CODEPATH*ORG

REPORT

SESSION MANAGEMENT

Mahmood Sakib

Broken Session Management:

Task: Complete a lesson without completing it.

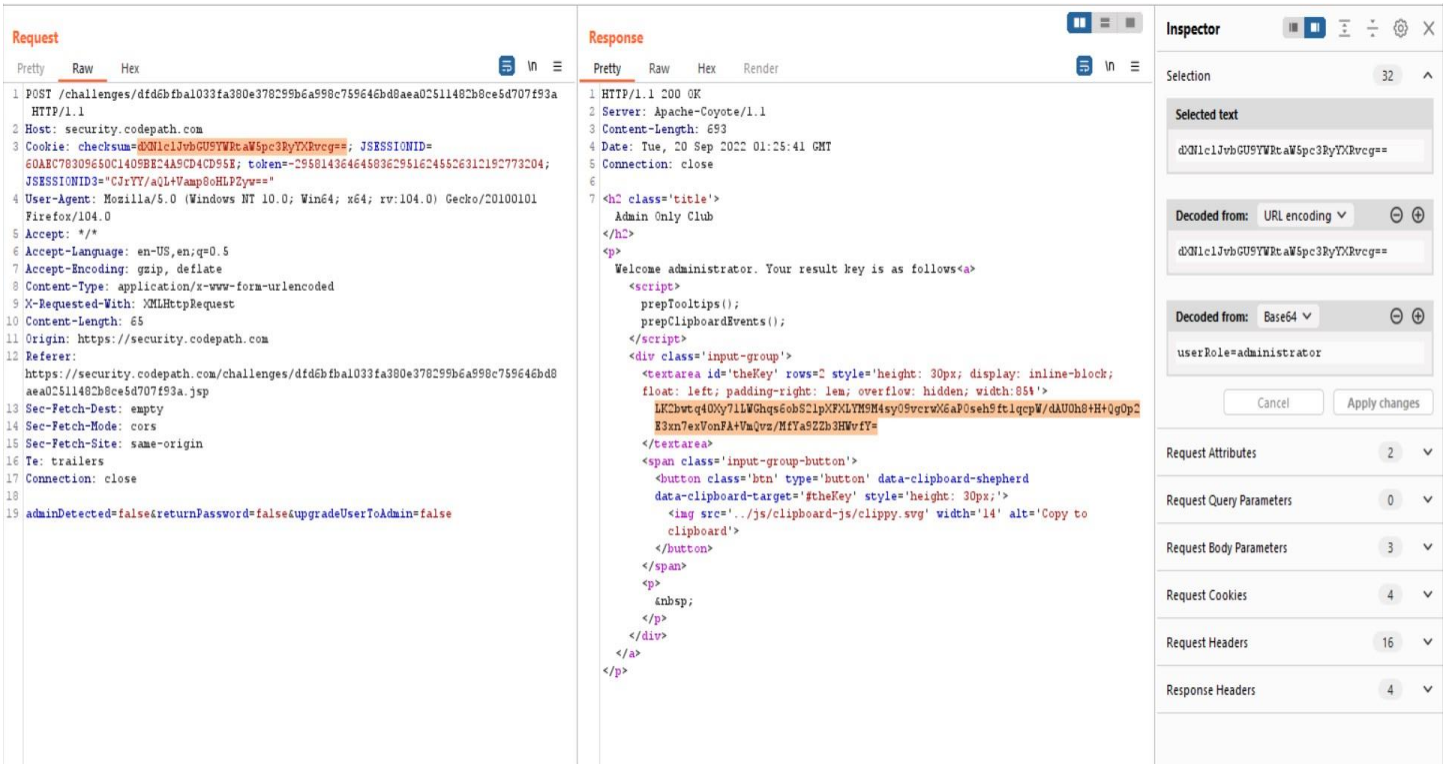
Running the website request with Burp I can see that, Cookie:lessonComplete=lessonNotComplete; To trick the server into thinking that I have already completed this lesson to retrieve the result key, I changed the value to Cookie:lessonComplete=lessonComplete . Which made it think that I have already completed the lesion and gave me the secret key!

Session Management 1:

Task: Gain admin privileges

Running the website with Burp suite, I can see that this website is using Cookie:checksum=dXNlclJvbGU9dXNlcg==; this checksum is using base64 encoding to hide a value. After decoding it, the value: userRole=user ;

To gain administrative privileges, I encoded the value: userRole=administrator with base64 and sent the request again to gain administrator privilege.



Session Management 2:

Task: Gain admin privileges

Only an admin of the following sub-application can retrieve the result key to this challenge.

Incorrect password for zoidberg22@shepherd.com

Username:

Password:

Sign In

Have you forgotten your password?

Reset Password

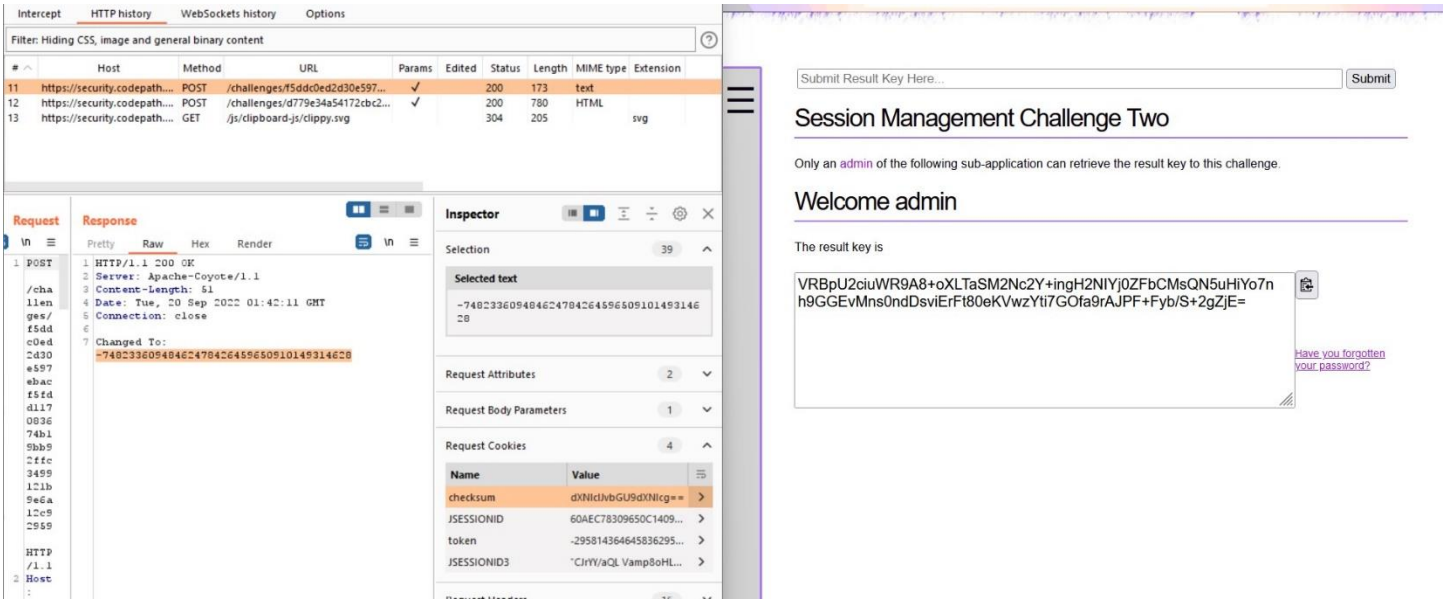
Please enter your email address. You will be sent an email with a new temporary password

zoidberg22@shepherd.(Reset Password

Password reset request sent.

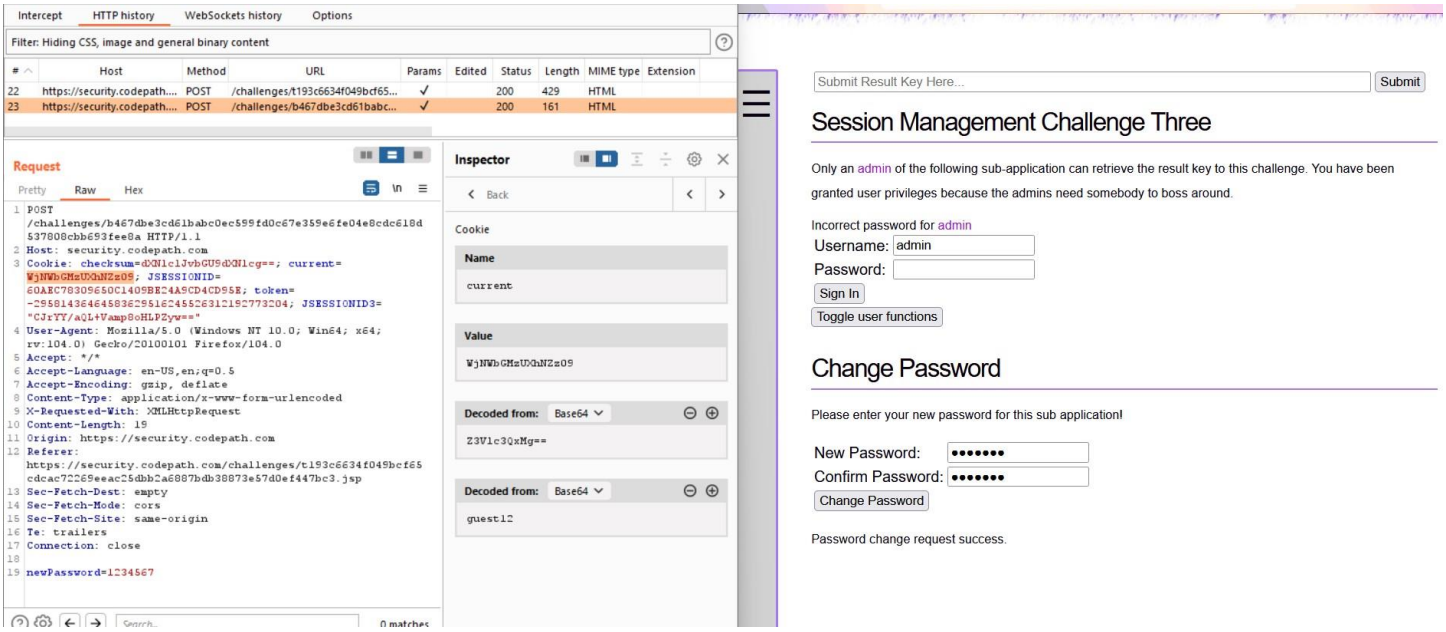
Using Burp Suite, after requesting password reset, I can see that the Response tab shows

"Changed To: -74823360948462478426459650910149314628" Which I assumed that the website assigned a new password and Burp was able to capture it. After using the given value in login section, I was able to successfully log in as an admin.



Session Management 3:

Task: Gain admin privileges



After requesting a password change for admin, I can see that the website assigned a new value to it's cookies. Which is current=WjNWbGMzUXhNZz09(this value is decoded twice with base64) = 'user12' At this point we can see that the website is resetting password for user12 not for admin. Therefore, I changed the current cookie value to 'admin' (after decoding it twice with base64) and were able to reset admin's password to '1234567' and gain access to the website