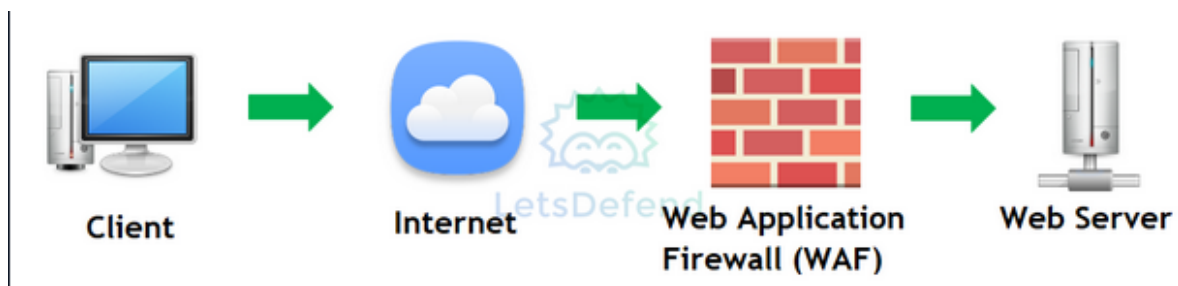


Web Application Firewall (WAF) Analysis Questions

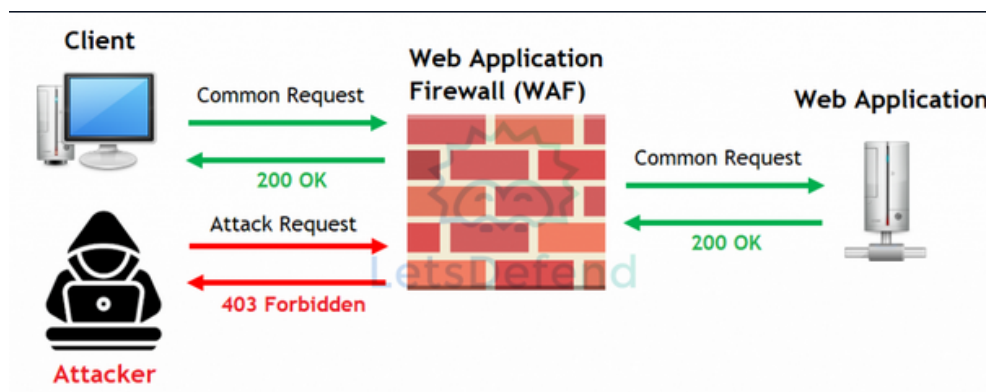
By: Ryan Stewart



Analyzing the provided Cloud logs:

1. In the **Cloudflare WAF** log, an HTTP request was sent to the IP address 185.220.102.244. What HTTP method does this HTTP request utilize?

```
ock", "clientASNDescription": "XXXXXXX", "clientAsn": "60533", "clientCountryName": "T1", "clientIP": "185.220.102.244", "clientRequestHTTPHost": "letsdefend.io", "clientRequestHTTPMethod": "GET", "clientRequestHTTPProtocol": "HTTP", "clientRequestPath": "/", "clientRequestQuery": "", "datetime": "2022-11-08T06:11:01Z", "rayName": "116c261b4efadsa1", "rulesetId": "d6292f3f4e0096fc85clad199sa2", "rulesetId": "d6292f3f4e0096fc85clad199sa2", "source": "firewallrules", "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7; rv:91.0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.72 Safari/90.0.4430.72", "matchIndex": 0, "metadata": [{"key": "filter", "value": "a5df0232dd13493a9349786843694552"}, {"key": "type", "value": "attack"}], "sampleInterval": 1}
```



2. According to the **AWS WAF** log, a request for a SQL Injection attack was blocked. What is the IP address that sent this request?

```
576280412771,"formatVersion":1,"webaclId":"arn:aws:wafv2:ap-southeast-2:111122223333:regional/webacl/Le  
PLE-2ARN-3ARN-4ARN-123456EXAMPLE","terminatingRuleId":"LetsDefend SQLi","terminatingRuleType":"REGULAR"  
CK","terminatingRuleMatchDetails":[{"conditionType":"SQL_INJECTION","sensitivityLevel":"HIGH","location  
tchedData":["10","AND","1"]}],{"httpSourceName":"-","httpSourceId":"-","ruleGroupList":[],"rateBasedRule  
erminatingMatchingRules":[],"httpRequest":{"clientIp":"185.220.101.35","country":"DE","headers":[{"name  
e":"localhost:1989"}, {"name":"User-Agent","value":"curl/7.61.1"}, {"name":"Accept","value":"*/*"}, {"name  
,"value":"10 AND  
/myUri","args":"","httpVersion":"HTTP/1.1","httpMethod":"GET","requestId":"rid"},"labels":[{"name":"val
```