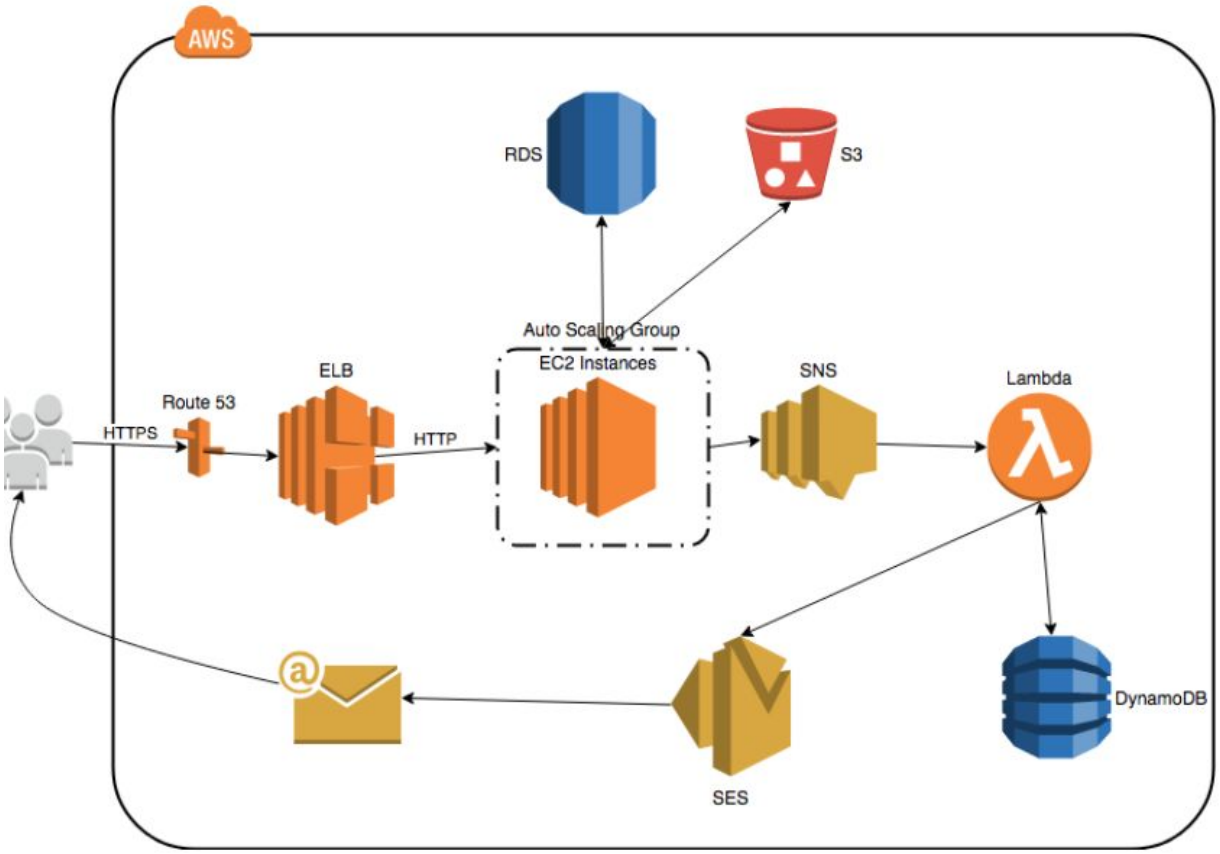
Report on Penetration Testing on the Note taking App(Web API)

Penetration testing :

A **penetration test**, colloquially known as a **pen test**, is an authorized simulated cyber attack on a computer system, performed to evaluate the security of the system. The test is performed to identify both weaknesses (also referred to as vulnerabilities), including the potential for unauthorized parties to gain access to the system's features and data, as well as strengths, enabling a full risk assessment to be completed.

The following diagram describes the complete overview of the developed Web API:



Therefore, to check the security of our built web API, we are using Kali Linux as the penetration testing tool.

Kali Linux:

Kali Linux is a Debian-based Linux distribution aimed at advanced Penetration Testing and Security Auditing. Kali contains several hundred tools which are geared towards various information security tasks, such as Penetration Testing, Security research, Computer Forensics and Reverse Engineering. Kali Linux is developed, funded and maintained by Offensive Security, a leading information security training company.

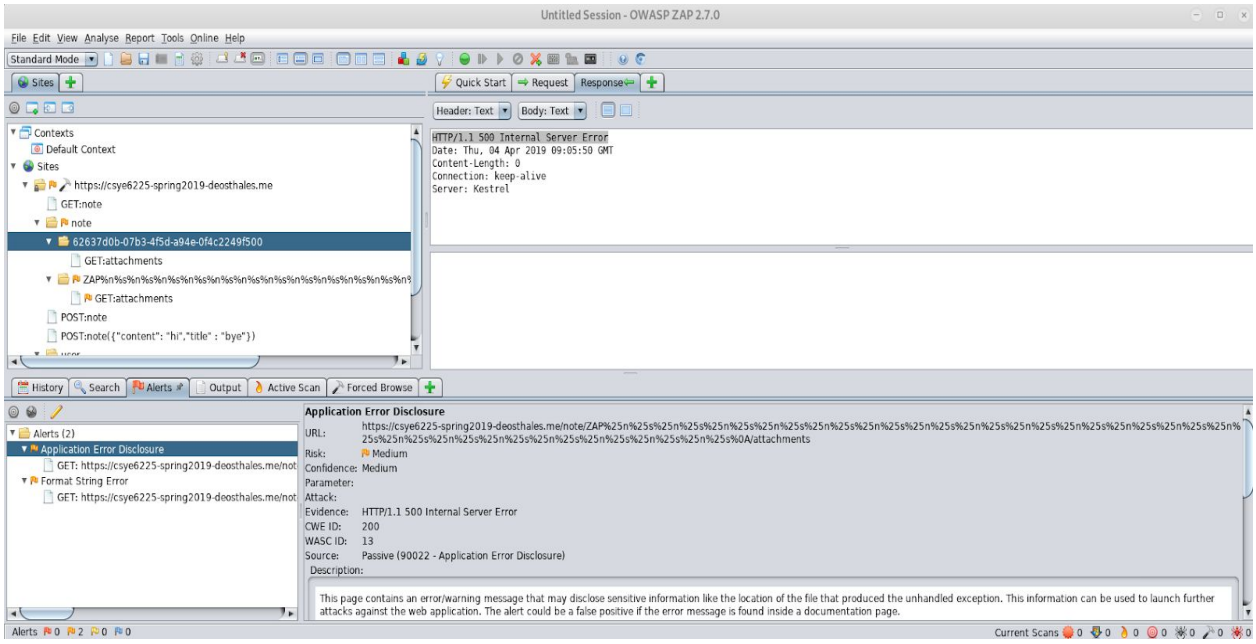
WAF(Web Application Firewall):

- AWS WAF is a web application firewall that helps protect your web applications from common web exploits that could affect application availability, compromise security, or consume excessive resources.
- AWS WAF gives you control over which traffic to allow or block to your web applications by defining customizable web security rules.
- You can use AWS WAF to create custom rules that block common attack patterns, such as SQL injection or cross-site scripting, and rules that are designed for your specific application.
- New rules can be deployed within minutes, letting you respond quickly to changing traffic patterns. Also, AWS WAF includes a full-featured API that you can use to automate the creation, deployment, and maintenance of web security rules.

Without AWS Web Application Firewall:

The following are the findings without using AWS WAF:

- There are two alerts when not using the WAF.
- The alerts are:
    1. Application Error Disclosure
    2. Format String Error



Attack Vendor:

1.ZAP-OWASP(With Web Application Firewall):

The Note Taking App endpoints would be entered in the attack field, and the Attack button would be pressed.The Zap has two steps,

1. Crawling - Carried out by Spider. Beginning from the supplied URL, the spider explore the app to determine all of the hyperlinks within it. The Spider tab at the bottom of the ZAP window will display the links as they are found. A passive scan will be carried out simultaneously in which is a passive scan is a harmless test that looks only for the responses and checks them against known vulnerabilities.

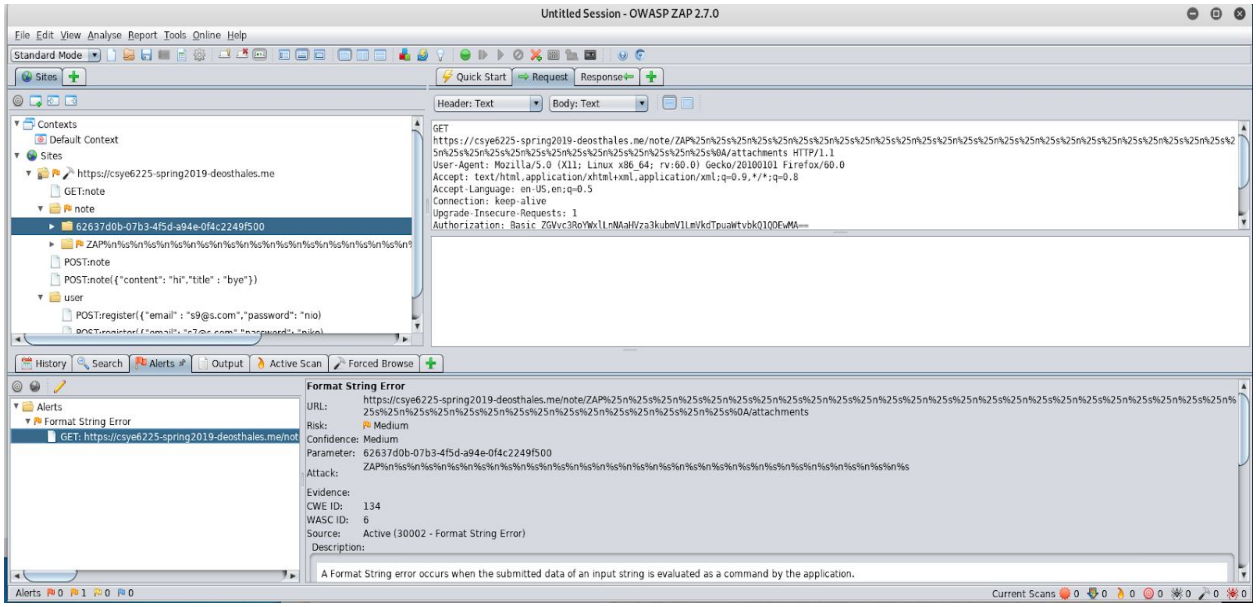
2. Active Scan - The Active Scan will launch, once the crawl is completed. ZAP will launch a variety of attack scenarios at the URLs listed in the Spider tab. Once the active scan has finished, the results will be displayed in the Alerts tab. This will contain all of the security issues found during both the Spider and Active scan. The alerts will be flagged according to their risk - red for High Priority, and green and yellow for Medium to Low Priority. Reports can be generated in multiple formats.

ZAP does not handle authentication by default. This means that any links requiring authentication will not be found or scanned. The Session Properties would be configured to include the login details that will allow ZAP access to the secure areas of your site.

The following are the findings when WAF is being used:

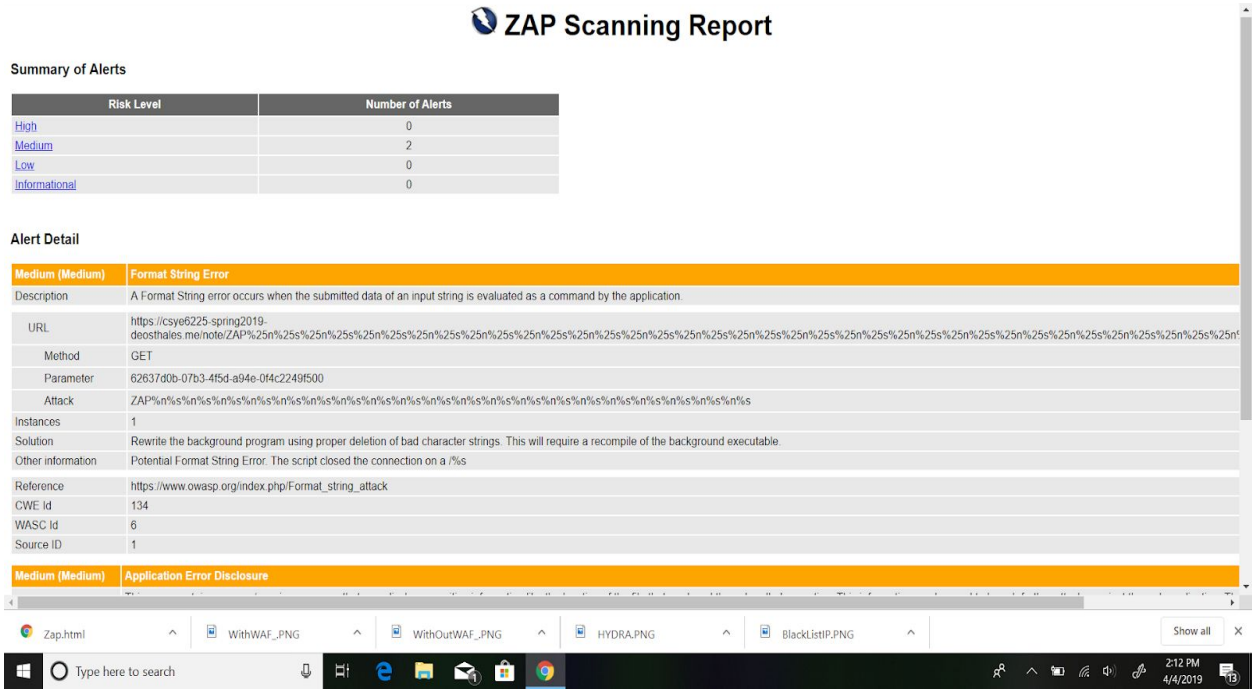
- There is one alert when using the WAF:

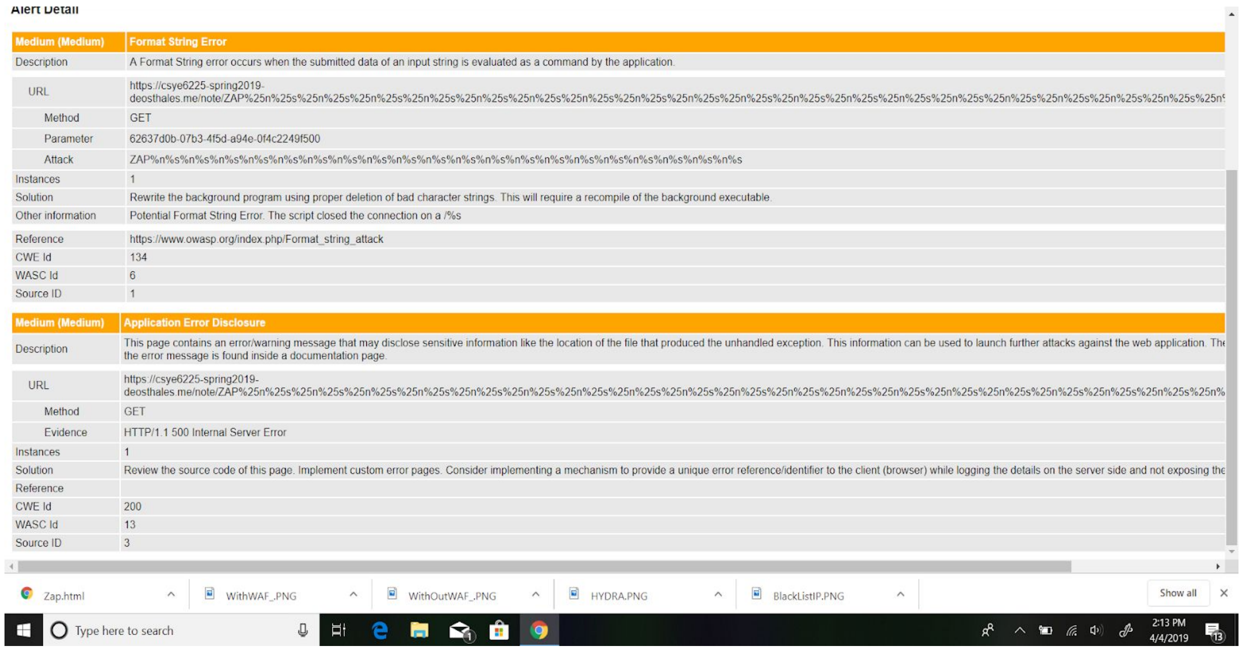
1. The alert is Format String Error



ZAP Scanning Report:

The detailed description of the ZAP-OWASP alerts can be found here:





Alert Detail

Medium (Medium)	Format String Error
Description	A Format String error occurs when the submitted data of an input string is evaluated as a command by the application.
URL	https://csye6225-spring2019-deosthales.me/note/ZAP%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%
Method	GET
Parameter	62637d0b-07b3-4f5d-a94e-0f4c2249f500
Attack	ZAP%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s
Instances	1
Solution	Rewrite the background program using proper deletion of bad character strings. This will require a recompile of the background executable.
Other information	Potential Format String Error. The script closed the connection on a /%s
Reference	https://www.owasp.org/index.php/Format_string_attack
CWE Id	134
WASC Id	6
Source ID	1

Medium (Medium)	Application Error Disclosure
Description	This page contains an error/warning message that may disclose sensitive information like the location of the file that produced the unhandled exception. This information can be used to launch further attacks against the web application. Th the error message is found inside a documentation page.
URL	https://csye6225-spring2019-deosthales.me/note/ZAP%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%
Method	GET
Evidence	HTTP/1.1 500 Internal Server Error
Instances	1
Solution	Review the source code of this page. Implement custom error pages. Consider implementing a mechanism to provide a unique error reference/identifier to the client (browser) while logging the details on the server side and not exposing the
Reference	
CWE Id	200
WASC Id	13
Source ID	3

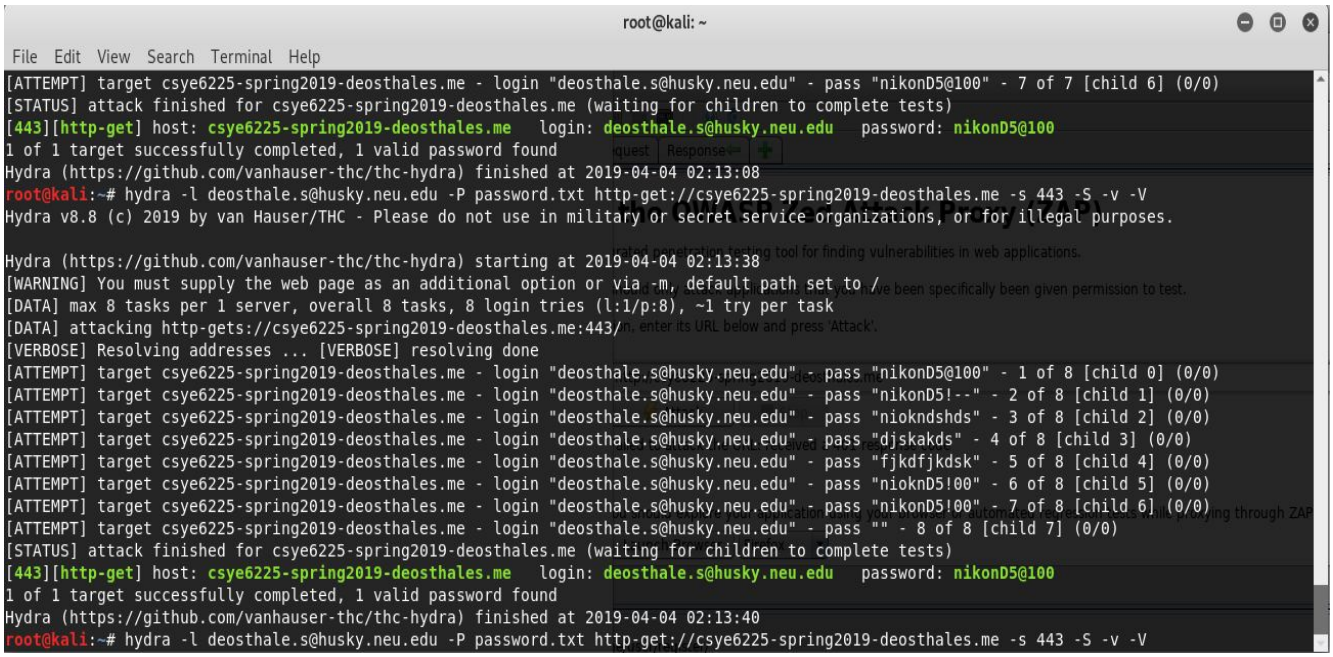
Vector Significance: Zed Attack Proxy is an easy-to-use integrated penetration testing tool for finding vulnerabilities in web applications. It is a Java interface. Zap functions as a web proxy as in it inspects the traffic from the client to the server. Zap can inspect the request and, response, and look for various security issues, like missing security headers.

2. *Hydra Kali:*

Hydra is a parallelized login cracker which supports numerous protocols to attack. It is very fast and flexible, and new modules are easy to add. This tool makes it possible for researchers and security consultants to show how easy it would be to gain unauthorized access to a system remotely.

Result :Hydra Kali is able to expose the user's password.

A list of passwords built by user when given to the hydra and will likely be combined with other known (easy passwords, such as 'password1, password2' etc) to carry out a brute force attack against the Note Taking App user authentication. Depending on the processing speed of the computer, Internet connection the brute force methodology will systematically go through each password until the correct one is discovered, if one exists.



Vector Significance: Hydra is a well-known tool for dictionary attacks on various devices which can support many different services. As the majority of users would have weak passwords and all too often they are easily guessed. Hydra serves to launch a relentless barrage of passwords at a login to guess the password. A little bit of social engineering and the chances of finding the correct password for a user are multiplied with Hydra.

3. *BlackList IP:*

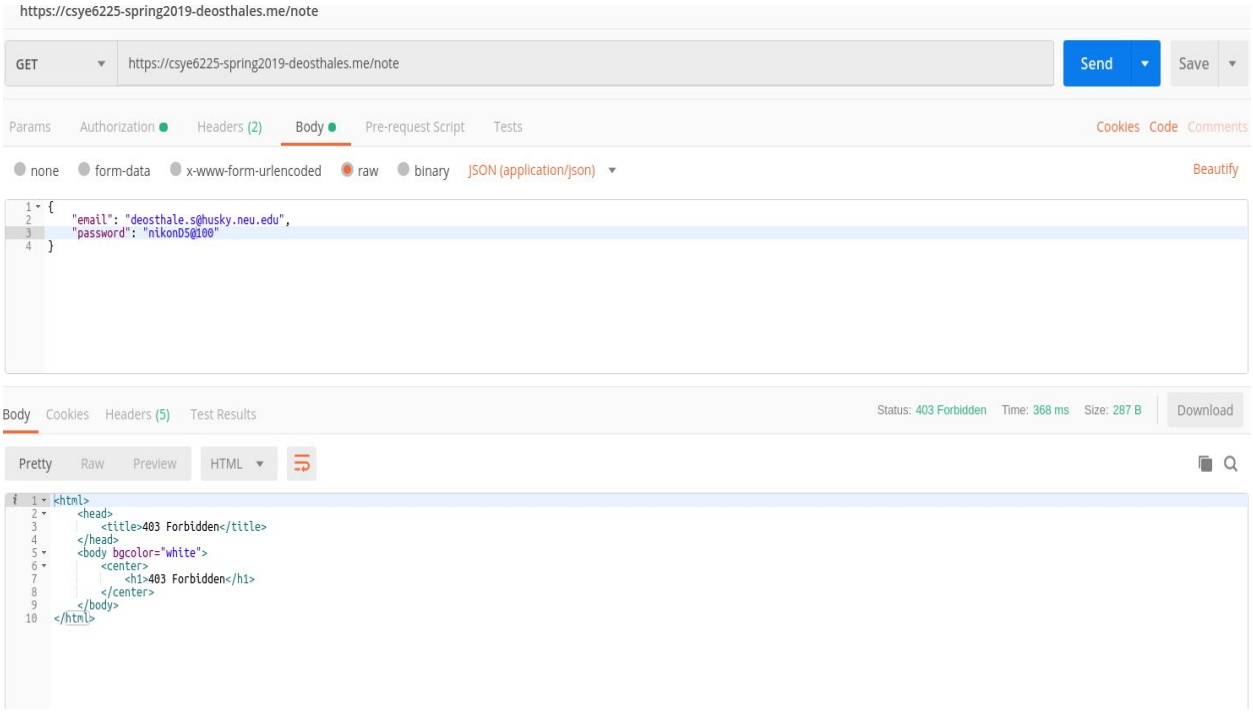
Blocking/BlackListing IP Addresses That Submit Bad Requests is the third attack vector we have used.

Using AWS Lambda, we can set a threshold of how many bad requests per minute our web application will tolerate from a given IP address. A bad request is one for which your CloudFront origin returns one of the following HTTP 40x status codes:

- 400, Bad Request
- 403, Forbidden
- 404, Not Found
- 405, Method Not Allowed

If users (based on IP addresses) exceed this error code threshold, Lambda automatically updates the AWS WAF rules to block IP addresses and specify for how long requests from those IP addresses should be blocked.

The web API cannot be accessed through the IP mentioned below or the below mentioned IP has been blacklisted.



Vector Significance:

Using AWS Lambda, we can set a threshold of how many bad requests per minute our web application will tolerate from a given IP address. A bad request is one for which your CloudFront origin returns one of the following HTTP 40x status codes:

- 400, Bad Request
- 403, Forbidden
- 404, Not Found
- 405, Method Not Allowed

If users (based on IP addresses) exceed this error code threshold, Lambda automatically updates the AWS WAF rules to block IP addresses and specify for how long requests from those IP addresses should be blocked.