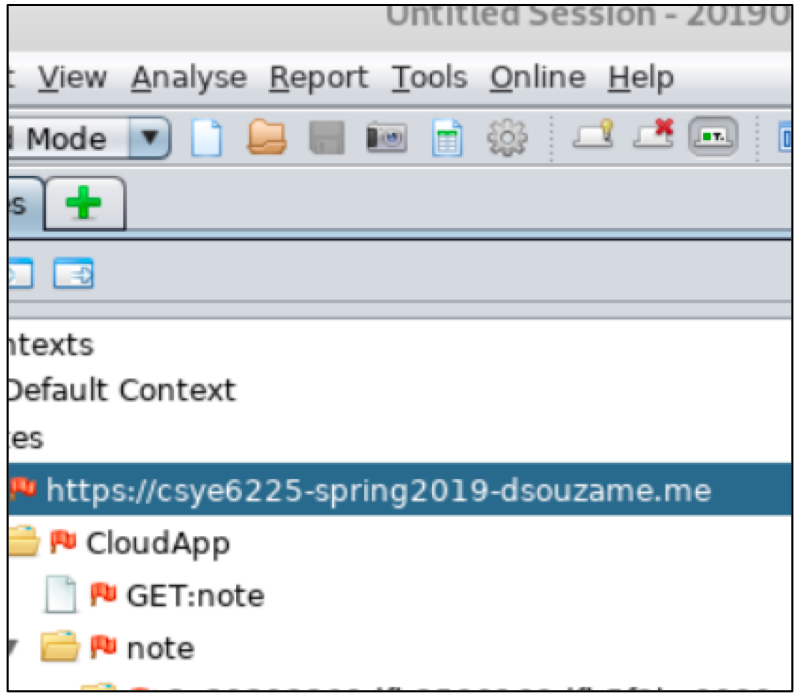
Penetration Testing

OWASP ZAP

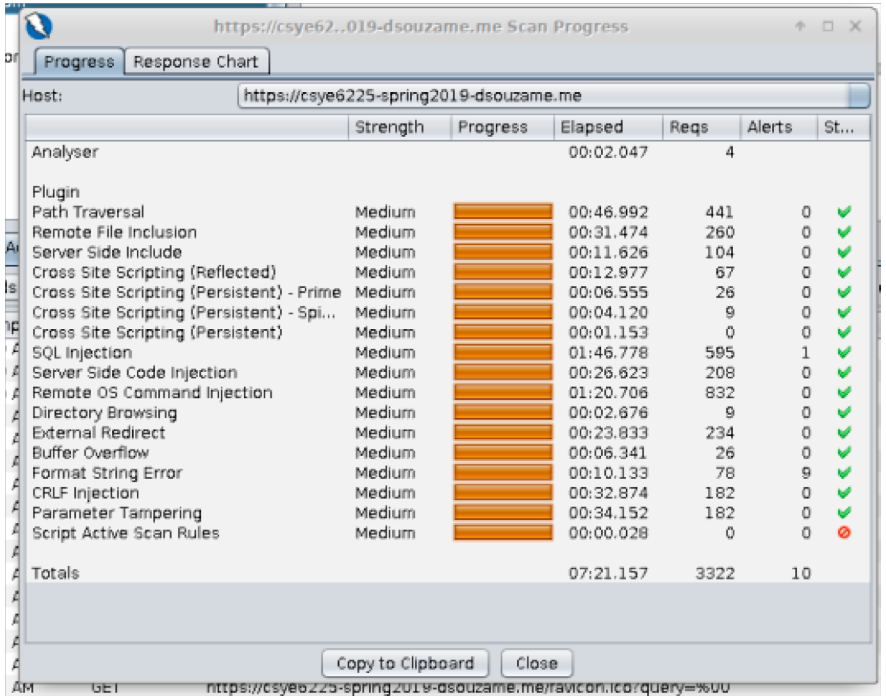
- The OWASP Zed Attack Proxy is a Java-based tool that comes with an intuitive graphical interface.



SQL Injection – Without WAF

- An SQL Injection vulnerability may affect any website or web application that uses an SQL database such as MySQL, Oracle, SQL Server, or others. Criminals may use it to gain unauthorized access to your sensitive data: customer information, personal data, trade secrets, intellectual property, and more. SQL Injection attacks are one of the oldest, most prevalent, and most dangerous web application vulnerabilities.

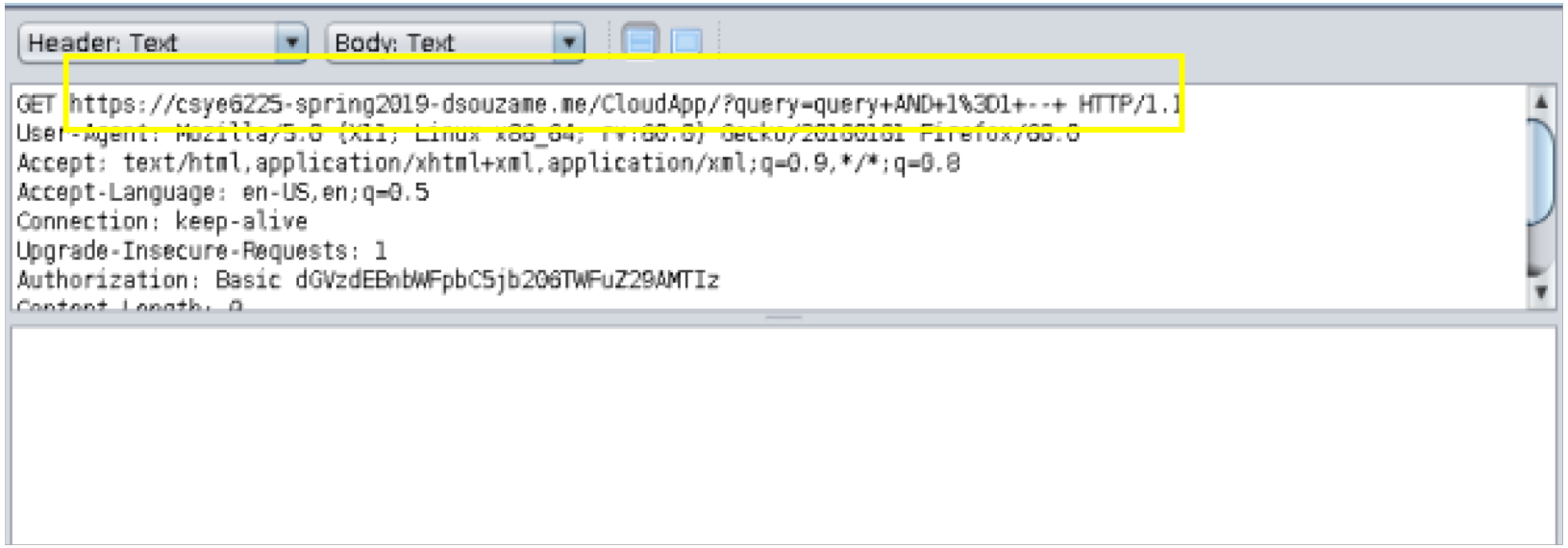
Active Scan



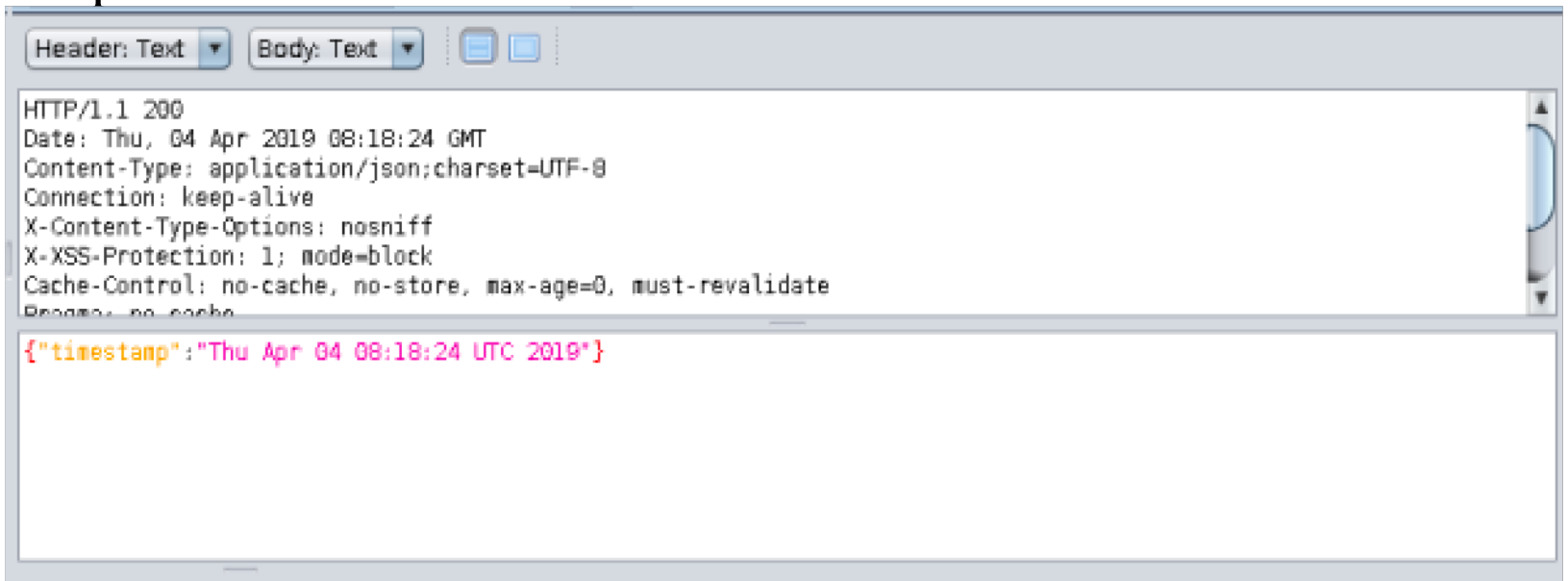
Alert Message

SQL Injection

Request



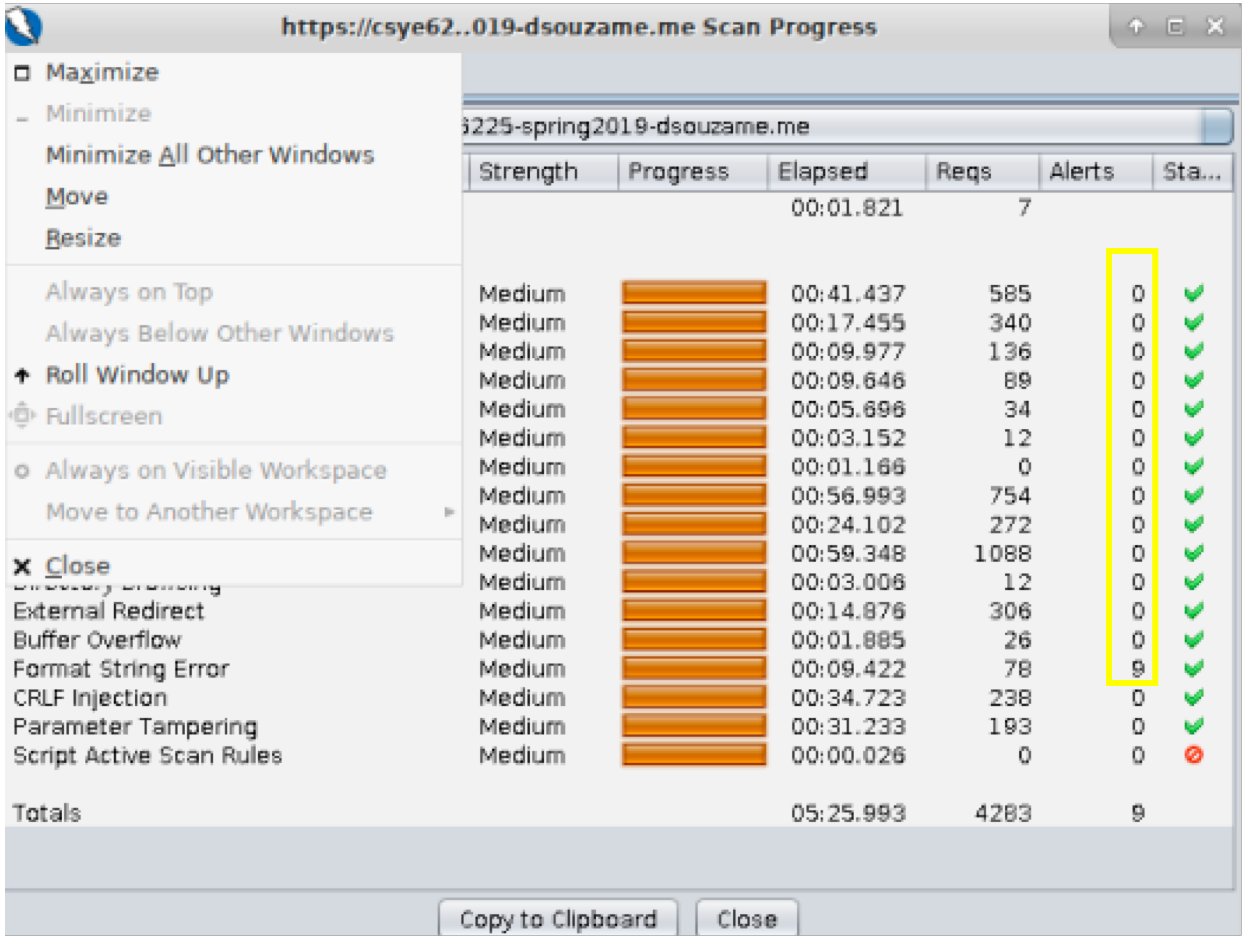
Response



Inference:
We can see that without WAF we are able to attack using SQL Injection in the URL with parameter query

SQL Injection – With WAF

Active Scan

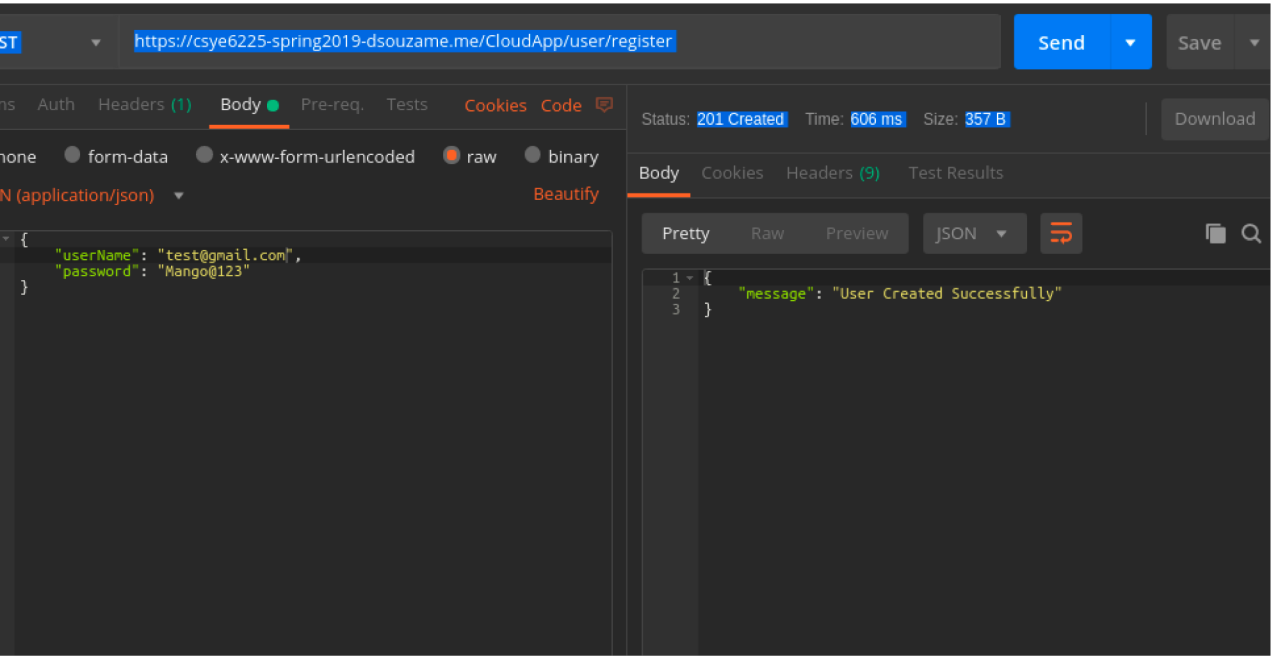


Inference:
We can see that with WAF we are unable to attack using SQL Injection in the URL with parameter query. Wee get a response 403 Forbidden

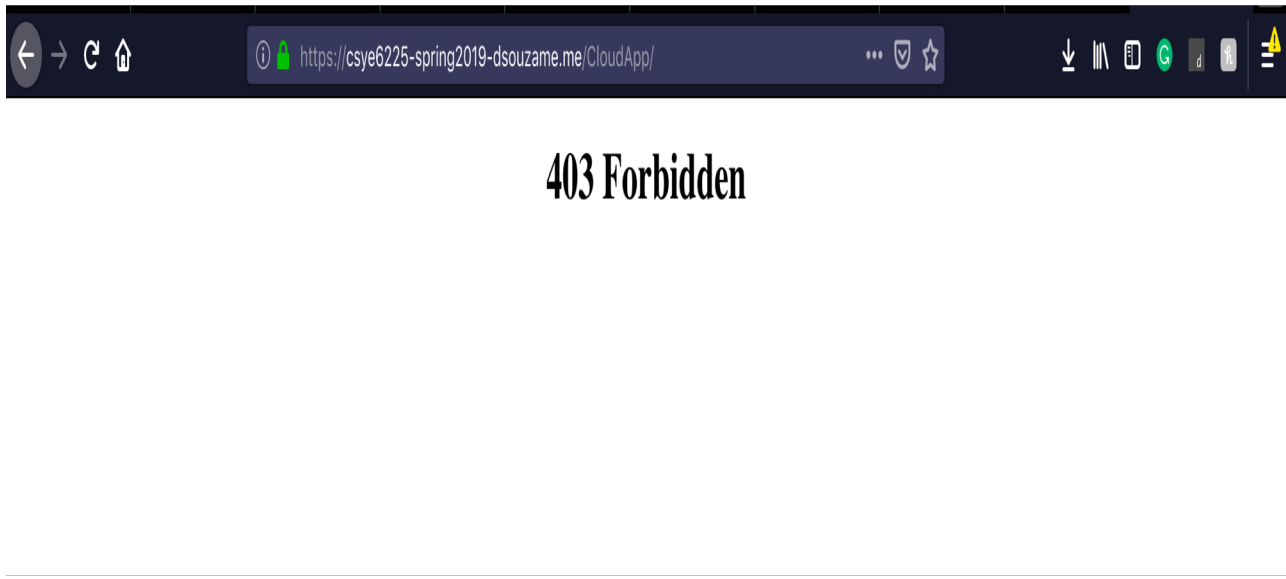
IP Blacklisting

- In computing, a **blacklist** is a basic access control mechanism that allows everyone access, except for the members of the black list (i.e. list of denied accesses).
- For testing purpose, we have blacklisted one of our IP Addresses.

Without WAF



With WAF

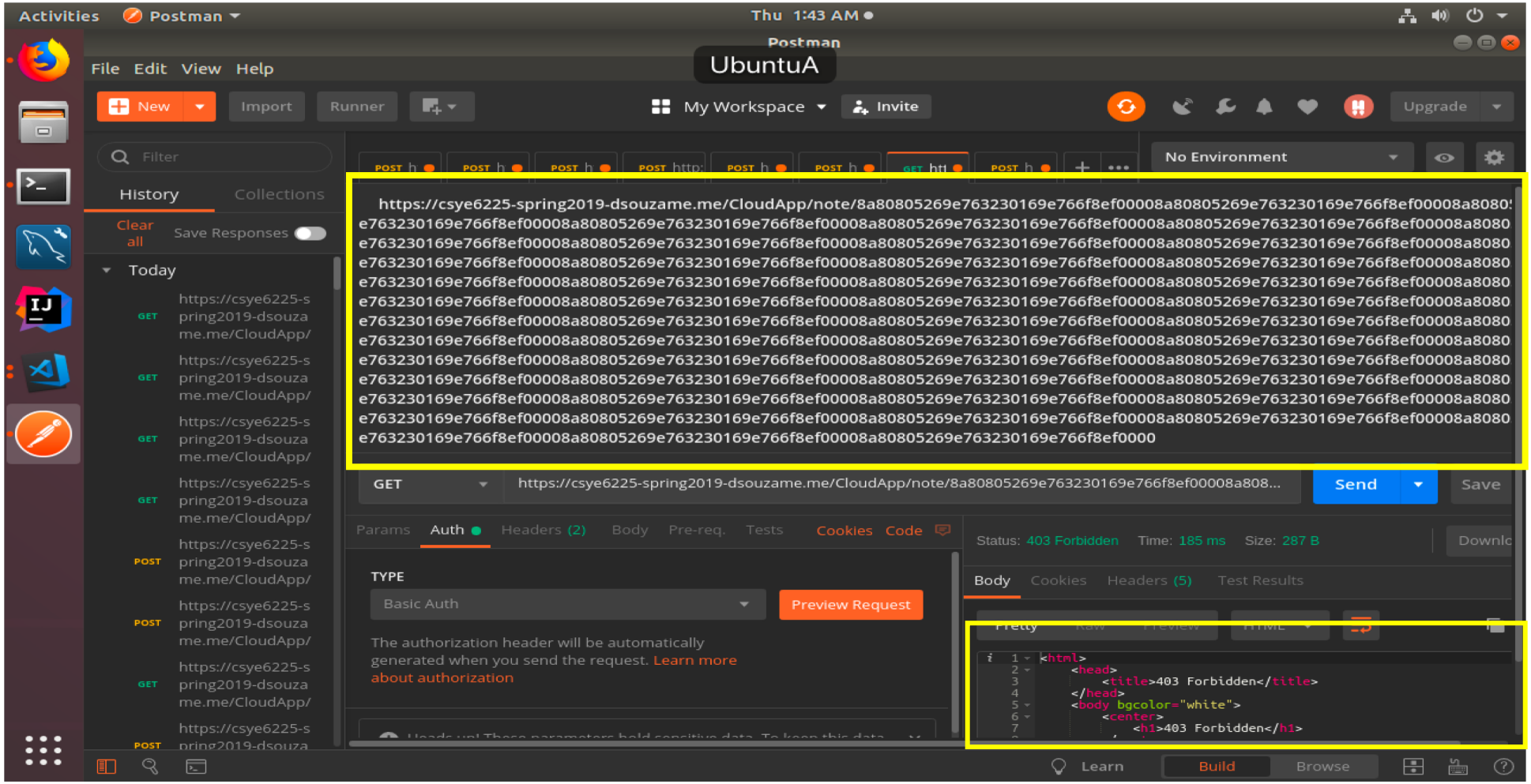


URL Length Constraint

- The web application has a regular URL which can be hit. Therefore the URL length is known. However hackers will manipulate the length or pass invalid tokens in order to access the URL

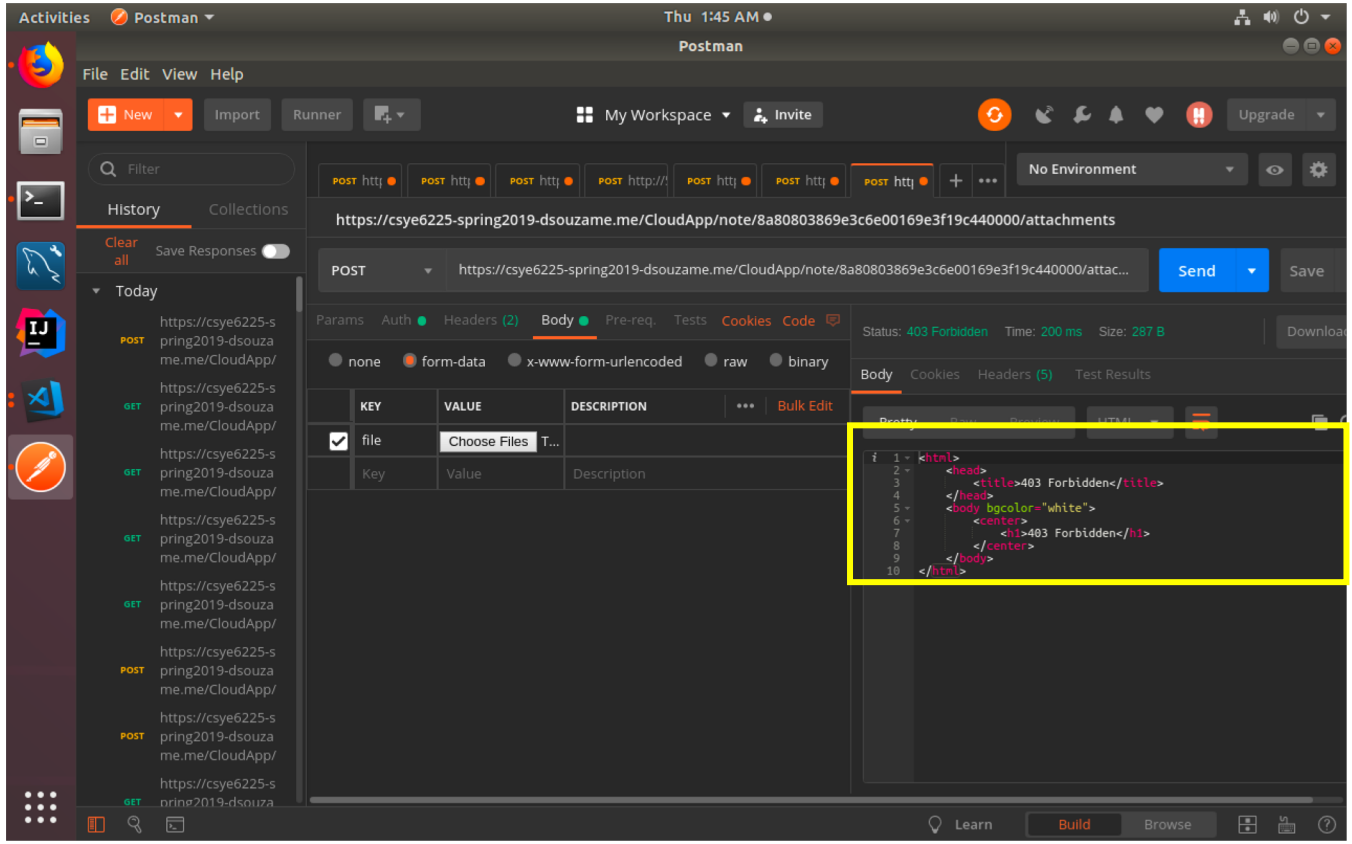
URL Length Constraint

- With WAF



Body Constraint : Attachment Size

- When uploading files to a web application, it has possible risk. Large file upload can cause client-side attacks or even database overload
- Without WAF: When we try to upload a large files, it will crash the web application.
- With WAF: When we try to upload a large files, we get a 403 Forbidden error since there is a body constraint



NMAP

- Nmap (“Network Mapper”) is a free and open source (license) utility for network discovery and security auditing. It allows you to probe a machine with packets to detect everything from running services and open ports to the operating system and software versions.