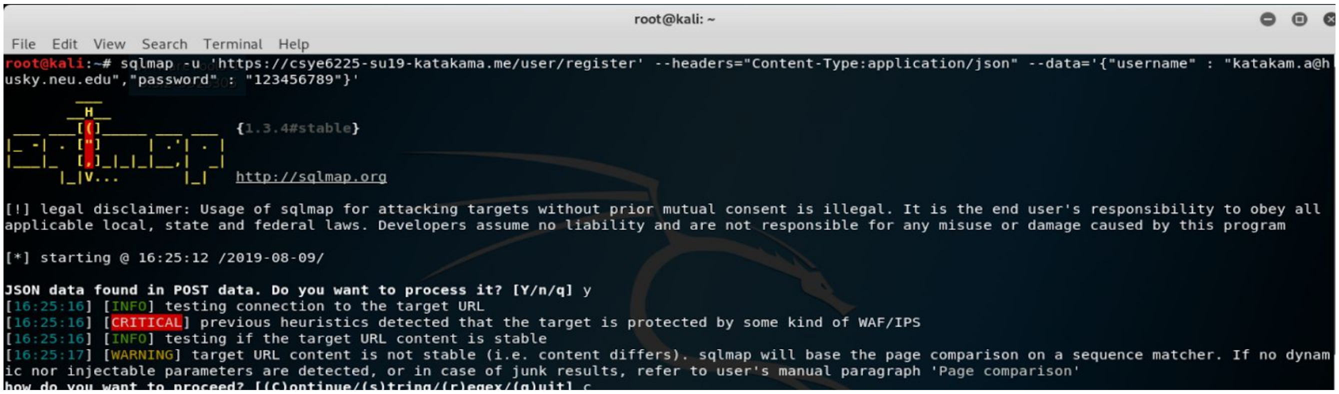
Penetration Testing

1. SQL Injection

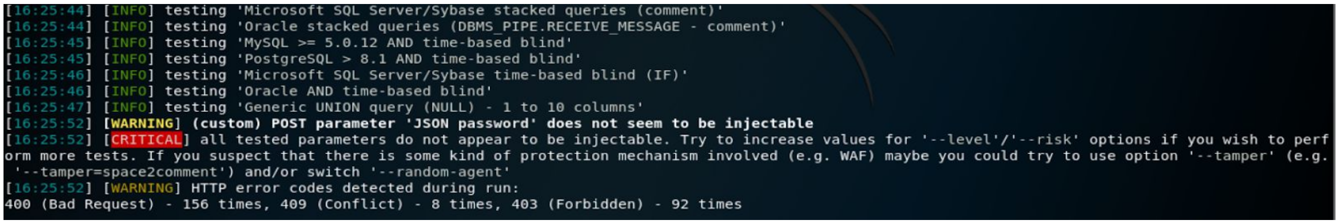
Reason for choosing this vulnerability: This kind of attack occurs when a malicious user tries to execute SQL queries to break into the web application. It is one of the most common types of security attacks. In order to prevent such attacks, the user input in the URL header must be sanitized.

Result: Used sqlmap to test the vulnerabilities with WAF the application throws HTTP status code-403 as sqlmap tries to hit many times the status code 403 is thrown 92 times. Whereas without WAF 403 error code is not thrown that means the injection was possible

With WAF

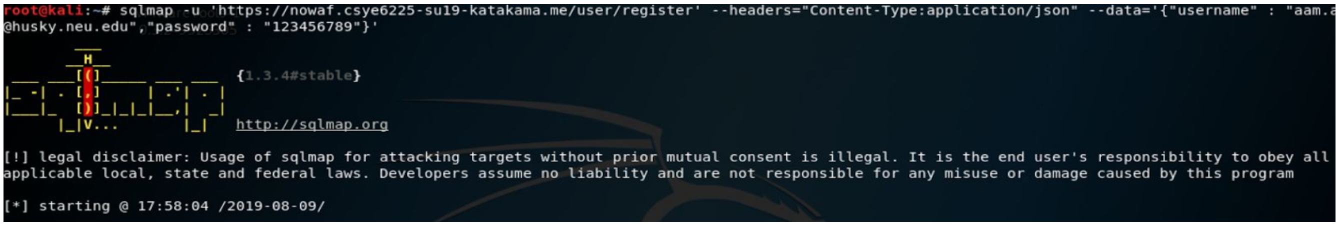


```
root@kali:~# sqlmap -u 'https://csye6225-su19-katakama.me/user/register' --headers="Content-Type:application/json" --data='{"username" : "katakam.a@h
usky.neu.edu","password" : "123456789"}'
        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.3.4#stable}
|_ -| . ["]     | .'| . |
|___|_  [,]_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all
applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 16:25:12 /2019-08-09/

JSON data found in POST data. Do you want to process it? [Y/n/q] y
[16:25:16] [INFO] testing connection to the target URL
[16:25:16] [CRITICAL] previous heuristics detected that the target is protected by some kind of WAF/IPS
[16:25:16] [INFO] testing if the target URL content is stable
[16:25:17] [WARNING] target URL content is not stable (i.e. content differs). sqlmap will base the page comparison on a sequence matcher. If no dynam
ic nor injectable parameters are detected, or in case of junk results, refer to user's manual paragraph 'Page comparison'
how do you want to proceed? [(C)ontinue/(s)tring/(r)egex/(q)uit] c
```

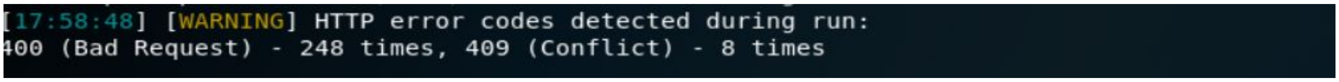


```
[16:25:44] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[16:25:44] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[16:25:45] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind'
[16:25:45] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[16:25:46] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[16:25:46] [INFO] testing 'Oracle AND time-based blind'
[16:25:47] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[16:25:52] [WARNING] (custom) POST parameter 'JSON password' does not seem to be injectable
[16:25:52] [CRITICAL] all tested parameters do not appear to be injectable. Try to increase values for '--level'/'--risk' options if you wish to perf
orm more tests. If you suspect that there is some kind of protection mechanism involved (e.g. WAF) maybe you could try to use option '--tamper' (e.g.
 '--tamper=space2comment') and/or switch '--random-agent'
[16:25:52] [WARNING] HTTP error codes detected during run:
400 (Bad Request) - 156 times, 409 (Conflict) - 8 times, 403 (Forbidden) - 92 times
```

Without WAF

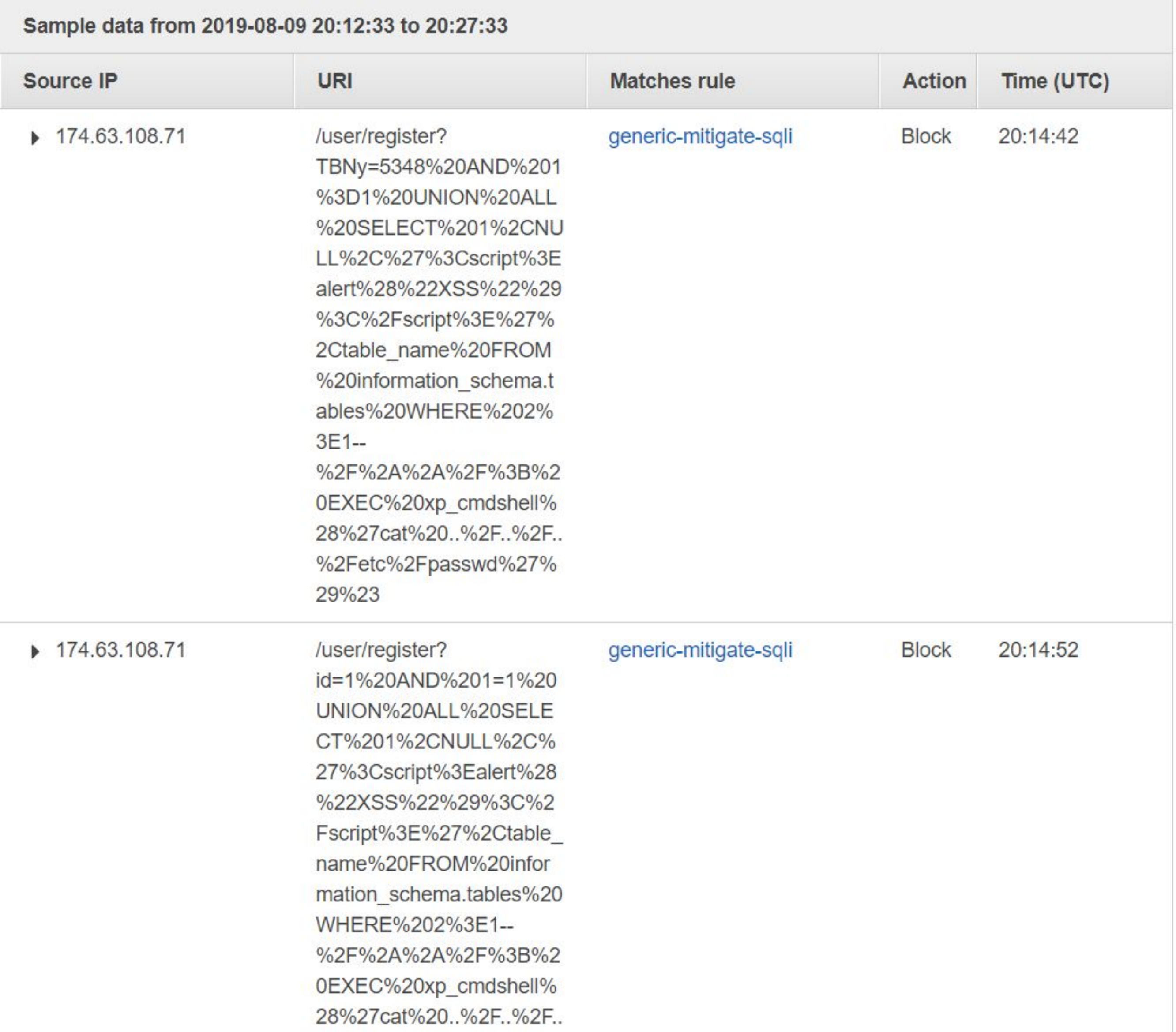


```
root@kali:~# sqlmap -u 'https://nowaf.csye6225-su19-katakama.me/user/register' --headers="Content-Type:application/json" --data='{"username" : "aam.a
@husky.neu.edu","password" : "123456789"}'
        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.3.4#stable}
|_ -| . [,]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all
applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 17:58:04 /2019-08-09/
```



```
[17:58:48] [WARNING] HTTP error codes detected during run:
400 (Bad Request) - 248 times, 409 (Conflict) - 8 times
```

Blocked Requests



Sample data from 2019-08-09 20:12:33 to 20:27:33

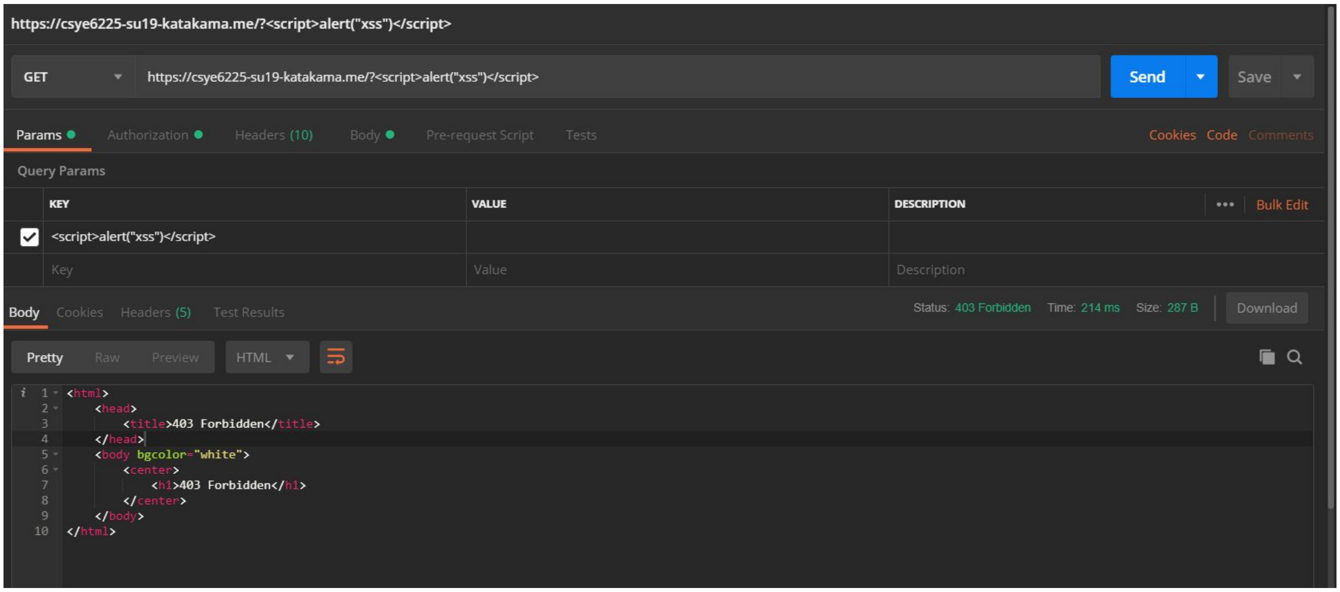
Source IP	URI	Matches rule	Action	Time (UTC)
▸ 174.63.108.71	/user/register?TBNy=5348%20AND%201%3D1%20UNION%20ALL%20SELECT%201%2CNULL%2C%27%3Cscript%3Ealert%28%22XSS%22%29%3C%2Fscript%3E%27%2Ctable_name%20FROM%20information_schema.tables%20WHERE%202%3E1--%2F%2A%2A%2F%3B%20EXEC%20xp_cmdshell%28%27cat%20..%2F..%2F..%2Fetc%2Fpasswd%27%29%23	generic-mitigate-sqli	Block	20:14:42
▸ 174.63.108.71	/user/register?id=1%20AND%201=1%20UNION%20ALL%20SELECT%201%2CNULL%2C%27%3Cscript%3Ealert%28%22XSS%22%29%3C%2Fscript%3E%27%2Ctable_name%20FROM%20information_schema.tables%20WHERE%202%3E1--%2F%2A%2A%2F%3B%20EXEC%20xp_cmdshell%28%27cat%20..%2F..%2F..	generic-mitigate-sqli	Block	20:14:52

2. XSS(Cross site scripting)

Reason for choosing this vulnerability: Cross-site scripting (XSS) is a type of injection security attack in which an attacker injects data, such as a malicious script into content from otherwise trusted websites. Cross-site scripting attacks happen when an untrusted source is allowed to inject its own code into a web application, and that malicious code is included with dynamic content delivered to a victim's browser

.

With WAF


https://csye6225-su19-katakama.me/?<script>alert("xss")</script>

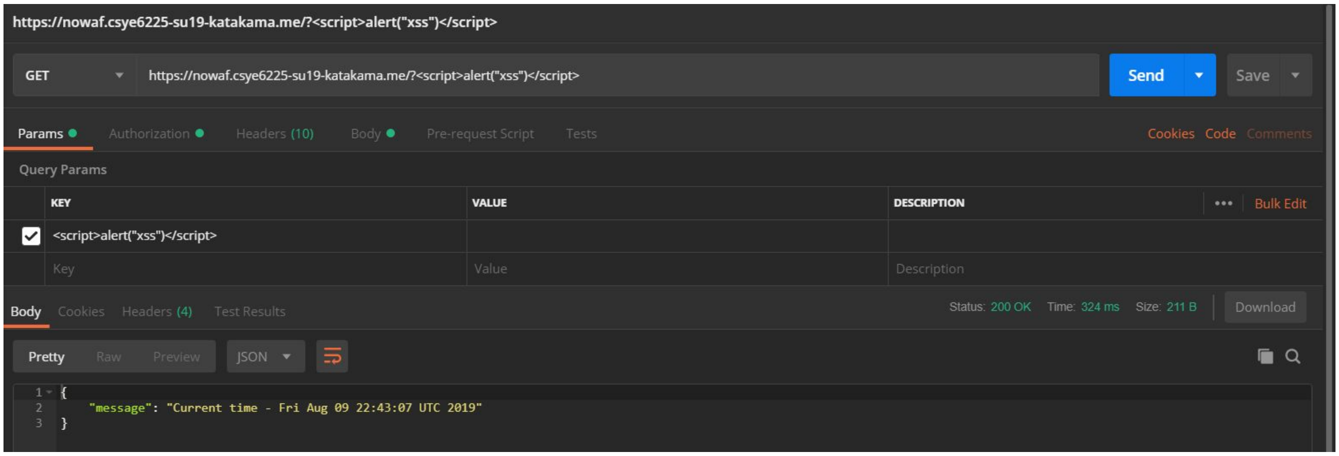
GET https://csye6225-su19-katakama.me/?<script>alert("xss")</script>

	KEY	VALUE	DESCRIPTION
☑	<script>alert("xss")</script>		
	Key	Value	Description

Status: 403 Forbidden Time: 214 ms Size: 287 B

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

Without WAF


https://nowaf.csye6225-su19-katakama.me/?<script>alert("xss")</script>

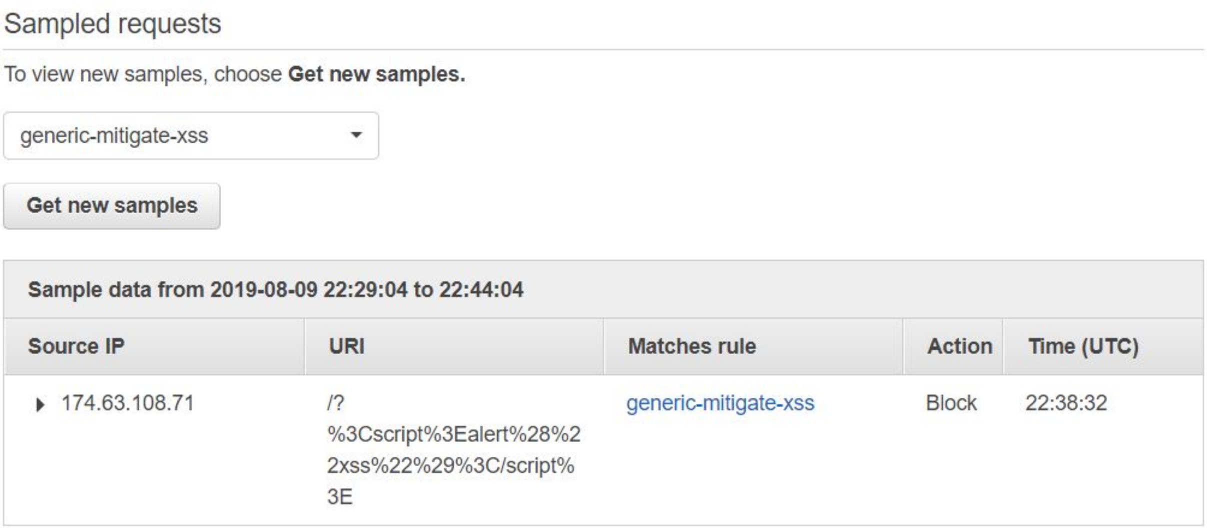
GET https://nowaf.csye6225-su19-katakama.me/?<script>alert("xss")</script>

	KEY	VALUE	DESCRIPTION
☑	<script>alert("xss")</script>		
	Key	Value	Description

Status: 200 OK Time: 324 ms Size: 211 B

```
{
    "message": "Current time - Fri Aug 09 22:43:07 UTC 2019"
}
```

Blocked Requests



Sampled requests

To view new samples, choose **Get new samples.**

Sample data from 2019-08-09 22:29:04 to 22:44:04

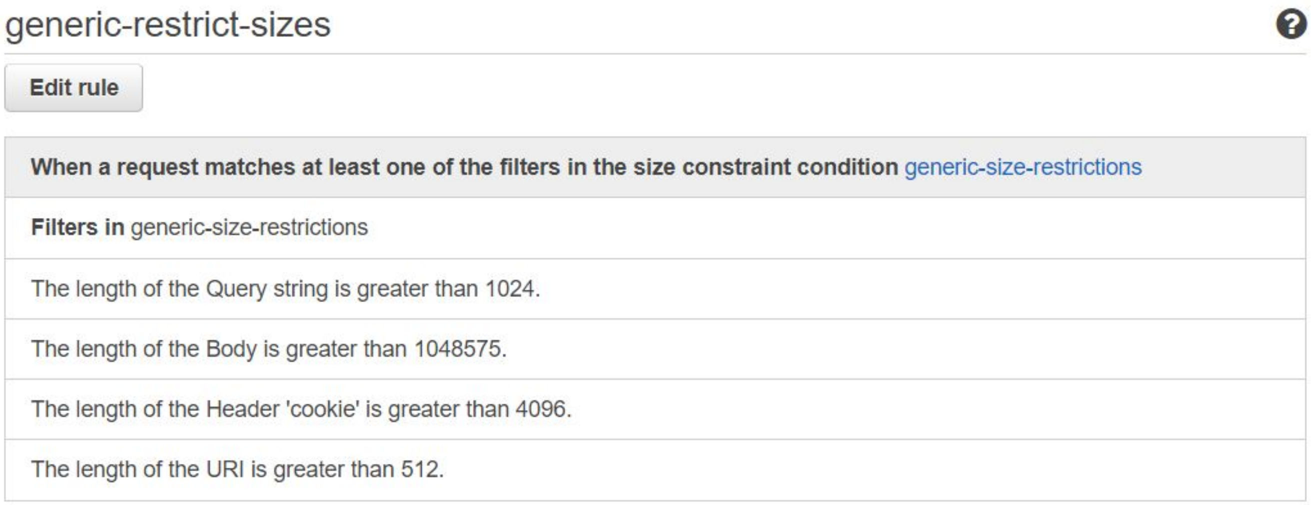
Source IP	URI	Matches rule	Action	Time (UTC)
174.63.108.71	/?%3Cscript%3Ealert%28%22xss%22%29%3C/script%3E	generic-mitigate-xss	Block	22:38:32

3.Vulnerability Type: Restricted attachment size

Reason for choosing this vulnerability: We restrict the attachment size as there might be some size constraints that are given to each user.

Result: When an attachment larger than the size specified is sent to the server, we get a 403 Forbidden Status Code.

With WAF*(File Size: 3.12GB)*



generic-restrict-sizes

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

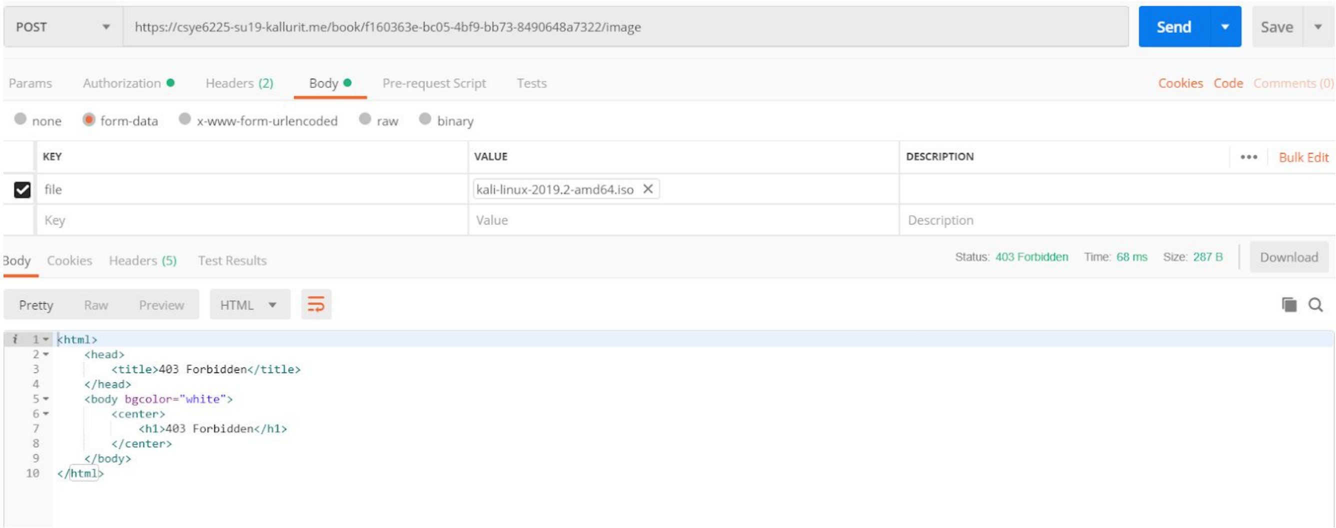
Filters in generic-size-restrictions

The length of the Query string is greater than 1024.

The length of the Body is greater than 1048575.

The length of the Header 'cookie' is greater than 4096.

The length of the URI is greater than 512.



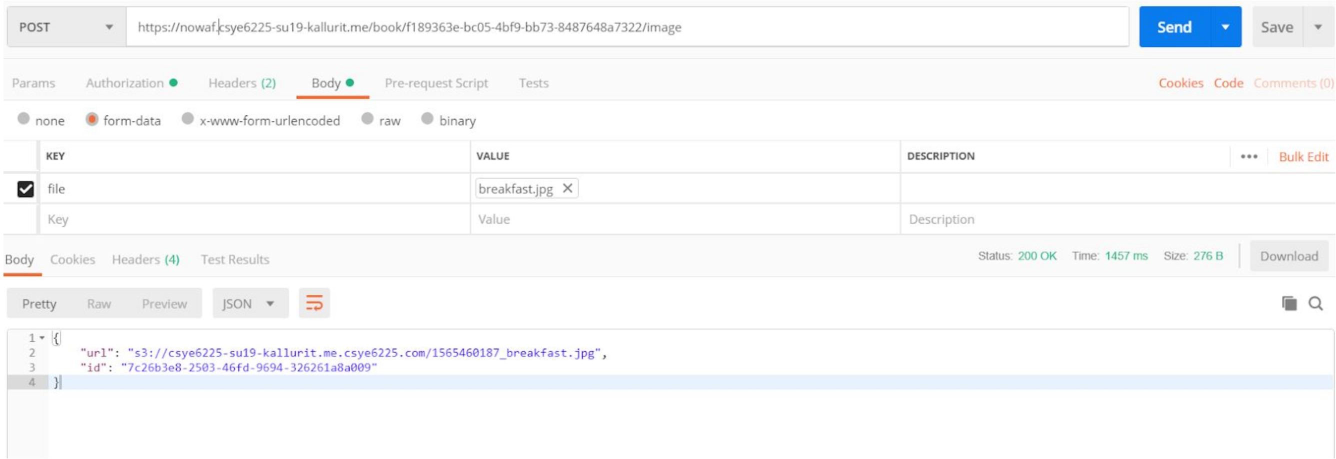
POST https://csye6225-su19-kallurit.me/book/f160363e-bc05-4bf9-bb73-8490648a7322/image

	KEY	VALUE	DESCRIPTION
☑	file	kali-linux-2019.2-amd64.iso	
	Key	Value	Description

Status: 403 Forbidden Time: 68 ms Size: 287 B

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

Without WAF



POST https://nowaf.csye6225-su19-kallurit.me/book/f189363e-bc05-4bf9-bb73-8487648a7322/image

	KEY	VALUE	DESCRIPTION
☑	file	breakfast.jpg	
	Key	Value	Description

Status: 200 OK Time: 1457 ms Size: 276 B

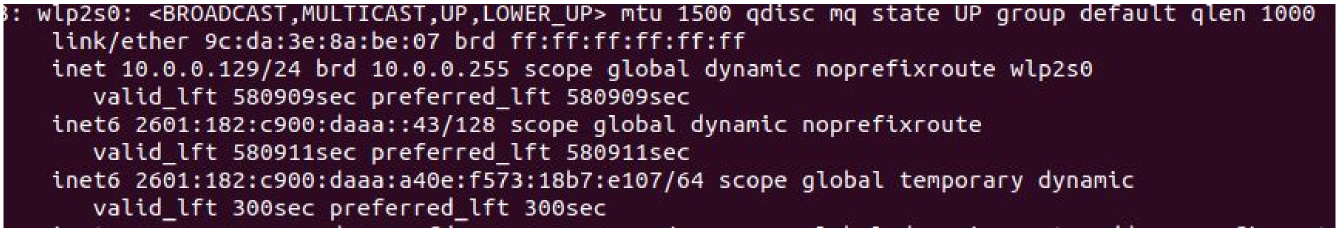
```
{
    "url": "s3://csye6225-su19-kallurit.me.csye6225.com/1565460187_breakfast.jpg",
    "id": "7c26b3e8-2503-46fd-9694-326261a8a009"
}
```

4.IP Blacklisting

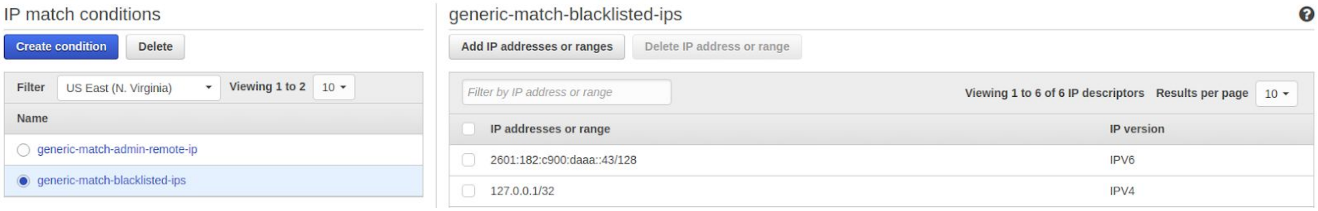
Reason for choosing this vulnerability: This restriction is placed in order to give only legitimate people access to the application and protect the application from hacking attacks.

Result: When a user from a blocked IP tries to access the application, the user is forbidden from accessing it and a Status Code of 403 is returned. If the IP is not blacklisted, the user can access the web application

With WAF



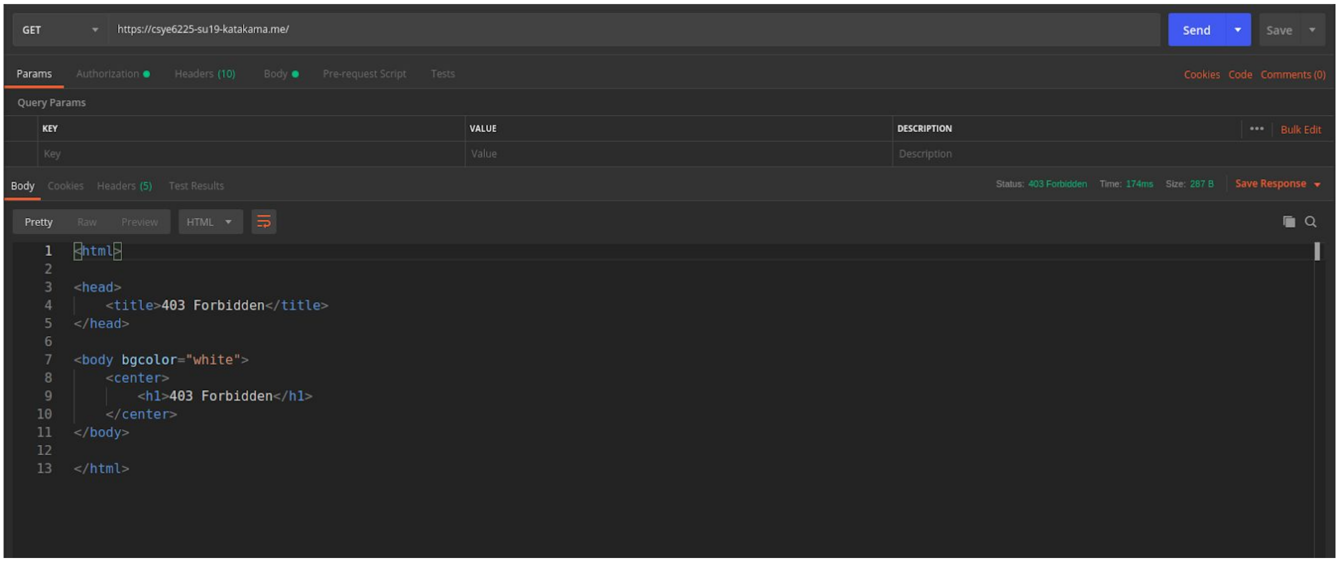
```
3: wlp2s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 9c:da:3e:8a:be:07 brd ff:ff:ff:ff:ff:ff
    inet 10.0.0.129/24 brd 10.0.0.255 scope global dynamic noprefixroute wlp2s0
       valid_lft 580909sec preferred_lft 580909sec
    inet6 2601:182:c900:daaa::43/128 scope global dynamic noprefixroute
       valid_lft 580911sec preferred_lft 580911sec
    inet6 2601:182:c900:daaa:a40e:f573:18b7:e107/64 scope global temporary dynamic
       valid_lft 300sec preferred_lft 300sec
```



IP match conditions
Create condition
Delete
Filter
US East (N. Virginia)
Viewing 1 to 2
10
Name
generic-match-blacklisted-ips
Add IP addresses or ranges
Delete IP address or range
Filter by IP address or range
Viewing 1 to 6 of 6 IP descriptors
Results per page
10

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

	IP addresses or range	IP version
□	2601:182:c900:daaa::43/128	IPV6
□	127.0.0.1/32	IPV4

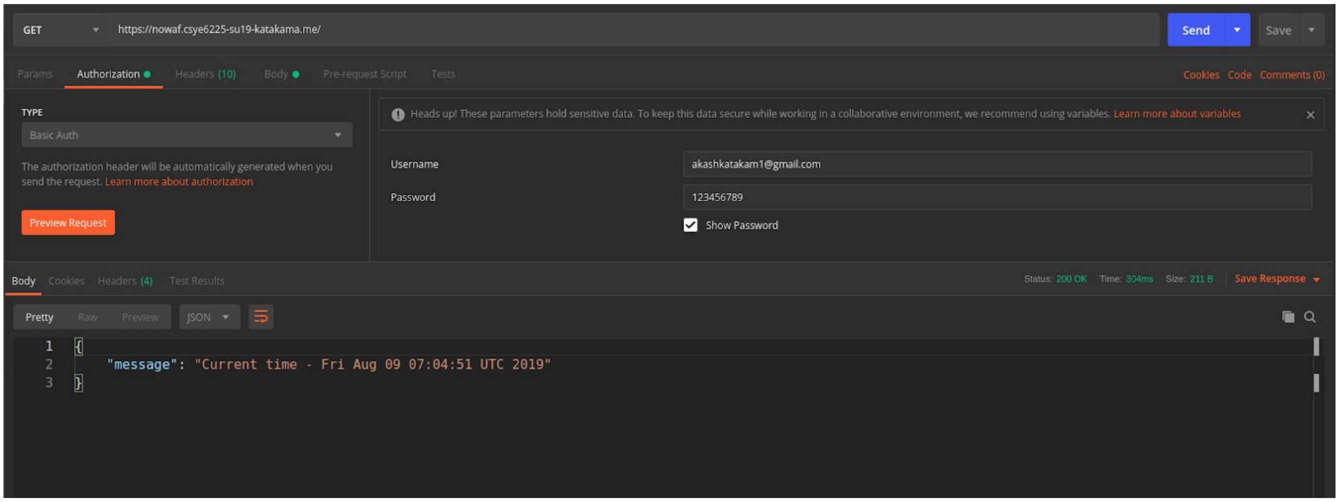


GET https://csye6225-su19-katakama.me/

Status: 403 Forbidden Time: 174ms Size: 287 B

```html
<html>

<head>
    <title>403 Forbidden</title>
</head>

<body bgcolor="white">
    <center>
        <h1>403 Forbidden</h1>
    </center>
</body>

</html>
```

Without WAF



GET https://nowaf.csye6225-su19-katakama.me/

TYPE: Basic Auth

The authorization header will be automatically generated when you send the request. Learn more about authorization

Heads up! These parameters hold sensitive data. To keep this data secure while working in a collaborative environment, we recommend using variables. Learn more about variables

Username: akashkatakam1@gmail.com

Password: 123456789

☑ Show Password

Status: 200 OK Time: 304ms Size: 211 B

```json
{
    "message": "Current time - Fri Aug 09 07:04:51 UTC 2019"
}
```