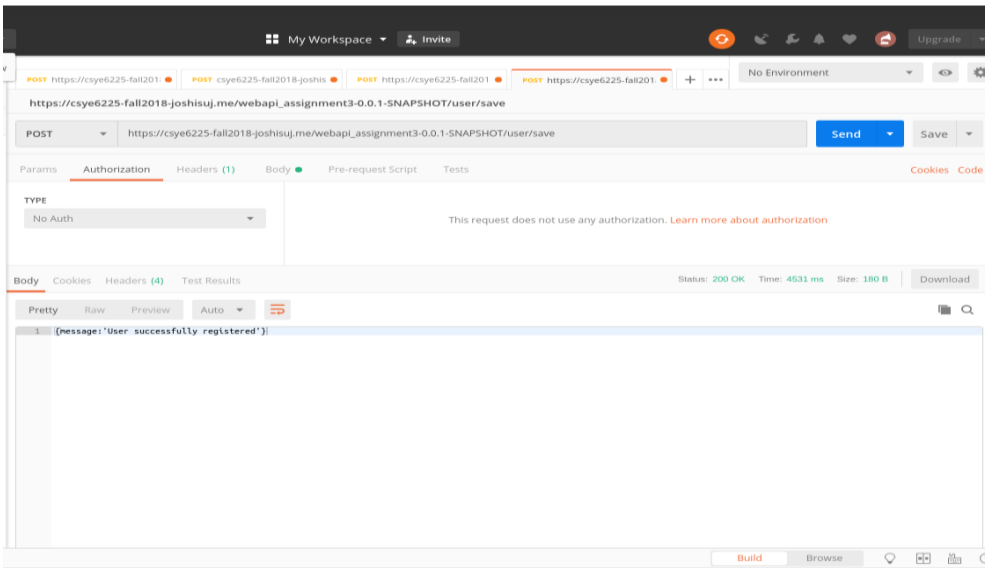
# NETWORKS STRUCTURES AND CLOUD COMPUTING

# ASSIGNMENT10

The following are the examples of attack vector and how we mitigated it

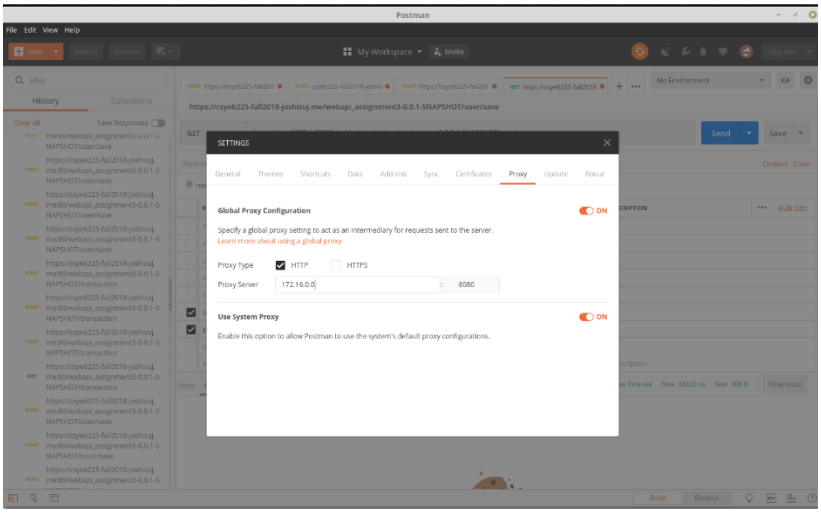
1. IP address Blocking: - IP Address blocking is a security measure that prevents a connection between a specific or group of IP addresses and a mail, web or Internet server. This is usually done to ban or block any undesirable sites and hosts from entering the server or node and causing harm to the network or individual computers. IP blocking is usually used by companies to prevent intrusion, allow remote access as well as limit the kinds of websites that can be accessed by employees in order to keep productivity high. Schools and other academic institutions also use IP address blocking for protection against unauthorized access of confidential records and data and for enforcing censorship.

   Before mitigation we could access the web application through any IP address



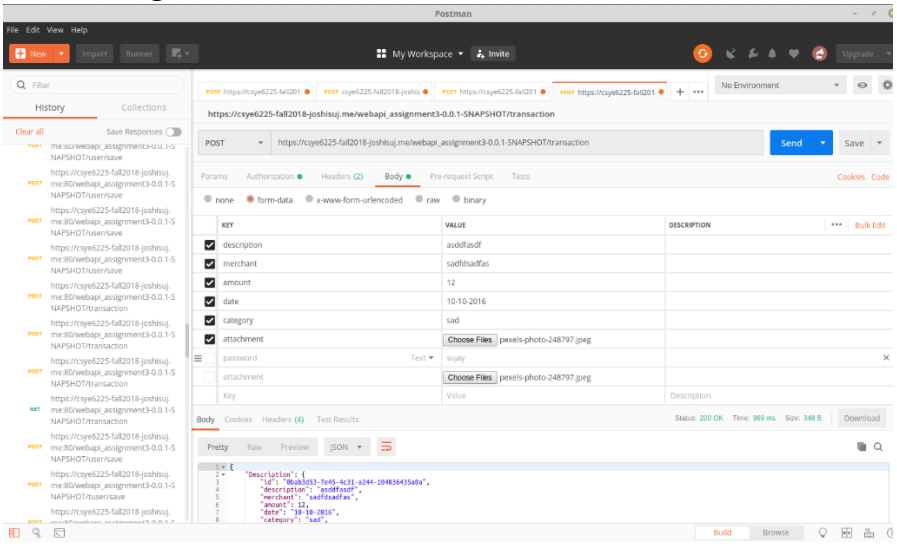

   We mitigate this problem by blacklisting certain IP's

   After Mitigation

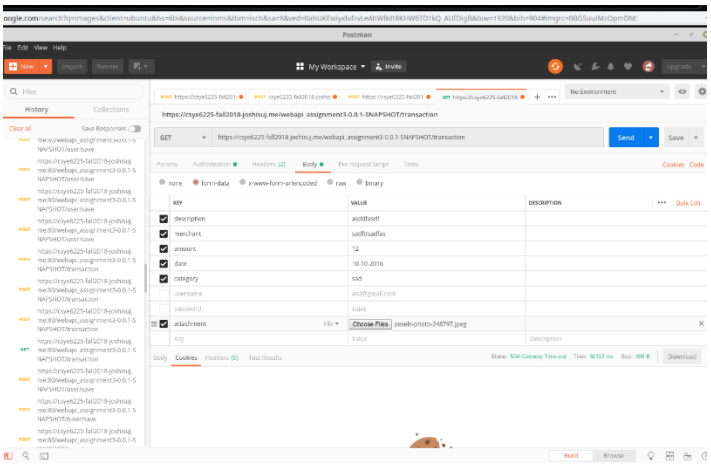



2. The body of the post request greater than certain bytes are not forwarded
   When attacker attack the web site they often try to attach large files or type text which is very large which often generates load on the web site, tending to cause denial of service. Therefore, to mitigate this issue we limit the request in the body to be less than 4096 bytes.

   Before mitigation



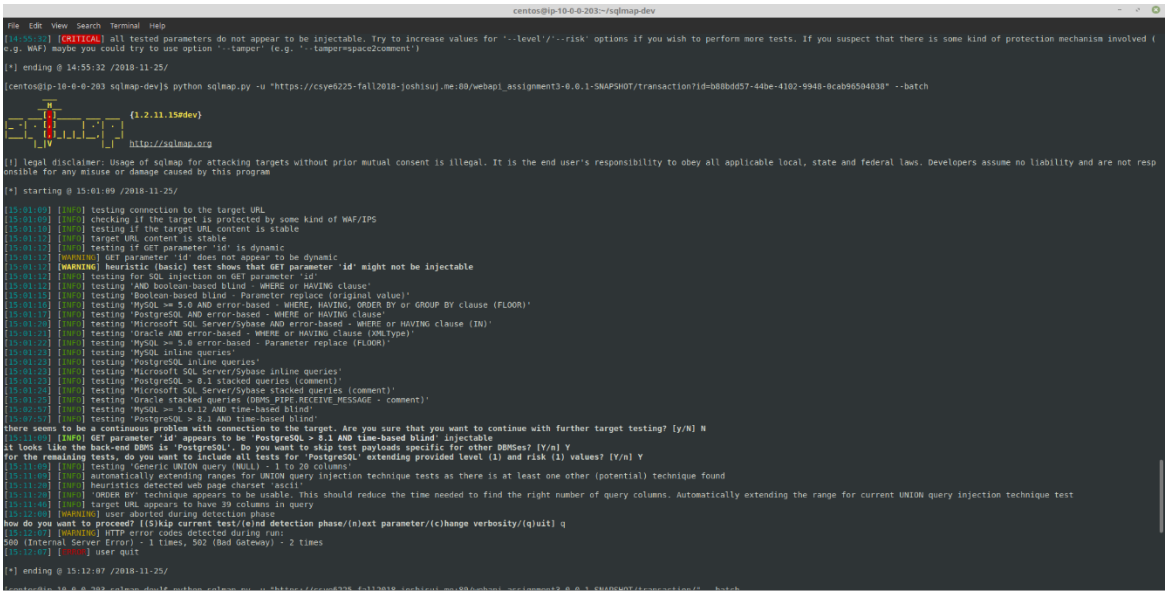

   After mitigation



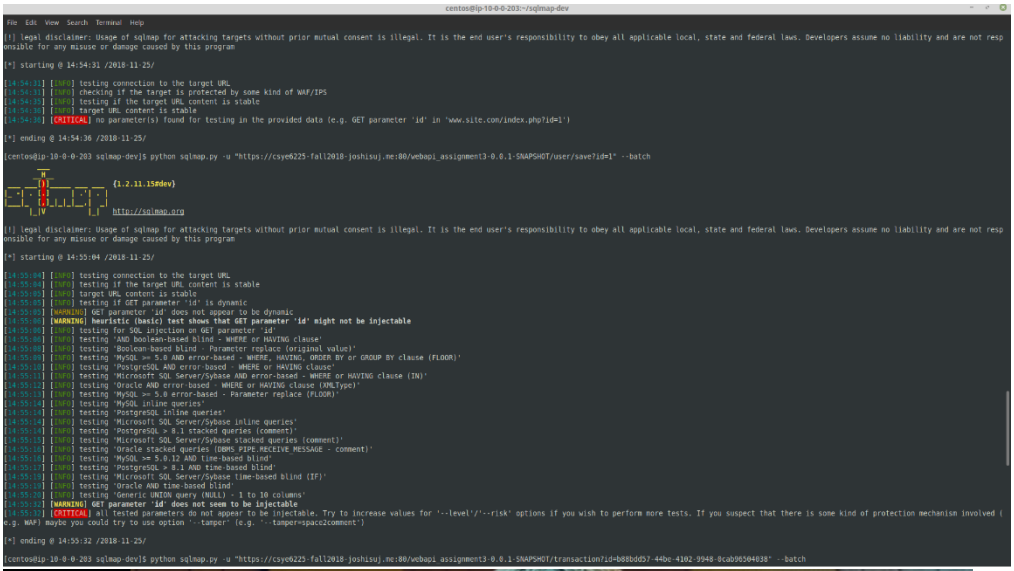
3. SQL Injection: - SQL injection is a code injection technique, used to attack data-driven applications, in which nefarious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). SQL injection must exploit a security vulnerability in an application's software, for example, when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. SQL injection is mostly known as an attack vector for websites but can be used to attack any type of SQL database.

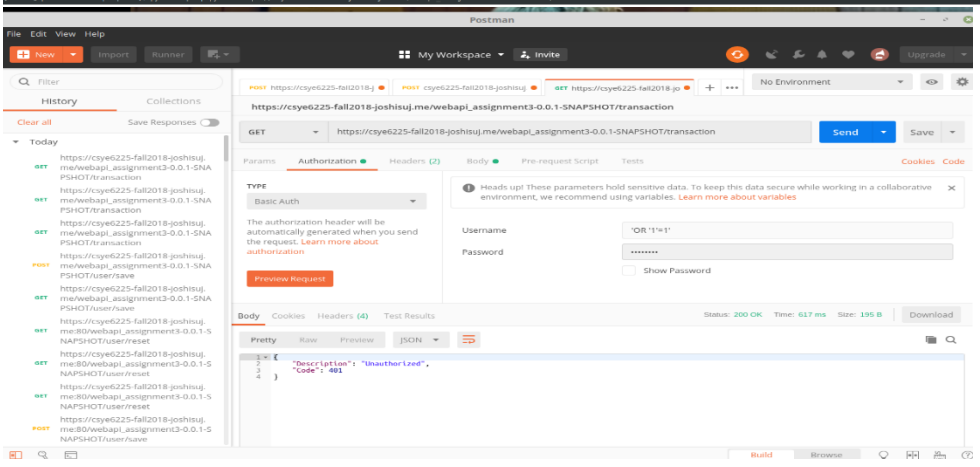
We have tested the SQL injection technique using Automatic SQL injection and database takeover tool.

Before Mitigation




After mitigating we got the Output be not injectable

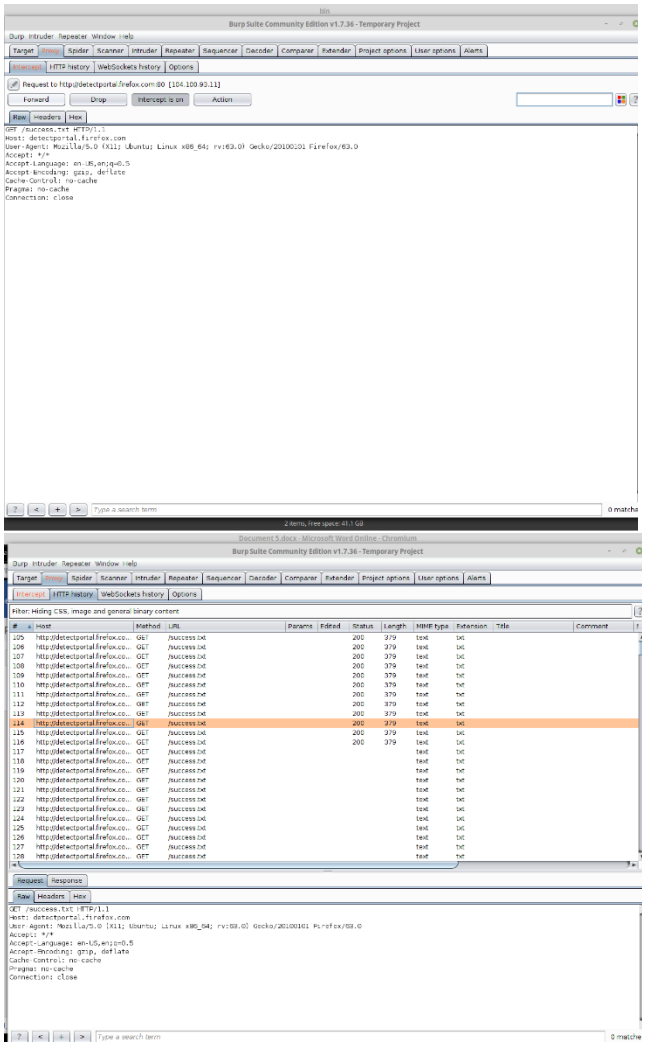


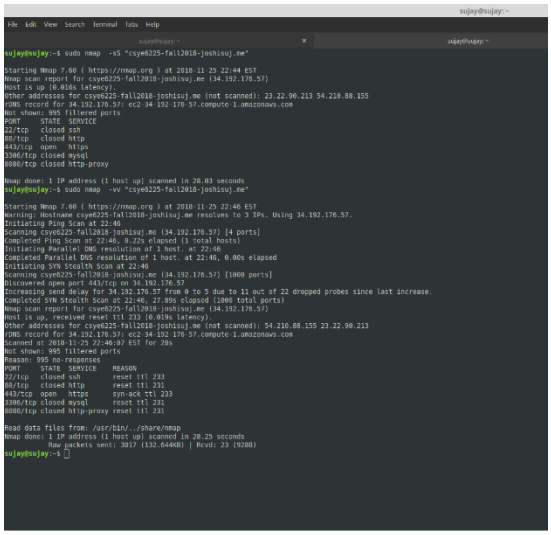
We have also implemented other security checks as follows

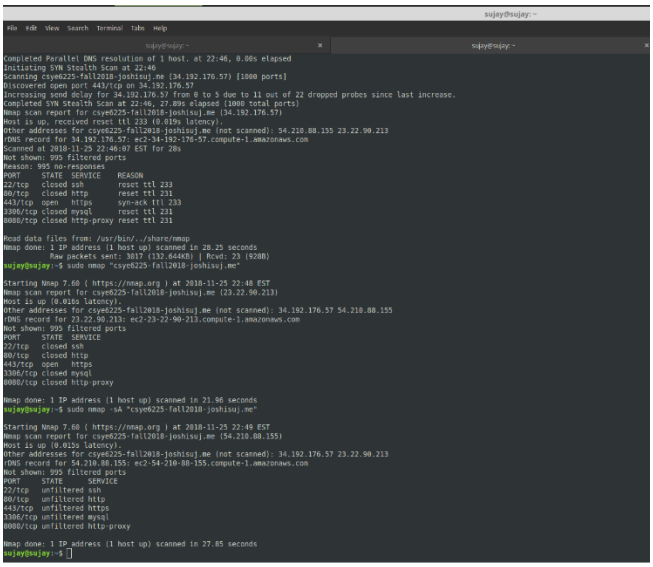
1. Cross-site request forgery, also known as one-click attack or session riding and abbreviated as CSRF (sometimes pronounced sea-surf[1]) or XSRF, is a type of malicious exploit of a website where unauthorized commands are transmitted from a user that the web application trusts. There are many ways in which a malicious website can transmit such commands; specially-crafted image tags, hidden forms, and JavaScript XMLHttpRequests, for example, can all work without the user's interaction or even knowledge.

   We have tried to intercept the data between the client and server and tried to change the data between them and application provided security by not allowing use to forward random data packets
   Software Used: Brup Suite



2. We have also tried to ping to application and check which all ports are open
   The application has on the https port open required for communication which is a good security in measure in our application
   Software Used: Nmap




Akash Bangera
Rishabh Jain
Punith Narayanswamy
Sujay Joshi