

# Burp Suite Community Edition

## Manual report

**IT Support Chatbot project:** Burp Suite vulnerability assessment report

**Sites:** <https://sec.cse.csusb.edu/team2/>

<https://sec.cse.csusb.edu/team2/jupyter>

**Manual report by:** Vedakshari Kanneti

### Objective:

- To detect and examine potential vulnerabilities in the chatbot system using Burp Suite Community Edition

### Methodology:

#### Approach:

- Capture and analyze HTTP requests and responses
- Test for common vulnerabilities such as SQL injection and security misconfigurations

### Findings

#### Overview Table:

Vulnerability	Severity	Description	Recommendation
Cross-Origin WebSocket Hijacking (CSWSH)	Low	Server blocks unauthorized WebSocket connections	Maintain configuration. Test for bypass.
Improper Origin Validation	Medium	Server relies on expected origins	Enhance origin verification with tokens
Security Misconfiguration	Low	Default WebSocket settings permit insecurity	Audit and update WebSocket settings

## Burp Suite Screenshots for <https://sec.cse.csusb.edu/team2/>

- Request and response in repeater after modifications

The screenshot shows the Burp Suite Repeater interface. The 'Request' tab is active, displaying a modified HTTP GET request to `/team2/_stcore/host-config`. The 'Response' tab shows the server's response, which is a JSON object containing a list of allowed origins and various security settings. The 'Inspector' panel on the right shows the request attributes, including the target URL and the request method.

**Request:**

```
1 GET /team2/_stcore/host-config HTTP/1.1
2 Host: sec.cse.csusb.edu
3 Sec-Ch-Ua-Platform: "Windows"
4 Accept-Language: en-US,en;q=0.9
5 Accept: application/json, text/plain, */*
6 Sec-Ch-Ua: "NotA_Brand";v="95", "Chromium";v="130"
7 Sec-Purpose: prefetch;prerender
8 Sec-Ch-Ua-Mobile: ?0
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 Purpose: prefetch
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: cors
13 Sec-Fetch-Dest: empty
14 Referer: https://sec.cse.csusb.edu/team2/
15 Accept-Encoding: gzip, deflate, br
16 Priority: u=1, i
17 Connection: keep-alive
```

**Response:**

```
1 HTTP/1.1 200 OK
2 Date: Mon, 25 Nov 2024 02:22:57 GMT
3 Server: TornadoServer/6.4.1
4 Strict-Transport-Security: max-age=63072000
5 Content-Type: application/json; charset=UTF-8
6 Cache-Control: no-cache
7 Etag: "706ea361a7ec785de3acd55cb3b1950b1cb06c9"
8 Content-Length: 654
9 Vary: Accept-Encoding
10 Keep-Alive: timeout=5, max=100
11 Connection: Keep-Alive
12
13 {
14   "allowedOrigins": [
15     "https://dev.stremlit.test",
16     "https://*.stremlit.apptest",
17     "https://*.stremlitapp.test",
18     "https://*.stremlitapp.com",
19     "https://share.stremlit.io",
20     "https://share-demo.stremlit.io",
21     "https://share-head.stremlit.io",
22     "https://share-staging.stremlit.io",
23     "https://*.demo.stremlit.run",
24     "https://*.head.stremlit.run",
25     "https://*.staging.stremlit.run",
26     "https://*.stremlit.run",
27     "https://*.demo.stremlit.app",
28     "https://*.head.stremlit.app",
29     "https://*.staging.stremlit.app",
30     "https://*.stremlit.app"
31   ],
32   "useExternalAuthToken": false,
33   "enableCustomParentMessages": false,
34   "enforceDownloadInNewTab": false,
35   "nativeUI": ""
36 }
```

## HTTP Requests

- List of HTTP requests captured while intercepting Academic Advisor Chatbot

The screenshot shows the Burp Suite HTTP History and Repeater interface. The 'HTTP History' tab is active, displaying a list of captured requests. The 'Repeater' tab is also visible, showing a modified HTTP GET request to `/team2/_stcore/host-config`. The 'Inspector' panel on the right shows the request attributes, including the target URL and the request method.

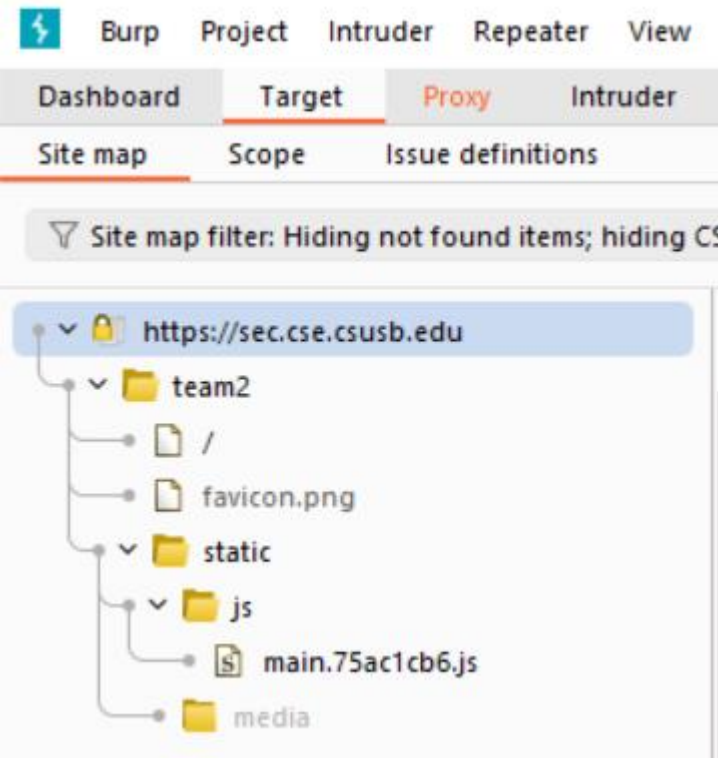
**HTTP History:**

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time	Listener port	Start response
1	https://sec.cse.csusb.edu	GET	/team2/			200	1377	HTML		Streamlit		✓	139.182.135.139		18:18:49.24 ...	8080	82
6	https://sec.cse.csusb.edu	GET	/team2/static/js/main.75ac1cb6.js			200	4508000	script	js			✓	139.182.135.139		18:18:54.24 ...	8080	62
7	https://sec.cse.csusb.edu	GET	/team2/_stcore/health									✓	139.182.135.139		18:18:54.24 ...	8080	
8	https://sec.cse.csusb.edu	GET	/team2/_stcore/host-config									✓	139.182.135.139		18:18:54.24 ...	8080	

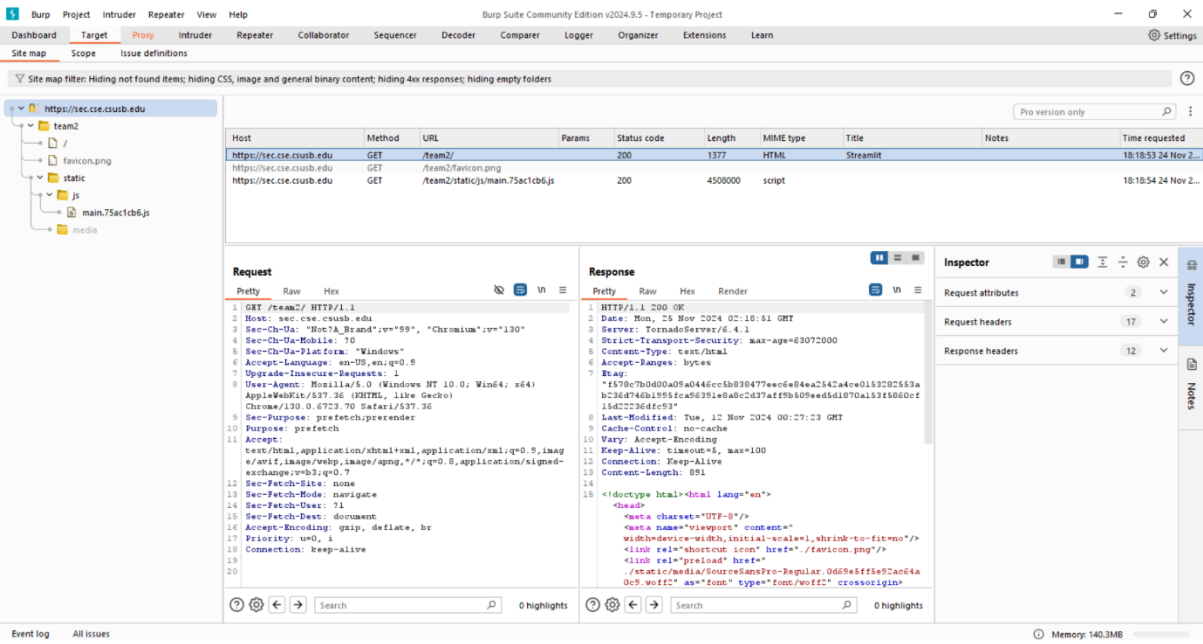
**Repeater:**

```
1 GET /team2/_stcore/host-config HTTP/1.1
2 Host: sec.cse.csusb.edu
3 Sec-Ch-Ua-Platform: "Windows"
4 Accept-Language: en-US,en;q=0.9
5 Accept: application/json, text/plain, */*
6 Sec-Ch-Ua: "NotA_Brand";v="95", "Chromium";v="130"
7 Sec-Purpose: prefetch;prerender
8 Sec-Ch-Ua-Mobile: ?0
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 Purpose: prefetch
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: cors
13 Sec-Fetch-Dest: empty
14 Referer: https://sec.cse.csusb.edu/team2/
15 Accept-Encoding: gzip, deflate, br
16 Priority: u=1, i
17 Connection: keep-alive
```

Sitemap analysis:



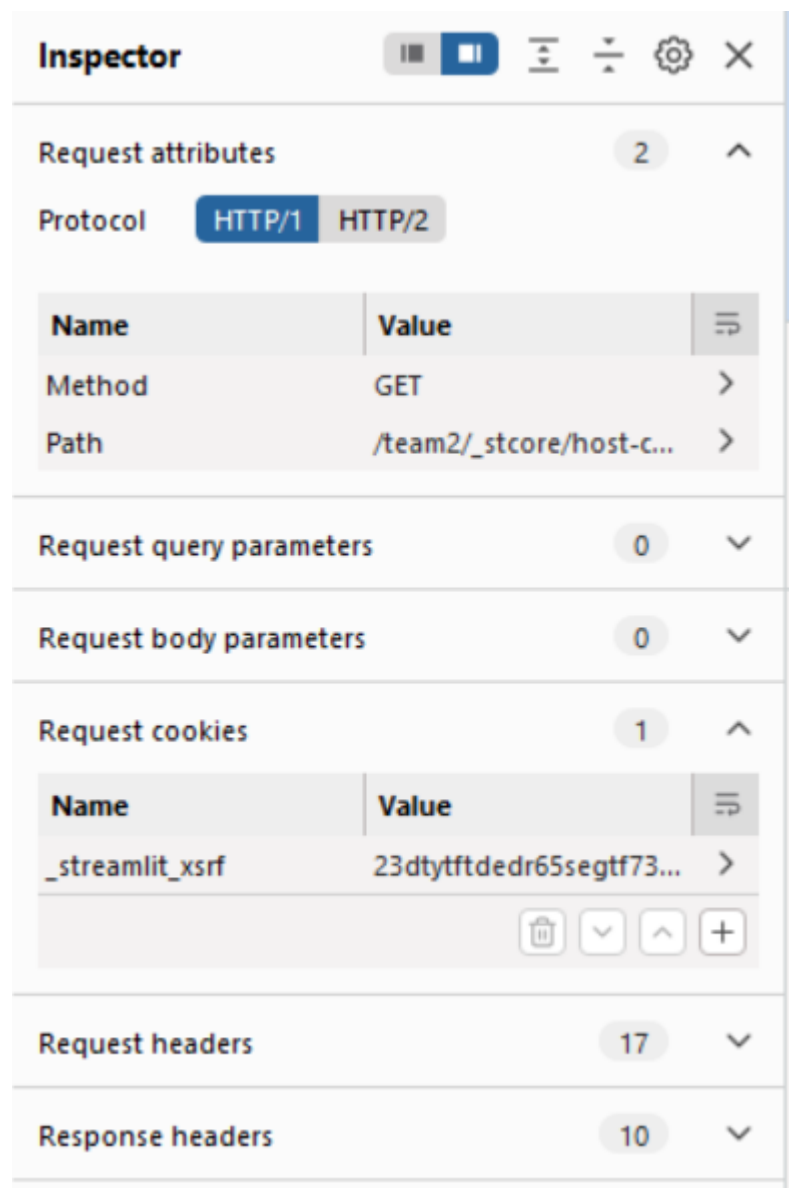
Sitemap Screenshot:



## Dash board inspector:

- **Request Headers:** "Connection: keep-alive" header keeps the connection open for multiple requests, improving network performance by reusing the same connection
- **Response Headers:** "vary: Accept -Encoding" the response may change based on the client's Accept-Encoding, typically to handle compressed formats like gzip or deflate

## Screenshots for Inspector:



Request headers			Response headers		
Name	Value		Name	Value	
Host	sec.cse.csusb.edu	>	Date	Mon, 25 Nov 2024 06:0...	>
Sec-Ch-Ua	"Not?A_Brand";v="99"...	>	Server	TornadoServer/6.4.1	>
Sec-Ch-Ua-Mobile	?0	>	Strict-Transport-Security	max-age=63072000	>
Sec-Ch-Ua-Platform	"Windows"	>	Content-Type	text/html	>
Accept-Language	en-US,en;q=0.9	>	Accept-Ranges	bytes	>
Upgrade-Insecure-Re...	1	>	Etag	"f578c7b0d00a09a044..."	>
User-Agent	Mozilla/5.0 (Windows...	>	Last-Modified	Tue, 12 Nov 2024 00:2...	>
Accept	text/html,application/...	>	Cache-Control	no-cache	>
Sec-Fetch-Site	none	>	Vary	Accept-Encoding	>
Sec-Fetch-Mode	navigate	>	Keep-Alive	timeout=5, max=100	>
Sec-Fetch-User	?1	>	Connection	Keep-Alive	>
Sec-Fetch-Dest	document	>	Content-Length	891	>
Accept-Encoding	gzip, deflate, br	>			
Priority	u=0, i	>			
Connection	keep-alive	>			
Cookie	-streamlit-xsrf=21ffgr...	>			

## Burp Suite Screenshots for <https://sec.cse.csusb.edu/team2/jupyter>

- Request and response in repeater after modifications

### Requests:

The screenshot shows the Burp Suite Repeater interface. The 'Request' tab is active, displaying a modified HTTP request. The 'Response' tab is also visible, showing the server's response. The 'Inspector' panel on the right shows the request and response headers and body.

**Request:**

```

1 GET /team2/jupyter/tree? HTTP/1.1
2 Host: sec.cse.csusb.edu
3 Accept-Language: en-US,en;q=0.9
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.6778.86 Safari/537.36
6 Sec-Purpose: prefetch;prerender
7 Purpose: prefetch
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: none
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-Dest: ?1
12 Sec-Fetch-Dest: document
13 Sec-Ch-Ua: "Chromium";v="131", "Not_A_Brand";v="24"
14 Sec-Ch-Ua-Mobile: ?0
15 Sec-Ch-Ua-Platform: "Windows"
16 Accept-Encoding: gzip, deflate, br
17 Priority: u=0, i
18 Connection: keep-alive
19
20

```

**Response:**

```

1 HTTP/1.1 200 OK (text/html)
2 Date: Mon, 25 Nov 2024 06:00:00 GMT
3 Server: TornadoServer/6.4.1
4 Strict-Transport-Security: max-age=63072000
5 Content-Type: text/html
6 Accept-Ranges: bytes
7 Etag: "f578c7b0d00a09a044..."
8 Last-Modified: Tue, 12 Nov 2024 00:20:00 GMT
9 Cache-Control: no-cache
10 Vary: Accept-Encoding
11 Keep-Alive: timeout=5, max=100
12 Connection: Keep-Alive
13 Content-Length: 891

```

**Inspector:**

- Request attributes: 2
- Request query parameters: 0
- Request body parameters: 0
- Request cookies: 0
- Request headers: 17
- Response headers: 12

# Responses:

1 x

+

Send

Cancel

<

>

Request

Response

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

29

HTTP/1.1 200 OK

Date: Tue, 26 Nov 2024 05:13:51 GMT

Server: TornadoServer/6.4.1

Strict-Transport-Security: max-age=63072000

Content-Type: text/html; charset=UTF-8

X-Content-Type-Options: nosniff

Content-Security-Policy: frame-ancestors 'self'; report-uri /teaml/jupyter/api/security/csp-report

Tag: "e71f1f32337b7ab4d89138093055fa76497f8f-gzip"

Set-Cookie: \_xsrf=C1953c05b01772397ad4705900d0064736596003b1f11732590031, expires=Thu, 26 Dec 2024 05:13:51 GMT; Path=/

Vary: Accept-Encoding

Content-Length: 20462

Keep-Alive: timeout=5, max=100

Connection: Keep-Alive

<!DOCTYPE HTML>

<html>

<head>

<meta charset="utf-8">

<title>

Home Page - Select or create a notebook

</title>

<link id="favicon" rel="shortcut icon" type="image/x-icon" href="/teaml/jupyter/static/base/images/favicon.ico?v=50afa725b5de6b00030139405b3862022d4e7d4a7c07e10e6d4643f30c9bfe6bb7e1ataic561aa3203440909a4b6fe7cd1e1747159330b3d51ab45400">

<meta http-equiv="X-UA-Compatible" content="IE=edge" />

<link rel="stylesheet" href="/teaml/jupyter/static/components/jquery-ui/dtsc/themes/smoothness/jquery-ui.min.css?v=aee962C670307f1e174f91e2da776c640f70959002c21170600b75950b2c7349a07f109a552b15ac8b11770a6c0d0c1a3bfc3b36a11c3c2e1a07c0ab" type="text/css" />

<link rel="stylesheet" href="/teaml/jupyter/static/components/jquery-typeahead/dtsc/jquery.typeahead.min.css?v=5edf53bfe6b3b1dda4f05940c5a7e2e62c1f15423e69c9816c742f63911c09ba2c529f8f47aebc7f46da207460347f56b11c0b70109a10071bada" type="text/css" />

<meta name="viewport" content="width=device-width, initial-scale=1.0">

<link rel="stylesheet" href="/teaml/jupyter/static/style/style.min.css?v=1e1abc38b672063a641ba468c6334c8d0f509729783ec9b7c6b4073004f5f056110c92c28aefb3dbf32e0e040f05b9f0470b411b669ed3d4f07511b1dca" type="text/css"/>

<link rel="stylesheet" href="/teaml/jupyter/custom/custom.css" type="text/css" />

<script src="/teaml/jupyter/static/components/es6-promise/promise.min.js?v=b6a335674136a63aeb5130f5ac9a50c256a5f435e6a09fef599491a040834a0b0f011ca7eaaca3b4ab6a2da2d3e1151567a2f171e60da1d0e5b5d5f84104" type="text/javascript" charset="utf-8">

<script src="/teaml/jupyter/static/components/react/react.production.min.js?v=9a0a0f94a316c0beddc2f7d5b5e0a13f0f04ec0244234c0ba0b042c6c01a0b6617e64f3675c2ebf337cb5b040e0b7b7b4d9377c5601d2c460d3d5de735" type="text/javascript">

<script src="/teaml/jupyter/static/components/react/react-dom.production.min.js?v=6fc60c1e730860ff04f57db0b5f2b0b9593a595710f3b4af4a10fb4e4ba2b4dd60644b42a0da0619a304946c943f05203641aa6fc01ec1b8ae84" type="text/javascript">

<script src="/teaml/jupyter/static/components/create-react-class/index.js?v=094ad57246e082b4c7e7d5e400acd6b30d06a4f4de4f342591e26761dc2ef1732cb419903104190070a77de12a1996de3e7da3a467db22b8da0f4610faec" type="text/javascript">

<script src="/teaml/jupyter/static/components/requirejs/require.js?v=437b40bb2137fa0ab90157e240c004dd5b1b57491173aa1d1f04c020c2a03d6df922d049e4015f7e5a369faa2e0b6a1000aae95b079b3bce0d41154f593" type="text/javascript" charset="utf-8">

<script>

require.config({

urlArgs: "v=20241126000343",

baseUrl: '/teaml/jupyter/static/',

paths: {

'auth/js/main': 'auth/js/main.min',

runtime: '/teaml/jupyter/custom',

nbextensions: '/teaml/jupyter/nbextensions',

kernelspecs: '/teaml/jupyter/kernelspecs',

underscore: 'components/underscore/underscore-min',

backbone: 'components/backbone/backbone-min',

}

)

</script>

Inspector

Request attributes

2

Request query parameters

0

Request body parameters

0

Request cookies

0

Request headers

17

Response headers

12

Done

21,143 bytes | 1,101 millis

Event log

All issues

Memory: 130.4MB

1 x

+

Send

Cancel

<

>

Request

Response

29

30

31

32

33

34

35

36

37

38

39

40

41

42

43

44

45

46

47

48

49

<link rel="stylesheet" href="/teaml/jupyter/static/style.min.css?v=1e1abc38b672063a641ba468c6334c8d0f509729783ec9b7c6b4073004f5f056110c92c28aefb3dbf32e0e040f05b9f0470b411b669ed3d4f07511b1dca" type="text/css"/>

<link rel="stylesheet" href="/teaml/jupyter/custom/custom.css" type="text/css" />

<script src="/teaml/jupyter/static/components/es6-promise/promise.min.js?v=b6a335674136a63aeb5130f5ac9a50c256a5f435e6a09fef599491a040834a0b0f011ca7eaaca3b4ab6a2da2d3e1151567a2f171e60da1d0e5b5d5f84104" type="text/javascript" charset="utf-8">

<script src="/teaml/jupyter/static/components/react/react.production.min.js?v=9a0a0f94a316c0beddc2f7d5b5e0a13f0f04ec0244234c0ba0b042c6c01a0b6617e64f3675c2ebf337cb5b040e0b7b7b4d9377c5601d2c460d3d5de735" type="text/javascript">

<script src="/teaml/jupyter/static/components/react/react-dom.production.min.js?v=6fc60c1e730860ff04f57db0b5f2b0b9593a595710f3b4af4a10fb4e4ba2b4dd60644b42a0da0619a304946c943f05203641aa6fc01ec1b8ae84" type="text/javascript">

<script src="/teaml/jupyter/static/components/create-react-class/index.js?v=094ad57246e082b4c7e7d5e400acd6b30d06a4f4de4f342591e26761dc2ef1732cb419903104190070a77de12a1996de3e7da3a467db22b8da0f4610faec" type="text/javascript">

<script src="/teaml/jupyter/static/components/requirejs/require.js?v=437b40bb2137fa0ab90157e240c004dd5b1b57491173aa1d1f04c020c2a03d6df922d049e4015f7e5a369faa2e0b6a1000aae95b079b3bce0d41154f593" type="text/javascript" charset="utf-8">

<script>

require.config({

urlArgs: "v=20241126000343",

baseUrl: '/teaml/jupyter/static/',

paths: {

'auth/js/main': 'auth/js/main.min',

runtime: '/teaml/jupyter/custom',

nbextensions: '/teaml/jupyter/nbextensions',

kernelspecs: '/teaml/jupyter/kernelspecs',

underscore: 'components/underscore/underscore-min',

backbone: 'components/backbone/backbone-min',

}

)

</script>

Inspector

Request attributes

2

Request query parameters

0

Request body parameters

0

Request cookies

0

Request headers

17

Response headers

12

Done

21,143 bytes | 1,101 millis

Event log

All issues

Memory: 130.4MB

RequestResponse

PrettyRawHexRender

50jed: 'components/jed/jed',

51jquery: 'components/jquery/jquery.min',

52json: 'components/requirejs-plugins/src/json',

53text: 'components/requirejs-text/text',

54bootstrap: 'components/bootstrap/dist/js/bootstrap.min',

55bootstrap-tour: 'components/bootstrap-tour/build/js/bootstrap-tour.min',

56jquery-ui: 'components/jquery-ui/dist/jquery-ui.min',

57moment: 'components/moment/min/moment-with-locales',

58codemirror: 'components/codemirror',

59termjs: 'components/xterm.js/xterm',

60typeahead: 'components/jquery-typeahead/dist/jquery.typeahead.min',

61

62

63map: {

64// for backward compatibility

65\*\*\*: {

66"jqueryui": "jquery-ui",

67

68},

69shim: {

70typeahead: {

71deps: ["jquery"],

72exports: "typeahead"

73

74underscore: {

75exports: '\_'

76

77},

78backbone: {

79deps: ["underscore", "jquery"],

80exports: "Backbone"

81

82},

83bootstrap: {

84deps: ["jquery"],

85exports: "bootstrap"

86

87},

88bootstrap-tour: {

89deps: ["bootstrap"],

90exports: "Tour"

91

92}

93

94

95

96

97

98

99

100

101

102

103

104

105

106

107

108

109

110

111

112

113

114

115

116

117

118

119

120

121

122

123

124

125

126

127

128

129

130

131

132

133

134

135

136

137

138

139

140

141

142

143

144

145

146

147

148

149

150

0 highlights

RequestResponse

PrettyRawHexRender

91

92

93

94

95

96

97

98

99

100

101

102

103

104

105

106

107

108

109

110

111

112

113

114

115

116

117

118

119

120

121

122

123

124

125

126

127

128

129

130

131

132

133

134

135

136

137

138

139

140

141

142

143

144

145

146

147

148

149

150

0 highlights

RequestResponse

PrettyRawHexRender

123

124

125

126

127

128

129

130

131

132

133

134

135

136

137

138

139

140

141

142

143

144

145

146

147

148

149

150

0 highlights

Request		Response
Pretty	Raw	Hex
151	Please enable it to proceed.	
152	</div>	
153	</noscript>	
154		
155	<div id="header" role="navigation" aria-label="Top Menu">	
156	<div id="newsId" style="display: none">	
157	<div class="alert alert-info" role="alert">	
158	<div style="display: flex">	
159	<div>	
160	<span class="label label-warning">	
161	UPDATE	
162	Read <a href="https://jupyter-notebook.readthedocs.io/en/latest/migrate_to_notebook7.html" style="text-decoration: underline;" target="_blank">	
163	the migration plan	
164	</a>	
165	to Notebook 7 to learn about the new features and the actions to take if you are using extensions	
166	Please note that updating to Notebook 7 might break some of your extensions.	
167	</div>	
168	<div style="margin-left: auto;">	
169	<a href="" onclick="alert('This message will not be shown anymore.');" return false;">	
170	<button type="button" class="btn btn-default btn-xs" id="dontShowId">	
171	Don't show anymore	
172	</button>	
173	</div>	
174	</div>	
175	</div>	
176	<div id="header-container" class="container">	
177	<div id="ipython_notebook" class="nav navbar-brand">	
178	<a href="/team1/jupyter/tree" title="dashboard">	
179		
180	</a>	

Request		Response
Pretty	Raw	Hex
181	</div>	
182		
183	<span class="flex-spacer">	
184	</span>	
185		
186	<span id="shutdown_widget">	
187	<button id="shutdown" class="btn btn-sm navbar-btn">	
188	title="Stop the Jupyter server">	
189	Quit	
190	</button>	
191	</span>	
192		
193		
194		
195		
196		
197		
198		
199		
200	<span id="login_widget">	
201		
202	</span>	
203		
204		
205		
206		
207	</div>	
208	<div class="header-bar">	
209	</div>	
210		
211	</div>	
212		
213	<div id="site">	
214		
215		



Request		Response		
		Pretty	Raw	Hex
217				
218		<div id="ipython-main-app" class="container">		
219		<div id="tab_content" class="tabbable" role="main">		
220		<ul id="tabs" class="nav nav-tabs">		
221		<li class="active">		
		<a href="#notebooks" data-toggle="tab">		
		Files		
		</a>		
		</li>		
222		<li>		
		<a href="#running" data-toggle="tab">		
		Running		
		</a>		
		</li>		
223		<li>		
		<a href="#clusters" data-toggle="tab" class="clusters_tab_link" >		
		Clusters		
		</a>		
		</li>		
224		</ul>		
225		<div class="tab-content">		
226		<div id="notebooks" class="tab-pane active">		
227		<div id="notebook_toolbar" class="row">		
228		<div class="col-sm-8 no-padding">		
229		<div class="dynamic-instructions">		
230		Select items to perform actions on them.		
231		</div>		
232		<div class="dynamic-buttons">		
233		<button title="Duplicate selected" aria-label="Duplicate selected" class="duplicate-button btn btn-default btn-xs" aria-describedby="tooltip1">		
		Duplicate		
		</button>		
234		<div role="tooltip" id="tooltip1" >		
		Duplicate selected		
		</div>		
235		<button title="Rename selected" aria-label="Rename selected" class="rename-button btn btn-default btn-xs" aria-describedby="tooltip2">		
		Rename		
		</button>		
236		<div role="tooltip" id="tooltip2" >		

Request		Response		
		Pretty	Raw	Hex
		Rename selected		
		</div>		
237		<button title="Move selected" aria-label="Move selected" class="move-button btn btn-default btn-xs" aria-describedby="tooltip3">		
		Move		
		</button>		
238		<div role="tooltip" id="tooltip3" >		
		Move selected		
		</div>		
239		<button title="Download selected" aria-label="Download selected" class="download-button btn btn-default btn-xs" aria-describedby="tooltip4">		
		Download		
		</button>		
240		<div role="tooltip" id="tooltip4" >		
		Download selected		
		</div>		
241		<button title="Shutdown selected notebook(s)" aria-label="Shutdown selected notebook(s)" class="shutdown-button btn btn-default btn-xs btn-warning" aria-describedby="tooltip5">		
		Shutdown		
		</button>		
242		<div role="tooltip" id="tooltip5" >		
		Shutdown selected notebook(s)		
		</div>		
243		<button title="View selected" aria-label="View selected" class="view-button btn btn-default btn-xs" aria-describedby="tooltip6">		
		View		
		</button>		
244		<div role="tooltip" id="tooltip6" >		
		View selected		
		</div>		
245		<button title="Edit selected" aria-label="Edit selected" class="edit-button btn btn-default btn-xs" aria-describedby="tooltip7">		
		Edit		
		</button>		
246		<div role="tooltip" id="tooltip7" >		
		Edit selected		
		</div>		

Request	Response		
Pretty	Raw	Hex	Render

```
247 <button title="Delete selected" aria-label="Delete selected" class="delete-button btn btn-default btn-xs btn-danger" aria-describedby=" 248 tooltip8"> 249   <i class="fa fa-trash"> 250 </i> 251 </button> 252 <div role="tooltip" id="tooltip8" > 253   Delete selected 254 </div> 255 </div> 256 <div class="col-sm-4 no-padding tree-buttons"> 257 <div class="pull-right"> 258   <form id='alternate_upload' class='alternate_upload'> 259     <span id='notebook_list_info"> 260       <span id="upload_span" class="btn btn-xs btn-default btn-upload" role="button" tabindex="0"> 261         <input id="upload_span_input" title="Click to browse for a file to upload." type="file" name="datafile" class="fileinput" multiple=' 262         multiple' tabindex="-1"> 263         Upload 264       </span> 265     </span> 266   </form> 267   <div id="new-buttons" class="btn-group"> 268     <button class="dropdown-toggle btn btn-default btn-xs" id="new-dropdown-button" data-toggle="dropdown"> 269       <span> 270         New 271       </span> 272       <span class="caret"> 273       </span> 274       <span class="sr-only"> 275         Toggle Dropdown 276       </span> 277     </button> 278     <ul id="new-menu" class="dropdown-menu" role="menu"> 279       <li role="menuitem" class="dropdown-header" id="notebook-kernels"> 280         Notebook: 281       </li> 282       <li role="presentation" class="divider"> 283       </li>
```

```
Request      Response
Pretty      Raw      Hex      Render
297          <input type="text" value="" class="form-control" style="width: 100%; height: 30px; border: 1px solid #ccc; border-radius: 4px; margin-bottom: 10px;"/>  
298          </input>  
299          </span>  
300          </div>  
301          <div class="dropdown-menu" style="border: 1px solid #ccc; border-radius: 4px; padding: 5px; margin-top: 5px; width: 100%; background-color: #fff; box-shadow: 0 5px 5px #888; z-index: 1000;"/>  
302          <div style="display: flex; justify-content: space-between; align-items: center; padding: 5px 10px; border-bottom: 1px solid #eee; margin-bottom: 5px;"/>  
303          <div style="font-size: 0.9em; color: #666; font-weight: normal; margin: 0;"/>  
304          <div style="font-size: 0.8em; color: #666; font-weight: normal; margin: 0;"/>  
305          <div style="display: flex; justify-content: space-between; align-items: center; padding: 5px 10px; border-top: 1px solid #eee; margin-top: 5px;"/>  
306          <div style="font-size: 0.9em; color: #666; font-weight: normal; margin: 0;"/>  
307          <div style="font-size: 0.8em; color: #666; font-weight: normal; margin: 0;"/>  
308          </div>  
309          </div>  
310          </div>  
311          </div>  
312          </div>  
313          </div>  
314          </div>  
315          </div>  
316          </div>  
317          </div>  
318          </div>  
319          </div>  
320          </div>  
321          </div>  
322          </div>  
323          </div>  
324          </div>  
325          </div>  
326          </div>  
327          </div>  
328          </div>  
329          </div>  
330          </div>  
331          </div>  
332          </div>  
333          </div>  
334          </div>  
335          </div>  
336          </div>  
337          </div>  
338          </div>  
339          </div>  
340          </div>  
341          </div>  
342          </div>  
343          </div>  
344          </div>  
345          </div>  
346          </div>  
347          </div>  
348          </div>  
349          </div>  
350          </div>  
351          </div>  
352          </div>  
353          </div>  
354          </div>  
355          </div>  
356          </div>  
357          </div>  
358          </div>  
359          </div>  
360          </div>  
361          </div>  
362          </div>  
363          </div>  
364          </div>  
365          </div>  
366          </div>  
367          </div>  
368          </div>  
369          </div>  
370          </div>  
371          </div>  
372          </div>  
373          </div>  
374          </div>  
375          </div>  
376          </div>  
377          </div>  
378          </div>  
379          </div>  
380          </div>  
381          </div>  
382          </div>  
383          </div>  
384          </div>  
385          </div>  
386          </div>  
387          </div>  
388          </div>  
389          </div>  
390          </div>  
391          </div>  
392          </div>  
393          </div>  
394          </div>  
395          </div>  
396          </div>  
397          </div>  
398          </div>  
399          </div>  
400          </div>  
401          </div>  
402          </div>  
403          </div>  
404          </div>  
405          </div>  
406          </div>  
407          </div>  
408          </div>  
409          </div>  
410          </div>  
411          </div>  
412          </div>  
413          </div>  
414          </div>  
415          </div>  
416          </div>  
417          </div>  
418          </div>  
419          </div>  
420          </div>  
421          </div>  
422          </div>  
423          </div>  
424          </div>  
425          </div>  
426          </div>  
427          </div>  
428          </div>  
429          </div>  
430          </div>  
431          </div>  
432          </div>  
433          </div>  
434          </div>  
435          </div>  
436          </div>  
437          </div>  
438          </div>  
439          </div>  
440          </div>  
441          </div>  
442          </div>  
443          </div>  
444          </div>  
445          </div>  
446          </div>  
447          </div>  
448          </div>  
449          </div>  
450          </div>  
451          </div>  
452          </div>  
453          </div>  
454          </div>  
455          </div>  
456          </div>  
457          </div>  
458          </div>  
459          </div>  
460          </div>  
461          </div>  
462          </div>  
463          </div>  
464          </div>  
465          </div>  
466          </div>  
467          </div>  
468          </div>  
469          </div>  
470          </div>  
471          </div>  
472          </div>  
473          </div>  
474          </div>  
475          </div>  
476          </div>  
477          </div>  
478          </div>  
479          </div>  
480          </div>  
481          </div>  
482          </div>  
483          </div>  
484          </div>  
485          </div>  
486          </div>  
487          </div>  
488          </div>  
489          </div>  
490          </div>  
491          </div>  
492          </div>  
493          </div>  
494          </div>  
495          </div>  
496          </div>  
497          </div>  
498          </div>  
499          </div>  
500          </div>  
501          </div>  
502          </div>  
503          </div>  
504          </div>  
505          </div>  
506          </div>  
507          </div>  
508          </div>  
509          </div>  
510          </div>  
511          </div>  
512          </div>  
513          </div>  
514          </div>  
515          </div>  
516          </div>  
517          </div>  
518          </div>  
519          </div>  
520          </div>  
521          </div>  
522          </div>  
523          </div>  
524          </div>  
525          </div>  
526          </div>  
527          </div>  
528          </div>  
529          </div>  
530          </div>  
531          </div>  
532          </div>  
533          </div>  
534          </div>  
535          </div>  
536          </div>  
537          </div>  
538          </div>  
539          </div>  
540          </div>  
541          </div>  
542          </div>  
543          </div>  
544          </div>  
545          </div>  
546          </div>  
547          </div>  
548          </div>  
549          </div>  
550          </div>  
551          </div>  
552          </div>  
553          </div>  
554          </div>  
555          </div>  
556          </div>  
557          </div>  
558          </div>  
559          </div>  
560          </div>  
561          </div>  
562          </div>  
563          </div>  
564          </div>  
565          </div>  
566          </div>  
567          </div>  
568          </div>  
569          </div>  
570          </div>  
571          </div>  
572          </div>  
573          </div>  
574          </div>  
575          </div>  
576          </div>  
577          </div>  
578          </div>  
579          </div>  
580          </div>  
581          </div>  
582          </div>  
583          </div>  
584          </div>  
585          </div>  
586          </div>  
587          </div>  
588          </div>  
589          </div>  
590          </div>  
591          </div>  
592          </div>  
593          </div>  
594          </div>  
595          </div>  
596          </div>  
597          </div>  
598          </div>  
599          </div>  
600          </div>  
601          </div>  
602          </div>  
603          </div>  
604          </div>  
605          </div>  
606          </div>  
607          </div>  
608          &
```

Request		Response		
		Pretty	Raw	Hex
333		</button>		
334		</div>		
335		</div>		
336		</div>		
337		</div>		
338		</div>		
339		<div id="running" class="tab-pane">		
340		<div id="running_toolbar" class="row">		
341		<div class="col-sm-8 no-padding">		
342		<span id="running_list_info">		
		Currently running Jupyter processes		
		</span>		
343		</div>		
344		<div class="col-sm-4 no-padding tree-buttons">		
345		<span id="running_buttons" class="pull-right">		
346		<button id="refresh_running_list" title="Refresh running list" aria-label="Refresh running list" class="btn btn-default btn-xs">		
		<i class="fa fa-refresh">		
		</i>		
		</button>		
		</span>		
347		</div>		
348		</div>		
349		<div class="panel-group" id="accordion">		
350		<div class="panel panel-default">		
351		<div class="panel-heading">		
352		<a data-toggle="collapse" data-target="#collapseOne" href="#">		
353		Terminals		
354		</a>		
355		</div>		
356		<div id="collapseOne" class="collapse in">		
357		<div class="panel-body">		
358		<div id="terminal_list">		
359		<div id="terminal_list_header" class="row list_placeholder">		
360		<div>		
361		There are no terminals running.		
362		</div>		
363		</div>		

Request		Response		
		Pretty	Raw	Hex
364		</div>		
365		</div>		
366		</div>		
367		</div>		
368		</div>		
369		<div class="panel panel-default">		
370		<div class="panel-heading">		
371		<a data-toggle="collapse" data-target="#collapseTwo" href="#">		
372		Notebooks		
373		</a>		
374		</div>		
375		<div id="collapseTwo" class="collapse in">		
376		<div class="panel-body">		
377		<div id="running_list">		
378		<div id="running_list_placeholder" class="row list_placeholder">		
379		<div>		
		There are no notebooks running.		
		</div>		
380		</div>		
381		</div>		
382		</div>		
383		</div>		
384		</div>		
385		</div>		
386		</div>		
387		<div id="clusters" class="tab-pane">		
388		Clusters tab is now provided by IPython parallel.		
389		See ' <a href="https://github.com/ipython/ipyparallel">a href="https://github.com/ipython/ipyparallel"</a> '		
		IPython parallel		
		</a>		
		' for installation details.		
390		</div>		
391		</div>		
		<!-- class:tab-content -->		
392		</div>		
		<!-- id:tab_content -->		
393		</div>		
		<!-- ipython-main-app -->		

```

395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427

```

```

</div>

<script src=
/teaml/jupyter/static/tree/js/main.min.js?v=17b01c53df313alc8db8c3dled29350f9b3415f9fdb158eac238d1fb5b0d7e122cde2bbe9754122366365ed03b74885dia7854b720351ble
25bed20198cf609" type="text/javascript" charset="utf-8">
</script>

<script type="text/javascript">
$(function){$.tooltip('enable')}
</script>

<script type="text/javascript">
function _remove_token_from_url() {
  if (window.location.search.length <= 1) {
    return;
  }
  var search_parameters = window.location.search.slice(1).split('&');
  for (var i = 0;
    i < search_parameters.length;
    i++) {
    if (search_parameters[i].split('=')[0] === 'token') {
      // remove token from search parameters
      search_parameters.splice(i, 1);
      var new_search = '';
      if (search_parameters.length) {
        new_search = '?' + search_parameters.join('&');
      }
      var new_url = window.location.origin +
        window.location.pathname +
        new_search +

```

```

Request  Response
Pretty  Raw  Hex  Render
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449

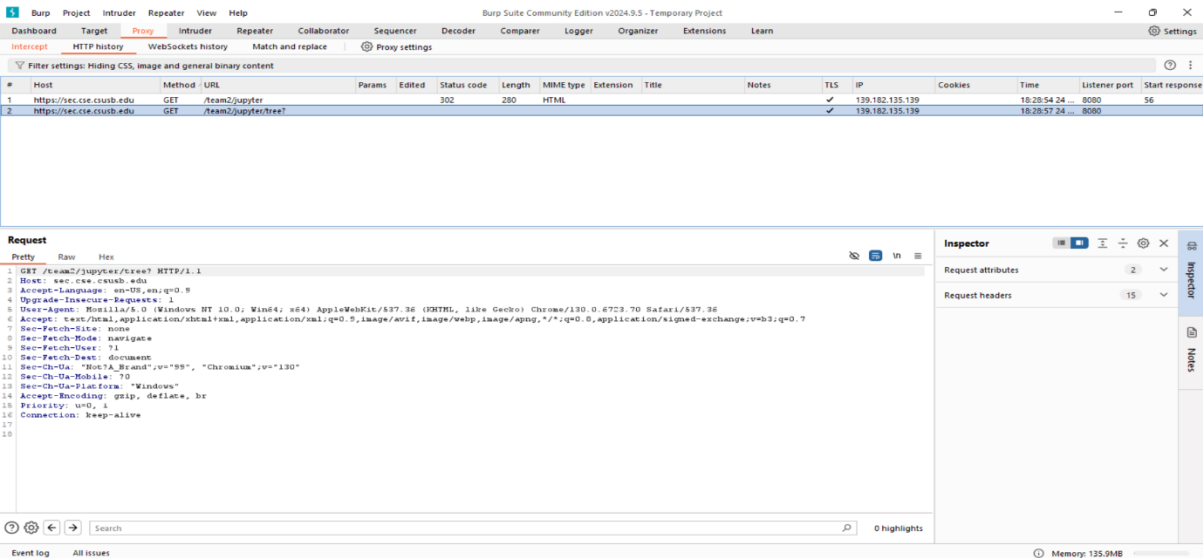
```

```

var new_search = '';
if (search_parameters.length) {
  new_search = '?' + search_parameters.join('&');
}
var new_url = window.location.origin +
  window.location.pathname +
  new_search +
  window.location.hash;
window.history.replaceState({
  }, new_url);
return;
}
_remove_token_from_url();
sys_info = {
  "notebook_version": "6.5.7", "notebook_path": "/opt/miniforge/envs/teaml_env/lib/python3.10/site-packages/notebook", "commit_source": "", "commit_hash":
  "", "sys_version": "3.10.15 | packaged by conda-forge | (main, Oct 16 2024, 01:24:24) [GCC 13.3.0]", "sys_executable":
  "/opt/miniforge/envs/teaml_env/bin/python3.10", "sys_platform": "linux", "platform": "Linux-6.1.0-23-amd64-x86_64-with-glibc2.36", "os_name": "posix",
  "default_encoding": "utf-8"
};
document.addEventListener('DOMContentLoaded', function () {
  const newsId = document.querySelector('#newsId');
  const dontShowId = document.querySelector('#dontShowId');
  const showNotebookNews = localStorage.getItem('showNotebookNews');
  dontShowId.addEventListener('click', () => {
    localStorage.setItem('showNotebookNews', false);
    newsId.style.display = 'none';
  });
  if (!showNotebookNews) newsId.style.display = 'inline';
});
</script>
</body>
</html>

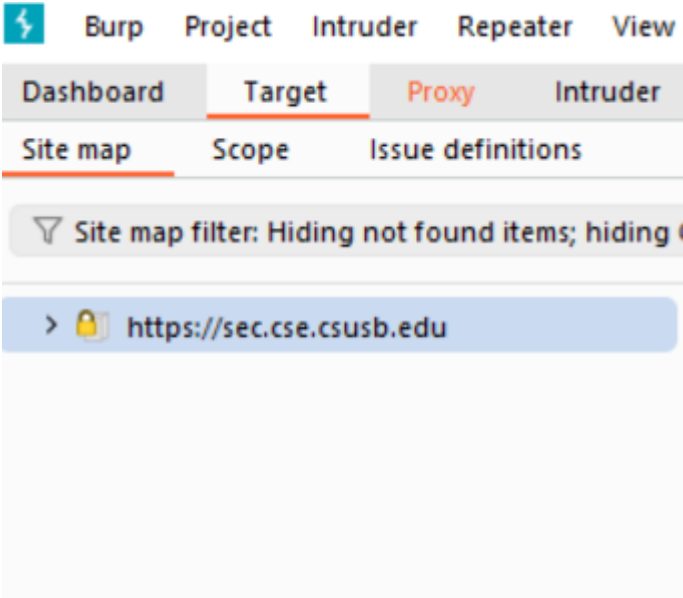
```

# HTTP Requests



## Sitemap analysis:

- Endpoint analyzed



## Sitemap Screenshots:

The screenshot displays the Burp Suite interface. At the top, the menu bar includes Burp, Project, Intruder, Repeater, View, and Help. Below it, the toolbar shows various tools like Dashboard, Target, Proxy, Intruder, Repeater, Collaborator, Sequencer, Decoder, Comparer, Logger, Organizer, Extensions, and Learn. The main window is divided into several panes. On the left, the 'Site map' pane shows a tree view of the website structure, with the URL 'https://sec.cse.csusb.edu' selected. The central pane displays a table of HTTP requests and responses. The table has columns for Host, Method, URL, Params, Status code, Length, MIME type, Title, Notes, and Time requested. The first row shows a GET request to '/team2/jupyter' with a status code of 302 and a length of 280. The second row shows a GET request to '/team2/jupyter/tree' with a status code of 200. The third row shows a GET request to '/team2/jupyter/tree?' with a status code of 200. Below the table, the 'Request' and 'Response' panes show the raw HTTP data. The 'Request' pane shows a GET request to '/team2/jupyter' with various headers like Host, Sec-CH-UA, Sec-CH-UA-Mobile, Sec-CH-UA-Platform, Accept-Language, Upgrade-Insecure-Requests, User-Agent, and Accept. The 'Response' pane shows a 302 Found status with headers like Date, Server, Strict-Transport-Security, Content-Type, Location, Content-Length, Keep-Alive, and Connection. On the right, the 'Inspector' pane shows the 'Request attributes' and 'Request headers' sections. The 'Request attributes' section shows the URL and the 'Request headers' section shows the headers of the request. The bottom status bar shows 'Event log', 'All issues', and 'Memory: 135.9MB'.

Host	Method	URL	Params	Status code	Length	MIME type	Title	Notes	Time requested
https://sec.cse.csusb.edu	GET	/team2/jupyter		302	280				19:28:57 24 Nov 2...
https://sec.cse.csusb.edu	GET	/team2/jupyter/tree		200					
https://sec.cse.csusb.edu	GET	/team2/jupyter/tree?		200					

**Request**

```
1 GET /team2/jupyter HTTP/1.1
2 Host: sec.cse.csusb.edu
3 Sec-CH-UA: "NotA_Brand";v="99", "Chromium";v="130"
4 Sec-CH-UA-Mobile: ?0
5 Sec-CH-UA-Platform: "Windows"
6 Accept-Language: en-US,en;q=0.9
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
9 AppleWebKit/537.36 (KHTML, like Gecko)
10 Chrome/130.0.6723.70 Safari/537.36
11 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
12 Sec-Fetch-Site: none
13 Sec-Fetch-Mode: navigate
14 Sec-Fetch-User: ?1
15 Sec-Fetch-Dest: document
16 Accept-Encoding: gzip, deflate, br
17 Priority: u=0, i
18 Connection: keep-alive
```

**Response**

```
1 HTTP/1.1 302 Found
2 Date: Mon, 25 Nov 2024 02:28:55 GMT
3 Server: TornadoServer/6.4.1
4 Strict-Transport-Security: max-age=63072000
5 Content-Type: text/html; charset=UTF-8
6 Location: /team2/jupyter/tree?
7 Content-Length: 0
8 Keep-Alive: timeout=5, max=100
9 Connection: Keep-Alive
```

**Inspector**

Request attributes: 2







Request headers: 15

Response headers: 8

## Dash board inspector

- **Request Headers:** "Connection: keep-alive" header keeps the connection open for multiple requests, improving network performance by reusing the same connection
- **Response Headers:** "vary: Accept -Encoding" the response may change based on the client's Accept-Encoding, typically to handle compressed formats like gzip or deflate

## Screenshots for inspector

**Inspector**      

Request attributes2 ^

Protocol **HTTP/1** HTTP/2





Name	Value	
Method	GET	>
Path	/team2/jupyter	>

Request query parameters0 v

Request body parameters0 v

Request cookies1 ^

Name	Value	
jupyter	23sdvhgfhdfnjd54gfd...	>



Request headers		
		16 ^
Name	Value	
Host	sec.cse.csusb.edu	>
Sec-Ch-Ua	"Not?A_Brand";v="99"...	>
Sec-Ch-Ua-Mobile	?0	>
Sec-Ch-Ua-Platform	"Windows"	>
Accept-Language	en-US,en;q=0.9	>
Upgrade-Insecure-Re...	1	>
User-Agent	Mozilla/5.0 (Windows...	>
Accept	text/html,application/...	>
Sec-Fetch-Site	none	>
Sec-Fetch-Mode	navigate	>
Sec-Fetch-User	?1	>
Sec-Fetch-Dest	document	>
Accept-Encoding	gzip, deflate, br	>
Priority	u=0, i	>
Connection	keep-alive	>
Cookie	jupyter=23sdvhgfhdf...	>

Response headers		
		8 ^
Name	Value	
Date	Mon, 25 Nov 2024 06:3...	>
Server	TornadoServer/6.4.1	>
Strict-Transport-Security	max-age=63072000	>
Content-Type	text/html; charset=UT...	>
Location	/team1/jupyter/tree?	>
Content-Length	0	>
Keep-Alive	timeout=5, max=100	>
Connection	Keep-Alive	>

## Conclusion:

### •HTTP Headers:

- “Connection: keep-alive” enhances performance but may pose security risks if not managed
- “Vary: Accept-Encoding” optimizes caching but could lead to cache poisoning if misconfigured