

HackerFrogs Afterschool

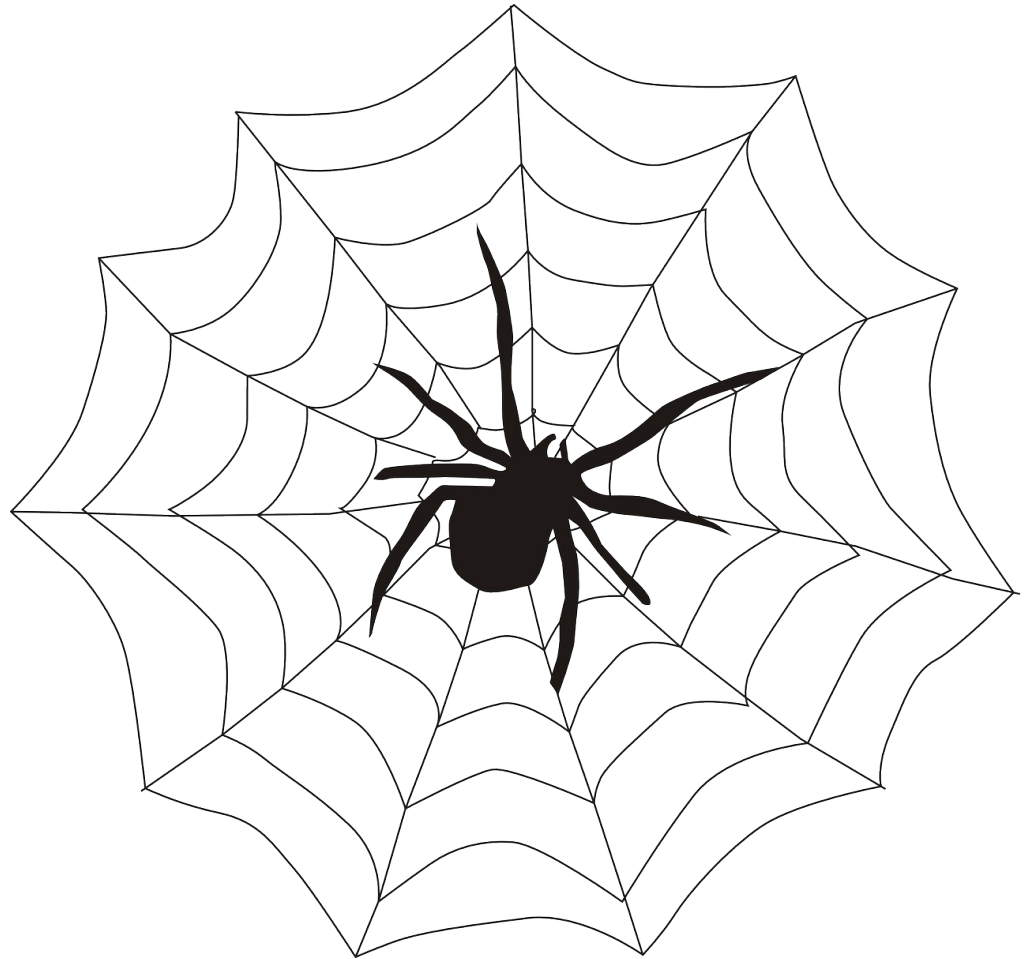
Web App 8: Burp Suite Pt. 2 of 2

Class:
Web App Hacking

Workshop Number:
AS-WEB-08

Document Version:
1.2

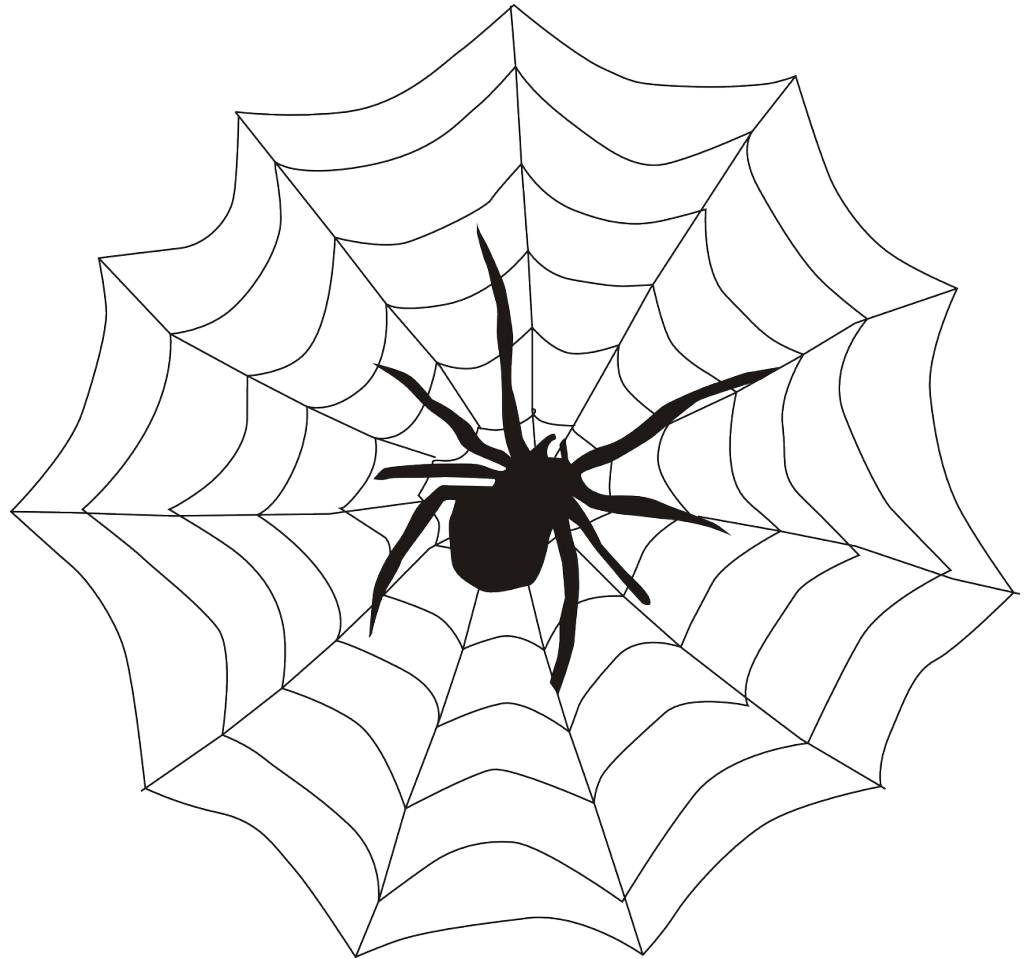
Special Requirements:
Registered account at
tryhackme.com



What We Learned In The Previous Workshop

This is the eighth intro to web app hacking workshop.

In the previous workshop we learned about the following web app hacking concepts:



Burp Suite

Burp Suite is the industry-standard software framework for testing web apps. It includes many different tools, and the following two tools:



Burp Proxy



The Burp Proxy server is what enables web traffic to be captured and recorded. It sits between the browser and the server, enabling traffic capture.

Burp Repeater



And the Burp Repeater is a tool which allows for manual web request manipulation and replay.

This Workshop's Topic

In this workshop, we'll be taking another look at Burp Suite, focusing in on the (arguably) most important tool, the Burp Repeater

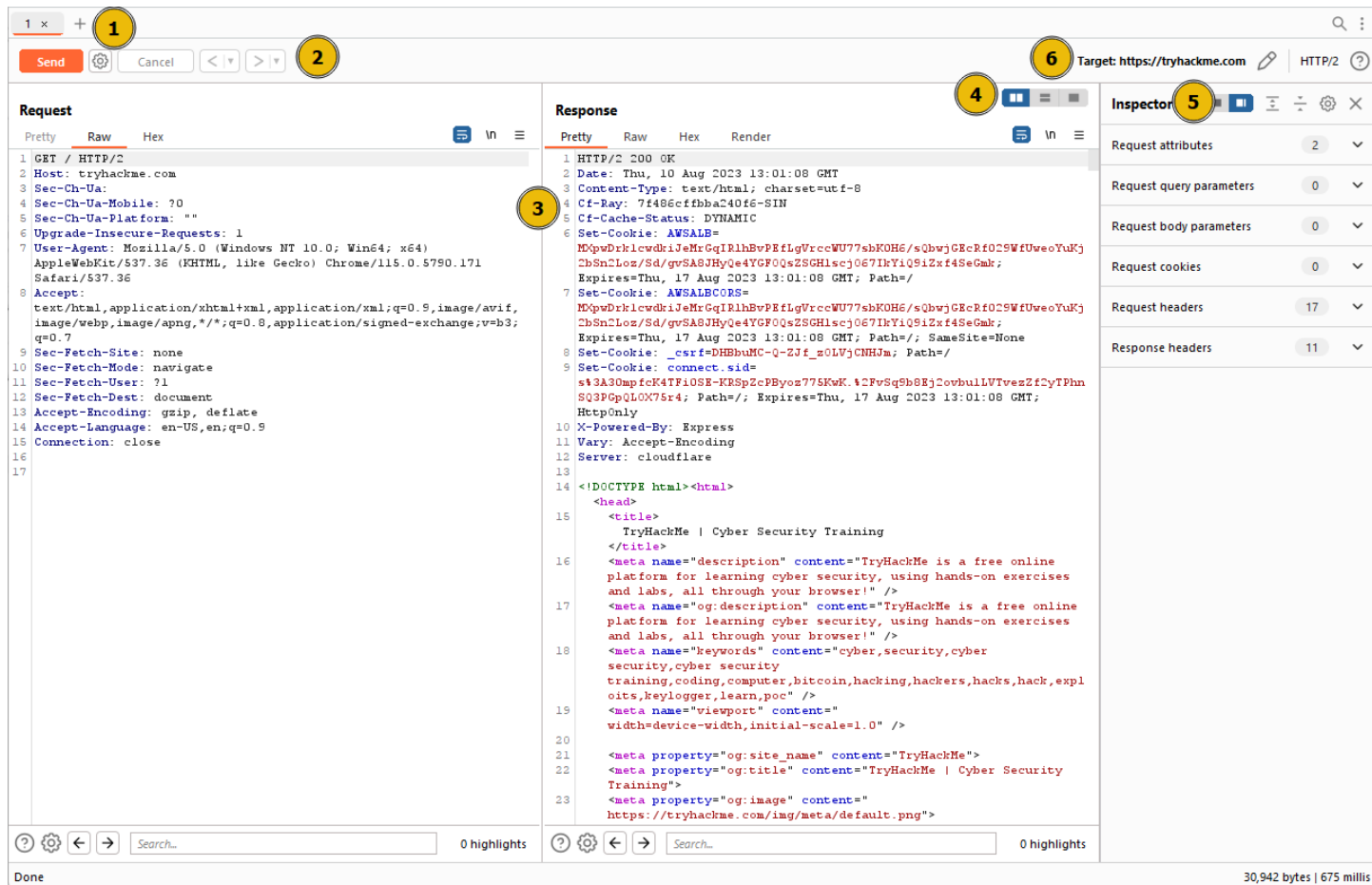


Let's Learn More With TryHackMe

Navigate to the following URL:

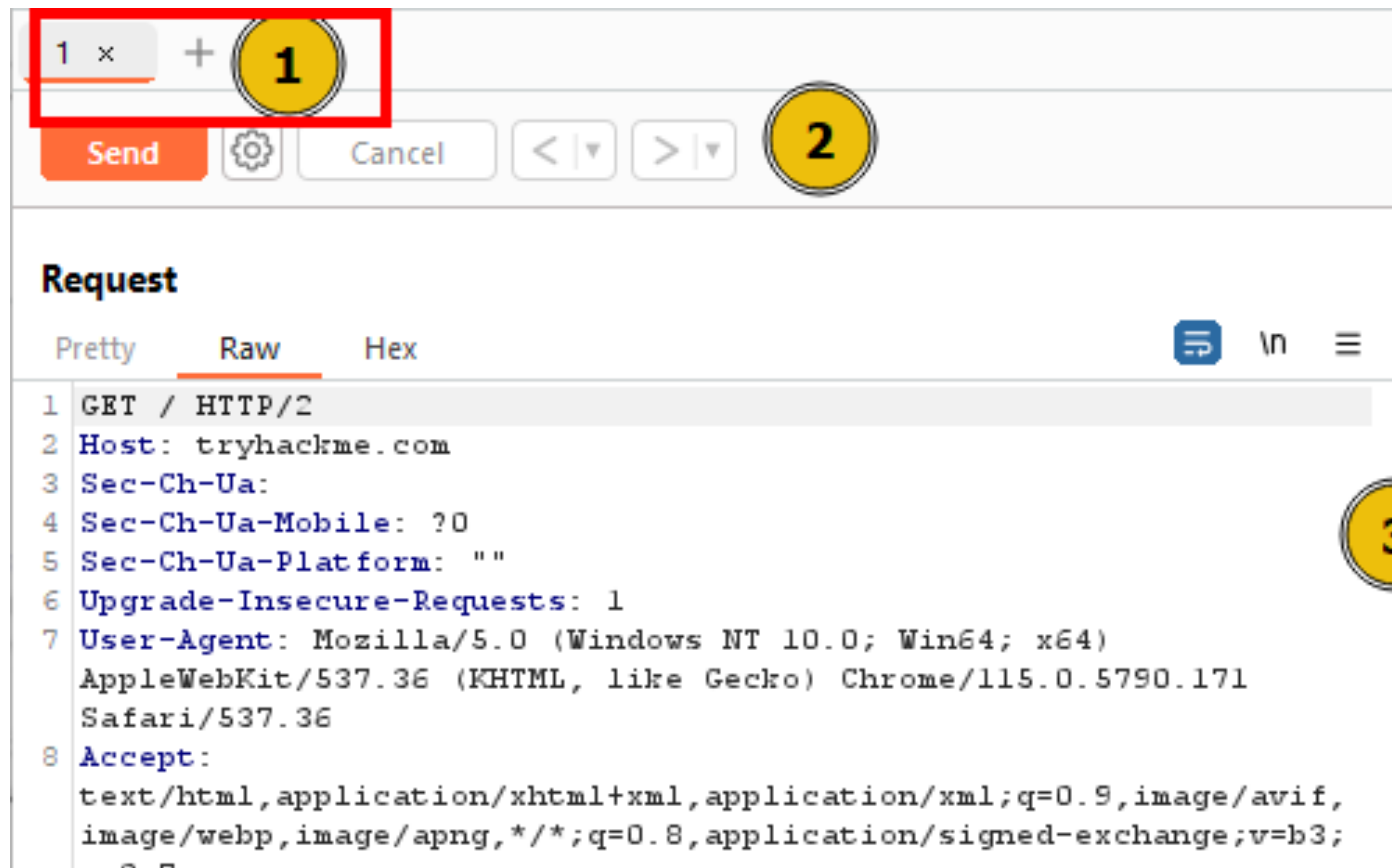
<https://tryhackme.com/r/room/burpsuitebasics>

T2 – What is Repeater?



This is what the Burp Repeater window typically looks like.

T2 – What is Repeater?



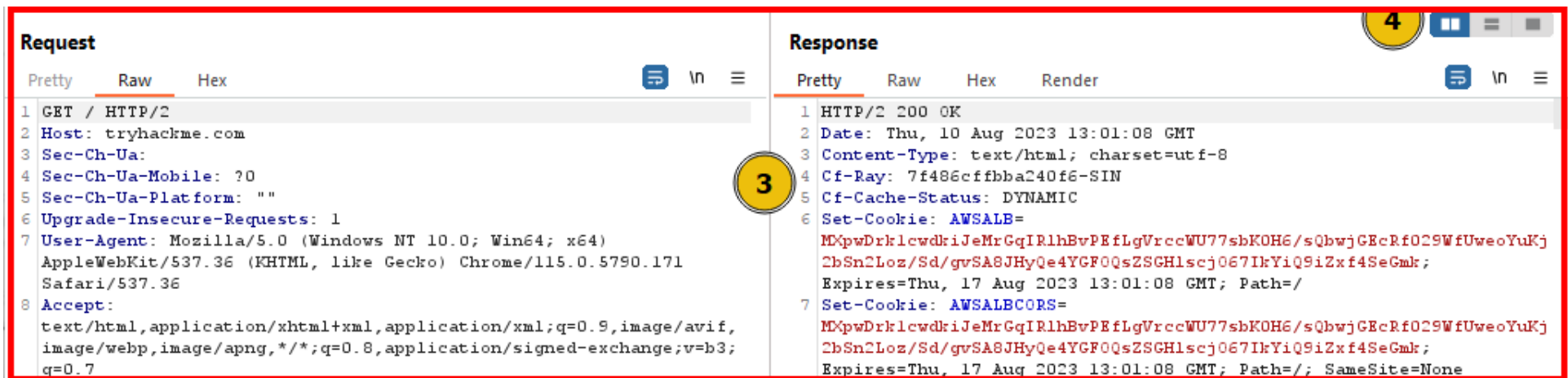
The Request List contains different tabs in the case there are multiple requests in the repeater.

T2 – What is Repeater?



The Request Controls allows sending, canceling and navigating of request history.

T2 – What is Repeater?



The screenshot displays the Repeater tool interface, which is used for sending and receiving HTTP requests and responses. The interface is divided into two main sections: 'Request' and 'Response'. The 'Request' section on the left shows a GET request to 'tryhackme.com' with various headers and an 'Accept' field. The 'Response' section on the right shows the corresponding HTTP 200 OK response, including headers like 'Date', 'Content-Type', 'Cf-Ray', 'Cf-Cache-Status', and 'Set-Cookie'. The 'Set-Cookie' field contains two cookies: 'AWSALB=' and 'AWSALBCORS='.

Request

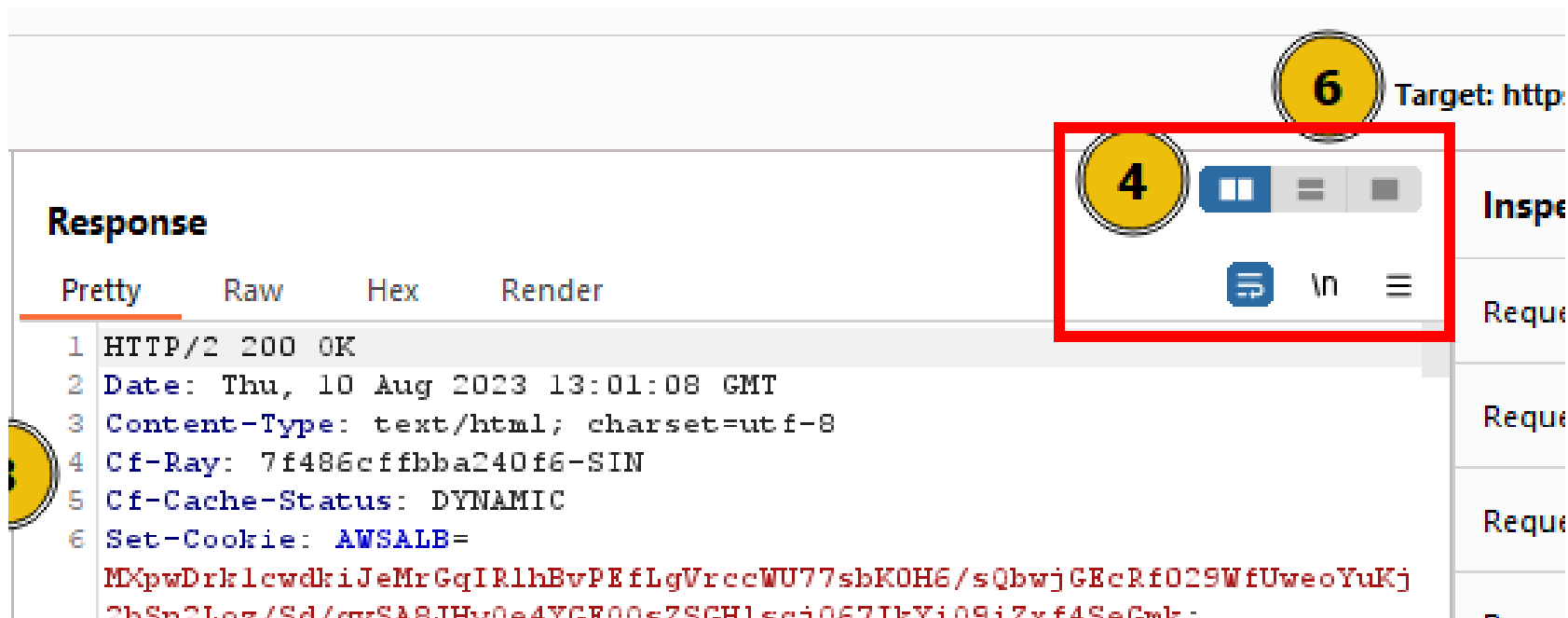
```
1 GET / HTTP/2
2 Host: tryhackme.com
3 Sec-Ch-Ua:
4 Sec-Ch-Ua-Mobile: ?0
5 Sec-Ch-Ua-Platform: ""
6 Upgrade-Insecure-Requests: 1
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.5790.171
  Safari/537.36
8 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,
  image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;
  q=0.7
```

Response

```
1 HTTP/2 200 OK
2 Date: Thu, 10 Aug 2023 13:01:08 GMT
3 Content-Type: text/html; charset=utf-8
4 Cf-Ray: 7f486cffbba240f6-SIN
5 Cf-Cache-Status: DYNAMIC
6 Set-Cookie: AWSALB=
  MXpwDrklcWdriJeMrCqIRlhBvPEfLgVrccWU77sbKOH6/sQbwjGEcRf029WfUweoYuKj
  2bSn2Loz/Sd/gvSA8JHyQe4YGF0QsZSGHlscj067IkYiQ9iZxf4SeGmk;
  Expires=Thu, 17 Aug 2023 13:01:08 GMT; Path=/
7 Set-Cookie: AWSALBCORS=
  MXpwDrklcWdriJeMrCqIRlhBvPEfLgVrccWU77sbKOH6/sQbwjGEcRf029WfUweoYuKj
  2bSn2Loz/Sd/gvSA8JHyQe4YGF0QsZSGHlscj067IkYiQ9iZxf4SeGmk;
  Expires=Thu, 17 Aug 2023 13:01:08 GMT; Path=/; SameSite=None
```

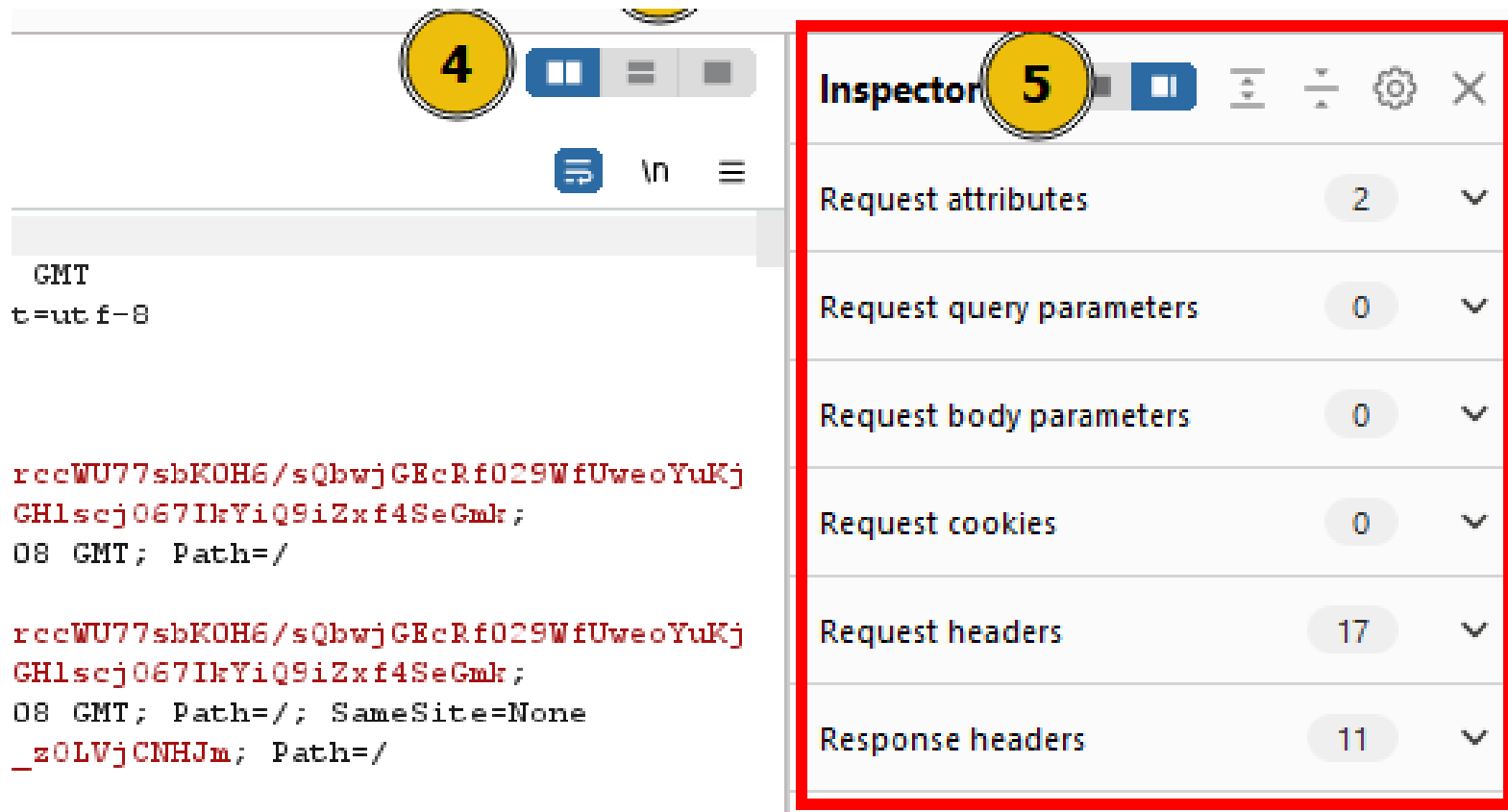
The Request and Response View displays request / response data, and allows modification.

T2 – What is Repeater?



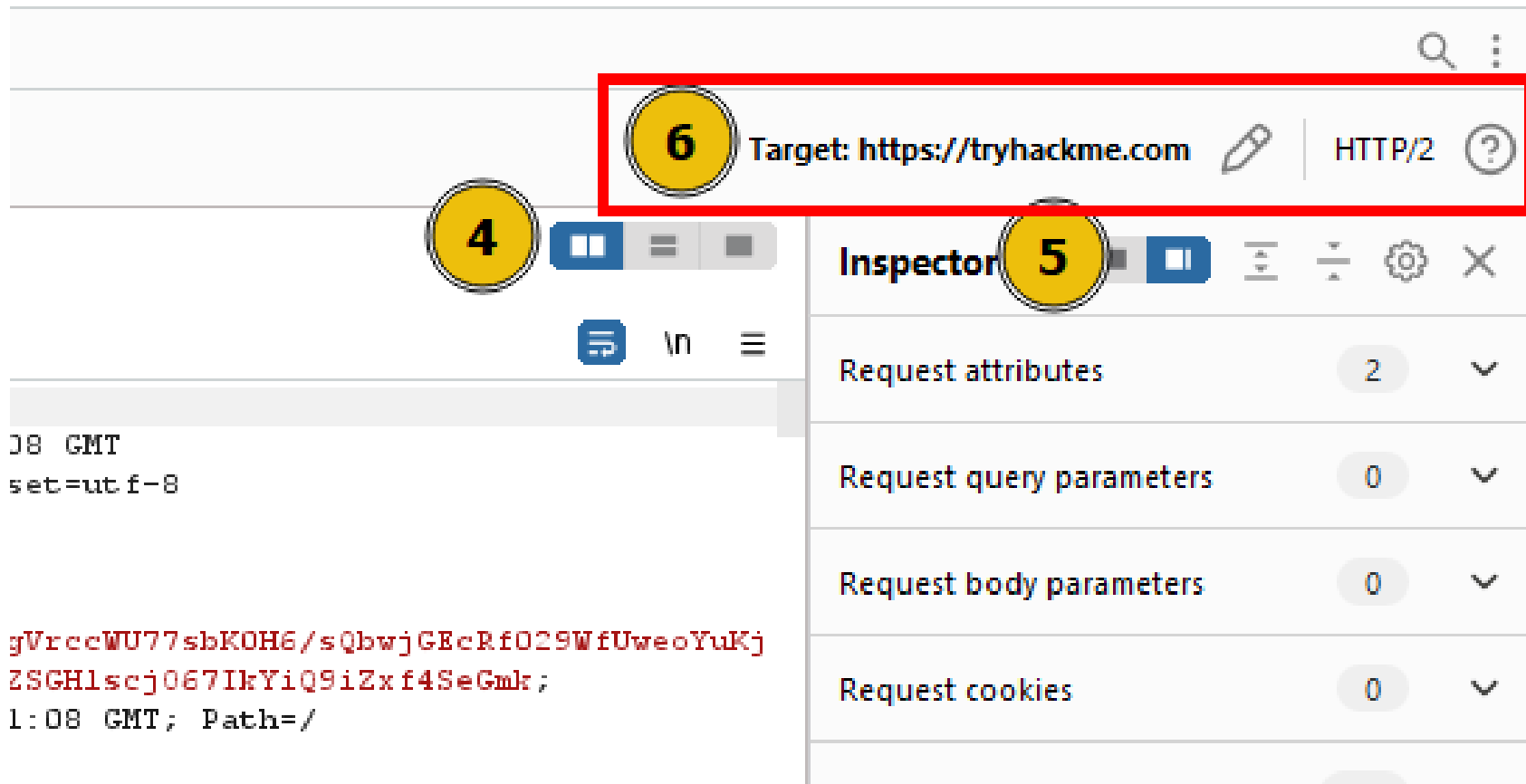
The Layout Options let us customize the Response / Response views.

T2 – What is Repeater?



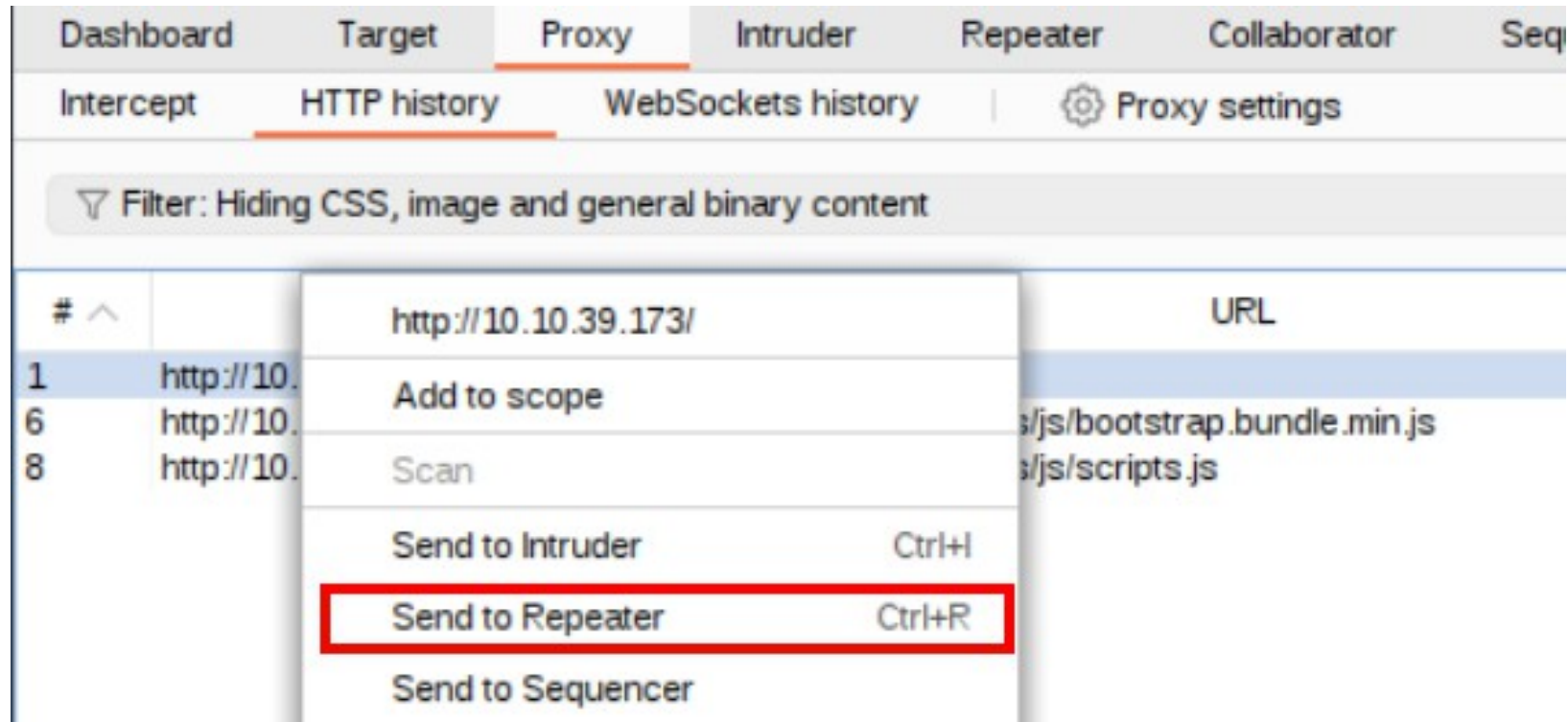
The Inspector allows us to analyze and modify requests separate from the rest of the body.

T2 – What is Repeater?



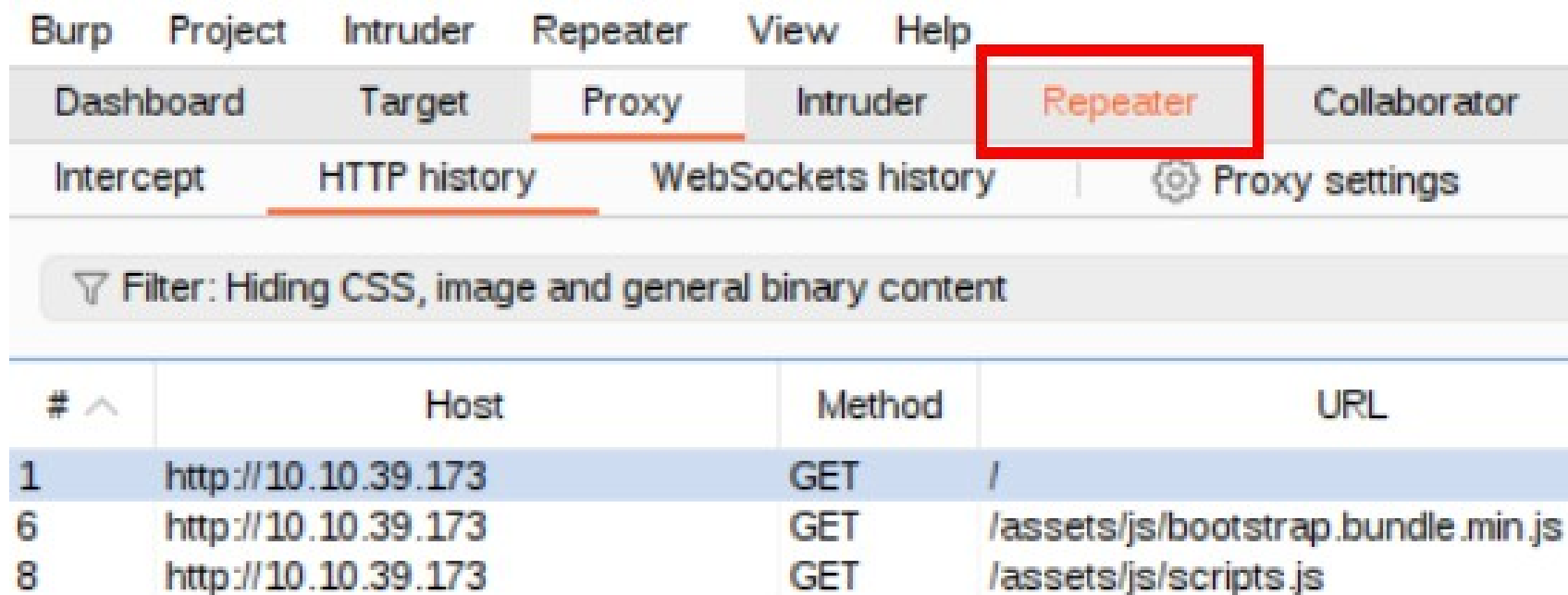
The Target field specifies which IP address or domain to send the requests to.

T3 – Basic Usage



You can send a request to the Repeater by right-clicking on the request or request window, then selecting the Send to Repeater option.

T3 – Basic Usage

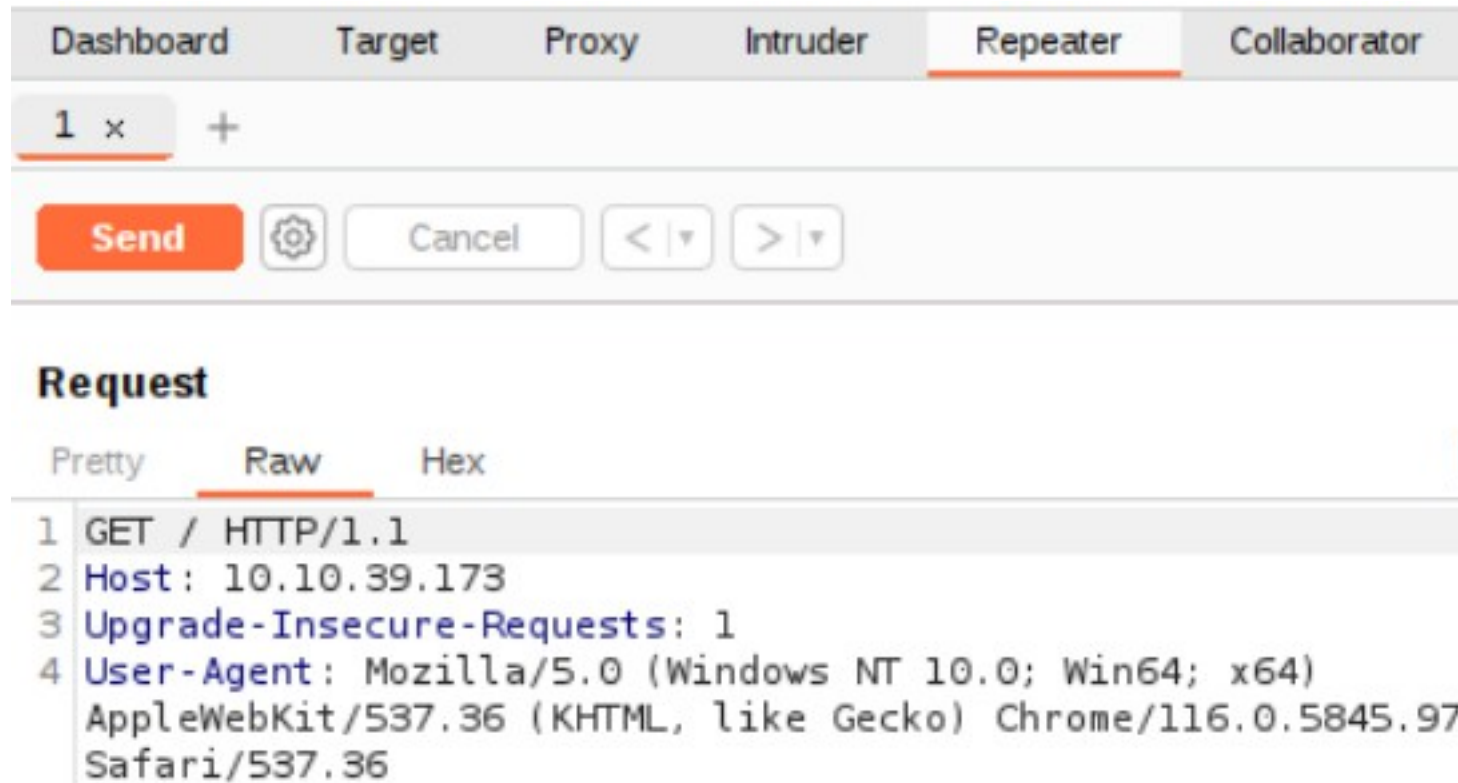


The screenshot shows the Burp Suite application window. The top menu bar includes 'Burp', 'Project', 'Intruder', 'Repeater', 'View', and 'Help'. Below this is a secondary menu bar with 'Dashboard', 'Target', 'Proxy', 'Intruder', 'Repeater' (highlighted in orange and enclosed in a red box), and 'Collaborator'. A third row of tabs includes 'Intercept', 'HTTP history' (highlighted with an orange underline), 'WebSockets history', and 'Proxy settings' (with a gear icon). Below these tabs is a filter bar that reads 'Filter: Hiding CSS, image and general binary content'. At the bottom is a table with four columns: '# ^', 'Host', 'Method', and 'URL'.

# ^	Host	Method	URL
1	http://10.10.39.173	GET	/
6	http://10.10.39.173	GET	/assets/js/bootstrap.bundle.min.js
8	http://10.10.39.173	GET	/assets/js/scripts.js

You'll see the Repeater tab turn orange, which indicates the request was sent to the Repeater.

T3 – Basic Usage



After clicking on the Repeater tab, you'll see the request.

T4 – Message Analysis Toolbar



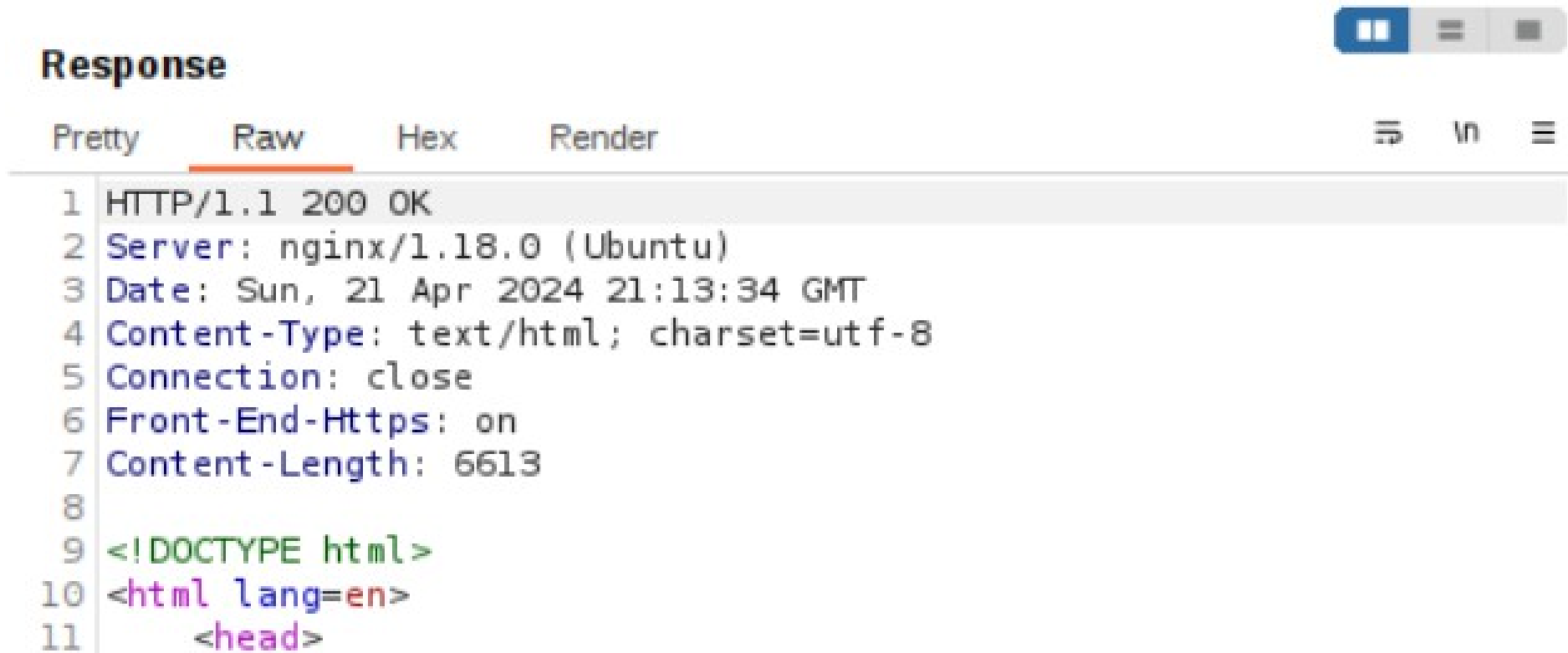
The Message Analysis toolbar allows the user to adjust the Response window output.

T4 – Message Analysis Toolbar



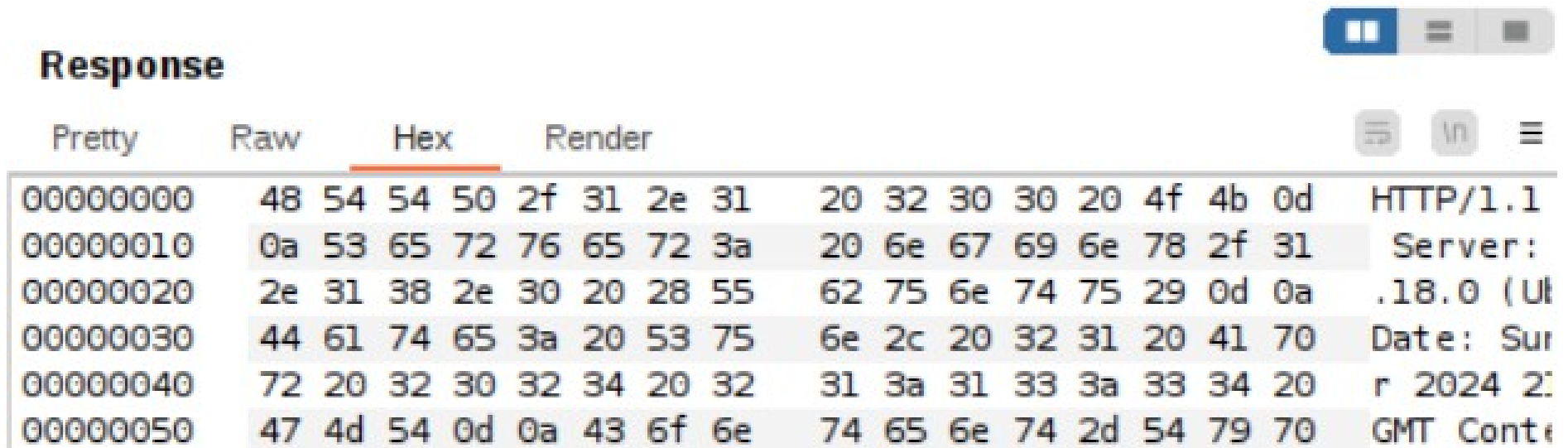
The Pretty option (which is set by default) applies formatting to improve readability.

T4 – Message Analysis Toolbar



The Raw option returns the response without any adjustment to its formatting.

T4 – Message Analysis Toolbar

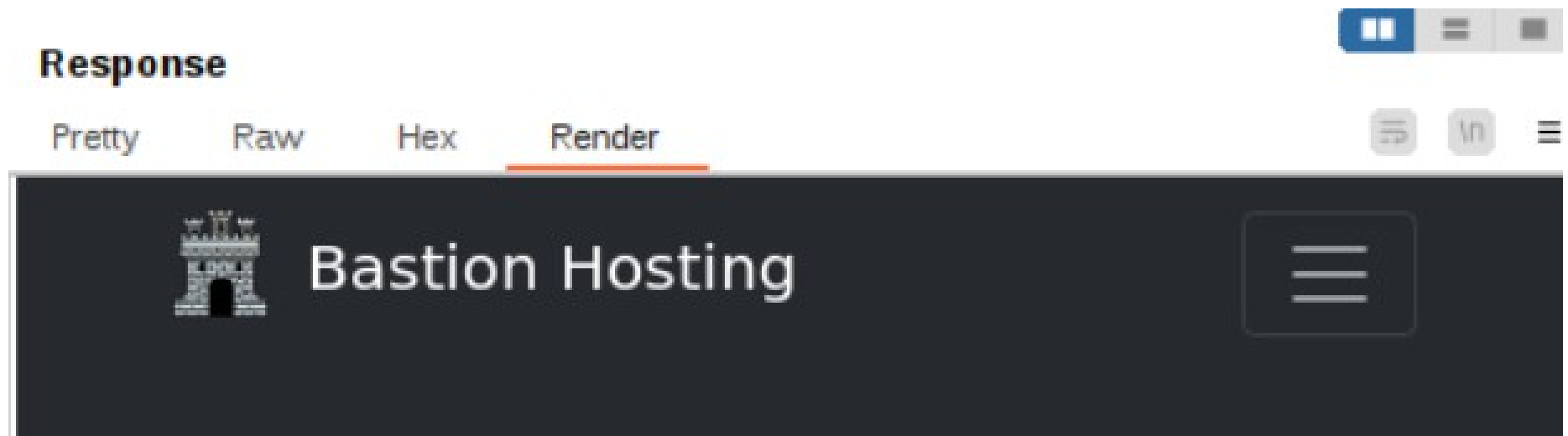


The screenshot displays the T4 Message Analysis Toolbar interface. At the top right, there are three icons: a blue square with two white vertical bars, a grey square with two horizontal bars, and a grey square with a single horizontal bar. Below these, the word "Response" is written in bold. To the right of "Response" are three more icons: a grey square with three horizontal bars, a grey square with the text "ln", and a grey square with three horizontal bars. The main area of the toolbar is a table with four columns: "Pretty", "Raw", "Hex", and "Render". The "Hex" column is currently selected, indicated by an orange underline. The table contains six rows of data, each representing a segment of the response. The first row shows the status line "HTTP/1.1". The second row shows the "Server:" header. The third row shows the "Date:" header. The fourth row shows the "Content-Type:" header. The fifth row shows the "Content-Length:" header. The sixth row shows the "Connection:" header. The "Hex" column displays the hexadecimal representation of the response data, and the "Render" column displays the ASCII output.

Pretty	Raw	Hex	Render
00000000	48 54 54 50 2f 31 2e 31	20 32 30 30 20 4f 4b 0d	HTTP/1.1
00000010	0a 53 65 72 76 65 72 3a	20 6e 67 69 6e 78 2f 31	Server:
00000020	2e 31 38 2e 30 20 28 55	62 75 6e 74 75 29 0d 0a	.18.0 (Ul
00000030	44 61 74 65 3a 20 53 75	6e 2c 20 32 31 20 41 70	Date: Sur
00000040	72 20 32 30 32 34 20 32	31 3a 31 33 3a 33 34 20	r 2024 2:
00000050	47 4d 54 0d 0a 43 6f 6e	74 65 6e 74 2d 54 79 70	GMT Cont

The Hex option returns the response in its hexadecimal rendering, with the ASCII output shown on the right-hand side.







T4 – Message Analysis Toolbar



And the Render option returns output that resembles how the webpage would be returned in a web browser.

T5 – Inspector

The Inspector allows users to change various request parameters when re-sending requests

Inspector      		
Request attributes	2	▼
Request query parameters	1	▼
Request body parameters	0	▼
Request cookies	2	▼
Request headers	19	▼
Response headers	3	▼

T8 – Extra-mile Challenge

Request

Pretty

Raw

Hex



ln

```
1 GET /about/id HTTP/1.1
2 Host: 10.10.33.238
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.97
  Safari/537.36
```

For the extra-mile challenge, we need to use the Repeater to perform a SQL injection attack on the app's **/about/ID** endpoint.

T8 – Extra-mile Challenge

Request

Pretty

Raw

Hex



ln

```
1 GET /about/id HTTP/1.1
2 Host: 10.10.33.238
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.97
  Safari/537.36
```

First we need to confirm the SQL injection vulnerability by causing an error.

T8 – Extra-mile Challenge

Invalid statement:

```
SELECT firstName,  
lastName, pfpLink, role,  
bio FROM people WHERE id  
= 2'
```

Next, we need to determine how many columns the original query returns.

T8 – Extra-mile Challenge



Then determine the name of the current database.

T8 – Extra-mile Challenge



Next, enumerate all the tables in the current database.

T8 – Extra-mile Challenge

1 2

4

id,firstName,lastName,pfpLink,role,shortRole,bio,notes

Then retrieve all columns in that table

T8 – Extra-mile Challenge

1 2

4

id,firstName,lastName,pfpLink,role,shortRole,bio,notes

Then retrieve all columns in that table

T8 – Extra-mile Challenge

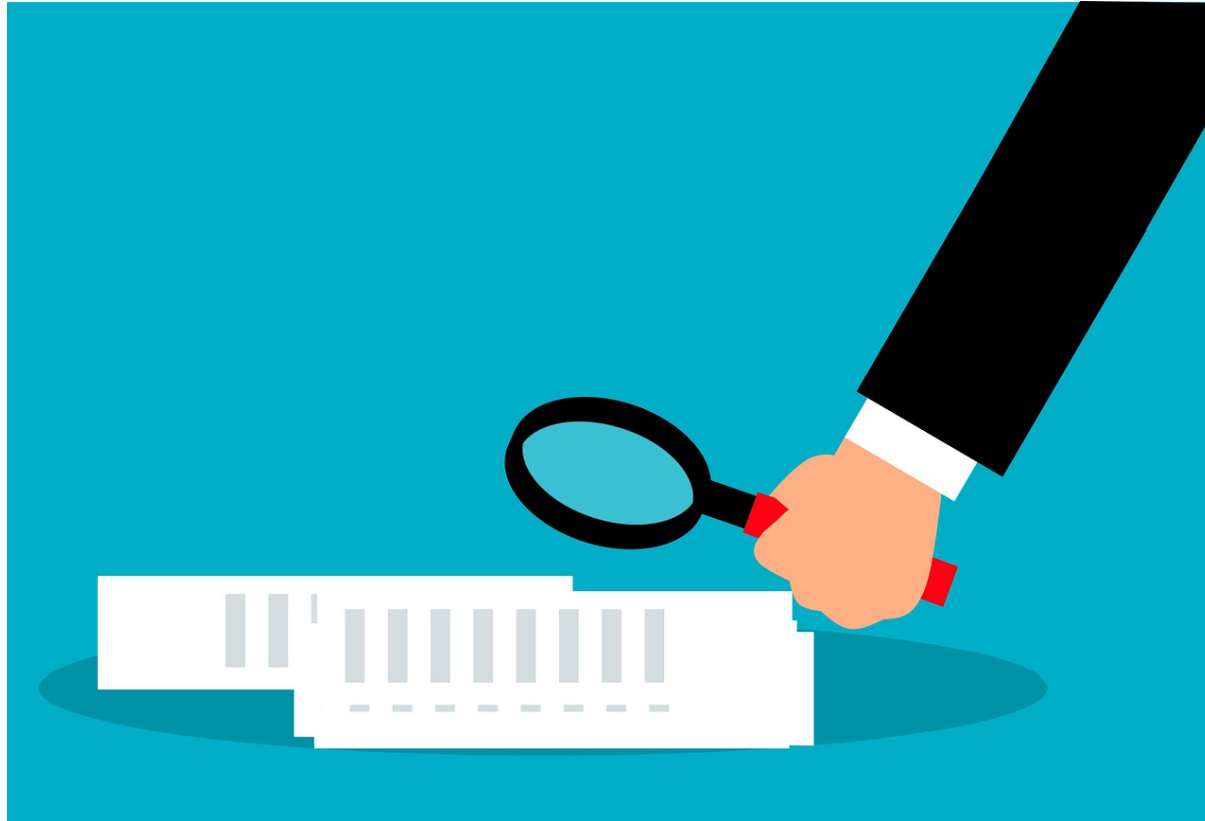
1 2

4

id,firstName,lastName,pfpLink,role,shortRole,bio,notes

Then retrieve all entries in those columns

Summary



Let's review the web exploitation concepts we learned in this workshop:

Burp Repeater



The Burp Repeater allows users to re-send web requests with modified contents.

Burp Repeater



We used the Repeater allows users to re-send web requests with modified contents, becoming more familiar with the tool in the process

What's Next?

This is the end of the HackerFrogs AfterSchool web app hacking workshops, and now that we've practiced Burp Suite, we should be able to learn about new web app hacking concepts on our own.



Extra Credit

Looking for more study material on this workshop's topics?

See this video's description for links to supplemental documents and exercises!



Until Next Time, HackerFrogs!

