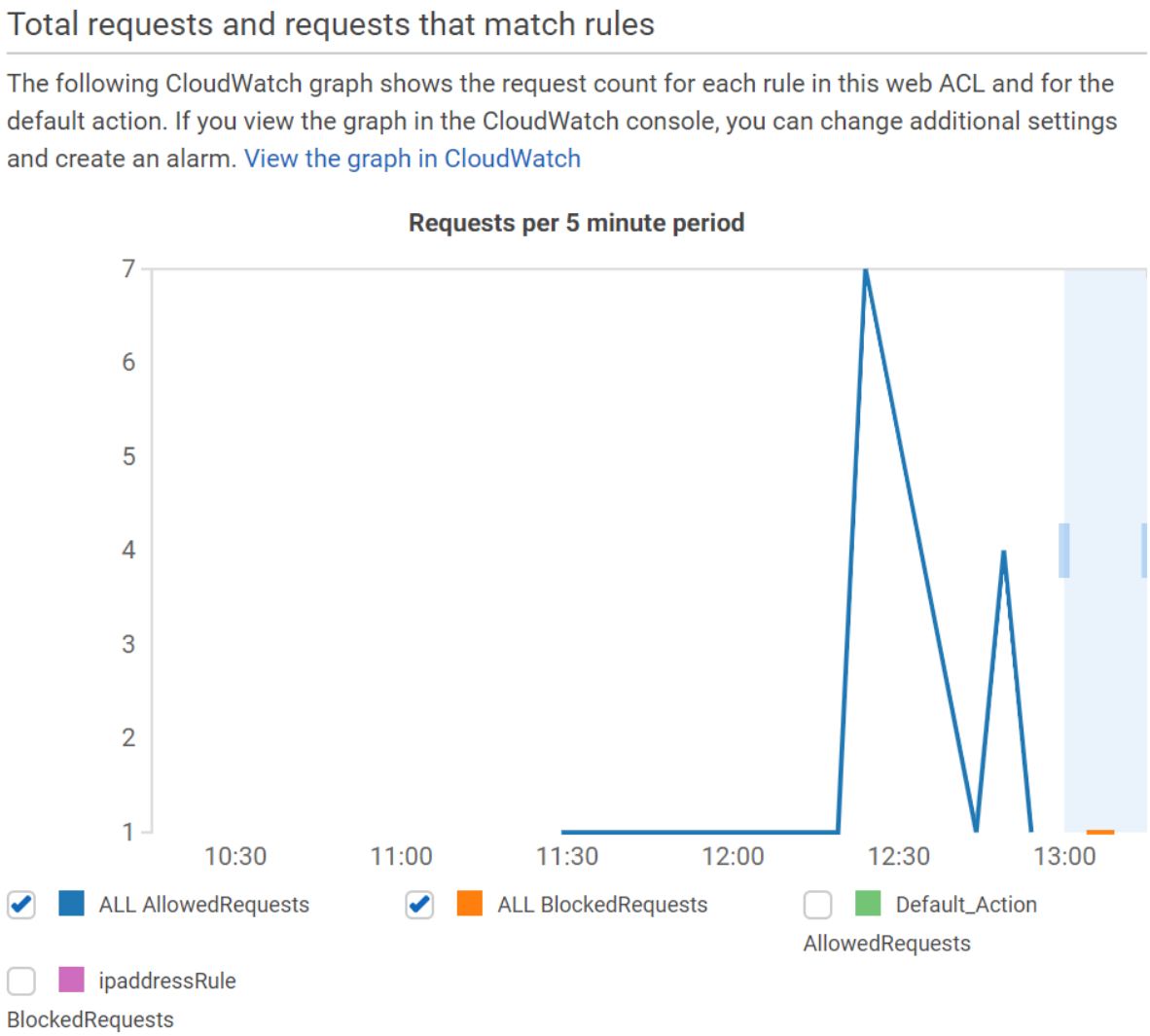
ATTACK VECTORS

Attack Vectors:

- IP address blocking
- SQL injection attack
- File size constraint
- Open port analysis

1. IP address blocking:

You can use this history to help identify and block IP addresses from malicious sources. This solution creates an AWS Lambda function that automatically parses access logs, counts the number of bad requests from unique source IP addresses, and updates AWS WAF to block further scans from those addresses.



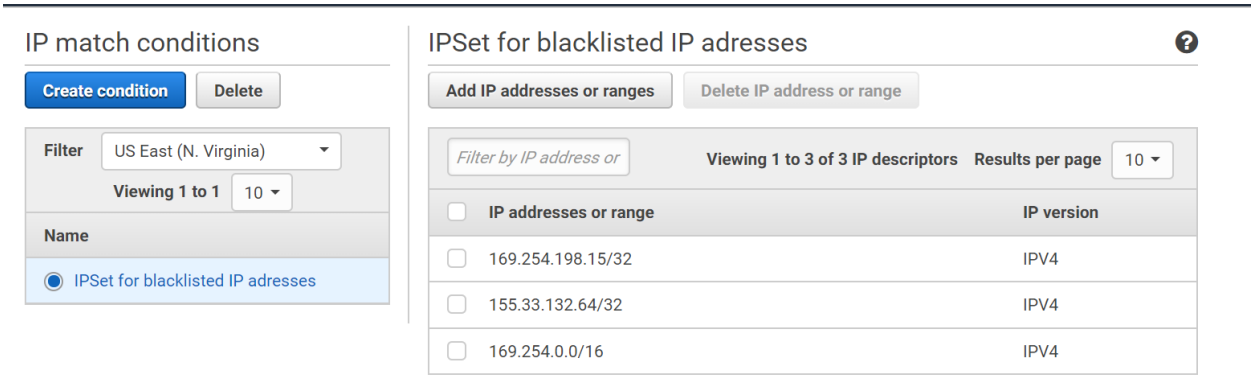
ATTACK VECTORS

- With WAF disabled:
  All the requests from IP address 155.33.132.64 are allowed.

Source IP	URI	Matches rule	Actio	Time (UTC)
71.6.143.90	/	DefaultAction	All ow	16:47:20
155.33.132.64	/librarymanageme... system-0.0.1-SNAPSHOT/user/register	DefaultAction	All ow	16:52:08
155.33.132.64	/librarymanageme... system-0.0.1-SNAPSHOT/user/register	DefaultAction	All ow	16:52:11
155.33.132.64	/librarymanageme... system-0.0.1-SNAPSHOT/user/register	DefaultAction	All ow	16:52:12
155.33.132.64	/librarymanageme... system-0.0.1-SNAPSHOT/user/register	DefaultAction	All ow	16:52:14
155.33.132.64	/librarymanageme... system-0.0.1-	DefaultAction	All ow	16:55:33

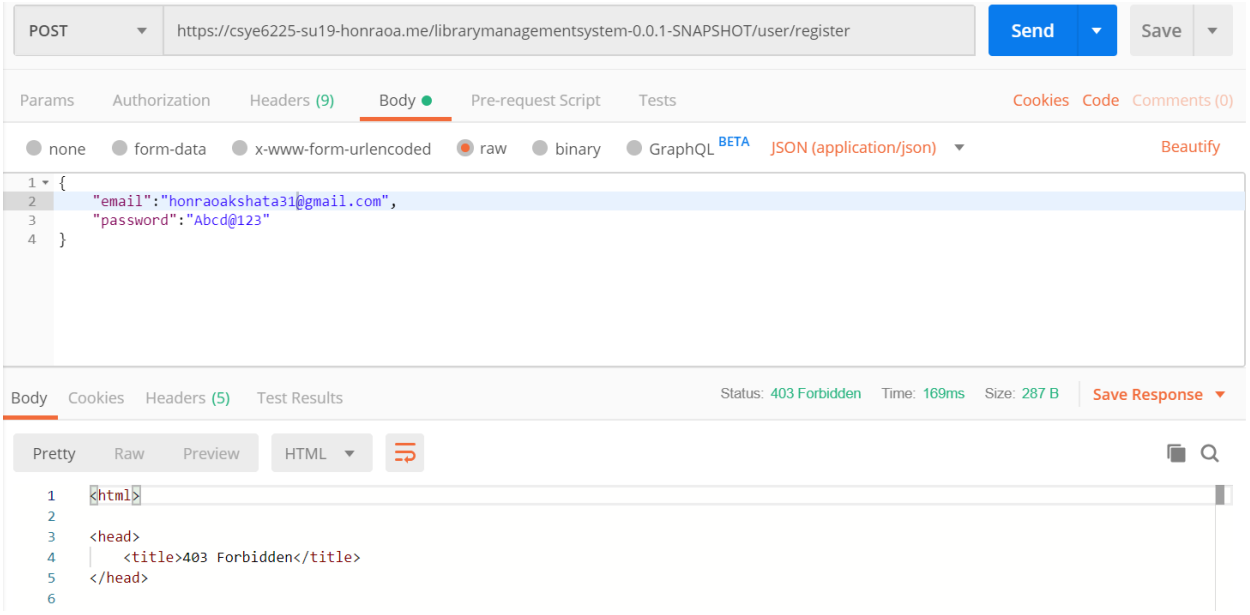
- With WAF Enabled:

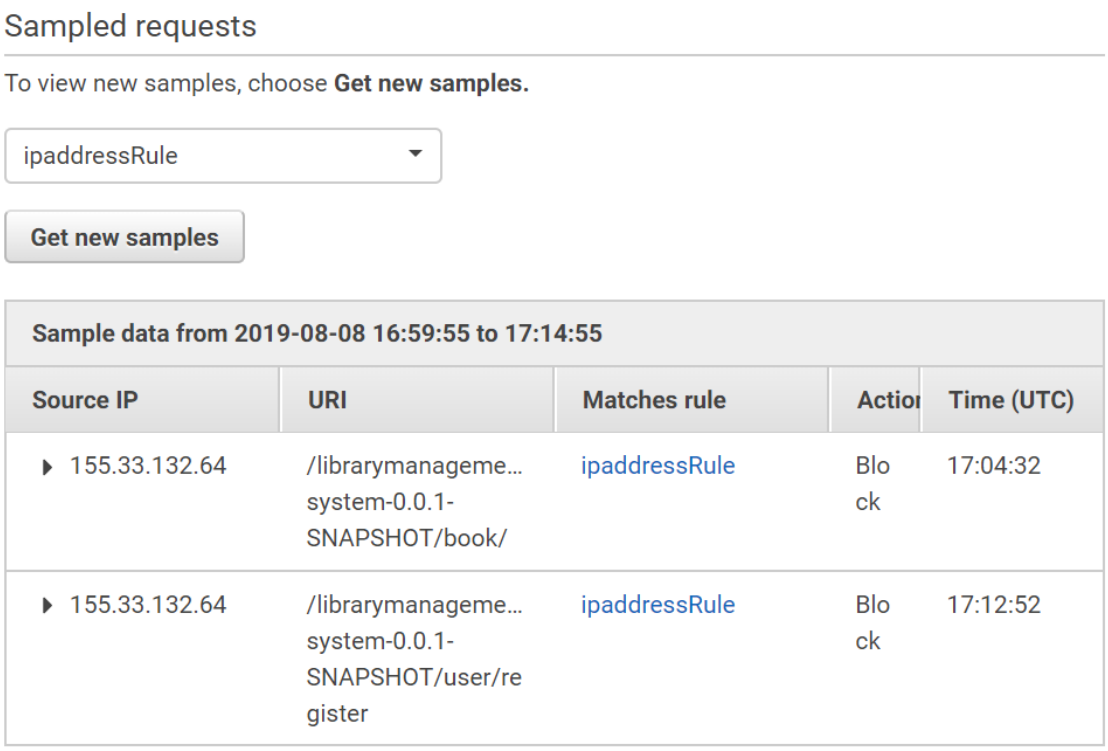
When 155.33.132.63 IP address is added to the blacklisted IP addresses range. All the requests from this IP address are blocked by WAF.



Request :Request made to /User/register endpoint with blocked IP address 155.33.132.64 gets 403 forbidden response from WAF application firewall.

ATTACK VECTORS





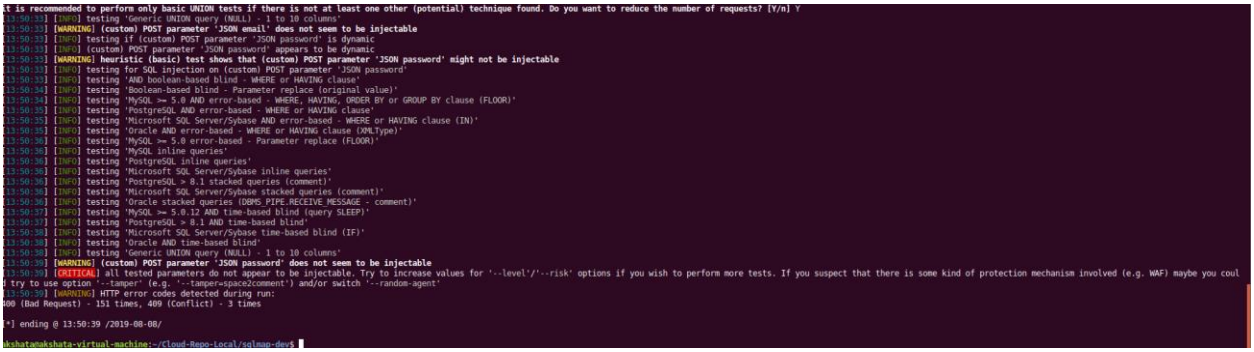
2. SQL INJECTION:

SQL Injection (SQLi) is a type of a injection attack that makes it possible to execute malicious SQL statements. These statements control a database server behind a web application. Attackers can use SQL Injection vulnerabilities to bypass application security measures. We choose this attack vector to check if our application has any SQL

injection vulnerabilities. It turns out that this application is protected as we have used Prepared Statements (Parameterized queries).
Command:

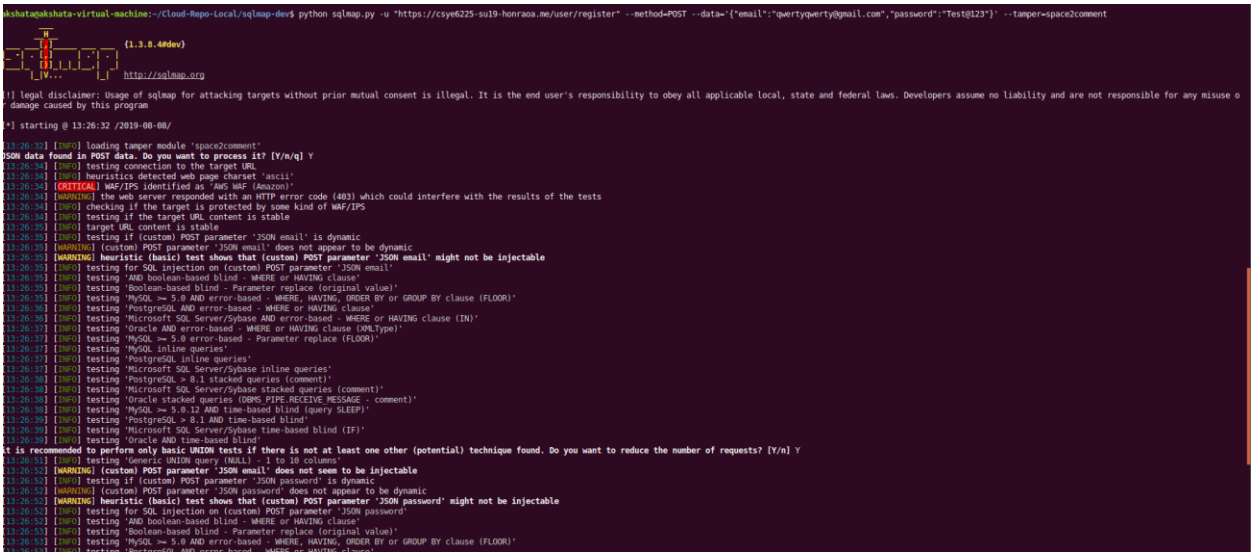
python sqlmap.py -u " https://csye6225-su19-honraoa.me/librarymanagementsystem-0.0.1-SNAPSHOT/user/register/" --method=POST --data='{"email":"honrao.a@gmail.com","password":"Test@123"}' --tamper=space2comment

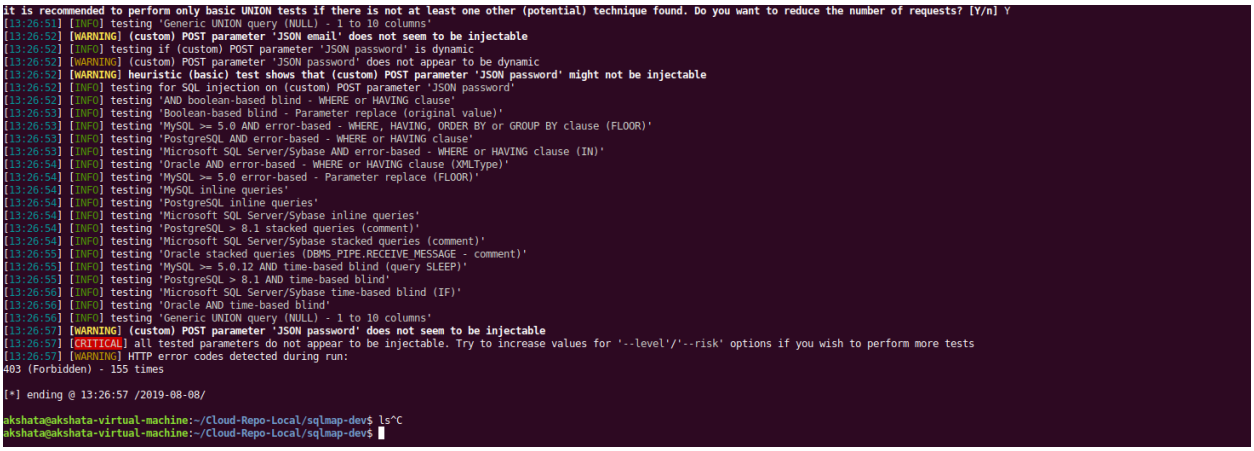
- WAF disabled:
  When WAF is disabled firwall doesn't forbid the attack but application security throws 400 bad request response to the sql injection attack .



- WAF enabled:
  When WAF is enabled firewall thorws 403 forbidden access to sql injection attack

ATTACK VECTORS

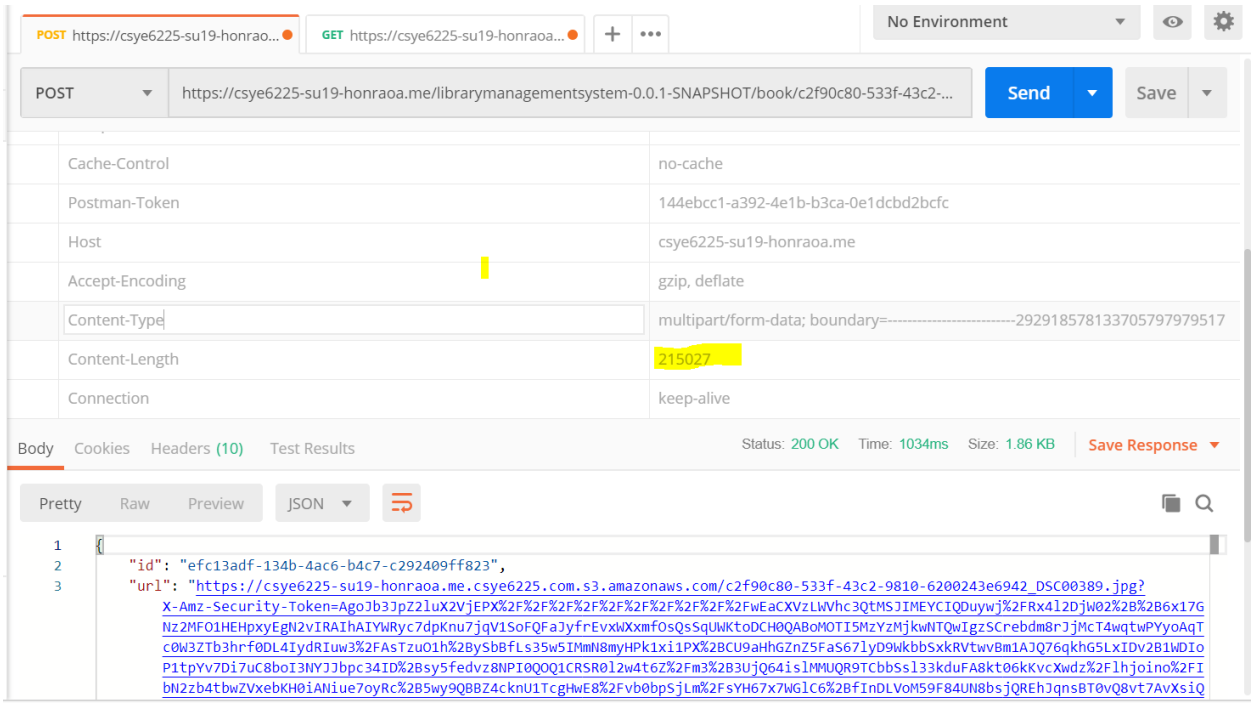




3. **File size constraint:**
   Any http request having body size greater than 200KB will not be allowed to process

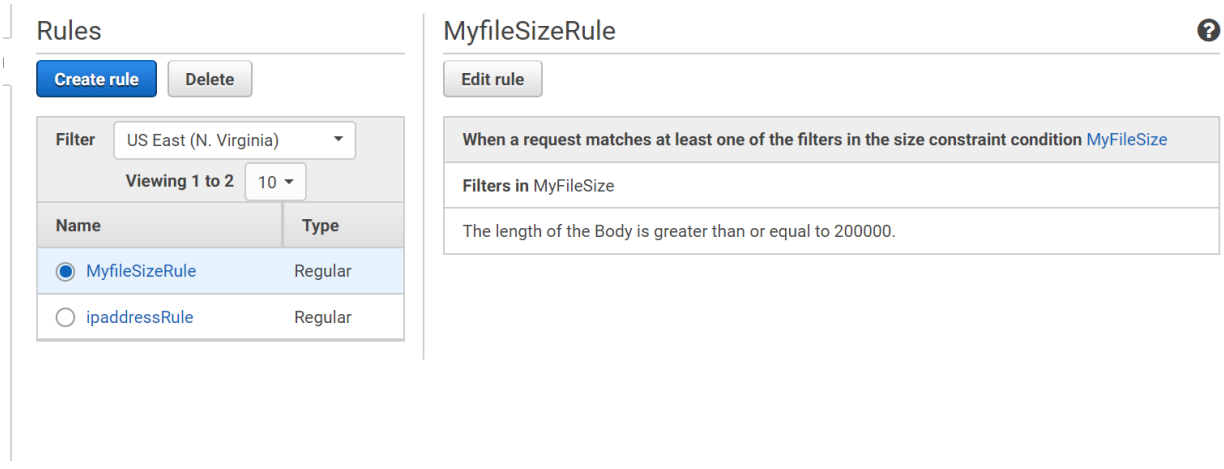
- With WAF disabled:
  When WAF is disabled there are no constraints on the body size so all the requests are processed .

ATTACK VECTORS

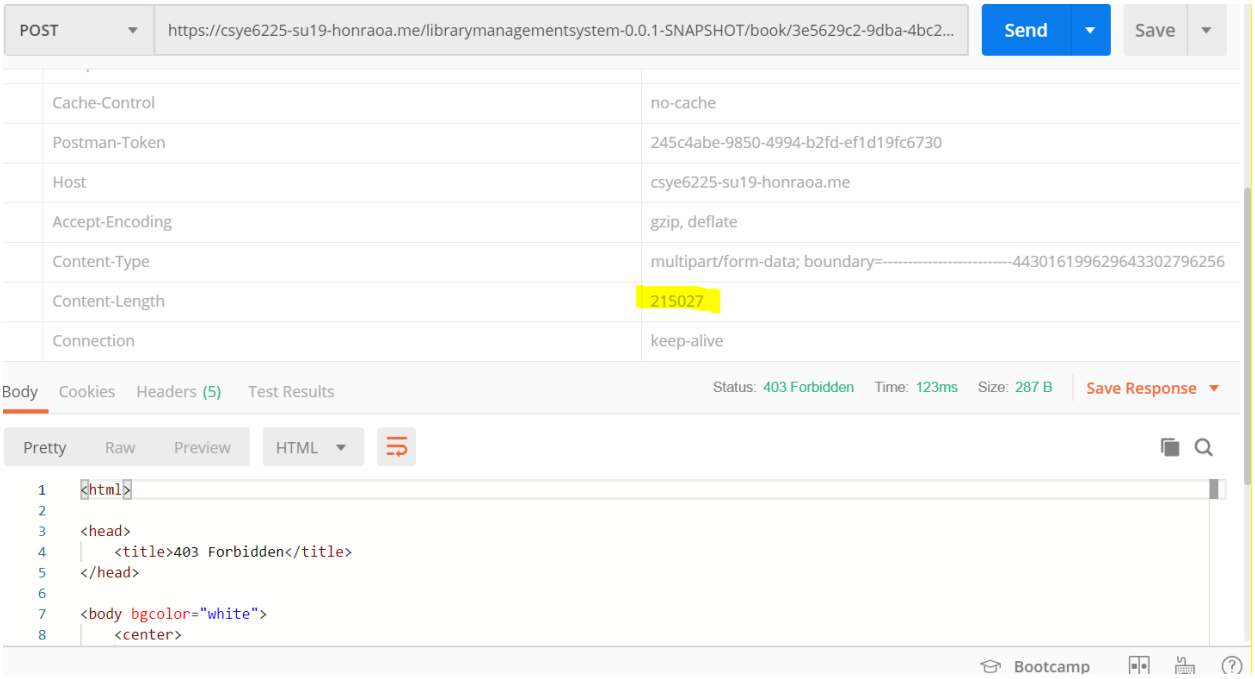


- With WAF enabled:

With body length exceeds the file constraint 200KB firewall will block that request and will return a 403 forbidden response.



ATTACK VECTORS



4. Checking all the open ports using nmap:

Nmap is used to discover hosts and services on a computer network by sending packets and analyzing the responses. After running nmap command on domain we can see that only https 443 port open except that all the open port have been closed by the firewall.