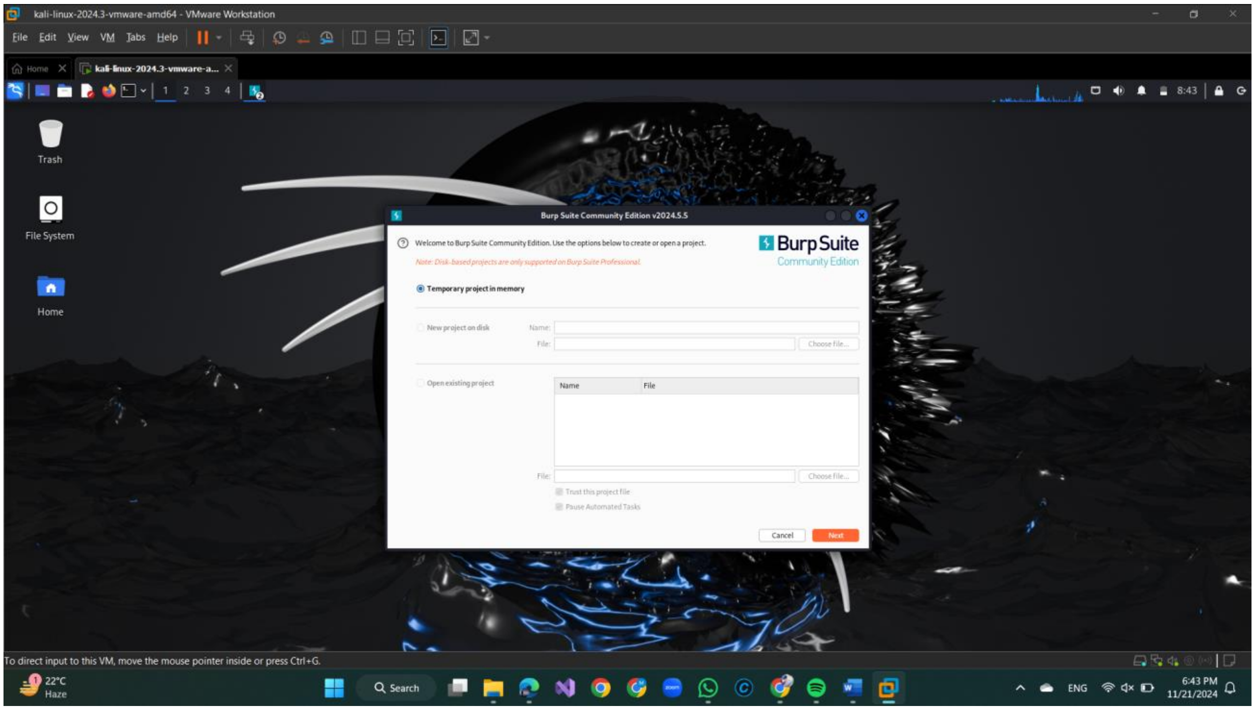
Task 1

Conduct a Penetration Test

Step 1: Setting Up Burp Suite

1. **Launch**:
   - Launch the community free edition of Burp Suite.



kali-linux-2024.3-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
kali-linux-2024.3-vmware-a...
Trash
File System
Home
8:43
Burp Suite Community Edition v2024.5.5
Burp Suite
Community Edition

Welcome to Burp Suite Community Edition. Use the options below to create or open a project.

Note: Disk-based projects are only supported on Burp Suite Professional.

● Temporary project in memory

○ New project on disk Name: File: Choose file...

○ Open existing project

Name	File

File: Choose file...

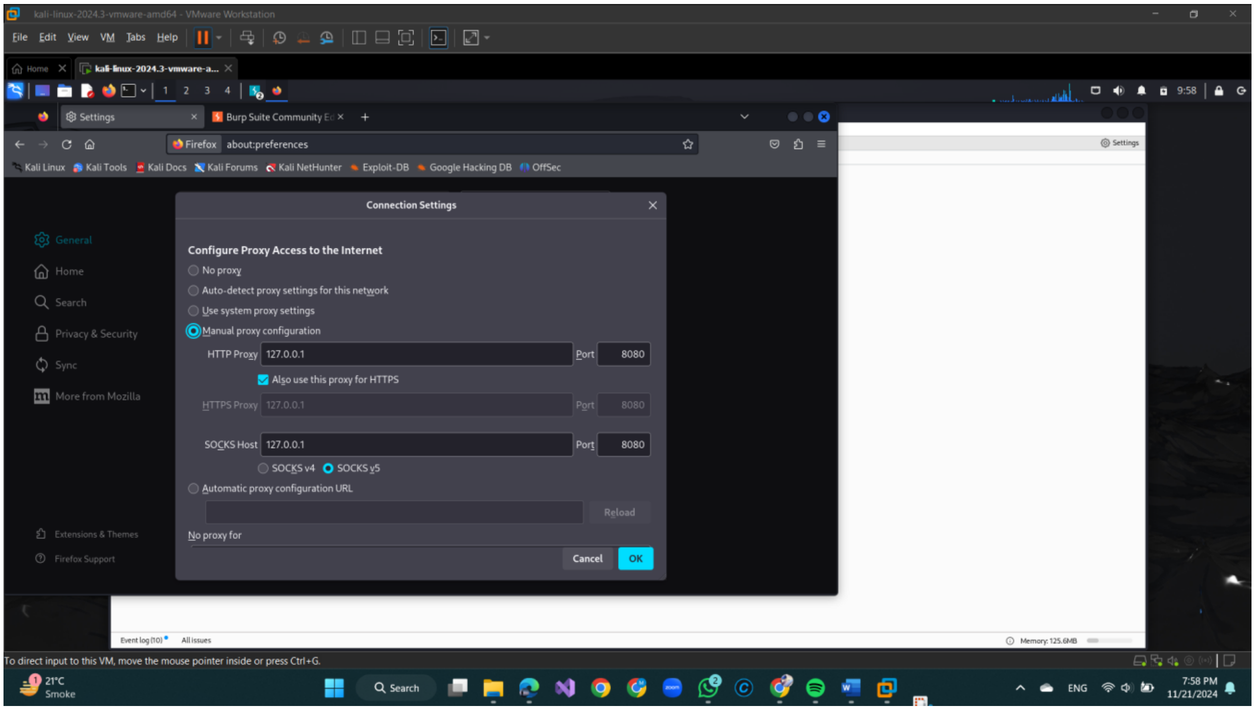
□ Trust this project file

□ Pause Automated Tasks

Cancel
Next
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
22°C
Haze
Search
ENG
6:43 PM
11/21/2024

Configure Your Browser:

- In Burp Suite, go to **Proxy > Intercept** and ensure "Intercept is off."
- **Set your browser to use Burp's proxy** (default: 127.0.0.1:8080).
  - In your browser's **Network Settings**, set manual proxy configuration to 127.0.0.1 for HTTP/HTTPS with port 8080.



Connection Settings

Configure Proxy Access to the Internet

○ No proxy

○ Auto-detect proxy settings for this network

○ Use system proxy settings

● Manual proxy configuration

HTTP Proxy 127.0.0.1 Port 8080

☑ Also use this proxy for HTTPS

HTTPS Proxy 127.0.0.1 Port 8080

SOCKS Host 127.0.0.1 Port 8080

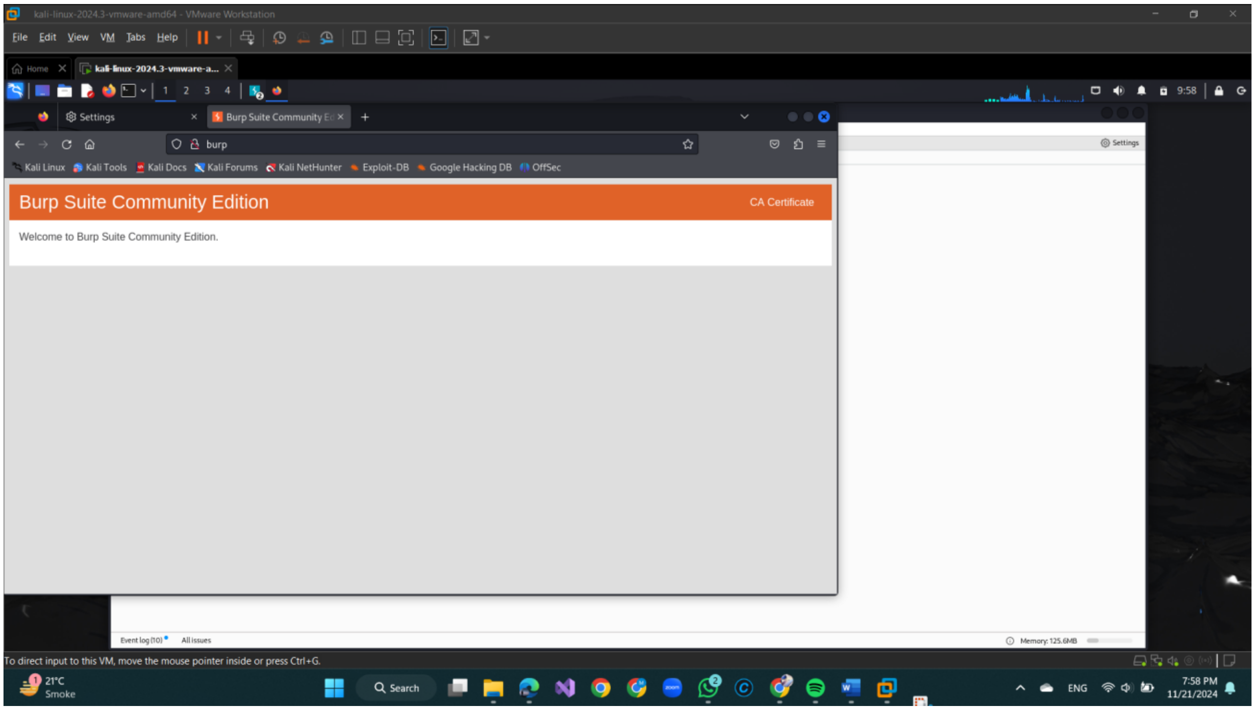
○ SOCKS v4 ● SOCKS v5

○ Automatic proxy configuration URL

No proxy for

Install Burp's CA Certificate:

- Open your browser and visit http://burp while Burp Suite is running.
- Download and install the CA certificate for analyzing HTTPS traffic.



burp

Burp Suite Community Edition

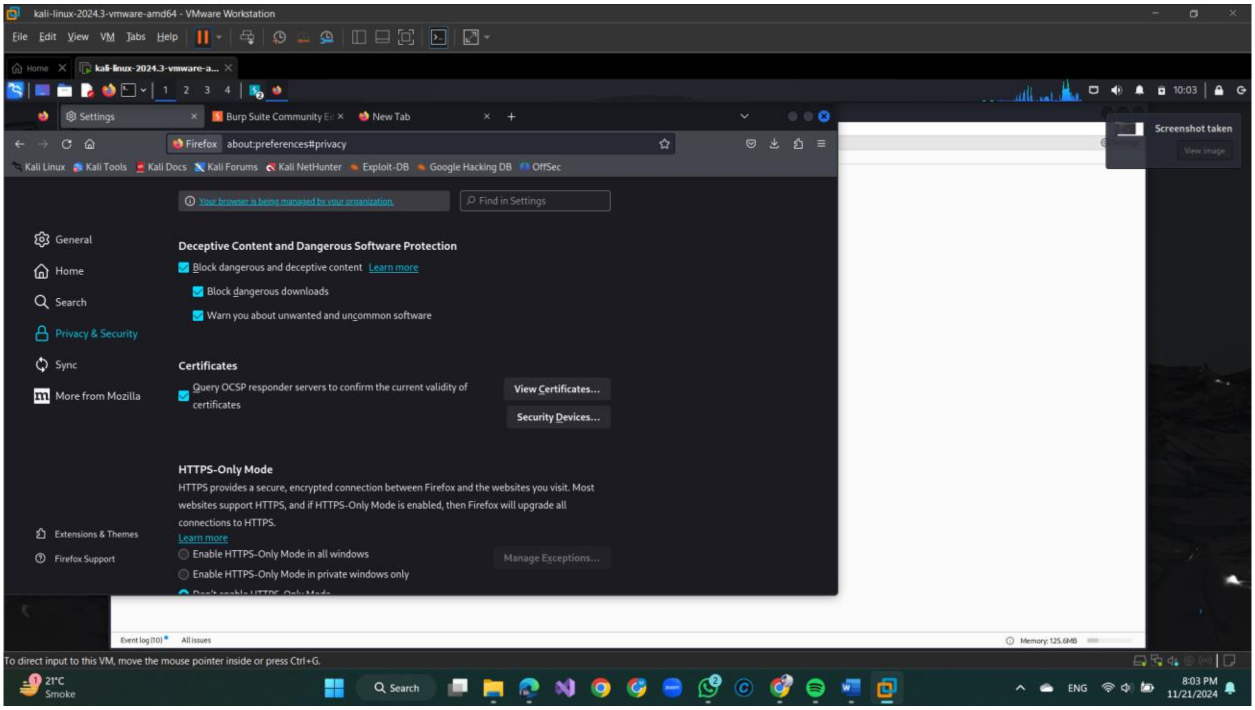
CA Certificate

Welcome to Burp Suite Community Edition.

Settings
Burp Suite Community Ed
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Go to Privacy & Settings

Click on view certificates then click on import.



Firefox about:preferences#privacy

Your browser is being managed by your organization.

Find in Settings

Deceptive Content and Dangerous Software Protection

☑ Block dangerous and deceptive content Learn more

☑ Block dangerous downloads

☑ Warn you about unwanted and uncommon software

Certificates

☑ Query OCSP responder servers to confirm the current validity of certificates

View Certificates…

Security Devices…

HTTPS-Only Mode

HTTPS provides a secure, encrypted connection between Firefox and the websites you visit. Most websites support HTTPS, and if HTTPS-Only Mode is enabled, then Firefox will upgrade all connections to HTTPS.

Learn more

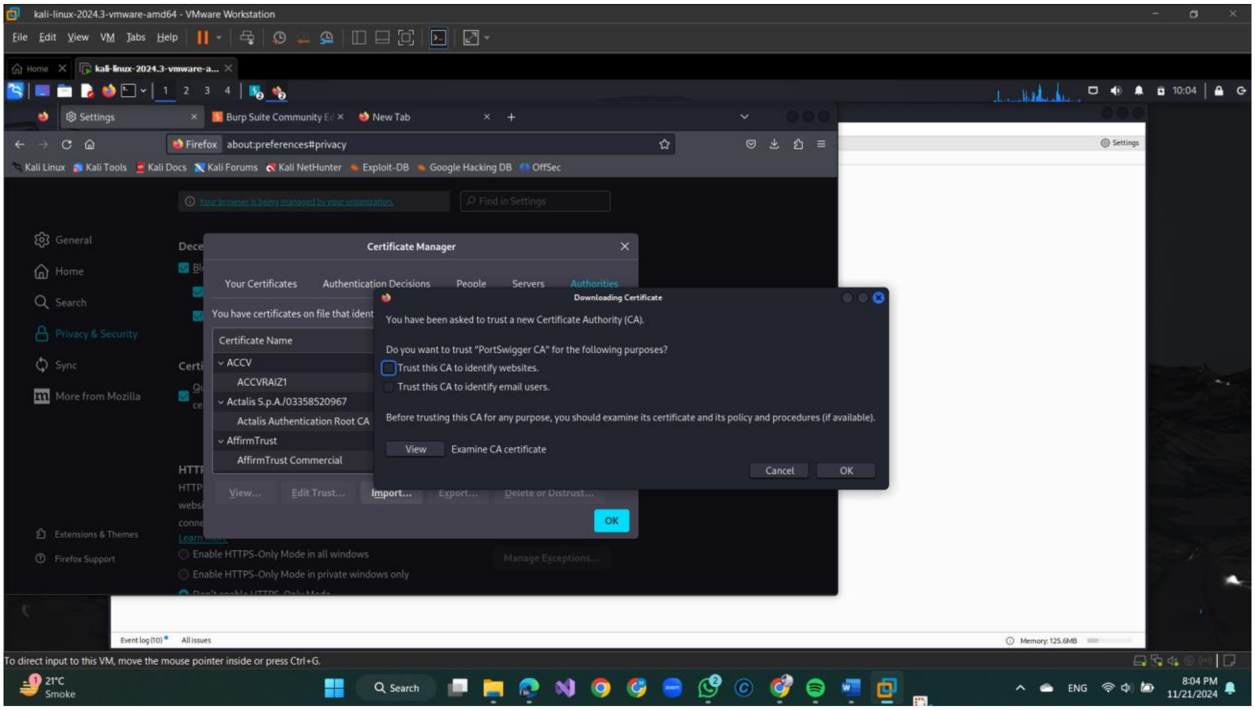
○ Enable HTTPS-Only Mode in all windows

○ Enable HTTPS-Only Mode in private windows only

Manage Exceptions…

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Check the Trust this CA to identity websites then click on ok.



Certificate Manager

Your Certificates | Authentication Decisions | People | Servers | Authorities

You have certificates on file that ident

Certificate Name

- ACCV
  - ACCVRAIZ1
- Actalis S.p.A./03358520967
  - Actalis Authentication Root CA
- AffirmTrust
  - AffirmTrust Commercial

View… Edit Trust… Import… Export… Delete or Distrust…

OK

Downloading Certificate

You have been asked to trust a new Certificate Authority (CA).

Do you want to trust "PortSwigger CA" for the following purposes?

□ Trust this CA to identify websites.

□ Trust this CA to identify email users.

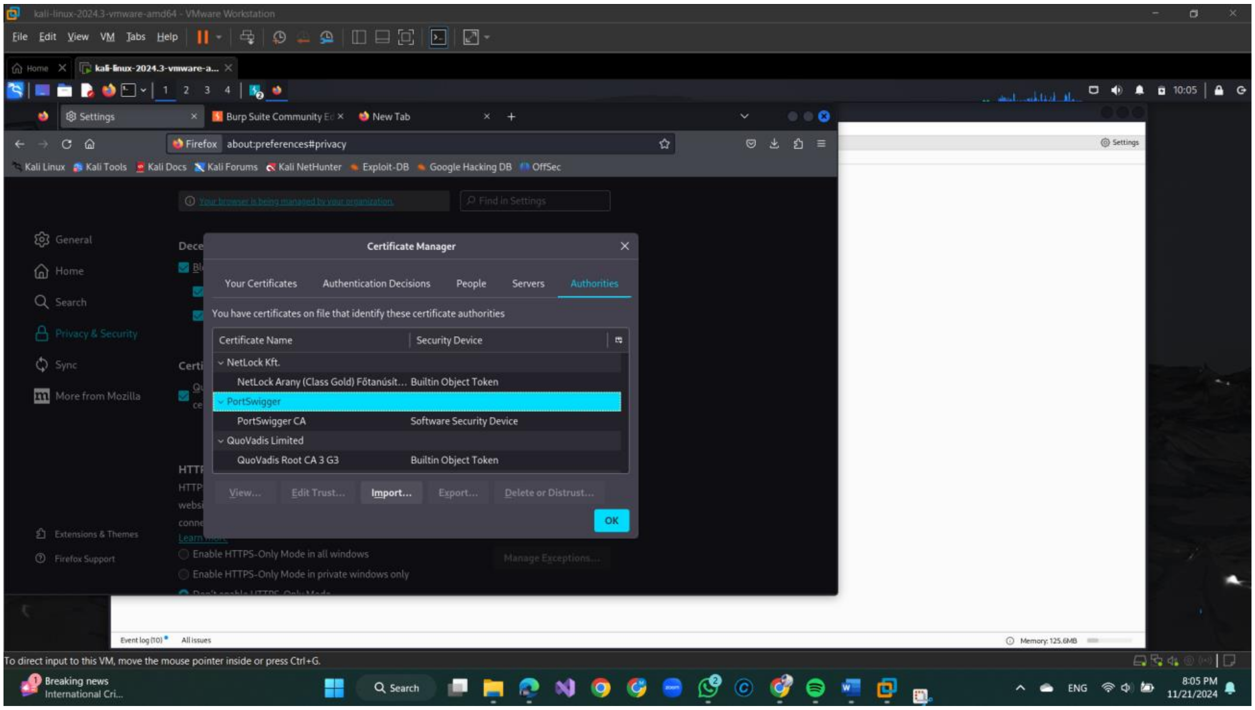
Before trusting this CA for any purpose, you should examine its certificate and its policy and procedures (if available).

View Examine CA certificate

Cancel OK

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Scroll Down & Click on PortSwigger then click ok



Certificate Manager

You have certificates on file that identify these certificate authorities

Certificate Name	Security Device
NetLock Kft.	
NetLock Arany (Class Gold) Főtanúsít…	Builtin Object Token
PortSwigger	
PortSwigger CA	Software Security Device
QuoVadis Limited	
QuoVadis Root CA 3 G3	Builtin Object Token

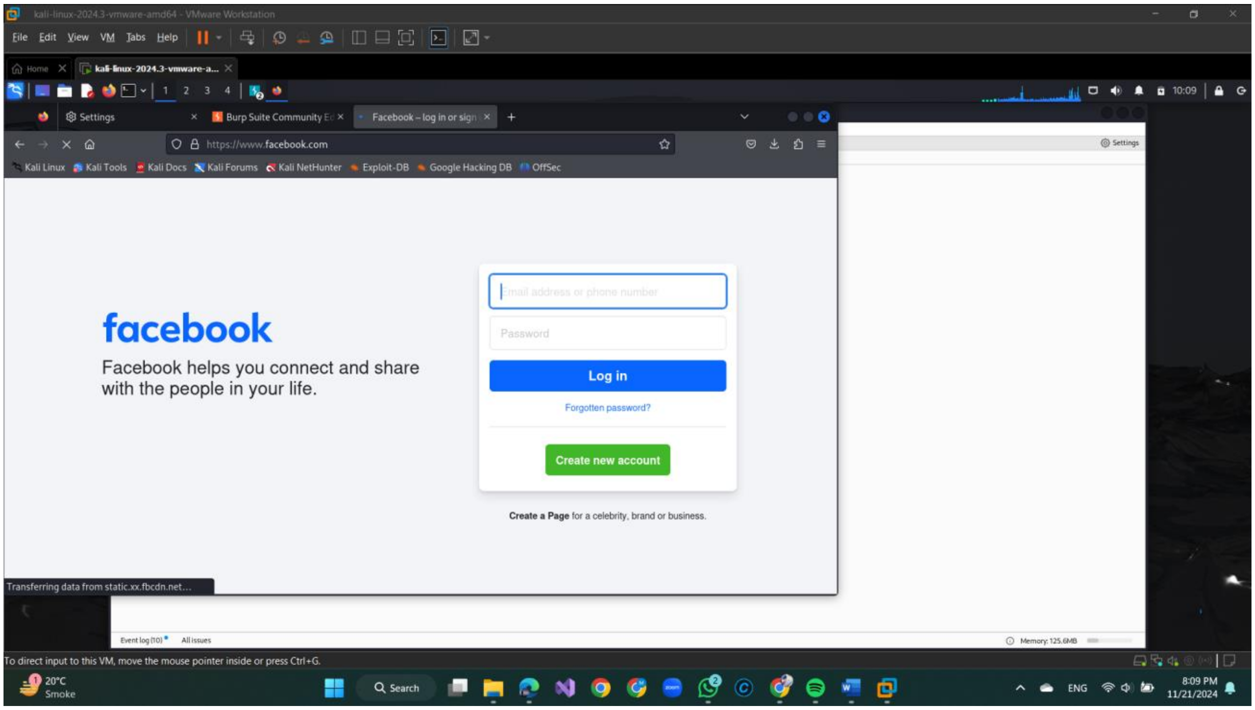
○ Enable HTTPS-Only Mode in all windows

○ Enable HTTPS-Only Mode in private windows only

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Step 2: Manual Testing with Proxy:

- Ensure **Intercept** is off in **Proxy**.
- Visit key pages of the web app (e.g., login forms) and enter test data.



Facebook helps you connect and share with the people in your life.

Transferring data from static.xx.fbcdn.net...

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

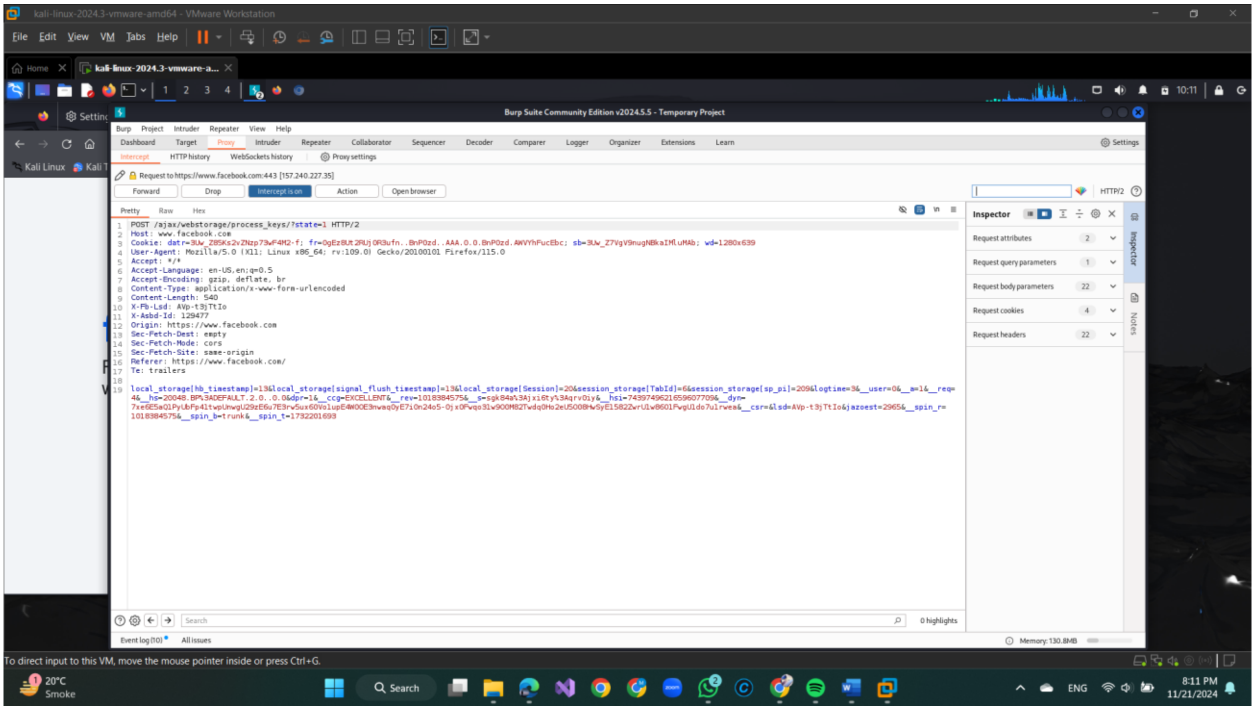
- View requests and responses between your browser and the web app in **Proxy > HTTP history**.

➢ **Automated Scanning**:

- In **Target > Site Map**, right-click the target domain and select **Scan**.
- Choose specific sections (like login pages or forms) for active scanning, checking for vulnerabilities such as SQL Injection and Cross-Site Scripting (XSS).

Step 3: Intercepting and Modifying Requests

1. **Intercepting**:
    - Turn **Intercept on** in **Proxy > Intercept**.
    - Perform an Action act as the web app (e.g., submit a form). The HTTP request will appear in Burp's **Intercept** tab.



Request to https://www.facebook.com:443 [157.240.227.35]

```
POST /ajax/webstorage/process_keys/?state=1 HTTP/2
Host: www.facebook.com
Cookie: datr=3Uw_Z85Ks2vZNzp73wF4M2-f; fr=0gEz8Ut2RUj0R3ufn..BnP0zd..AAA.0.0.BnP0zd.AWVYhFucEbc; sb=3Uw_Z7VgV9nugNBkaIMluMAb; wd=1280x639
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 540
X-Fb-Lsd: AVp-t3jTtIo
X-Asbd-Id: 129477
Origin: https://www.facebook.com
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Referer: https://www.facebook.com/
Te: trailers

local_storage[hb_timestamp]=13&local_storage[signal_flush_timestamp]=13&local_storage[Session]=20&session_storage[TabId]=6&session_storage[sp_pi]=209&logtime=3&__user=0&__a=1&__req=
4&__hs=20048.BP%3ADEFAULT.2.0..0.0&dpr=1&__ccg=EXCELLENT&__rev=1018384575&__s=sgk84a%3Ajxi6ty%3Aqrv0iy&__hsi=7439749621659607709&__dyn=
7xe6E5aQ1PyUbFp41twpUnwgU29zE6u7E3rw5ux60VolupE4W0OE3nwaq0yE7i0n24o5-0jx0Fwqo31w900M82Twdq0Ho2eU5008HwSyE15822wrU1w8601FwgU1do7ulrwea&__csr=&lsd=AVp-t3jTtIo&jazoest=2965&__spin_r=
1018384575&__spin_b=trunk&__spin_t=1732201693
```

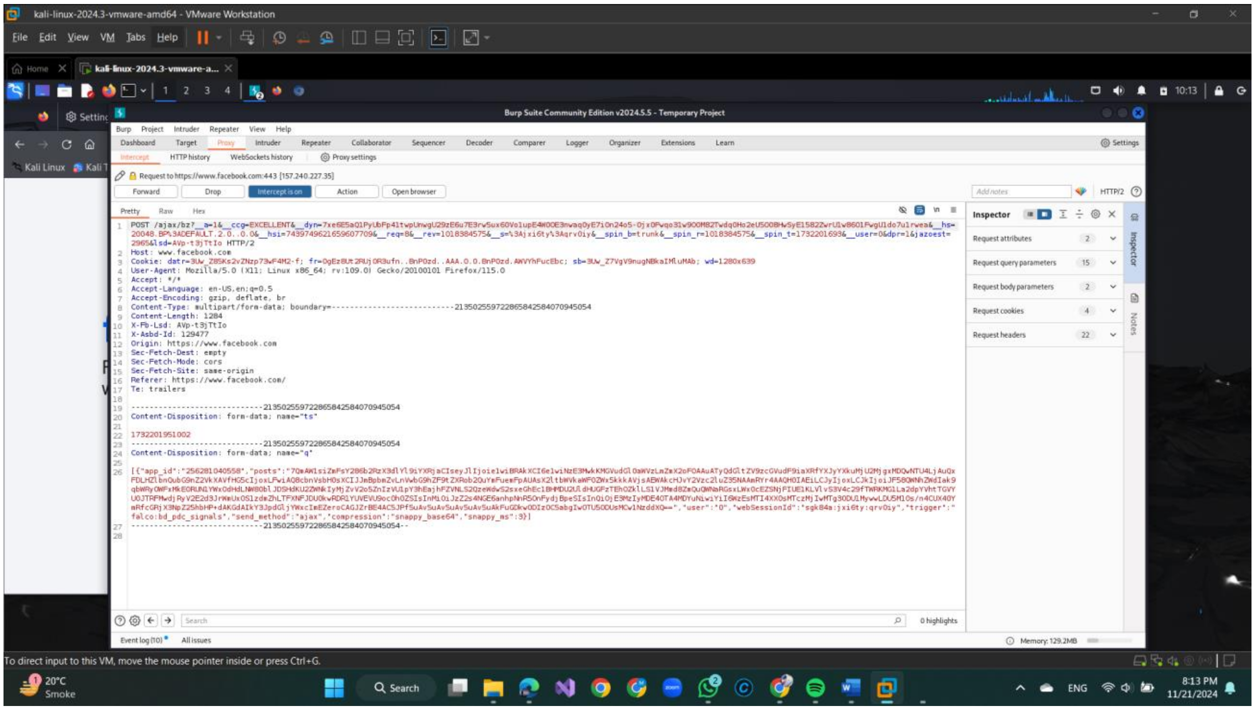
Event log (10) All issues

Memory: 130.8MB

To direct input to this VM, move the pointer inside or press Ctrl+G.

Modifying Requests:

- You can edit the parameters in the request before forwarding it to the server.
- Example: Modify the parameter to ' OR 1=1-- to test for SQL Injection and forward the request.
- Observe the response from the server to identify potential vulnerabilities.


kali-linux-2024.3-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
kali-linux-2024.3-vmware-a...
1 2 3 4
10:13
Burp Suite Community Edition v2024.5.5 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Intercept HTTP history WebSockets history Proxy settings
Forward
Drop
Intercept is on
Action
Open browser
Pretty Raw Hex
Add notes
HTTP/2
Inspector
Request attributes 2
Request query parameters 15
Request body parameters 2
Request cookies 4
Request headers 22
Notes
Search
0 highlights
Event log (10)
All issues
Memory: 129.2MB
20°C
Smoke
Search
ENG
8:13 PM
11/21/2024

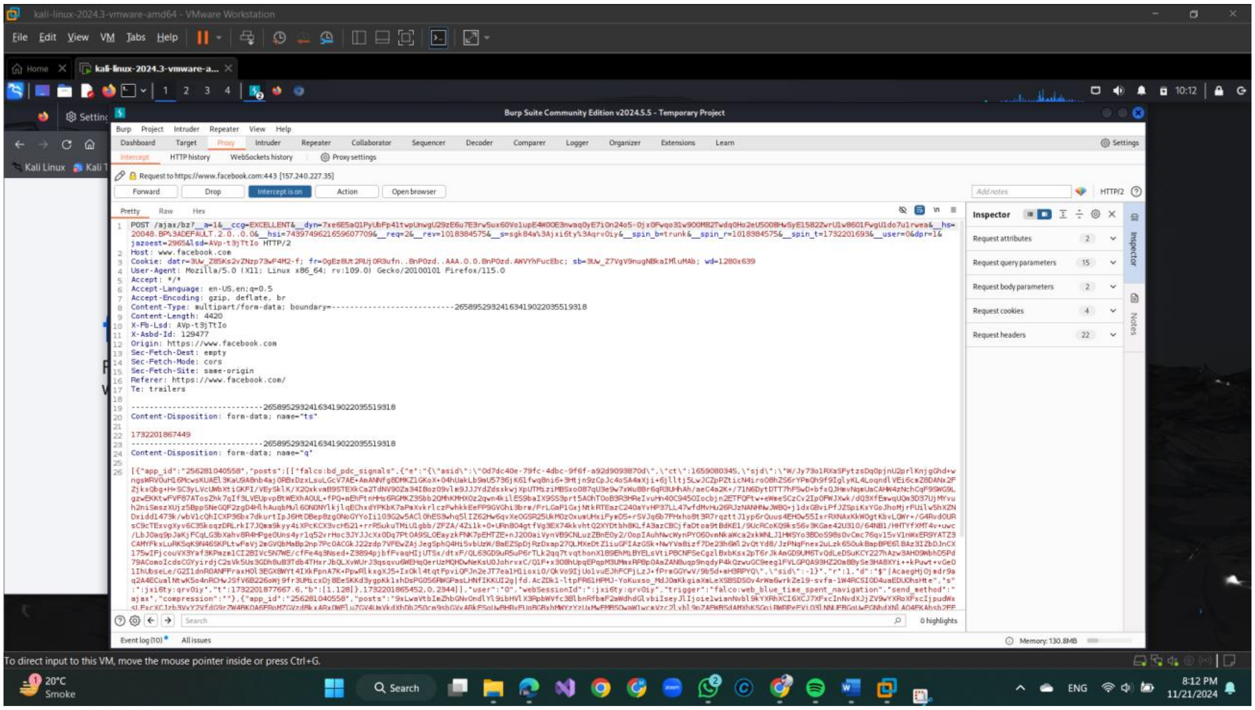
Request to https://www.facebook.com:443 [157.240.227.35]

```
POST /ajax/bz?__a=1&__ccg=EXCELLENT&__dyn=7xe6E5aQ1PyUbFp41twpUnwgU29zE6u7E3rw5ux60Vo1upE4W0OE3nwaq0yE7i0n24o5-0jx0Fwqo31w900M82Twdq0Ho2eU5O08HwSyE15822wrU1w8601FwgU1do7u1rwea&__hs=
20048.BP%3ADEFAULT.2.0..0.0&__hsi=7439749621659607709&__req=8&__rev=1018384575&__s=%3Ajxi6ty%3Aqrv0iy&__spin_b=trunk&__spin_r=1018384575&__spin_t=1732201693&__user=0&dpr=1&jazoest=
2965&lsd=AVp-t3jTtIo HTTP/2
Host: www.facebook.com
Cookie: datr=3Uw_Z85Ks2vZNzp73wF4M2-f; fr=0gEz8Ut2RUj0R3ufn..BnP0zd..AAA.0.0.BnP0zd.AWVYhFucEbc; sb=3Uw_Z7VgV9nugNBkaIMluMAb; wd=1280x639
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: multipart/form-data; boundary=---------------------------213502559722865842584070945054
Content-Length: 1284
X-Fb-Lsd: AVp-t3jTtIo
X-Asbd-Id: 129477
Origin: https://www.facebook.com
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Referer: https://www.facebook.com/
Te: trailers

-----------------------------213502559722865842584070945054
Content-Disposition: form-data; name="ts"

1732201951002
-----------------------------213502559722865842584070945054
Content-Disposition: form-data; name="q"

[{"app_id":"256281040558","posts":"7QmAW1siZmFsY2B6b2RzX3dlYl9iYXRjaCIseyJlIjoie1wiBRAkXCI6e1wiNzE3MwkKMGVudGl0aWVzLmZmX2oFOAAuATyQdGltZV9zcGVudF9iaXRfYXJyYXkuMjU2MjgxMDQwNTU4LjAuQx
FDLHZlbnQubG9nZ2VkXAVfHG5cIjoxLFwiAQ8cbnVsbH0sXCIJJmBpbmZvLnVwbG9hZF9tZXRob2QuYmFuemFpAUAsX2ltbWVkaWF0ZWx5kkkAVjsABWAkcHJvY2Vzc2luZ35NAAmRYr4AAQHOIAEiLCJyIjoxLCJkIjoiJF58QWNhZWdIak9
qbWRyOWFxMkEORUN1YWxOdHdLNW8OblJDSHdKU2ZWNkIyMjZvV2o5ZnIzVU1pY3hEajhFZVNLS2QzeWdwS2sxeGhEc1BHMDU2UldHUGFzTEhOZklLS1VJMmd8ZmQuQWNaRGsxLWxOcEZSNjFIUE1KLVlvS3V4c29fTWRKMG1La2dpYVhtTGVY
U0JTRFMwdjRyV2E2d3JrWmUxOS1zdmZhLTFXNFJDU0kwRDR1YUVEVU9ocOh0ZSIsInMiOiJzZ2s4NGE6anhpNnR5OnFydjBpeSIsInQiOjE3MzIyMDE4OTA4MDYuNiwiYiI6WzEsMTI4XX0sMTczMjIwMTg3ODU1MywwLDU5M10s/n4CUX40Y
mRfcGRjX3NpZ25hbHP+dAKGdAIkY3JpdGljYWxcImEZeroCAGJZrBE4ACSJPfSuAvSuAvSuAvSuAvSuAkFuGDkwODIzOCSabgIwOTU5ODUsMCwlNzddXQ==","user":"0","webSessionId":"sgk84a:jxi6ty:qrv0iy","trigger":"
falco:bd_pdc_signals","send_method":"ajax","compression":"snappy_base64","snappy_ms":3}]
-----------------------------213502559722865842584070945054--
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Step 4: Testing for Vulnerabilities

1. **SQL Injection**:
   - Use **Proxy > Intercept** or **Repeater** (explained later) to modify input fields or URL parameters (e.g., entering ' OR 1=1-- in a login form) and test for SQL Injection.
2. **Cross-Site Scripting (XSS)**:
   - Inject script tags (e.g., <script>alert('XSS')</script>) into input fields.
   - If the script runs in the browser, the application is vulnerable to XSS.
3. **Cross-Site Request Forgery (CSRF)**:
   - Use **Repeater** to craft and send requests without proper CSRF tokens to test if the app lacks protection against unauthorized actions.



Request to https://www.facebook.com:443 [157.240.227.35]

```
POST /ajax/bz?__a=1&__ccg=EXCELLENT&__dyn=7xe6E5aQ1PyUbFp41twpUnwgU29zE6u7E3rw5ux60Vo1upE4W0OE3nwaq0yE7i0n24o5-0jx0Fwqo31w900M82Twdq0Ho2eU500BHwSyE15822wrU1w8601FwgU1do7u1rwea&__hs=20048.BP%3ADEFAULT.2.0..0.0&__hsi=7439749621659607709&__req=2&__rev=1018384575&__s=sgk84a%3Ajxi6ty%3Aqrv0iy&__spin_b=trunk&__spin_r=1018384575&__spin_t=1732201693&__user=0&dpr=1&jazoest=2965&lsd=AVp-t3jTtIo HTTP/2
Host: www.facebook.com
Cookie: datr=3Uw_Z8SKs2vZNzp73wF4M2-f; fr=0gEz8Ut2RUj0R3ufn..BnP0zd..AAA.0.0.BnP0zd.AWVYhFucEbc; sb=3Uw_Z7VgV9nugNBkaIMluMAb; wd=1280x639
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: multipart/form-data; boundary=---------------------------26589529324163419022035519318
Content-Length: 4420
X-Fb-Lsd: AVp-t3jTtIo
X-Asbd-Id: 129477
Origin: https://www.facebook.com
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Referer: https://www.facebook.com/
Te: trailers

-----------------------------26589529324163419022035519318
Content-Disposition: form-data; name="ts"

1732201867449
-----------------------------26589529324163419022035519318
Content-Disposition: form-data; name="q"

[{"app_id":"256281040558","posts":[["falco:bd_pdc_signals",{"e":"{\"asid\":\"0d7dc40e-79fc-4dbc-9f6f-a92d9093870d\",\"ct\":1659080345,\"sjd\":\"W/Jy73o1RXaSFytzsDq0pjnU2prlKnjgGhd+w
ngsWRV0uH16McwsKUAEl3KaU9A8nb4aj0RBxDzxLsuLGcV7AE+AmANNfg8DMKZ1GKoX+04hUakLb9mU5736jK61fwq8ni6+3Htjn9zCpJc4oSA4mXji+6jlltj5LwJCZpPZticN4iro08hZS6rYPm0h9f9IglyKL4Loqndl VEi6cmZ8DANx2F
ZjkxQbg+H+SC3yLVcUWbXtiGKFI/VEySklK/X2QxkvmB9STEXkCa2TdNV90Za34IBoz09vlm9JJJYdZdsxkwjXpUTMiziMBSxo087qU3e9w7xWu88r6qR3UHhAh/aeC4a2K+/71N6DytDTT7hF5wD+bfxQJHmvNqmUaCAHW4zNchCqF9SWG9L
gzwEKKtwFVF87ATosZhk7qIf3LVEUpvpBtWEXhAOUL+fPQ+mEhFtnHHs6RGMKZ3Sbb20MhKMHX0z2qwn4kilES9baIX9SS3prt5A0hT0oB3R3HReIvuHn40C9450Iocbjn2ETFQFtw+eWmeSCzCv2Ip0FWJXwk/dQ3XfEmwqUQm3D37UjMYvu
h2niSmszXUjz5BppSNeGQF2zgD4HlhAuqbMul6ONONYlkjlqEChxdYPKbK7aPmXvkrlczPwhkkEeFP9GVGhi3brm/FrLGaP1GxjNtkRTEazC240aYvHP37LL47wfdMvHu26RJzNANHNwJWBQ+jldxGBviPfJZSpiKxYGoJhoMjrFUilw5hXZN
Dxidd1473k/wbV1cQhICXP36bx7dkurtIpJ6HtDBep8zg0NoGYYoIi103G2w5ACl0hES3whq5lIZ62Hw6qvXeOGSR25UkM0zOxumUHxiFymD5+rSVJq6b7FHxho8t3R7rqzttJ1yp6rQuus4EHOw55IxrRXNAxKkW0gtKbvLQWr+/G4RvdOUR
sC9cTExvgXyv6C35koqzDRLrkI7JQma9kyy4iXPcKCX3vcH521+rrR5ukuTMiUlgbb/ZFZA/4Zilk+0+URn804gtfVg3EX74kkvhtQ2XYDtbh8KLfA3azCBCjfaDtoa9tBdKE1/9UcRCoKQ9ks56v3KGae42U310/64NB1/HHTYfXMT4v+uwc
/LbJ0aq9pJaKjFCqLG3bXahv8R4HPge0Uns4yrlq52vrHoc3JYJJcXx0Dq7PtOA9SLOEayzkFNK7pEHTZE+nJ200aiVynVB9CNLuzZBnE0y2/0opIAuhNwcWynPY06OvmNkaWca2xkWNLJ1HWSYo3BDoS98s0vCmc76qv15vV1nWxER9YATZ3
CAMYFkxLuRKSqK9N46SKPLtwFaVj2mGVQbMaBp2np7PcOACGkJ22zdp7VFEwZAjJegSphQ4HiSvbUzW/BaEZSpDjRzDxap27QLMXeDtZliuGFIAzGSk+NwYVa8izf7De23h6Wl2vQtYd8/JzPNqFnex2uLzk65OukBapBPE6lBAz3IZbDJnCX
175wIFjcouVX3Yaf3KPmzmlCI2BIVc5N7WE/cfFe4q3Nsed+Z3894pjbfFvaqHIjUTSx/dtxF/QL63GD9uR5uP6rTLk2qq7tvqthonX189EhMiBYELsVtiPBCNFSeCgzlBxbKsx2pT6rJkAmGD9UM6TvQdLeDSuKCY227hAzw3AH09WbhD5Pd
79ACom oIcdsCGYyirdjC2sVk5Us3GDh8uB3Tdb4THxrJbQLXvWUrJ3qsqvu6WEHqQerUzMQHDwNeKsU0JohrvxC/Q1F+x308hUpqEPqpM3UMmxRPBp0AaZAN8uqp9nqdyP4kQzwuGC9eeg1FVLGPQA93HZ20a8BySe3HABXYi++kPuwt+vGeD
1IhUbseLe/G2I1dnR0ANFFraxH0l3EGX8WYt4IXkFpnA7K+PpwRlkxgXJ5+IxOkl4tqtFpviOFJn2eJT7ea1H1ioxi0/QkVo9IjUolvuEJhFCFjLzJ+fPrmGGYwV/9b5d+mH3RPYQ\",\"sid\":-1}","r":1,"d":"$^|AcaegHjOjmdr9a
q2A4ECualNtwK5o4nRCHwJSfV6B226oWj9fr3UMicxDj8EeSKKd3ygpKklxhDsPG0S6RWGPasLHNfIKKUI2g|fd.AcZDkl-ltpFR61HPMJ-YoKuxso_MdJ0mKkgiaXmLeXS8SDSOv4rWa6wrkZe19-svfa-1W4RCSIOD4uaEDUOhsHte","s"
:":jxi6ty:qrv0iy","t":1732201877667.6,"b":[1,128]},1732201865452,0,2344]],"user":"0","webSessionId":":jxi6ty:qrv0iy","trigger":"falco:web_blue_time_spent_navigation","send_method":"
ajax","compression":""},{"app_id":"256281040558","posts":"9xLwaVtbImZhbGNvOndlYl9ibHVlX3RpbWVfc3BlbnRfbmF2aWdhdGlvbiIseyJlIjoielwianNvbl9kYXRhXCI6XCJ7XFxcInNvdXJjZV9wYXRoXFxcIjpudWx
```

- **Conclusion**

No vulnerabilities were found after testing the Facebook login page using Burp Suite. This outcome suggests that Facebook has implemented strong security measures to protect against common web vulnerabilities, such as SQL Injection and cross-site Scripting (XSS).