CODEPATH*ORG

REPORT

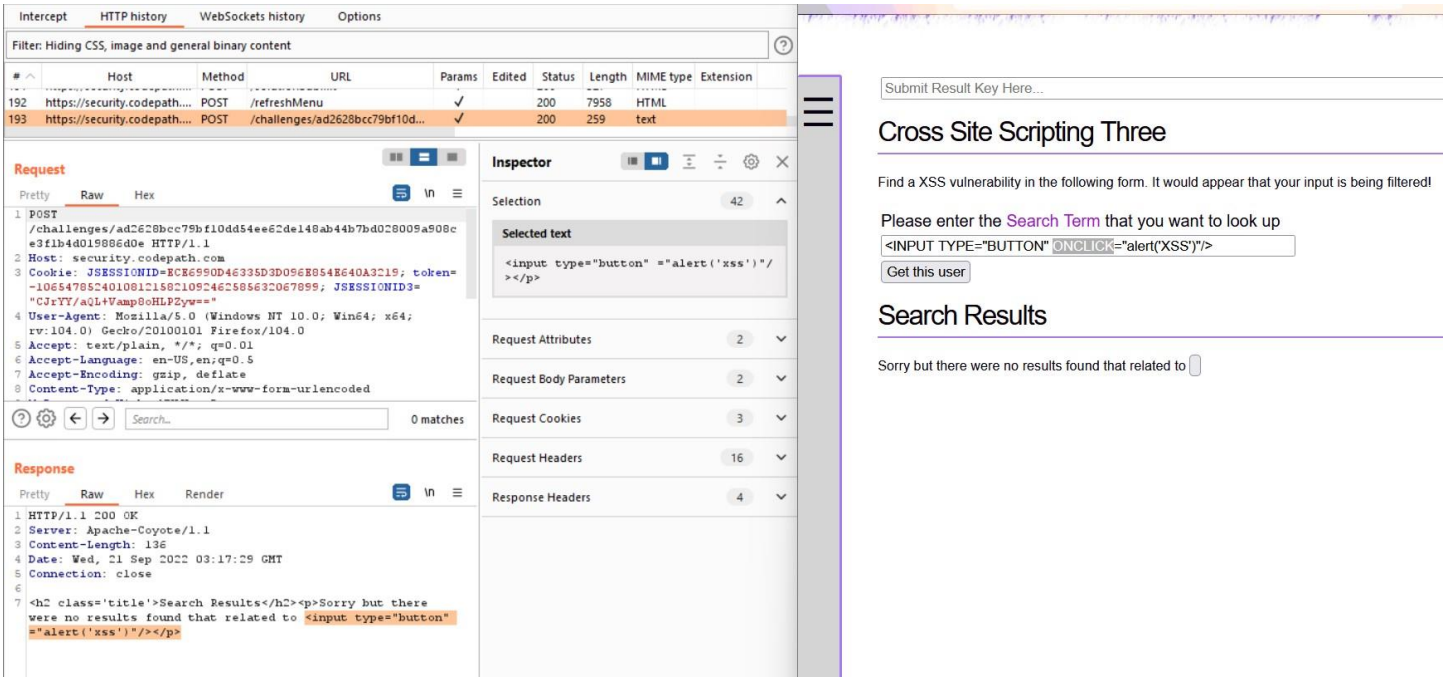
CROSS SITE SCRIPTING (XSS)

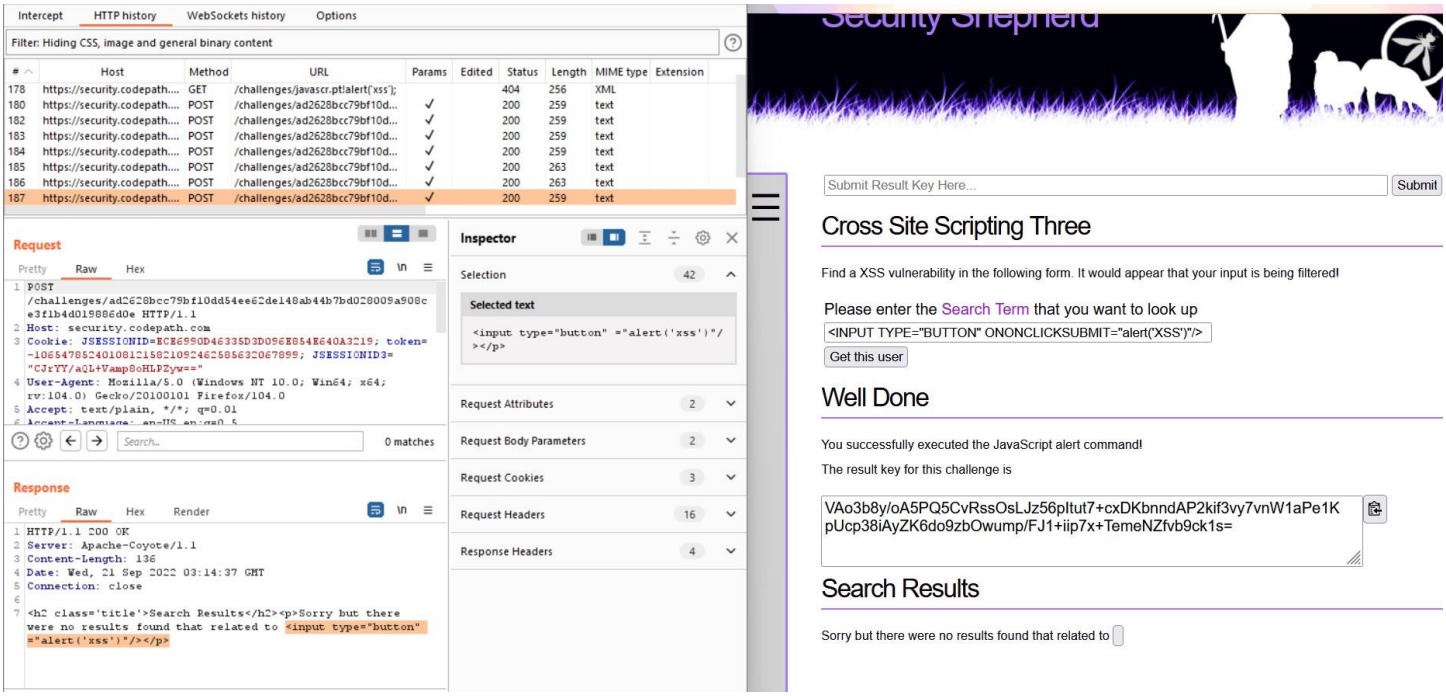
Mahmood Sakib

XSS 01:

Task: Find a XSS vulnerability.

Running the website request with Burp Suite and putting malicious code inside the form I can see that the website is filtering out the 'ONCLICK' part from the code. To escape from the filter, I used 'ONONCLICKSUBMIT' and got the flag!





XSS 02:

Task: Find a XSS vulnerability:

Running the website request with Burp Suite and putting malicious code inside the form I can see that the website is filtering out the ‘ “ ‘ part from the malicious code. To escape from the filter, I used ‘ “” ’ and got the flag!