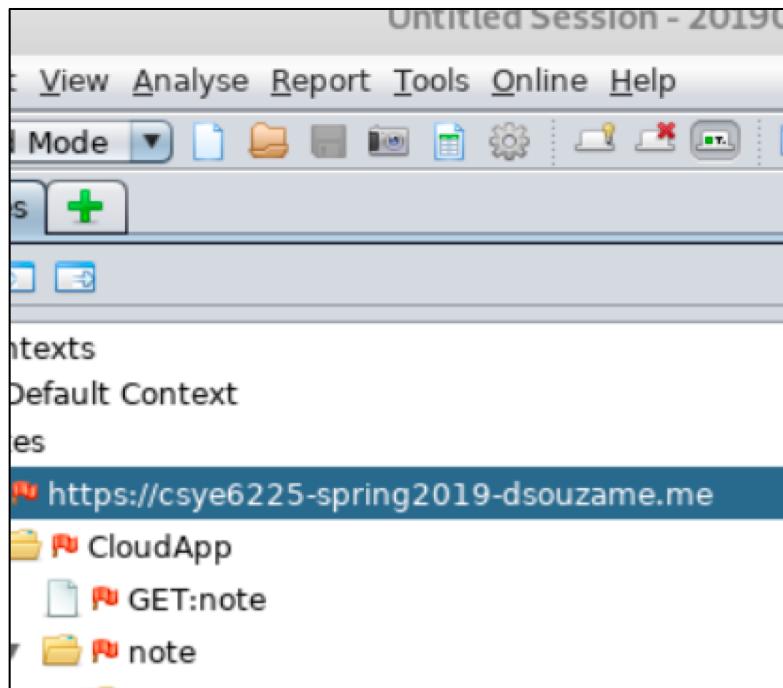


Penetration Testing

OWASP ZAP

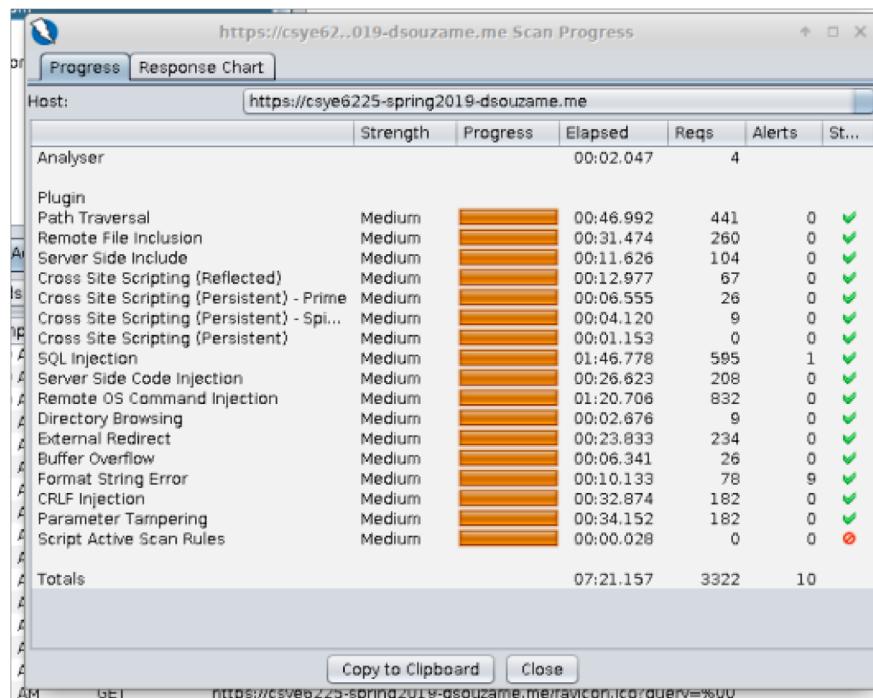
- The OWASP Zed Attack Proxy is a Java-based tool that comes with an intuitive graphical interface.



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.

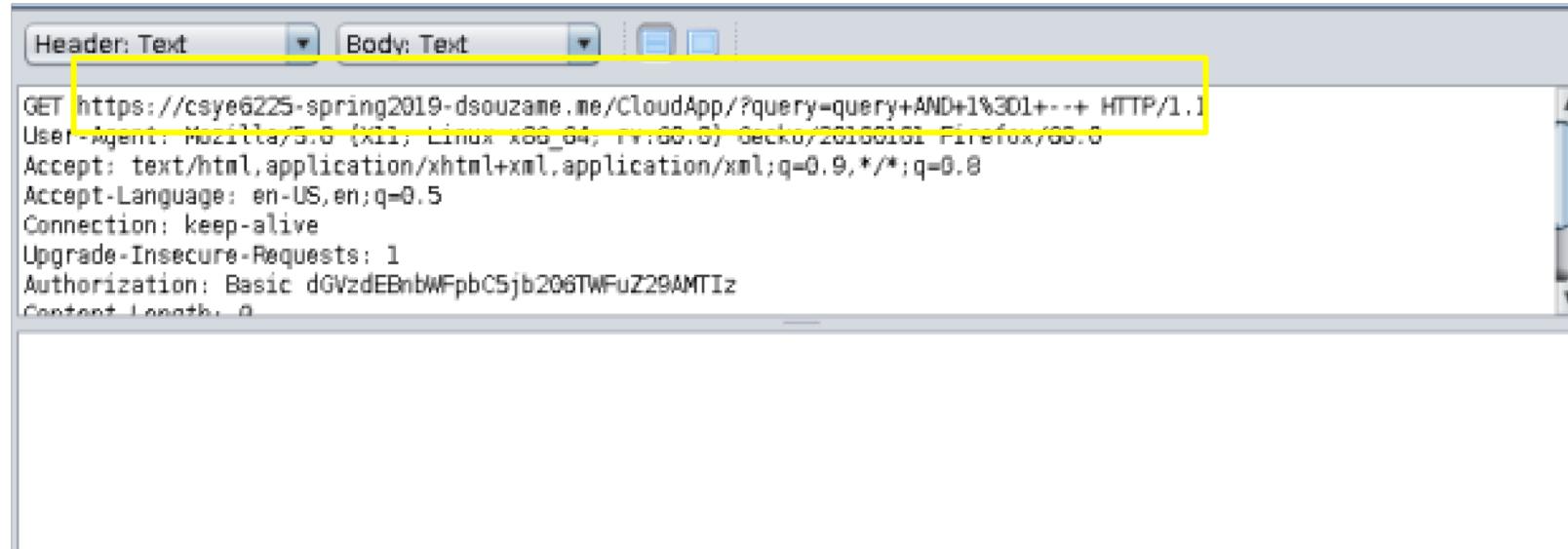
Active Scan



Alert Message



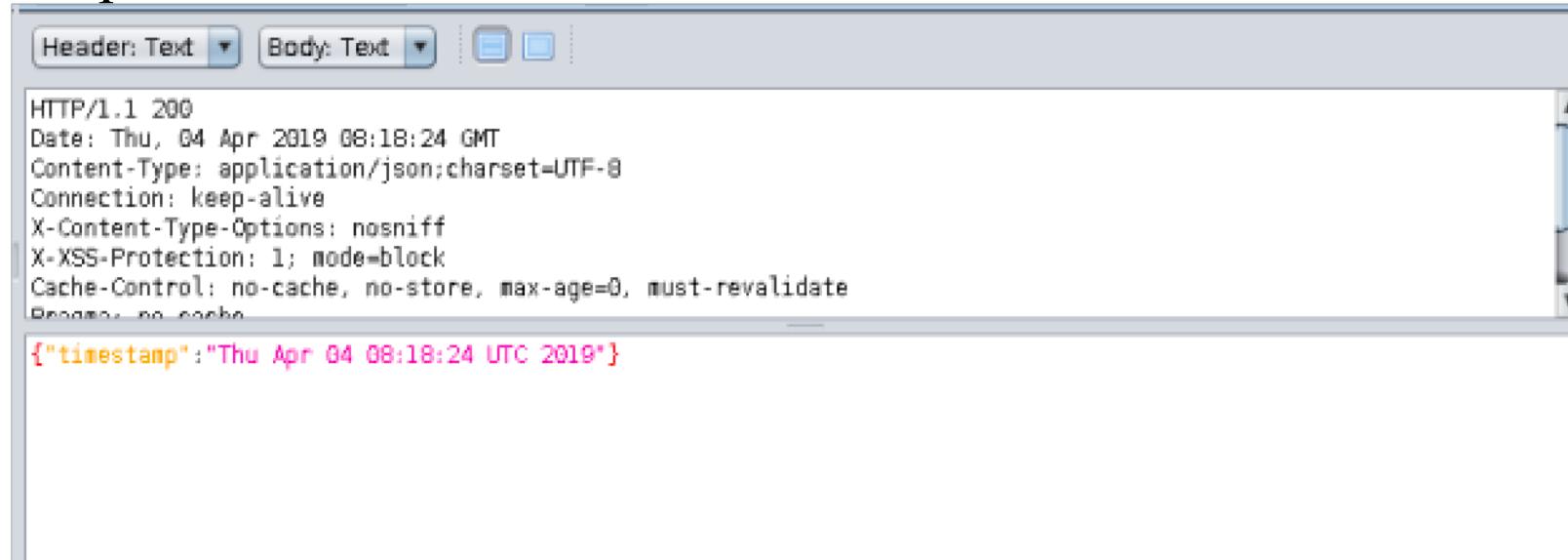
SQL Injection Request



The screenshot shows a network traffic capture interface with two tabs: "Header: Text" and "Body: Text". The "Header: Text" tab is selected and highlighted with a yellow box. It displays the following HTTP request headers:

```
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:68.0) Gecko/20100101 Firefox/68.0
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



The screenshot shows a network traffic capture interface with two tabs: "Header: Text" and "Body: Text". The "Header: Text" tab is selected and displays the following HTTP response headers:

```
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
```

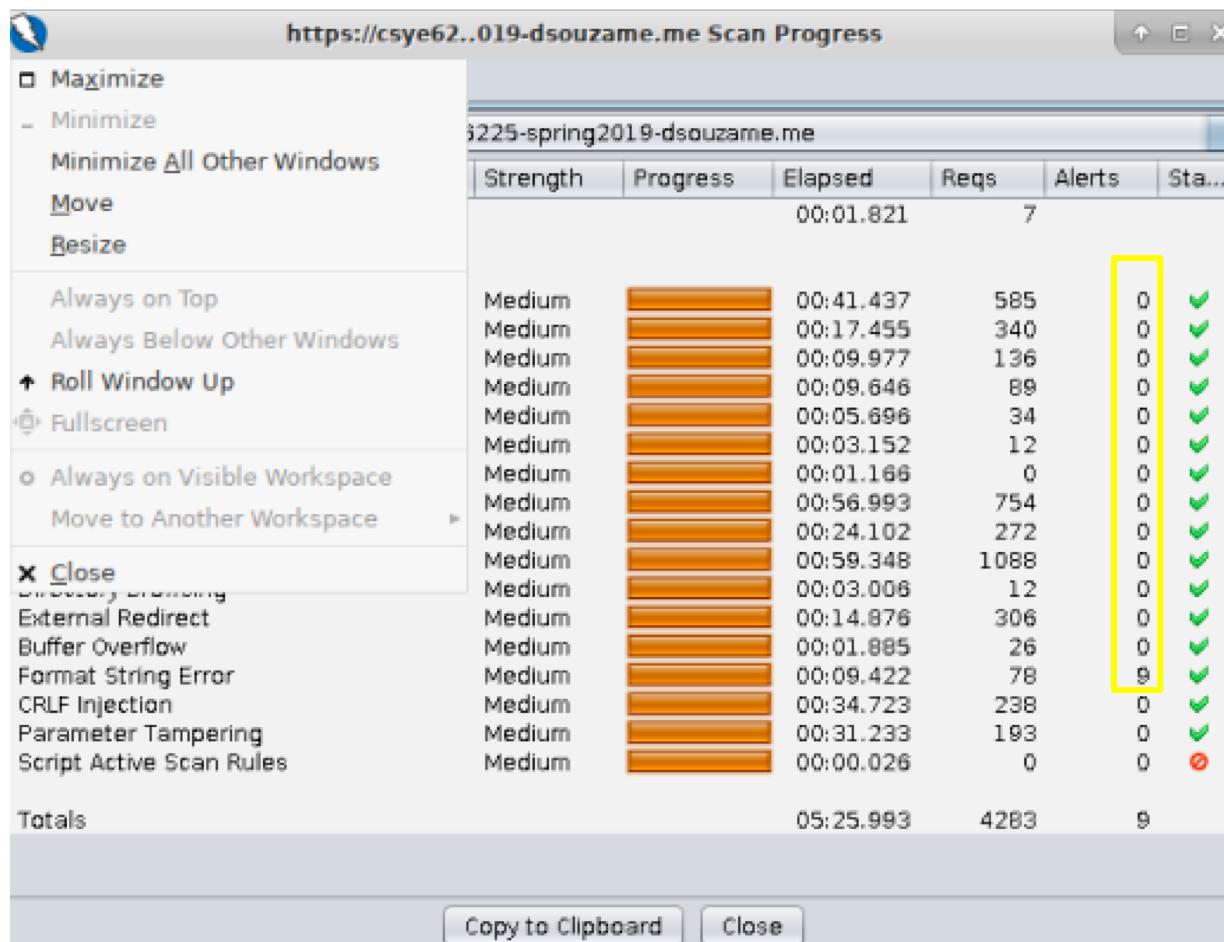
The "Body: Text" tab shows the JSON response body:

```
{"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 a Postman request to `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 of the response is a JSON object:

```
{  
  "user": {  
    "user": "test@gmail.com",  
    "password": "Mango@123"  
  }  
}
```

With WAF

The screenshot shows a Postman request to `https://csye6225-spring2019-dsouzame.me/CloudApp/`. The response status is `403 Forbidden`.

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

The screenshot shows the Postman application interface. The left sidebar displays a history of API requests. The main workspace shows a request for a URL that is excessively long, resulting in a 403 Forbidden error. The request details and response body are visible.

Request URL: `https://csye6225-spring2019-dsouzame.me/CloudApp/note/8a80805269e763230169e766f8ef00008a80805269e763230169e766f8ef00008a8080...e763230169e766f8ef00008a80805269e763230169e766f8ef00008a80805269e763230169e766f8ef00008a8080`

Status: 403 Forbidden

Response Body (Pretty):

```
i 1 > <html>
2 >   <head>
3 >     <title>403 Forbidden</title>
4 >   </head>
5 >   <body bgcolor="white">
6 >     <center>
7 >       <h1>403 Forbidden</h1>
```

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 contains the following HTML:

```
i 1 <html>
2 <head>
3   <title>403 Forbidden</title>
4 </head>
5 <body bgcolor="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.

```
nmap done. 0/11 addresses (0 hosts up) scanned in 0.11 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
8080/tcp   open  http-proxy
```