

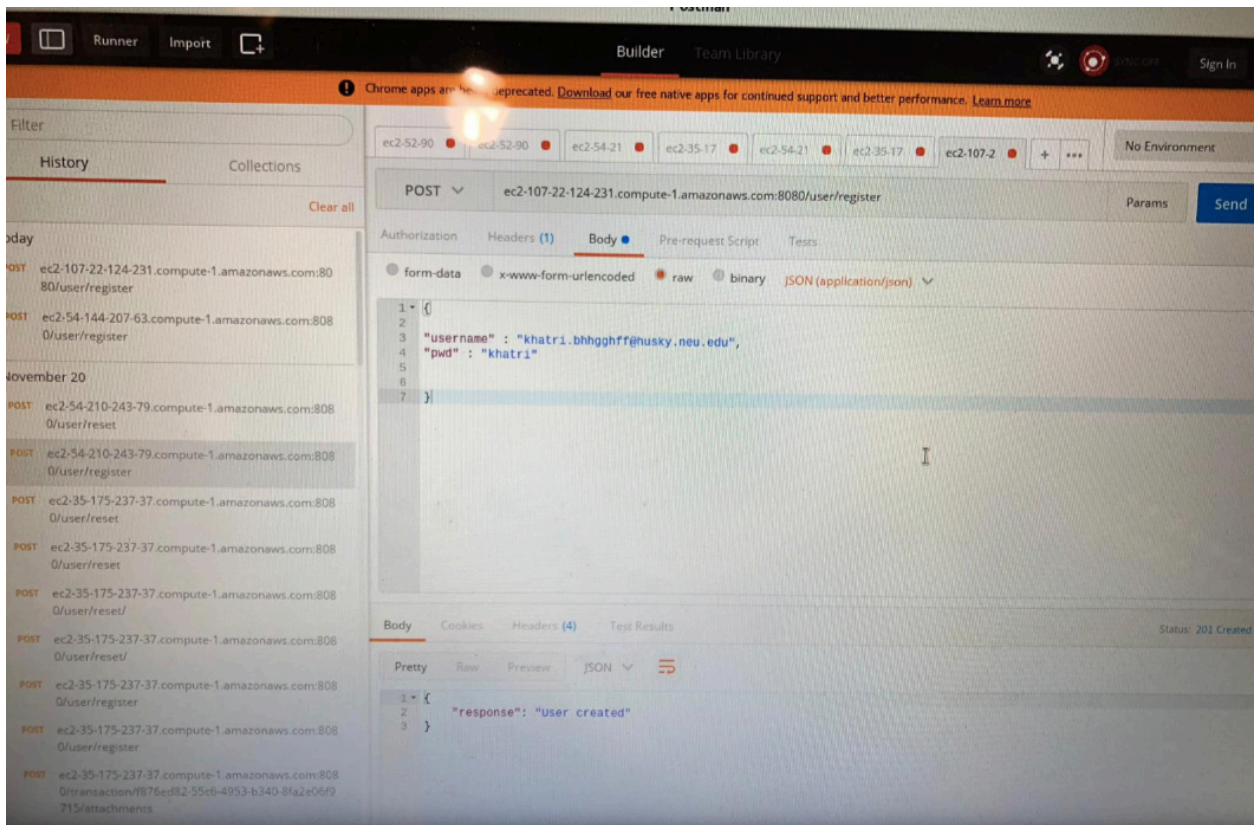
csye6225-fall2018

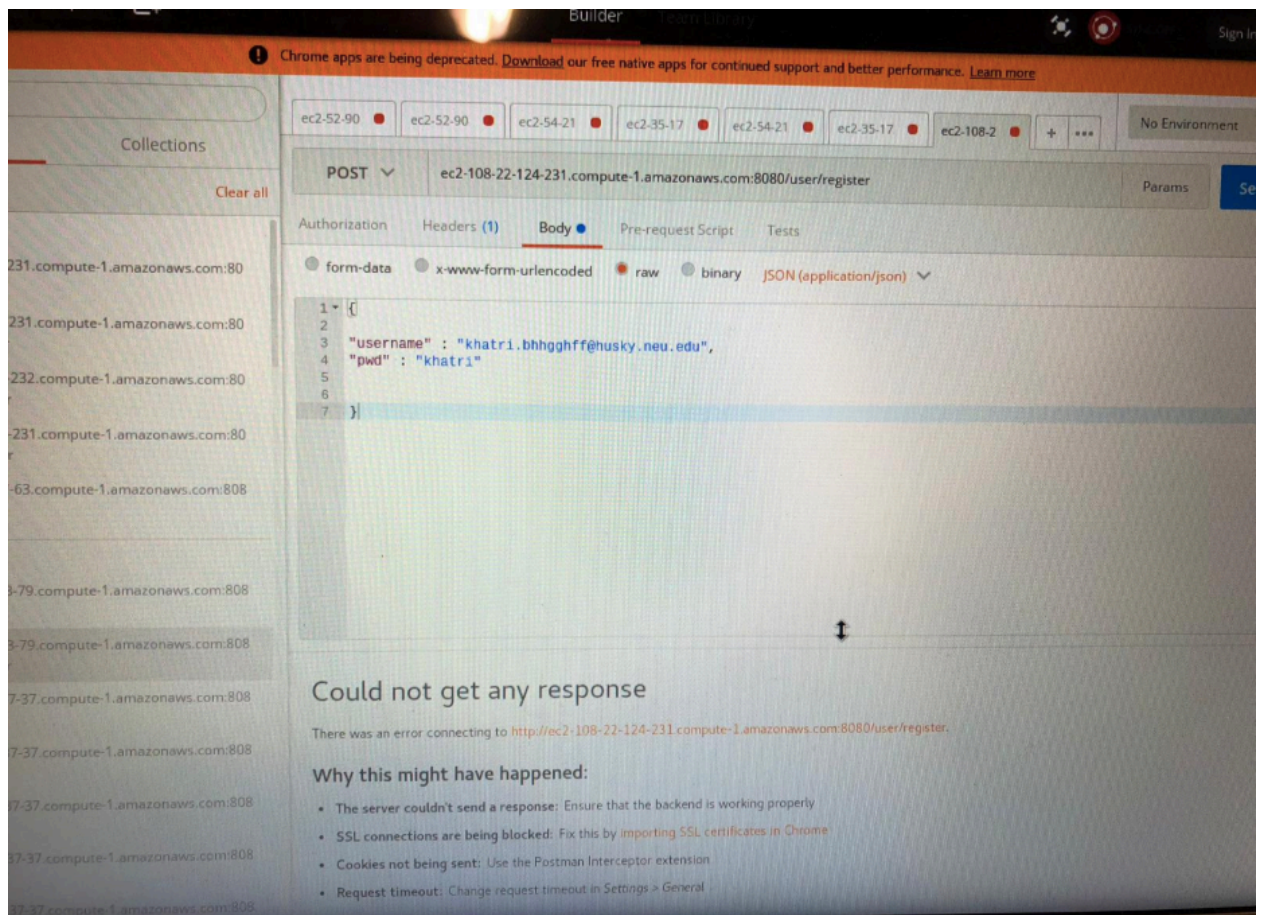
Team Members:

1. Sayali Gaikawad - gaikawad.s@husky.neu.edu
2. Akul Nigam - nigam.a@husky.neu.edu
3. Pankaj Sahani - sahani.p@husky.neu.edu
4. Chintan Shah - shah.c@husky.neu.edu

1) Penetration Test 1

- Attack Vector: IP Match Testing
- Result: The following screenshots represents IP Match Testing with and without WAF with the IP defined in range which much be allowed when I am hitting with my host IP and when I change the IP, WAF will block this hit.





- Why did you choose this specific attack vector?

IP Address blocking is a security measure that prevents a connection between a specific or group of IP addresses and a mail, web. 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.

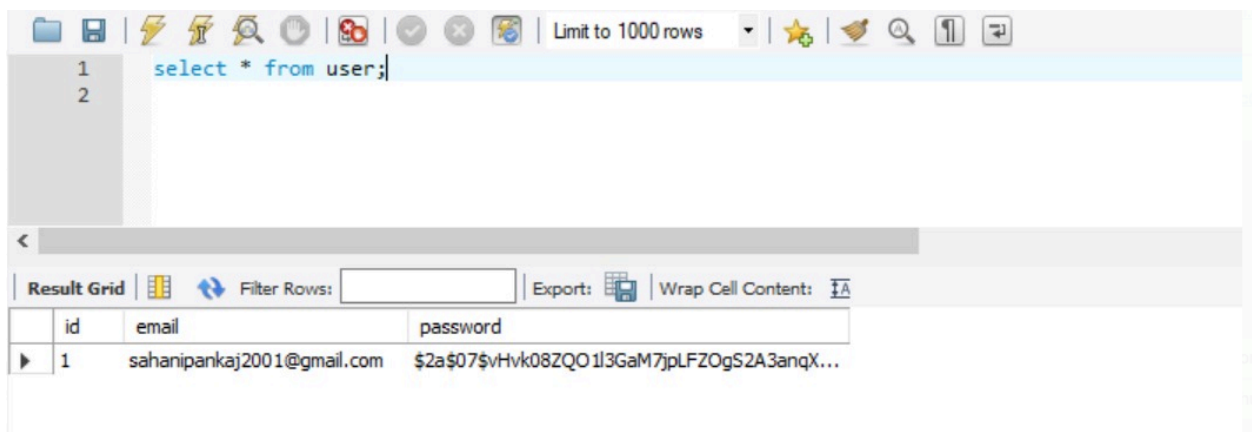
An IP address ban can effectively prevent a user from connecting to a certain web host. However, this is complicated when the user uses dynamic IP allocation since the IP cannot be pinpointed and a group or block of IP addresses has to be blocked, resulting in collateral damage as some ISPs share IP addresses for multiple users.

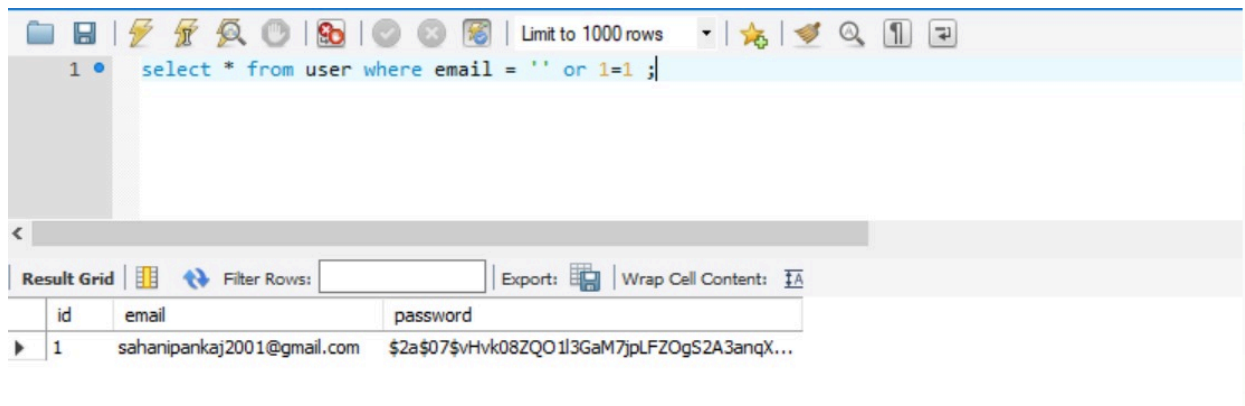
IP address banning also can limit syndication of specific content to a specific region since each country or region has specific IP addresses mapped to it. This has a devastating effect for an entire population since they can all be blocked from accessing most of the Internet. This has been done to Nigeria because of the perception that most businesses coming from the region are fraudulent, which adversely affected legitimate businesses as well.

2) Penetration Test 2

- Attack Vector: SQL Injection
- Result:

This technique is used for code injection for information driven applications in which we test the username and secret key verification while instead of username or secret key when given `1=1` (which is in every case genuine) the code which is defenseless against assaults shows the outcome as when validated username and password is given.





- Why did you choose this specific attack vector?

SQL Injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements (also commonly referred to as a malicious payload) that control a web application's database server (also commonly referred to as a Relational Database Management System – RDBMS). Since an SQL Injection vulnerability could possibly affect any website or web application that makes use of an SQL-based database, the vulnerability is one of the oldest, most prevalent and most dangerous of web application vulnerabilities.

There are several types of SQL injection, but they all involve an attacker inserting arbitrary SQL into a web application database query. The simplest form of SQL injection is through user input. Web applications typically accept user input through a form, and the front end passes the user input to the back-end database for processing. If the web application fails to sanitize user input, an attacker can inject SQL of their choosing into the back-end database and delete, copy, or modify the contents of the database

Mitigating SQL injection attacks is not difficult, but even the smartest and best-intentioned developers still make mistakes. Detection is therefore an important component of mitigating the risk of a SQL injection attack. A web application firewall (WAF) can detect and block basic SQL injection attacks.