Report

A1- Injection

Without WAF

Attacked the application using OWASP ZAP tool and found that SQL Injection was possible. Alert details are as follows-

High (Medium)	SQL Injection
Description	SQL injection may be possible.
URL	https://csye6225-fall2018-chandwanid.me//transaction/8a8080cd67512ea401675137df450000/attachments?query=query%27+AND+%271%27%3D%271%27+--+
Method	POST
Parameter	Query
Attack	query' OR '1'='1' --
URL	https://csye6225-fall2018-chandwanid.me/transaction/8a8080cd67512ea401675137df450000?query=query%27+AND+%271%27%3D%271%27+--+
Method	GET
Parameter	Query
Attack	query' AND '1'='1' --
Instances	2
Other information	The page results were successfully manipulated using the boolean conditions [query' AND '1'='1' --] and [query' OR '1'='1' --] The parameter value being modified was stripped from the HTML output for the purposes of the comparison Data was NOT returned for the original parameter. The vulnerability was detected by successfully retrieving more data than originally returned, by manipulating the parameter
Reference	https://www.owasp.org/index.php/Top_10_2010-A1 https://www.owasp.org/index.php/SQL_Injection_Prevention_Cheat_Sheet

With WAF, No sql Injection could be performed

A3 – Cross-site Scripting

As pe the ZAP attack report it was found that the web browser XSS Protection was not enabled. Details are as follows-

Low (Medium)	**Web Browser XSS Protection Not Enabled**
Description	Web Browser XSS Protection is not enabled, or is disabled by the configuration of the 'X-XSS-Protection' HTTP response header on the web server
URL	https://csye6225-fall2018-bhargavan.me/transaction
Method	POST
Parameter	X-XSS-Protection
URL	https://csye6225-fall2018-bhargavan.me/transaction/6483876289463284623 9/attachments
Method	POST
Parameter	X-XSS-Protection
Instances	2
Solution	Ensure that the web browser's XSS filter is enabled, by setting the X-XSS-Protection HTTP response header to '1'.
Other information	The X-XSS-Protection HTTP response header allows the web server to enable or disable the web browser's XSS protection mechanism. The following values would attempt to enable it: X-XSS-Protection: 1; mode=block X-XSS-Protection: 1; report=http://www.example.com/xss The following values would disable it: X-XSS-Protection: 0 The X-XSS-Protection HTTP response header is currently supported on Internet Explorer, Chrome and Safari (WebKit). Note that this alert is only raised if the response body could potentially contain an XSS payload (with a text-based content type, with a non-zero length).
Reference	https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet https://blog.veracode.com/2014/03/guidelines-for-setting-security-headers/
CWE Id	933
WASC Id	14
Source ID	3

The same alert was raised even when the WAF was active

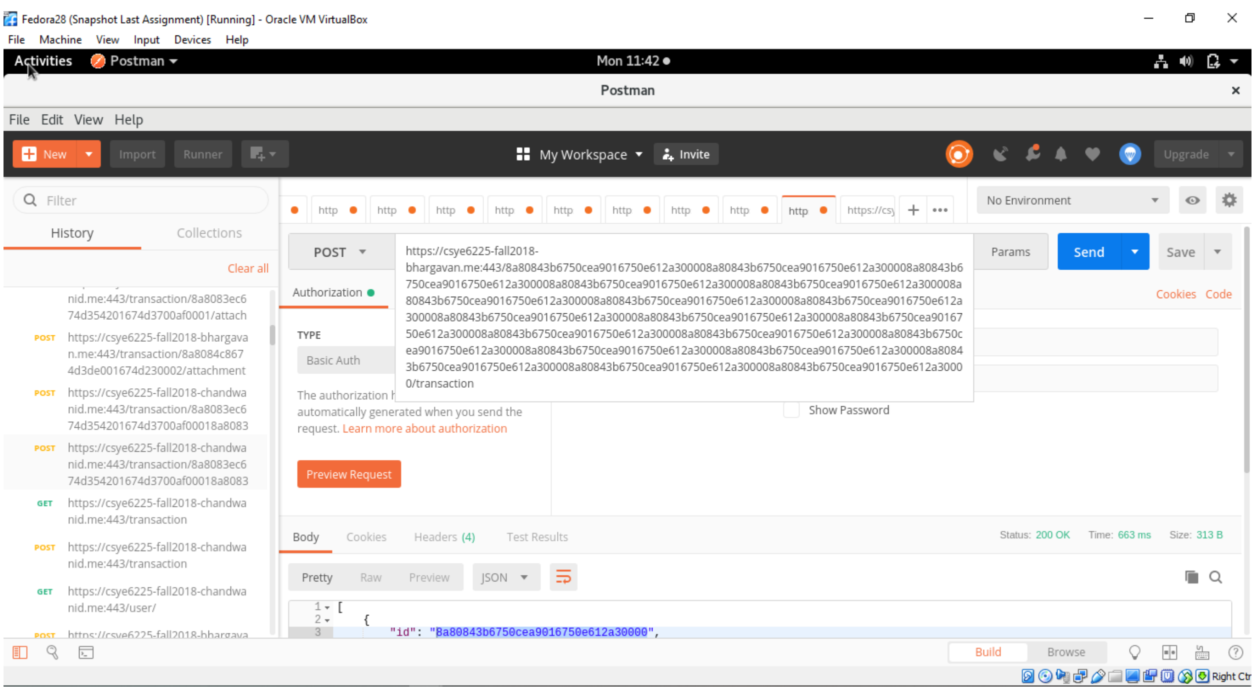
Low (Medium)	**Web Browser XSS Protection Not Enabled**
Description	Web Browser XSS Protection is not enabled, or is disabled by the configuration of the 'X-XSS-Protection' HTTP response header on the web server
URL	https://csye6225-fall2018-chandwanid.me//transaction/8a8080cd67512ea401675137df450000/attachments
Method	POST
Parameter	X-XSS-Protection
URL	https://csye6225-fall2018-chandwanid.me/
Method	GET
Parameter	X-XSS-Protection
URL	https://csye6225-fall2018-chandwanid.me/transaction
Method	POST
Parameter	X-XSS-Protection
URL	https://csye6225-fall2018-chandwanid.me/transaction/8a8080cd67512ea401675137df450000/attachments
Method	POST
Parameter	X-XSS-Protection
Instances	4
Solution	Ensure that the web browser's XSS filter is enabled, by setting the X-XSS-Protection HTTP response header to '1'.
Other information	The X-XSS-Protection HTTP response header allows the web server to enable or disable the web browser's XSS protection mechanism. The following values would attempt to enable it: X-XSS-Protection: 1; mode=block X-XSS-Protection: 1; report=http://www.example.com/xss The following values would disable it: X-XSS-Protection: 0 The X-XSS-Protection HTTP response header is currently supported on Internet Explorer, Chrome and Safari (WebKit).

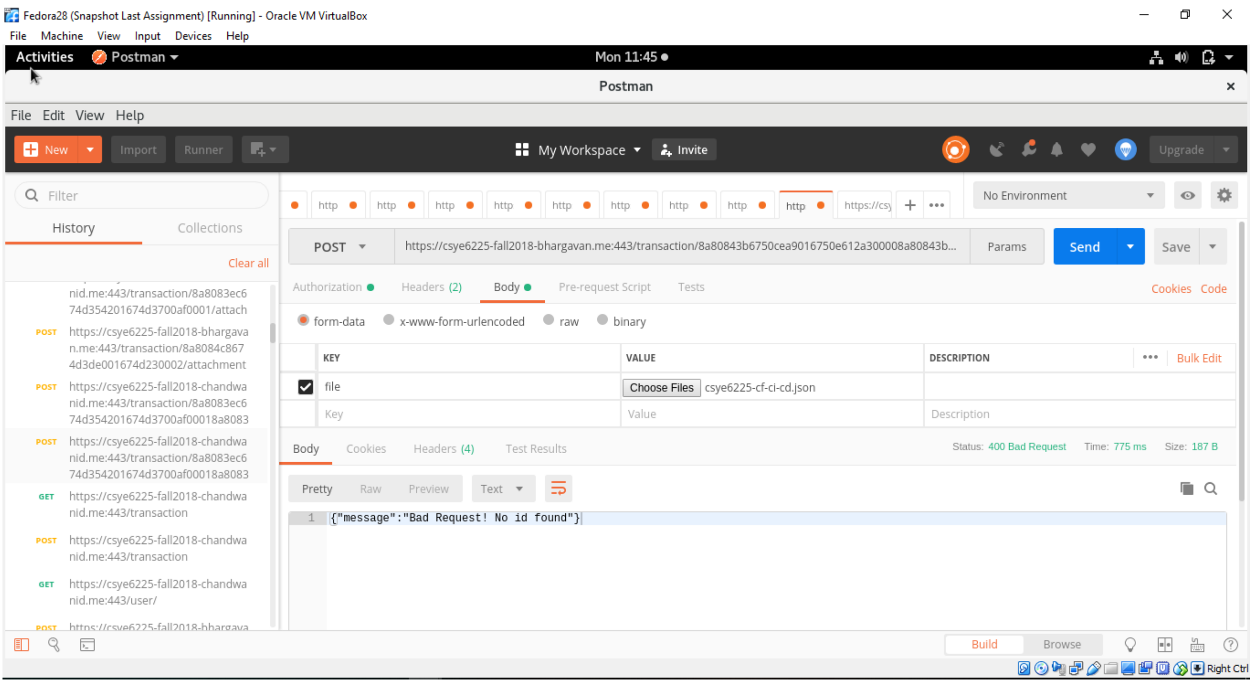
	Note that this alert is only raised if the response body could potentially contain an XSS payload (with a text-based content type, with a non-zero length).
Reference	https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet https://blog.veracode.com/2014/03/guidelines-for-setting-security-headers/
CWE Id	933
WASC Id	14
Source ID	3

A7 – Insufficient Attack Protection

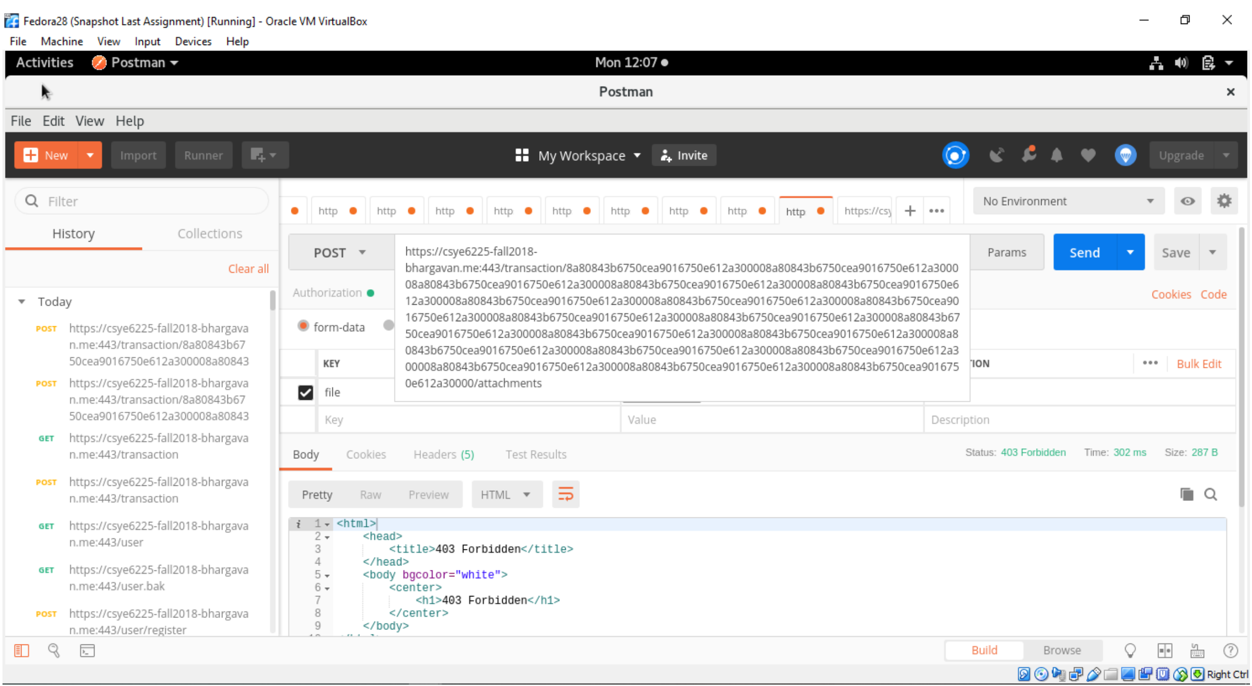
As part of Manual attack crafting, this attack involves requests that a normal user would never send. Although APIs of our application detect invalid input, we wish to see if the attack could be made by changing the parameters in request URL.

Without WAF the request is able to reach the controller and database.

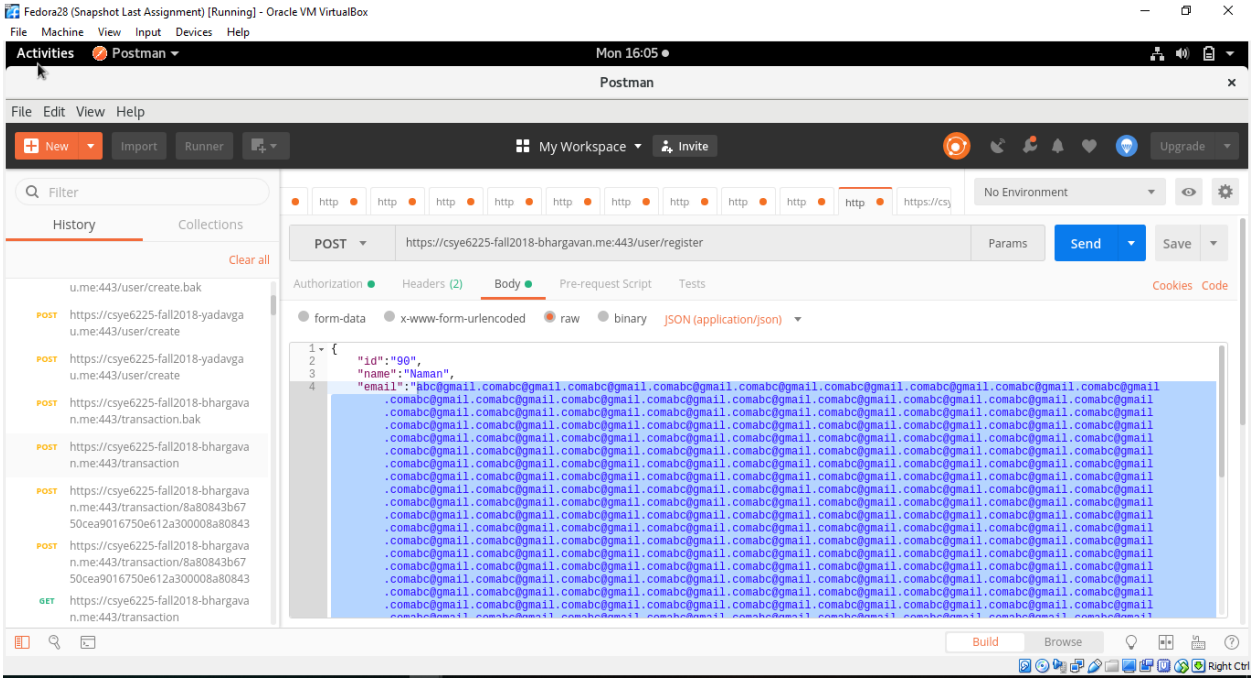


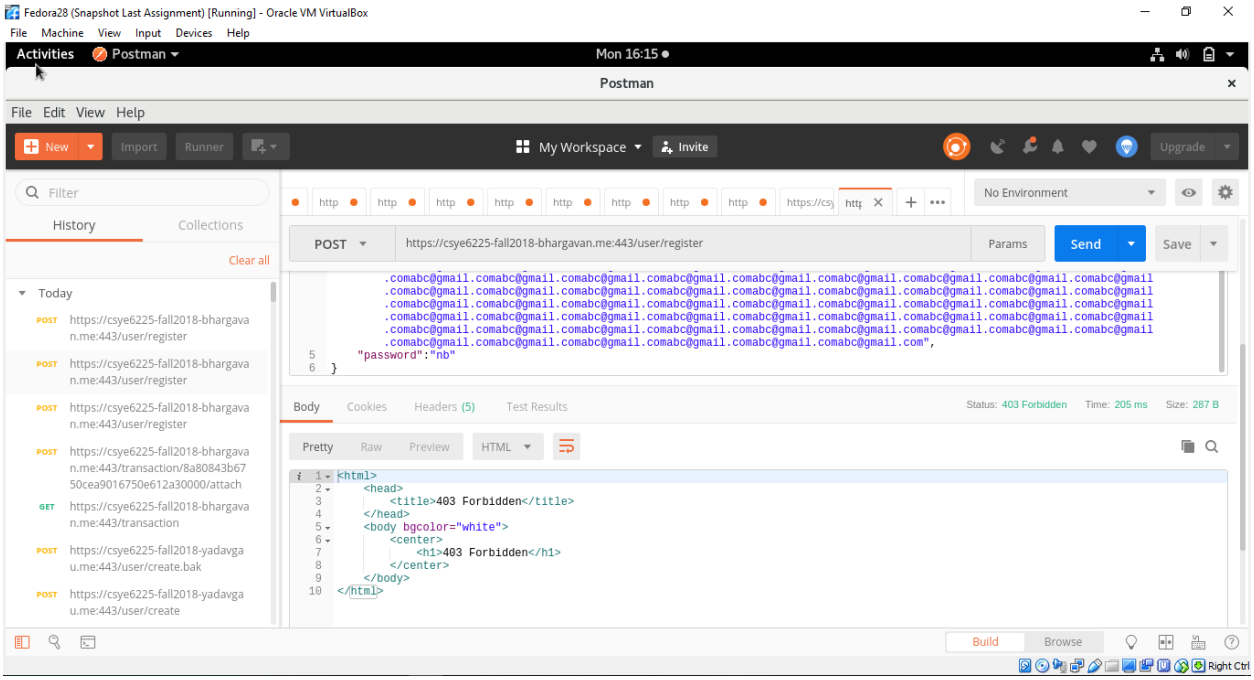


With WAF since the body length is restricted the request is not allowed.

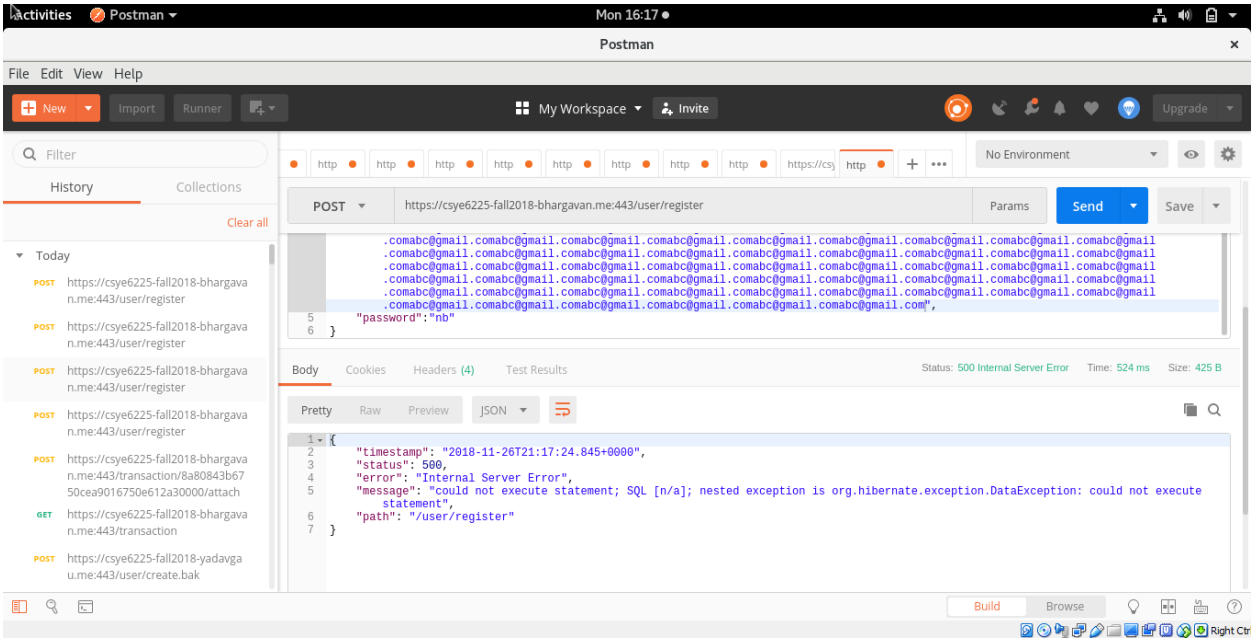


Also when we change the body length beyond restriction limits WAF blocks the request





Without WAF request reaches the controller and browser


Activities
Postman
Mon 16:17
Postman
File Edit View Help
New
Import
Runner
My Workspace
Invite
Upgrade
Filter
History
Collections
Clear all
Today
POST https://csye6225-fall2018-bhargavan.me:443/user/register
POST https://csye6225-fall2018-bhargavan.me:443/user/register
POST https://csye6225-fall2018-bhargavan.me:443/user/register
POST https://csye6225-fall2018-bhargavan.me:443/user/register
POST https://csye6225-fall2018-bhargavan.me:443/transaction/8a80843b6750cea9016750e612a30000/attach
GET https://csye6225-fall2018-bhargavan.me:443/transaction
POST https://csye6225-fall2018-yadavgau.me:443/user/create.bak
No Environment
POST
https://csye6225-fall2018-bhargavan.me:443/user/register
Params
Send
Save
.comabc@gmail.comabc@gmail.comabc@gmail.comabc@gmail.comabc@gmail.com",
"password":"nb"
}
Body
Cookies
Headers (4)
Test Results
Status: 500 Internal Server Error
Time: 524 ms
Size: 425 B
Pretty
Raw
Preview
JSON
{
"timestamp": "2018-11-26T21:17:24.845+0000",
"status": 500,
"error": "Internal Server Error",
"message": "could not execute statement; SQL [n/a]; nested exception is org.hibernate.exception.DataException: could not execute statement",
"path": "/user/register"
}
Build
Browse