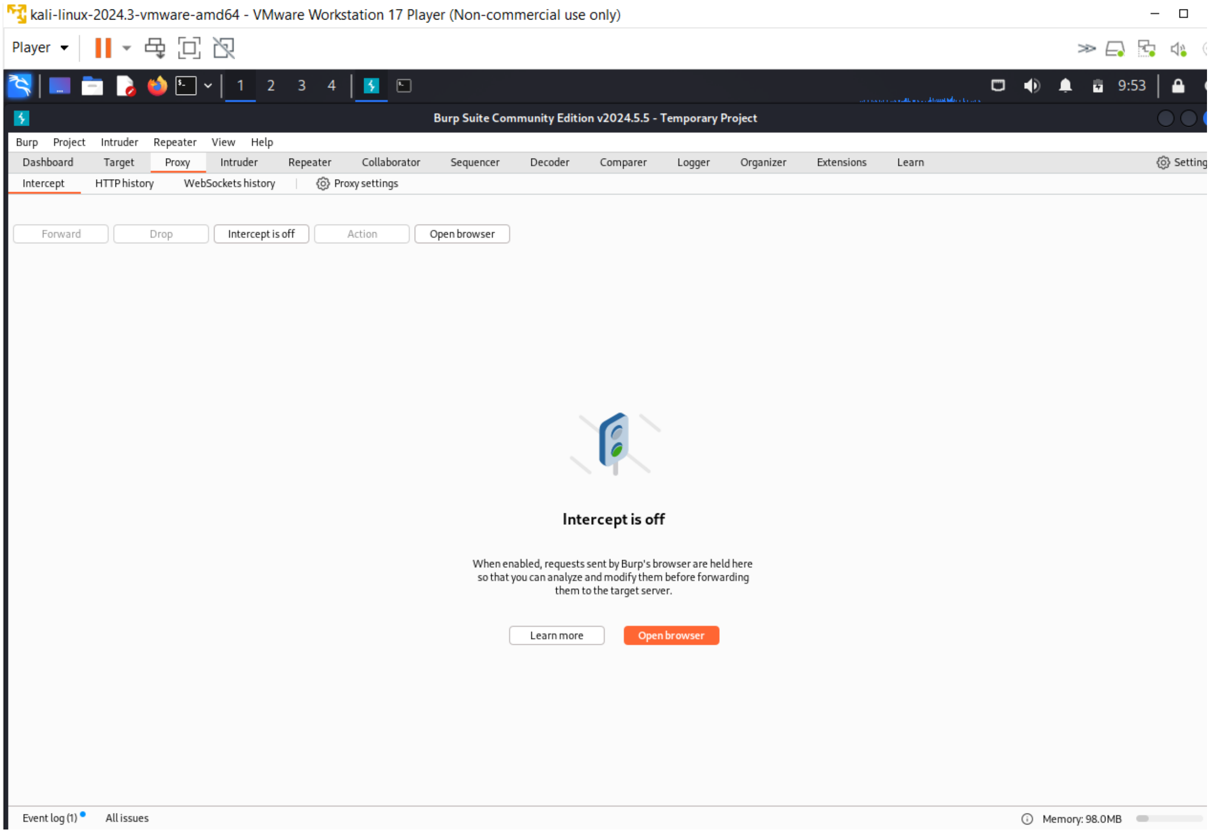
USING BURP SUITE TO INTERCEPT CLIENT-SIDE REQUEST

TOOL: KALI LINUX

Burp Suite is a popular web application security testing tool used by security professionals and ethical hackers to identify vulnerabilities in web applications. It provides a comprehensive set of tools for tasks such as:

1. **Intercepting Proxy**: Allows users to inspect and modify HTTP/S traffic between the browser and the web server in real-time.
2. **Scanner**: Automated scanning capabilities to identify common web vulnerabilities like SQL injection, cross-site scripting (XSS), and others.
3. **Intruder**: A powerful tool for automating customized attacks against web applications, such as brute force attacks or parameter fuzzing.
4. **Repeater**: Enables manual testing of individual HTTP requests by modifying and resending them to see how the application responds.
5. **Sequencer**: Analyzes the randomness of session tokens and other identifiers to assess their security.
6. **Extender**: Allows users to enhance Burp Suite’s functionality through plugins or custom extensions.

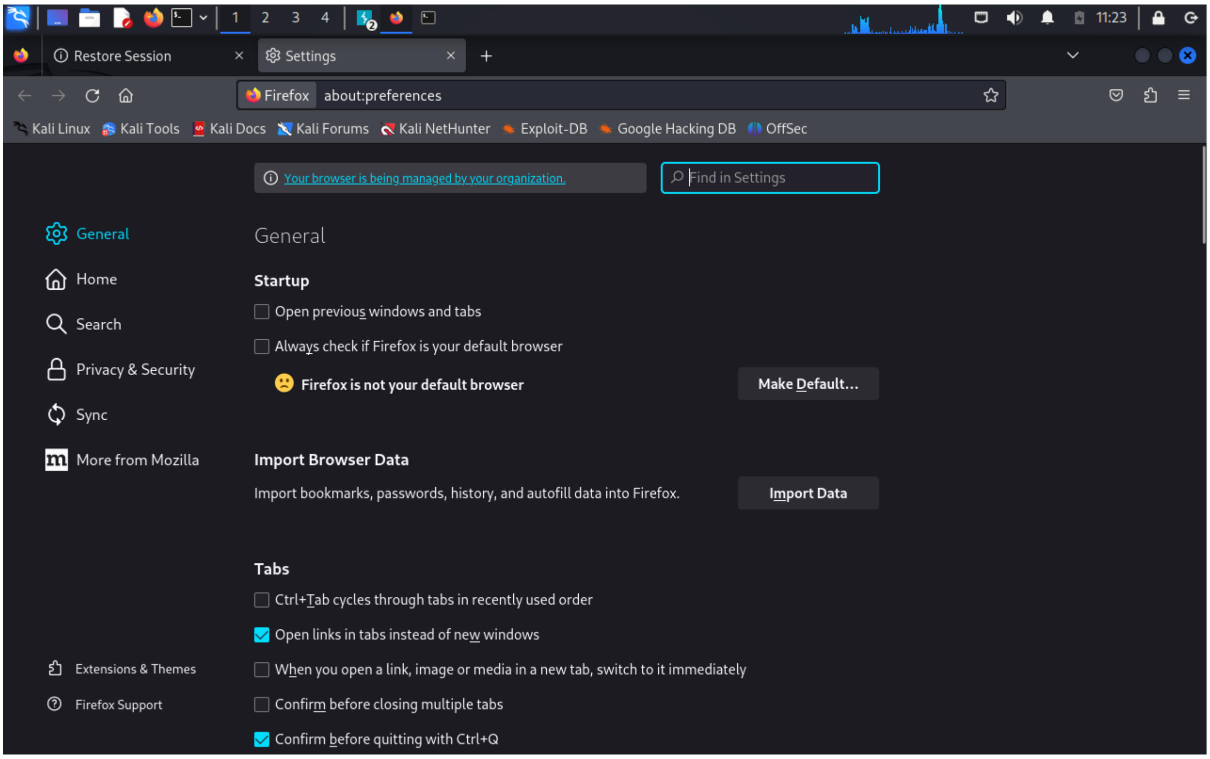
Burp Suite is widely used in penetration testing, vulnerability assessment, and web application security research. It helps security professionals find and fix security issues before they can be exploited by attackers.



kali-linux-2024.3-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
1 2 3 4
9:53
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 off Action Open browser
Learn more Open browser
Event log (1) All issues
Memory: 98.0MB

Intercept is off

When enabled, requests sent by Burp's browser are held here so that you can analyze and modify them before forwarding them to the target server.



Your browser is being managed by your organization.

General

Startup

- ☐ Open previous windows and tabs
- ☐ Always check if Firefox is your default browser

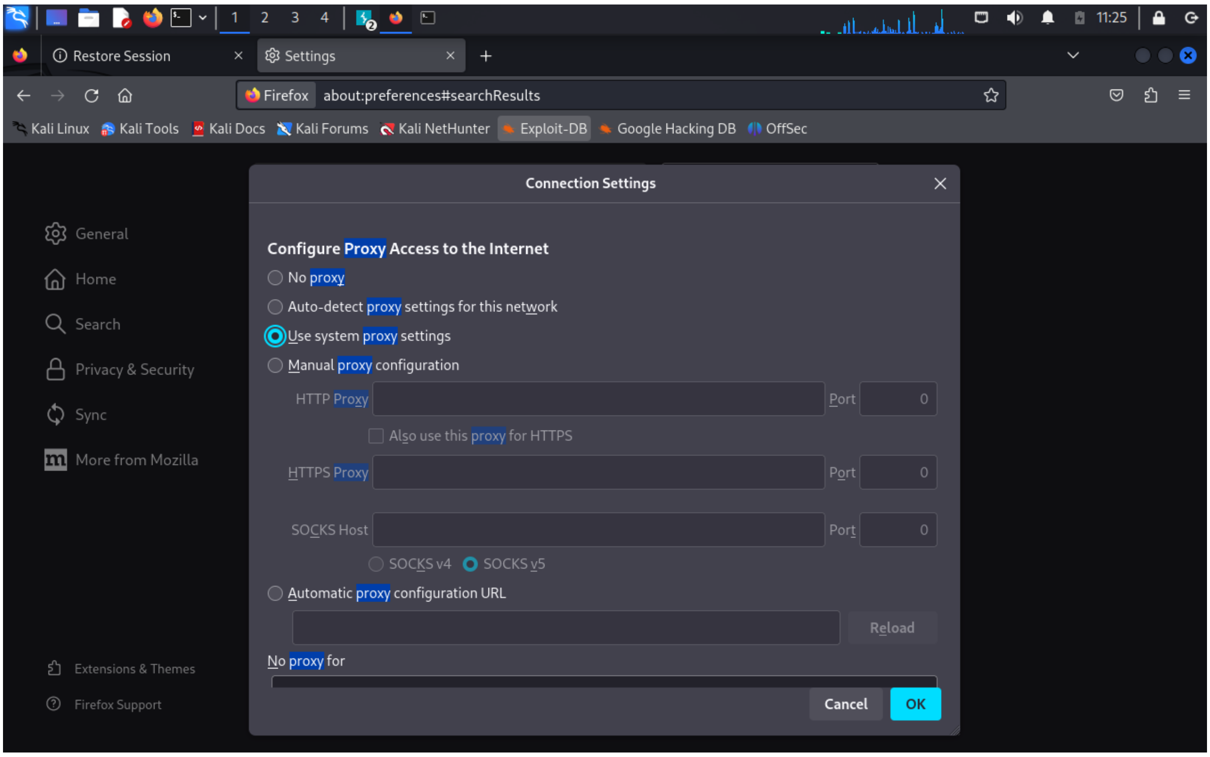
Firefox is not your default browser

Import Browser Data

Import bookmarks, passwords, history, and autofill data into Firefox.

Tabs

- ☐ Ctrl+Tab cycles through tabs in recently used order
- ☑ Open links in tabs instead of new windows
- ☐ When you open a link, image or media in a new tab, switch to it immediately
- ☐ Confirm before closing multiple tabs
- ☑ Confirm before quitting with Ctrl+Q


1 2 3 4
11:25
Restore Session
Settings
Firefox about:preferences#searchResults
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
General
Home
Search
Privacy & Security
Sync
More from Mozilla
Extensions & Themes
Firefox Support

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 ______ Port 0

□ Also use this proxy for HTTPS

HTTPS Proxy ______ Port 0

SOCKS Host ______ Port 0

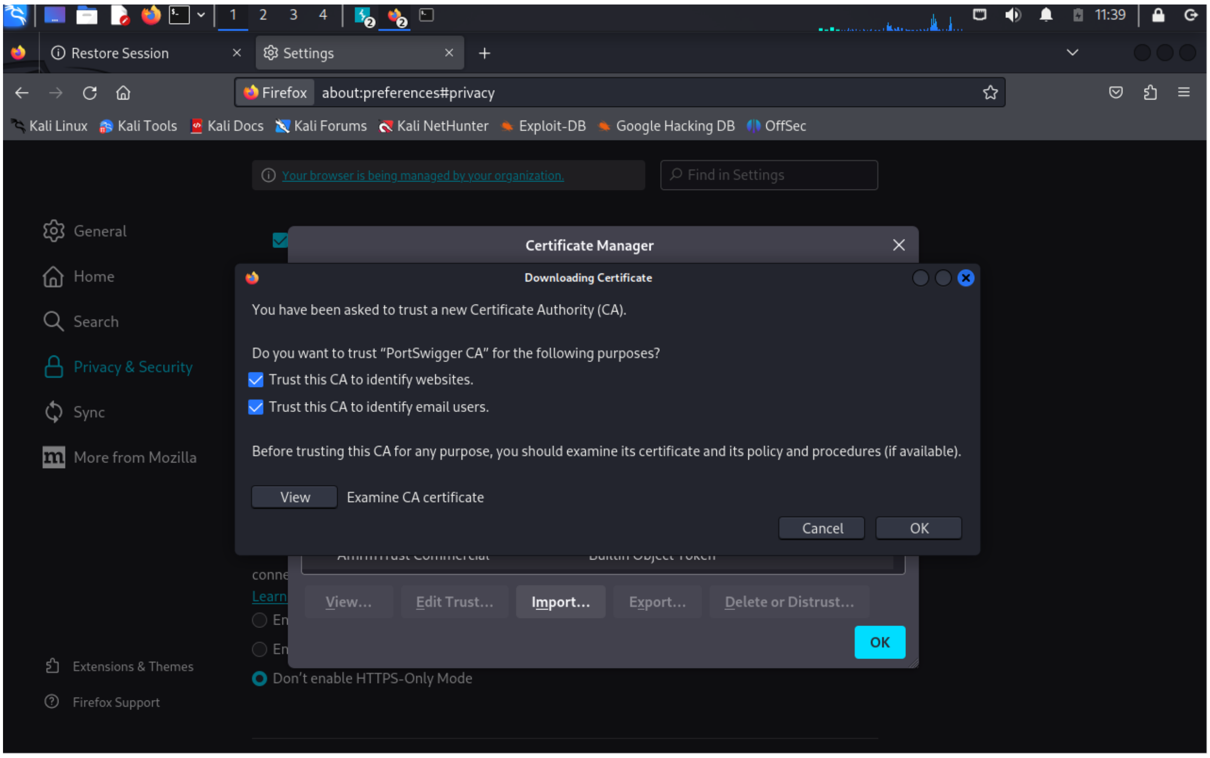
○ SOCKS v4 ● SOCKS v5

○ Automatic proxy configuration URL

Reload

No proxy for

Cancel OK


1 2 3 4
11:39
Restore Session
Settings
Firefox about:preferences#privacy
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Your browser is being managed by your organization.
Find in Settings
General
Home
Search
Privacy & Security
Sync
More from Mozilla
Extensions & Themes
Firefox Support
Certificate Manager
View... Edit Trust... Import... Export... Delete or Distrust...
OK
Don't enable HTTPS-Only Mode

Downloading Certificate

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

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

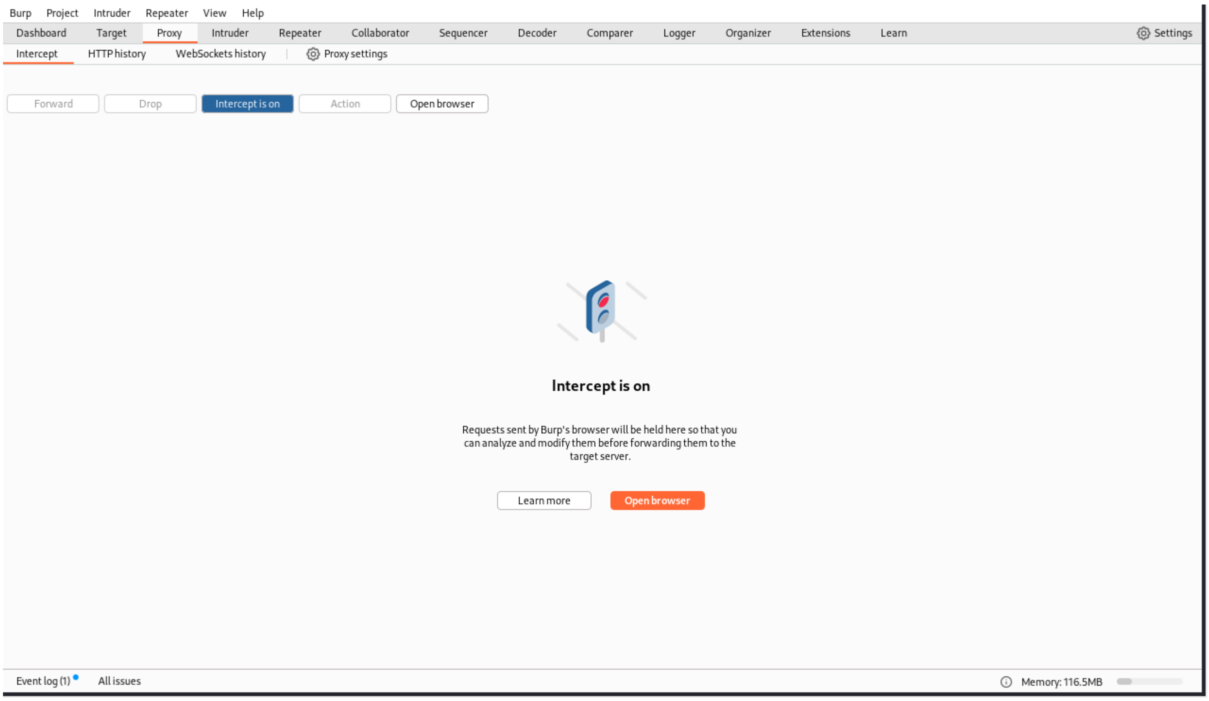
☑ Trust this CA to identify websites.

☑ 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).

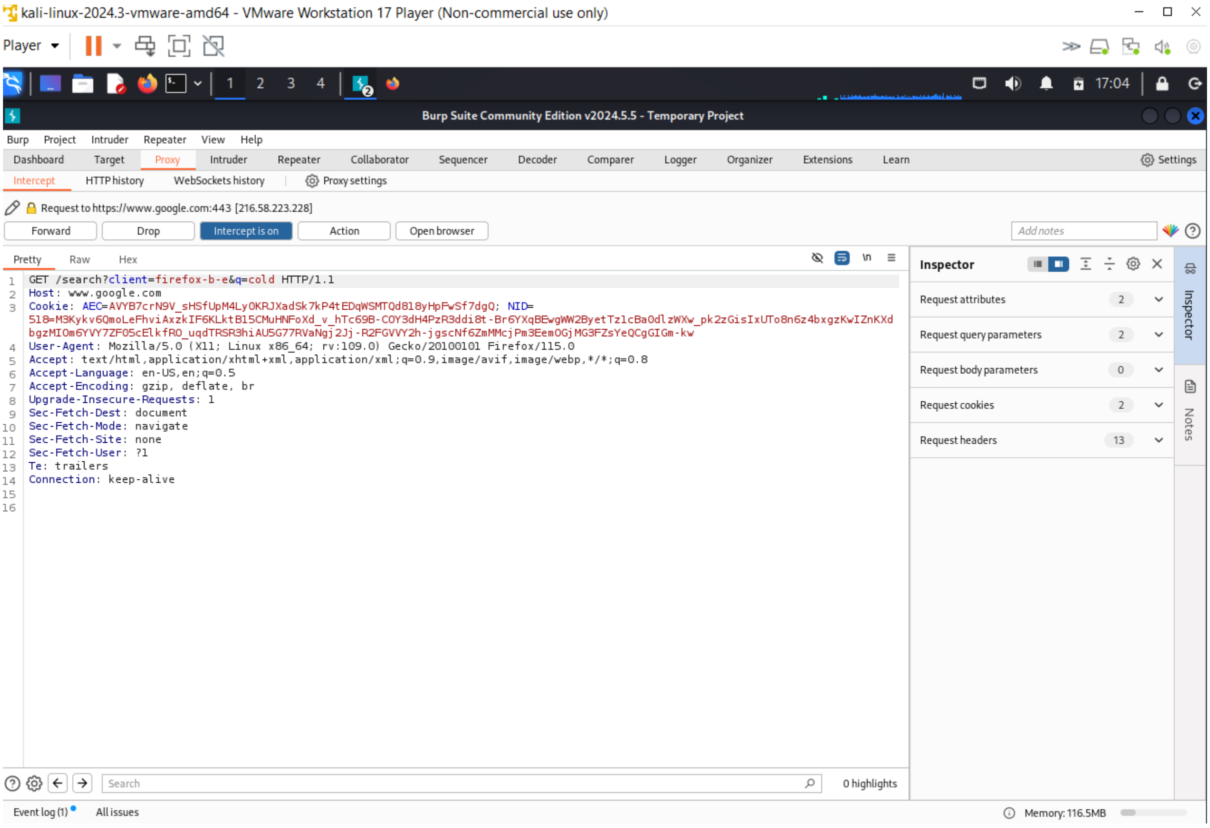
View Examine CA certificate

Cancel OK


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
Learn more
Open browser
Event log (1) All issues
Memory: 116.5MB

Intercept is on

Requests sent by Burp's browser will be held here so that you can analyze and modify them before forwarding them to the target server.


kali-linux-2024.3-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
1 2 3 4
17:04
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
Add notes
Pretty Raw Hex
Inspector
Notes
Search
0 highlights
Event log (1) All issues
Memory: 116.5MB

Request to https://www.google.com:443 [216.58.223.228]

```
GET /search?client=firefox-b-e&q=cold HTTP/1.1
Host: www.google.com
Cookie: AEC=AVYB7crN9V_sHSfUpM4Ly0KRJXadSk7kP4tEDqWSMTQd818yHpFwSf7dgQ; NID=
518=M3Kykv6QmoLeFhviAxzkIF6KLktB15CMuHNFoXd_v_hTc69B-COY3dH4PzR3ddi8t-Br6YXqBEwgWW2ByetTz1cBa0dlzWXw_pk2zGisIxUTo8n6z4bxgzKwIZnKXd
bgzMIOm6YVY7ZF05cElkfRO_uqdTRSR3hiAU5G77RVaNgj2Jj-R2FGVVY2h-jgscNf6ZmMMcjPm3EemOGjMG3FZsYeQCgGIGm-kw
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Te: trailers
Connection: keep-alive
```

Request attributes	2
Request query parameters	2
Request body parameters	0
Request cookies	2
Request headers	13