CSYE-6225 SUMMER 2019
PENETRATION TESTING

Attack Vectors:

1. SQL Injection
2. File size constraint

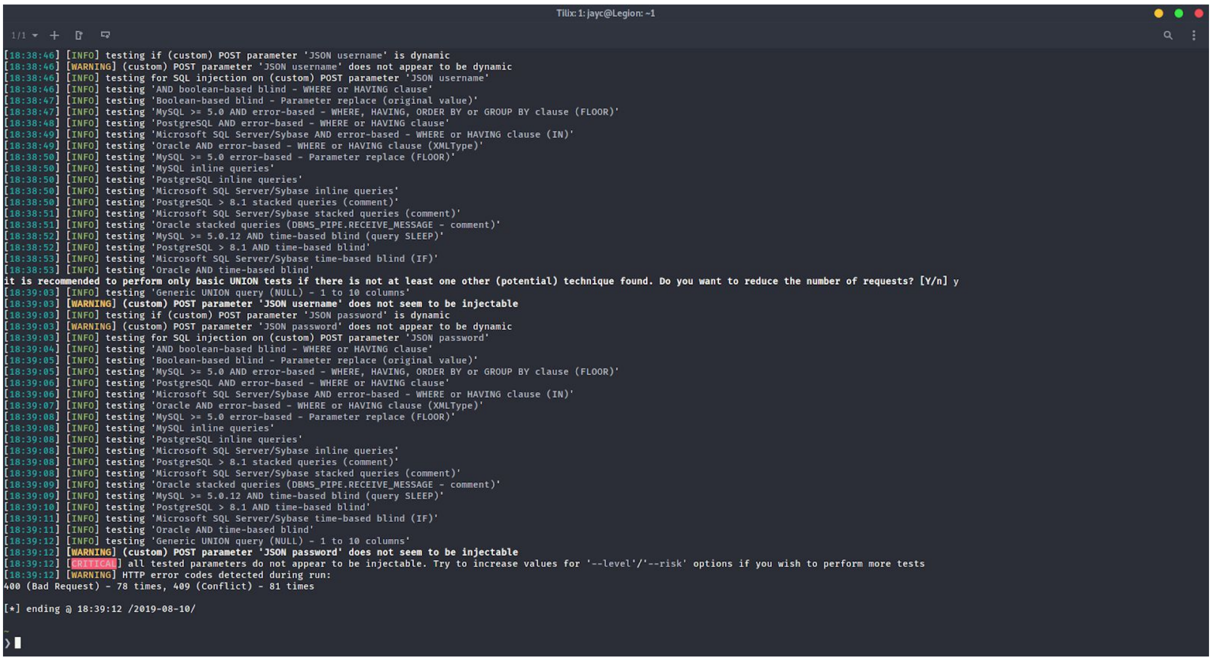
1. SQL Injection

SQL injection is an attack where it is possible to execute SQL statements through the URI. The attacker will add SQL queries in the URI which will be executed on the server. The attacker may even be able to delete the whole database if this vulnerability exists. We will test our application for any SQL injection vulnerability using sqlmap tool. The command to test our application is:

```
sqlmap -u " https://csye6225-su19-chitaliaj.me/users/register/" --method=POST
--data='{"email":"jayccc@gmail.com","password":"Test@123"}'
--tamper=space2comment
```

WAF disabled:

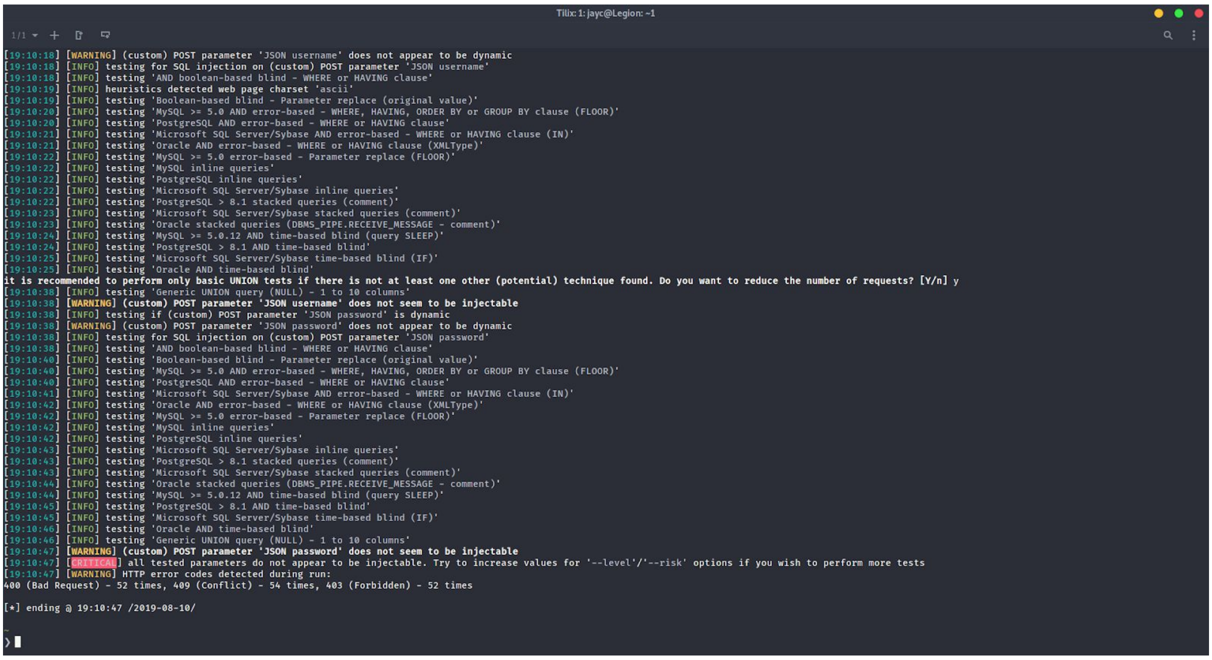
Our application is already protected from such attacks because we have used parameterized queries. The screenshot shows the response code being **400 - Bad Request or 409- Conflict.**



```
[18:38:46] [INFO] testing if (custom) POST parameter 'JSON username' is dynamic
[18:38:46] [WARNING] (custom) POST parameter 'JSON username' does not appear to be dynamic
[18:38:46] [INFO] testing for SQL injection on (custom) POST parameter 'JSON username'
[18:38:46] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[18:38:47] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[18:38:47] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[18:38:48] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[18:38:49] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[18:38:49] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[18:38:50] [INFO] testing 'MySQL >= 5.0 error-based - Parameter replace (FLOOR)'
[18:38:50] [INFO] testing 'MySQL inline queries'
[18:38:50] [INFO] testing 'PostgreSQL inline queries'
[18:38:50] [INFO] testing 'Microsoft SQL Server/Sybase inline queries'
[18:38:50] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[18:38:51] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[18:38:51] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[18:38:52] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[18:38:52] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[18:38:53] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[18:38:53] [INFO] testing 'Oracle AND time-based blind'
it is recommended to perform only basic UNION tests if there is not at least one other (potential) technique found. Do you want to reduce the number of requests? [Y/n] y
[18:39:03] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[18:39:03] [WARNING] (custom) POST parameter 'JSON username' does not seem to be injectable
[18:39:03] [INFO] testing if (custom) POST parameter 'JSON password' is dynamic
[18:39:03] [WARNING] (custom) POST parameter 'JSON password' does not appear to be dynamic
[18:39:03] [INFO] testing for SQL injection on (custom) POST parameter 'JSON password'
[18:39:04] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[18:39:05] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[18:39:05] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[18:39:06] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[18:39:06] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[18:39:07] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[18:39:08] [INFO] testing 'MySQL >= 5.0 error-based - Parameter replace (FLOOR)'
[18:39:08] [INFO] testing 'MySQL inline queries'
[18:39:08] [INFO] testing 'PostgreSQL inline queries'
[18:39:08] [INFO] testing 'Microsoft SQL Server/Sybase inline queries'
[18:39:08] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[18:39:08] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[18:39:09] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[18:39:09] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[18:39:10] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[18:39:11] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[18:39:11] [INFO] testing 'Oracle AND time-based blind'
[18:39:12] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[18:39:12] [WARNING] (custom) POST parameter 'JSON password' does not seem to be injectable
[18:39:12] [CRITICAL] all tested parameters do not appear to be injectable. Try to increase values for '--level'/'--risk' options if you wish to perform more tests
[18:39:12] [WARNING] HTTP error codes detected during run:
400 (Bad Request) - 78 times, 409 (Conflict) - 81 times

[*] ending @ 18:39:12 /2019-08-10/

~
❯
```

WAF enabled:

When WAF is enabled, response code **403 - Forbidden** is being displayed.



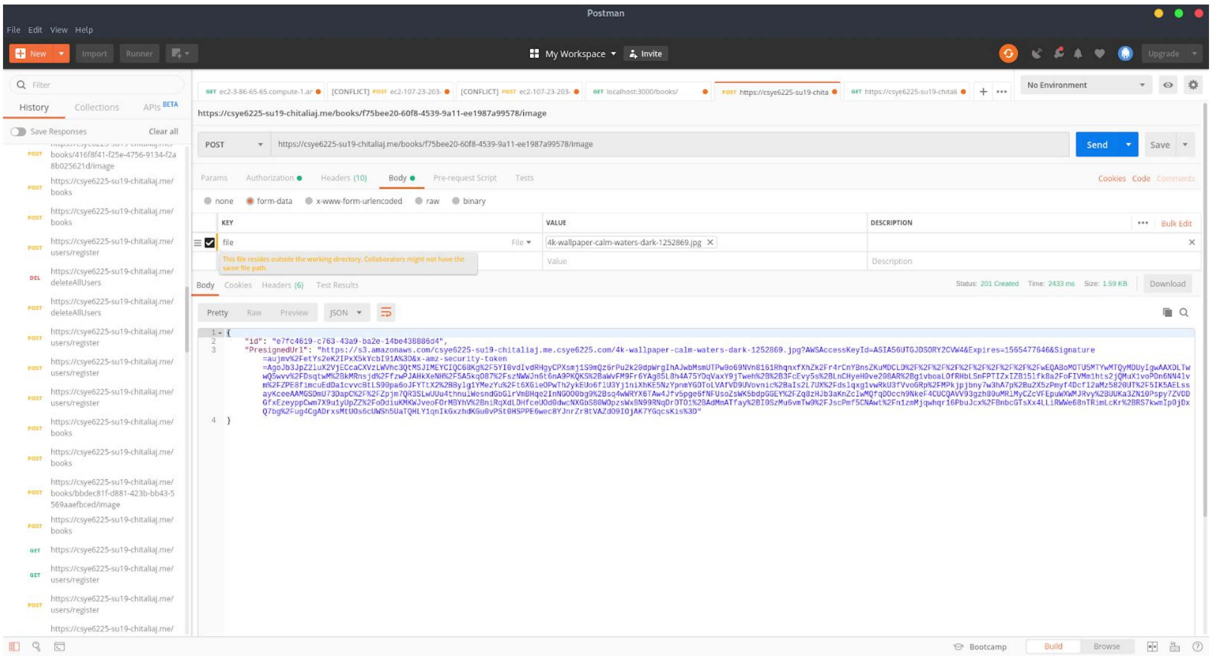
```
[19:10:18] [WARNING] (custom) POST parameter 'JSON username' does not appear to be dynamic
[19:10:18] [INFO] testing for SQL injection on (custom) POST parameter 'JSON username'
[19:10:18] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[19:10:19] [INFO] heuristics detected web page charset 'ascii'
[19:10:19] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[19:10:20] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[19:10:20] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[19:10:21] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[19:10:21] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[19:10:22] [INFO] testing 'MySQL >= 5.0 error-based - Parameter replace (FLOOR)'
[19:10:22] [INFO] testing 'MySQL inline queries'
[19:10:22] [INFO] testing 'PostgreSQL inline queries'
[19:10:22] [INFO] testing 'Microsoft SQL Server/Sybase inline queries'
[19:10:22] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[19:10:23] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[19:10:23] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[19:10:24] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[19:10:24] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[19:10:25] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[19:10:25] [INFO] testing 'Oracle AND time-based blind'
it is recommended to perform only basic UNION tests if there is not at least one other (potential) technique found. Do you want to reduce the number of requests? [Y/n] y
[19:10:38] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[19:10:38] [WARNING] (custom) POST parameter 'JSON username' does not seem to be injectable
[19:10:38] [INFO] testing if (custom) POST parameter 'JSON password' is dynamic
[19:10:38] [WARNING] (custom) POST parameter 'JSON password' does not appear to be dynamic
[19:10:38] [INFO] testing for SQL injection on (custom) POST parameter 'JSON password'
[19:10:38] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[19:10:40] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[19:10:40] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[19:10:40] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[19:10:41] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[19:10:42] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[19:10:42] [INFO] testing 'MySQL >= 5.0 error-based - Parameter replace (FLOOR)'
[19:10:42] [INFO] testing 'MySQL inline queries'
[19:10:42] [INFO] testing 'PostgreSQL inline queries'
[19:10:43] [INFO] testing 'Microsoft SQL Server/Sybase inline queries'
[19:10:43] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[19:10:43] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[19:10:44] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[19:10:44] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[19:10:45] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[19:10:45] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[19:10:46] [INFO] testing 'Oracle AND time-based blind'
[19:10:46] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[19:10:47] [WARNING] (custom) POST parameter 'JSON password' does not seem to be injectable
[19:10:47] [CRITICAL] all tested parameters do not appear to be injectable. Try to increase values for '--level'/'--risk' options if you wish to perform more tests
[19:10:47] [WARNING] HTTP error codes detected during run:
400 (Bad Request) - 52 times, 409 (Conflict) - 54 times, 403 (Forbidden) - 52 times

[*] ending @ 19:10:47 /2019-08-10/

~
❯
```

2. File Size Constraint

If the request body size exceed 4MB then it will not be allowed. We choose this attack vector because body size of over 4MB will very quickly exhaust our storage resources.

Without WAF:

The screenshot below has the body size of above **7MB** because of the image but since WAF is disabled, the request went through and it was processed.



POST books/416f8f41-f25e-4756-9134-f2a8b025621d/image
POST https://csye6225-su19-chitaliaj.me/books
POST https://csye6225-su19-chitaliaj.me/books
POST https://csye6225-su19-chitaliaj.me/users/register
DEL https://csye6225-su19-chitaliaj.me/deleteAllUsers
POST https://csye6225-su19-chitaliaj.me/deleteAllUsers
POST https://csye6225-su19-chitaliaj.me/users/register
POST https://csye6225-su19-chitaliaj.me/users/register
POST https://csye6225-su19-chitaliaj.me/users/register
POST https://csye6225-su19-chitaliaj.me/books
POST https://csye6225-su19-chitaliaj.me/books
POST https://csye6225-su19-chitaliaj.me/books/bbdec81f-d881-423b-bb43-5569aaefbced/image
POST https://csye6225-su19-chitaliaj.me/books
GET https://csye6225-su19-chitaliaj.me/
GET https://csye6225-su19-chitaliaj.me/users/register
POST https://csye6225-su19-chitaliaj.me/users/register
https://csye6225-su19-chitaliaj.me/

https://csye6225-su19-chitaliaj.me/books/f75bee20-60f8-4539-9a11-ee1987a99578/image

POST https://csye6225-su19-chitaliaj.me/books/f75bee20-60f8-4539-9a11-ee1987a99578/image

○ none ● form-data ○ x-www-form-urlencoded ○ raw ○ binary

	KEY	VALUE	DESCRIPTION
☑	file (File)	4k-wallpaper-calm-waters-dark-1252869.jpg	
		Value	Description

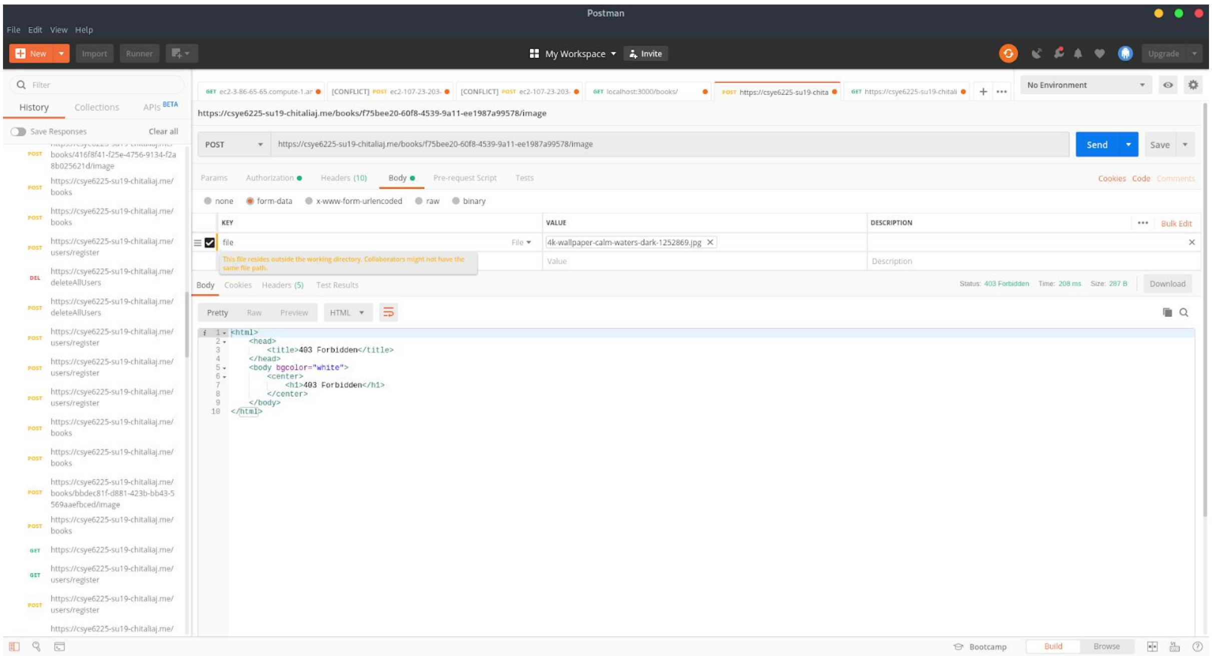
This file resides outside the working directory. Collaborators might not have the same file path.

Status: 201 Created Time: 2433 ms Size: 1.59 KB

```
{
    "id": "e7fc4619-c763-43a9-ba2e-14be438886d4",
    "PresignedUrl": "https://s3.amazonaws.com/csye6225-su19-chitaliaj.me.csye6225.com/4k-wallpaper-calm-waters-dark-1252869.jpg?AWSAccessKeyId=ASIA56UTGJDSORY2CVW4&Expires=1565477646&Signature
        =aujmv%2FetYs2eK2IPxX5kYcbI91A%3D&x-amz-security-token
        =AgoJb3JpZ2luX2VjECcaCXVzLWVhc3QtMSJIMEYCIQC68Kg%2F5YI0vdIvdRHgyCPXsmj1S9mQz6rPu2k20dpWrgIhAJwbMsmUTPw9o69NVn8161RhqnxfXhZk2Fr4rCnYBnsZKuMDCLD%2F%2F%2F%2F%2F%2F%2F%2F%2F%2F%2FwEQABoMOTU5MTYwMTQyMDUyIgwAAXDLTw
        wQ5wvv%2FDsqtwM%2BkMRnsjd%2FfzwPJAHkXeNH%2F5A5kq087%2FszNWWJn6t6nA9PKQKS%2BaWvFM9Fr6YAg85L8h4A75YDqVaxY9jTweh%2B%2B3FcEvy5s%2BLnCHyeH0ve208AR%2Bg1vboaLOfRHbLSnFPTIZxIZB15lfk8a2FoFIVMm1hts2jQMuX1voPDn6NN4lv
        m%2FZPE8fimcuEdDa1cvvcBtLS90pa6oJFYTtX2%2BBylg1YMezYu%2Ft6XGieOPwTh2ykEUo6flU3YjlniXhKE5NzYpnmYGDToLVAfVD9UVovnic%2BaIs2L7UX%2Fdslqxg1vwRkU3fVvoGRp%2FMPkjpjbny7w3hA7p%2Bu2X5zPmyf4Dcfl2aMz5820UT%2F5IK5AELss
        ayKceeAAMGSDmU73DapC%2F%2FZpjm7QR3SLwUUu4thnulWesndGbGlrVmBHqe2InNGOO0bg9%2Bsq4wWRYX6TAw4Jfv5pge6fNFUsoZsWK5bdpGGEY%2FZq8zHJb3aKnZcIwMQfqDOcch9NkeF4CUCQAVV93gzh80uMRlMyCZcVFEpuWXWMJRvy%2BUUKa3ZN10Pspy7ZVOD
        GfxEzeyppCwm7X9u1yUpZZ%2FoDdiuKMKWJveoFOrMBYhV%2BniRqXdLDHfceUOd0dwcNXGbS80WOpzsWx8N99RNqDrDTO1%2BAdMmATfay%2BI0SzMu6vmTw0%2FJscPmf5CNAwt%2Fn1zmMjqwhqr16PbuJcx%2FBnbcGTsXx4LLiRWWe68nTRimLcKr%2BRS7kwmIp0jDx
        Q7bg%2Fug4CgADrxsMtUOs6cUWSh5UaTQHLY1qnIkGxzhdKGu0vPSt0HSPPE6wec8YJnrZrBtVAZdO9IOjAK7YGqcsKis%3D"
}
```

WAF enabled:

With WAF enabled, the request will not go through and **403 - Forbidden** will be the response.



GET ec2-3-86-65-65.compute-1.ar | [CONFLICT] POST ec2-107-23-203- | [CONFLICT] POST ec2-107-23-203- | GET localhost:3000/books/ | POST https://csye6225-su19-chita | GET https://csye6225-su19-chitali

POST books/416f8f41-f25e-4756-9134-f2a8b025621d/image
POST https://csye6225-su19-chitaliaj.me/books
POST https://csye6225-su19-chitaliaj.me/books
POST https://csye6225-su19-chitaliaj.me/users/register
DEL https://csye6225-su19-chitaliaj.me/deleteAllUsers
POST https://csye6225-su19-chitaliaj.me/deleteAllUsers
POST https://csye6225-su19-chitaliaj.me/users/register
POST https://csye6225-su19-chitaliaj.me/users/register
POST https://csye6225-su19-chitaliaj.me/users/register
POST https://csye6225-su19-chitaliaj.me/books
POST https://csye6225-su19-chitaliaj.me/books
POST https://csye6225-su19-chitaliaj.me/books/bbdec81f-d881-423b-bb43-5569aaefbced/image
POST https://csye6225-su19-chitaliaj.me/books
GET https://csye6225-su19-chitaliaj.me/
GET https://csye6225-su19-chitaliaj.me/users/register
POST https://csye6225-su19-chitaliaj.me/users/register
https://csye6225-su19-chitaliaj.me/

https://csye6225-su19-chitaliaj.me/books/f75bee20-60f8-4539-9a11-ee1987a99578/image

POST https://csye6225-su19-chitaliaj.me/books/f75bee20-60f8-4539-9a11-ee1987a99578/image

○ none ● form-data ○ x-www-form-urlencoded ○ raw ○ binary

	KEY	VALUE	DESCRIPTION
☑	file (File)	4k-wallpaper-calm-waters-dark-1252869.jpg	
		Value	Description

This file resides outside the working directory. Collaborators might not have the same file path.

Status: 403 Forbidden Time: 208 ms Size: 287 B

```
<html>
    <head>
        <title>403 Forbidden</title>
    </head>
    <body bgcolor="white">
        <center>
            <h1>403 Forbidden</h1>
        </center>
    </body>
</html>
```