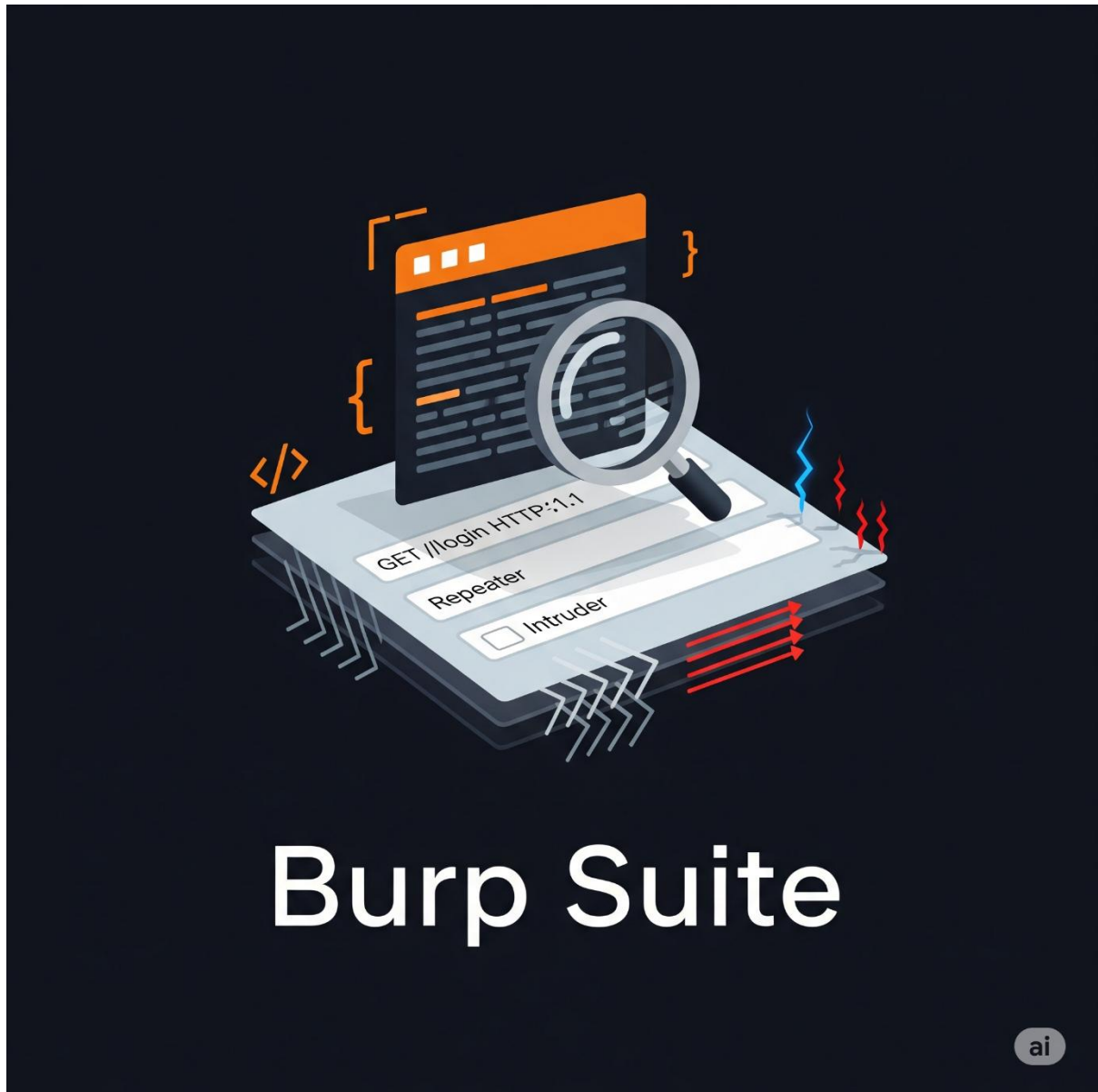
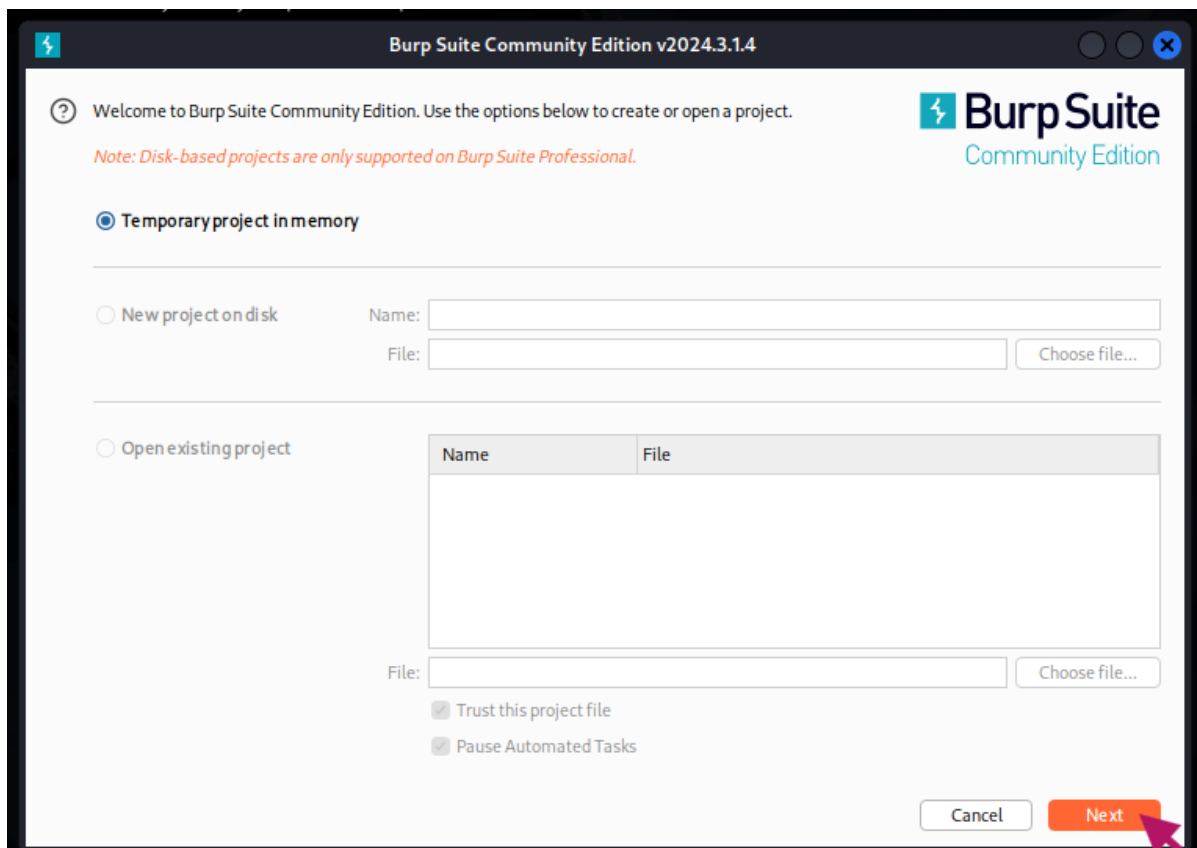
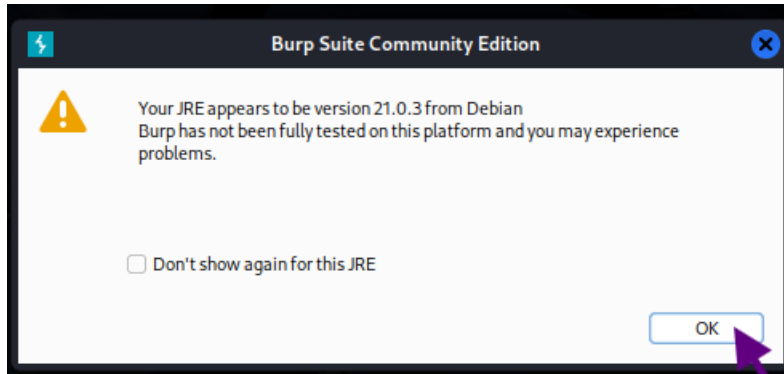
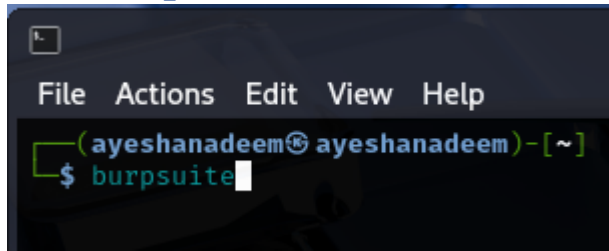
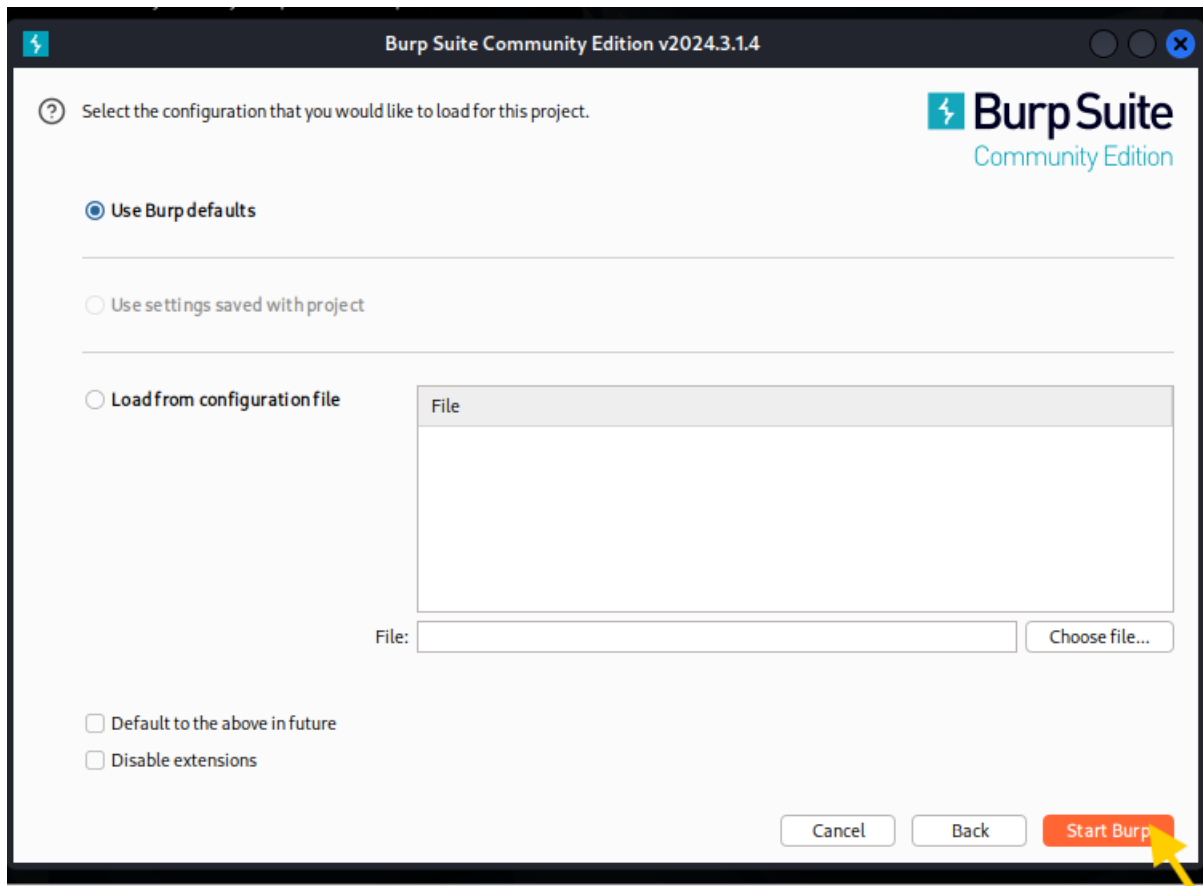


Day 9 of Learning Cyber Security**Platform: Kali Linux****Name:** Ayesha Nadeem**Topic:** BurpSuite**Contact Me:** ayeshanm8@gmail.com**Date:** 9th July, 2025

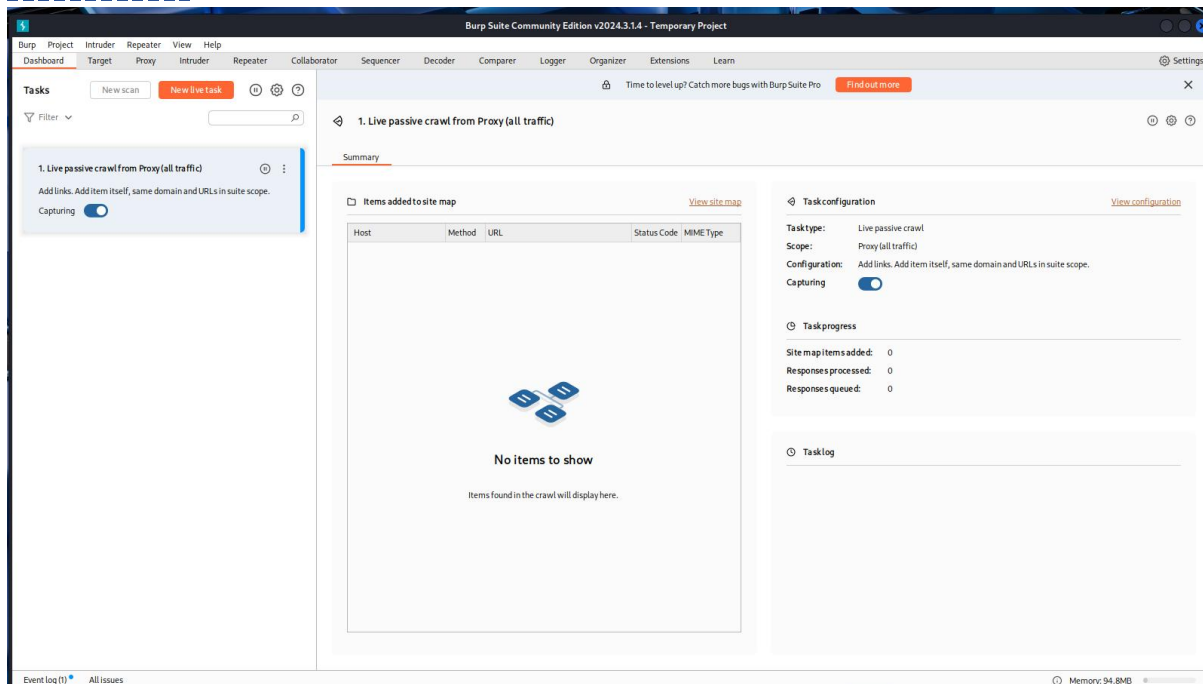
BurpSuite: The Web App Analyzer

Start BurpSuite





Dashboard



Step 1:

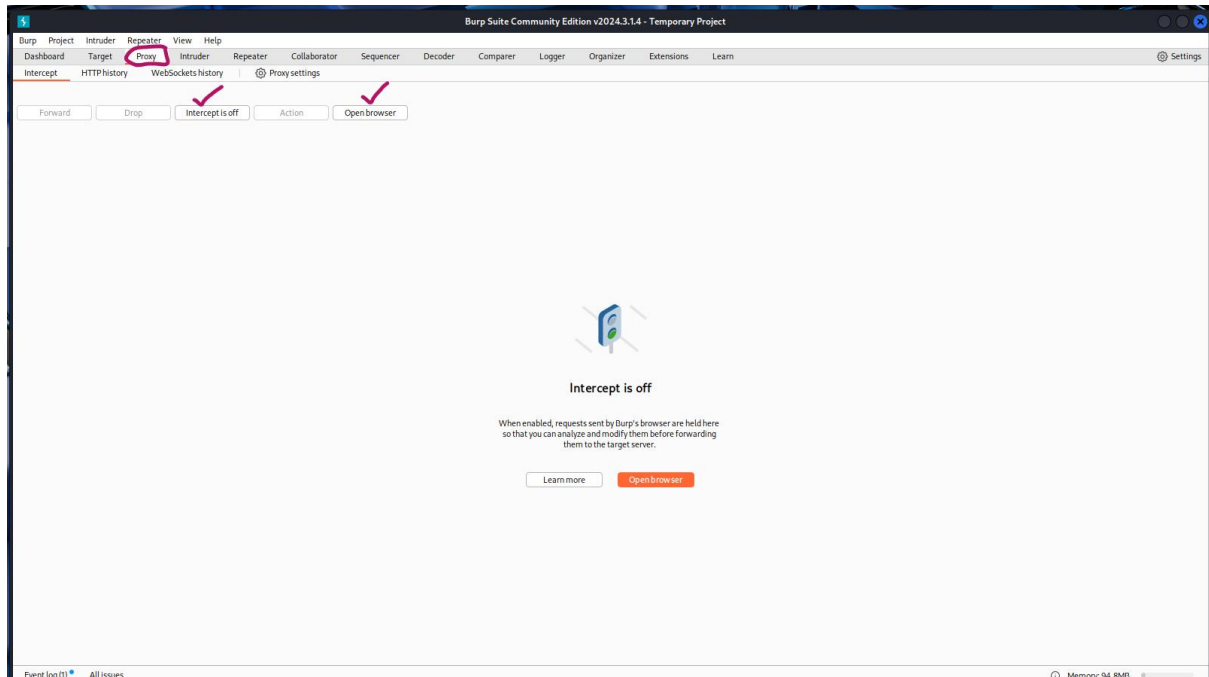
Go to Proxy Tab

Step 2:

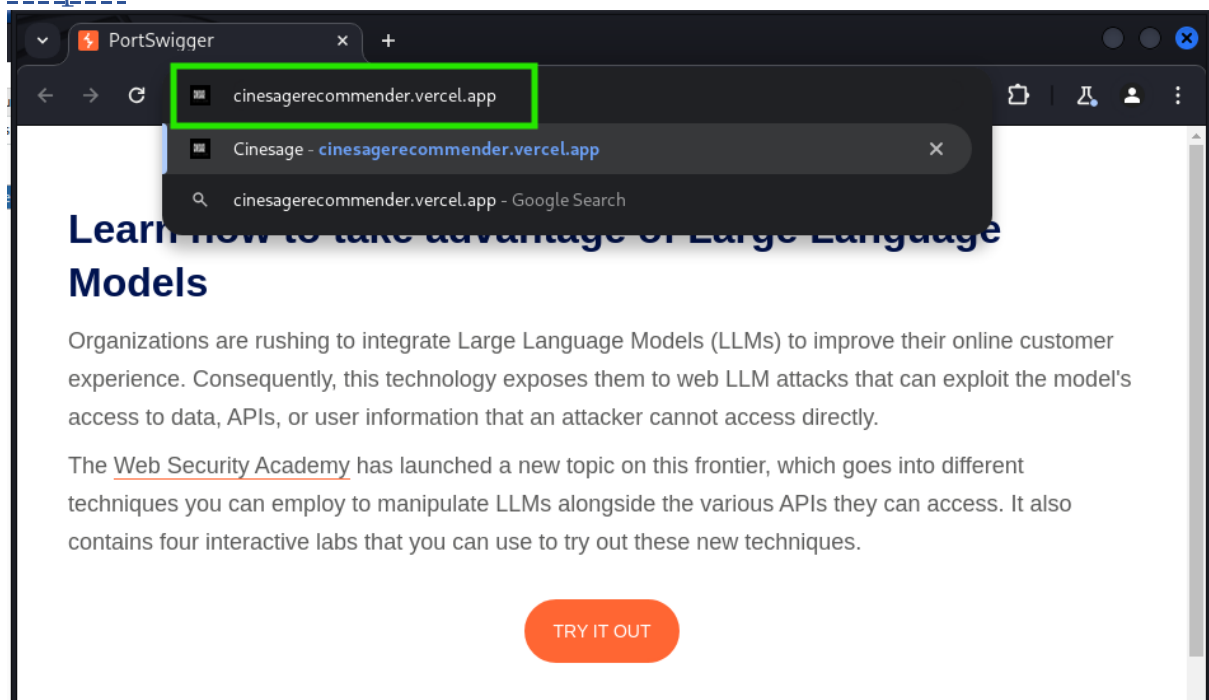
On the Intercept

Step 3:

Click on Open Browser

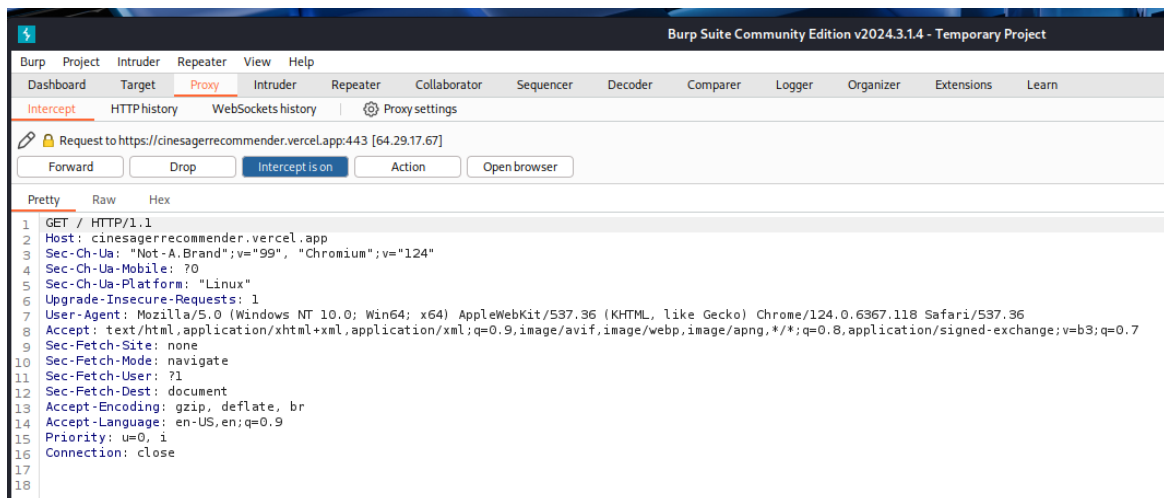


Step 4:

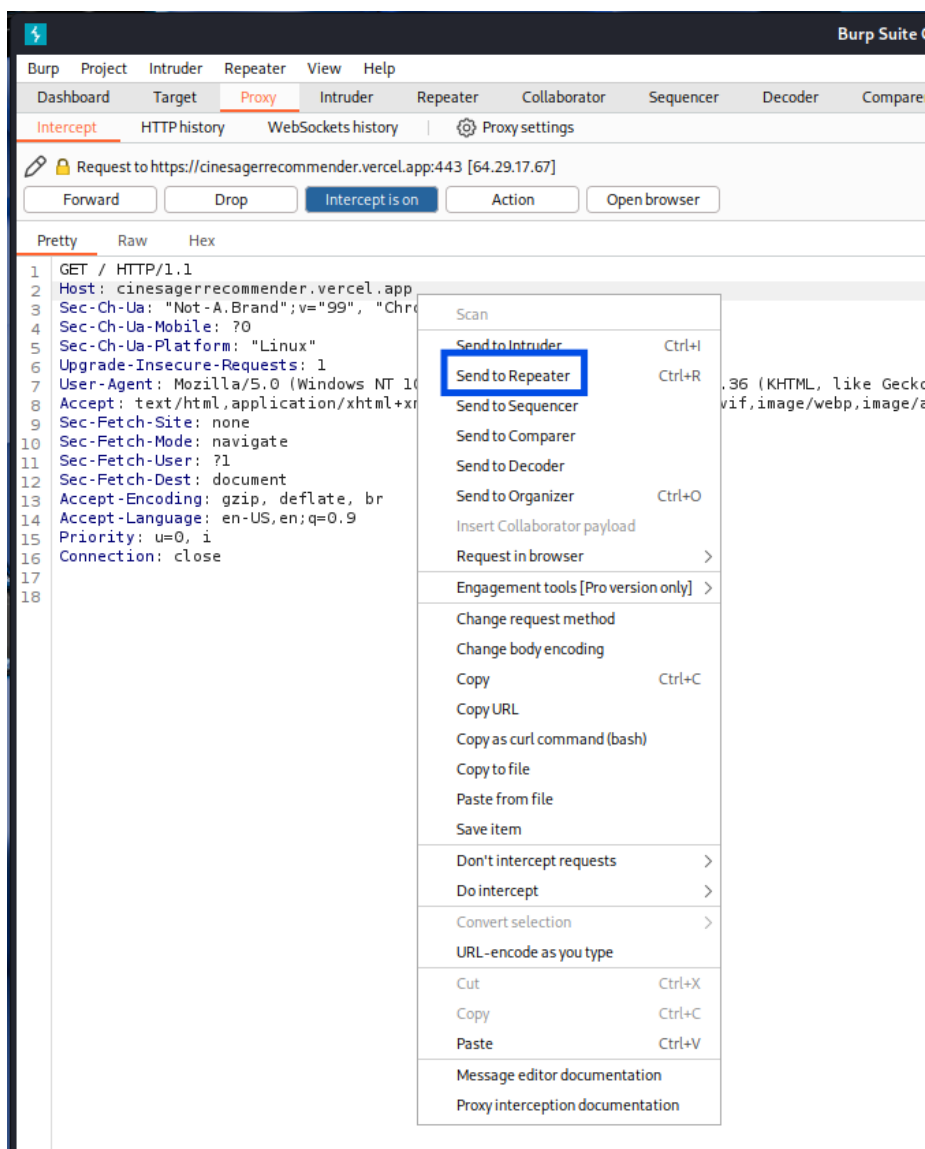


Step 5:

First packet comes in burpsuite proxy tab

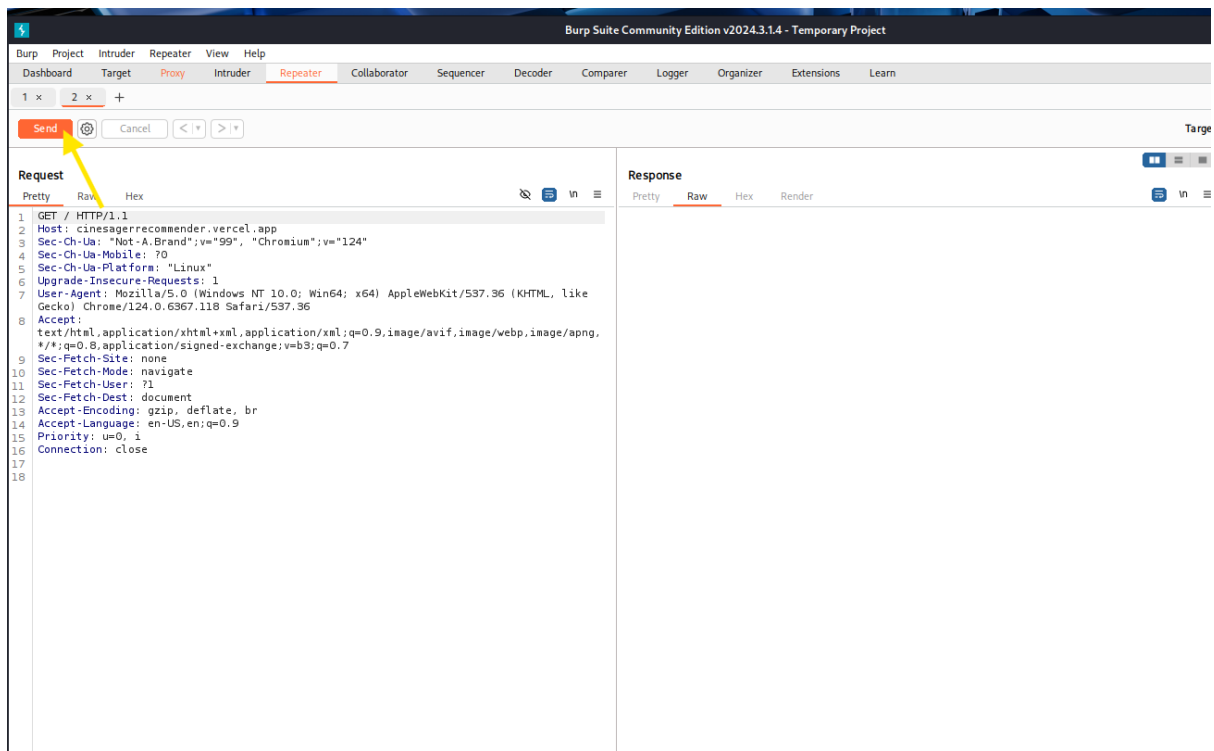


Right click anywhere and select “send to repeater”.

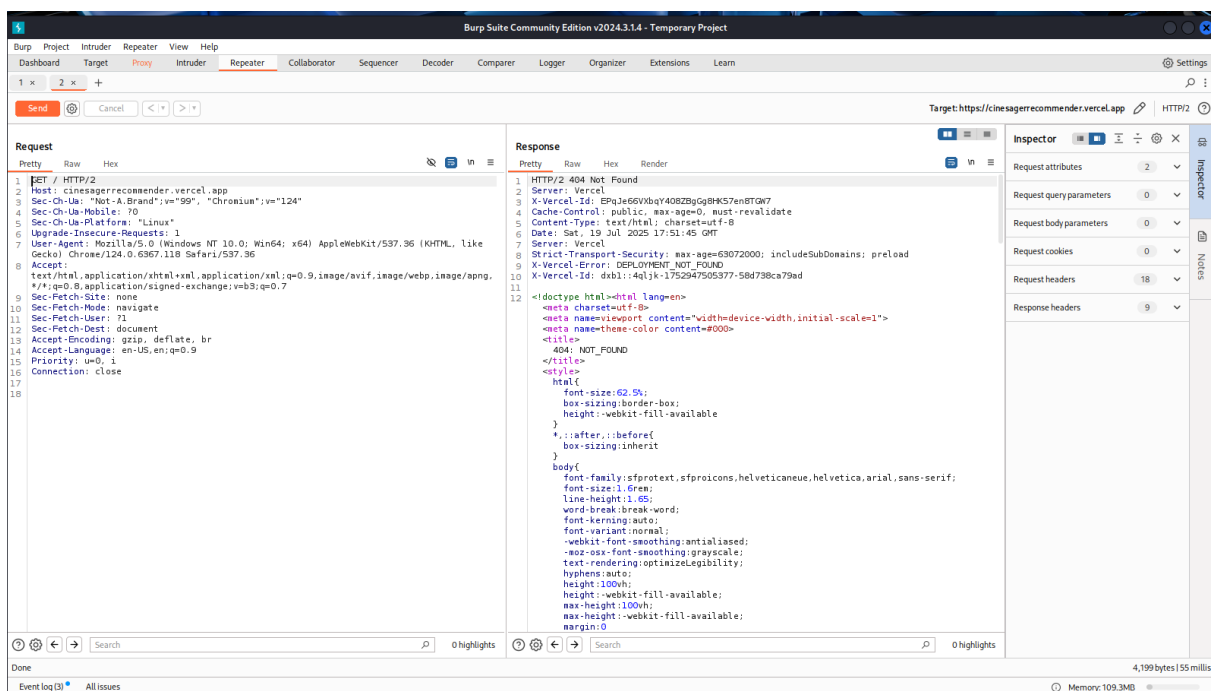


Step 6:

From here you can make changes in header content (like overwrite session key), fetch information as well. Then send it to server

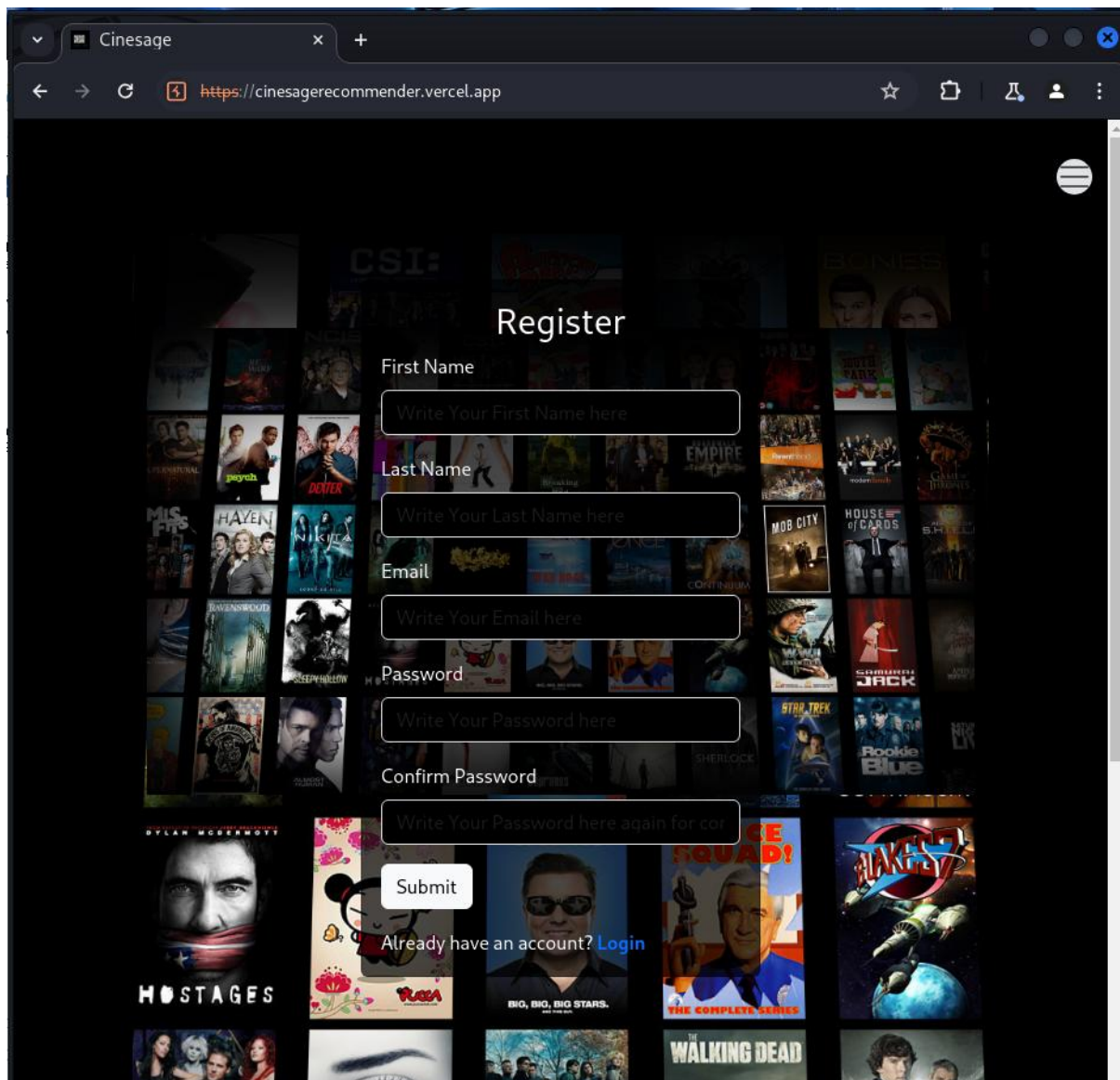
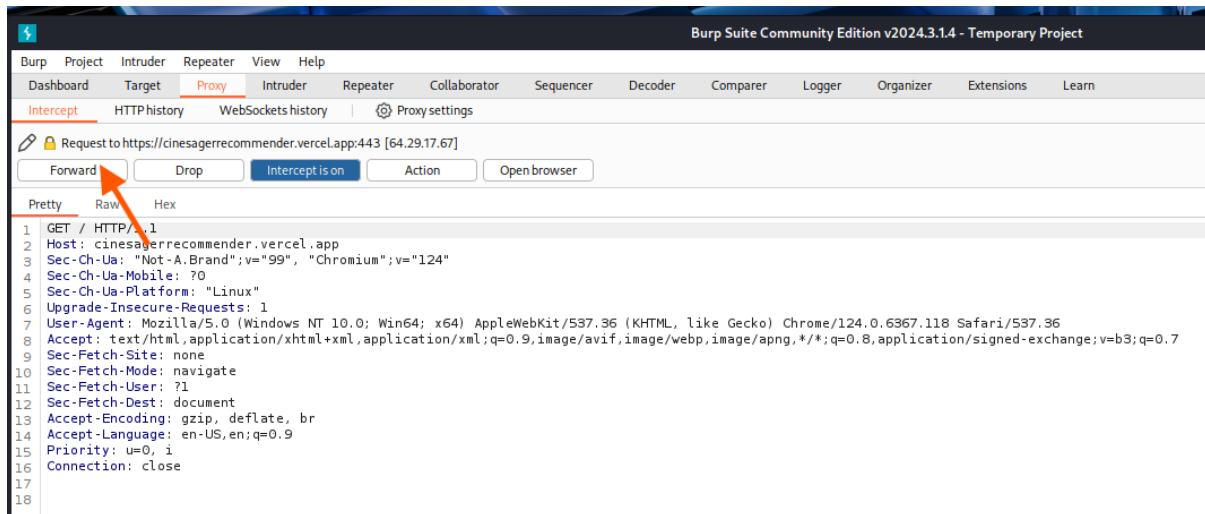


Server response will first comes in burpsuite, instead of client browser. In its response, you can fetch important content like server name, database name, html code of page, and token ID etc.



Step 7:

Click on forward to pass server response to client.



Gathered Information:

[illegible][illegible]

Request		Response	
Pretty	Raw	Pretty	Raw
16	Referer: https://cinesagegrecommender.vercel.app/ Accept-Encoding: gzip, deflate, br Priority: u=1, i	1 HTTP/2 200 OK 2 X-Client-Wire-Protocol: h3 3 X-Http-Session-Id: rK4sMP2Y8VDU=s1zrZAKI6GBKoR3taKYaacSsxXdcFE 4 Content-Type: text/plain; charset=utf-8 5 Date: Wed, 18 Jun 2025 04:06:33 GMT 6 Server: ESF 7 Content-Length: 54 8 X-Xss-Protection: 0 9 X-Frame-Options: SAMEORIGIN 10 X-Content-Type-Options: nosniff 11 Access-Control-Allow-Origin: https://cinesagegrecommender.vercel.app 12 Vary: origin 13 Access-Control-Allow-Credentials: true 14 Access-Control-Expose-Headers: x-client-wire-protocol,x-http-session-id 15 Alt-Svc: h3=":443"; ma=259200,h3-29=":443"; ma=259200	
17		15 16 [[{"c","279d2bvuntHk0RsvAXxajw","",8,12,30000}]] 17	

Below the request details, there are two tabs: "Event log" and "All issues". The "Event log" tab is currently selected and shows a single event.

Event log	All issues
<div> Warning: The response contains a large amount of binary data (base64 encoded) which may indicate a security issue or a corrupted response. </div>	

The screenshot displays the Burp Suite interface with the 'Repeater' tab selected. A HTTP request is shown on the left, and the corresponding response is on the right. The response headers include 'Strict-Transport-Security: max-age=63072000; includeSubDomains; preload', which is highlighted with a red box. The response body shows an HTML document type declaration and a head section with meta and link tags.

Request	Response
<pre> 1 GET / HTTP/2 2 Host: competitioncyber.vercel.app 3 Cache-Control: max-age=0 4 Sec-Ch-Ua: "NotA_Brand";v="99", "Chromium";v="130" 5 Sec-Ch-Ua-Mobile: 70 6 Sec-Ch-Ua-Platform: "Linux" 7 Accept-Language: en-US,en;q=0.9 8 Upgrade-Insecure-Requests: 1 9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70 Safari/537.36 10 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 11 Sec-Fetch-Site: none 12 Sec-Fetch-Mode: navigate 13 Sec-Fetch-User: ?1 14 Sec-Fetch-Dest: document 15 Accept-Encoding: gzip, deflate, br 16 Priority: u=0, i 17 18 </pre>	<pre> 1 HTTP/2 200 OK 2 Server: Vercel 3 X-Vercel-Id: drb87vvZqTq3D0t7zpyh2lJdooT3hnp 4 Access-Control-Allow-Origin: * 5 Age: 227624 6 Cache-Control: public, max-age=0, must-revalidate 7 Content-Disposition: inline 8 Content-Type: text/html; charset=utf-8 9 Date: Wed, 18 Jun 2025 04:40:21 GMT 10 Etag: W/"0804255bdefb7b01b12142efa26615a7" 11 Server: Vercel 12 Strict-Transport-Security: max-age=63072000; includeSubDomains; preload 13 Vary: RSC, Next-Router-State-Tree, Next-Router-Prefetch, Next-Router-Segment-Prefetch 14 X-Matched-Path: / 15 X-Nextjs-Prerender: 1 16 X-Nextjs-State-Time: 300 17 X-Vercel-Cache: HIT 18 X-Vercel-Id: dxb1:qrrgb-1750221621244-f00fa5600afa 19 20 <!DOCTYPE html><html lang="en"> <head> <meta charset="utf-8"/> <meta name="viewport" content="width=device-width, initial-scale=1"/> <link rel="preload" href=" </pre>

Burp Suite Community Edition v2024.3.1.4 - Temporary Project

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Organizer Extensions Learn

1 x 2 x 3 x 4 x 5 x 6 x 7 x 8 x +

Send Cancel < >

Request

1 GET /clients.html HTTP/2
 2 Host: www.yumasoft.com
 3 Sec-CH-UA: "Not-A.Brand";v="99", "Chromium";v="124"
 4 Sec-CH-UA-Mobile: ?0
 5 Sec-CH-UA-Platform: "Linux"
 6 Upgrade-Insecure-Requests: 1
 7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.118 Safari/537.36
 8 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
 9 Sec-Fetch-Site: same-origin
 10 Sec-Fetch-Mode: navigate
 11 Sec-Fetch-User: ?1
 12 Sec-Fetch-Dest: document
 13 Referer: https://www.yumasoft.com/
 14 Accept-Encoding: gzip, deflate, br
 15 Accept-Language: en-US,en;q=0.9
 16 Priority: u=0, i
 17
 18

Response

```

69 </p>
70 <div class="content-box row" id="sw">
71 <div class="col-xs-12 col-sm-4">
72 
73 </div>
74 <div class="col-xs-12 col-sm-8">
75 <div class="title-c">
76 <span style="font-weight: bold">
77   Shop-Ware
78 </span>
79 </div>
80 <div class="site-link">
81 <a href="http://www.shop-ware.com">www.shop-ware.com</a>
82 </div>
83 <div class="text">
84 Shop-Ware's shop management software provides professional-grade
85 solutions to the industry's leading automotive repair businesses.
86 </div>
87 <div class="text">
88 <b>Business model:</b> Offshore Development Center.<br />
89 <b>Technologies:</b> Ruby on Rails, React.js, JavaScript,
90 HTML/CSS, typescript.
91 </div>
92 </div>
93 <div class="col-xs-12 col-sm-4">
94 
95 </div>
96 <div class="col-xs-12 col-sm-8">
97 <div class="title-c">
98 <span style="font-weight: bold">
99   Certified
100 </span>
101 </div>
102 <div class="site-link">
  
```

0 highlights


Yumasoft

https://www.yumasoft.com/clients.html#certified

Yumasoft

management of our development teams, by paying close attention to detail, and by putting state-of-the-art technology to use.

These are some of the many clients we have served:

 **Shop-Ware**
 www.shop-ware.com

Shop-Ware's shop management software provides professional-grade solutions to the industry's leading automotive repair businesses.

Business model: Offshore Development Center.
Technologies: Ruby on Rails, React.js, JavaScript, HTML/CSS, typescript.

Request		Response	
Pretty	Raw	Pretty	Raw
1 GET /scrollreveal HTTP/2	1 Host: unpk.com	1 HTTP/2 302 Found	1 Date: Sat, 19 Jul 2025 18:36:42 GMT
2 Sec-Ch-Ua: "Not-A.Brand";v="99", "Chromium";v="124"	2 Sec-Ch-Ua-Mobile: 70	2 Content-Type: text/plain; charset=UTF-8	2 Content-Length: 55
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.118 Safari/537.36	3 Sec-Ch-Ua-Platform: "Linux"	3 Location: /scrollreveal@4.0.9/dist/scrollreveal.js	3 Access-Control-Allow-Origin: *
4 Accept: */*	4 Sec-Fetch-Site: cross-site	4 Cache-Control: public, max-age=60, s-maxage=300	4 Cross-Origin-Resource-Policy: cross-origin
5 Sec-Fetch-Mode: no-cors	5 Sec-Fetch-Dest: script	5 Vary: Accept-Encoding	5 Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
6 Referer: https://www.yumasoft.com/	6 Accept-Encoding: gzip, deflate, br	6 X-Content-Type-Options: nosniff	6 Server: cloudflare
7 Accept-Language: en-US,en;q=0.9	7 Priority: u=2	7 CT-Ray: 961c59687a08318-SIN	7 Alt-Svc: h3=":443"; ma=86400
		8 Redirecting to /scrollreveal@4.0.9/dist/scrollreveal.js	

Request		Response	
Pretty	Raw	Pretty	Raw
1 GET /translation.html HTTP/2	1 Host: www.yumasoft.com	1 HTTP/2 200 OK	1 Server: nginx
2 Sec-Ch-Ua: "Not-A.Brand";v="99", "Chromium";v="124"	2 Accept: */*	2 Date: Sat, 19 Jul 2025 18:38:13 GMT	2 Content-Type: text/html
3 X-Requested-With: XMLHttpRequest	3 Sec-Ch-Ua-Mobile: 70	3 Last-Modified: Tue, 29 Aug 2023 19:25:47 GMT	3 Vary: Accept-Encoding
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.118 Safari/537.36	4 Sec-Ch-Ua-Platform: "Linux"	4 Expires: Thu, 15 Jan 2026 18:38:13 GMT	4 Cache-Control: max-age=15552000
5 Sec-Fetch-Site: same-origin	5 Sec-Fetch-Mode: cors	5 Host-Header: 8431280b0c35cb1147f8ba998a563a7	5 X-Proxy-Cache-Info: D111
6 Sec-Fetch-Dest: empty	6 Referer: https://www.yumasoft.com/index.html	6 <div class="s-link facebook">	6
7 Accept-Encoding: gzip, deflate, br	7 Accept-Language: en-US,en;q=0.9	7 	7
8 Priority: u=1, i		8 </div>	8 <div class="s-link twitter">
		9 	9
		10 >	

Request		Response	
Pretty	Raw	Pretty	Raw
1 GET /maps/api/maps?map=204?csp_test=true HTTP/2	1 Host: maps.googleapis.com	1 HTTP/2 200 OK	1 Content-Type: application/json; charset=UTF-8
2 Sec-Ch-Ua: "Not-A.Brand";v="99", "Chromium";v="124"	2 Sec-Ch-Ua-Mobile: 70	2 Vary: Origin	2 Vary: X-Origin
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.118 Safari/537.36	3 Sec-Ch-Ua-Platform: "Linux"	3 Date: Sat, 19 Jul 2025 18:40:00 GMT	3 Server: scaffolding on HTTPServer2
4 Accept: */*	4 Origin: https://www.google.com	3 Content-Length: 3	3 X-Xss-Protection: 0
5 X-Client-Data: Consyde	5 Sec-Fetch-Site: cross-site	3 X-Frame-Options: SAMEORIGIN	3 X-Content-Type-Options: nosniff
6 Sec-Fetch-Mode: cors	6 Sec-Fetch-Dest: empty	3 Access-Control-Allow-Credentials: true	3 Access-Control-Expose-Headers:
7 Referer: https://www.google.com/	7 Accept-Encoding: gzip, deflate, br	3 vary, vary, vary, content-encoding, date, server, content-length	3 Alt-Svc: h3=":443"; ma=2592000, h3-29=":443"; ma=2592000
8 Accept-Language: en-US,en;q=0.9	8 Priority: u=1, i		

Request		Response	
Pretty	Raw	Pretty	Raw
1 GET /maps/vt?pb=11e511e41117121386531314906914125612m311e012m13174050009612m311e212sspotlit151113m1312sen13sUS15e289112m511e6812m211set12sRoadmap14e2112m311e3712m111ssmartmaps14e015e111e312s147083502127m161299174093m15114e111e911e211y992e7069331975893712y1615161345659993373112e2f9e2f11b8v6696214e211141151634612x955664809018b1115sgcidk3kcompound_building12b018b016b018b06client-google-maps-embed&token=65333 HTTP/2	2 Host: www.google.com	1 HTTP/2 200 OK	1 Content-Type: image/webp
3 Sec-Ch-Ua: "Not-A.Brand";v="99", "Chromium";v="124"	3 Sec-Ch-Ua-Mobile: 70	2 Date: Sat, 19 Jul 2025 18:43:23 GMT	2 Expires: Sat, 19 Jul 2025 18:58:23 GMT
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.118 Safari/537.36	4 Sec-Ch-Ua-Platform: "Linux"	3 Cache-Control: public, max-age=900	3 Access-Control-Allow-Origin: *
5 Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8	5 X-Client-Data: COHYgE=	3 Cross-Origin-Resource-Policy: cross-origin	3 Etag: 01ca92c3a3c6de52e
6 Sec-Fetch-Site: same-origin	6 Sec-Fetch-Mode: no-cors	3 Content-Security-Policy: script-src 'none'; object-src 'none'; base-uri 'none'	3 X-Content-Type-Options: nosniff
7 Referer: https://www.google.com/maps/embed?pb=11e511e41117121386531314906914125612m311e012m13174050009612m311e212sspotlit151113m1312sen13sUS15e289112m511e6812m211set12sRoadmap14e2112m311e3712m111ssmartmaps14e015e111e312s147083502127m161299174093m15114e111e911e211y992e7069331975893712y1615161345659993373112e2f9e2f11b8v6696214e211141151634612x955664809018b1115sgcidk3kcompound_building12b018b016b018b06client-google-maps-embed&token=65333	7 Accept-Encoding: gzip, deflate, br	3 X-Server-Version-Bin: CgoIBCO1OLD8hgB	3 Content-Security-Policy-Report-Only: script-src 'none'; form-action 'none'; frame-src 'none'; report-uri https://csp.withgoogle.com/csp/scaffolding/mspthpsdsghrhc:115:0
8 Accept-Language: en-US,en;q=0.9	8 Priority: 1	3 Cross-Origin-Opener-Policy-Report-Only: same-origin; report-to=mspthpsdsghrhc:115:0	3 Report-To: [{"group": "mspthpsdsghrhc:115:0", "max_age": 2592000, "endpoints": [{"url": "https://csp.withgoogle.com/csp/report-to/scaffolding/mspthpsdsghrhc:115:0"}]}]
		3 Server: scaffolding on HTTPServer2	3 Content-Length: 3454
		3 X-Xss-Protection: 0	3 X-Frame-Options: SAMEORIGIN
		3 Server-Timing: gfet4t7; dur=171	3 Alt-Svc: h3=":443"; ma=2592000, h3-29=":443"; ma=2592000
		22 RIFWFBEPVPLS/yA? %H: -0P0F0R60 "m#0c?b?y{W1%{5\Y00v10 -PK Z FV: MD@Ejy68q=m",Iqi	23 :A40 8t1p(d<
		23 :yAU0CUIHqba0-?Y\$w=s=IEXN3w-,-'iA*6E9Ew1CTL2 qE3i-U('c1ayz00i00bD)~.WuaEZ=4V6,8-0"oc	24 H17[1]c?IFm"78V01EchMA+i_tUe{01bA, Ag,e1}iqh3-00u0"v1C1vBU/0_0_id0006A-B#-0uE56w0n-Em0

[illegible]

The screenshot displays the browser's developer tools, specifically the Network tab, showing a GET request to `https://api.arxoselabs.com`. The Request tab is active, showing the raw request details. The Response tab is also visible, showing the raw response details.

Request Tab:

- Method:** GET
- URL:** `https://api.arxoselabs.com`
- Headers:**
 - `Host: uber-api.arxoselabs.com`
 - `Sec-CH-UA: "Not-A.Brand";v="99", "Chromium";v="124"`
 - `Sec-CH-UA-Platform: "Linux"`
 - `Sec-CH-UA-Mobile: 0`
 - `User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.118 Safari/537.36`
 - `Content-Type: text/plain;charset=UTF-8`
 - `Accept: */*`
 - `Origin: https://auth.uber.com`
 - `Sec-Fetch-Site: cross-site`
 - `Sec-Fetch-Mode: cors`
 - `Sec-Fetch-Dest: empty`
 - `Referer: https://auth.uber.com/`
 - `Accept-Encoding: gzip, deflate, br`
 - `Accept-Language: en-US,en;q=0.9`
 - `Priority: u=1, 1`
- Body:**

```
{
  "id": "a75688cb-1ee0-42d6-8215-a02ee97c2091",
  "publicKey": "30000F36-CADF-490C-929A-C6A7D08B33C4",
  "keyUsage": {
    "capVersion": "3.5.0",
    "mode": "inline",
    "suppressed": false
  },
  "platform": "Linux x86_64",
  "connection": {
    "effectiveType": "3g",
    "rtt": 1050,
    "downlink": 1.45
  },
  "error": {
    "source": null,
    "error": "GET_DATA_SYSTEM_ERROR",
    "details": {
      "name": "Error",
      "msg": "getSettings error message: Network Error occurred"
    }
  }
}
```

Response Tab:

- Status:** 200 OK
- Content-Type:** `text/plain;charset=UTF-8`
- Server:** `cloudfront`
- Date:** `Sat, 19 Oct 2024 10:36:13 GMT`
- Access-Control-Allow-Origin:** `*`
- X-Cache:** `Miss from cloudfront`
- Server-Timing:**
 - `cdn-cache-hit,cdn-pop:desc="MCT50-PL",cdn-rid:desc="yzJfPPf58Myr5X6Xoh2ZHvJfLqR9QsLo6WZr9tWbCjbnGUpQmH0H==",cdn-hit-layer:desc="REC",cdn-downstream-fbl:dur=985`
- Other Headers:**
 - `Alt-Svc: h3="443"; aa=86400`
 - `X-Amz-Cf-Id: yzJfPPf58Myr5X6Xoh2ZHvJfLqR9QsLo6WZr9tWbCjbnGUpQmH0H==`
 - `X-Xss-Protection: 1; mode=block`
 - `Referrer-Policy: strict-origin-when-cross-origin`
 - `X-Content-Type-Options: nosniff`
 - `Strict-Transport-Security: max-age=31536000; includeSubDomains`
 - `Accept-CH: Device-Memory, Sec-CH-UA, Sec-CH-UA-Arch, Sec-CH-UA-Bitness, Sec-CH-DPR, Sec-CH-UA-Full-Version-List, Sec-CH-UA-Mobile, Sec-CH-UA-Model, Sec-CH-Viewport-Width, Sec-CH-UA-Platform, Sec-CH-UA-Platform-Version, Sec-CH-Width, Sec-CH-UA-Form-Factors`

Request

1 **POST** /v2/breeze-init-req HTTP/2
 2 Host: auth.uber.com
 3 **Content-Type:** application/json
 4 **Content-Length:** 151402
 5 **Sec-Ch-Ua:** "Not A Brand";v="99", "Chromium";v="124"
 6 **Sec-Ch-Ua-Platform:** "Linux"
 7 **Sec-Ch-Ua-Mobile:** ?0
 8 **User-Agent:** Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.118 Safari/537.36
 9 **Content-Type:** text/plain; charset=UTF-8
 10 **Origin:** https://auth.uber.com
 11 **Referer:** https://auth.uber.com/v2/breeze-init-req_id=64e9b924-cfd6-4d19-8f89-90882c34258f&breeze_e_local_zone=dca22&next_url=https%3A%2F%2Fauth.uber.com%2Flogin-redirect%2F%3FpreviousPath%3D%252Flooking&s_flow_id=84dCx3ql&state=5zrgsq5-d-9GZcRjthpFyUX6ni9y80KZ2dAtdYPIruY%3D
 12 **Accept-Encoding:** gzip, deflate, br
 13 **Accept-Language:** en-US,en;q=0.9
 14 **Priority:** u=4, i
 15 {

Response

1 HTTP/2 200 OK
 2 Date: Sat, 19 Jul 2025 18:53:12 GMT
 3 **Content-Type:** text/plain; charset=utf-8
 4 **Content-Length:** 2
 5 Load: q=38
 6 **Server:** edge-gateway.web
 7 **X-Request-Id:** 86bacd47-9e86-471f-a0fa-e67841d412e3
 8 **X-Uber-App:** edge-gateway-web
 9 **X-Uber-Rtapi-Duration:** 27
 10 **X-Frame-Options:** SAMEORIGIN
 11 **Cache-Control:** max-age=0
 12 **X-Envoy-Upstream-Service-Time:** 29
 13 **Strict-Transport-Security:** max-age=31536000
 14 **X-Content-Type-Options:** nosniff
 15 **X-Xss-Protection:** 1; mode=block
 16 **CF-Cache-Status:** DYNAMIC
 17 **X-Uber-Edge:** e4-dca18:v:996055069,ufe:production-cloudflare:compute-0:dca22.cloudflare:production:default
 18 **Server:** cloudflare
 19 **CF-Ray:** 961c6b953a82c904-KHI
 20
 21 OK