REPORT

Attacks on web application with and without the AWS WAF

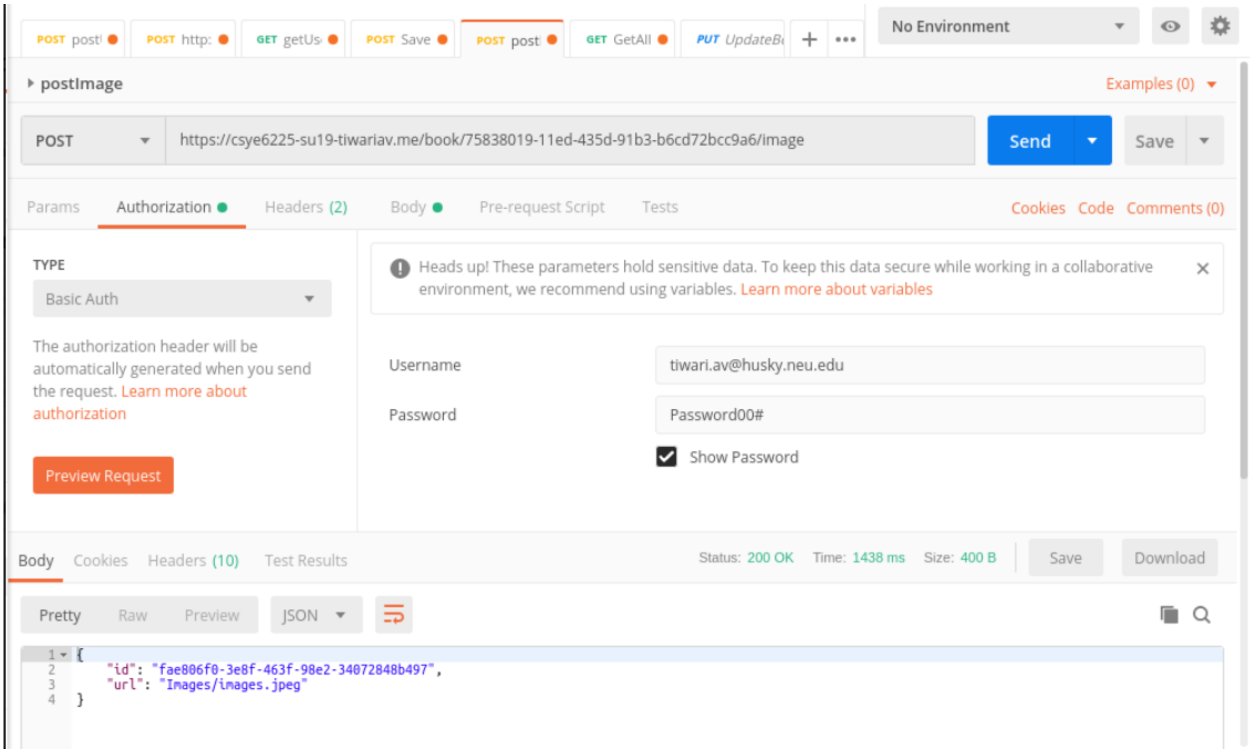
Attack Vector 1: File attachment size is large

Reason:

There is a probability that when a client request for file upload, they don't know about the document size that is permitted. Likewise, at some point they accidentally upload an image that isn't allowed. This outcomes in affecting the performance and efficiency of the application. So, we should prevent the clients from uploading such files utilizing firewall. This will keep the application ready for action proficiently. We have exhibited this by considering the request body size restrictions.

Testing:

We are uploading a file of __________ as our attachment to the book. It will give us the file size error. In this test, we pass large sized file, these files should not be attached to the book because they might induce considerable latency on our instances.



POST https://csye6225-su19-tiwariav.me/book/75838019-11ed-435d-91b3-b6cd72bcc9a6/image

TYPE: Basic Auth

The authorization header will be automatically generated when you send the request. Learn more about authorization

Heads up! These parameters hold sensitive data. To keep this data secure while working in a collaborative environment, we recommend using variables. Learn more about variables

Username: tiwari.av@husky.neu.edu

Password: Password00#

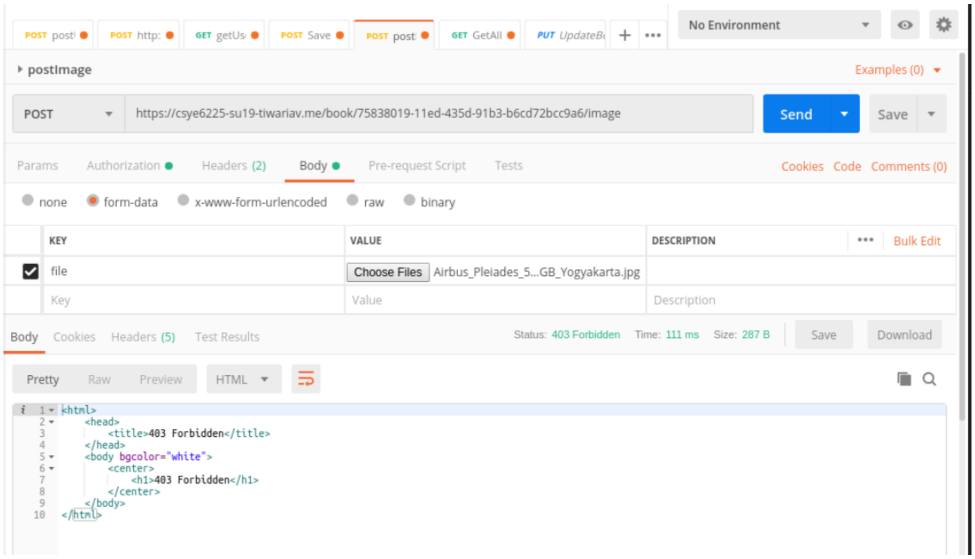
☑ Show Password

Status: 200 OK Time: 1438 ms Size: 400 B

```
{
    "id": "fae806f0-3e8f-463f-98e2-34072848b497",
    "url": "Images/images.jpeg"
}
```

Result:

Post Web Application Firewall setup, the firewall checks on the request body size and restricts user from uploading big files before letting the request reach the application.



postImage

POST https://csye6225-su19-tiwariav.me/book/75838019-11ed-435d-91b3-b6cd72bcc9a6/image

Body: ○ none ● form-data ○ x-www-form-urlencoded ○ raw ○ binary

	KEY	VALUE	DESCRIPTION
☑	file	Choose Files Airbus_Pleiades_5...GB_Yogyakarta.jpg	
	Key	Value	Description

Body Cookies Headers (5) Test Results — Status: 403 Forbidden Time: 111 ms Size: 287 B

```
<html>
    <head>
        <title>403 Forbidden</title>
    </head>
    <body bgcolor="white">
        <center>
            <h1>403 Forbidden</h1>
        </center>
    </body>
</html>
```

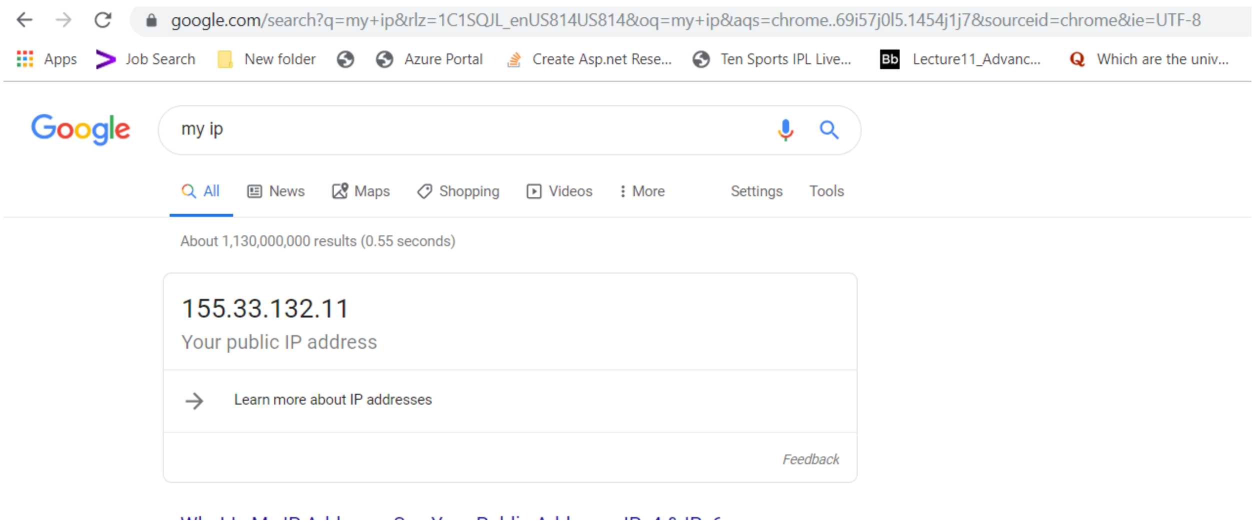
Attack Vector 2: Blacklisted the unauthorized IP Address

Reason:

Nowadays applications are very prone to getting hacked or be a victim of malicious data and unwanted requests so as to leak the confidential information. The IP addresses from where such attempts are being made should be monitored and blocked.

Testing :

We will run the application with your IP and domain name of the application. If the application returns a message in the json format, then your IP address isn't in the blocked IP address list. But, if the application returns a "403 Forbidden" message, your IP has been hindered by the server.



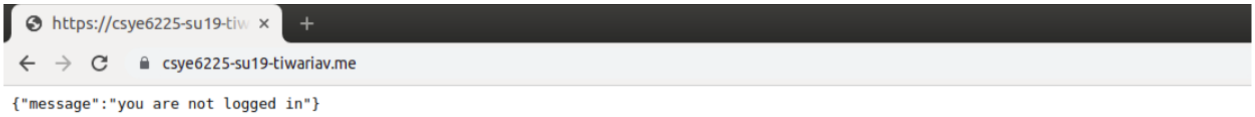
google.com/search?q=my+ip&rlz=1C1SQJL_enUS814US814&oq=my+ip&aqs=chrome..69i57j0l5.1454j1j7&sourceid=chrome&ie=UTF-8

my ip

About 1,130,000,000 results (0.55 seconds)

155.33.132.11

Your public IP address

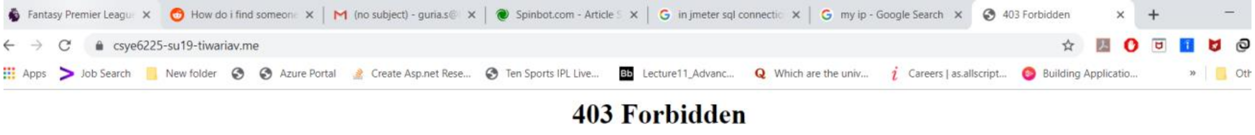


```
{"message":"you are not logged in"}
```

Result:

Using AWS WAF, we were able to block the unwanted users by putting IP addresses or ranges of IP addresses to the block list. The requests and fake transactions from such IPs are blocked.

Here, IP address is the one which is put under IP blocked list.



403 Forbidden

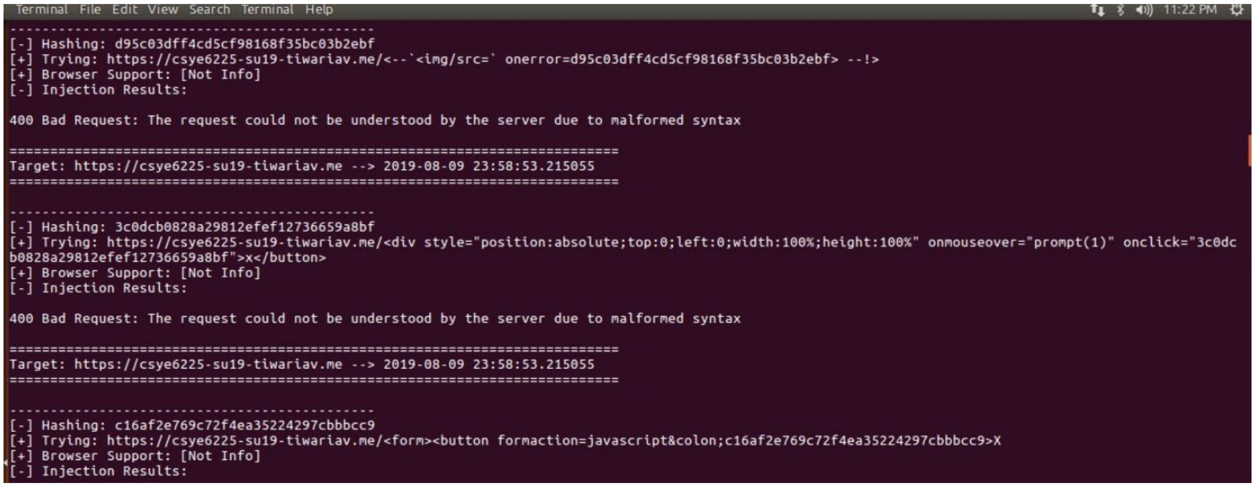
Attack 3 : Cross Site Scripting

Reason:

Cross-site scripting (XSS) is a type of computer security vulnerability typically found in web applications. It is a way of bypassing the SOP concept in a vulnerable web application. XSS enables attackers to inject client-side scripts into web pages viewed by other users. A cross-site scripting vulnerability may be used by attackers to bypass access controls such as the same-origin policy.

Testing:

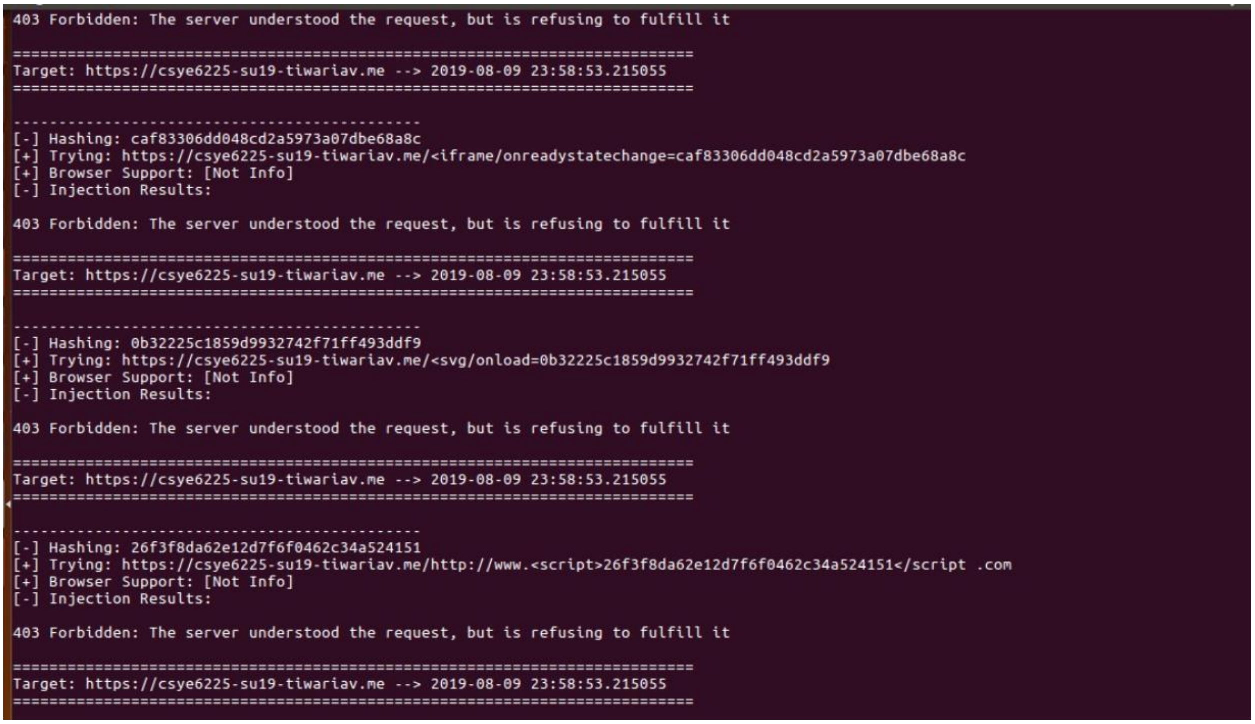
In this case, we will try to inject the application by modifying the query string and attack the domain name. The request is shown as bad request due to error in syntax but the attack is not handled by the application.



```
---------------------------------------------
[-] Hashing: d95c03dff4cd5cf98168f35bc03b2ebf
[+] Trying: https://csye6225-su19-tiwariav.me/<--`<img/src=` onerror=d95c03dff4cd5cf98168f35bc03b2ebf> --!>
[+] Browser Support: [Not Info]
[-] Injection Results:

400 Bad Request: The request could not be understood by the server due to malformed syntax

===========================================================================
Target: https://csye6225-su19-tiwariav.me --> 2019-08-09 23:58:53.215055
===========================================================================

---------------------------------------------
[-] Hashing: 3c0dcb0828a29812efef12736659a8bf
[+] Trying: https://csye6225-su19-tiwariav.me/<div style="position:absolute;top:0;left:0;width:100%;height:100%" onmouseover="prompt(1)" onclick="3c0dc
b0828a29812efef12736659a8bf">x</button>
[+] Browser Support: [Not Info]
[-] Injection Results:

400 Bad Request: The request could not be understood by the server due to malformed syntax

===========================================================================
Target: https://csye6225-su19-tiwariav.me --> 2019-08-09 23:58:53.215055
===========================================================================

---------------------------------------------
[-] Hashing: c16af2e769c72f4ea35224297cbbbcc9
[+] Trying: https://csye6225-su19-tiwariav.me/<form><button formaction=javascript&colon;c16af2e769c72f4ea35224297cbbbcc9>X
[+] Browser Support: [Not Info]
[-] Injection Results:
```

Result:

The attack is handled by the application successfully and 403 forbidden error message is shown, which prevents hackers from hitting the application with unwanted query strings.



```
403 Forbidden: The server understood the request, but is refusing to fulfill it

===========================================================================
Target: https://csye6225-su19-tiwariav.me --> 2019-08-09 23:58:53.215055
===========================================================================

---------------------------------------------
[-] Hashing: caf83306dd048cd2a5973a07dbe68a8c
[+] Trying: https://csye6225-su19-tiwariav.me/<iframe/onreadystatechange=caf83306dd048cd2a5973a07dbe68a8c
[+] Browser Support: [Not Info]
[-] Injection Results:

403 Forbidden: The server understood the request, but is refusing to fulfill it

===========================================================================
Target: https://csye6225-su19-tiwariav.me --> 2019-08-09 23:58:53.215055
===========================================================================

---------------------------------------------
[-] Hashing: 0b32225c1859d9932742f71ff493ddf9
[+] Trying: https://csye6225-su19-tiwariav.me/<svg/onload=0b32225c1859d9932742f71ff493ddf9
[+] Browser Support: [Not Info]
[-] Injection Results:

403 Forbidden: The server understood the request, but is refusing to fulfill it

===========================================================================
Target: https://csye6225-su19-tiwariav.me --> 2019-08-09 23:58:53.215055
===========================================================================

---------------------------------------------
[-] Hashing: 26f3f8da62e12d7f6f0462c34a524151
[+] Trying: https://csye6225-su19-tiwariav.me/http://www.<script>26f3f8da62e12d7f6f0462c34a524151</script .com
[+] Browser Support: [Not Info]
[-] Injection Results:

403 Forbidden: The server understood the request, but is refusing to fulfill it

===========================================================================
Target: https://csye6225-su19-tiwariav.me --> 2019-08-09 23:58:53.215055
===========================================================================
```