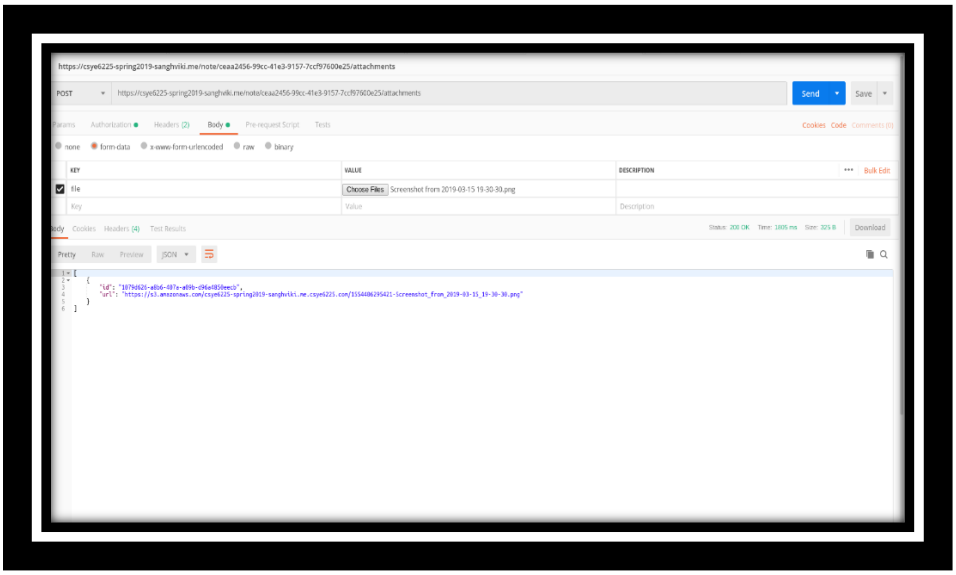
CSYE 6225 Spring 2019 Assignment 8

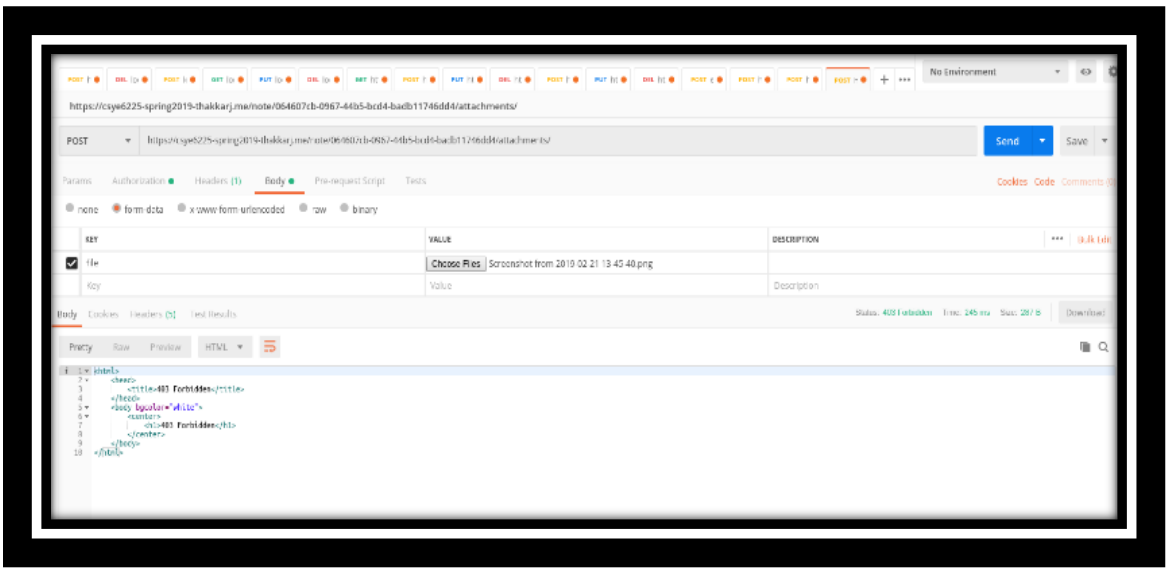
1. Unrestricted file size

- Result: Using waf, we can put restriction on the size of the attachment file that can be uploaded.
- Reason for use: The application is open for uploading different sizes of files without detecting its size. The consequences of unrestricted file upload can vary, including complete system takeover, an overloaded file system or database, forwarding attacks to back-end systems, client-side attacks, or simple defacement. Uploaded files can be abused to exploit other vulnerable sections of an application when a file on the same or a trusted server is needed (can again lead to client-side or server-side attacks)

Without WAF



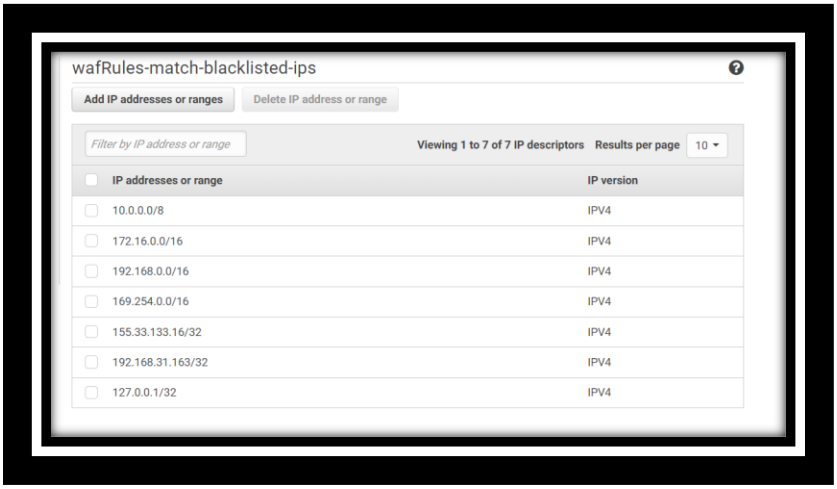
With WAF



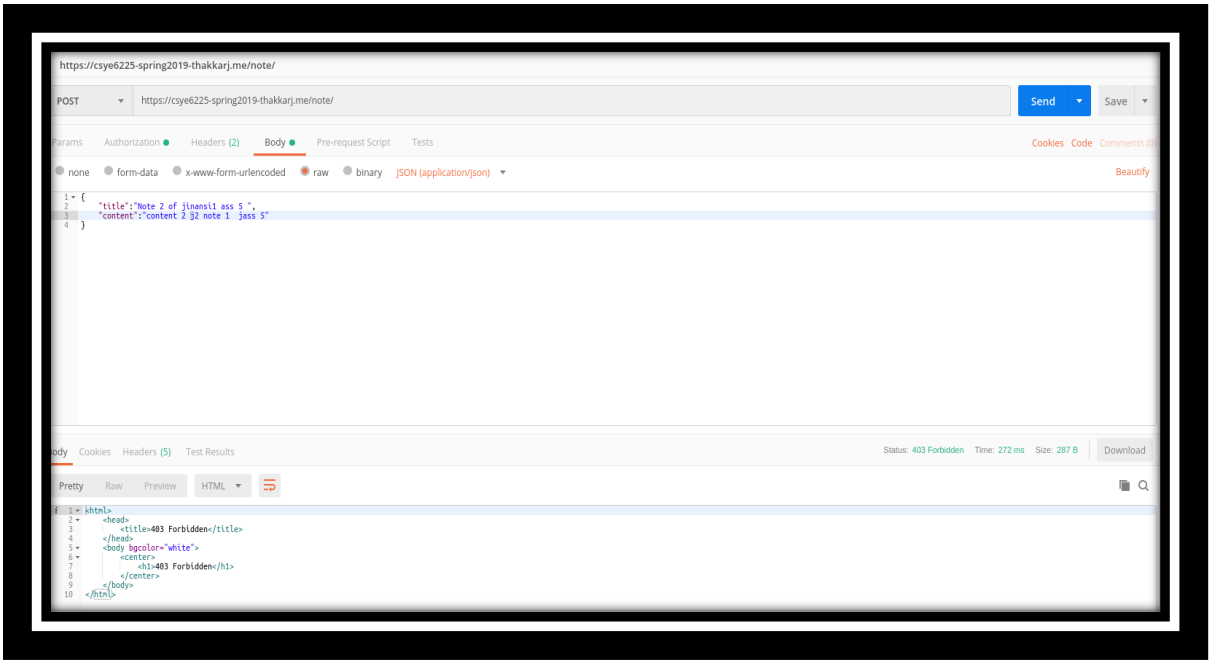
2. Blacklist IP Address

- Result: Using WAF, we can add IPs to blacklist to block access to application from malicious attacks.
- Reason: A WAF that operates based on blacklist (negative Security model) protect against known attacks. This is useful if there is a need to temporarily or permanently block an IP address.

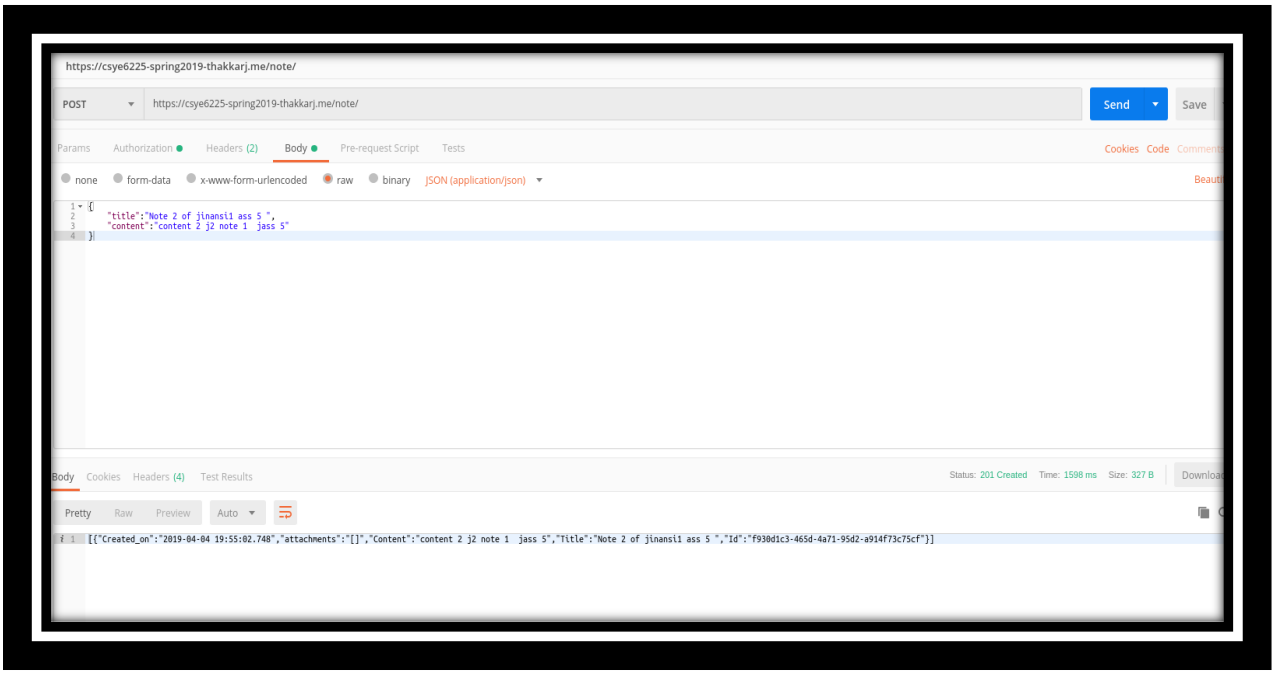
Blocked IPs



Accessing from blocked IPs



Removing IP from Block list

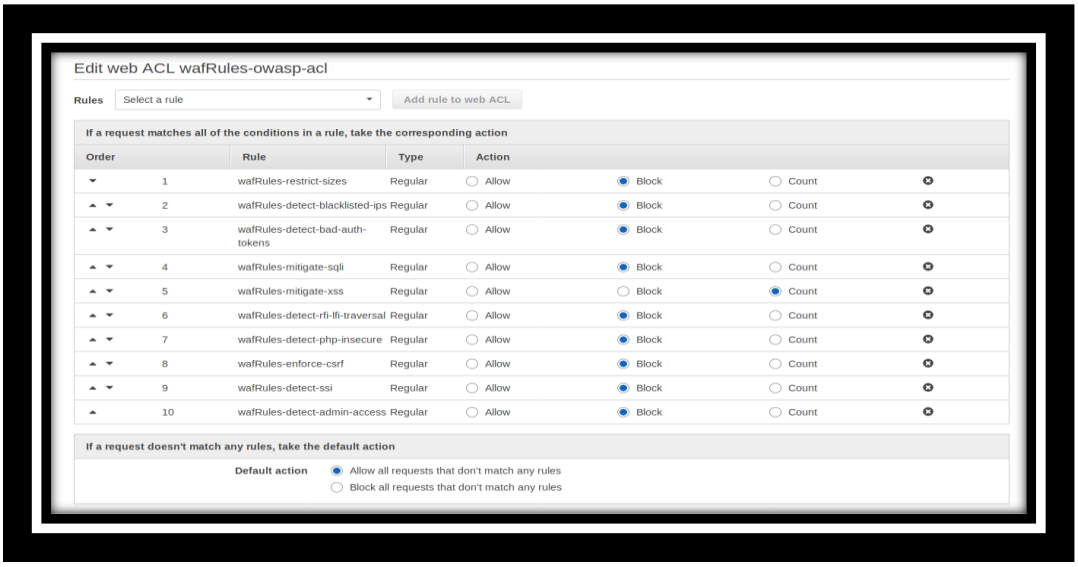


3. XSS WAF

Cross-site scripting (XSS) is used by attackers to inject malicious code into vulnerable web applications. Unlike other web application attacks (such as SQL injection) attackers are not directly targeting the application. Instead, the application is a means for attacking the application user.

Before activating XSS WAF :

The hacker can access the application by embedding the script



After activating XSS WAF :

The hacker will not be able to access the application