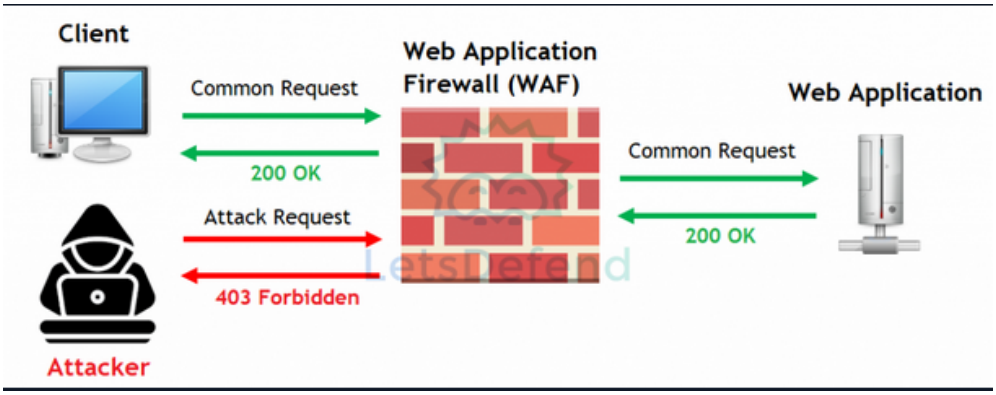
Web Application Firewall (WAF) Analysis Questions

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?


```
ck","clientASNDescription":"XXXXXXX","clientAsn":"60533","clientCountryName":"TI","clientIP":"185.220.1
tRequestHTTPHost":"letsdefend.io","clientRequestHTTPMethodName":"GET","clientRequestHTTPProtocol":"HTTP
equestPath":"/","clientRequestQuery":"","datetime":"2022-11-08T06:11:01Z","rayName":"116c261b4efadsa1",
d6292f3f4e0096fc85cladl99sa2","rulesetId":"","source":"firewallrules","userAgent":"Mozilla/5.0
.0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.72
","matchIndex":0,"metadata":[{"key":"filter","value":"a5df0232dd13493a9349786843694552"},{"key":"type","
er"}],"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?