Assignment -10
Penetration Testing Report

AWS WAF is a web application firewall which allows you to monitor the HTTP and HTTPS requests that are forwarded to an Amazon API Gateway API, Amazon CloudFront or an Application Load Balancer. It also allows controlled access to your content. Based on your rules such as the IP addresses that requests originate from or the values of query strings, CloudFront or an Application Load Balancer responds to requests either with the requested content or with an HTTP 403 status code (Forbidden).

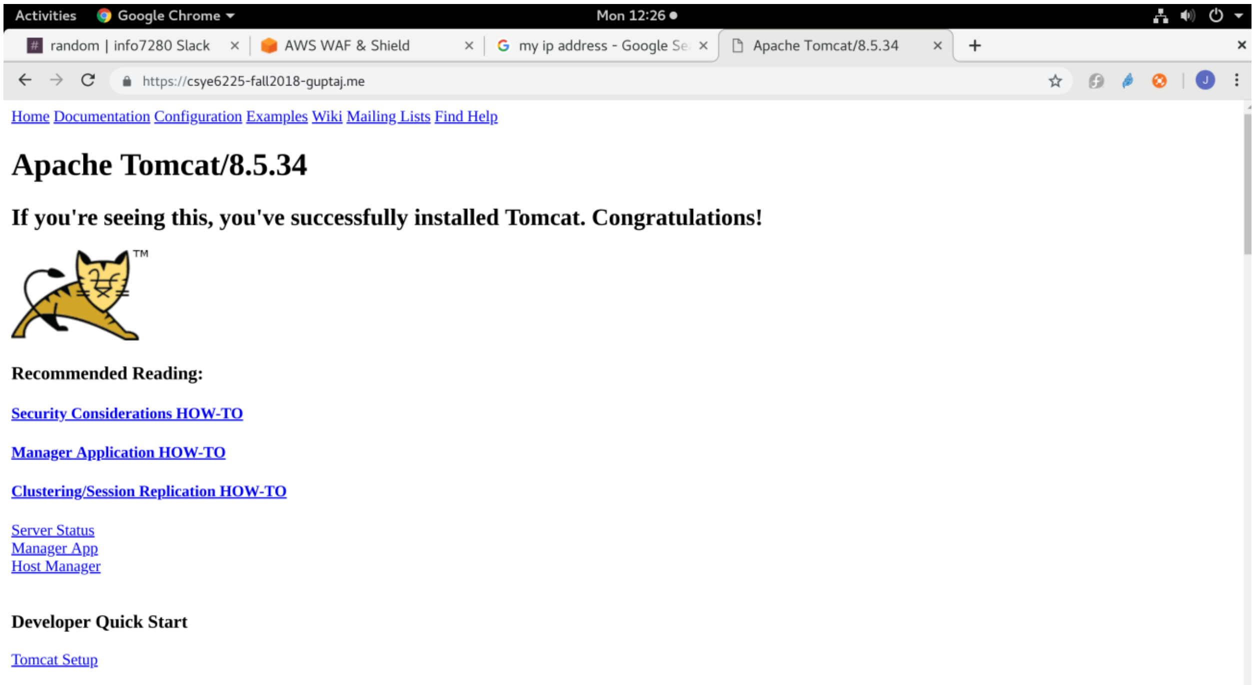
Attack Vectors:

- **IP Blacklist**

  This attack vector allows to matches IP addresses that should not be allowed to access content. IP address blacklisting is a method of protecting Web and other Internet servers from malicious attacks. This is accomplished by setting rules within server software or hardware routers regarding what traffic will be considered an attack, and then preventing the computers creating that traffic from connecting again.

  Screenshot without WAF:

  This image shows we are able to hit the request.


Activities
Google Chrome
Mon 12:26
random | info7280 Slack
AWS WAF & Shield
my ip address - Google Se
Apache Tomcat/8.5.34
https://csye6225-fall2018-guptaj.me
Home Documentation Configuration Examples Wiki Mailing Lists Find Help

Apache Tomcat/8.5.34

If you're seeing this, you've successfully installed Tomcat. Congratulations!

Recommended Reading:

Security Considerations HOW-TO

Manager Application HOW-TO

Clustering/Session Replication HOW-TO

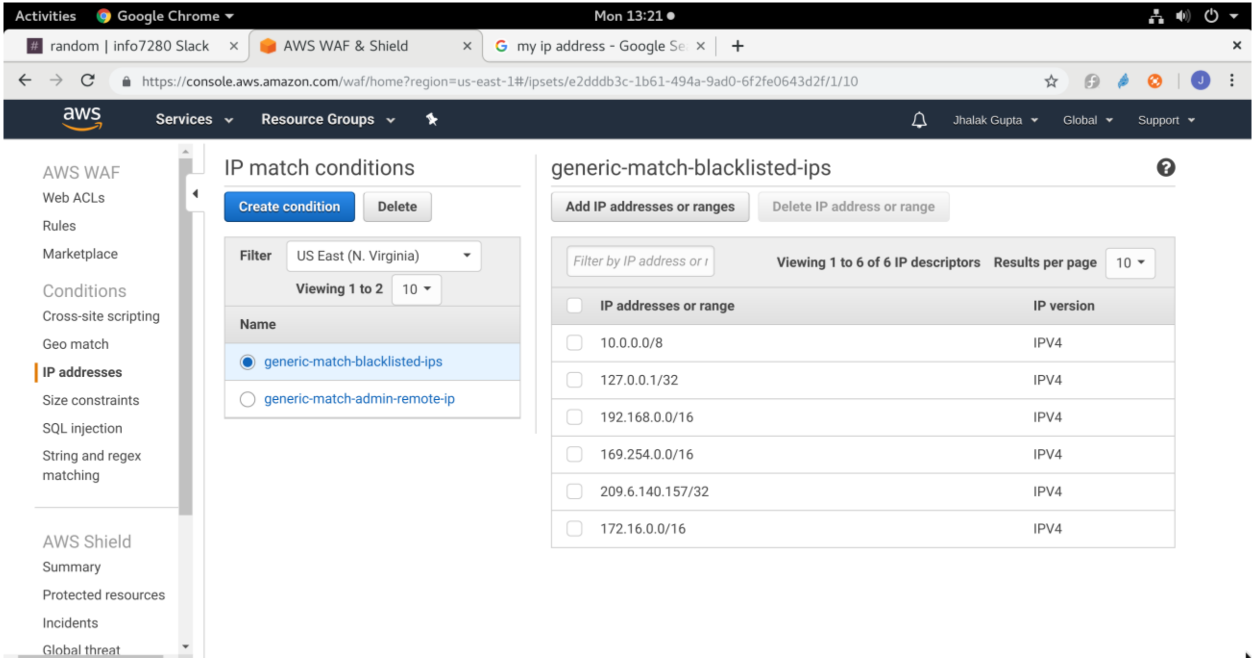
Server Status
Manager App
Host Manager

Developer Quick Start

Tomcat Setup

Screenshot with WAF:

Below image shows the rule which lists blacklisted IPs:



https://console.aws.amazon.com/waf/home?region=us-east-1#/ipsets/e2dddb3c-1b61-494a-9ad0-6f2fe0643d2f/1/10

IP match conditions

Filter: US East (N. Virginia)

Viewing 1 to 2 10

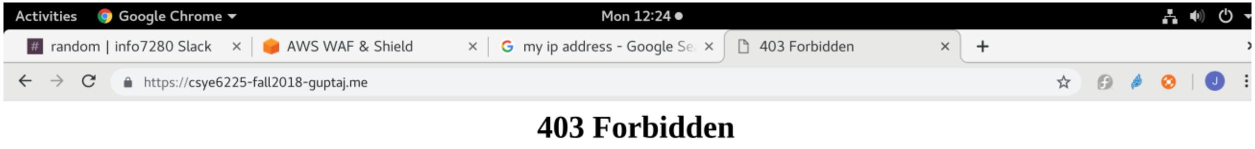
Name
● generic-match-blacklisted-ips
○ generic-match-admin-remote-ip

generic-match-blacklisted-ips

Viewing 1 to 6 of 6 IP descriptors Results per page 10

□ IP addresses or range	IP version
□ 10.0.0.0/8	IPV4
□ 127.0.0.1/32	IPV4
□ 192.168.0.0/16	IPV4
□ 169.254.0.0/16	IPV4
□ 209.6.140.157/32	IPV4
□ 172.16.0.0/16	IPV4

After this rule is applied, the request from blacklisted IP address is forbidden:



https://csye6225-fall2018-guptaj.me

403 Forbidden

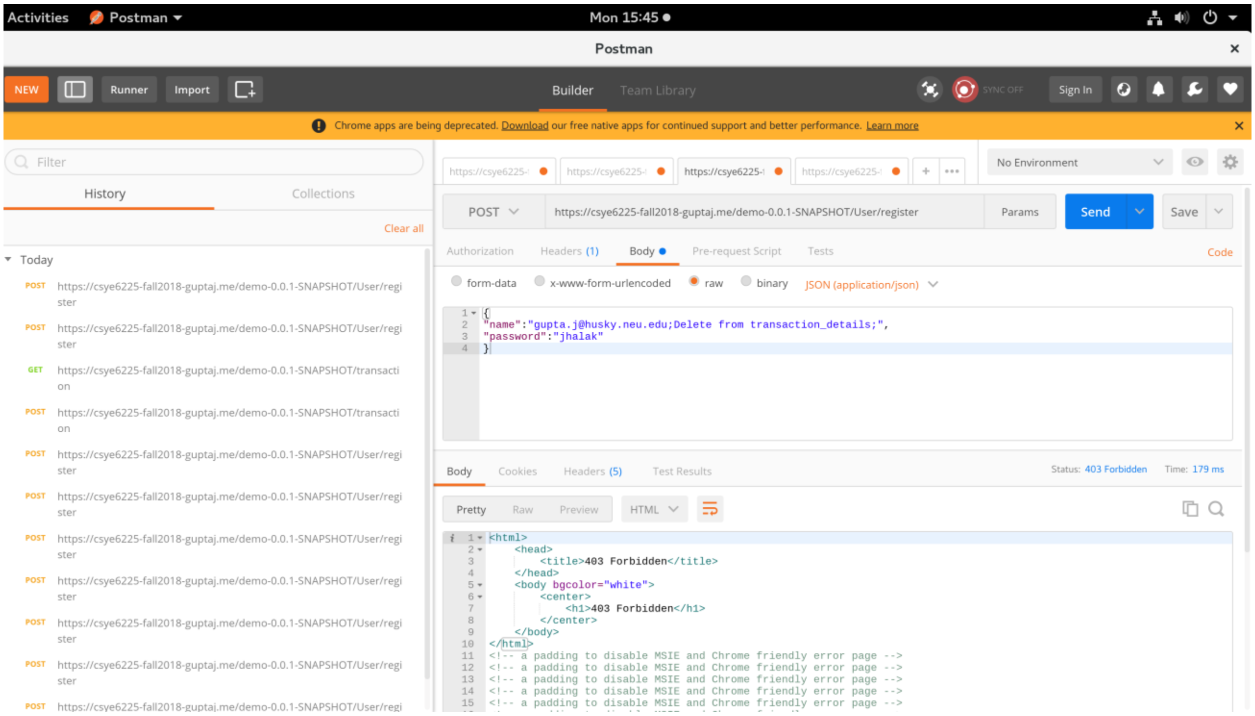
We have chosen this attack vector because there are a lot of malicious users or attackers who tries to attack your web application. So once you identify you can add such IPs to blacklists to protect your web application from such attacks.

- ### SQL Injection:

  SQL injection is a code injection technique that might destroy your database. SQL injection is one of the most common web hacking techniques. SQL injection is the placement of malicious code in SQL statements, via web page input. It usually occurs when you ask a user for input, like their username/userid, and instead of a name/id, the user gives you an SQL statement that you will **unknowingly** run on your database.

  Screenshot with WAF:

  At the time of user register if we enter username and append a query to delete transactions it says 403 forbidden because the WAF rule is in place to mitigate SQL Injection Attacks.



POST https://csye6225-fall2018-guptaj.me/demo-0.0.1-SNAPSHOT/User/register
POST https://csye6225-fall2018-guptaj.me/demo-0.0.1-SNAPSHOT/User/register
GET https://csye6225-fall2018-guptaj.me/demo-0.0.1-SNAPSHOT/transaction
POST https://csye6225-fall2018-guptaj.me/demo-0.0.1-SNAPSHOT/transaction
POST https://csye6225-fall2018-guptaj.me/demo-0.0.1-SNAPSHOT/User/register
POST https://csye6225-fall2018-guptaj.me/demo-0.0.1-SNAPSHOT/User/register
POST https://csye6225-fall2018-guptaj.me/demo-0.0.1-SNAPSHOT/User/register
POST https://csye6225-fall2018-guptaj.me/demo-0.0.1-SNAPSHOT/User/register
POST https://csye6225-fall2018-guptaj.me/demo-0.0.1-SNAPSHOT/User/register
POST https://csye6225-fall2018-guptaj.me/demo-0.0.1-SNAPSHOT/User/register
POST https://csye6225-fall2018-guptaj.me/demo-0.0.1-SNAPSHOT/User/regi

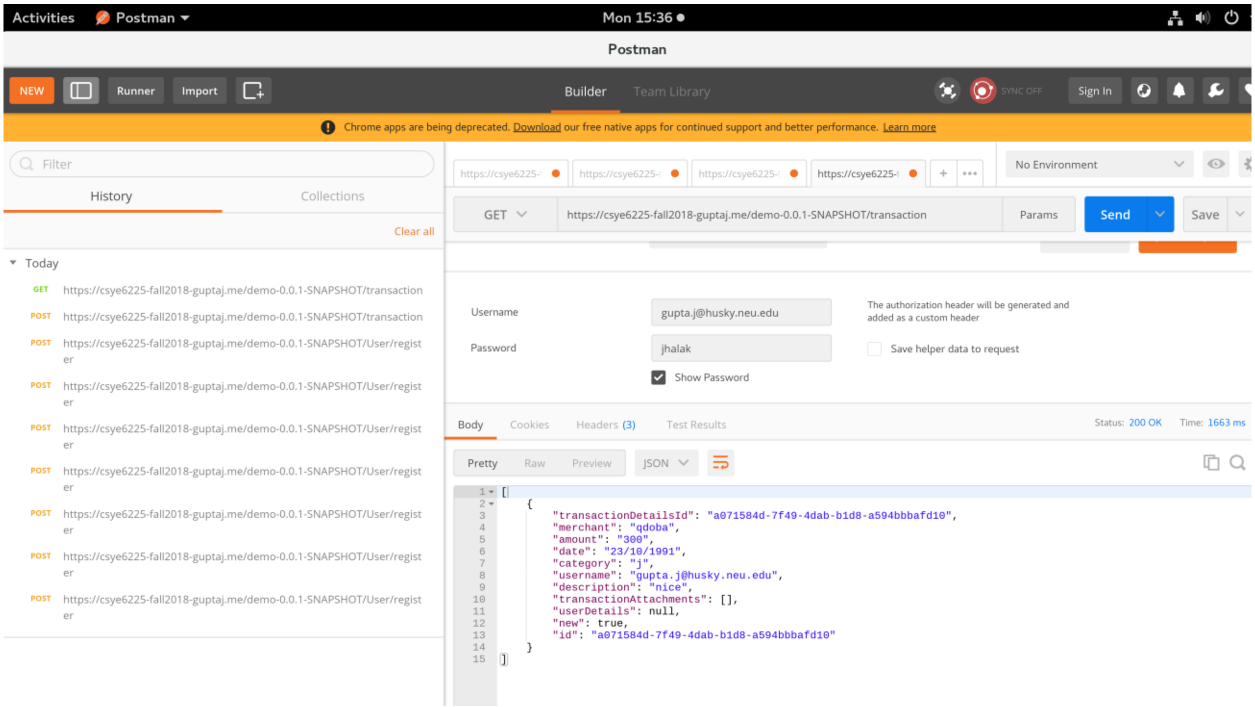
POST https://csye6225-fall2018-guptaj.me/demo-0.0.1-SNAPSHOT/User/register

```
{
"name":"gupta.j@husky.neu.edu;Delete from transaction_details;",
"password":"jhalak"
}
```

Status: 403 Forbidden Time: 179 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 -->
```

This shows that transactions are not deleted:



Chrome apps are being deprecated. Download our free native apps for continued support and better performance. Learn more

Today

GET https://csye6225-fall2018-guptaj.me/demo-0.0.1-SNAPSHOT/transaction
POST https://csye6225-fall2018-guptaj.me/demo-0.0.1-SNAPSHOT/transaction
POST https://csye6225-fall2018-guptaj.me/demo-0.0.1-SNAPSHOT/User/register
POST https://csye6225-fall2018-guptaj.me/demo-0.0.1-SNAPSHOT/User/register
POST https://csye6225-fall2018-guptaj.me/demo-0.0.1-SNAPSHOT/User/register
POST https://csye6225-fall2018-guptaj.me/demo-0.0.1-SNAPSHOT/User/register
POST https://csye6225-fall2018-guptaj.me/demo-0.0.1-SNAPSHOT/User/register
POST https://csye6225-fall2018-guptaj.me/demo-0.0.1-SNAPSHOT/User/register
POST https://csye6225-fall2018-guptaj.me/demo-0.0.1-SNAPSHOT/User/register

GET https://csye6225-fall2018-guptaj.me/demo-0.0.1-SNAPSHOT/transaction

Username: gupta.j@husky.neu.edu
Password: jhalak

The authorization header will be generated and added as a custom header

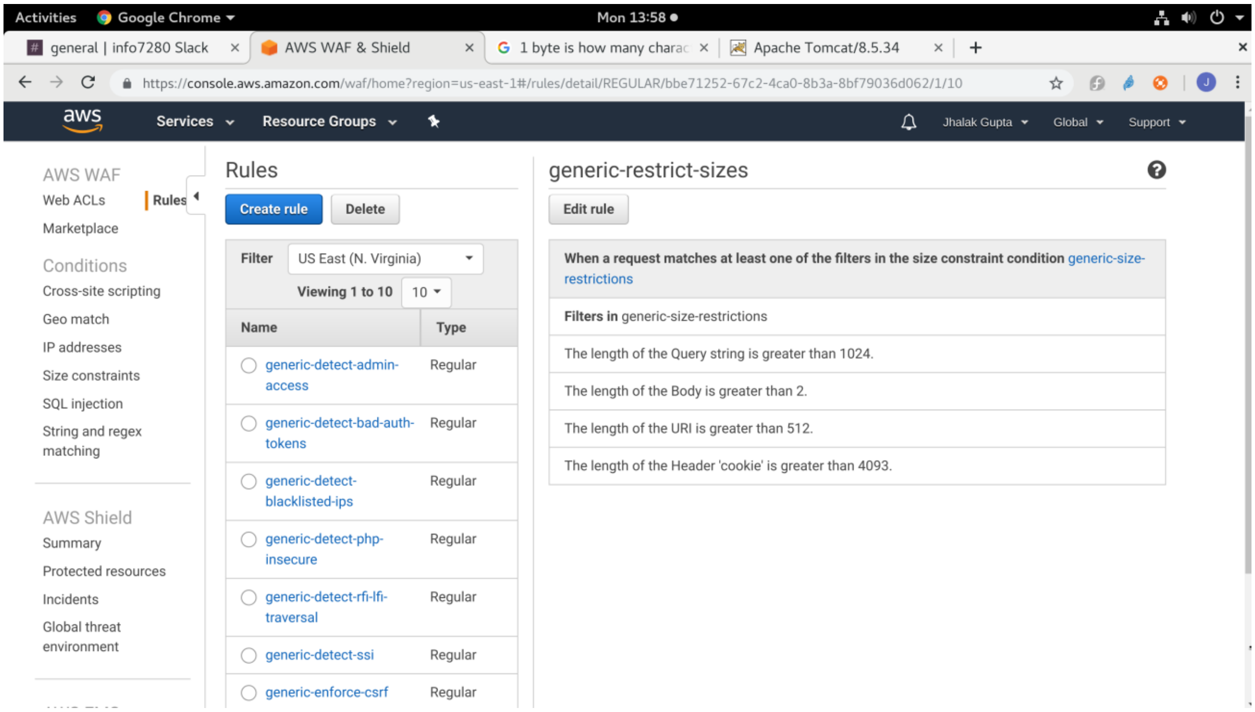
□ Save helper data to request
☑ Show Password

Status: 200 OK Time: 1663 ms

```
[
    {
        "transactionDetailsId": "a071584d-7f49-4dab-b1d8-a594bbbafd10",
        "merchant": "qdoba",
        "amount": "300",
        "date": "23/10/1991",
        "category": "j",
        "username": "gupta.j@husky.neu.edu",
        "description": "nice",
        "transactionAttachments": [],
        "userDetails": null,
        "new": true,
        "id": "a071584d-7f49-4dab-b1d8-a594bbbafd10"
    }
]
```

We have chosen this attack vector because it is one of the most common attack vectors listed by OWASP, which comes under category SQL Injection Attack where the input is used as it is and an SQL statement will **unknowingly** run on your database in the application. This can lead to heavy data losses and data security breach.

- **Unvalidated Input/ Content Length Exceeded:**
  The request body content exceeded the maximum allowable length defined in the URL Profile for the URL space. Max Content Length specified on: SECURITY POLICIES > URL Protection, OR WEBSITES > Website Profiles > URL Profiles.
  Screenshots:
  Below snapshot shows the rule defined with length of body greater than 2:


https://console.aws.amazon.com/waf/home?region=us-east-1#/rules/detail/REGULAR/bbe71252-67c2-4ca0-8b3a-8bf79036d062/1/10

Rules

Filter: US East (N. Virginia) Viewing 1 to 10

Name	Type
generic-detect-admin-access	Regular
generic-detect-bad-auth-tokens	Regular
generic-detect-blacklisted-ips	Regular
generic-detect-php-insecure	Regular
generic-detect-rfi-lfi-traversal	Regular
generic-detect-ssi	Regular
generic-enforce-csrf	Regular

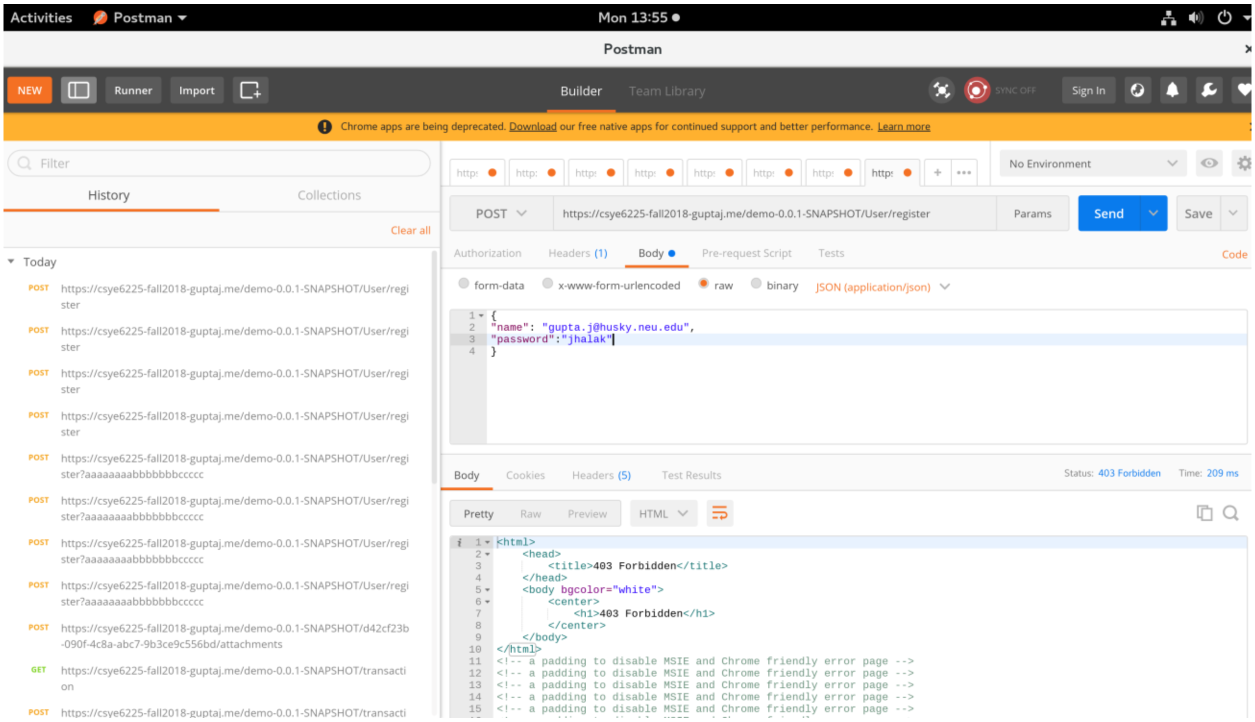
generic-restrict-sizes

When a request matches at least one of the filters in the size constraint condition generic-size-restrictions

Filters in generic-size-restrictions

- The length of the Query string is greater than 1024.
- The length of the Body is greater than 2.
- The length of the URI is greater than 512.
- The length of the Header 'cookie' is greater than 4093.

This snapshot shows that now it is not allowing body content to be greater than specified:


POST https://csye6225-fall2018-guptaj.me/demo-0.0.1-SNAPSHOT/User/register

Body: raw, JSON (application/json)

```
{
"name": "gupta.j@husky.neu.edu",
"password":"jhalak"
}
```

Status: 403 Forbidden Time: 209 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 -->
```

History – Today

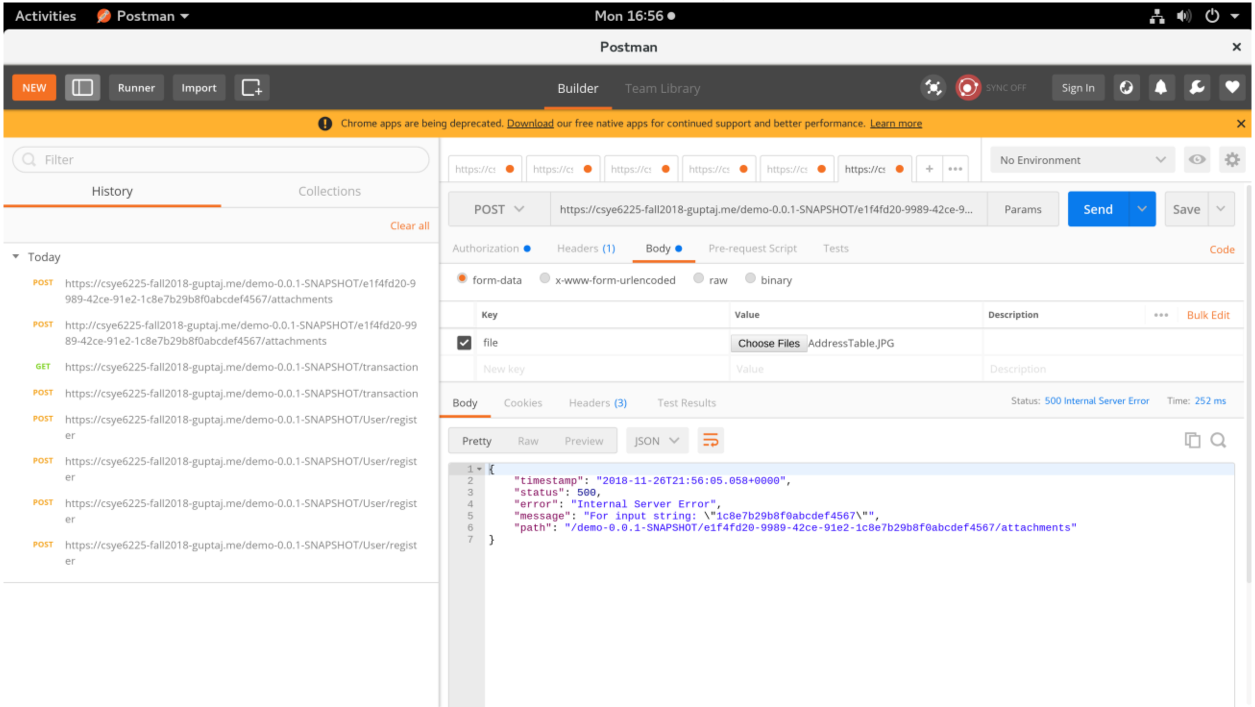
```
POST https://csye6225-fall2018-guptaj.me/demo-0.0.1-SNAPSHOT/User/register
POST https://csye6225-fall2018-guptaj.me/demo-0.0.1-SNAPSHOT/User/register
POST https://csye6225-fall2018-guptaj.me/demo-0.0.1-SNAPSHOT/User/register
POST https://csye6225-fall2018-guptaj.me/demo-0.0.1-SNAPSHOT/User/register
POST https://csye6225-fall2018-guptaj.me/demo-0.0.1-SNAPSHOT/User/register?aaaaaaaabbbbbbbbcccccc
POST https://csye6225-fall2018-guptaj.me/demo-0.0.1-SNAPSHOT/User/register?aaaaaaaabbbbbbbbcccccc
POST https://csye6225-fall2018-guptaj.me/demo-0.0.1-SNAPSHOT/User/register?aaaaaaaabbbbbbbbcccccc
POST https://csye6225-fall2018-guptaj.me/demo-0.0.1-SNAPSHOT/User/register?aaaaaaaabbbbbbbbcccccc
POST https://csye6225-fall2018-guptaj.me/demo-0.0.1-SNAPSHOT/d42cf23b-090f-4c8a-abc7-9b3ce9c556bd/attachments
GET  https://csye6225-fall2018-guptaj.me/demo-0.0.1-SNAPSHOT/transaction
POST https://csye6225-fall2018-guptaj.me/demo-0.0.1-SNAPSHOT/transacti
```

We have chosen this attack vector because it is one of the most common attack vectors listed by OWASP, which comes under category unvalidated input where the input is not sanitized and used as it is in the application. We have implemented this rule so that we can prevent attackers to add some malicious content and append some scripts in the request body content and breach the security of web application.

- ❖ **Unvalidated Input/ URI Length Exceeded:**

Web applications use input from HTTP requests (and occasionally files) to determine how to respond. Attackers can tamper with any part of an HTTP request, including the url, querystring, headers, cookies, form fields, and hidden fields, to try to bypass the site's security mechanisms. That is why we are restricting the length of URI to avoid such kind of attacks.

Screenshot without WAF: It shows that we are trying to insert some added characters in transaction ID while adding an attachment and we are getting error.



Today

POST https://csye6225-fall2018-guptaj.me/demo-0.0.1-SNAPSHOT/e1f4fd20-9989-42ce-91e2-1c8e7b29b8f0abcdef4567/attachments

POST http://csye6225-fall2018-guptaj.me/demo-0.0.1-SNAPSHOT/e1f4fd20-9989-42ce-91e2-1c8e7b29b8f0abcdef4567/attachments

GET https://csye6225-fall2018-guptaj.me/demo-0.0.1-SNAPSHOT/transaction

POST https://csye6225-fall2018-guptaj.me/demo-0.0.1-SNAPSHOT/transaction

POST https://csye6225-fall2018-guptaj.me/demo-0.0.1-SNAPSHOT/User/register

POST https://csye6225-fall2018-guptaj.me/demo-0.0.1-SNAPSHOT/User/register

POST https://csye6225-fall2018-guptaj.me/demo-0.0.1-SNAPSHOT/User/register

POST https://csye6225-fall2018-guptaj.me/demo-0.0.1-SNAPSHOT/User/register

POST https://csye6225-fall2018-guptaj.me/demo-0.0.1-SNAPSHOT/e1f4fd20-9989-42ce-9...

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

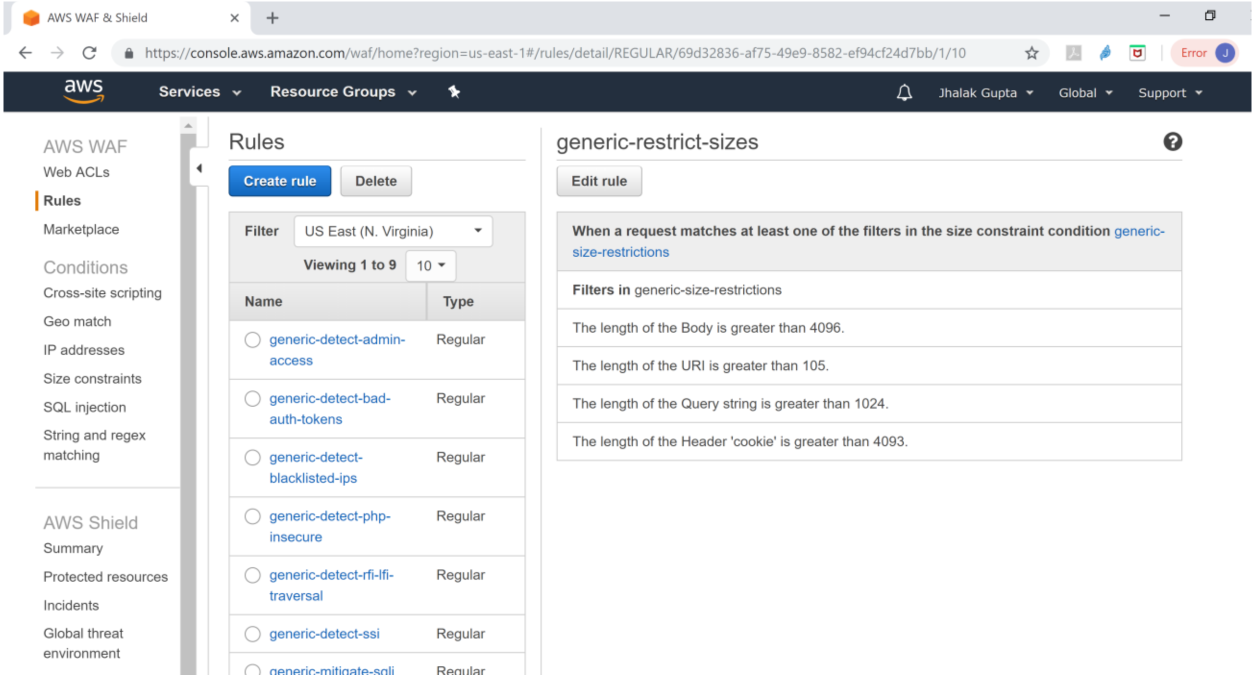
	Key	Value	Description
☑	file	Choose Files AddressTable.JPG	
	New key	Value	Description

Status: 500 Internal Server Error Time: 252 ms

```
{
    "timestamp": "2018-11-26T21:56:05.058+0000",
    "status": 500,
    "error": "Internal Server Error",
    "message": "For input string: \"1c8e7b29b8f0abcdef4567\"",
    "path": "/demo-0.0.1-SNAPSHOT/e1f4fd20-9989-42ce-91e2-1c8e7b29b8f0abcdef4567/attachments"
}
```

Screenshot with WAF:

Below image shows the rule that if length of URI as greater than 105 then it should prevent such requests:



Rules

Filter: US East (N. Virginia)

Viewing 1 to 9 | 10

Name	Type
○ generic-detect-admin-access	Regular
○ generic-detect-bad-auth-tokens	Regular
○ generic-detect-blacklisted-ips	Regular
○ generic-detect-php-insecure	Regular
○ generic-detect-rfi-lfi-traversal	Regular
○ generic-detect-ssi	Regular
○ generic-mitigate-sqli	Regular

generic-restrict-sizes

When a request matches at least one of the filters in the size constraint condition generic-size-restrictions

Filters in generic-size-restrictions

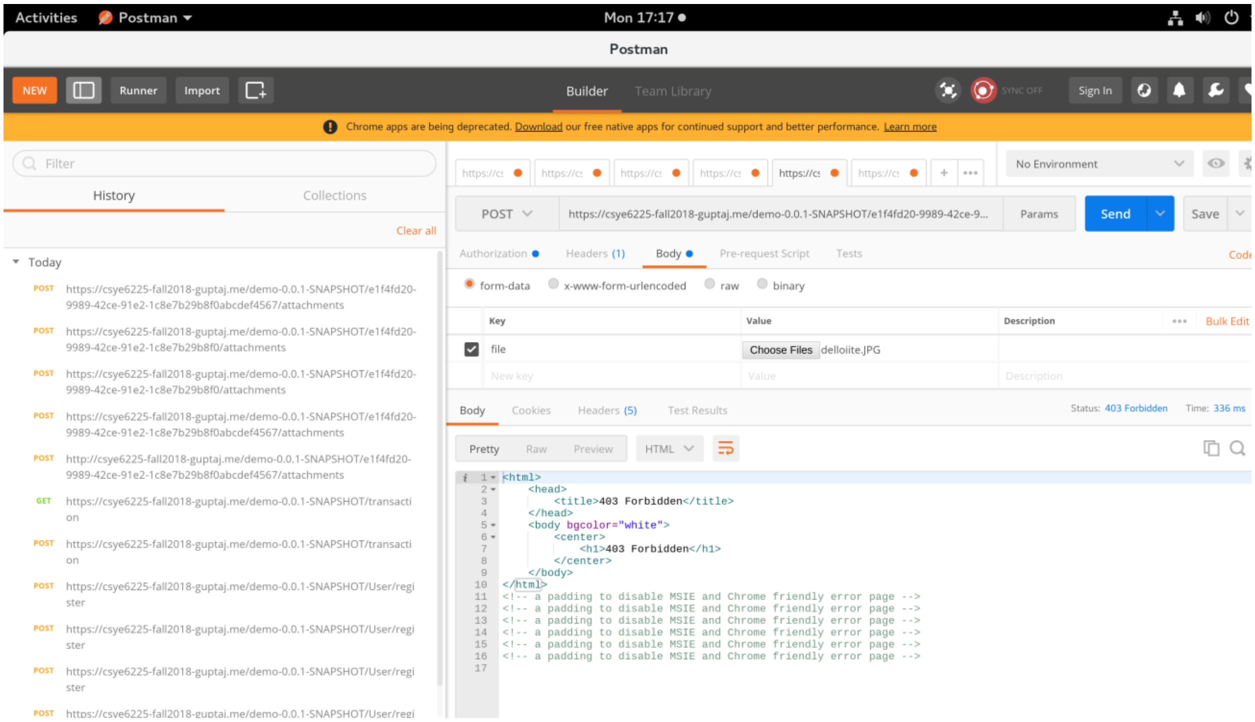
The length of the Body is greater than 4096.

The length of the URI is greater than 105.

The length of the Query string is greater than 1024.

The length of the Header 'cookie' is greater than 4093.

Below image shows that bad request is forbidden:



Chrome apps are being deprecated. Download our free native apps for continued support and better performance. Learn more

Today

- POST https://csye6225-fall2018-guptaj.me/demo-0.0.1-SNAPSHOT/e1f4fd20-9989-42ce-91e2-1c8e7b29b8f0abcdef4567/attachments
- POST https://csye6225-fall2018-guptaj.me/demo-0.0.1-SNAPSHOT/e1f4fd20-9989-42ce-91e2-1c8e7b29b8f0/attachments
- POST https://csye6225-fall2018-guptaj.me/demo-0.0.1-SNAPSHOT/e1f4fd20-9989-42ce-91e2-1c8e7b29b8f0/attachments
- POST https://csye6225-fall2018-guptaj.me/demo-0.0.1-SNAPSHOT/e1f4fd20-9989-42ce-91e2-1c8e7b29b8f0abcdef4567/attachments
- POST http://csye6225-fall2018-guptaj.me/demo-0.0.1-SNAPSHOT/e1f4fd20-9989-42ce-91e2-1c8e7b29b8f0abcdef4567/attachments
- GET https://csye6225-fall2018-guptaj.me/demo-0.0.1-SNAPSHOT/transaction
- POST https://csye6225-fall2018-guptaj.me/demo-0.0.1-SNAPSHOT/transaction
- POST https://csye6225-fall2018-guptaj.me/demo-0.0.1-SNAPSHOT/User/register
- POST https://csye6225-fall2018-guptaj.me/demo-0.0.1-SNAPSHOT/User/register
- POST https://csye6225-fall2018-guptaj.me/demo-0.0.1-SNAPSHOT/User/register
- POST https://csye6225-fall2018-guptaj.me/demo-0.0.1-SNAPSHOT/User/regi

POST https://csye6225-fall2018-guptaj.me/demo-0.0.1-SNAPSHOT/e1f4fd20-9989-42ce-9...

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

	Key	Value	Description
☑	file	Choose Files delloiite.JPG	
	New key	Value	Description

Status: 403 Forbidden Time: 336 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 -->
```

We have chosen this attack vector because it is one of the most common attack vectors listed by OWASP, which comes under category unvalidated input where the input is not sanitized and used as it is in the application. We have implemented this rule so that we can prevent attackers to add some malicious characters in the URL and breach the security of web application.