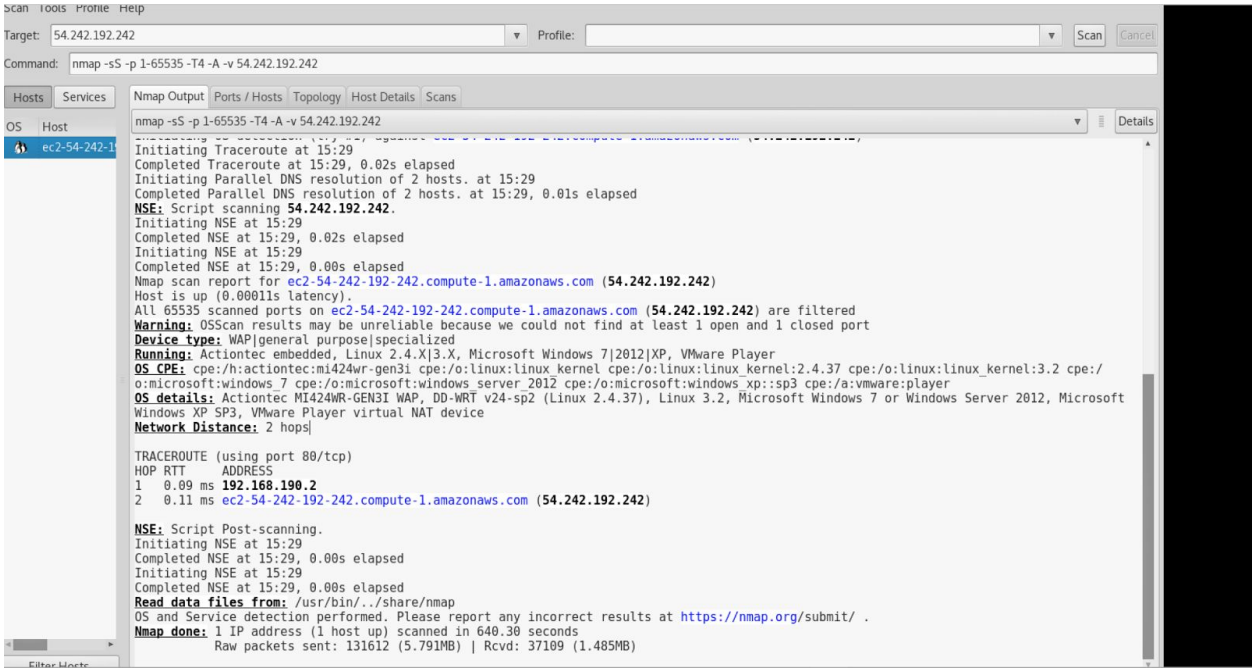
Before Choosing Attack Vector I have tried to ping their EC2 instance and it was not ON,So we can't able to do any kind of attack on the website that is not hosted on cloud:

```
Paras:final paras$ cd
Paras:~ paras$ nslookup www.neu-csye6225-spring2017-team7.me
Server:         75.75.75.75
Address:        75.75.75.75#53

** server can't find www.neu-csye6225-spring2017-team7.me: NXDOMAIN

Paras:~ paras$ nslookup www.neu-csye6225-spring2017-team-7.me
Server:         75.75.75.75
Address:        75.75.75.75#53

Non-authoritative answer:
Name:   www.neu-csye6225-spring2017-team-7.me
Address: 34.204.71.161

Paras:~ paras$ ping 34.204.71.161
PING 34.204.71.161 (34.204.71.161): 56 data bytes
Request timeout for icmp_seq 0
Request timeout for icmp_seq 1
Request timeout for icmp_seq 2
Request timeout for icmp_seq 3
Request timeout for icmp_seq 4
Request timeout for icmp_seq 5
Request timeout for icmp_seq 6
Request timeout for icmp_seq 7
Request timeout for icmp_seq 8
^C
--- 34.204.71.161 ping statistics ---
10 packets transmitted, 0 packets received, 100.0% packet loss
Paras:~ paras$
```

Attack Vectors:

1. NMAP:("Network Mapper") is a free and open source (license) utility for network discovery and security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime.

Result:



~I have chosen this Attack vector to get the open ports in their security Group and this will help me in making their Website weak as I will plan my attack on the basis of open port.

~Steps Developers should take:

Open very less port, the ports that are useful like 80 or 443 and Its better to have the security at hypervisor level as well.

2) **Burp Suite as Attack Vector**

Burp Suite is one of the popular tools for performing security assessment/testing for web applications. It can be used to run both manual and automated scans and consist of different tools such as a proxyserver, a web spider, scanner, intruder, repeater, sequencer, decoder, collaborator and extender. Among all these functionalities intruder and scanner are most commonly use tools which can perform automated attacks on web applications.

Both these tools (intruder and scanner) use a **default set of attack vectors**(Fig. 1) to test and detectvulnerabilities like SQL Injection, Cross Site Scripting(XSS) and many

more

steps performed :-

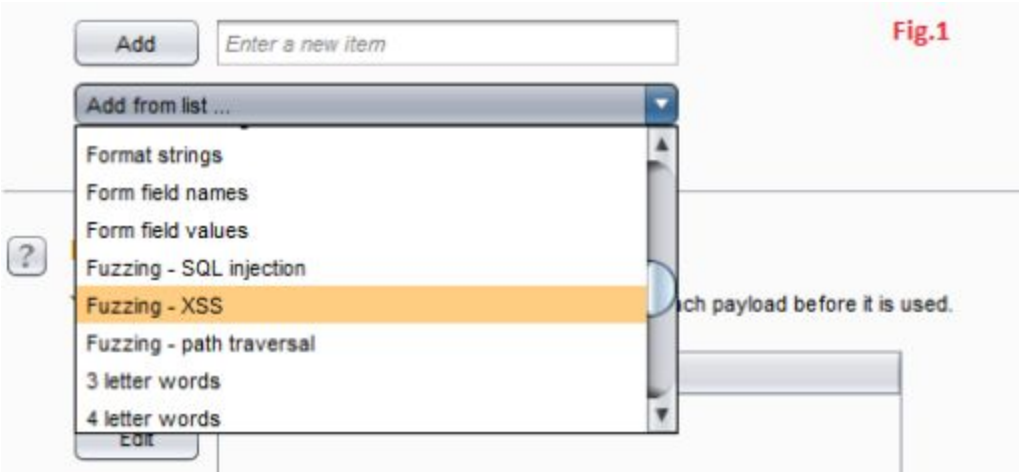


Fig.1

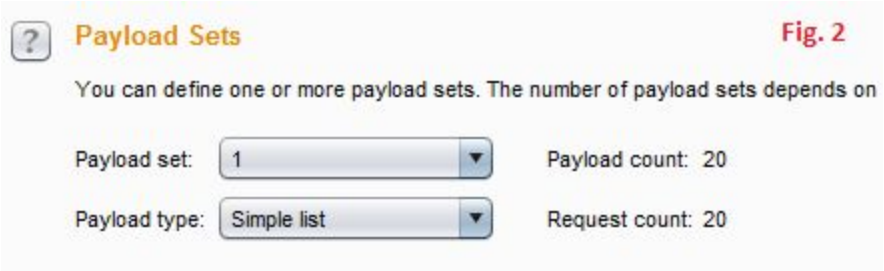


Fig. 2

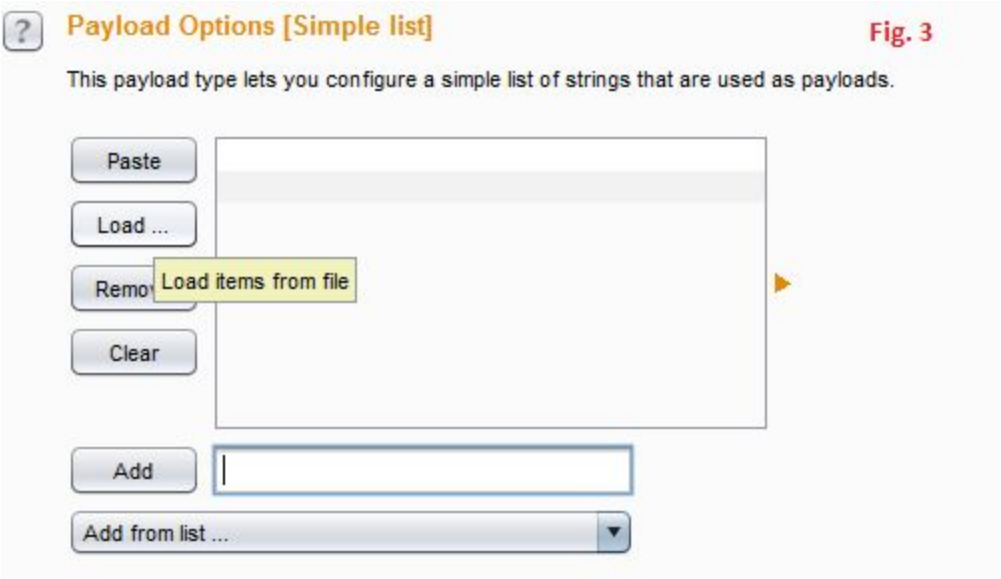
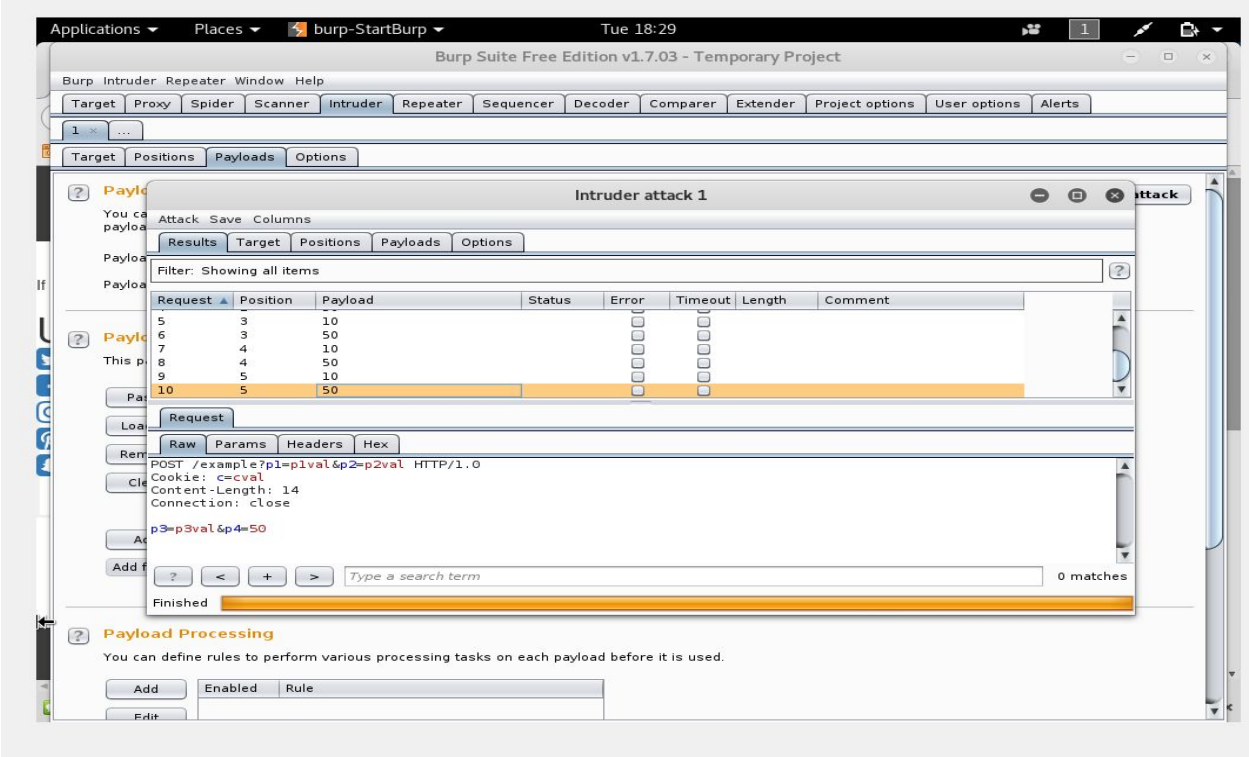


Fig. 3

Permanently adding these payloads to the Burp Suite default list will make tasks easy for the tester and will also make testing more efficient. It is suggested that testing team

should have common repositories for attack vectors that can be updated on a regular basis as new attack vectors originate on daily basis, the same can be shared among all team members.

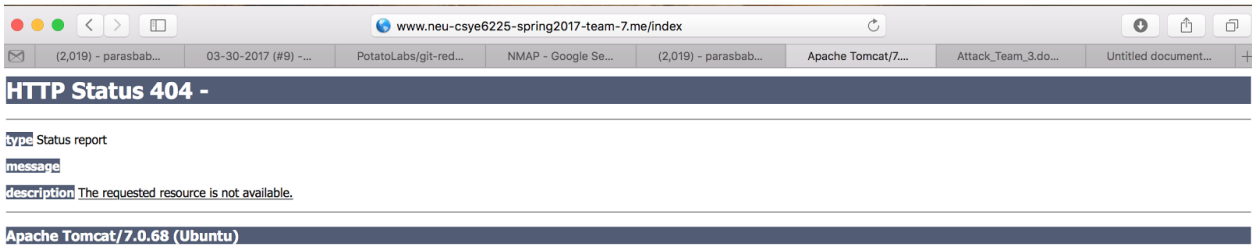


Result :- As seen above we are getting the 404 Error message while trying this method. We followed the above steps and deciphered that most of the content didn't have any injection in the URL

Protect:
Use Security Encoded Library

3)
Wireshark to capture Packets

I want to see the flow of the messages from one hop to other and if there is any encryption used or not but as ther site is down, I can't able to do that

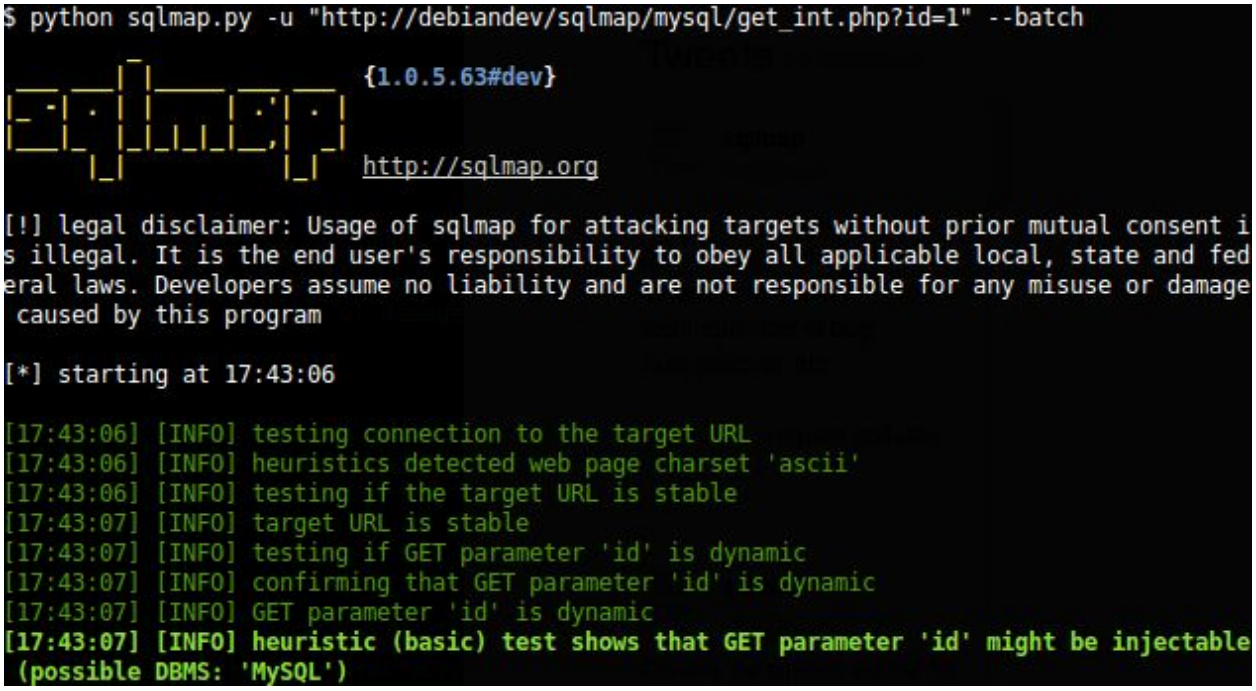


Result: None

Reason(Protection):

The flow should be done with use of Nonces and timestamps to protect the Man in the middle ,Replay and Reflection Attack.

4) **sqlmap** is an open source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over of database servers. It comes with a powerful detection engine, many niche features for the ultimate penetration tester and a broad range of switches lasting from database fingerprinting, over data fetching from the database, to accessing the underlying file system and executing commands on the operating system via out-of-band connections.



Result : Website was down

We have used this attack vector for sql injection as We know that is has used Mysql database or if there is any other database as well then also its been detected

Protection:

Cunning use of character encoding and other tricks can get round those functions