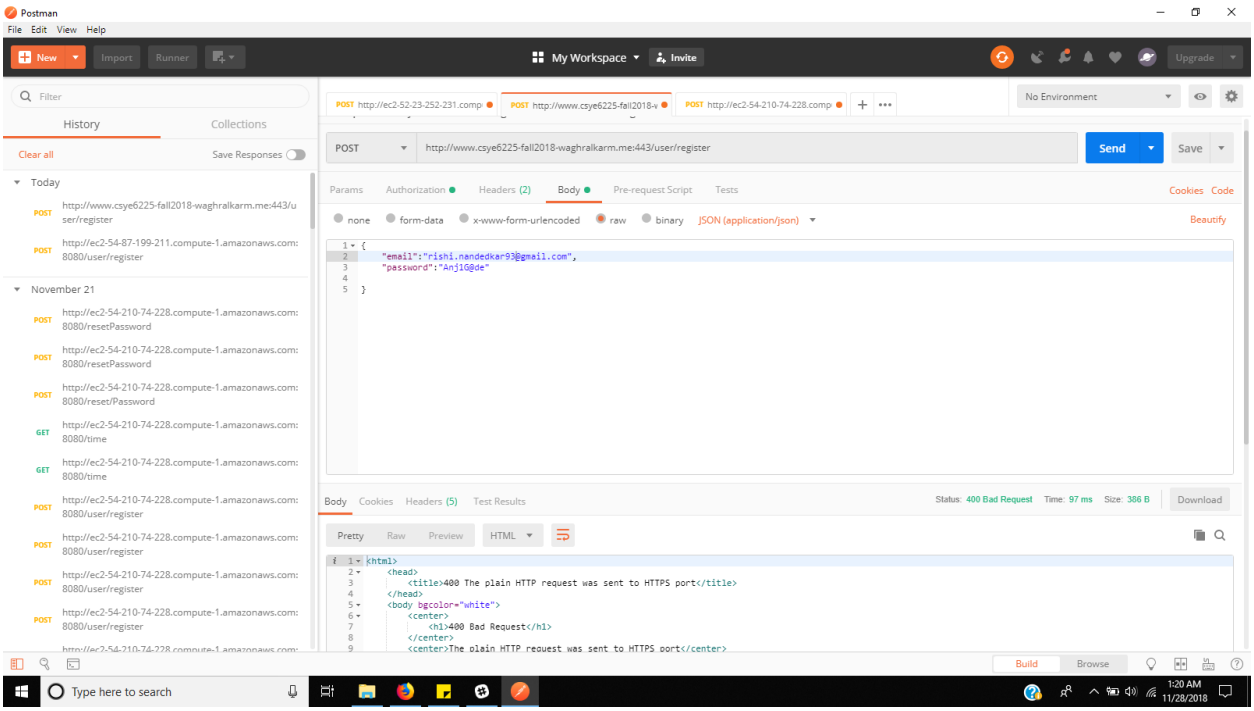
Penetration Testing

The objective of the Assignment 10 is to identify and test your application against at least 3 attack vectors that do not exploit UI vulnerabilities.

Attack Vector 1: Manual IP Blocking

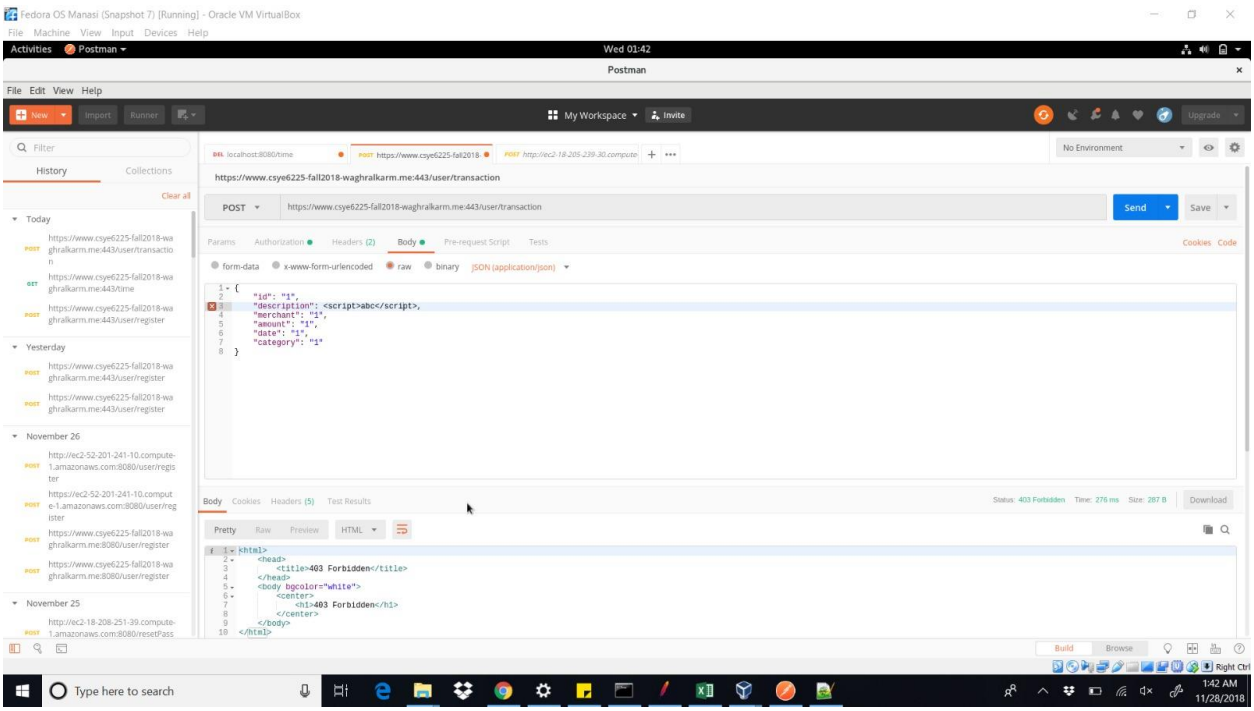
Result:



Reason for choosing this vector: In real-world scenario, an attack on our web application can be coming from specific IP address many times. This type of attack can be avoided using the AWS WAF. In WAF, we can specify the IPv4 or IPv6 address from where the attack is originating and block that IP address. This can be a very common form of attack on our website and needs to be stopped immediately.

Attack Vector 2: Cross Site Scripting

Result:



Reason for choosing this vector: Cross-site scripting (XSS) flaws occur when web applications include user-provided data in webpages that is sent to the browser without proper sanitization.

Attack Vector 3: Too large body size

Result: The web application doesn't not accept the request which is greater than the size specified.

Reason for choosing this vector: We might have a limit on storing the content submitted by the user. To implement this limit, we stop the user from attaching receipts which are greater than the specified size say 1MB.

.