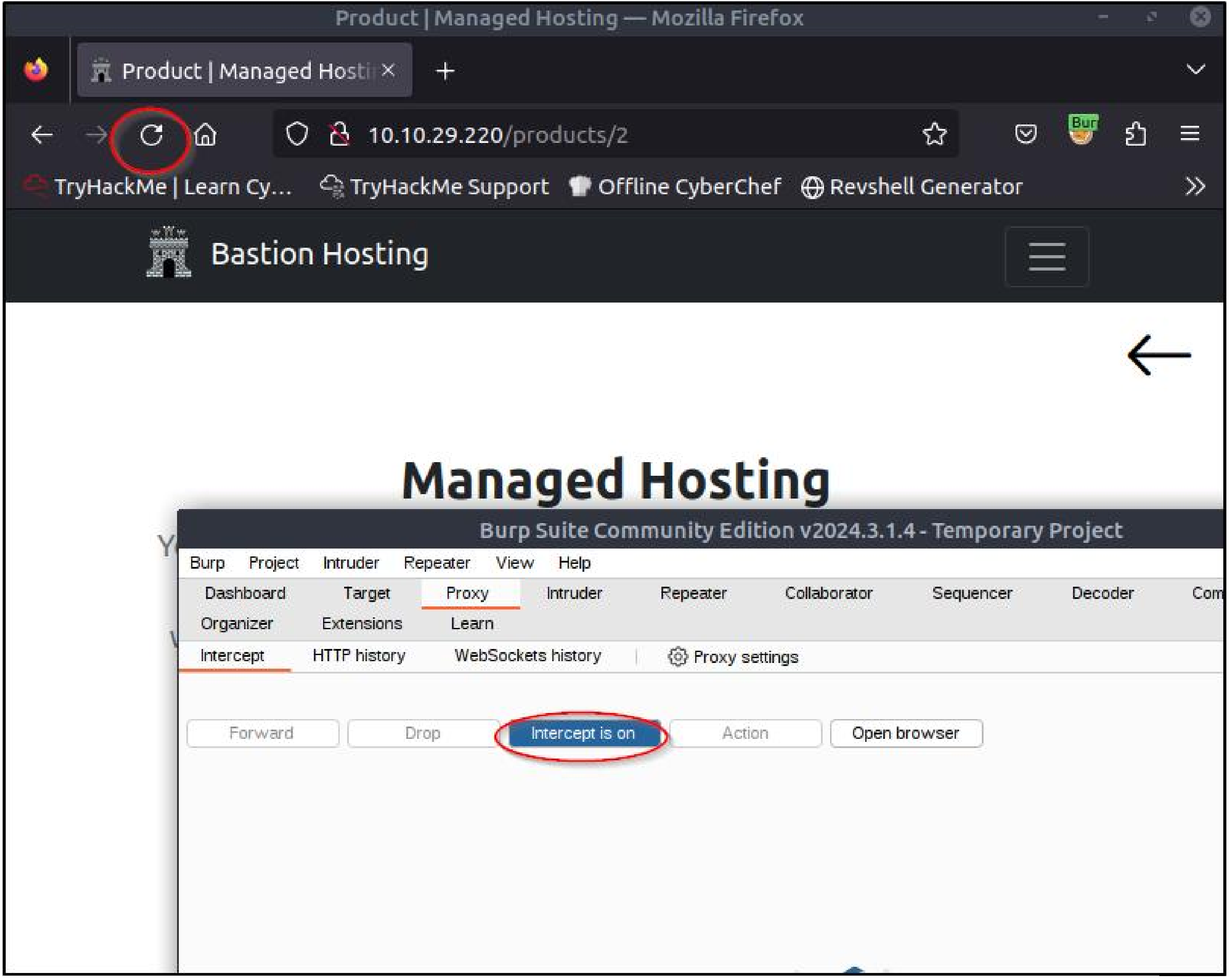
Bastion Hosting

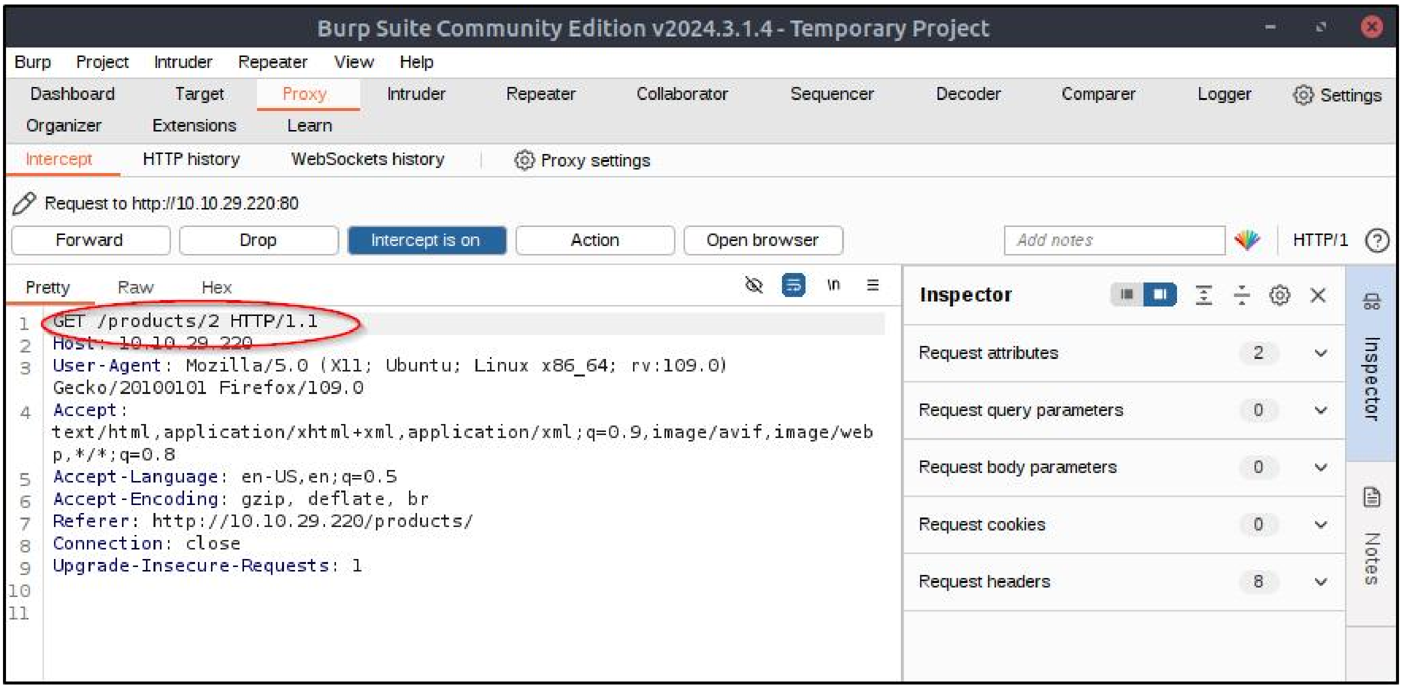
Managed Hosting

You provide us with the files, we will do the rest! When you use our managed hosting option, we will handle it all. You give us the webapp and we will ensure that it gets served to your customers. This option is especially effective when combined with our Web Design and Domain Registration services

## STEP 2: Capture a Request

- Enable Burp Intercept again and refresh the product page in order to capture the request in the Proxy tab.



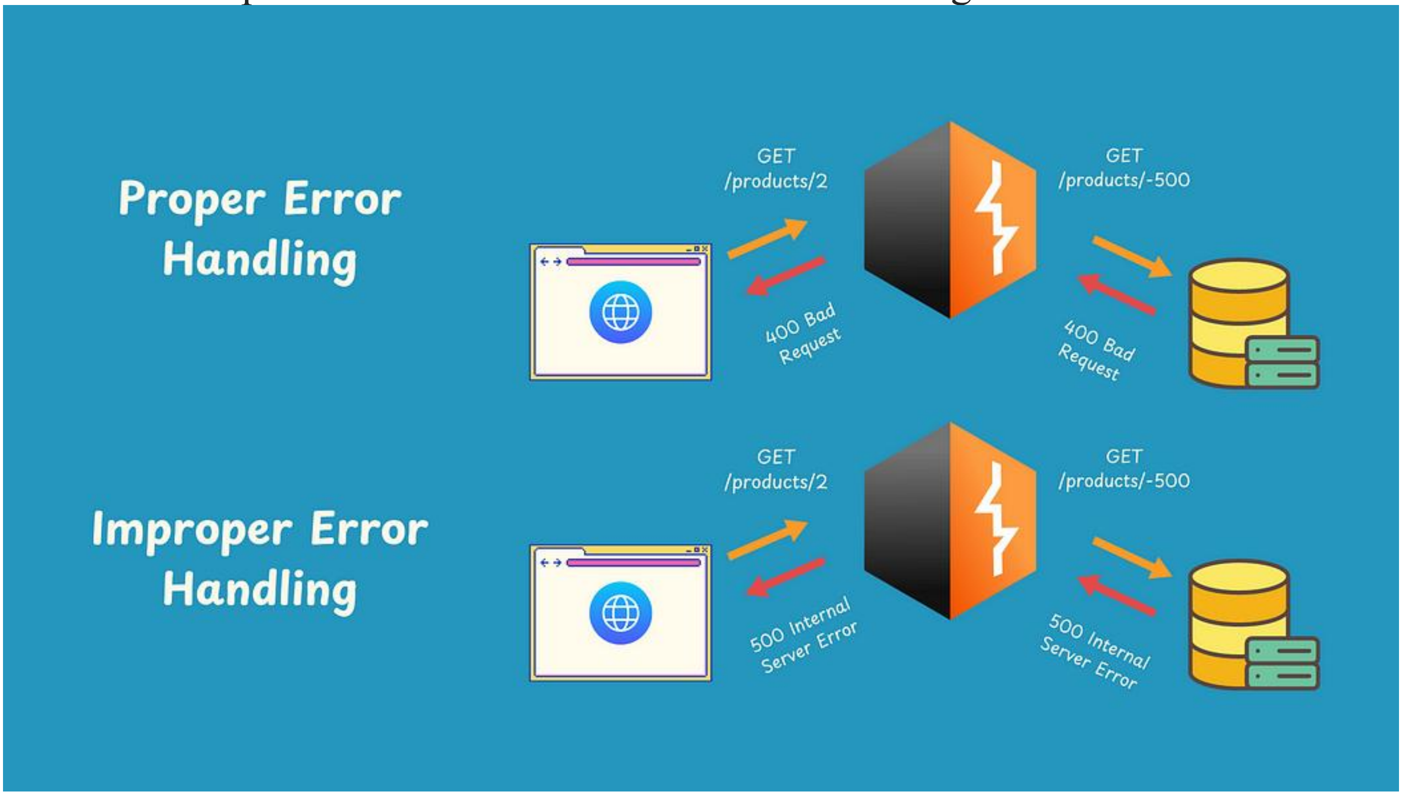


Request to http://10.10.29.220:80

```
GET /products/2 HTTP/1.1
Host: 10.10.29.220
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0)
Gecko/20100101 Firefox/109.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/web
p,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: http://10.10.29.220/products/
Connection: close
Upgrade-Insecure-Requests: 1
```

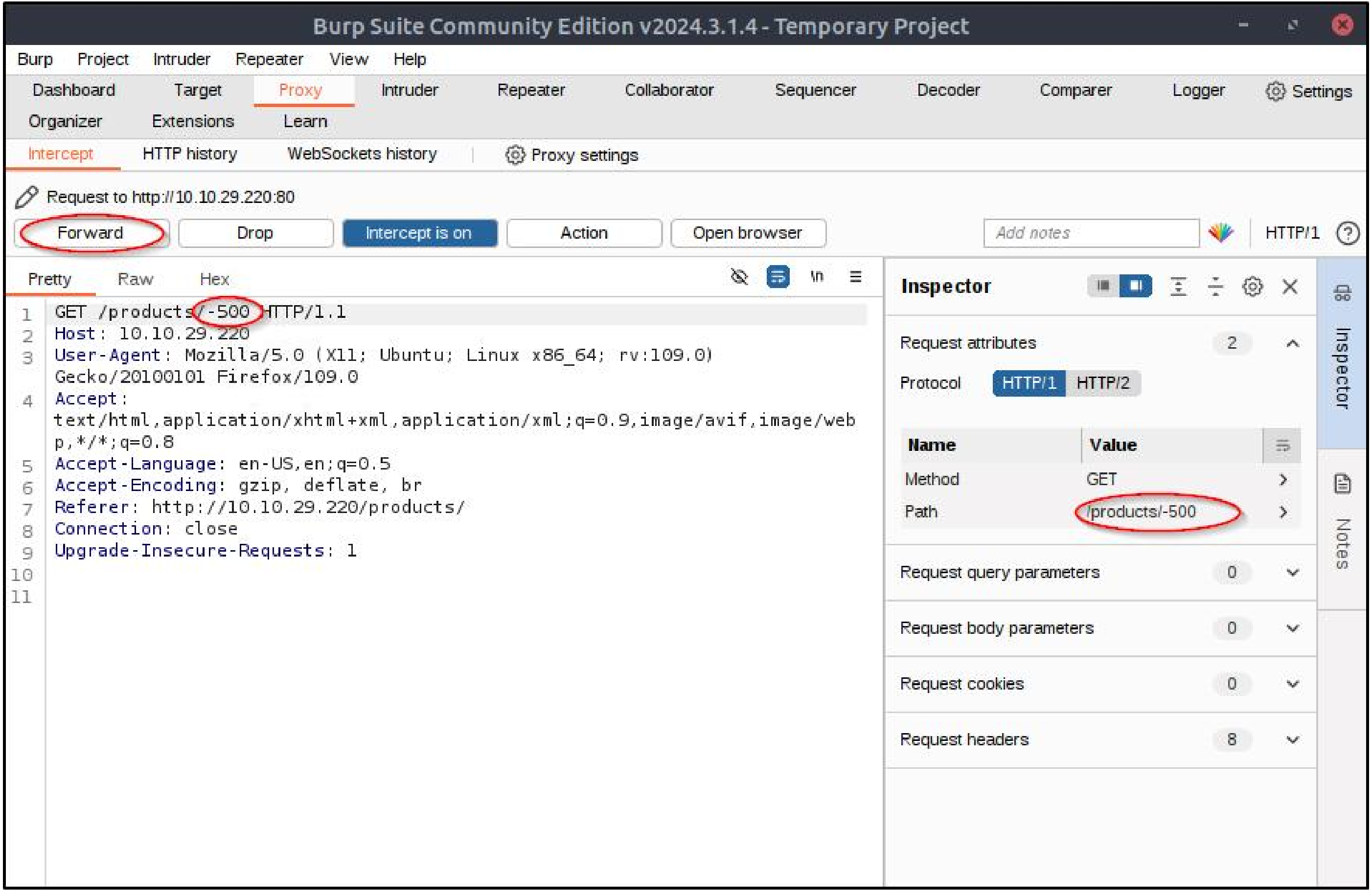
## STEP 3: Modify the Request

- Our goal is to test whether or not the application is properly validating inputs, thereby protecting against potential vulnerabilities.
- We can test for proper input validation by seeing how it responds to an unexpected condition. The product number in the target URL must be a positive integer within a certain range (e.g., */products/1* to */products/99*).
- What happens if we change the path to a negative number? How will the application respond? Proper error handling means that the endpoint should return a status code: 400 BAD REQUEST . A status code: 500 Internal Server Error typically means that an unhandled exception or error occurred on the server. This could be due to the application trying to process the negative value in a way that it wasn't designed to handle, leading to a crash or unexpected behavior.
- The server should not return 500 Internal Server Error for invalid inputs. This indicates a problem with the server-side validation logic.



- Before this request reaches the web application, modify the value of the GET path to -500. Once the path is altered, Forward the modified request to the web server. This can be done in the actual request on the left, or through the Inspector tab on the right.

**Made by Moeez Javed**

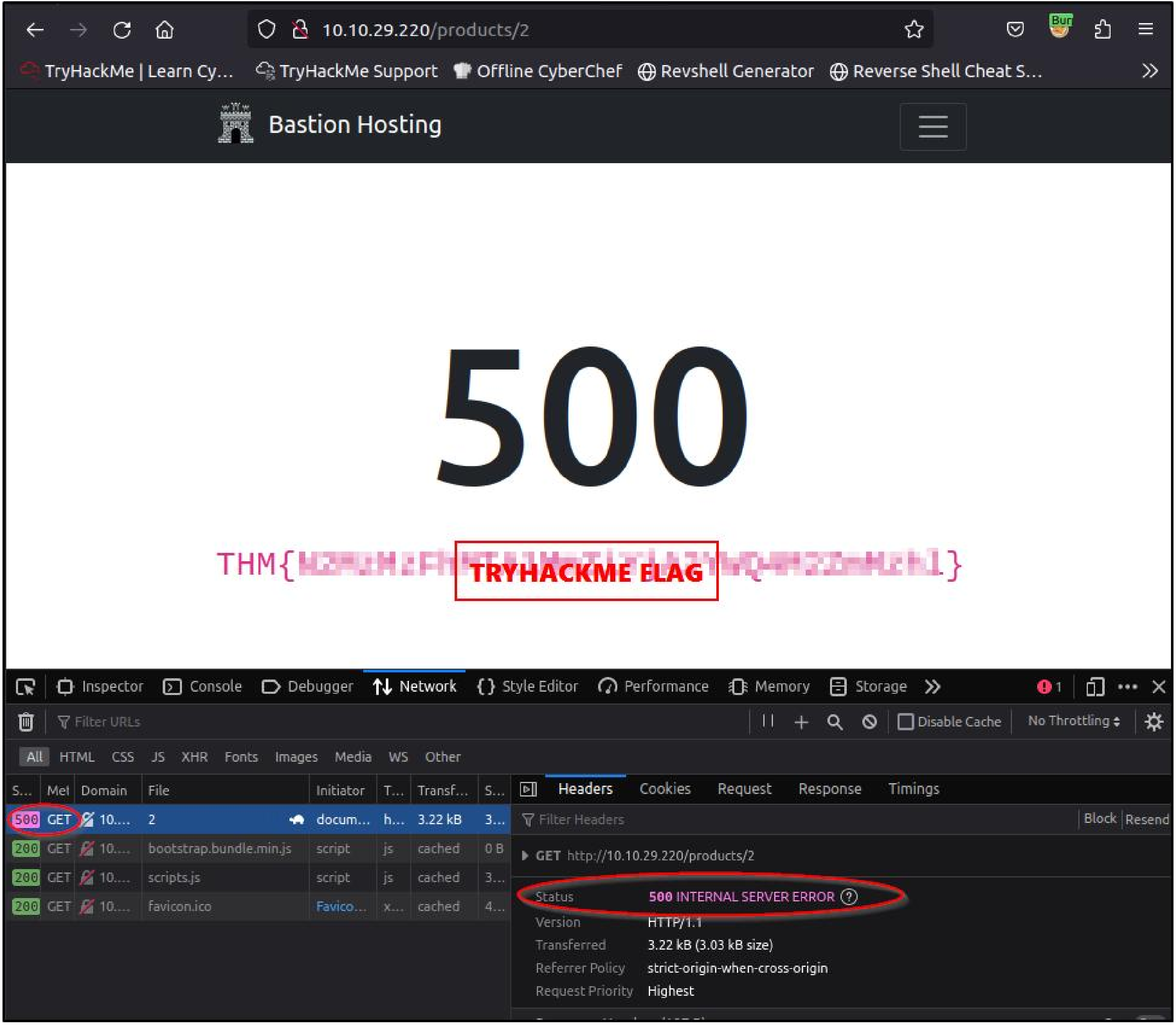


Burp Suite Community Edition v2024.3.1.4 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Settings
Organizer Extensions Learn
Intercept HTTP history WebSockets history Proxy settings
Request to http://10.10.29.220:80
Forward Drop Intercept is on Action Open browser
Add notes
HTTP/1
Pretty Raw Hex
Inspector
Request attributes 2
Protocol HTTP/1 HTTP/2
Request query parameters 0
Request body parameters 0
Request cookies 0
Request headers 8
Inspector
Notes

```
GET /products/-500 HTTP/1.1
Host: 10.10.29.220
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0)
Gecko/20100101 Firefox/109.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/web
p,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: http://10.10.29.220/products/
Connection: close
Upgrade-Insecure-Requests: 1


```

| Name | Value |
|---|---|
| Method | GET |
| Path | /products/-500 |

## STEP 4: Analyze the Response



10.10.29.220/products/2

TryHackMe | Learn Cy… TryHackMe Support Offline CyberChef Revshell Generator Reverse Shell Cheat S…

Bastion Hosting

500

THM{[redacted]}

TRYHACKME FLAG

| S… | Met | Domain | File | Initiator | T… | Transf… | S… |
|---|---|---|---|---|---|---|---|
| 500 | GET | 10.… | 2 | docum… | h… | 3.22 kB | 3… |
| 200 | GET | 10.… | bootstrap.bundle.min.js | script | js | cached | 0 B |
| 200 | GET | 10.… | scripts.js | script | js | cached | 3… |
| 200 | GET | 10.… | favicon.ico | Favico… | x… | cached | 4… |

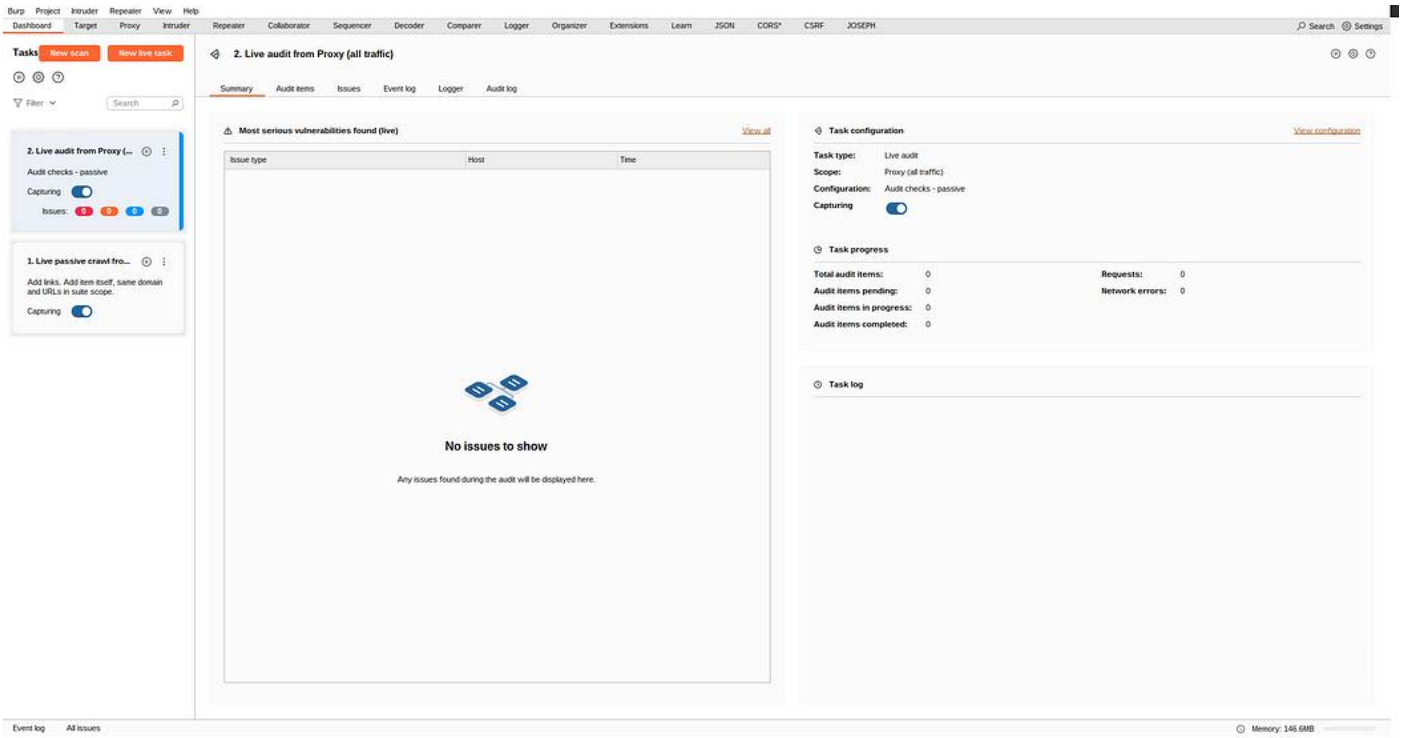
GET http://10.10.29.220/products/2

| | |
|---|---|
| Status | 500 INTERNAL SERVER ERROR |
| Version | HTTP/1.1 |
| Transferred | 3.22 kB (3.03 kB size) |
| Referrer Policy | strict-origin-when-cross-origin |
| Request Priority | Highest |

The presence of a 500 Internal Server Error when providing invalid input can be a sign of a potential vulnerability. It may indicate that the application does not have adequate error handling and input validation, which could be exploited by an attacker to cause denial of service, information disclosure, or other unintended behavior.

Using Burp Proxy is an efficient method to quickly test input validation. However, testing various input variations (e.g., a positive number out of range or a character value) would require multiple requests and interceptions. Fortunately, Burp Repeater simplifies this process.

We have covered how to set up and configure Burp Suite with FoxyProxy, observed how traffic is logged and mapped, and learned how to intercept, modify, and forward requests in real time. For those engaged in penetration testing or bug bounty hunting, much of your time will be spent using Burp Repeater and Burp Intruder. Hopefully, you learned a lot from this guide. In **Key Components of Burp Suite:**


Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn JSON CORS* CSRF JOSEPH
Search Settings
Tasks
New scan
New live task
Filter
Search
Summary Audit items Issues Event log Logger Audit log
View all
View configuration
Event log All issues
Memory: 146.6MB

2. Live audit from Proxy (…
Audit checks - passive
Capturing
Issues: 0 0 0 0

1. Live passive crawl fro…
Add links. Add item itself, same domain and URLs in suite scope.
Capturing

2. Live audit from Proxy (all traffic)

Most serious vulnerabilities found (live)

| Issue type | Host | Time |
|---|---|---|

No issues to show

Any issues found during the audit will be displayed here.

Task configuration

Task type: Live audit
Scope: Proxy (all traffic)
Configuration: Audit checks - passive
Capturing

Task progress

Total audit items: 0
Audit items pending: 0
Audit items in progress: 0
Audit items completed: 0
Requests: 0
Network errors: 0

Task log

- **Proxy Server:** Allows interception of traffic between your browser and the target application for detailed inspection and modification.
- **Scanner:** Automated vulnerability scanner for detecting security weaknesses within web applications.
- **Intruder:** A powerful tool for carrying out attacks against web apps, such as brute forcing, custom query attacks, and more.
- **Repeater:** Facilitates the manual modification and resending of individual HTTP requests.
- **Sequencer:** Analyzes the quality of randomness in an application’s session tokens.
- **Decoder:** A tool for decoding and encoding data into various formats.

**Focus on Automatic Vulnerability Scanner:** The automatic vulnerability scanner is a highlight of Burp Suite, designed to efficiently scan web applications for vulnerabilities. It performs both passive and active scans to provide a thorough examination of possible security issues.

## Features of the Automatic Scanner:

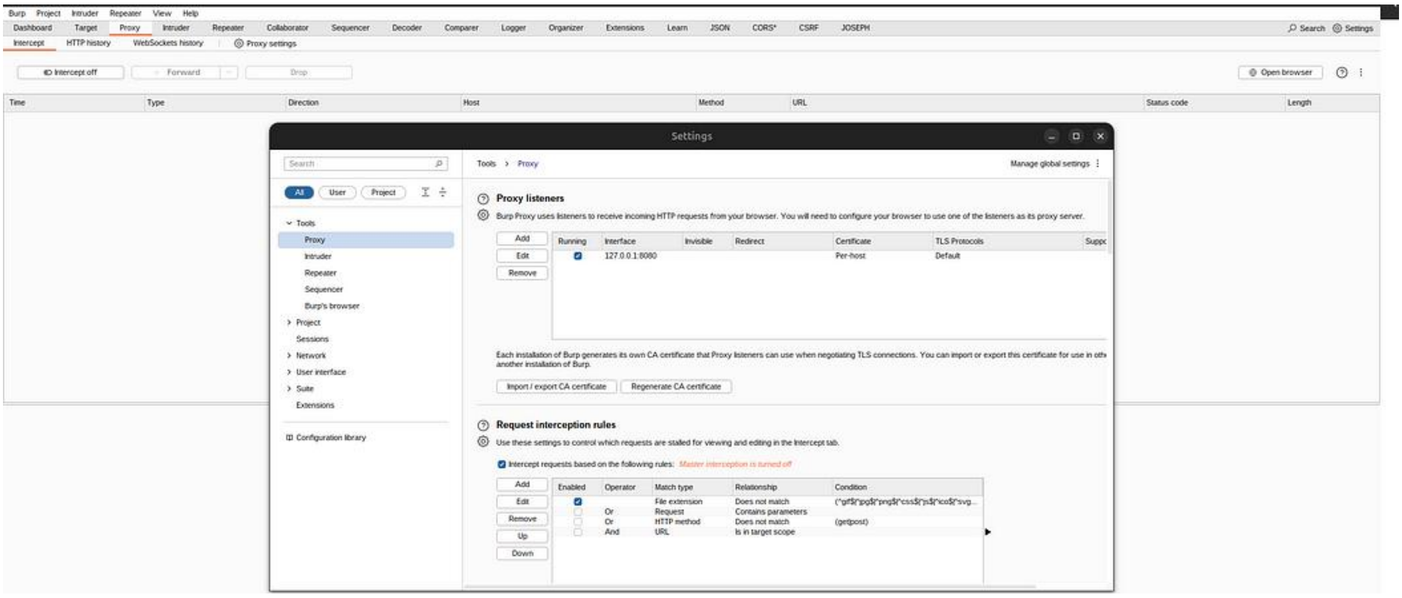
- **Comprehensive Scanning:** Combines both passive analysis as traffic passes through the proxy and active probing of known security vulnerabilities.
- **Configurable Levels of Testing:** Allows detailed control over the depth and breadth of tests conducted, which helps in managing testing speed and impact on the application.
- **Detailed Reporting:** Generates reports that categorize found vulnerabilities by type and severity, offering detailed evidence and remediation advice.

**Why Use Burp Suite's Automatic Scanner?** Using the automatic scanner can significantly streamline the vulnerability assessment process. It provides a fast, efficient method to identify weaknesses, which can then be examined in detail using Burp Suite's other tools. This capability makes it an invaluable part of the security testing toolkit, especially in environments where rapid testing and retesting are required.

# Running and Using the Automatic Vulnerability Scanner in Burp Suite

## Setting Up and Starting a Scan:

## Configure the Proxy:


Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn JSON CORS* CSRF JOSEPH
Search Settings
Intercept HTTP history WebSockets history Proxy settings
Intercept off
Forward
Drop
Open browser
Time Type Direction Host Method URL Status code Length
Settings
Search
All User Project
Tools
Proxy
Intruder
Repeater
Sequencer
Burp's browser
Project
Sessions
Network
User interface
Suite
Extensions
Configuration library
Tools > Proxy
Manage global settings
Add
Edit
Remove
Import / export CA certificate
Regenerate CA certificate
Add
Edit
Remove
Up
Down

**Proxy listeners**

Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser to use one of the listeners as its proxy server.

| Running | Interface | Invisible | Redirect | Certificate | TLS Protocols | Suppo |
|---|---|---|---|---|---|---|
| ☑ | 127.0.0.1:8080 | | | Per-host | Default | |

Each installation of Burp generates its own CA certificate that Proxy listeners can use when negotiating TLS connections. You can import or export this certificate for use in oth another installation of Burp.

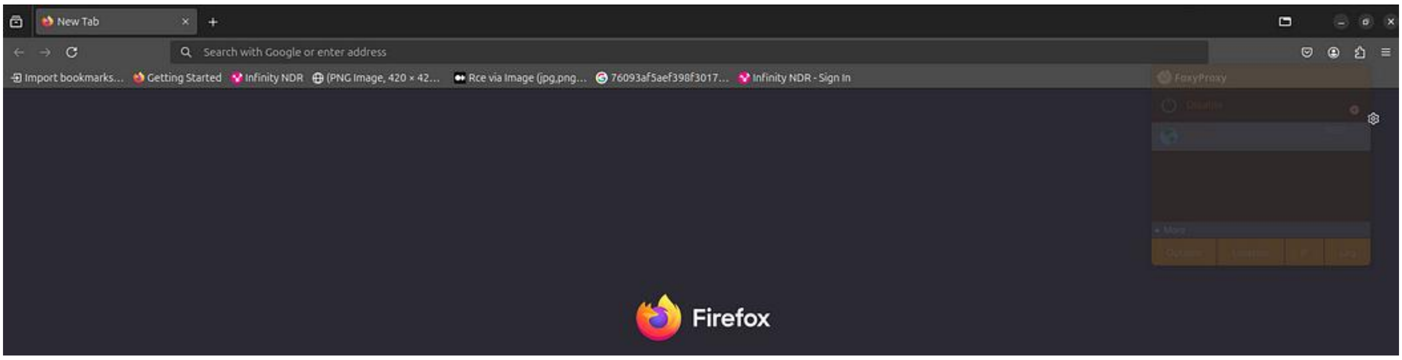
**Request interception rules**

Use these settings to control which requests are stalled for viewing and editing in the Intercept tab.

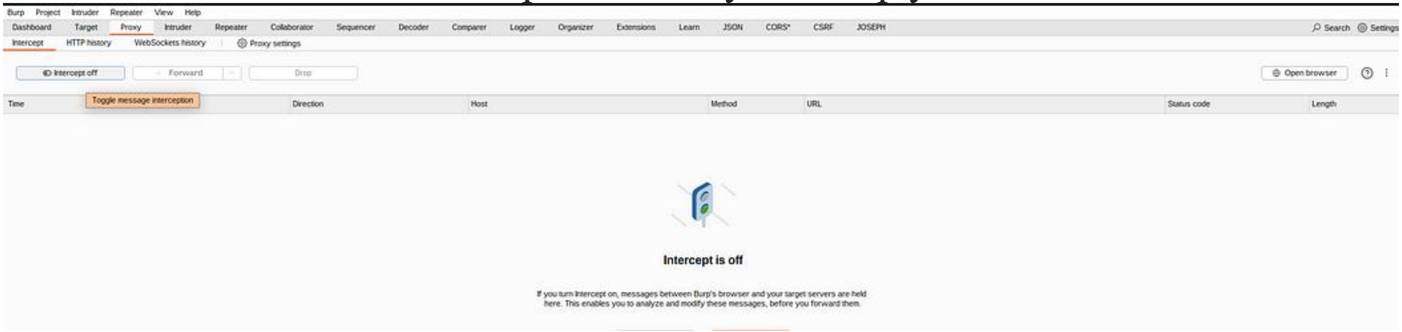
☑ Intercept requests based on the following rules: Master interception is turned off

| Enabled | Operator | Match type | Relationship | Condition |
|---|---|---|---|---|
| ☑ | | File extension | Does not match | (^gif$\|^jpg$\|^png$\|^css$\|^js$\|^ico$\|^svg... |
| □ | Or | Request | Contains parameters | |
| □ | Or | HTTP method | Does not match | (get\|post) |
| □ | And | URL | Is in target scope | |

- Ensure Burp Suite is set as the proxy server in your browser's network settings. In your browser I strongly recommended to use "FoxyProxy" extension.



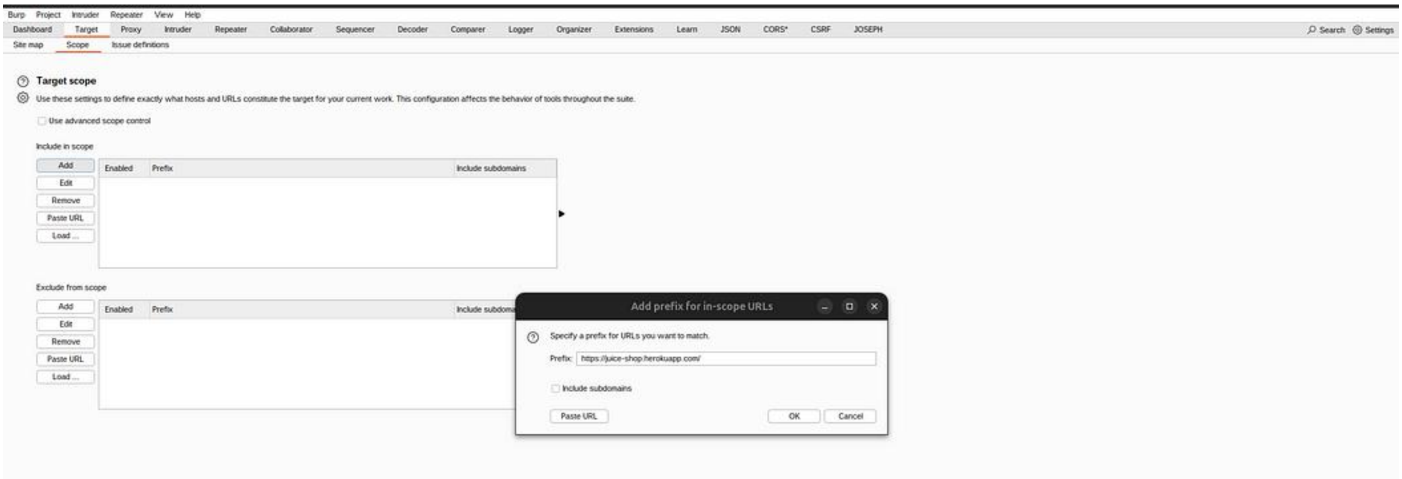
- This allows all web traffic to flow through Burp Suite, enabling it to capture and manipulate requests and responses.
- Access the **Proxy** tab and ensure the **Intercept** is on "Off" mode so that traffic flows without interruption while you set up your scan.



Intercept is off

If you turn Intercept on, messages between Burp's browser and your target servers are held here. This enables you to analyze and modify these messages, before you forward them.

## Define the Scope:



Target scope

Use these settings to define exactly what hosts and URLs constitute the target for your current work. This configuration affects the behavior of tools throughout the suite.

□ Use advanced scope control

Include in scope

Exclude from scope

Add prefix for in-scope URLs

Specify a prefix for URLs you want to match.

Prefix: https://juice-shop.herokuapp.com/

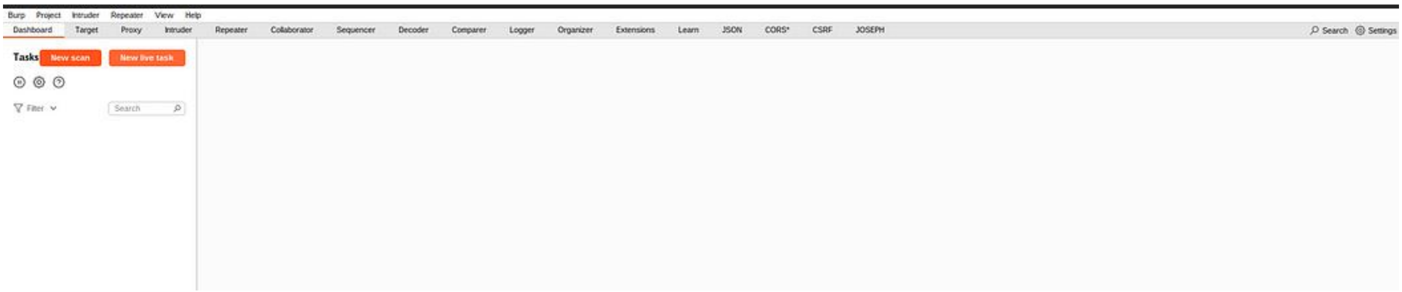
□ Include subdomains

- Navigate to the **Target** tab, right-click on the domain you want to test, and choose "Add to scope" if it's not already defined. This ensures that Burp Scanner focuses only on your target, avoiding external sites.

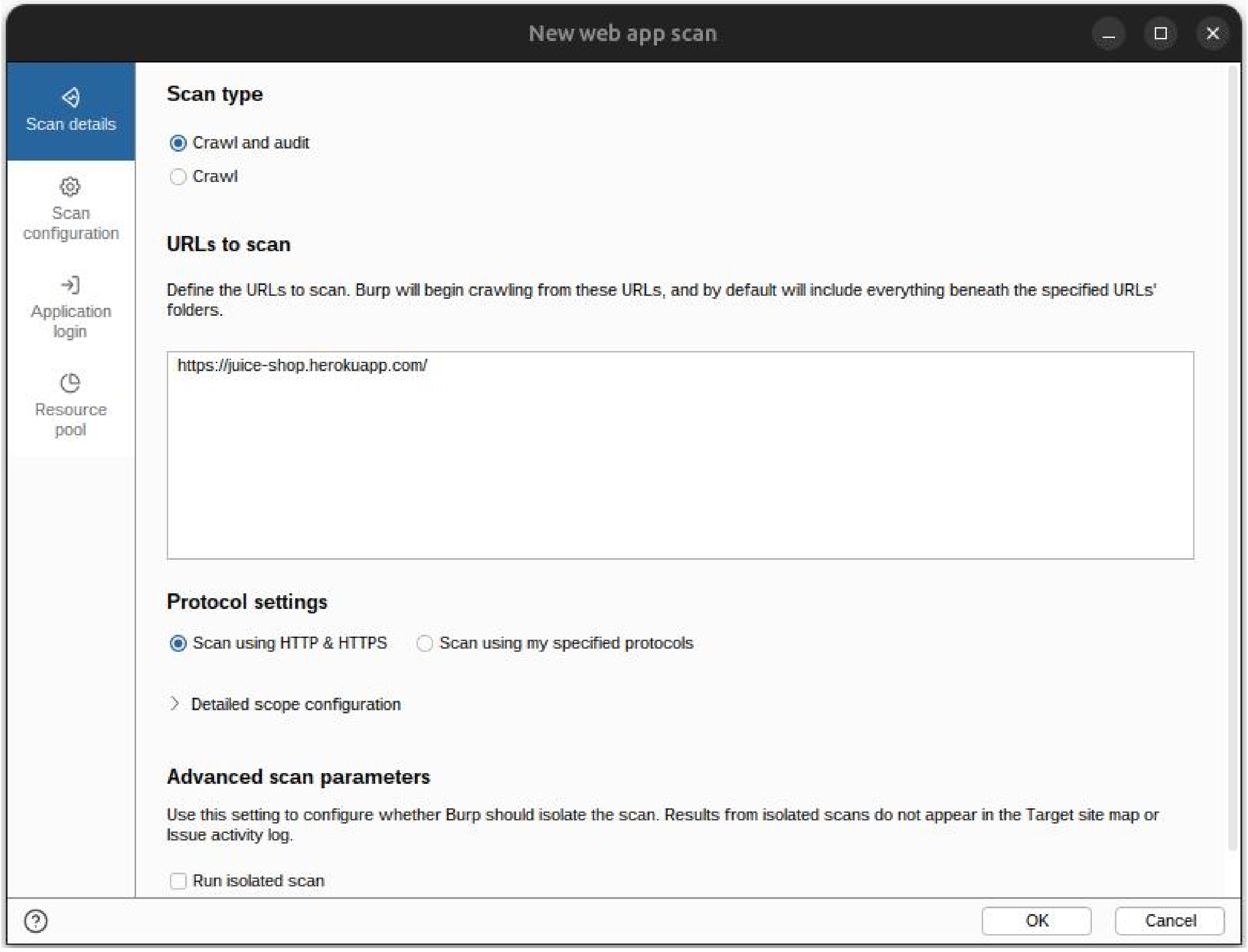
- Confirm scope configuration in the **Scope** tab under **Target** to ensure accuracy.

## Start the Scan:

- Go to the **Dashboard** tab and click on “New Scan.”



- Select either **Crawl and Audit** for a comprehensive scan or **Audit selected items** if you want to scan specific requests you’ve previously captured or modified.



**Scan type**

● Crawl and audit

○ Crawl

**URLs to scan**

Define the URLs to scan. Burp will begin crawling from these URLs, and by default will include everything beneath the specified URLs' folders.

https://juice-shop.herokuapp.com/

**Protocol settings**

● Scan using HTTP & HTTPS ○ Scan using my specified protocols

> Detailed scope configuration

**Advanced scan parameters**

Use this setting to configure whether Burp should isolate the scan. Results from isolated scans do not appear in the Target site map or Issue activity log.

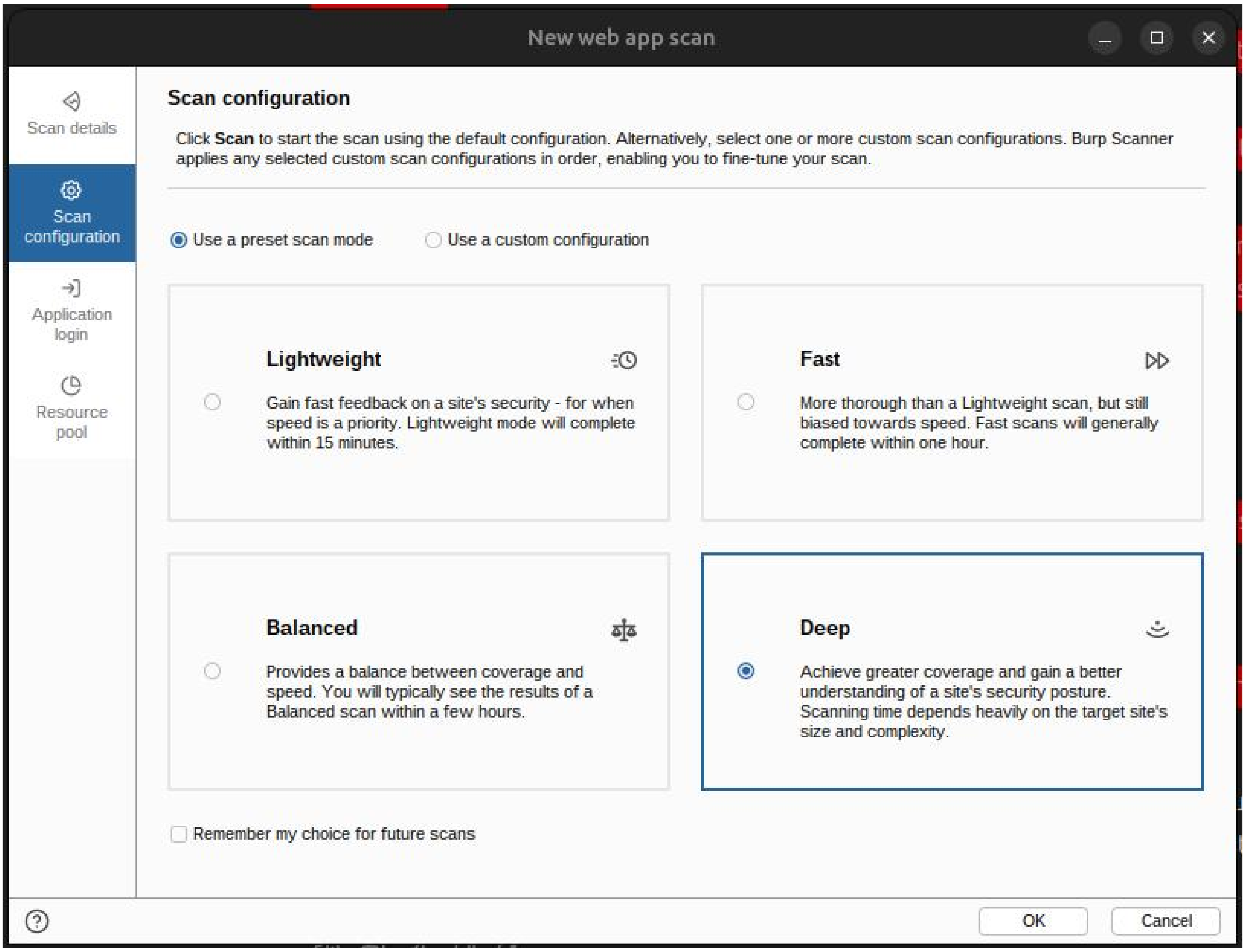
□ Run isolated scan

- Configure the scan settings by choosing the types of crawl and audit functions to perform. You can customize settings such as the number of concurrent requests, the types of data to submit in forms, and the handling of new cookies.

### Configure Scan Details:

- Under the **New Scan** setup, detail any specific cookies, headers, or request modifications that your scan should use. This step is crucial for applications that require authentication or custom headers to access.
- Use the **Crawl Strategy** options to determine how aggressively Burp Suite explores application content. Adjust the **Audit Speed** to control the balance between speed and server impact.

Burp Suite's vulnerability scanner, you can choose from different scan configurations, each designed to suit various scanning needs and scenarios. These configurations — light, balanced, deep, and fast — affect how thoroughly the scanner probes the target application and the load it imposes on the server. Here's a detailed look at each mode:



Scan configuration

Click **Scan** to start the scan using the default configuration. Alternatively, select one or more custom scan configurations. Burp Scanner applies any selected custom scan configurations in order, enabling you to fine-tune your scan.

● Use a preset scan mode ○ Use a custom configuration

○ **Lightweight**
Gain fast feedback on a site's security - for when speed is a priority. Lightweight mode will complete within 15 minutes.

○ **Fast**
More thorough than a Lightweight scan, but still biased towards speed. Fast scans will generally complete within one hour.

○ **Balanced**
Provides a balance between coverage and speed. You will typically see the results of a Balanced scan within a few hours.

● **Deep**
Achieve greater coverage and gain a better understanding of a site's security posture. Scanning time depends heavily on the target site's size and complexity.

□ Remember my choice for future scans

## Light Scan

- **Purpose:** The light scan is designed for minimal impact on the target's performance. It is best used when the target system is known to be sensitive to higher loads or when you need a quick overview without a detailed vulnerability assessment.
- **Characteristics:** This mode uses fewer requests and less aggressive methods. It generally avoids intensive tests that are likely to cause issues or noticeable performance degradation on the target.
- **Use Case:** Ideal for an initial quick check of a production system to identify glaring security issues without affecting the system's availability or performance.

## Balanced Scan

- **Purpose:** As the name suggests, this mode offers a balance between thoroughness and performance impact. It's designed to be a good default setting for most use cases.
- **Characteristics:** The balanced scan performs a more comprehensive examination than the light scan, but it does not delve as deeply as the deep scan. It carefully manages the trade-off between speed and load on the network or application.
- **Use Case:** Suitable for regular security diagnostics where you need a thorough assessment but cannot afford significant system impact. This is the go-to for routine scans in development or staging environments.

## Deep Scan

- **Purpose:** The deep scan is meant for the most exhaustive vulnerability assessment when maximum coverage is required, and the performance impact is a secondary concern.
- **Characteristics:** This mode is the most resource-intensive, utilizing a wide array of tests and attempting various inputs to uncover as many issues as possible. It can potentially impact system performance due to the high number of requests and complex attack simulations.

- **Use Case:** Best used in secure environments like pre-production or testing environments where you can afford downtime or performance degradation. It's ideal when preparing for security certifications or audits.

## Fast Scan

- **Purpose:** The fast scan focuses on speed, making it suitable for situations where time is critical. It scans quickly to give a rapid insight into the security posture of an application.
- **Characteristics:** It prioritizes speed over thoroughness, executing only the fastest tests. While it can identify obvious vulnerabilities, it may miss deeper, more subtle issues.
- **Use Case:** Useful for repeated scans during a rapid development phase when immediate feedback is necessary. It's also beneficial for initial scans in a larger security assessment process to quickly identify high-level vulnerabilities.

## Choosing the Right Mode

Selecting the right scan configuration depends on your specific needs:

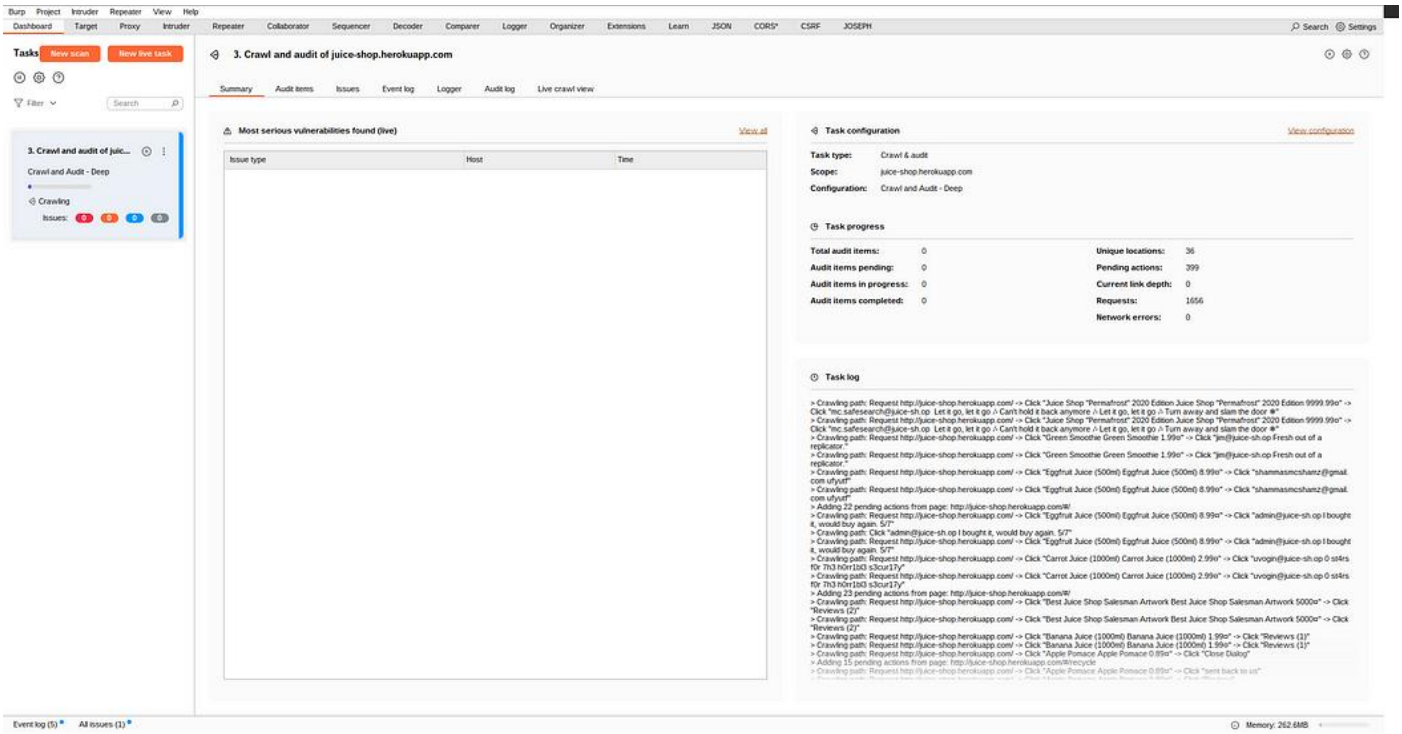
- **Risk Tolerance:** How critical is the application? How sensitive is the data it handles?
- **Environment:** Are you scanning a production system or a test environment?
- **Objective:** Is the goal to get a quick overview or an exhaustive examination?
- **Resource Availability:** How much impact on performance can the target system handle during the scan?

## Monitoring and Analyzing Results:

1. **Monitor the Scan:**

- Track the progress in the **Dashboard** where Burp Suite displays real-time information about requests made, issues found, and the overall progress of the scan.

- Use the live scanning report to review preliminary findings as they are identified.


Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn JSON CORS* CSRF JOSEPH
Search Settings
Tasks New scan New live task
Filter Search
3. Crawl and audit of juic...
Crawl and Audit - Deep
Crawling
Issues: 0 0 0 0
Summary Audit items Issues Event log Logger Audit log Live crawl view
View all
View configuration
Event log (5) All issues (1)
Memory: 262.6MB

3. Crawl and audit of juice-shop.herokuapp.com

Most serious vulnerabilities found (live)

| Issue type | Host | Time |
|---|---|---|

Task configuration

Task type: Crawl & audit
Scope: juice-shop.herokuapp.com
Configuration: Crawl and Audit - Deep

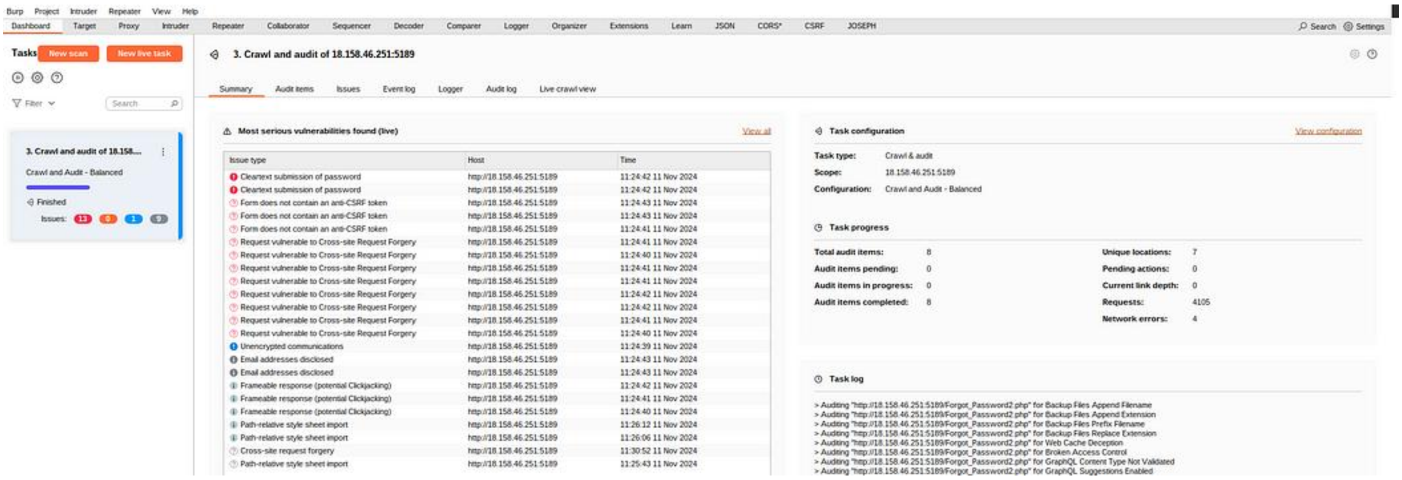
Task progress

| | | | |
|---|---|---|---|
| Total audit items: | 0 | Unique locations: | 36 |
| Audit items pending: | 0 | Pending actions: | 399 |
| Audit items in progress: | 0 | Current link depth: | 0 |
| Audit items completed: | 0 | Requests: | 1656 |
| | | Network errors: | 0 |

Task log

```
> Crawling path: Request http://juice-shop.herokuapp.com/ -> Click "Juice Shop "Permafrost" 2020 Edition Juice Shop "Permafrost" 2020 Edition 9999.99¤" -> Click "mc.safesearch@juice-sh.op  Let it go, let it go ♪ Can't hold it back anymore ♪ Let it go, let it go ♪ Turn away and slam the door ❄"
> Crawling path: Request http://juice-shop.herokuapp.com/ -> Click "Juice Shop "Permafrost" 2020 Edition Juice Shop "Permafrost" 2020 Edition 9999.99¤" -> Click "mc.safesearch@juice-sh.op  Let it go, let it go ♪ Can't hold it back anymore ♪ Let it go, let it go ♪ Turn away and slam the door ❄"
> Crawling path: Request http://juice-shop.herokuapp.com/ -> Click "Green Smoothie Green Smoothie 1.99¤" -> Click "jim@juice-sh.op Fresh out of a replicator."
> Crawling path: Request http://juice-shop.herokuapp.com/ -> Click "Green Smoothie Green Smoothie 1.99¤" -> Click "jim@juice-sh.op Fresh out of a replicator."
> Crawling path: Request http://juice-shop.herokuapp.com/ -> Click "Eggfruit Juice (500ml) Eggfruit Juice (500ml) 8.99¤" -> Click "shammasmcshamz@gmail.com ufyutf"
> Crawling path: Request http://juice-shop.herokuapp.com/ -> Click "Eggfruit Juice (500ml) Eggfruit Juice (500ml) 8.99¤" -> Click "shammasmcshamz@gmail.com ufyutf"
> Adding 22 pending actions from page: http://juice-shop.herokuapp.com/#/
> Crawling path: Request http://juice-shop.herokuapp.com/ -> Click "Eggfruit Juice (500ml) Eggfruit Juice (500ml) 8.99¤" -> Click "admin@juice-sh.op I bought it, would buy again. 5/7"
> Crawling path: Click "admin@juice-sh.op I bought it, would buy again. 5/7"
> Crawling path: Request http://juice-shop.herokuapp.com/ -> Click "Eggfruit Juice (500ml) Eggfruit Juice (500ml) 8.99¤" -> Click "admin@juice-sh.op I bought it, would buy again. 5/7"
> Crawling path: Request http://juice-shop.herokuapp.com/ -> Click "Carrot Juice (1000ml) Carrot Juice (1000ml) 2.99¤" -> Click "uvogin@juice-sh.op 0 st4rs f0r 7h3 h0rr1bl3 s3cur17y"
> Crawling path: Request http://juice-shop.herokuapp.com/ -> Click "Carrot Juice (1000ml) Carrot Juice (1000ml) 2.99¤" -> Click "uvogin@juice-sh.op 0 st4rs f0r 7h3 h0rr1bl3 s3cur17y"
> Adding 23 pending actions from page: http://juice-shop.herokuapp.com/#/
> Crawling path: Request http://juice-shop.herokuapp.com/ -> Click "Best Juice Shop Salesman Artwork Best Juice Shop Salesman Artwork 5000¤" -> Click "Reviews (2)"
> Crawling path: Request http://juice-shop.herokuapp.com/ -> Click "Best Juice Shop Salesman Artwork Best Juice Shop Salesman Artwork 5000¤" -> Click "Reviews (2)"
> Crawling path: Request http://juice-shop.herokuapp.com/ -> Click "Banana Juice (1000ml) Banana Juice (1000ml) 1.99¤" -> Click "Reviews (1)"
> Crawling path: Request http://juice-shop.herokuapp.com/ -> Click "Banana Juice (1000ml) Banana Juice (1000ml) 1.99¤" -> Click "Reviews (1)"
> Crawling path: Request http://juice-shop.herokuapp.com/ -> Click "Apple Pomace Apple Pomace 0.89¤" -> Click "Close Dialog"
> Adding 15 pending actions from page: http://juice-shop.herokuapp.com/#/recycle
> Crawling path: Request http://juice-shop.herokuapp.com/ -> Click "Apple Pomace Apple Pomace 0.89¤" -> Click "sent back to us"
```

## Analyze the Vulnerabilities:


Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn JSON CORS* CSRF JOSEPH
Search Settings
Tasks New scan New live task
Filter Search
3. Crawl and audit of 18.158....
Crawl and Audit - Balanced
Finished
Issues: 13 0 1 9
Summary Audit items Issues Event log Logger Audit log Live crawl view
View all
View configuration

3. Crawl and audit of 18.158.46.251:5189

Most serious vulnerabilities found (live)

| Issue type | Host | Time |
|---|---|---|
| Cleartext submission of password | http://18.158.46.251:5189 | 11:24:42 11 Nov 2024 |
| Cleartext submission of password | http://18.158.46.251:5189 | 11:24:42 11 Nov 2024 |
| Form does not contain an anti-CSRF token | http://18.158.46.251:5189 | 11:24:43 11 Nov 2024 |
| Form does not contain an anti-CSRF token | http://18.158.46.251:5189 | 11:24:43 11 Nov 2024 |
| Form does not contain an anti-CSRF token | http://18.158.46.251:5189 | 11:24:41 11 Nov 2024 |
| Request vulnerable to Cross-site Request Forgery | http://18.158.46.251:5189 | 11:24:41 11 Nov 2024 |
| Request vulnerable to Cross-site Request Forgery | http://18.158.46.251:5189 | 11:24:40 11 Nov 2024 |
| Request vulnerable to Cross-site Request Forgery | http://18.158.46.251:5189 | 11:24:41 11 Nov 2024 |
| Request vulnerable to Cross-site Request Forgery | http://18.158.46.251:5189 | 11:24:41 11 Nov 2024 |
| Request vulnerable to Cross-site Request Forgery | http://18.158.46.251:5189 | 11:24:42 11 Nov 2024 |
| Request vulnerable to Cross-site Request Forgery | http://18.158.46.251:5189 | 11:24:42 11 Nov 2024 |
| Request vulnerable to Cross-site Request Forgery | http://18.158.46.251:5189 | 11:24:41 11 Nov 2024 |
| Request vulnerable to Cross-site Request Forgery | http://18.158.46.251:5189 | 11:24:40 11 Nov 2024 |
| Unencrypted communications | http://18.158.46.251:5189 | 11:24:39 11 Nov 2024 |
| Email addresses disclosed | http://18.158.46.251:5189 | 11:24:43 11 Nov 2024 |
| Email addresses disclosed | http://18.158.46.251:5189 | 11:24:43 11 Nov 2024 |
| Frameable response (potential Clickjacking) | http://18.158.46.251:5189 | 11:24:42 11 Nov 2024 |
| Frameable response (potential Clickjacking) | http://18.158.46.251:5189 | 11:24:41 11 Nov 2024 |
| Frameable response (potential Clickjacking) | http://18.158.46.251:5189 | 11:24:40 11 Nov 2024 |
| Path-relative style sheet import | http://18.158.46.251:5189 | 11:26:12 11 Nov 2024 |
| Path-relative style sheet import | http://18.158.46.251:5189 | 11:26:06 11 Nov 2024 |
| Cross-site request forgery | http://18.158.46.251:5189 | 11:30:52 11 Nov 2024 |
| Path-relative style sheet import | http://18.158.46.251:5189 | 11:25:43 11 Nov 2024 |

Task configuration

Task type: Crawl & audit
Scope: 18.158.46.251:5189
Configuration: Crawl and Audit - Balanced

Task progress

| | | | |
|---|---|---|---|
| Total audit items: | 8 | Unique locations: | 7 |
| Audit items pending: | 0 | Pending actions: | 0 |
| Audit items in progress: | 0 | Current link depth: | 0 |
| Audit items completed: | 8 | Requests: | 4105 |
| | | Network errors: | 4 |

Task log

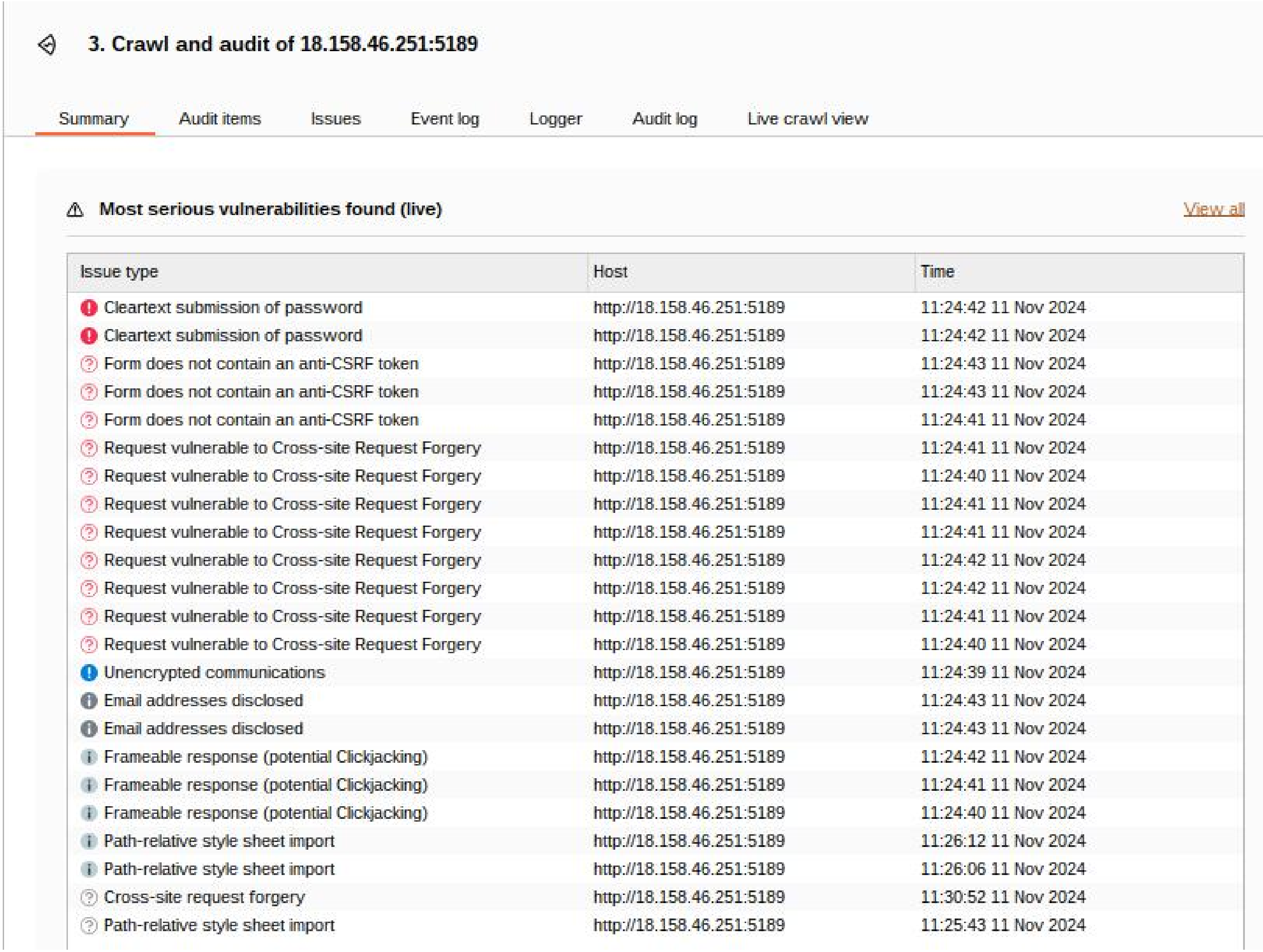
```
> Auditing "http://18.158.46.251:5189/Forgot_Password2.php" for Backup Files Append Filename
> Auditing "http://18.158.46.251:5189/Forgot_Password2.php" for Backup Files Append Extension
> Auditing "http://18.158.46.251:5189/Forgot_Password2.php" for Backup Files Prefix Filename
> Auditing "http://18.158.46.251:5189/Forgot_Password2.php" for Backup Files Replace Extension
> Auditing "http://18.158.46.251:5189/Forgot_Password2.php" for Web Cache Deception
> Auditing "http://18.158.46.251:5189/Forgot_Password2.php" for Broken Access Control
> Auditing "http://18.158.46.251:5189/Forgot_Password2.php" for GraphQL Content Type Not Validated
> Auditing "http://18.158.46.251:5189/Forgot_Password2.php" for GraphQL Suggestions Enabled
```

23 vulnerabilities found(13 critical)

- After the scan completes, review the results under the **Issue Activity** tab. Here, each identified vulnerability will be listed with its type, path, severity, and confidence rating.

- Click on an issue to see detailed information, including a description, the affected URL, the request/response that revealed the issue, and remediation advice.

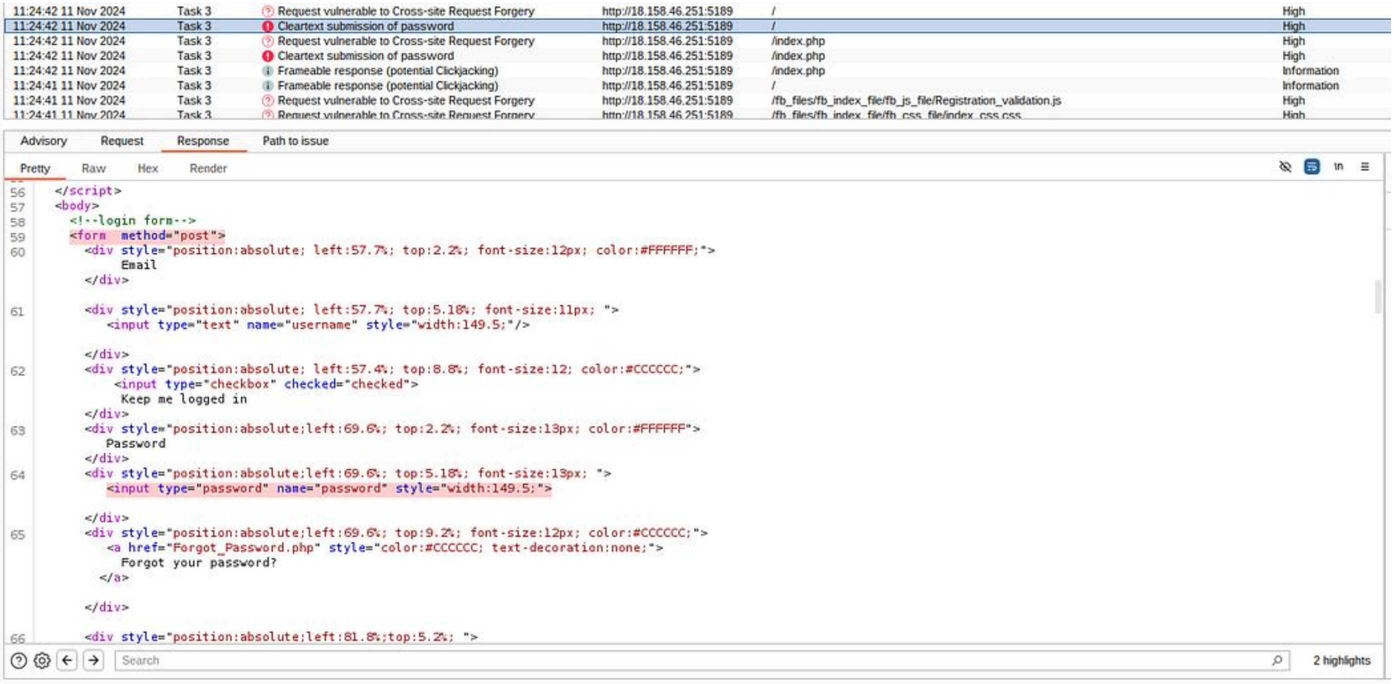
**Made by Moeez Javed**



## 3. Crawl and audit of 18.158.46.251:5189

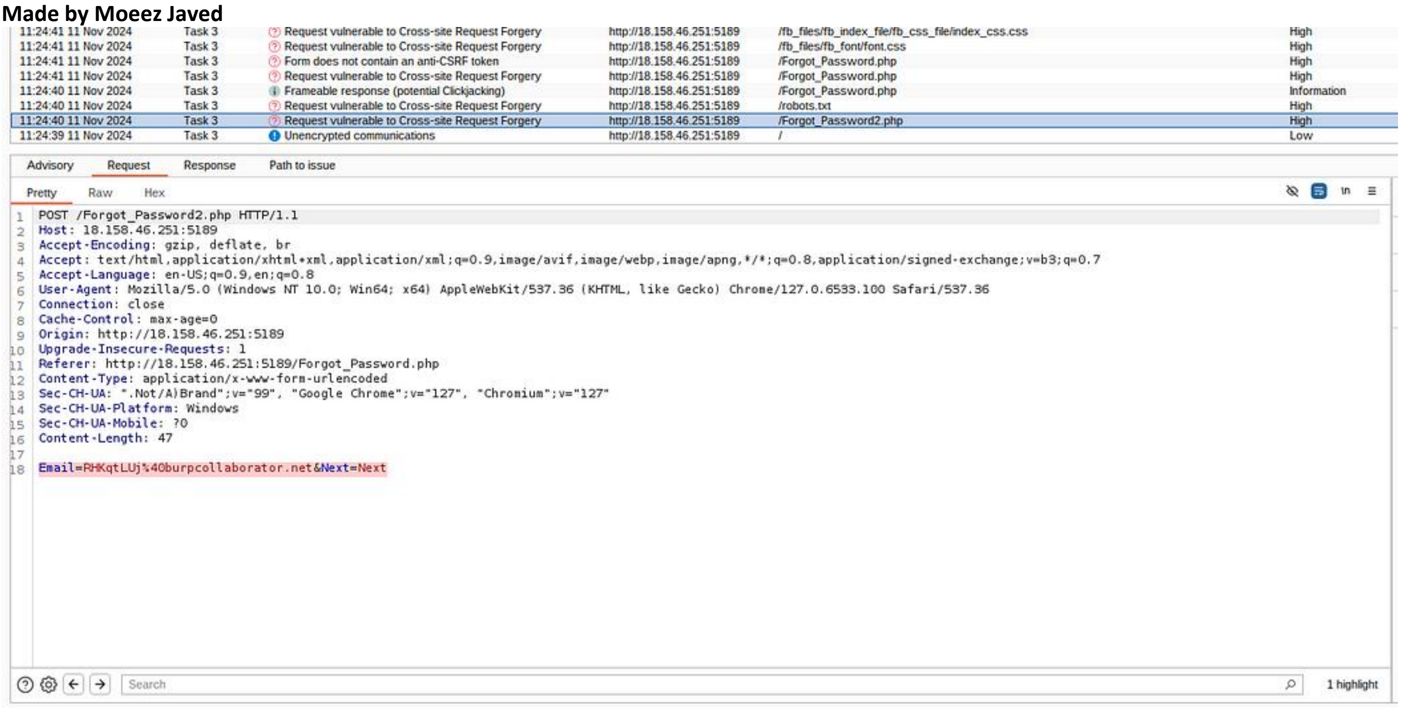
### ⚠ Most serious vulnerabilities found (live)

| Issue type | Host | Time |
|---|---|---|
| Cleartext submission of password | http://18.158.46.251:5189 | 11:24:42 11 Nov 2024 |
| Cleartext submission of password | http://18.158.46.251:5189 | 11:24:42 11 Nov 2024 |
| Form does not contain an anti-CSRF token | http://18.158.46.251:5189 | 11:24:43 11 Nov 2024 |
| Form does not contain an anti-CSRF token | http://18.158.46.251:5189 | 11:24:43 11 Nov 2024 |
| Form does not contain an anti-CSRF token | http://18.158.46.251:5189 | 11:24:41 11 Nov 2024 |
| Request vulnerable to Cross-site Request Forgery | http://18.158.46.251:5189 | 11:24:41 11 Nov 2024 |
| Request vulnerable to Cross-site Request Forgery | http://18.158.46.251:5189 | 11:24:40 11 Nov 2024 |
| Request vulnerable to Cross-site Request Forgery | http://18.158.46.251:5189 | 11:24:41 11 Nov 2024 |
| Request vulnerable to Cross-site Request Forgery | http://18.158.46.251:5189 | 11:24:41 11 Nov 2024 |
| Request vulnerable to Cross-site Request Forgery | http://18.158.46.251:5189 | 11:24:42 11 Nov 2024 |
| Request vulnerable to Cross-site Request Forgery | http://18.158.46.251:5189 | 11:24:42 11 Nov 2024 |
| Request vulnerable to Cross-site Request Forgery | http://18.158.46.251:5189 | 11:24:41 11 Nov 2024 |
| Request vulnerable to Cross-site Request Forgery | http://18.158.46.251:5189 | 11:24:40 11 Nov 2024 |
| Unencrypted communications | http://18.158.46.251:5189 | 11:24:39 11 Nov 2024 |
| Email addresses disclosed | http://18.158.46.251:5189 | 11:24:43 11 Nov 2024 |
| Email addresses disclosed | http://18.158.46.251:5189 | 11:24:43 11 Nov 2024 |
| Frameable response (potential Clickjacking) | http://18.158.46.251:5189 | 11:24:42 11 Nov 2024 |
| Frameable response (potential Clickjacking) | http://18.158.46.251:5189 | 11:24:41 11 Nov 2024 |
| Frameable response (potential Clickjacking) | http://18.158.46.251:5189 | 11:24:40 11 Nov 2024 |
| Path-relative style sheet import | http://18.158.46.251:5189 | 11:26:12 11 Nov 2024 |
| Path-relative style sheet import | http://18.158.46.251:5189 | 11:26:06 11 Nov 2024 |
| Cross-site request forgery | http://18.158.46.251:5189 | 11:30:52 11 Nov 2024 |
| Path-relative style sheet import | http://18.158.46.251:5189 | 11:25:43 11 Nov 2024 |



| | | | | | |
|---|---|---|---|---|---|
| 11:24:42 11 Nov 2024 | Task 3 | Request vulnerable to Cross-site Request Forgery | http://18.158.46.251:5189 | / | High |
| 11:24:42 11 Nov 2024 | Task 3 | Cleartext submission of password | http://18.158.46.251:5189 | / | High |
| 11:24:42 11 Nov 2024 | Task 3 | Request vulnerable to Cross-site Request Forgery | http://18.158.46.251:5189 | /index.php | High |
| 11:24:42 11 Nov 2024 | Task 3 | Cleartext submission of password | http://18.158.46.251:5189 | /index.php | High |
| 11:24:42 11 Nov 2024 | Task 3 | Frameable response (potential Clickjacking) | http://18.158.46.251:5189 | /index.php | Information |
| 11:24:41 11 Nov 2024 | Task 3 | Frameable response (potential Clickjacking) | http://18.158.46.251:5189 | / | Information |
| 11:24:41 11 Nov 2024 | Task 3 | Request vulnerable to Cross-site Request Forgery | http://18.158.46.251:5189 | /fb_files/fb_index_file/fb_js_file/Registration_validation.js | High |
| 11:24:41 11 Nov 2024 | Task 3 | Request vulnerable to Cross-site Request Forgery | http://18.158.46.251:5189 | /fb_files/fb_index_file/fb_css_file/index_css.css | High |

```
</script>
<body>
  <!--login form-->
  <form  method="post">
    <div style="position:absolute; left:57.7%; top:2.2%; font-size:12px; color:#FFFFFF;">
          Email
    </div>

    <div style="position:absolute; left:57.7%; top:5.18%; font-size:11px; ">
       <input type="text" name="username" style="width:149.5;"/>

    </div>
    <div style="position:absolute; left:57.4%; top:8.8%; font-size:12; color:#CCCCCC;">
        <input type="checkbox" checked="checked">
         Keep me logged in
    </div>
    <div style="position:absolute;left:69.6%; top:2.2%; font-size:13px; color:#FFFFFF">
       Password
    </div>
    <div style="position:absolute;left:69.6%; top:5.18%; font-size:13px; ">
       <input type="password" name="password" style="width:149.5;">

    </div>
    <div style="position:absolute;left:69.6%; top:9.2%; font-size:12px; color:#CCCCCC;">
       <a href="Forgot_Password.php" style="color:#CCCCCC; text-decoration:none;">
         Forgot your password?
      </a>

    </div>

    <div style="position:absolute;left:81.8%;top:5.2%; ">
```



| | | | | | |
|---|---|---|---|---|---|
| 11:24:41 11 Nov 2024 | Task 3 | Request vulnerable to Cross-site Request Forgery | http://18.158.46.251:5189 | /fb_files/fb_index_file/fb_css_file/index_css.css | High |
| 11:24:41 11 Nov 2024 | Task 3 | Request vulnerable to Cross-site Request Forgery | http://18.158.46.251:5189 | /fb_files/fb_font/font.css | High |
| 11:24:41 11 Nov 2024 | Task 3 | Form does not contain an anti-CSRF token | http://18.158.46.251:5189 | /Forgot_Password.php | High |
| 11:24:41 11 Nov 2024 | Task 3 | Request vulnerable to Cross-site Request Forgery | http://18.158.46.251:5189 | /Forgot_Password.php | High |
| 11:24:40 11 Nov 2024 | Task 3 | Frameable response (potential Clickjacking) | http://18.158.46.251:5189 | /Forgot_Password.php | Information |
| 11:24:40 11 Nov 2024 | Task 3 | Request vulnerable to Cross-site Request Forgery | http://18.158.46.251:5189 | /robots.txt | High |
| 11:24:40 11 Nov 2024 | Task 3 | Request vulnerable to Cross-site Request Forgery | http://18.158.46.251:5189 | /Forgot_Password2.php | High |
| 11:24:39 11 Nov 2024 | Task 3 | Unencrypted communications | http://18.158.46.251:5189 | / | Low |

```
POST /Forgot_Password2.php HTTP/1.1
Host: 18.158.46.251:5189
Accept-Encoding: gzip, deflate, br
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.6533.100 Safari/537.36
Connection: close
Cache-Control: max-age=0
Origin: http://18.158.46.251:5189
Upgrade-Insecure-Requests: 1
Referer: http://18.158.46.251:5189/Forgot_Password.php
Content-Type: application/x-www-form-urlencoded
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="127", "Chromium";v="127"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Content-Length: 47

Email=RHKqtLUj%40burpcollaborator.net&Next=Next
```

## 1. Review and Report:

- Utilize the detailed analysis provided by Burp Suite to prioritize issues based on their severity and the specific security needs of your application.
- Export the findings using the reporting tools in Burp Suite for compliance, auditing, or further analysis.

## Best Practices for Using the Scanner:

- Always ensure that you have legal permission to scan the target application.
- Regularly update Burp Suite to take advantage of the latest security tests and vulnerability definitions.
- Validate critical findings manually to confirm vulnerabilities and understand their impact.

## Task: Burp Suite Hands-on Lab

**Objective:** The purpose of this lab is to give students practical experience in using Burp Suite for web application security testing. By completing this task, students will learn how to set up Burp Suite, intercept and modify HTTP requests, analyze responses, and use the automatic vulnerability scanner effectively.

## Task 1: Setting Up Burp Suite

1. Install and open Burp Suite on your Kali Linux system.
2. Configure your browser to use Burp Suite as a proxy.

3. Install Burp's CA certificate into your browser for HTTPS traffic interception.
4. Verify that Burp Suite is correctly intercepting traffic by turning on the intercept feature and loading a website.
5. Document your setup steps with screenshots.

## Task 2: Site Mapping & Scoping

1. Navigate to (website) while Burp Suite is running.
2. Observe how Burp Suite builds a **Site Map**.
3. Identify different website resources and their status (visited vs. unvisited).
4. Set the **scope** to focus only on TryHackMe's domain.
5. Filter the Site Map to show only **in-scope** items.
6. Provide a summary of what you found in the Site Map and why setting a scope is important.

## Task 3: Intercepting and Modifying Requests

1. Disable Burp Intercept and visit the target page: http://10.10.29.220/products.
2. Click on a product's **See More** link and note the URL format (e.g., /products/3).
3. Enable Burp Intercept, refresh the product page, and capture the request.
4. Modify the request by changing the product ID to -500 and forward it.
5. Analyze the response:

    1. What HTTP status code is returned?
    2. Does the server handle the invalid input correctly?
    3. What are the possible security implications?

6. Document your findings with screenshots and explanations.

## Task 4: Using Burp Repeater for Input Validation Testing

1. Send the captured request to **Burp Repeater**.
2. Modify the product ID with different values:

    1. A negative number
    2. A very large number
    3. A non-numeric value (e.g., ABC)

3. Analyze how the application responds to each input.
4. Based on your observations, describe whether the web application has proper input validation.

## Task 5: Running the Burp Suite Automatic Vulnerability Scanner

1. Ensure your target (TryHackMe) is added to **scope**.
2. Go to the **Dashboard** and initiate a **New Scan**.
3. Select **Crawl and Audit** for a comprehensive scan.
4. Configure scan settings:

    1. Define authentication (if required)
    2. Set **Scan Mode** (choose from Light, Balanced, Deep, Fast)
    3. Enable request throttling (to avoid detection or overload)

5. Monitor scan progress and analyze the reported vulnerabilities.
6. Take a screenshot of the scan results and summarize:

1. Number of vulnerabilities found
2. Severity breakdown (Critical, High, Medium, Low)
3. One or two key vulnerabilities identified
4. Possible remediation strategies

## Task 6: Reporting and Documentation

1. Summarize your findings in a structured report:

    1. Overview of the tests performed
    2. Key vulnerabilities discovered
    3. Impact analysis
    4. Recommendations for security improvements

2. Save your Burp Suite scan report as a PDF and submit it along with your written analysis.

## Evaluation Criteria:

- Correct configuration and setup of Burp Suite (10 points)
- Accurate site mapping and scoping (10 points)
- Successful interception and modification of requests (20 points)
- Use of Burp Repeater for input validation testing (20 points)
- Completion and documentation of an automatic vulnerability scan (30 points)
- Well-structured final report (10 points)

### Submission Deadline:

All students must submit their reports and Burp Suite findings by **[Insert Due Date]**.

### Note:

This task is for educational purposes only. Do not attempt to test unauthorized websites or systems without explicit permission.

### Good Luck!