Burp Suite: Repeater

Learn how to use Repeater to duplicate requests in Burp Suite.

Task 2 What is Repeater?

Question	Answer
Which sections gives us a more intuitive control over our requests?	Inspector

Task 3 Basic Usage

Question	Answer
Which view will populate when sending a request from the Proxy module to Repeater?	Request

Task 4 Message Analysis Toolbar

Question	Answer
Which option allows us to visualize the page as it would appear in a web browser?	Render

Task 5 Inspector

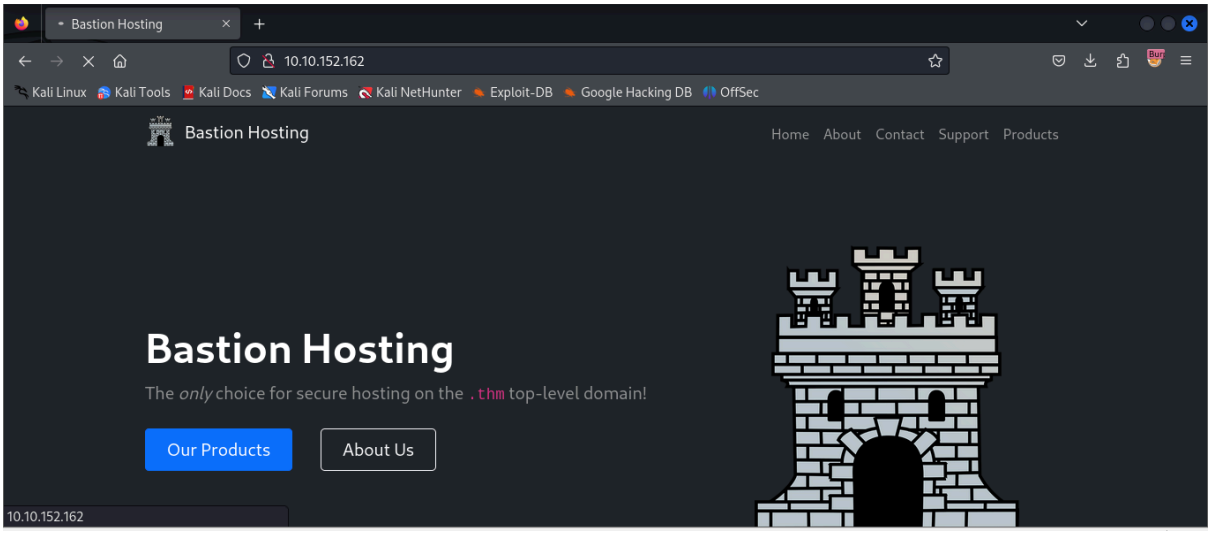
Question	Answer
Which section in Inspector is specific to POST requests?	Body Parameters

Task 6 Practical Example

What is the flag you receive?

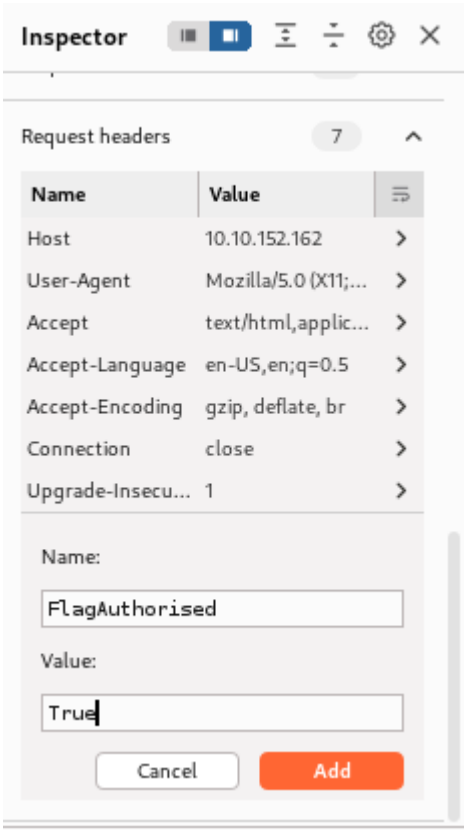
Answer: **THM{Yzg2MWI2ZDhlYzdlNGFiZTUzZTIzMzVi}**

➔ I visited the target web app on my browser

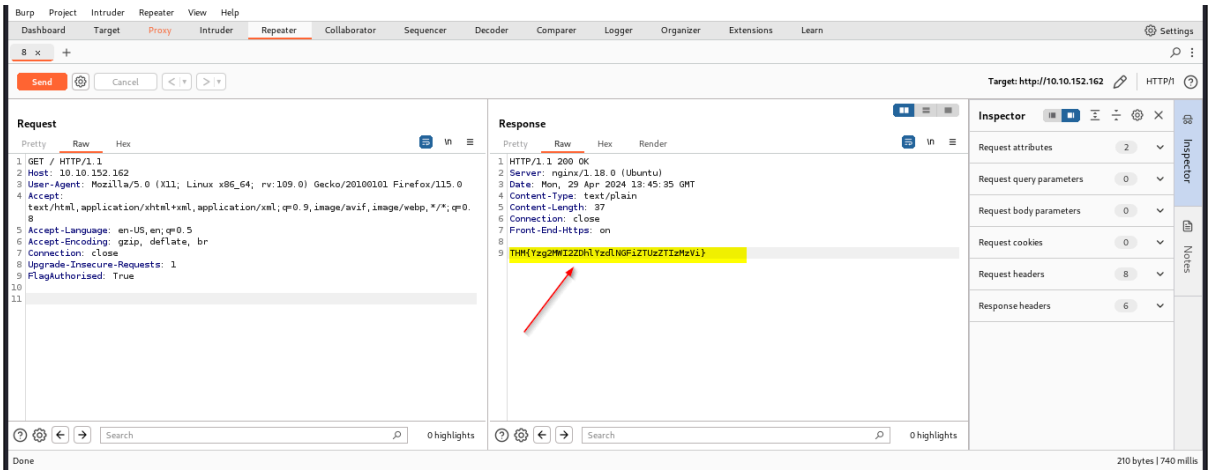


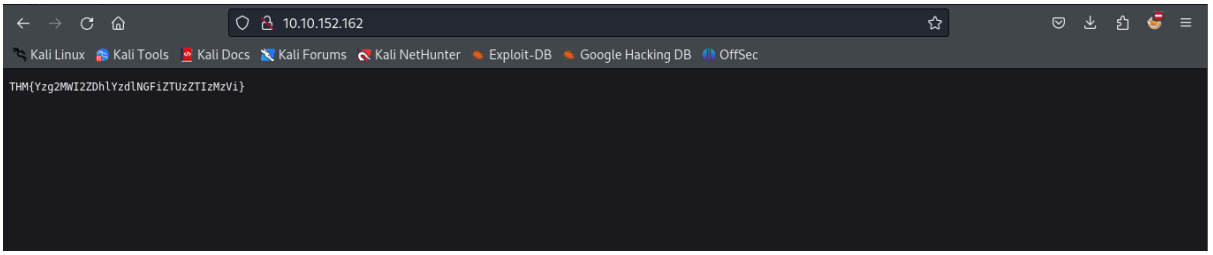
➔ I switched on my proxy and intercept, captured a request to http://10.10.152.162/ in the Proxy module

➔ Then, I added a header called FlagAuthorised and set it to have a value of True



➔ I sent the request to the Repeater and got my flag.

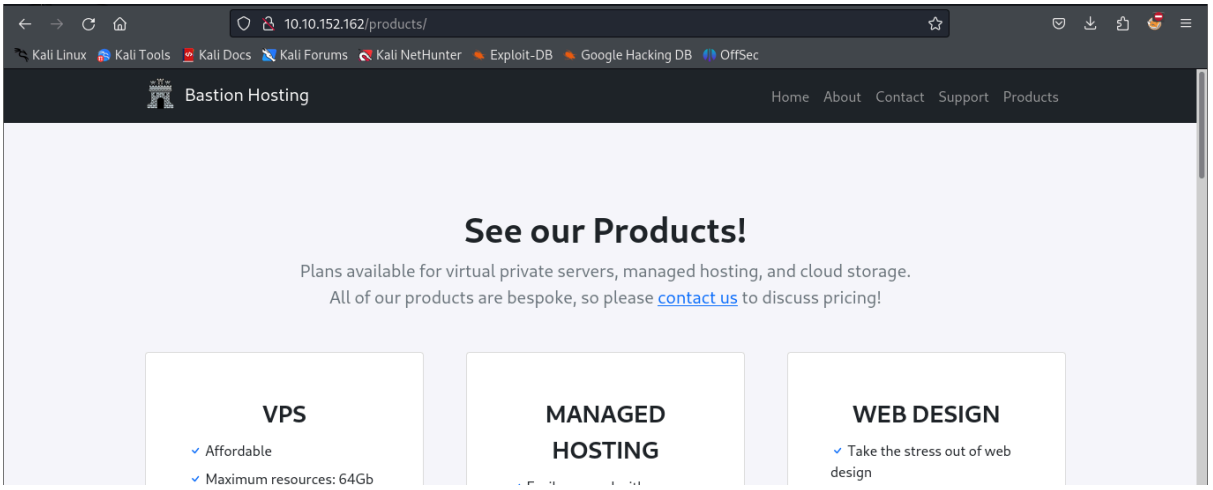




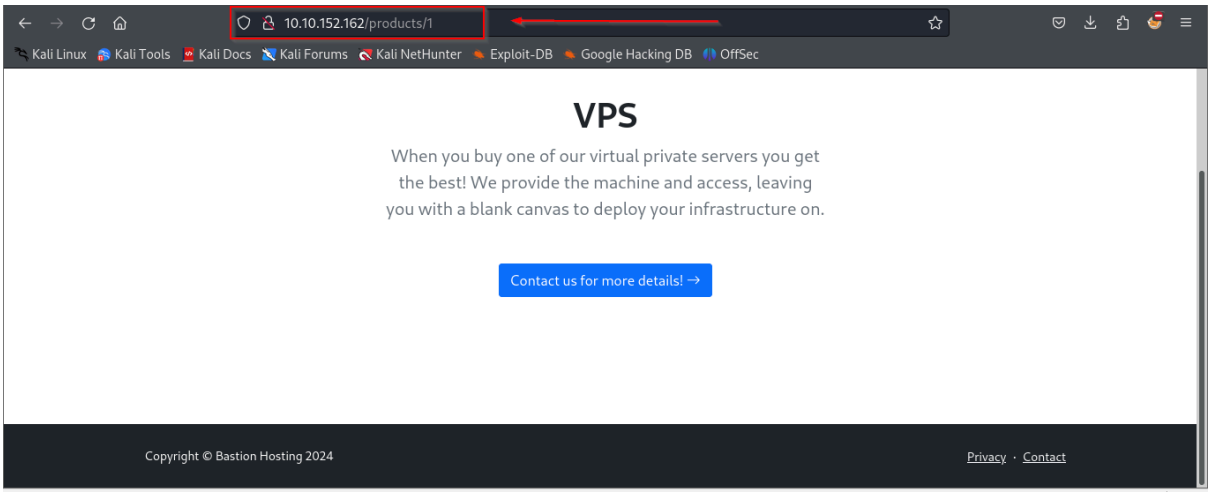
Task 7 Challenge

Enable intercept again and capture a request to one of the numeric products endpoints in the Proxy module, then forward it to Repeater.

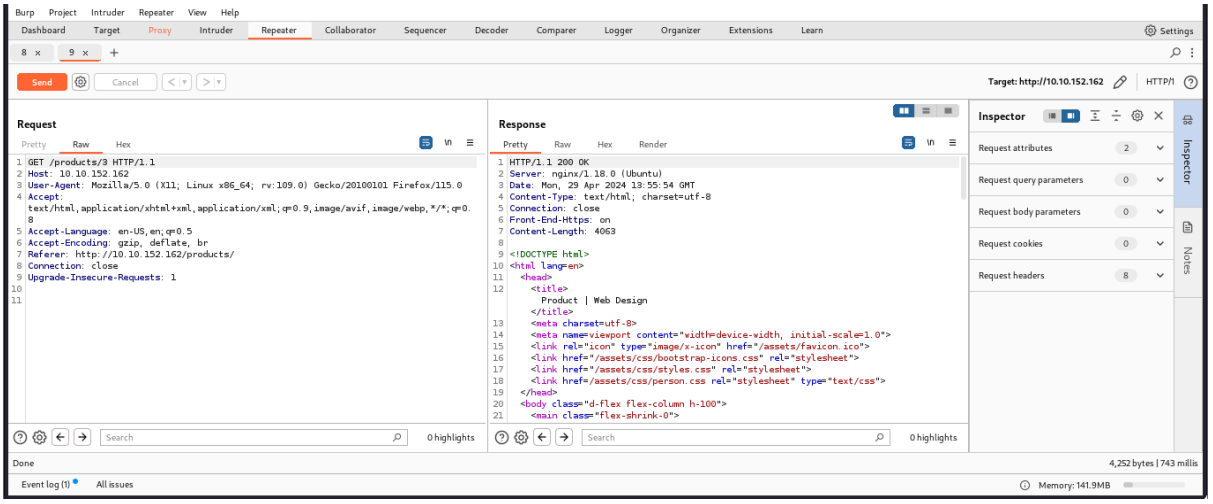
➔ I made sure the intercept is disabled in the Proxy module and navigated to http://10.10.152.162/products/.



➔ Then, I clicked on some of the See More links and i saw that i am redirected to a numeric endpoint.



➔ I enabled intercept again and captured a request to numeric products 3 endpoint in the Proxy module, then forwarded it to Repeater.

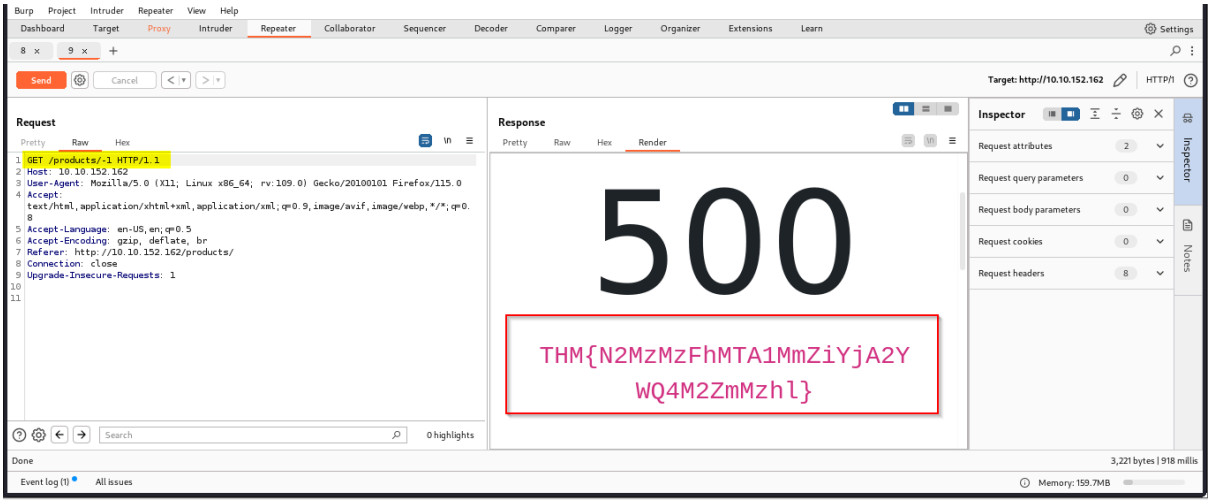


See if you can get the server to error out with a "500 Internal Server Error" code by changing the number at the end of the request to extreme inputs.

What is the flag you receive when you cause a 500 error in the endpoint?

Answer: **THM{N2MzMzFhMTA1MmZiYjA2YWQ4M2ZmMzhl}**

➔ I changed the number at the end of the request to -1 and got the flag under render tab of the response



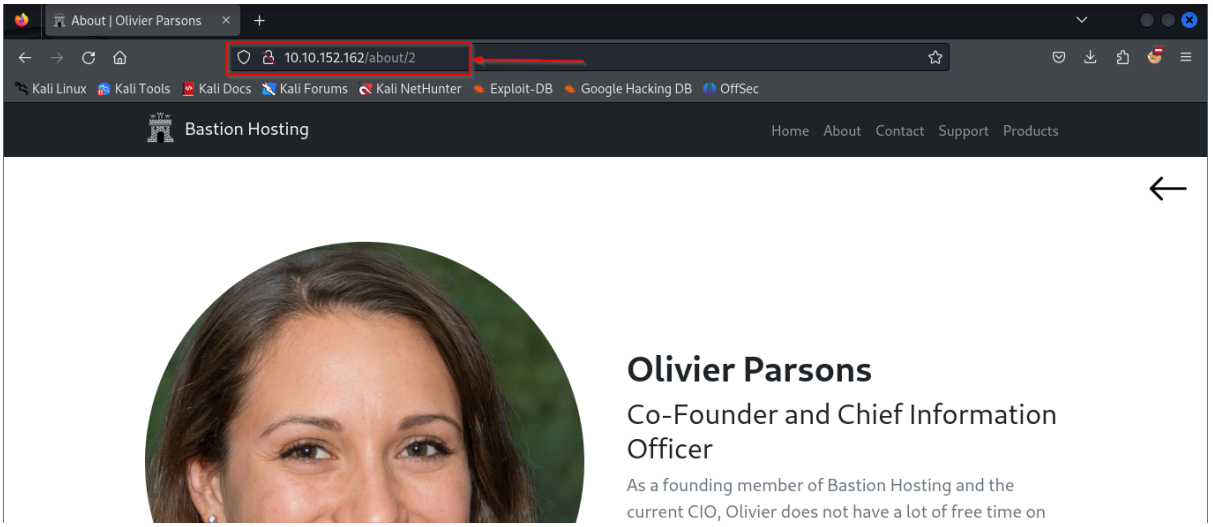
Task 8 Extra-mile Challenge

Exploit the union SQL injection vulnerability in the site.

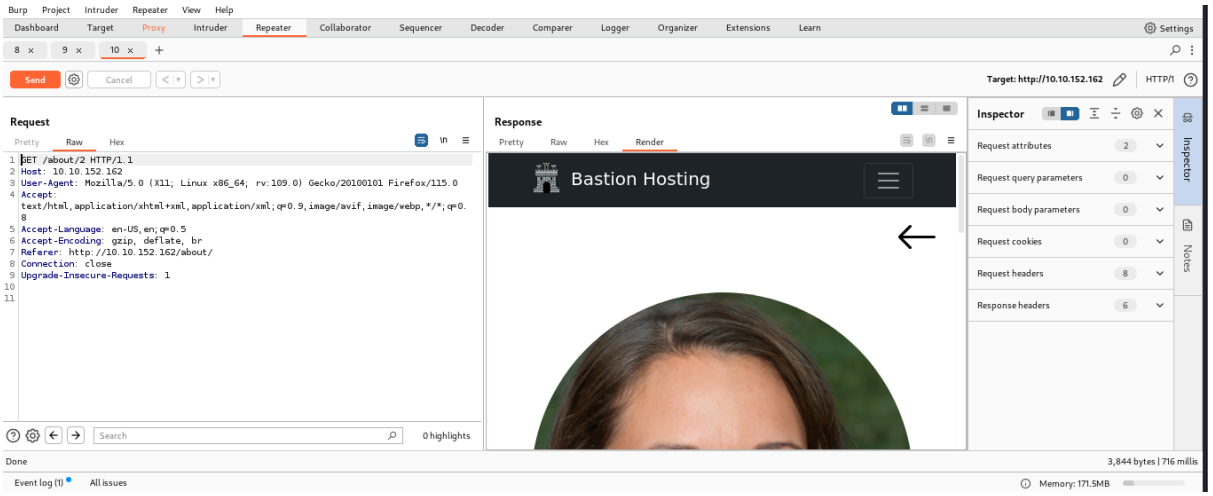
What is the flag?

Answer: THM{ZGE3OTUyZGMyMzkwNjJmZjg3Mzk1NjJh}

➔ I captured a request to http://10.10.152.162/about/2 in the Burp Proxy.

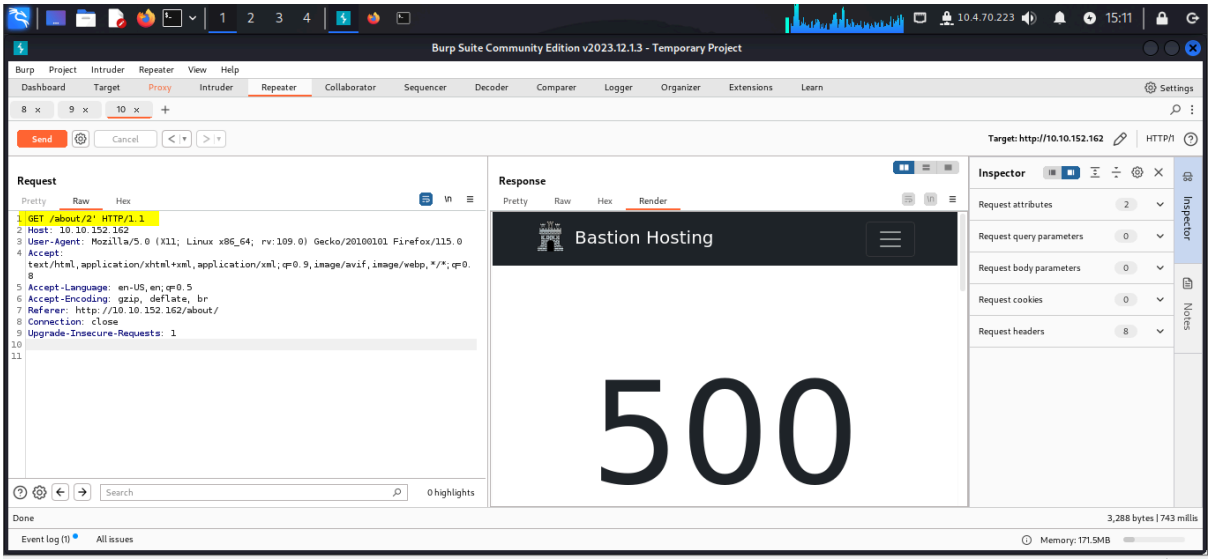


➔ Then, i sent it to the Repeater.

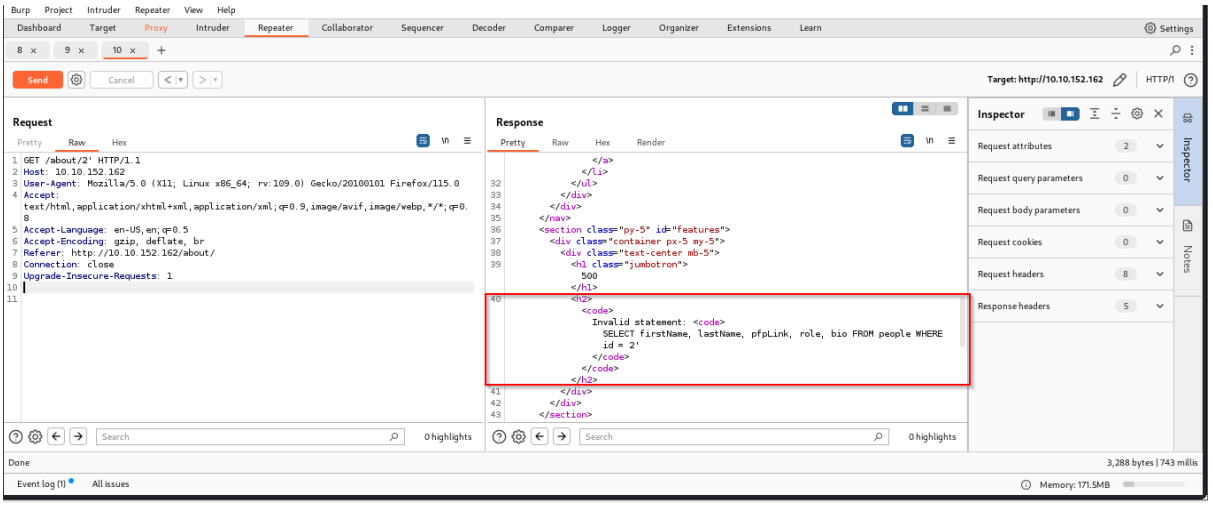


➔ To confirm that a vulnerability exists, I added a single apostrophe (‘) to cause the server to error, this will show the presence of a simple SQLi.

➔ I added the apostrophe after the "2" at the end of the path and sent the request



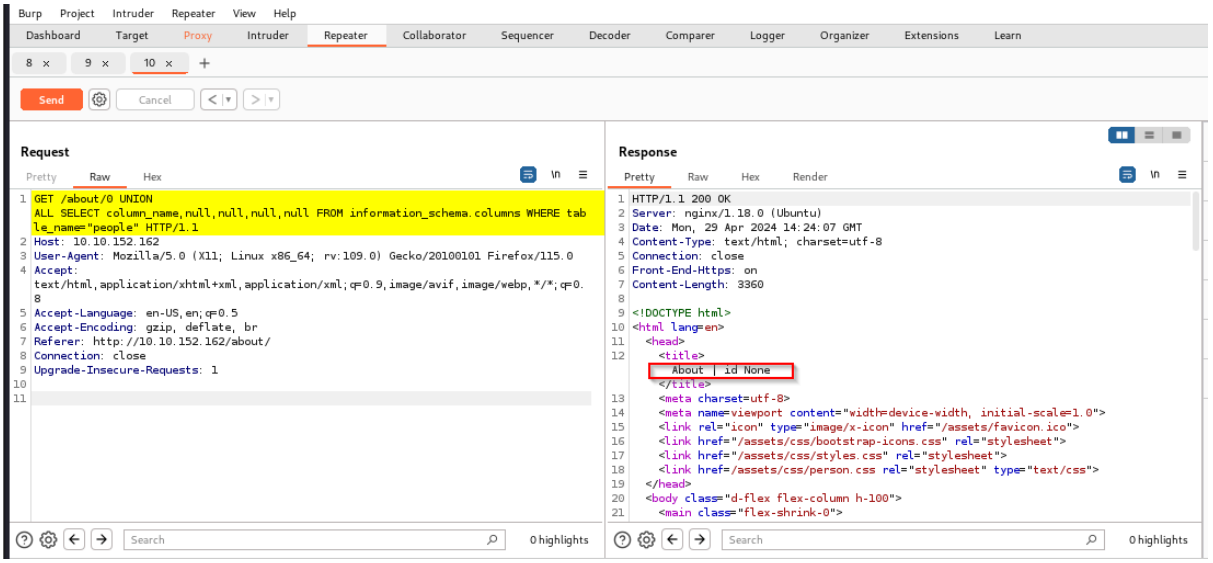
➔ I looked through the body of the server's response, around line 40. The server is telling us the query we tried to execute:



➔ This is an extremely useful error message that the server should not be sending.
➔ I used the payload below and sent it

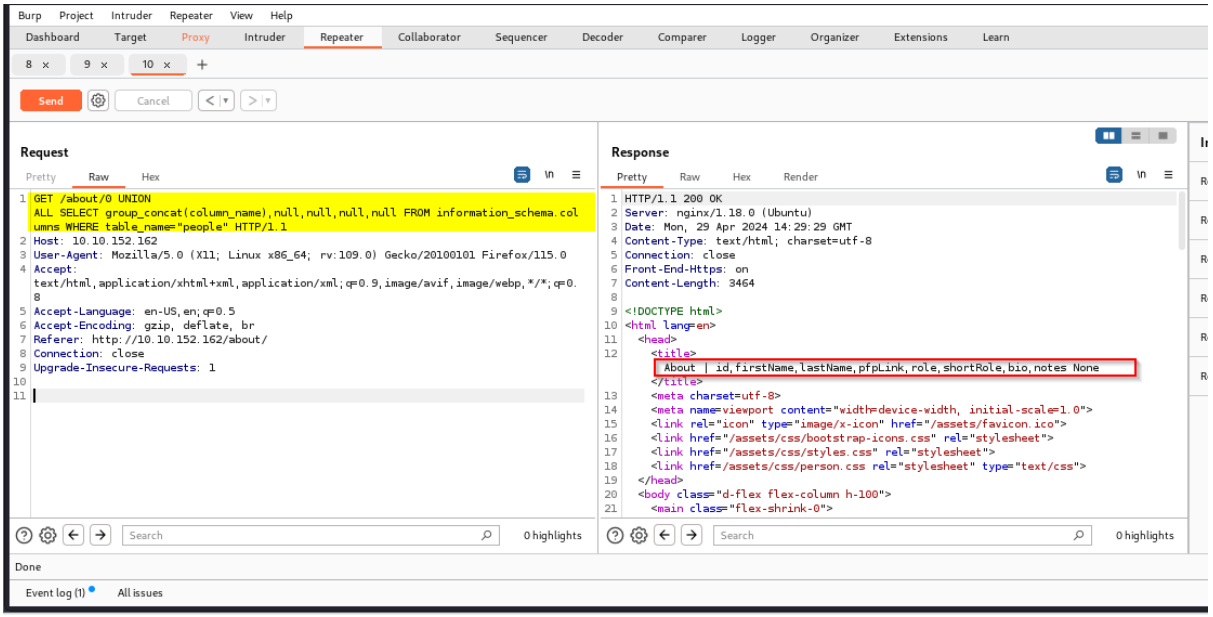
Payload: /about/0 UNION ALL SELECT column_name,null,null,null,null FROM information_schema.columns WHERE table_name="people"

➔ I see that the first column name (id) is none



➔ To see all of the matching items, i used another payload that includes the group_concat() function

Payload: /about/0 UNION ALL SELECT group_concat(column_name),null,null,null,null FROM information_schema.columns WHERE table_name="people"



➔ This means I have successfully identified eight columns in this table: id, firstName, lastName, pfpLink, role, shortRole, bio, and notes.

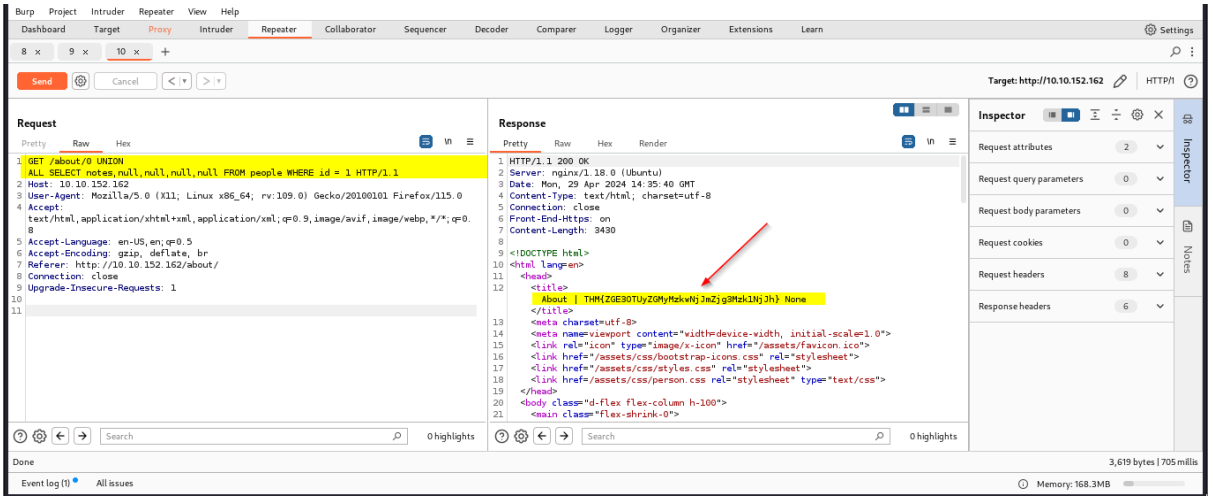
➔ Since our target column is notes, I used the payload

Payload: /about/0 UNION ALL SELECT notes,null,null,null,null FROM people WHERE id = 1

Where:

➔ The name of the table: people.
➔ The name of the target column: notes.
➔ The ID of the CEO is 1; this can be found simply by clicking on Jameson Wolfe's profile on the /about/ page and checking the ID in the URL.

➔ Then i get the flag



END!!!