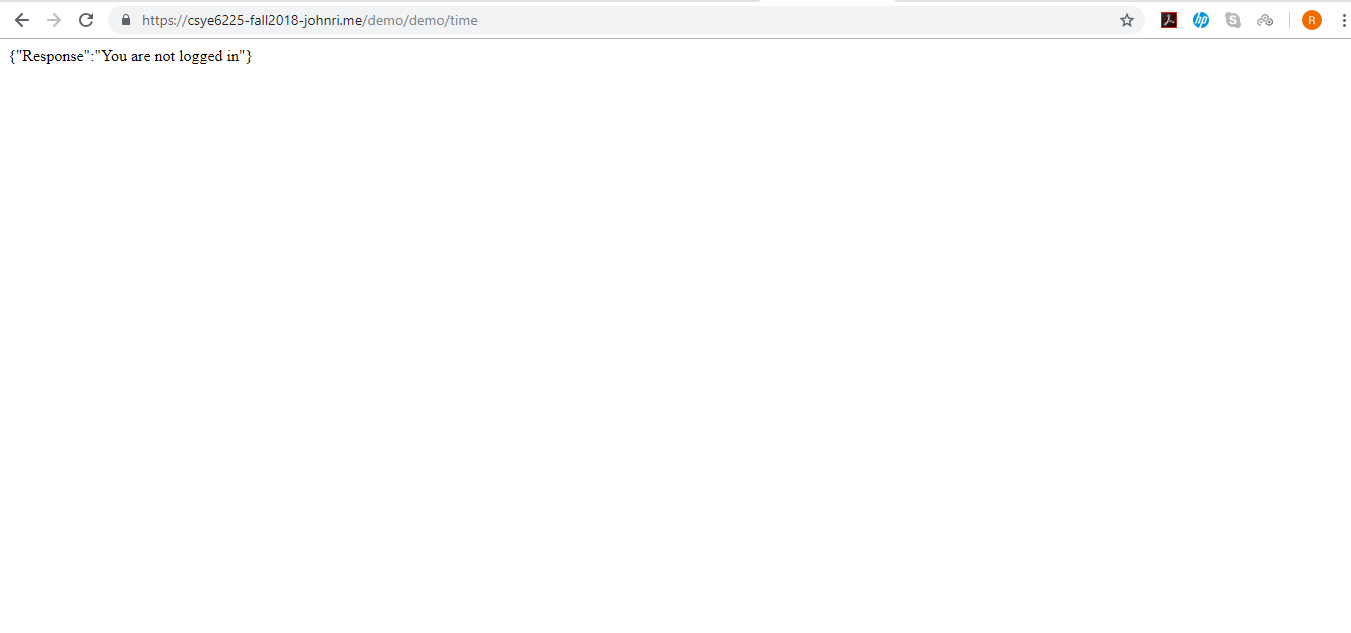
**Assignment 10: Web Application Firewall**

**Attack Vector 1: Blacklisting unauthorized IP addresses**

**Why did you choose this specific attack vector**: Security of web application is of prime importance and thus allowing only trusted IPs play an important role. Suspicious activity like spam or viruses can be kept away from the web application and secure it.

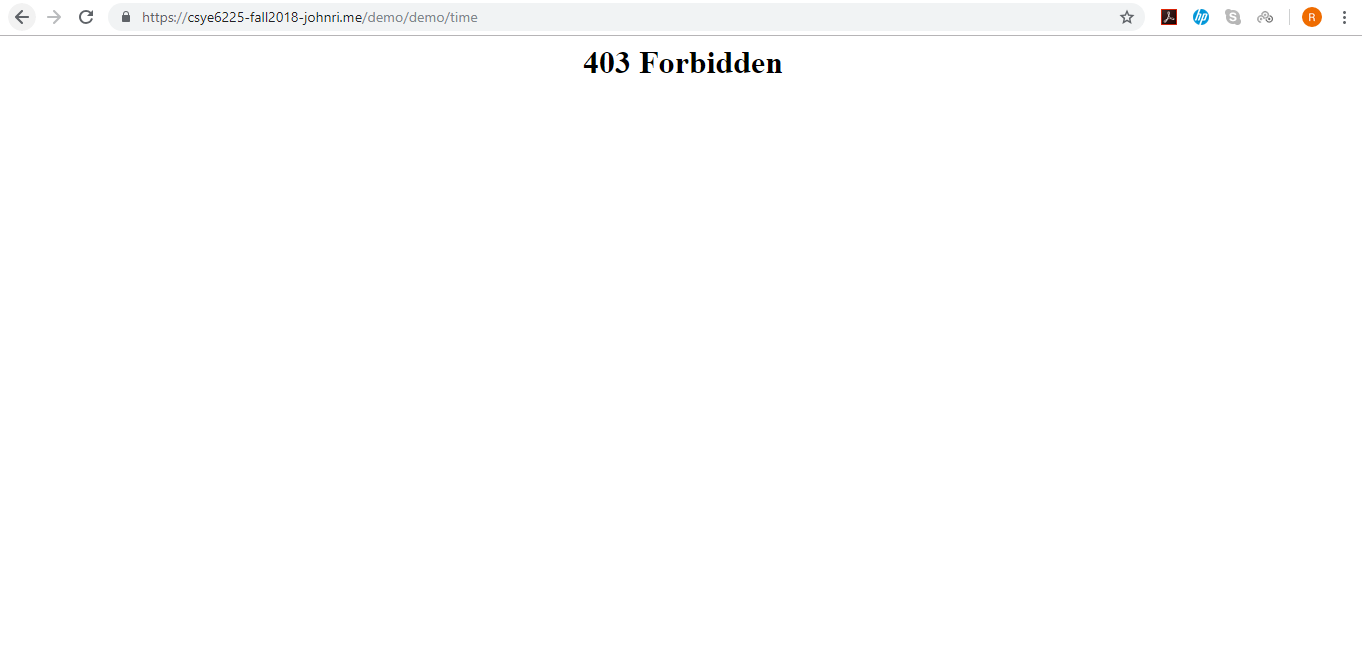
**Testing:**

Try to hit the web application using your own domain name. Since this IP is not blacklisted, the web application will show up like below. In this vector, initially all IP addresses can access the web application.



**Result:**

After setting up the WAF rules, the IP address is now blacklisted and can no longer access the web application and throws a “403 Forbidden” error.



**Attack Vector 2: Size constraints when uploading larger attachments in transactions**

**Why did you choose this specific attack vector:**

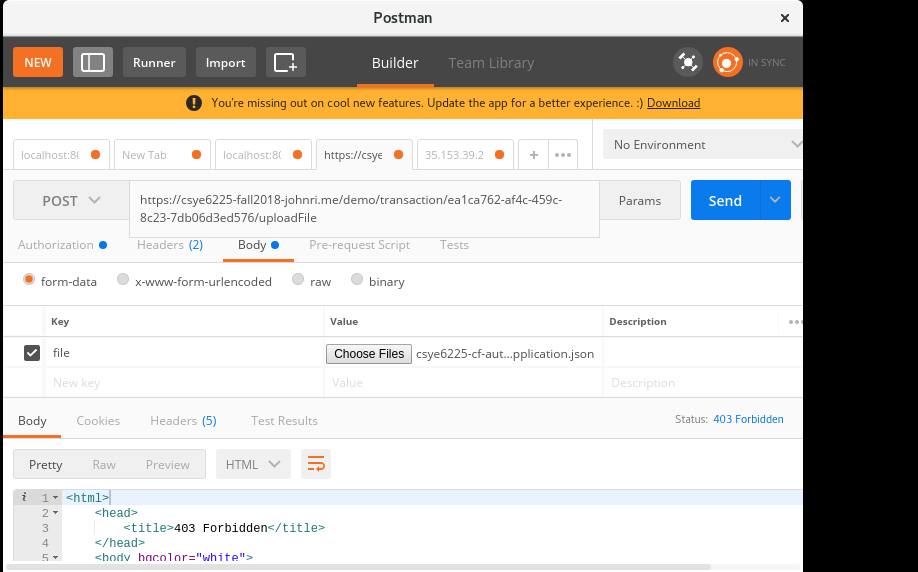
At times, users using the web application may either knowingly/ unknowingly upload larger attachments that can slow down or cause the application to malfunction. Hence, to prevent this we can setup rules that limit the size of the attachments so that users are compelled to attach the attachments within the given size limit.

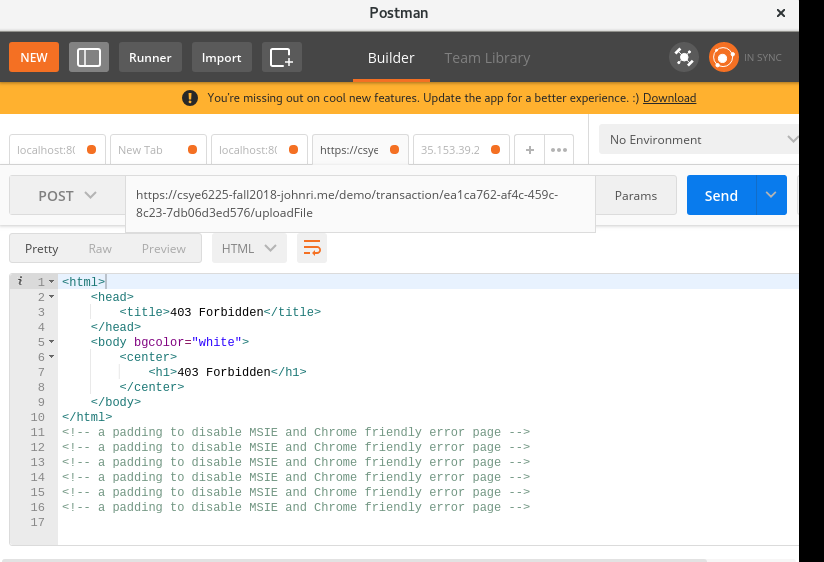
**Testing:**

Initially attachments less than 200 Mb can be attached easily to the transaction.

**Result:**

Tried attaching a file that was greater than 200 bytes which throws a Forbidden error.





**Attack Vector 3: Size constraints on requesting URL**

