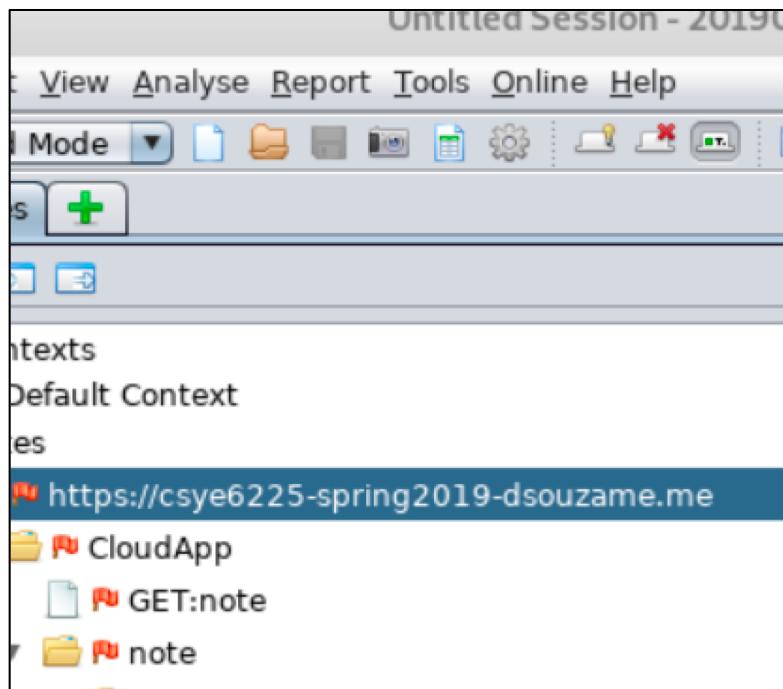


Penetration Testing

OWASP ZAP

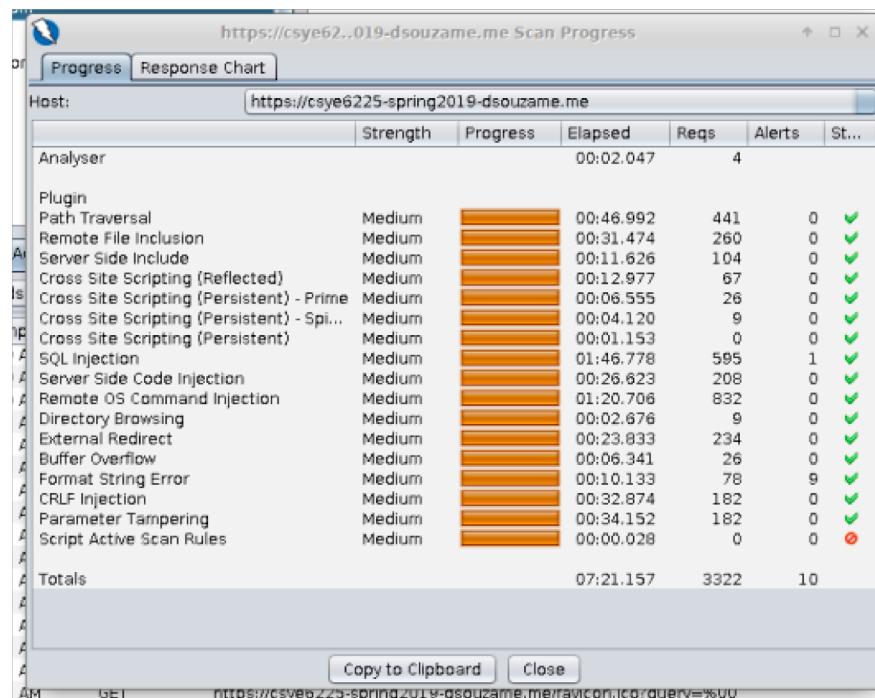
- The OWASP Zed Attack Proxy is a Java-based tool that comes with an intuitive graphical interface.



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.

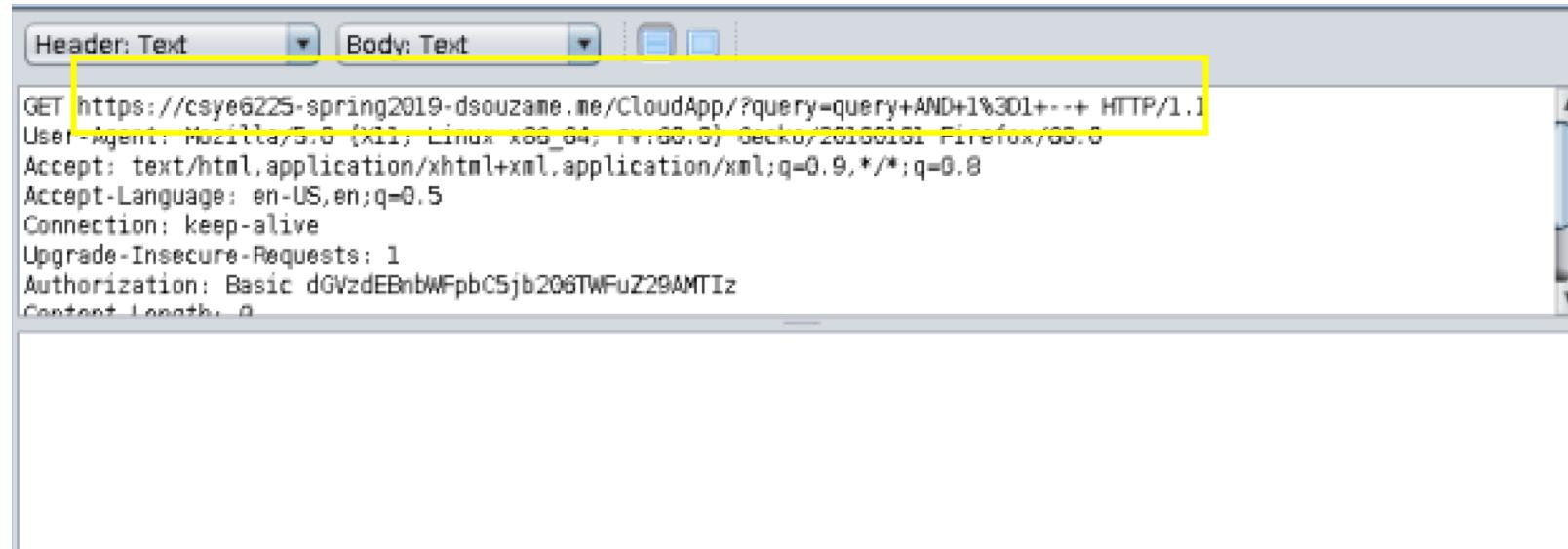
Active Scan



Alert Message

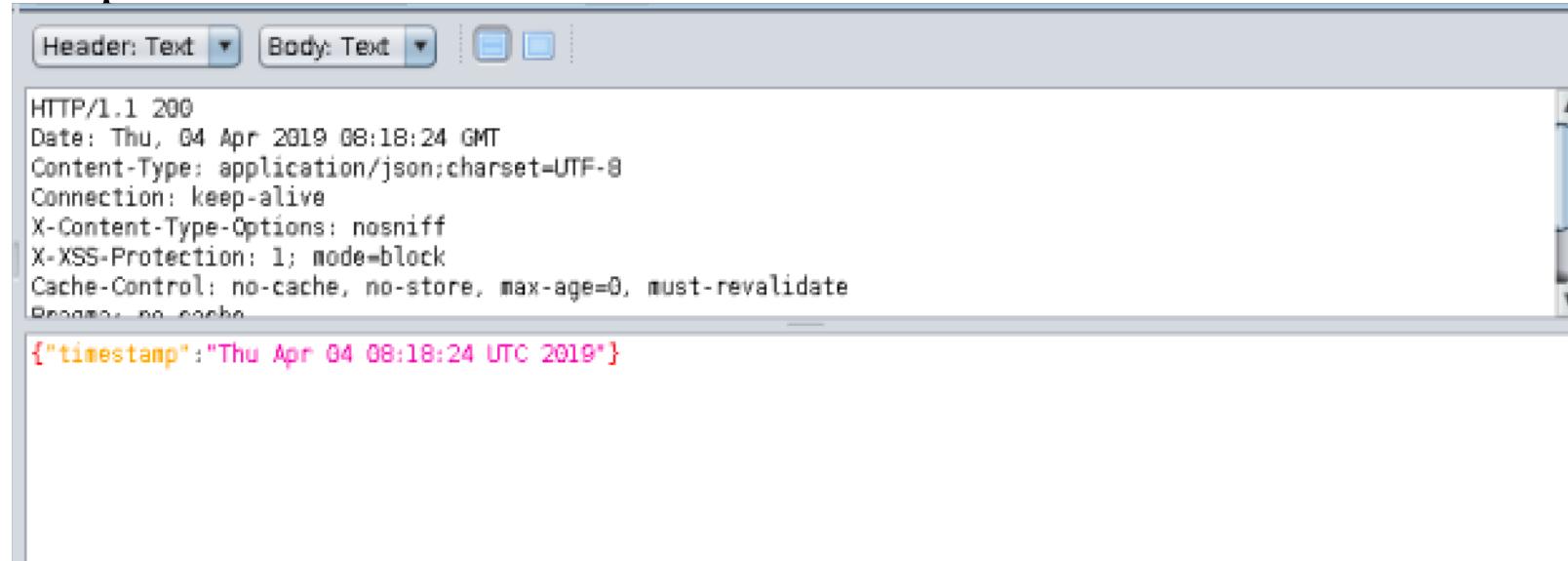


SQL Injection Request



```
Header: Text Body: Text  
GET https://csye6225-spring2019-dsouzame.me/CloudApp/?query=query+AND+1%3D1++ HTTP/1.1  
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:69.0) Gecko/20100101 Firefox/69.0  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8  
Accept-Language: en-US,en;q=0.5  
Connection: keep-alive  
Upgrade-Insecure-Requests: 1  
Authorization: Basic dGVzdEBnbWFpbC5jb206TWFuZ29AMTlz  
Content-Length: 0
```

Response

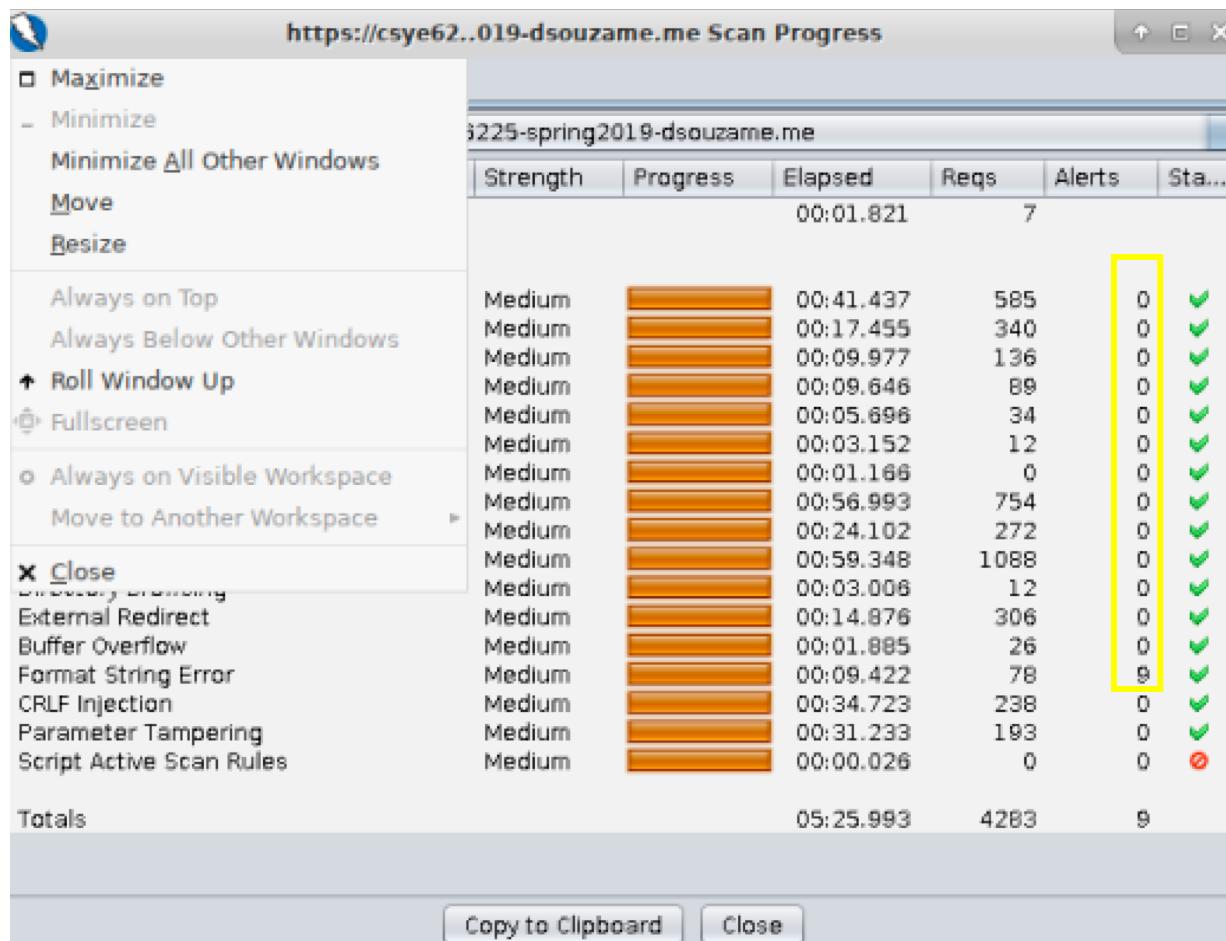


```
Header: Text Body: Text  
HTTP/1.1 200  
Date: Thu, 04 Apr 2019 08:18:24 GMT  
Content-Type: application/json; charset=UTF-8  
Connection: keep-alive  
X-Content-Type-Options: nosniff  
X-XSS-Protection: 1; mode=block  
Cache-Control: no-cache, no-store, max-age=0, must-revalidate  
Pragma: no-cache  
  
{"timestamp": "Thu Apr 04 08:18:24 UTC 2019"}
```

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. We 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

The screenshot shows the Postman interface with a successful API call. The URL is <https://csye6225-spring2019-dsouzame.me/CloudApp/user/register>. The response status is 201 Created, time is 606 ms, and size is 357 B. The Body tab displays a JSON response:

```
{"message": "User Created Successfully"}
```

With WAF

The screenshot shows the Postman interface with a failed API call due to WAF. The URL is <https://csye6225-spring2019-dsouzame.me/CloudApp/>. The response is a 403 Forbidden error.

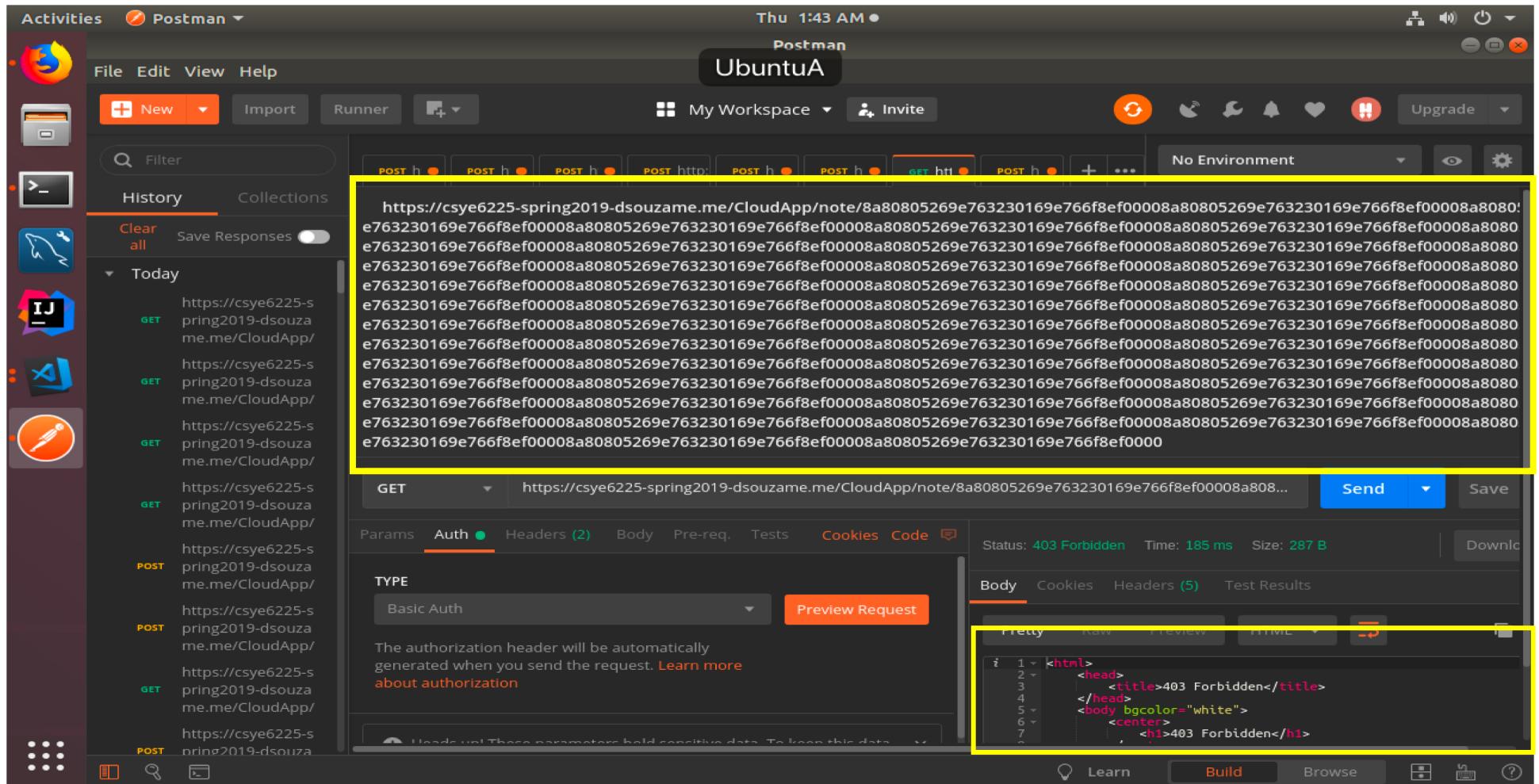
403 Forbidden

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

The screenshot shows the Postman application interface. In the center, a POST request is being made to the URL <https://csye6225-spring2019-dsouzame.me/CloudApp/note/8a80803869e3c6e00169e3f19c440000/attachments>. The 'Body' tab is selected, showing a single key-value pair: 'file' with a 'Choose Files' button. The response status is 403 Forbidden, with a response size of 287 B. The response body is displayed in a code block, which is highlighted with a yellow border:

```
i 1 <html>
2 <head>
3   <title>403 Forbidden</title>
4 </head>
5 <body background="white">
6   <center>
7     <h1>403 Forbidden</h1>
8   </center>
9 
10 </body>
11 </html>
```

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.

```
root@kali:~# nmap csye6225-spring2019-dsouzame.me -F
Starting Nmap 7.70 ( https://nmap.org ) at 2019-04-03 16:49 UTC
Nmap scan report for csye6225-spring2019-dsouzame.me (34.202.212.219)
Host is up (0.0080s latency).
Other addresses for csye6225-spring2019-dsouzame.me (not scanned): 34.220.229.56
rDNS record for 34.202.212.219: ec2-34-202-212-219.compute-1.amazonaws.com → Public IP Address
Not shown: 96 filtered ports
PORT      STATE SERVICE
22/tcp    closed ssh
80/tcp    open  http → All available PORTs
443/tcp   open  https
8080/tcp  closed http-proxy
Nmap done: 1 IP address (1 host up) scanned in 1.92 seconds
```

```
root@kali:~# nmap csye6225-spring2019-dsouzame.me -F
Starting Nmap 7.70 ( https://nmap.org ) at 2019-04-04 14:55 UTC
Nmap scan report for csye6225-spring2019-dsouzame.me (34.235.245.185)
Host is up (0.0073s latency).
Other addresses for csye6225-spring2019-dsouzame.me (not scanned): 34.197.141.66
rDNS record for 34.235.245.185: ec2-34-235-245-185.compute-1.amazonaws.com
Not shown: 98 filtered ports
PORT      STATE SERVICE
443/tcp   open  https → When WAF is enabled
8080/tcp  open  http-proxy → we can see only the
                           open ports
```