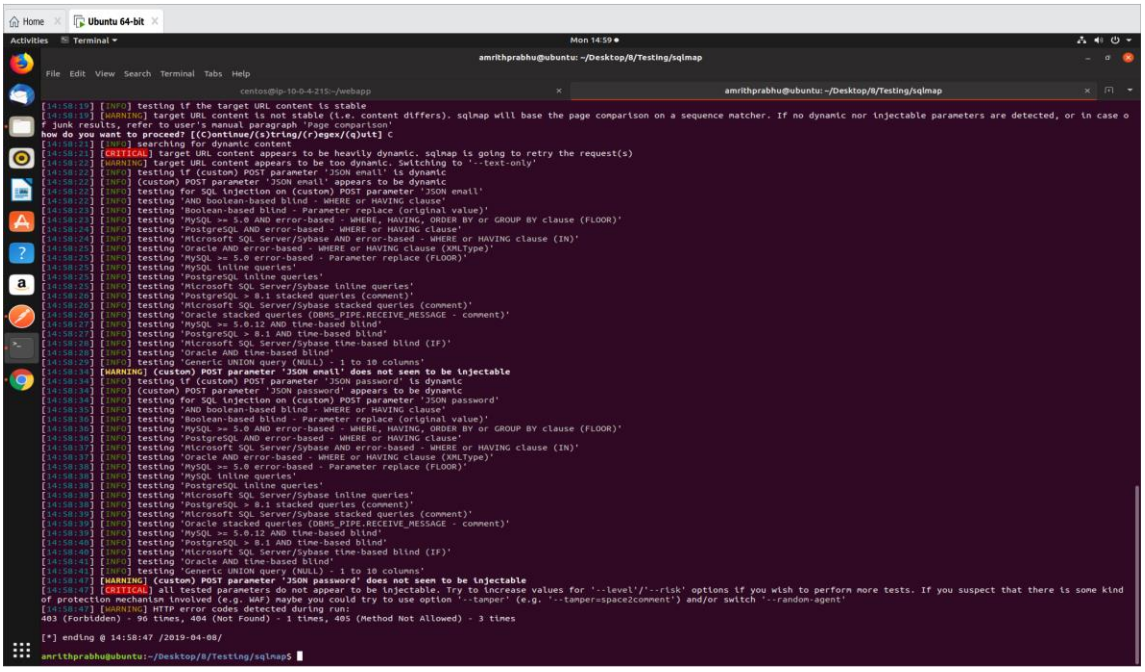
SQL Injection Attack:

Below is the SQL injection attack performed on the WebApp.

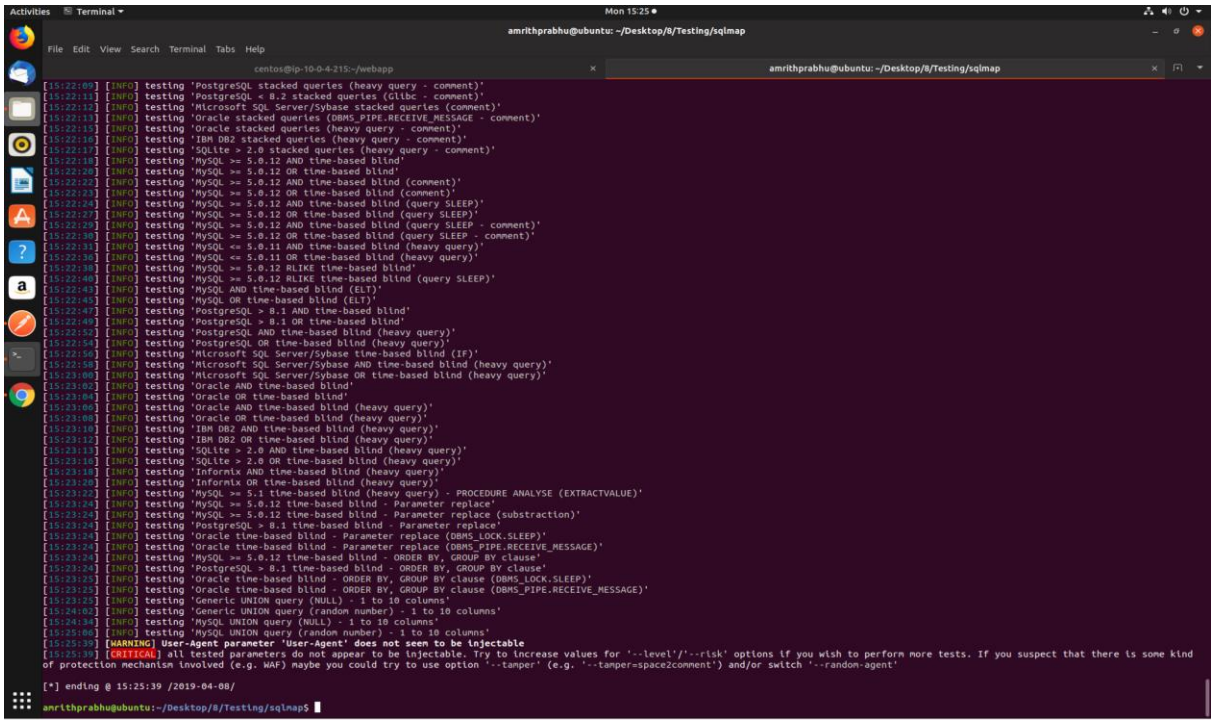
SQL injection attack results: a. WAF Enabled:

When Web Application Firewall is enabled SQL injection attack is forbidden with 403 error code as shown below.



b. WAF disabled:

When Web Application Firewall is disabled, firewall doesn't forbid the attack, however the API call is denied with error 502 (Bad Gateway) as the web application framework provides the security against SQL injection attack.



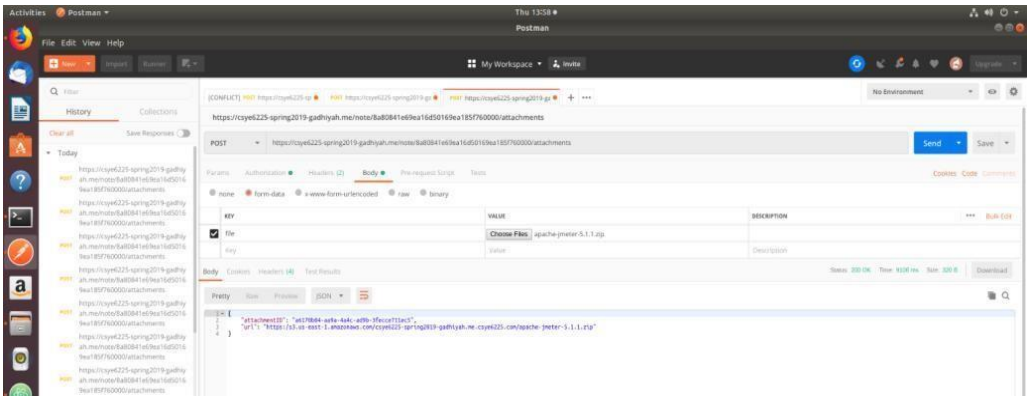
File size restriction:

Firewall rule is added to block the file attachment to note if file size greater than 1MB.

Without firewall: File with size 56 MB successfully attached to note and stored in S3 as there is no such restriction.

a. **WAF disabled (To restrict file size):**

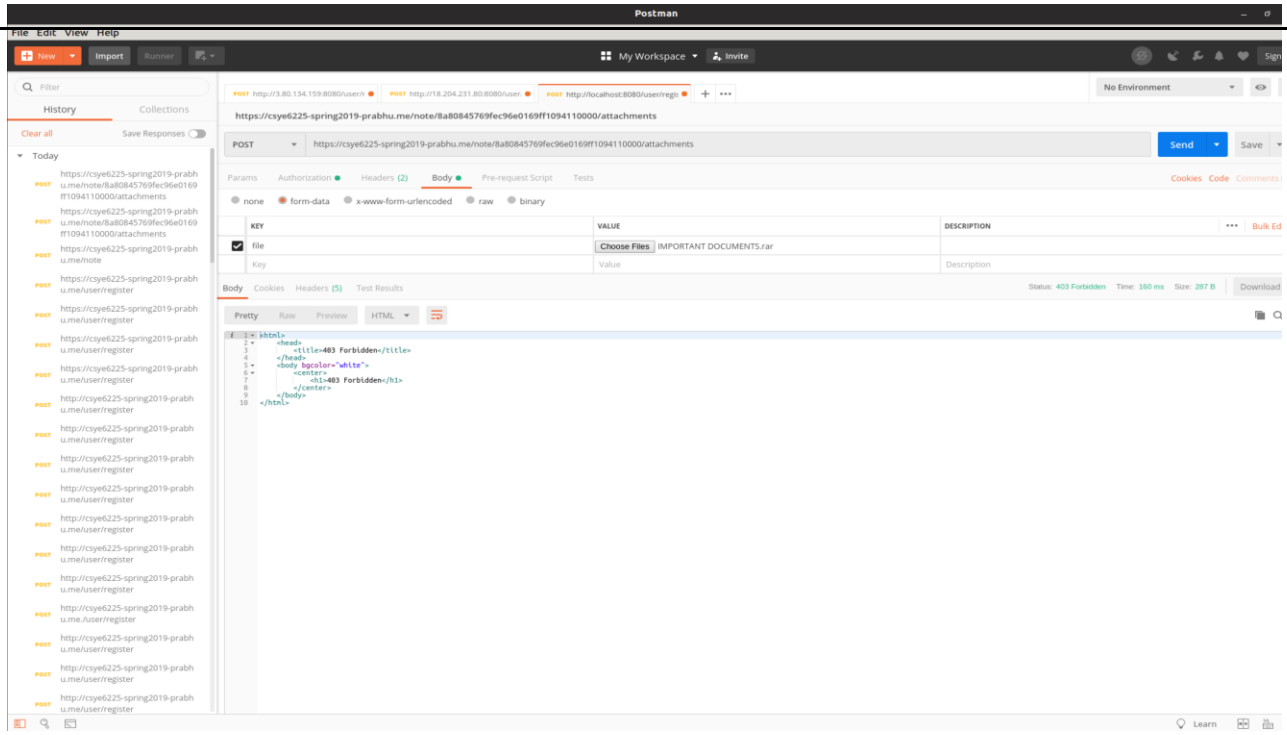
Successfully able to attach the large sized file and stored into S3



b. **WAF Enabled:**

With WAF enabled there is restriction on the size of the file to be attached. Below screenshot shows failure to attach the file due to its size 403 forbidden error is thrown.

When file with smaller size is used the attachment is successful and file stores to S3 refer the below screen shots.

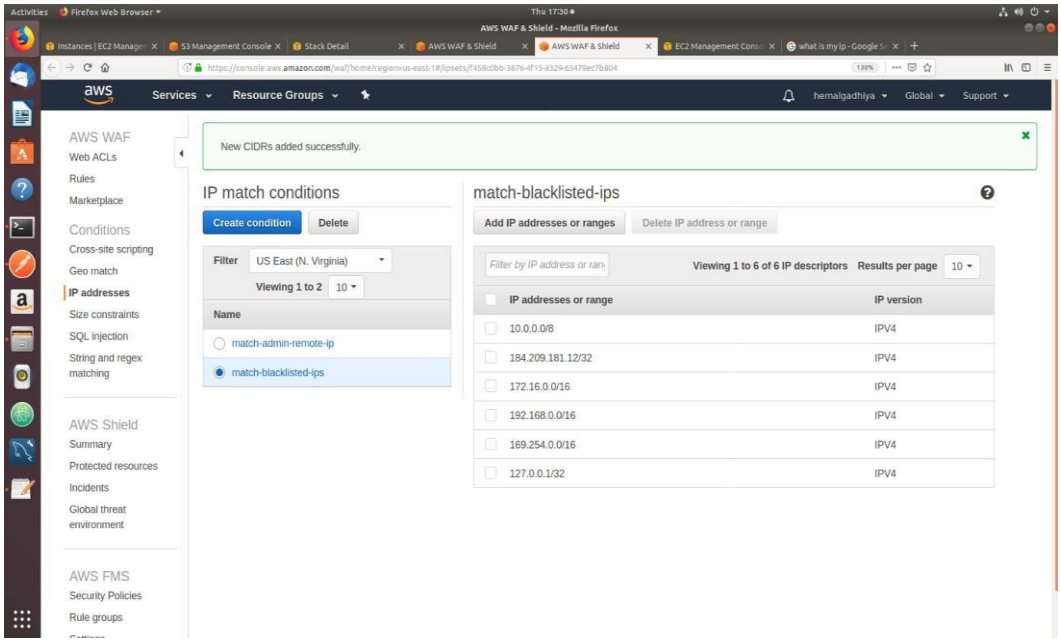


Firewall rule to block blacklist IP.

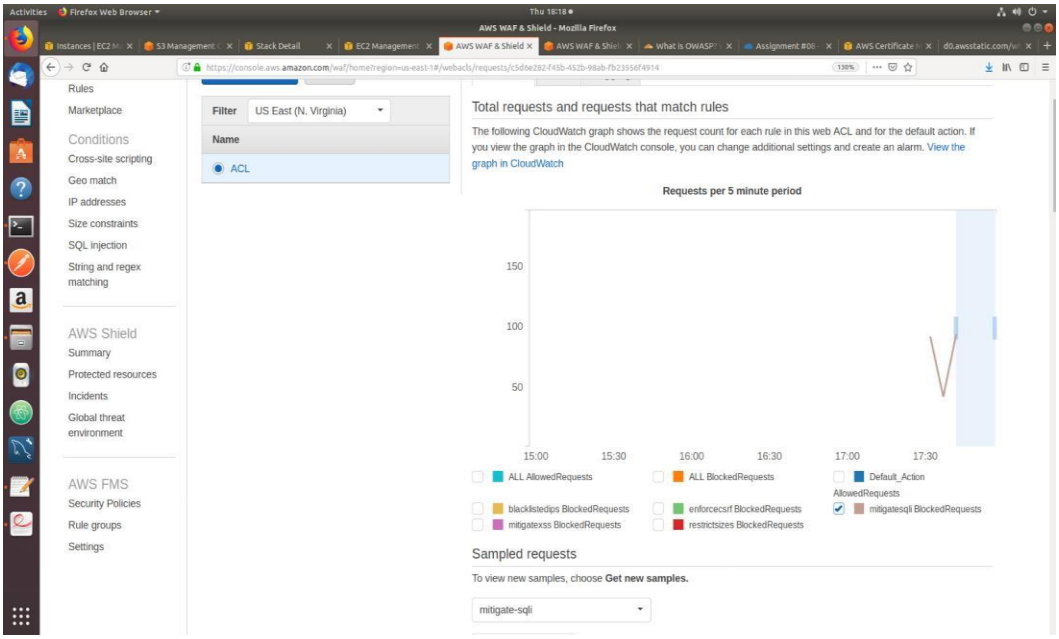
WAF rule can be set to block specific IP address (Blacklisting IP address). And when the web request (API call) is made from that IP address the HTTP request is dropped by the firewall.

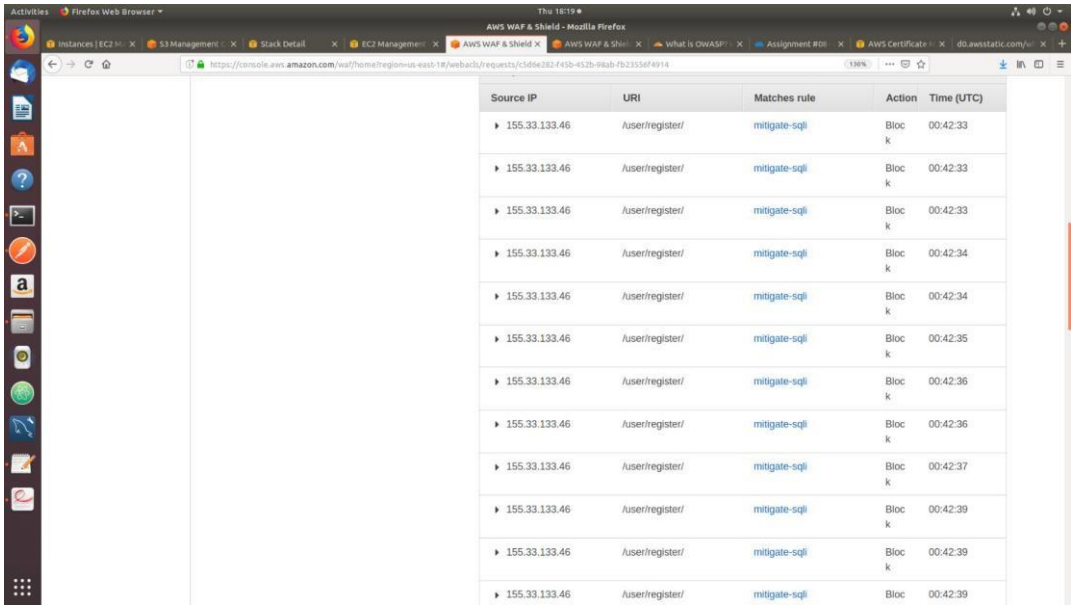
In our example:

We determine the public IP address of our machine add that IP address to list of blacklisted IP addresses as below:



When API call is made from blacklisted IP`s these calls will be blocked by WAF which can be seen from AWS console refer below screenshot:




Activities
Firefox Web Browser
Thu 18:19
AWS WAF & Shield - Mozilla Firefox
https://console.aws.amazon.com/waf/home?region=us-east-1#/webacls/requests/c5d6e282-f45b-452b-98ab-fb23556f4914
Source IP
URI
Matches rule
Action
Time (UTC)
155.33.133.46 /user/register/ mitigate-sqli Block 00:42:33
155.33.133.46 /user/register/ mitigate-sqli Block 00:42:33
155.33.133.46 /user/register/ mitigate-sqli Block 00:42:33
155.33.133.46 /user/register/ mitigate-sqli Block 00:42:34
155.33.133.46 /user/register/ mitigate-sqli Block 00:42:34
155.33.133.46 /user/register/ mitigate-sqli Block 00:42:35
155.33.133.46 /user/register/ mitigate-sqli Block 00:42:36
155.33.133.46 /user/register/ mitigate-sqli Block 00:42:36
155.33.133.46 /user/register/ mitigate-sqli Block 00:42:37
155.33.133.46 /user/register/ mitigate-sqli Block 00:42:39
155.33.133.46 /user/register/ mitigate-sqli Block 00:42:39
155.33.133.46 /user/register/ mitigate-sqli Block 00:42:39