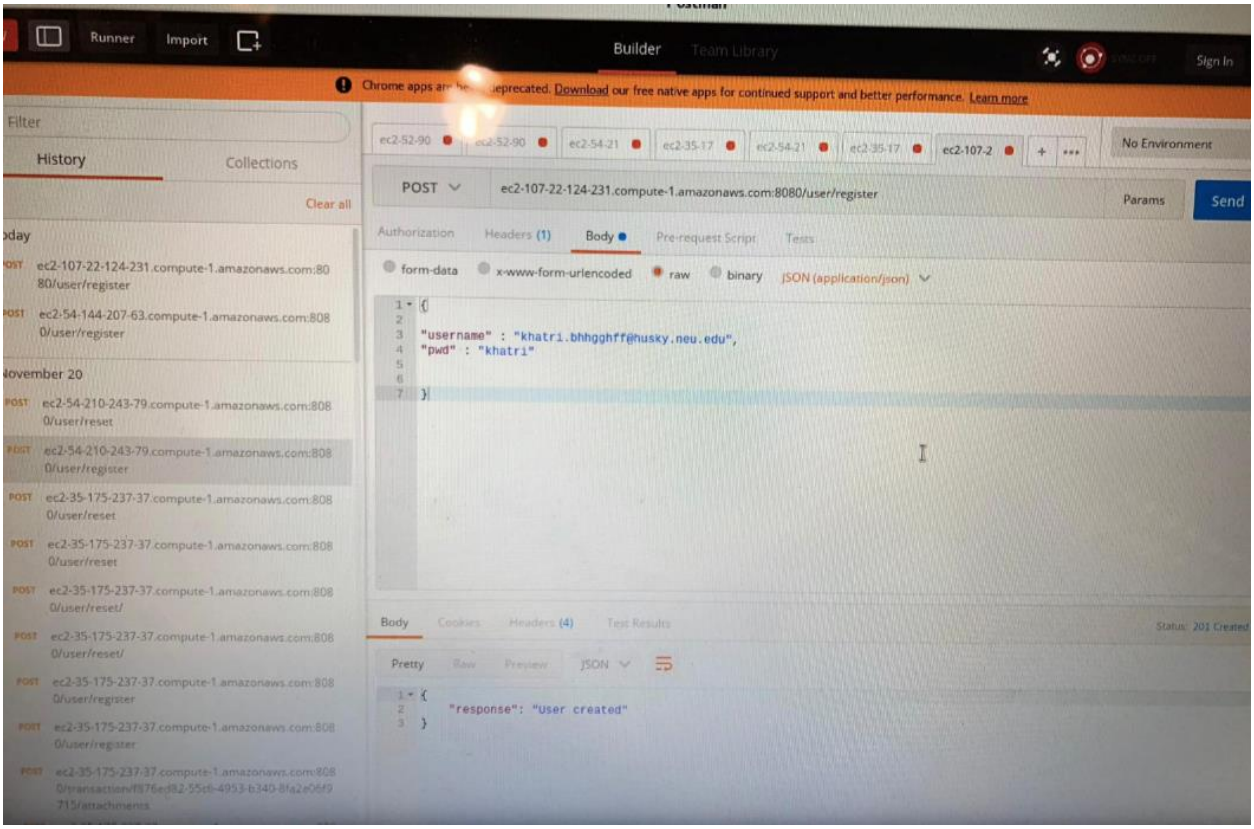
csye6225-fall2018

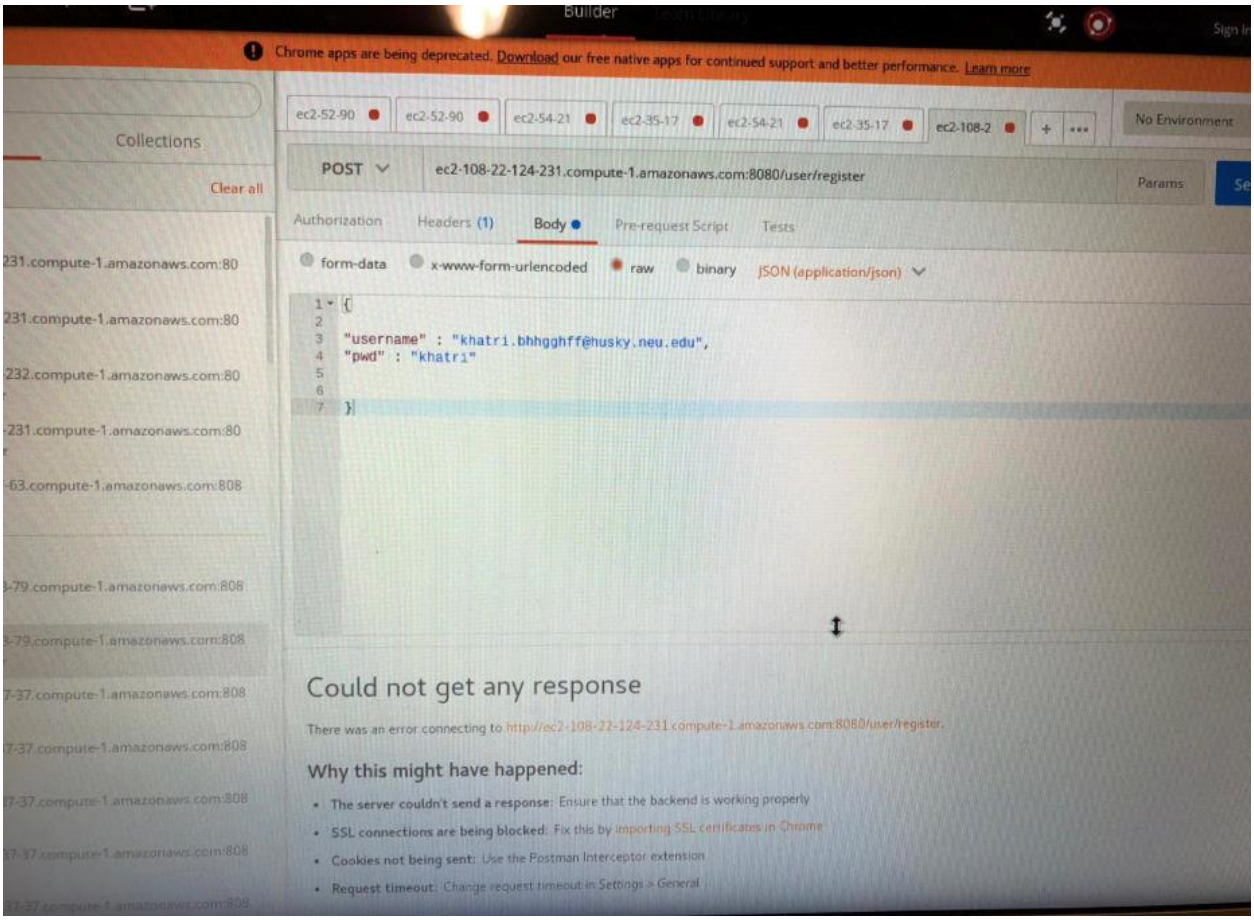
Team Members:

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.

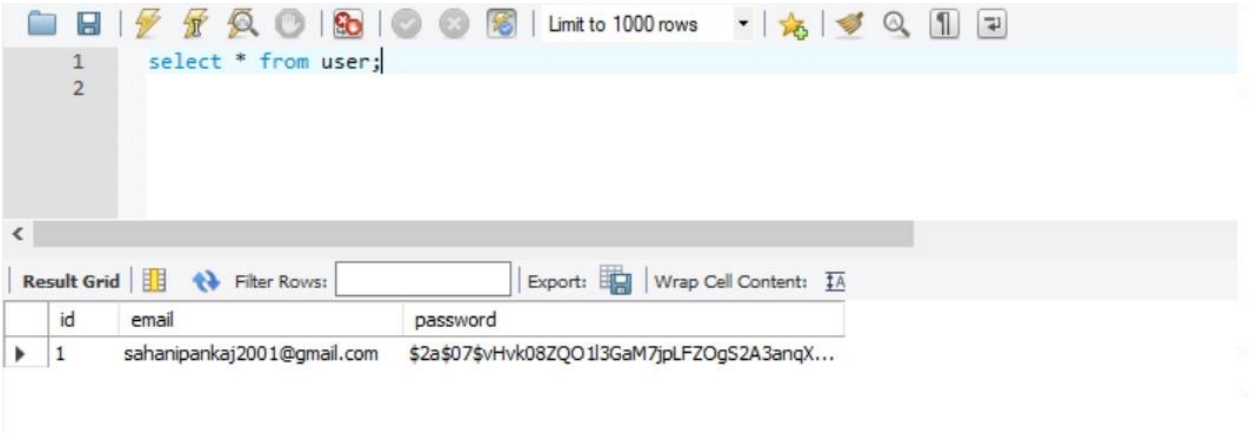
An IP address ban can effectively prevent a user from connecting to a certain web host. However, this is complicated when the user uses dynamic IP allocation since the IP cannot be pinpointed and a group or block of IP addresses has to be blocked, resulting in collateral damage as some ISPs share IP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

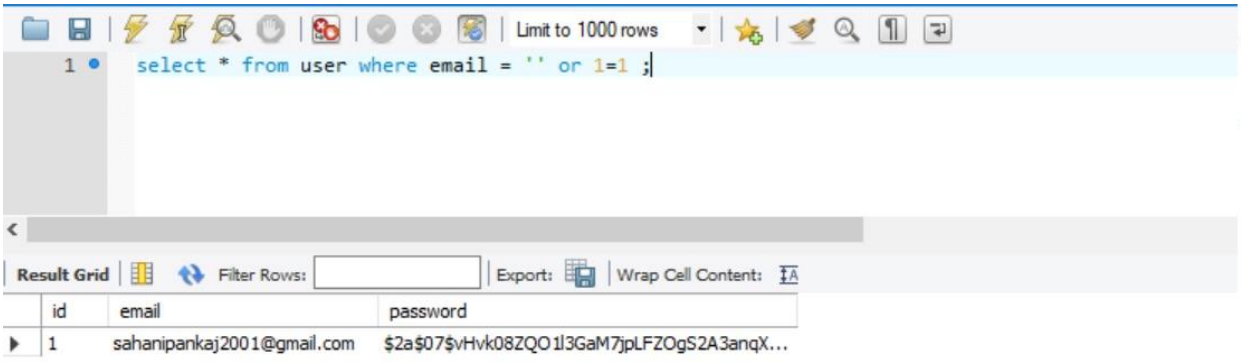
IP address banning also can limit syndication of specific content to a specific region since each country or region has specific IP addresses mapped to it. This has a devastating effect for an entire population since they can all be blocked from accessing most of the Internet. This has been done to Nigeria 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.

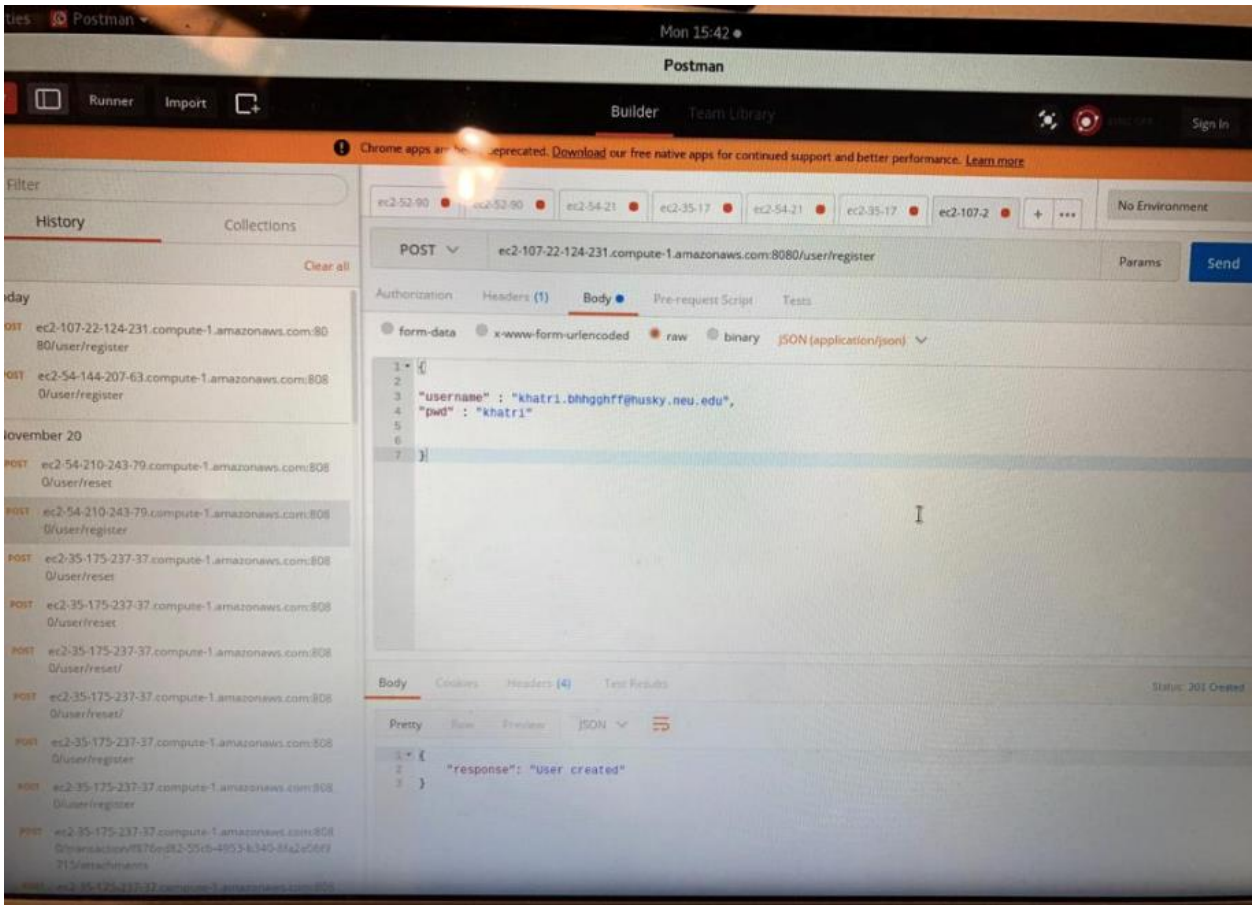
There are several types of SQL injection, but they all involve an attacker inserting arbitrary SQL into a web application database query. The simplest form of SQL injection is through user input. Web applications typically accept user input through a form, and the front end passes the user input to the 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

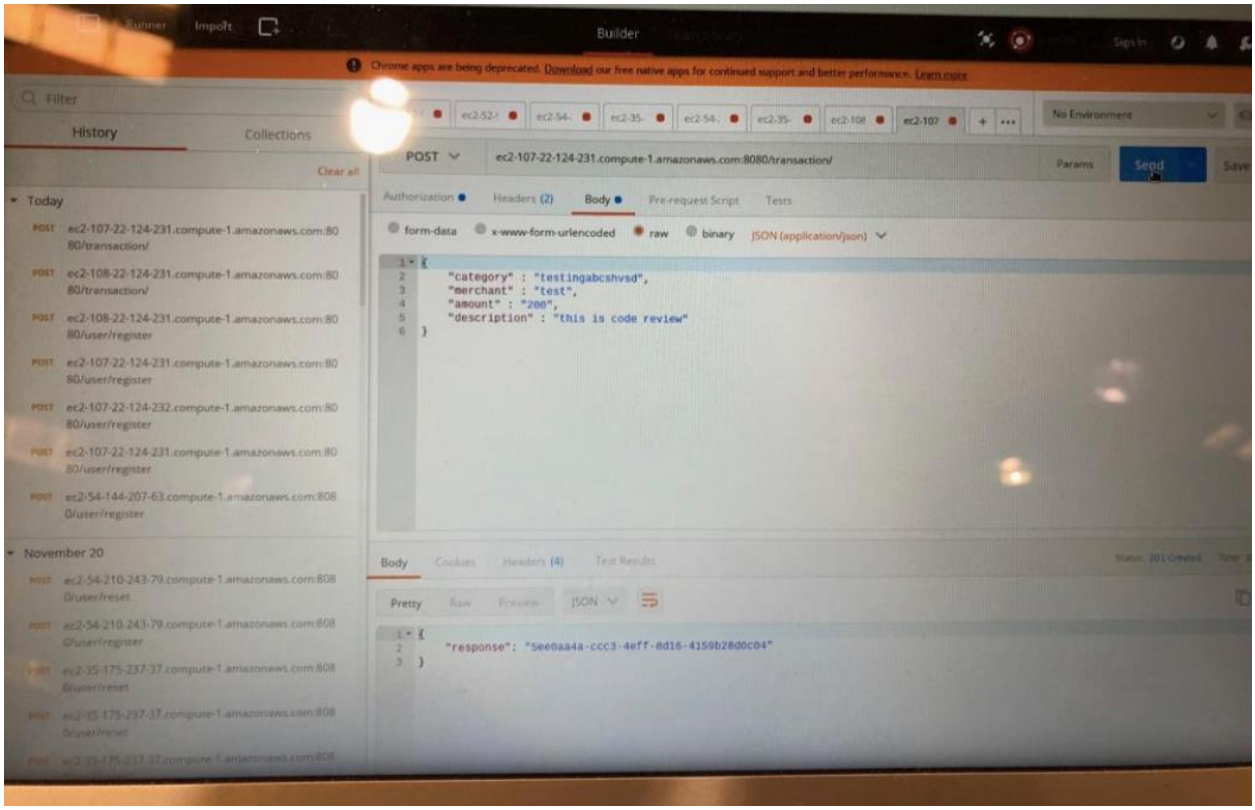
Mitigating SQL injection attacks is not difficult, but even the smartest and best-intentioned developers still make mistakes. Detection is therefore an important component of mitigating the risk of a SQL injection attack. A web application firewall (WAF) can detect and block basic SQL injection attacks.

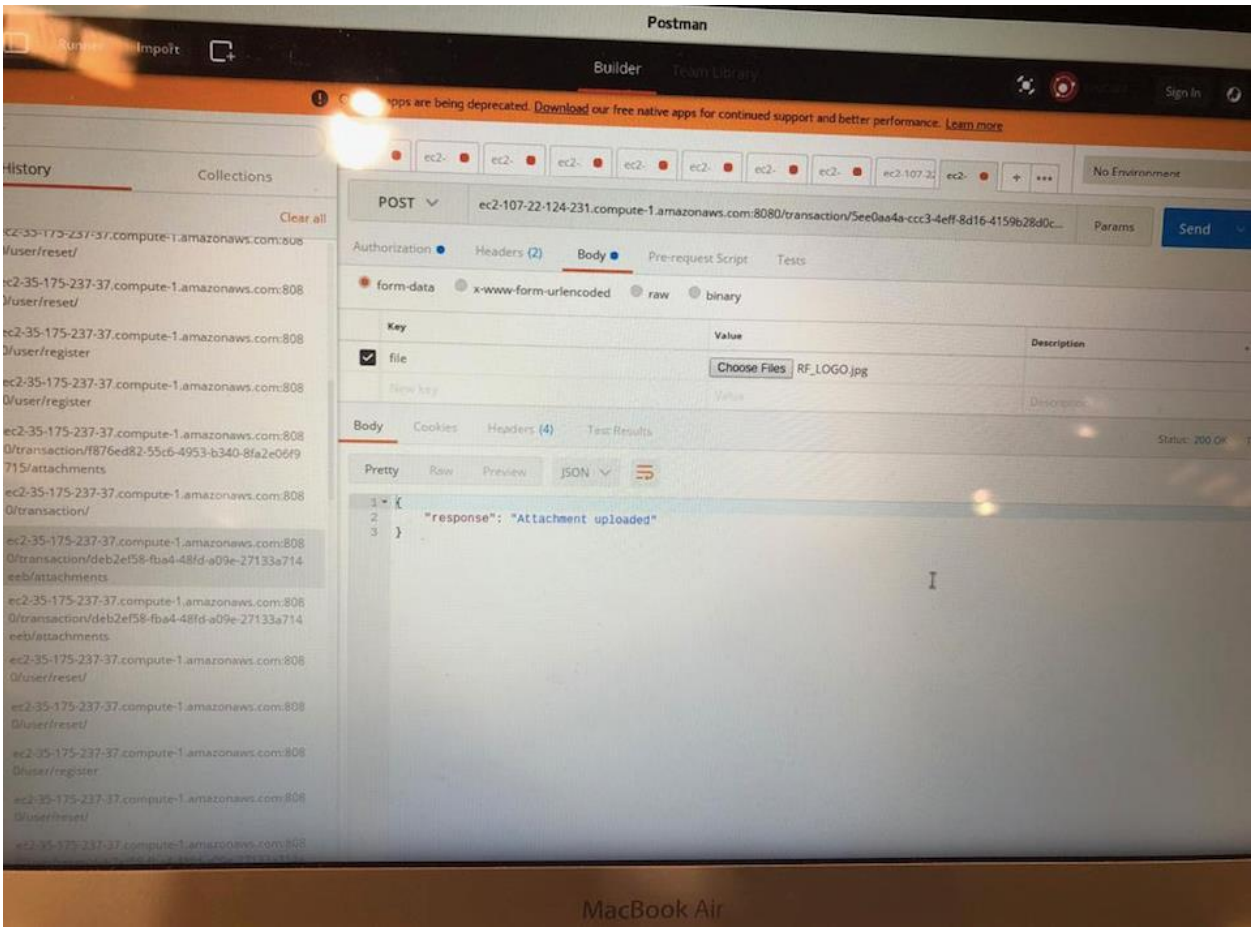
3) Penetration Test 3

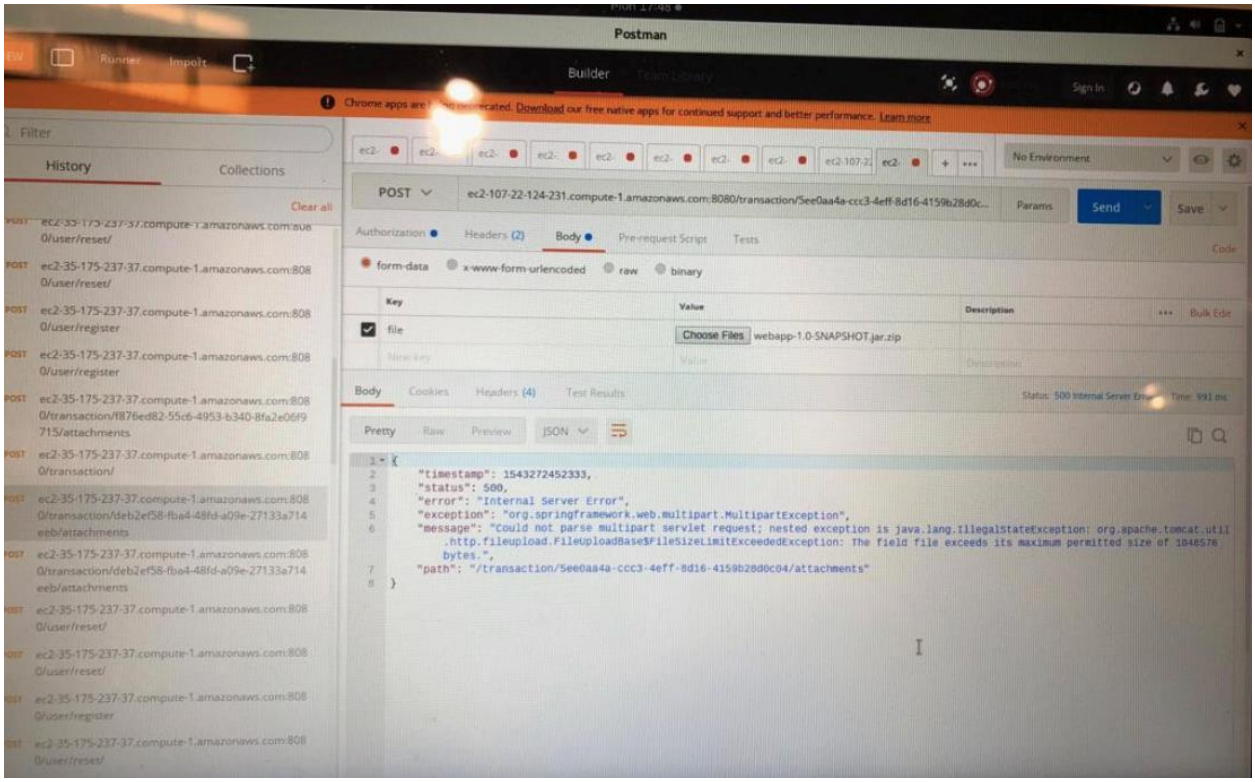
- Attack Vector: Large Body Match
- Result:

We are testing 'attachment post' in our code. An attacker can pass a large file to the S3 bucket deliberately and can induce considerable delays to our instance and can also crash the instance as well. To prevent this, we can restrict the maximum size of the files being posted into our S3 bucket.


Postman
Mon 15:42
Postman
Runner
Import
Builder
Team Library
Sign In
Chrome apps are deprecated. Download our free native apps for continued support and better performance. Learn more
Filter
History
Collections
Clear all
ec2-107-22-124-231.compute-1.amazonaws.com:8080/user/register
ec2-54-144-207-63.compute-1.amazonaws.com:8080/user/register
November 20
ec2-54-210-243-79.compute-1.amazonaws.com:8080/user/reset
ec2-54-210-243-79.compute-1.amazonaws.com:8080/user/register
ec2-35-175-237-37.compute-1.amazonaws.com:8080/user/reset
ec2-35-175-237-37.compute-1.amazonaws.com:8080/user/reset
ec2-35-175-237-37.compute-1.amazonaws.com:8080/user/reset/
ec2-35-175-237-37.compute-1.amazonaws.com:8080/user/reset/
ec2-35-175-237-37.compute-1.amazonaws.com:8080/user/register
ec2-35-175-237-37.compute-1.amazonaws.com:8080/user/register
No Environment
POST
ec2-107-22-124-231.compute-1.amazonaws.com:8080/user/register
Params
Send
Authorization
Headers (1)
Body
Pre-request Script
Tests
form-data
x-www-form-urlencoded
raw
binary
JSON (application/json)
{
"username" : "khatri.bhhgghff@husky.neu.edu",
"pwd" : "khatri"
}
Body
Cookies
Headers (4)
Test Results
Status: 201 Created
Pretty
Raw
Preview
JSON
{
"response": "User created"
}


Runner
Import
Builder
Sign In
Chrome apps are being deprecated. Download our free native apps for continued support and better performance. Learn more
Filter
History
Collections
Clear all
Today
POST ec2-107-22-124-231.compute-1.amazonaws.com:8080/transaction/
POST ec2-108-22-124-231.compute-1.amazonaws.com:8080/transaction/
POST ec2-108-22-124-231.compute-1.amazonaws.com:8080/user/register
POST ec2-107-22-124-231.compute-1.amazonaws.com:8080/user/register
POST ec2-107-22-124-232.compute-1.amazonaws.com:8080/user/register
POST ec2-107-22-124-231.compute-1.amazonaws.com:8080/user/register
POST ec2-54-144-207-63.compute-1.amazonaws.com:8080/user/register
November 20
POST ec2-54-210-243-79.compute-1.amazonaws.com:8080/user/reset
POST ec2-54-210-243-79.compute-1.amazonaws.com:8080/user/register
GET ec2-35-175-237-37.compute-1.amazonaws.com:8080/user/reset
POST ec2-35-175-237-37.compute-1.amazonaws.com:8080/user/reset
No Environment
POST
ec2-107-22-124-231.compute-1.amazonaws.com:8080/transaction/
Params
Send
Save
Authorization
Headers (2)
Body
Pre-request Script
Tests
form-data
x-www-form-urlencoded
raw
binary
JSON (application/json)
{
"category" : "testingabcshvsd",
"merchant" : "test",
"amount" : "200",
"description" : "this is code review"
}
Body
Cookies
Headers (4)
Test Results
Status: 201 Created
Pretty
Raw
Preview
JSON
{
"response": "5ee0aa4a-ccc3-4eff-8d16-4159b28d0c04"
}


Postman
Import
Builder
Team Library
Sign In
apps are being deprecated. Download our free native apps for continued support and better performance. Learn more
History
Collections
Clear all
No Environment
POST
ec2-107-22-124-231.compute-1.amazonaws.com:8080/transaction/5ee0aa4a-ccc3-4eff-8d16-4159b28d0c...
Params
Send
Authorization
Headers (2)
Body
Pre-request Script
Tests
form-data
x-www-form-urlencoded
raw
binary
Key
Value
Description
file
Choose Files
RF_LOGO.jpg
Body
Cookies
Headers (4)
Test Results
Status: 200 OK
Pretty
Raw
Preview
JSON
{
"response": "Attachment uploaded"
}
MacBook Air



- Why did you choose this specific attack vector?

  Large attachments can result in causing crash or hanging the postman. If we use GET request with large data, it will hang, load forever without responding. The response is also extremely slow with large responses. It delays the scrolling on large sized data. Moreover, the application crashes searching a large response.