

# **CSYE6225**

Summer 2019

Penetration Testing and Web Application Firewall

Submitted by:

Ishita Chausalkar(001448216)

Prathamesh Tambe(001494644)

Jiawei Zhao(001495711)

## 1. IP Blacklisting-

My public IP:

```
ishita@ubuntu:~/ccwebapp/infrastructure/aws/cloudformation$ curl ifconfig.me
155.33.133.27ishita@ubuntu:~/ccwebapp/infrastructure/aws/cloudformation$
```

Running the dig command on my domain:

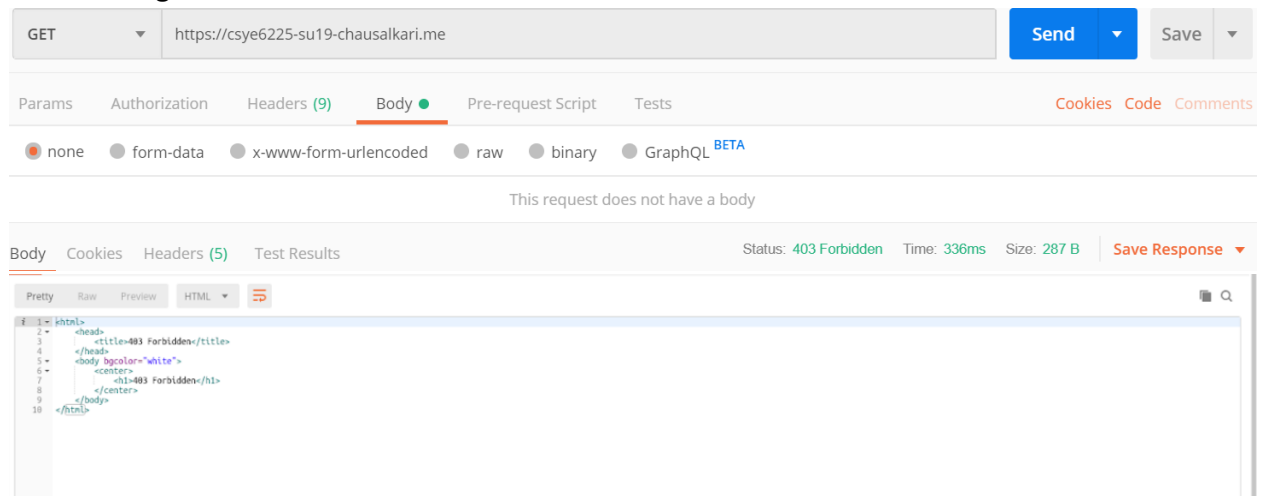
```
ishita@ubuntu:~$ curl ifconfig.me
155.33.133.27ishita@ubuntu:~$ dig www.csye6225-su19-chausalkari.me

; <<>> DiG 9.11.3-1ubuntu1.8-Ubuntu <<>> www.csye6225-su19-chausalkari.me
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 55052
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;www.csye6225-su19-chausalkari.me. IN      A

;; Query time: 248 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Fri Aug 09 20:41:36 PDT 2019
;; MSG SIZE rcvd: 61
```

After adding IP to blacklist in the rules of the WAF :



The screenshot shows the AWS IAM console interface. At the top, a GET request to `https://csye6225-su19-chausalkari.me` is shown. The request is blocked by WAF with a 403 Forbidden status. The response body shows an HTML error page with the title `403 Forbidden` and the message `403 Forbidden`.

Result: My IP address has been blacklisted.

Why IP Blacklisting?

Attackers choose this attack vector as they access hundreds of valid usernames and passwords combinations for credential stuffing, default administrator account list and dictionary attack tools.

## 2. Attack Vector- Injection:

By inserting malicious data into the SQL queries, an attacker can alter the intent of requests and cause unexpected harmful result.

SELECT \* from user;

```
Database changed
mysql> select * from user;
+----+-----+-----+-----+
| id | username | password | cdate |
+----+-----+-----+-----+
| 1 | ishitachausalkar01@gmail.com | $2b$10$sggEaHfb9UX0hTXPoWAhSuqQK0I4eJ0VpS108AfFkqjRQxqN00Mu | 2019-06-03 17:47:29 |
| 2 | ishitachausalkar01@gmail.com | $2b$10$/ZMDfKzsf4yo7xgHix0Vde0TKbmVMSc93eJ9Fp3Kss3kbAIAaZzq | 2019-06-06 17:32:17 |
| 3 | chausalkar.@husky.neu.edu | $2b$10$3TebDEZ.RzQnRn1jmRnh0..oT5x.YSeok6IwE63af4pzoX4WYP0Ci | 2019-06-06 17:41:47 |
| 4 | chausalkar.i@husky.neu.edu | $2b$10$gQ0UvltLVUNww87IVrKe9exqMfzmsvjh9iLRZ4bsNJWbHxKuQHfQ2 | 2019-06-06 17:42:01 |
| 5 | sumit@gmail.com | $2b$10$D5jy/KmH0iWiPAgTPK3uFuasgB5BsnqXgCMTdWwADK4KU0oHekaYq | 2019-06-07 12:16:42 |
| 6 | ish01@gmail.com | $2b$10$3BEDohhU8TN0IRL084zqudg/qg8K6xzbjs1WooZIQFj77sdVM73K | 2019-06-13 15:28:38 |
| 7 | prath@gmail.com | $2b$10$w1PZN7pPDVwHV00bQx90ee0XNm7ZMcK2xSgG8G7vn8ZbFk1GVjA82 | 2019-06-28 17:08:17 |
| 8 | prathamesh@gmail.com | $2b$10$8T6yWSQkuBB8lQ5.EXw1uX0pfSAspwACLGv/6BakbXIjw2RtcBZe | 2019-07-01 14:34:42 |
+----+-----+-----+-----+
8 rows in set (0.00 sec)
```

SELECT \* from user where id=100;

```
mysql> mysql> select * from user where id=100;
ERROR 1146 (42S02): Table 'books.userom' doesn't exist
mysql>
```

SELECT \* from user where id=100 OR 1=1;

This will give a result as we have ORed condition 1=1 which will always be true

```
mysql> select * from user where id=100 or 1=1;
+----+-----+-----+-----+
| id | username | password | cdate |
+----+-----+-----+-----+
| 1 | ishitachausalkar01@gmail.com | $2b$10$sggEaHfb9UX0hTXPoWAhSuqQK0I4eJ0VpS108AfFkqjRQxqN00Mu | 2019-06-03 17:47:29 |
| 2 | ishitachausalkar01@gmail.com | $2b$10$/ZMDfKzsf4yo7xgHix0Vde0TKbmVMSc93eJ9Fp3Kss3kbAIAaZzq | 2019-06-06 17:32:17 |
| 3 | chausalkar.@husky.neu.edu | $2b$10$3TebDEZ.RzQnRn1jmRnh0..oT5x.YSeok6IwE63af4pzoX4WYP0Ci | 2019-06-06 17:41:47 |
| 4 | chausalkar.i@husky.neu.edu | $2b$10$gQ0UvltLVUNww87IVrKe9exqMfzmsvjh9iLRZ4bsNJWbHxKuQHfQ2 | 2019-06-06 17:42:01 |
| 5 | sumit@gmail.com | $2b$10$D5jy/KmH0iWiPAgTPK3uFuasgB5BsnqXgCMTdWwADK4KU0oHekaYq | 2019-06-07 12:16:42 |
| 6 | ish01@gmail.com | $2b$10$3BEDohhU8TN0IRL084zqudg/qg8K6xzbjs1WooZIQFj77sdVM73K | 2019-06-13 15:28:38 |
| 7 | prath@gmail.com | $2b$10$w1PZN7pPDVwHV00bQx90ee0XNm7ZMcK2xSgG8G7vn8ZbFk1GVjA82 | 2019-06-28 17:08:17 |
| 8 | prathamesh@gmail.com | $2b$10$8T6yWSQkuBB8lQ5.EXw1uX0pfSAspwACLGv/6BakbXIjw2RtcBZe | 2019-07-01 14:34:42 |
+----+-----+-----+-----+
8 rows in set (0.02 sec)
```

The attacker can modify the query by using this technique and get anything done like deleting data

Select \* from user where id=10 OR 1=1; Drop Table user;

```
mysql> select * from user OR 1=1; Drop Table user;
ERROR 1064 (42000): You have an error in your SQL syntax;
Query OK, 0 rows affected (0.09 sec)

mysql> select * from user;
ERROR 1146 (42S02): Table 'books.user' doesn't exist
mysql>
```

As we can see the table does not exist. The query went through. Any attacker can use this to insert malicious data and behavior.

Result: The table was deleted even though the query was incorrect. But after using WAF, we can see the domain is stable.

```
lshita@ubuntu:~$ sqlmap -u https://csye6225-su19-chausalkari.me
[+] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local
some no liability and are not responsible for any misuse or damage caused by this program
[*] starting at 16:01:10

[16:01:10] [INFO] testing connection to the target URL
[16:01:10] [INFO] heuristics detected web page charset 'ascii'
[16:01:10] [WARNING] the web server responded with an HTTP error code (502) which could interfere with the results of the tests
[16:01:10] [INFO] checking if the target is protected by some kind of WAF/IPS/IDS
[16:01:10] [INFO] testing if the target URL content is stable
```

## Why Injection?

Attackers use any source of data as an injection vector, environment variables, parameters, external and internal web services and these vulnerabilities are very often in SQL. Injection can result in data loss and denial of access.

### 3. Attack Vector- File size limit:

Firewall rule added to block file attachment size greater than 1 mb.

Without Firewall if the file size is greater than 1Mb, it will give no warning or restriction.

But with the WAF restriction: it will throw error 403 forbidden request

POST https://csye6225-su19-chausalkari.me/486f2010-0e85-4bcd-bc81-280975340bb7

Send Save

Params Authorization Headers (9) Body Pre-request Script Tests Cookies Code Comments

none form-data x-www-form-urlencoded raw binary GraphQL BETA

KEY	VALUE	DESCRIPTION
image		
image	1-wtc-america-architecture-374710.jpg	
Key	Value	Description

Body Cookies Headers (5) Test Results Status: 502 Bad Gateway Time: 169ms Size: 293 B Save Response

```
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 </body>
10</html>
```

## Result:

Since the size is greater than 1 Mb, the web app is throwing error 404 not found. If this limit is not set, the Denial of Service attack can be done by the attackers.

## Why File Size limit?

Attackers can use this type of attack vector to keep the web app channel engaged which can lead to Denial of Service attack leading to low traffic to the web app.