Penetration Testing Report

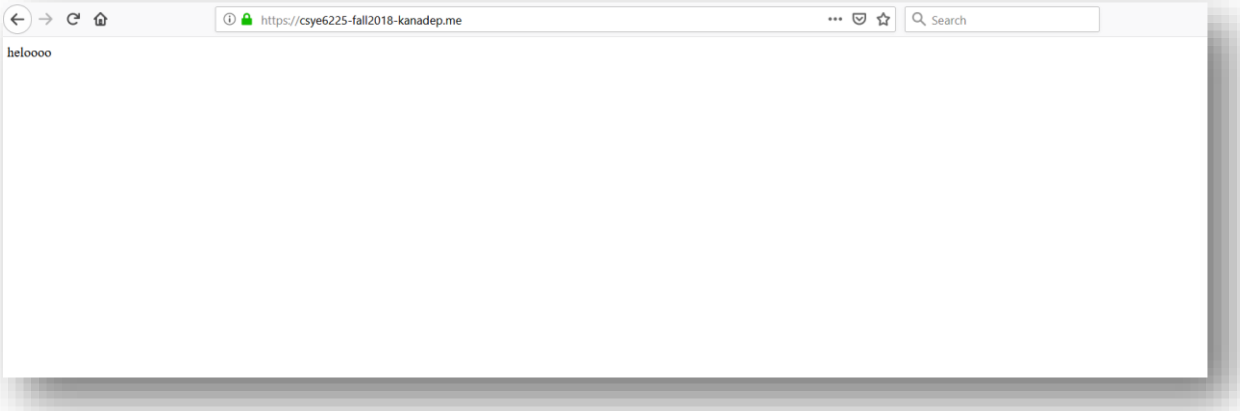
1.

IP Blacklist: Matches IP addresses that should not be allowed to access content.

Result:

Without rules

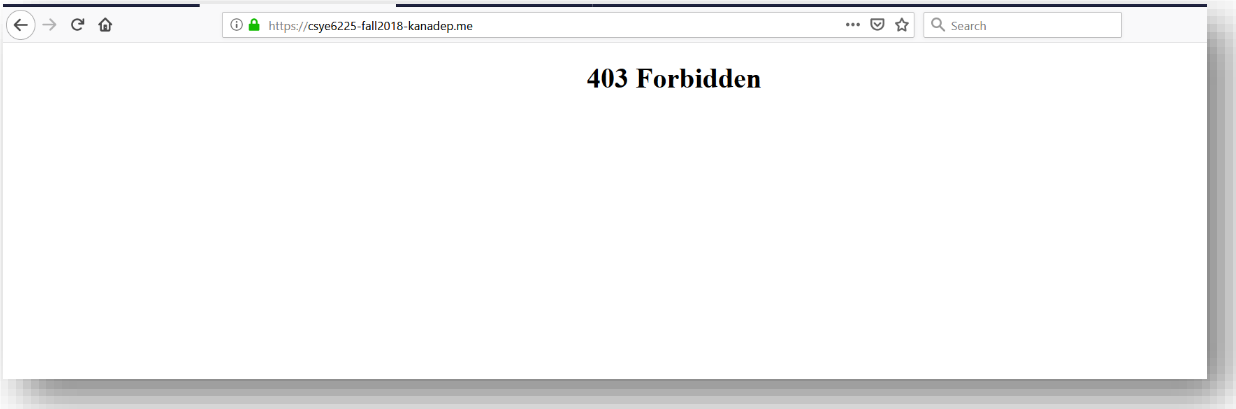
url: https://csye6225-fall2018-bengret.me/



heloooo

With rules

url: https://csye6225-fall2018-kanadep.me/



403 Forbidden

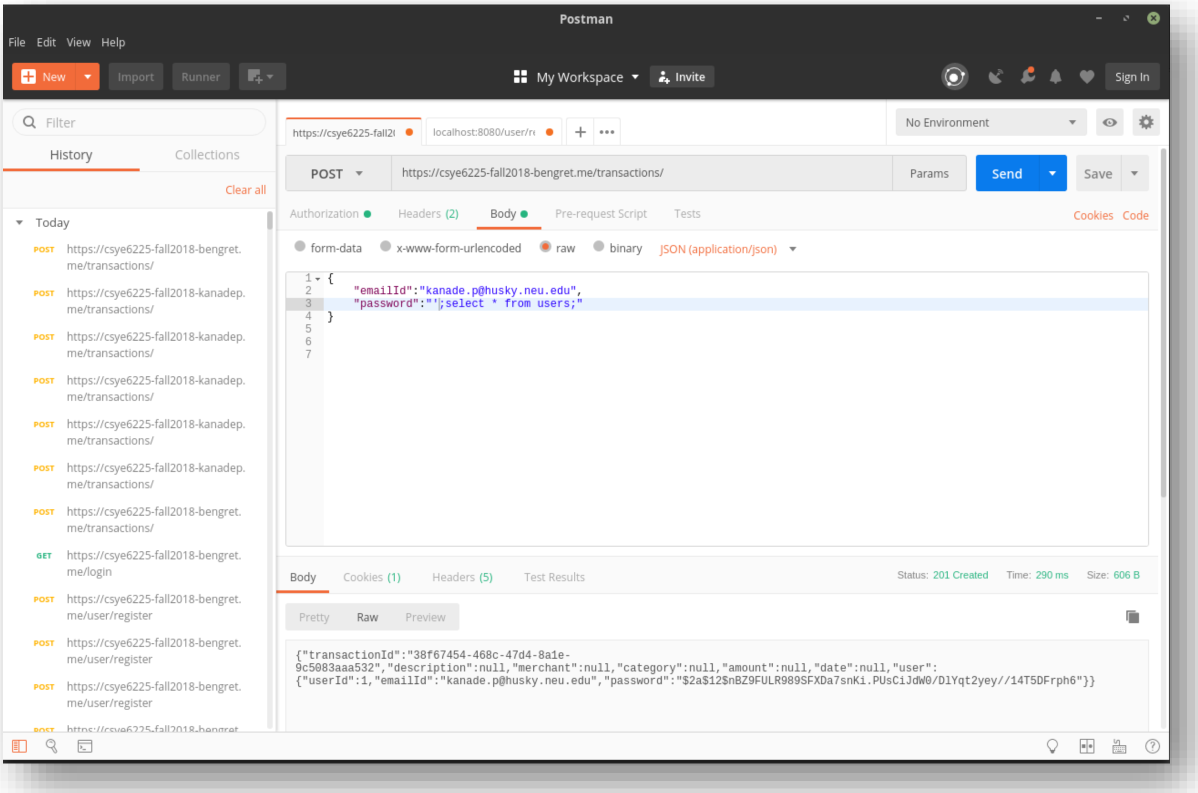
Why?

Having the white list of IPs, reduces the attack surface by denying traffic from blocked IPs.

2. **SQL Injection Attacks:** Matches attempted SQLi patterns in the BODY
Result:

Without rules

url: https://csye6225-fall2018-bengret.me/transactions/


Postman
File Edit View Help
New
Import
Runner
My Workspace
Invite
Sign In
Filter
History
Collections
Clear all
Today
POST https://csye6225-fall2018-bengret.me/transactions/
POST https://csye6225-fall2018-kanadep.me/transactions/
POST https://csye6225-fall2018-kanadep.me/transactions/
POST https://csye6225-fall2018-kanadep.me/transactions/
POST https://csye6225-fall2018-kanadep.me/transactions/
POST https://csye6225-fall2018-kanadep.me/transactions/
POST https://csye6225-fall2018-bengret.me/transactions/
GET https://csye6225-fall2018-bengret.me/login
POST https://csye6225-fall2018-bengret.me/user/register
POST https://csye6225-fall2018-bengret.me/user/register
POST https://csye6225-fall2018-bengret.me/user/register
POST https://csye6225-fall2018-bengret
https://csye6225-fall2(
localhost:8080/user/re
No Environment
Params
Send
Save
Authorization
Headers (2)
Body
Pre-request Script
Tests
Cookies
Code
Cookies (1)
Headers (5)
Test Results
Pretty
Raw
Preview

POST https://csye6225-fall2018-bengret.me/transactions/

Body: ○ form-data ○ x-www-form-urlencoded ● raw ○ binary JSON (application/json)

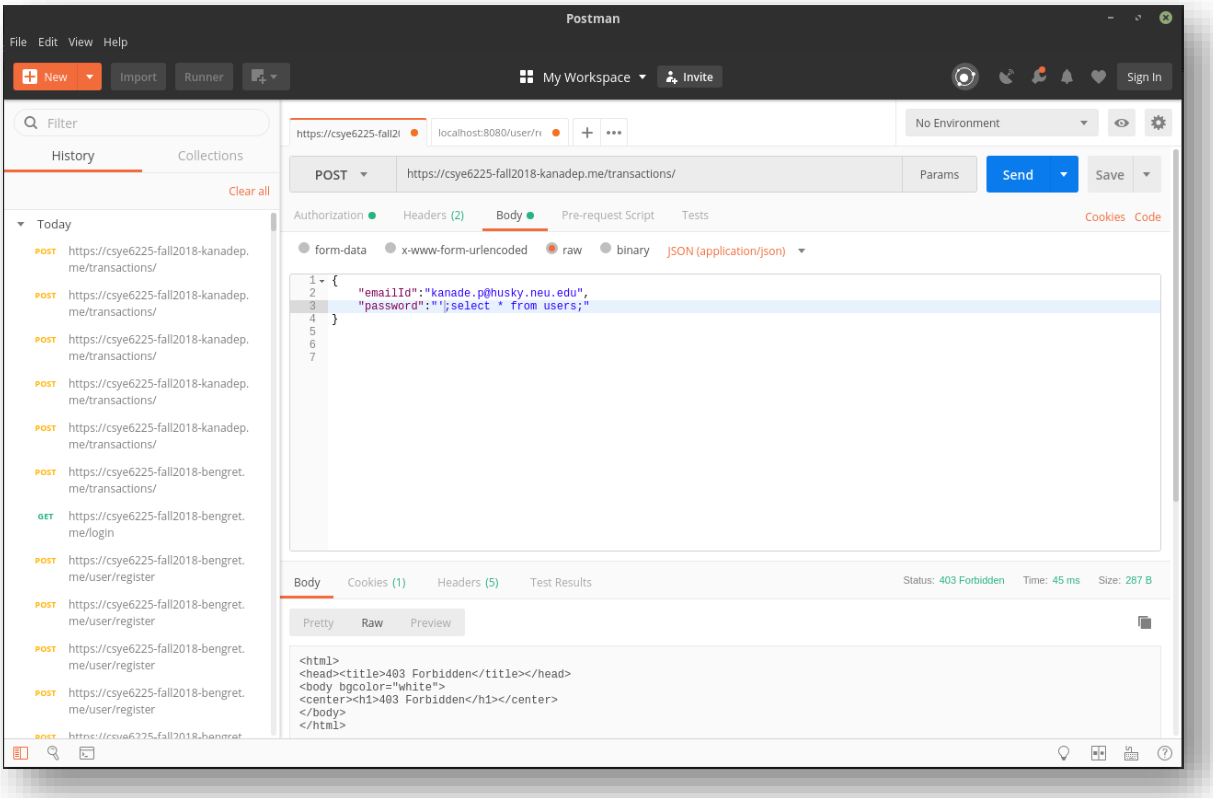
```
{
    "emailId":"kanade.p@husky.neu.edu",
    "password":"';select * from users;"
}
```

Status: 201 Created Time: 290 ms Size: 606 B

```
{"transactionId":"38f67454-468c-47d4-8a1e-
9c5083aaa532","description":null,"merchant":null,"category":null,"amount":null,"date":null,"user":
{"userId":1,"emailId":"kanade.p@husky.neu.edu","password":"$2a$12$nBZ9FULR989SFXDa7snKi.PUsCiJdW0/DlYqt2yey//14T5DFrph6"}}
```

With rules

url: https://csye6225-fall2018-kanadep.me/ transactions/



Postman

History

Today

- POST https://csye6225-fall2018-kanadep.me/transactions/
- POST https://csye6225-fall2018-kanadep.me/transactions/
- POST https://csye6225-fall2018-kanadep.me/transactions/
- POST https://csye6225-fall2018-kanadep.me/transactions/
- POST https://csye6225-fall2018-kanadep.me/transactions/
- POST https://csye6225-fall2018-bengret.me/transactions/
- GET https://csye6225-fall2018-bengret.me/login
- POST https://csye6225-fall2018-bengret.me/user/register
- POST https://csye6225-fall2018-bengret.me/user/register
- POST https://csye6225-fall2018-bengret.me/user/register
- POST https://csye6225-fall2018-bengret.me/user/register
- POST https://csye6225-fall2018-bengret

POST https://csye6225-fall2018-kanadep.me/transactions/

Body: ○ form-data ○ x-www-form-urlencoded ● raw ○ binary JSON (application/json)

```
{
    "emailId":"kanade.p@husky.neu.edu",
    "password":"';select * from users;"
}
```

Status: 403 Forbidden Time: 45 ms Size: 287 B

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

Why?

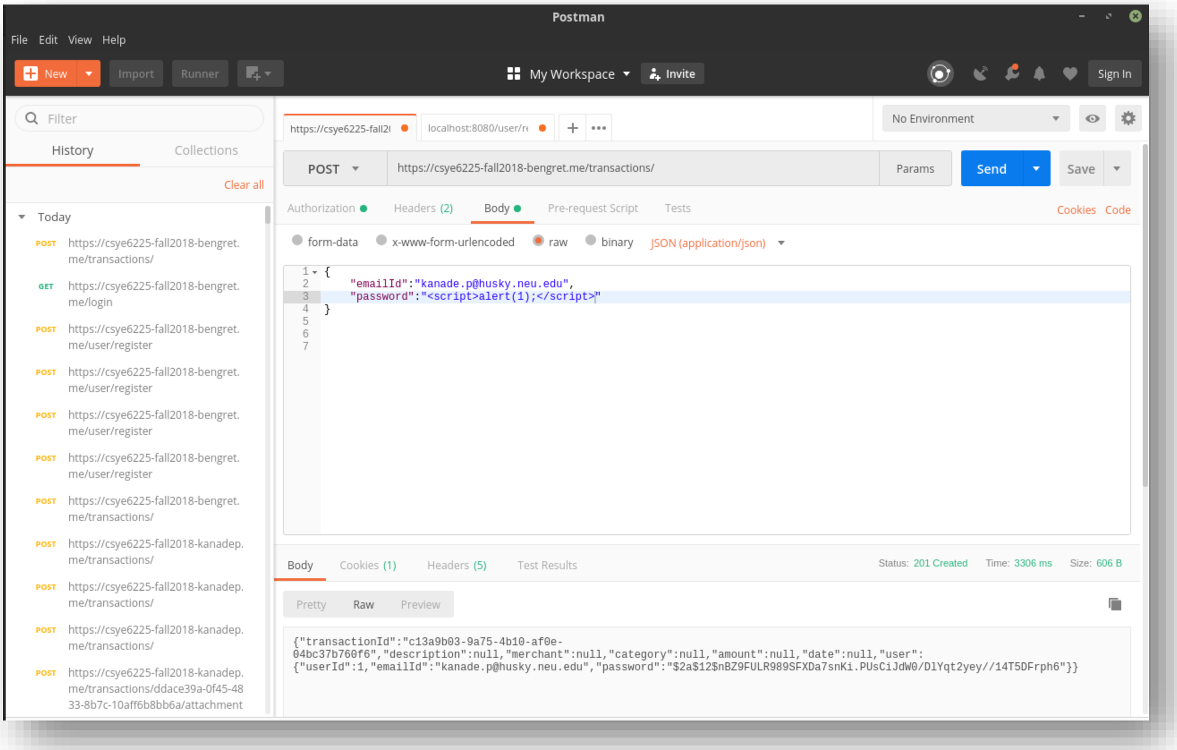
Most application stores sensitive data in databases which when reveals causes great business impact.

3. **Cross Site Scripting Attacks:** Matches attemped XSS patterns in the BODY.

Result:

<u>Without rules</u>

url: https://csye6225-fall2018-bengret.me/transactions/



POST https://csye6225-fall2018-bengret.me/transactions/

Body: ○ form-data ○ x-www-form-urlencoded ● raw ○ binary JSON (application/json)

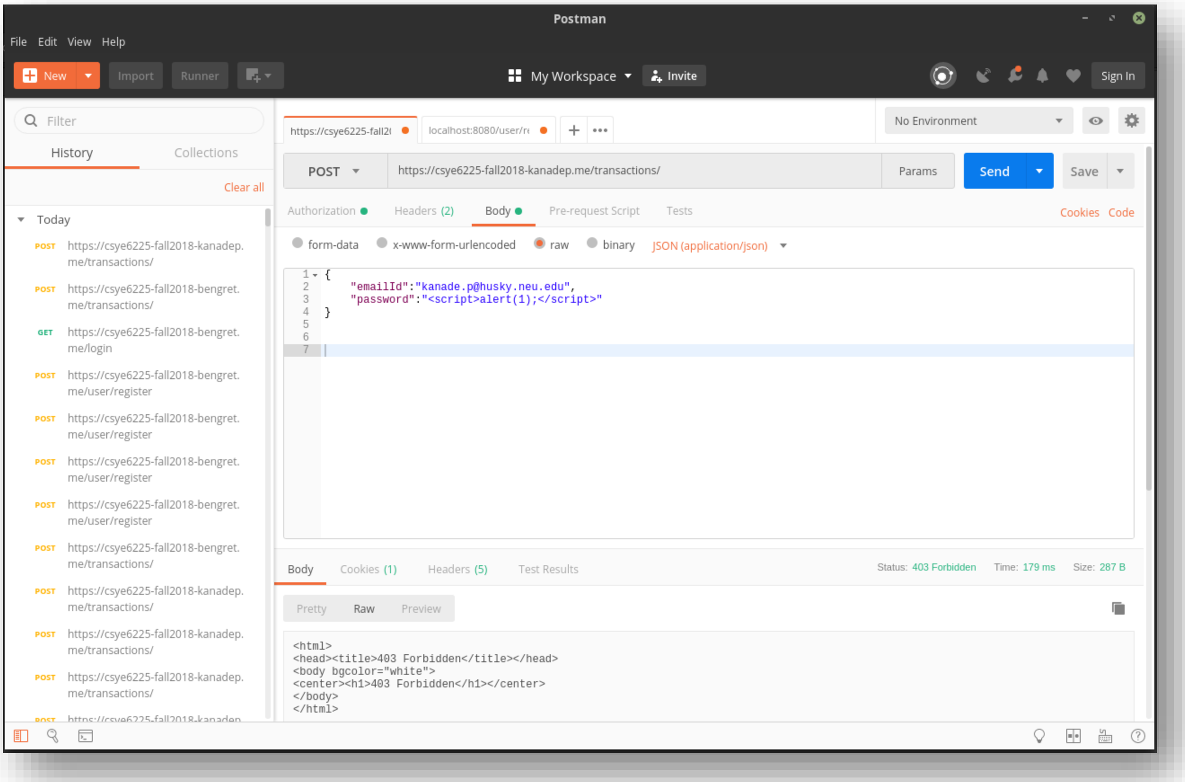
```
{
    "emailId":"kanade.p@husky.neu.edu",
    "password":"<script>alert(1);</script>"
}
```

Body Cookies (1) Headers (5) Test Results Status: 201 Created Time: 3306 ms Size: 606 B

```
{"transactionId":"c13a9b03-9a75-4b10-af0e-
04bc37b760f6","description":null,"merchant":null,"category":null,"amount":null,"date":null,"user":
{"userId":1,"emailId":"kanade.p@husky.neu.edu","password":"$2a$12$nBZ9FULR989SFXDa7snKi.PUsCiJdW0/DlYqt2yey//14T5DFrph6"}}
```

POST https://csye6225-fall2018-bengret.me/transactions/
GET https://csye6225-fall2018-bengret.me/login
POST https://csye6225-fall2018-bengret.me/user/register
POST https://csye6225-fall2018-bengret.me/user/register
POST https://csye6225-fall2018-bengret.me/user/register
POST https://csye6225-fall2018-bengret.me/user/register
POST https://csye6225-fall2018-bengret.me/transactions/
POST https://csye6225-fall2018-kanadep.me/transactions/
POST https://csye6225-fall2018-kanadep.me/transactions/
POST https://csye6225-fall2018-kanadep.me/transactions/
POST https://csye6225-fall2018-kanadep.me/transactions/ddace39a-0f45-4833-8b7c-10aff6b8bb6a/attachment

With rules
url: https://csye6225-fall2018-kanadep.me/transactions/



- POST https://csye6225-fall2018-kanadep.me/transactions/
- POST https://csye6225-fall2018-bengret.me/transactions/
- GET https://csye6225-fall2018-bengret.me/login
- POST https://csye6225-fall2018-bengret.me/user/register
- POST https://csye6225-fall2018-bengret.me/user/register
- POST https://csye6225-fall2018-bengret.me/user/register
- POST https://csye6225-fall2018-bengret.me/user/register
- POST https://csye6225-fall2018-bengret.me/transactions/
- POST https://csye6225-fall2018-kanadep.me/transactions/
- POST https://csye6225-fall2018-kanadep.me/transactions/
- POST https://csye6225-fall2018-kanadep.me/transactions/
- POST https://csye6225-fall2018-kanadep.

POST https://csye6225-fall2018-kanadep.me/transactions/

Body: ○ form-data ○ x-www-form-urlencoded ● raw ○ binary JSON (application/json)

```
{
    "emailId":"kanade.p@husky.neu.edu",
    "password":"<script>alert(1);</script>"
}


```

Body Status: 403 Forbidden Time: 179 ms Size: 287 B

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

Why?

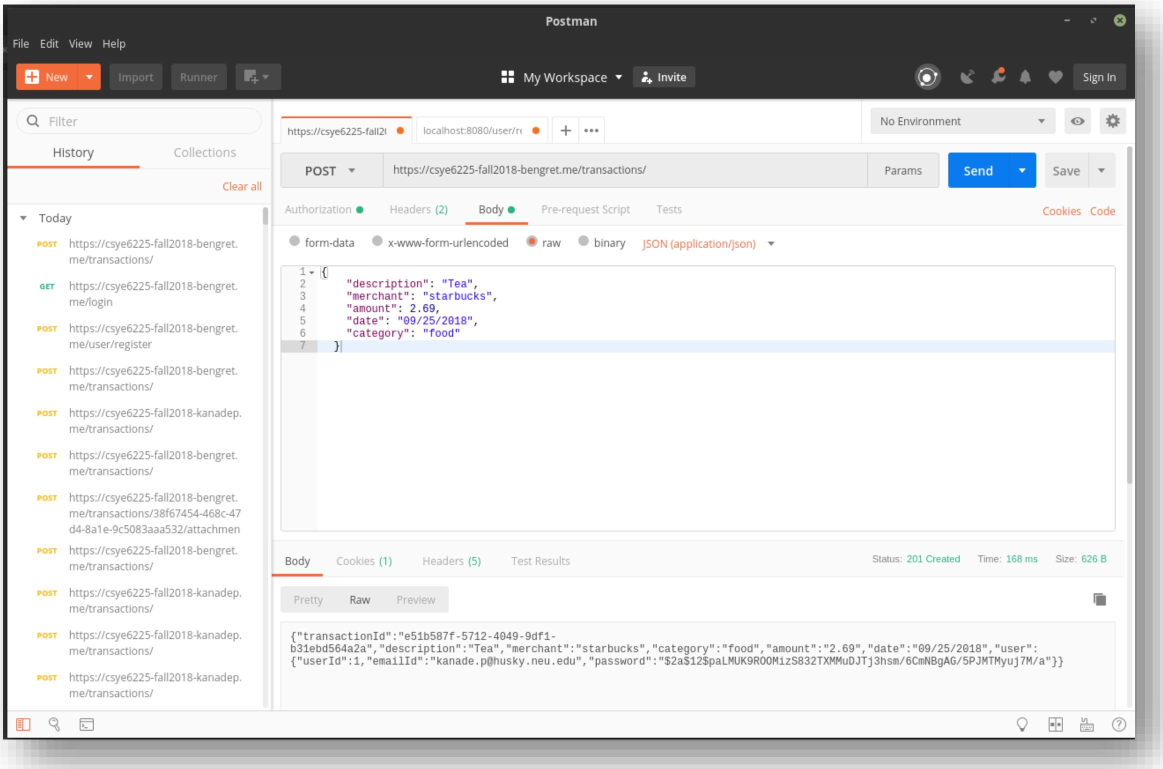
Script injection are one of the easiest forms of injection which may be used to reveal session cookies, which opens the application to more serious attacks. Hence safe guarding the application is very important.

4. **Size restrictions:** Enforce consistent request hygiene, limit size of key elements.

Result:

<u>Without rules</u>

url: https://csye6225-fall2018-bengret.me/transactions/



History:

- POST https://csye6225-fall2018-bengret.me/transactions/
- GET https://csye6225-fall2018-bengret.me/login
- POST https://csye6225-fall2018-bengret.me/user/register
- POST https://csye6225-fall2018-bengret.me/transactions/
- POST https://csye6225-fall2018-kanadep.me/transactions/
- POST https://csye6225-fall2018-bengret.me/transactions/
- POST https://csye6225-fall2018-bengret.me/transactions/38f67454-468c-47d4-8a1e-9c5083aaa532/attachmen
- POST https://csye6225-fall2018-bengret.me/transactions/
- POST https://csye6225-fall2018-kanadep.me/transactions/
- POST https://csye6225-fall2018-kanadep.me/transactions/
- POST https://csye6225-fall2018-kanadep.me/transactions/

POST https://csye6225-fall2018-bengret.me/transactions/

○ form-data ○ x-www-form-urlencoded ● raw ○ binary JSON (application/json)

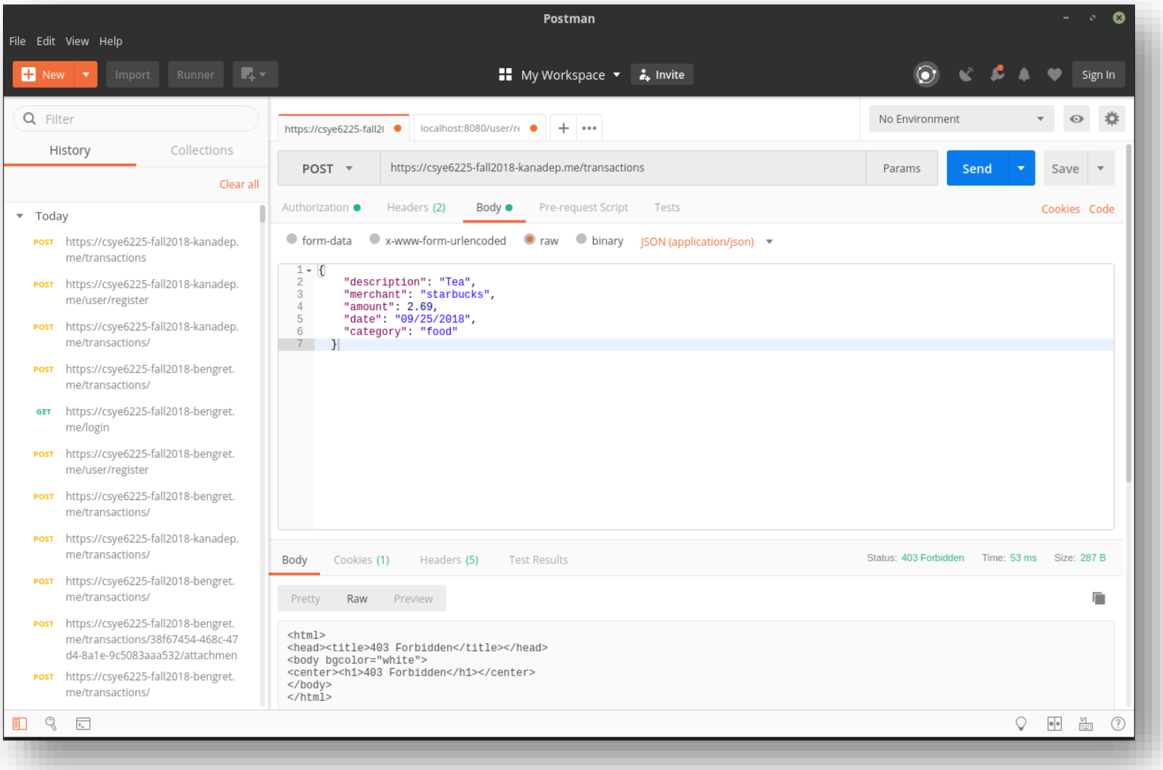
```
{
    "description": "Tea",
    "merchant": "starbucks",
    "amount": 2.69,
    "date": "09/25/2018",
    "category": "food"
  }
```

Body Cookies (1) Headers (5) Test Results Status: 201 Created Time: 168 ms Size: 626 B

```
{"transactionId":"e51b587f-5712-4049-9df1-
b31ebd564a2a","description":"Tea","merchant":"starbucks","category":"food","amount":"2.69","date":"09/25/2018","user":
{"userId":1,"emailId":"kanade.p@husky.neu.edu","password":"$2a$12$paLMUK9ROOMizS832TXMMuDJTj3hsm/6CmNBgAG/5PJMTMyuj7M/a"}}
```

With rules

url: https://csye6225-fall2018-kanadep.me/transactions/



POST https://csye6225-fall2018-kanadep.me/transactions

POST https://csye6225-fall2018-kanadep.me/transactions
POST https://csye6225-fall2018-kanadep.me/user/register
POST https://csye6225-fall2018-kanadep.me/transactions/
POST https://csye6225-fall2018-bengret.me/transactions/
GET https://csye6225-fall2018-bengret.me/login
POST https://csye6225-fall2018-bengret.me/user/register
POST https://csye6225-fall2018-bengret.me/transactions/
POST https://csye6225-fall2018-kanadep.me/transactions/
POST https://csye6225-fall2018-bengret.me/transactions/
POST https://csye6225-fall2018-bengret.me/transactions/38f67454-468c-47d4-8a1e-9c5083aaa532/attachmen
POST https://csye6225-fall2018-bengret.me/transactions/

```
{
    "description": "Tea",
    "merchant": "starbucks",
    "amount": 2.69,
    "date": "09/25/2018",
    "category": "food"
  }
```

Status: 403 Forbidden Time: 53 ms Size: 287 B

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

Why?

Uploading size consumes the resources in the server end which might create denial of service attacks. Hence checking for the file size and extensions is the good practise.