Ryan Christopher

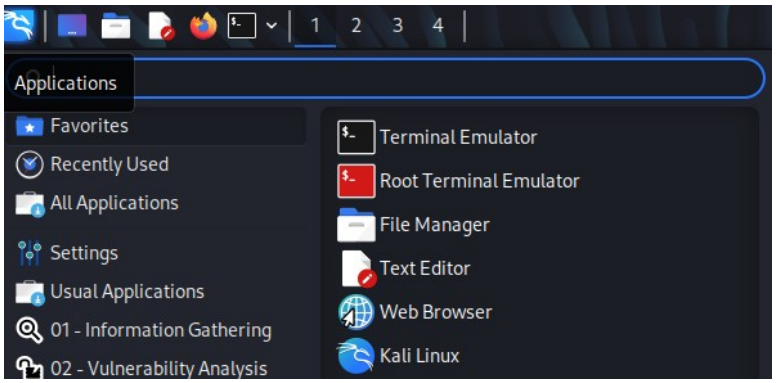
CS695 – Lab 5

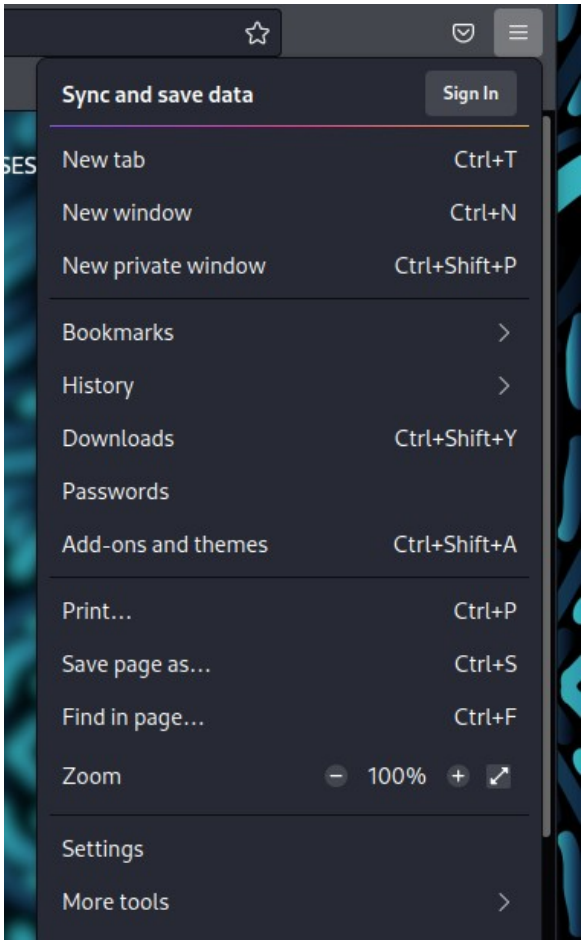
Web Browser Security

Table of Contents:

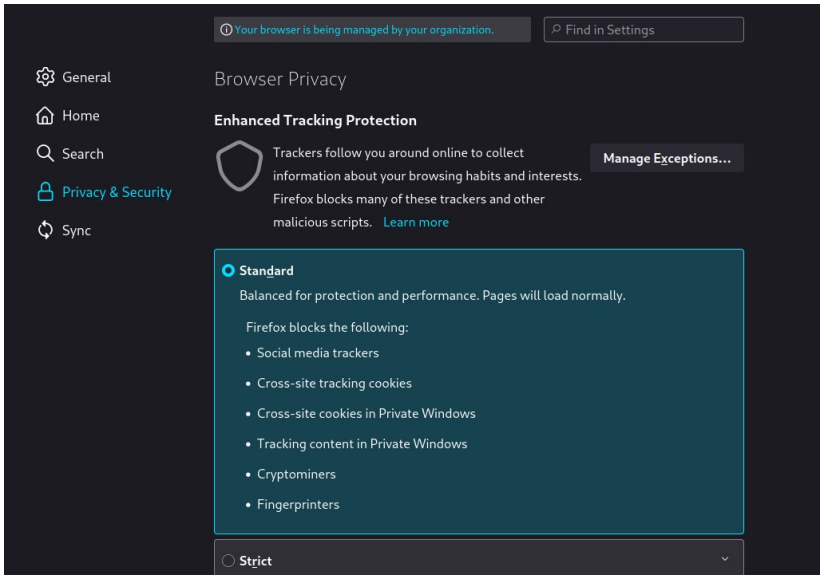
Part 1 – History

1)

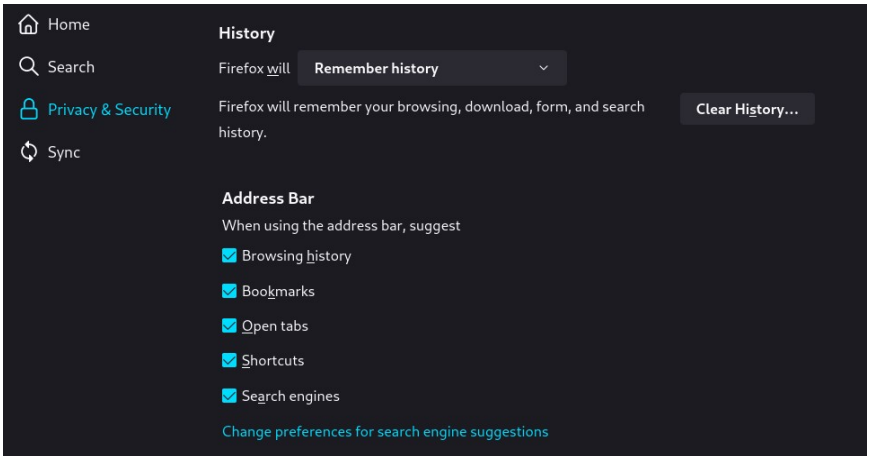




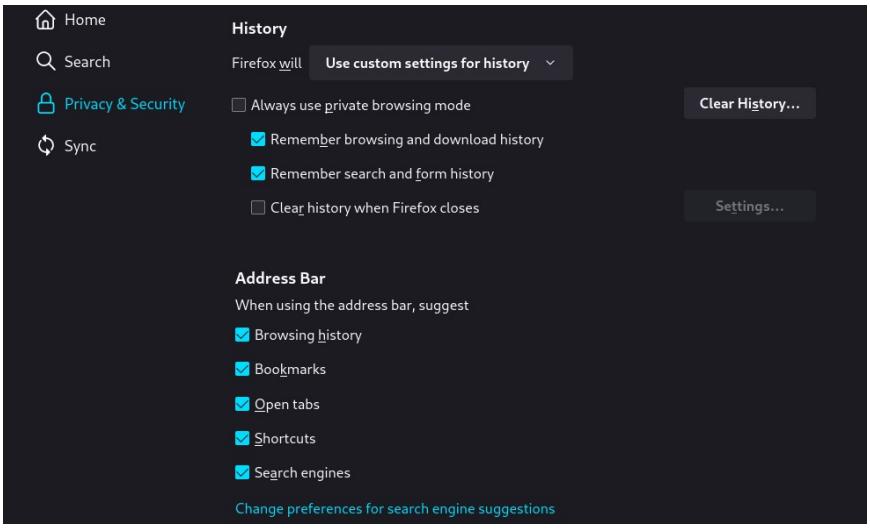
2)


Your browser is being managed by your organization.
Find in Settings
General
Home
Search
Privacy & Security
Sync
Browser Privacy
Enhanced Tracking Protection
Trackers follow you around online to collect information about your browsing habits and interests. Firefox blocks many of these trackers and other malicious scripts. Learn more
Manage Exceptions...
Standard
Balanced for protection and performance. Pages will load normally.
Firefox blocks the following:
Social media trackers
Cross-site tracking cookies
Cross-site cookies in Private Windows
Tracking content in Private Windows
Cryptominers
Fingerprinters
Strict

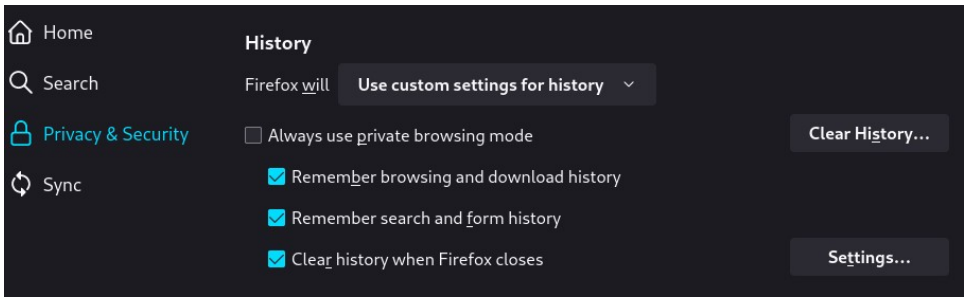
3)

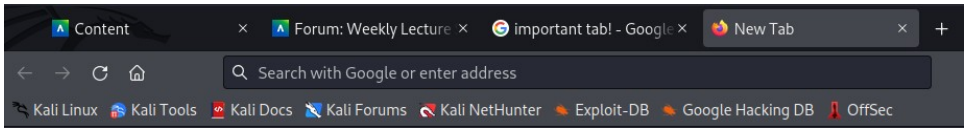

Home
Search
Privacy & Security
Sync
History
Firefox will
Remember history
Firefox will remember your browsing, download, form, and search history.
Clear History...
Address Bar
When using the address bar, suggest
Browsing history
Bookmarks
Open tabs
Shortcuts
Search engines
Change preferences for search engine suggestions

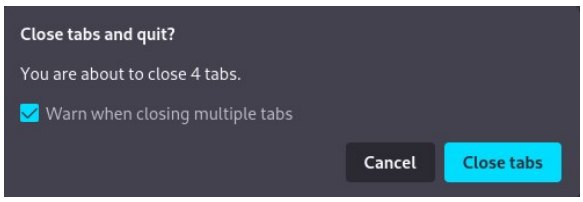
4)

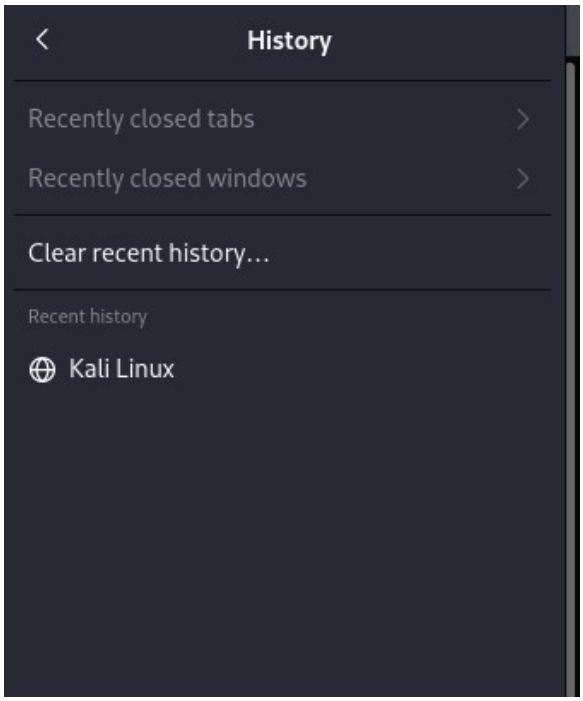

Home
Search
Privacy & Security
Sync
History
Firefox will
Use custom settings for history
Always use private browsing mode
Remember browsing and download history
Remember search and form history
Clear history when Firefox closes
Clear History...
Settings...
Address Bar
When using the address bar, suggest
Browsing history
Bookmarks
Open tabs
Shortcuts
Search engines
Change preferences for search engine suggestions

5)









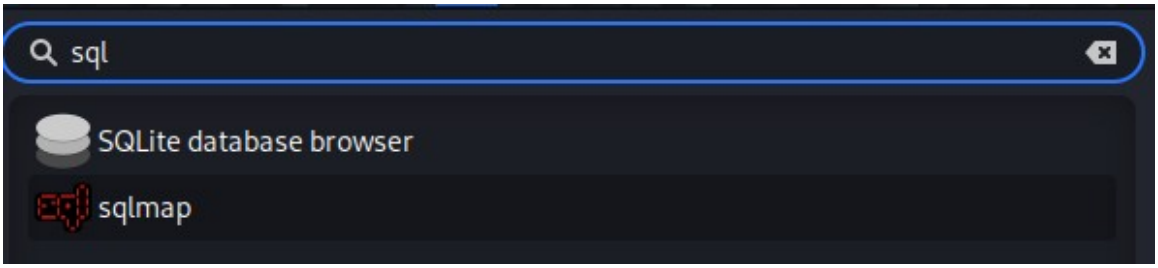
Despite having had four tabs open (3 of which with addresses), when I closed Firefox and reopened it there was no record of them in the history tab. Additionally, when I went to close Firefox, it provided a warning that normally isn't there since the history of the tabs was not going to be kept.

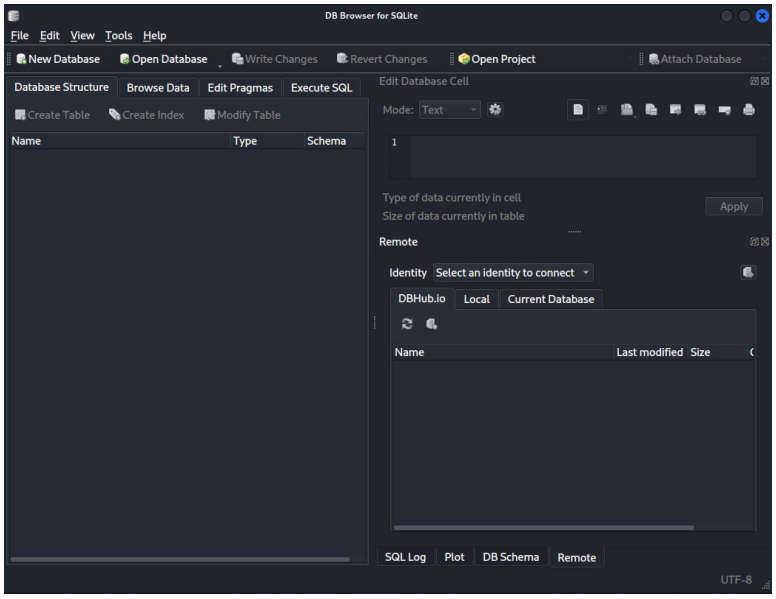
6)

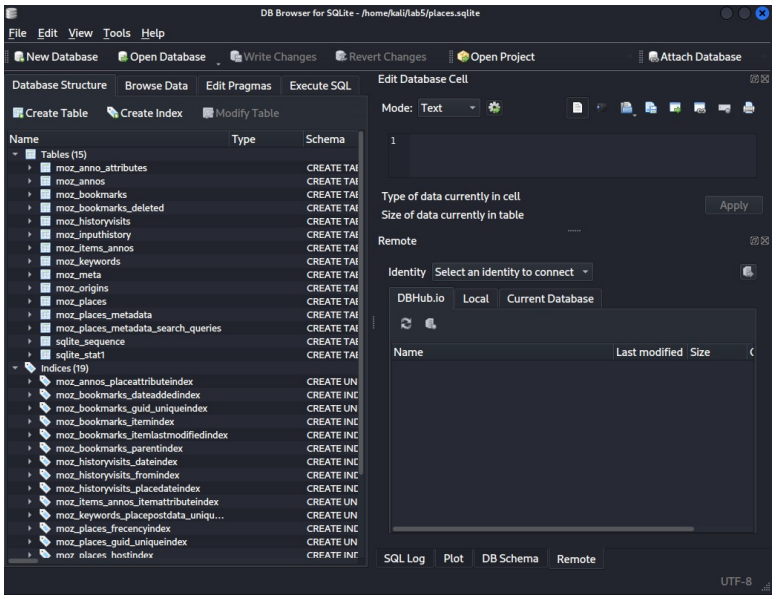
```
┌──(kali㉿kali)-[/home]
└─$ ls ~/.mozilla/firefox/
 1e8yjaop.default       'Crash Reports'  'Pending Pings'
 9s1ft63l.default-esr    installs.ini     profiles.ini

┌──(kali㉿kali)-[/home]
└─$ ls ~/.mozilla/firefox/9s1ft63l.default-esr
addons.json                extension-preferences.json  search.json.mozlz4
addonStartup.json.lz4      extensions.json             security_state
AlternateServices.txt      favicons.sqlite             serviceworker.txt
bookmarkbackups            features                    sessionCheckpoints.json
broadcast-listeners.json   formhistory.sqlite          shield-preference-experiments.json
cert9.db                   handlers.json               SiteSecurityServiceState.txt
cert_override.txt          key4.db                     storage
compatibility.ini          lock                        storage.sqlite
containers.json            minidumps                   times.json
content-prefs.sqlite       permissions.sqlite          weave
cookies.sqlite             pkcs11.txt                  webappsstore.sqlite
crashes                    places.sqlite               xulstore.json
datareporting              prefs.js
enumerate_devices.txt      protections.sqlite
```

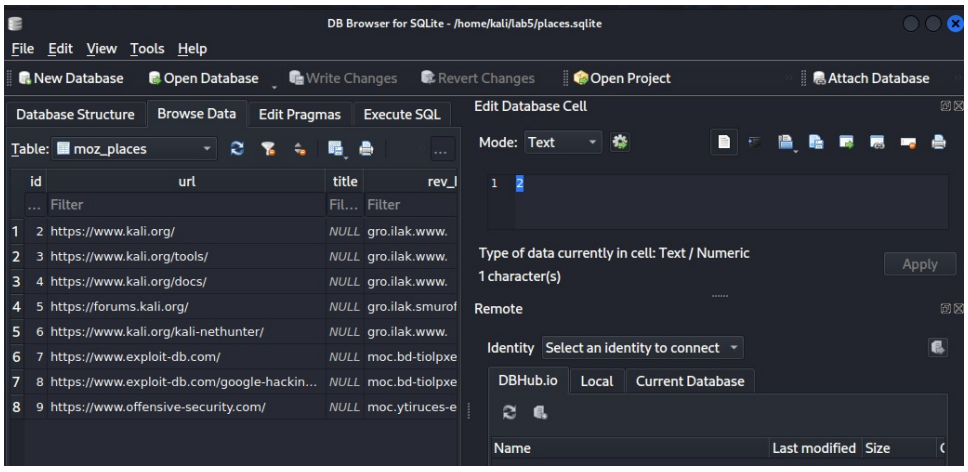
7)

```
┌──(kali㉿kali)-[~]
└─$ mkdir lab5

┌──(kali㉿kali)-[~]
└─$ cp ~/.mozilla/firefox/9s1ft63l.default-esr/places.sqlite ./lab5/

┌──(kali㉿kali)-[~]
└─$ ls lab5/
places.sqlite
```

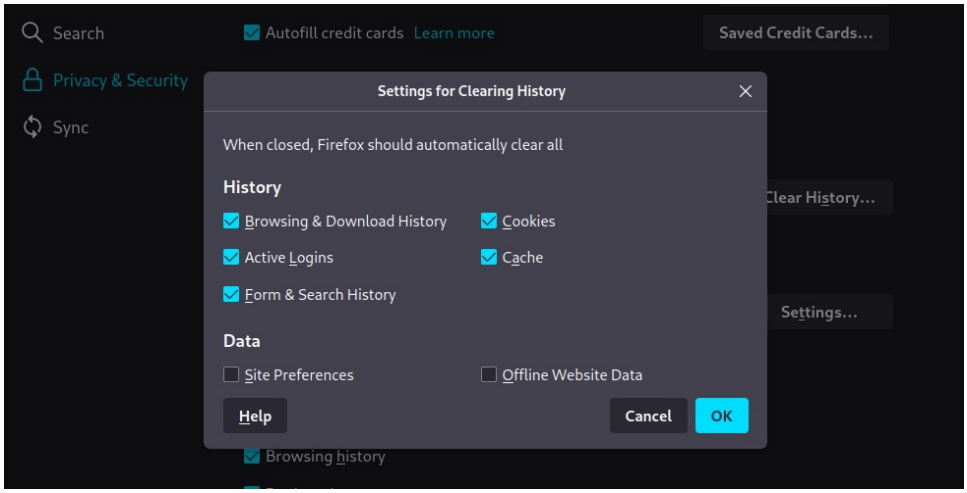



DB Browser for SQLite
File Edit View Tools Help
New Database
Open Database
Write Changes
Revert Changes
Open Project
Attach Database
Database Structure
Browse Data
Edit Pragmas
Execute SQL
Edit Database Cell
Create Table
Create Index
Modify Table
Mode: Text
Name
Type
Schema
Type of data currently in cell
Size of data currently in table
Apply
Remote
Identity
Select an identity to connect
DBHub.io
Local
Current Database
Name
Last modified
Size
SQL Log
Plot
DB Schema
Remote
UTF-8


DB Browser for SQLite - /home/kali/lab5/places.sqlite
File Edit View Tools Help
New Database
Open Database
Write Changes
Revert Changes
Open Project
Attach Database
Database Structure
Browse Data
Edit Pragmas
Execute SQL
Edit Database Cell
Create Table
Create Index
Modify Table
Mode: Text
Name
Type
Schema
Tables (15)
moz_anno_attributes
moz_annos
moz_bookmarks
moz_bookmarks_deleted
moz_historyvisits
moz_inputhistory
moz_items_annos
moz_keywords
moz_meta
moz_origins
moz_places
moz_places_metadata
moz_places_metadata_search_queries
sqlite_sequence
sqlite_stat1
Indices (19)
moz_annos_placeattributeindex
moz_bookmarks_dateaddedindex
moz_bookmarks_guid_uniqueindex
moz_bookmarks_itemindex
moz_bookmarks_itemlastmodifiedindex
moz_bookmarks_parentindex
moz_historyvisits_dateindex
moz_historyvisits_fromindex
moz_historyvisits_placedateindex
moz_items_annos_itemattributeindex
moz_keywords_placepostdata_uniqu...
moz_places_frecencyindex
moz_places_guid_uniqueindex
moz_places_hostindex
Type of data currently in cell
Size of data currently in table
Apply
Remote
Identity
Select an identity to connect
DBHub.io
Local
Current Database
Name
Last modified
Size
SQL Log
Plot
DB Schema
Remote
UTF-8

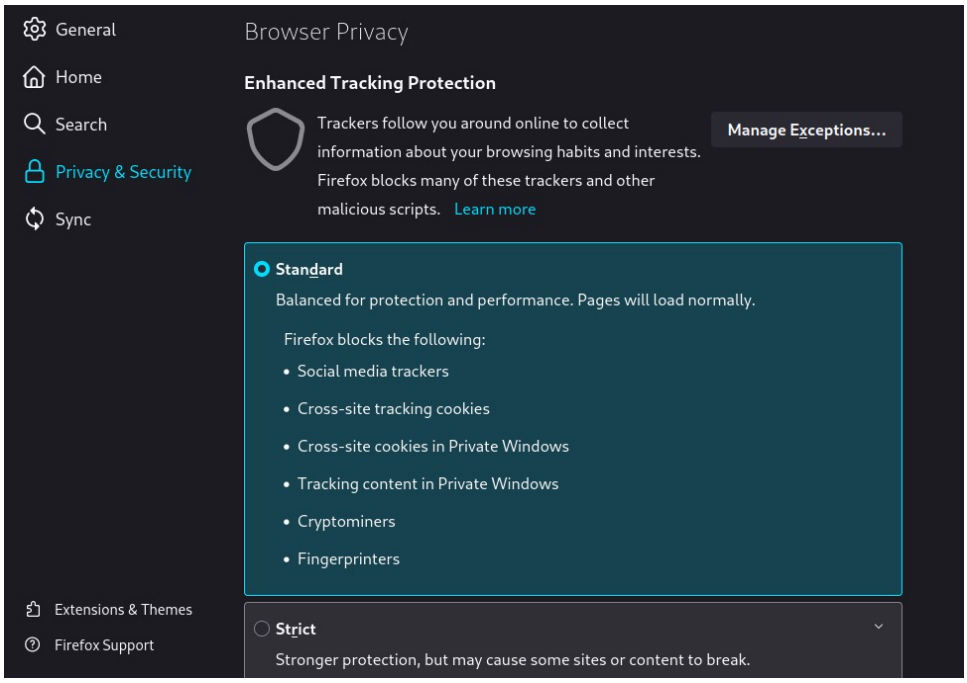

DB Browser for SQLite - /home/kali/lab5/places.sqlite
File Edit View Tools Help
New Database
Open Database
Write Changes
Revert Changes
Open Project
Attach Database
Database Structure
Browse Data
Edit Pragmas
Execute SQL
Edit Database Cell
Table: moz_places
Mode: Text
id
url
title
rev_l
Filter
1 2 https://www.kali.org/ NULL gro.ilak.www.
2 3 https://www.kali.org/tools/ NULL gro.ilak.www.
3 4 https://www.kali.org/docs/ NULL gro.ilak.www.
4 5 https://forums.kali.org/ NULL gro.ilak.smurof
5 6 https://www.kali.org/kali-nethunter/ NULL gro.ilak.www.
6 7 https://www.exploit-db.com/ NULL moc.bd-tiolpxe
7 8 https://www.exploit-db.com/google-hackin... NULL moc.bd-tiolpxe
8 9 https://www.offensive-security.com/ NULL moc.ytiruces-e
Type of data currently in cell: Text / Numeric
1 character(s)
Apply
Remote
Identity
Select an identity to connect
DBHub.io
Local
Current Database
Name
Last modified
Size

8)

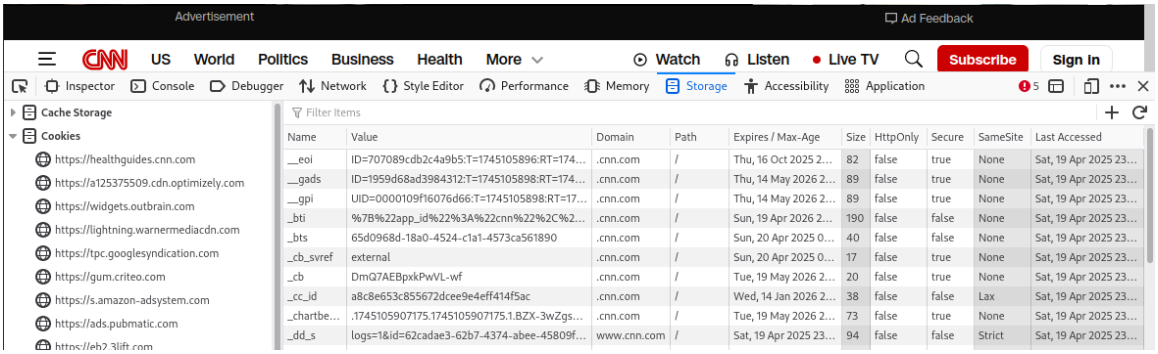

Search
Privacy & Security
Sync
Autofill credit cards Learn more
Saved Credit Cards...
Settings for Clearing History
When closed, Firefox should automatically clear all
History
Browsing & Download History
Cookies
Active Logins
Cache
Form & Search History
Data
Site Preferences
Offline Website Data
Help
Cancel
OK
Clear History...
Settings...
Browsing history

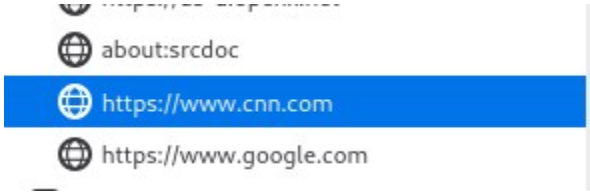
Part 2 – Tracker and Cookies

9)



10)



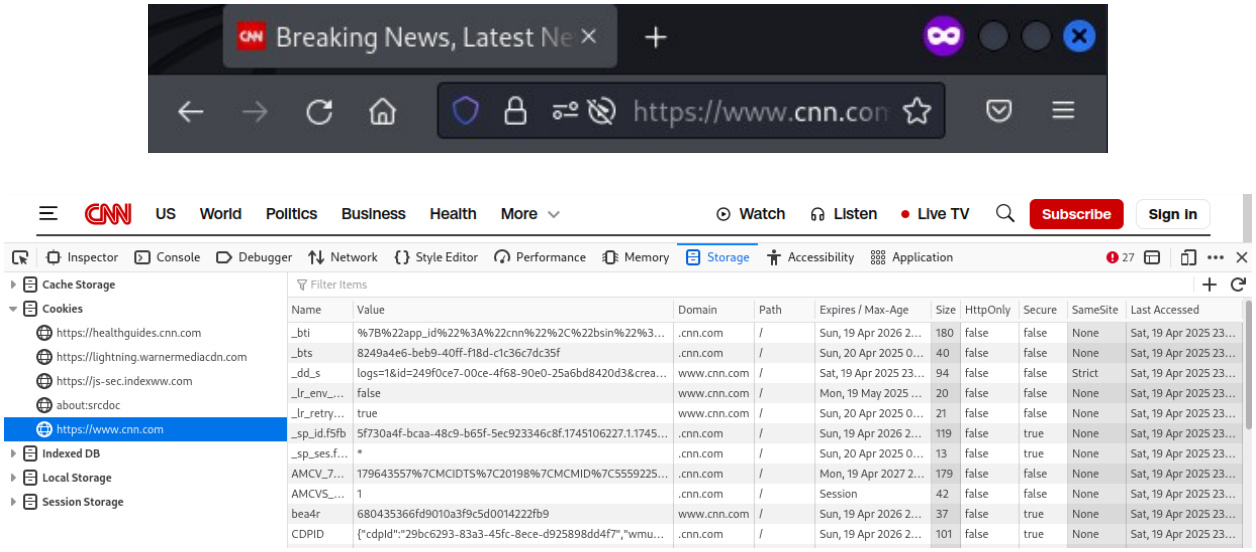


Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
__eoi	ID=707089cdb2c4a9b5:T=...	.cnn.com	/	Thu, 16 Oct 2025 2...	82	false	true	None	Sat, 19 Apr 2025 23...
__gads	ID=1959d68ad3984312:T=...	.cnn.com	/	Thu, 14 May 2026 2...	89	false	true	None	Sat, 19 Apr 2025 23...
__gpi	UID=0000109f16076d66:T...	.cnn.com	/	Thu, 14 May 2026 2...	89	false	true	None	Sat, 19 Apr 2025 23...
_cb_svref	external	.cnn.com	/	Sun, 20 Apr 2025 0...	17	false	true	None	Sat, 19 Apr 2025 23...
_cb	DmQ7AEBpxkPwVL-wf	.cnn.com	/	Tue, 19 May 2026 2...	20	false	true	None	Sat, 19 Apr 2025 23...
_cc_id	a8c8e653c855672dcee9e4...	.cnn.com	/	Wed, 14 Jan 2026 2...	38	false	false	Lax	Sat, 19 Apr 2025 23...
_chartbe...	.1745105907175.17451059...	.cnn.com	/	Tue, 19 May 2026 2...	73	false	true	None	Sat, 19 Apr 2025 23...
_dd_s	logs=1&id=90c77d34-9d53...	www.cnn.com	/	Sat, 19 Apr 2025 23...	94	false	false	Strict	Sat, 19 Apr 2025 23...
_iiq_ab_...	%7B%2295%22%3A%22...	www.cnn.com	/	Session	35	false	false	None	Sat, 19 Apr 2025 23...
_iiq_fdata	%7B%22pcid%22%3A%2...	www.cnn.com	/	Session	224	false	false	None	Sat, 19 Apr 2025 23...
_lr_env_...	false	www.cnn.com	/	Mon, 19 May 2025 ...	20	false	false	None	Sat, 19 Apr 2025 23...
_lr_retry...	true	www.cnn.com	/	Sun, 20 Apr 2025 0...	21	false	false	None	Sat, 19 Apr 2025 23...
pubcid...	zix7LPQsHA%3D%3D	.cnn.com	/	Thu, 16 Oct 2025 2...	27	false	false	Lax	Sat, 19 Apr 2025 23...
_pubcid	a1cb4fbc-cc99-41d1-972c-...	.cnn.com	/	Thu, 16 Oct 2025 2...	43	false	false	Lax	Sat, 19 Apr 2025 23...
_scor_uid	5a32d2618e6f4aa5960c74...	.cnn.com	/	Thu, 14 May 2026 2...	41	false	true	None	Sat, 19 Apr 2025 23...
_sp_id.f5fb	2d73a93e-9909-4237-a51...	.cnn.com	/	Sun, 19 Apr 2026 2...	119	false	true	None	Sat, 19 Apr 2025 23...
_sp_ses.f...	*	.cnn.com	/	Sun, 20 Apr 2025 0...	13	false	true	None	Sat, 19 Apr 2025 23...

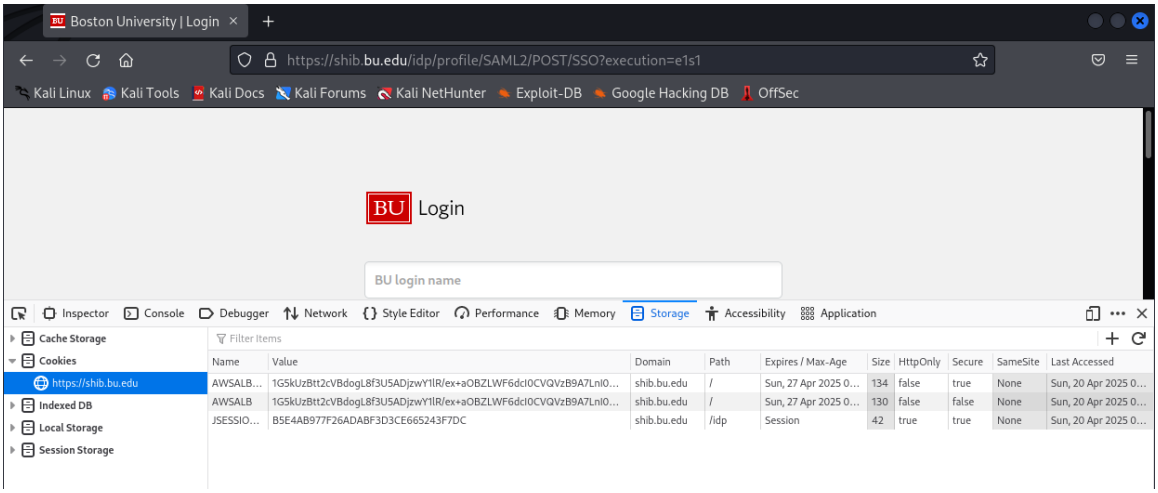
https://ssum-sec.casalemedia.com
https://sdk.openwebmp.com
https://prebid.a-mo.net

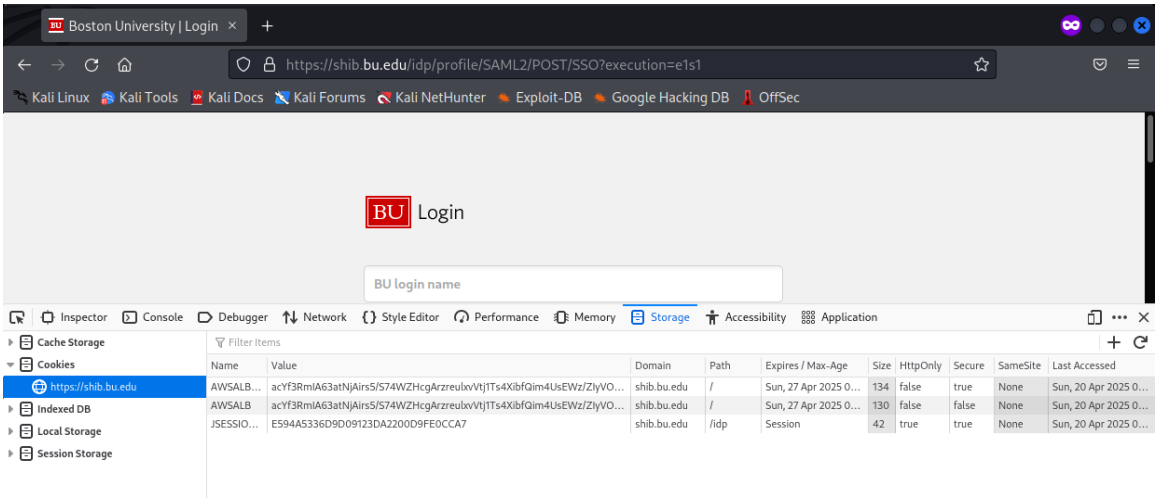
https://a12537550 9.cdn.optimizely.com
https://widgets.outbrain.com
https://lightning.warnermediacdn.com
https://tpc.googlesyndication.com
https://gum.criteo.com
https://s.amazon-adsystem.com
https://ads.pubmatic.com
https://eb2.3lift.com
https://contextual.media.net
https://eus.rubiconproject.com
https://js-sec.indexww.com
https://ssum-sec.casalemedia.com
https://sdk.openwebmp.com
https://prebid.a-mo.net
https://us-u.openx.net
about:srcdoc
https://www.cnn.com

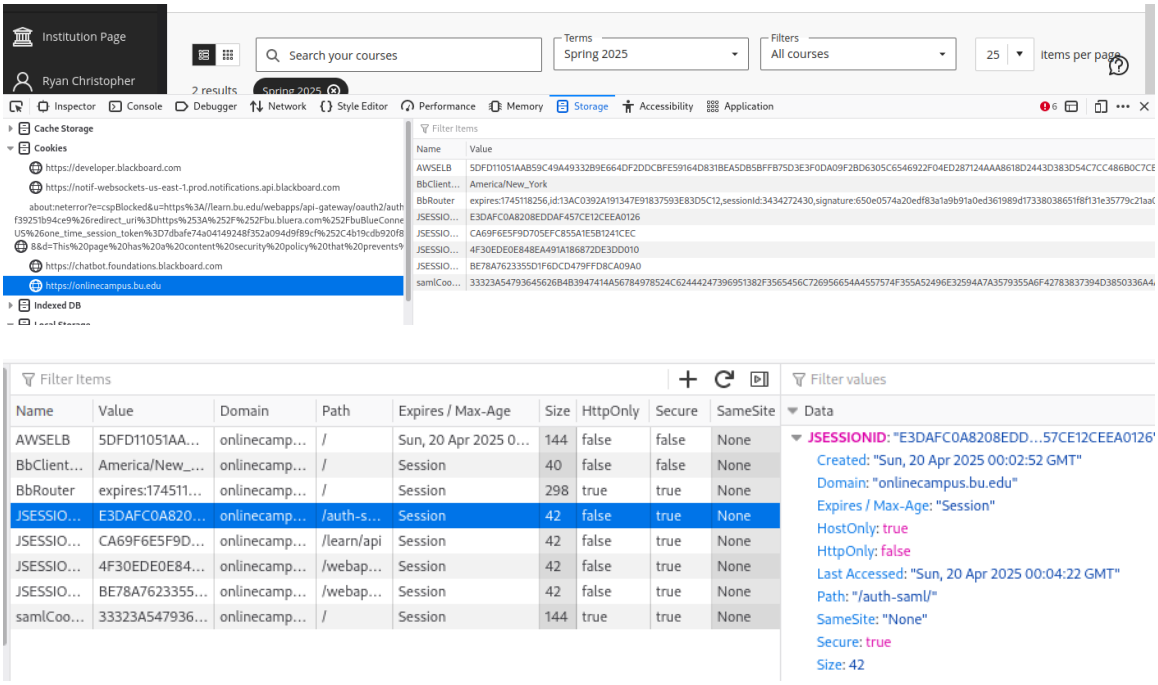
11)


Breaking News, Latest Ne
https://www.cnn.com
CNN
US
World
Politics
Business
Health
More
Watch
Listen
Live TV
Subscribe
Sign In
Inspector
Console
Debugger
Network
Style Editor
Performance
Memory
Storage
Accessibility
Application
Cache Storage
Cookies
https://healthguides.cnn.com
https://lightning.warnermediacdn.com
https://js-sec.indexww.com
about:srcdoc
https://www.cnn.com
Indexed DB
Local Storage
Session Storage
Filter Items
Name | Value | Domain | Path | Expires / Max-Age | Size | HttpOnly | Secure | SameSite | Last Accessed
_bti | %7B%22app_id%22%3A%22cnn%22%2C%22bsin%22%3... | .cnn.com | / | Sun, 19 Apr 2026 2... | 180 | false | false | None | Sat, 19 Apr 2025 23...
_bts | 8249a4e6-beb9-40ff-f18d-c1c36c7dc35f | .cnn.com | / | Sun, 20 Apr 2025 0... | 40 | false | false | None | Sat, 19 Apr 2025 23...
_dd_s | logs=1&id=249f0ce7-00ce-4f68-90e0-25a6bd8420d3&crea... | www.cnn.com | / | Sat, 19 Apr 2025 23... | 94 | false | false | Strict | Sat, 19 Apr 2025 23...
_lr_env_... | false | www.cnn.com | / | Mon, 19 May 2025 ... | 20 | false | false | None | Sat, 19 Apr 2025 23...
_lr_retry... | true | www.cnn.com | / | Sun, 20 Apr 2025 0... | 21 | false | false | None | Sat, 19 Apr 2025 23...
_sp_id.f5fb | 5f730a4f-bcaa-48c9-b65f-5ec923346c8f.1745106227.1.1745... | .cnn.com | / | Sun, 19 Apr 2026 2... | 119 | false | true | None | Sat, 19 Apr 2025 23...
_sp_ses.f... | * | .cnn.com | / | Sun, 20 Apr 2025 0... | 13 | false | true | None | Sat, 19 Apr 2025 23...
AMCV_7... | 1796435557%7CMCIDTS%7C20198%7CMCMID%7C5559225... | .cnn.com | / | Mon, 19 Apr 2027 2... | 179 | false | false | None | Sat, 19 Apr 2025 23...
AMCVS_... | 1 | .cnn.com | / | Session | 42 | false | false | None | Sat, 19 Apr 2025 23...
bea4r | 680435366fd9010a3f9c5d0014222fb9 | www.cnn.com | / | Sun, 19 Apr 2026 2... | 37 | false | true | None | Sat, 19 Apr 2025 23...
CDPID | {"cdpId":"29bc6293-83a3-45fc-8ece-d925898dd4f7","wmu... | .cnn.com | / | Sun, 19 Apr 2026 2... | 101 | false | true | None | Sat, 19 Apr 2025 23...

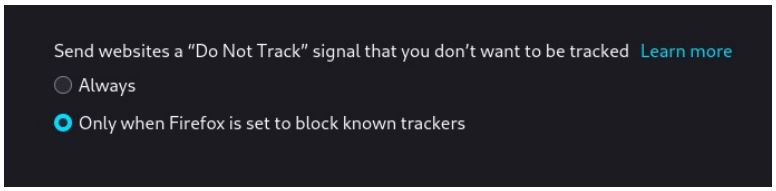
12)

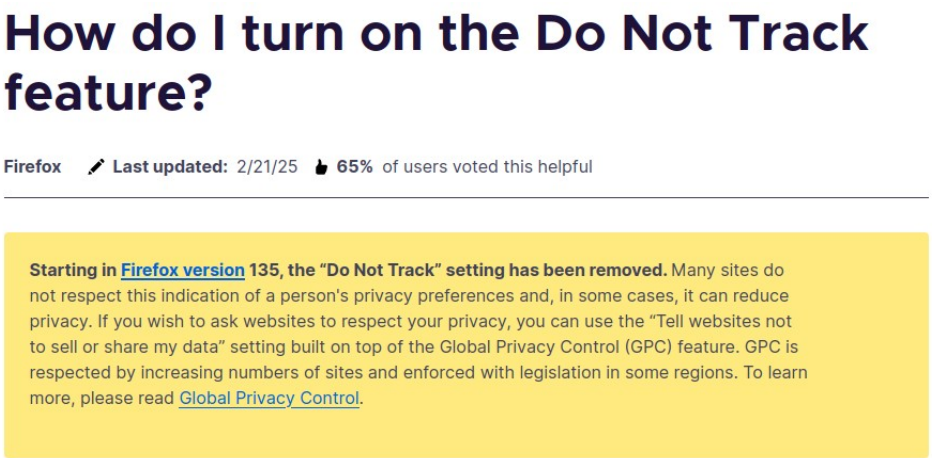

Boston University | Login
https://shib.bu.edu/idp/profile/SAML2/POST/SSO?execution=e1s1
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
BU Login
BU login name
Inspector
Console
Debugger
Network
Style Editor
Performance
Memory
Storage
Accessibility
Application
Cache Storage
Cookies
https://shib.bu.edu
Indexed DB
Local Storage
Session Storage
Filter Items
Name | Value | Domain | Path | Expires / Max-Age | Size | HttpOnly | Secure | SameSite | Last Accessed
AWSALB... | 1G5kUzBtt2cVBdogL8f3U5ADjzwY1lR/ex+aOBZLWF6dcI0CVQVzB9A7LnI0... | shib.bu.edu | / | Sun, 27 Apr 2025 0... | 134 | false | true | None | Sun, 20 Apr 2025 0...
AWSALB | 1G5kUzBtt2cVBdogL8f3U5ADjzwY1lR/ex+aOBZLWF6dcI0CVQVzB9A7LnI0... | shib.bu.edu | / | Sun, 27 Apr 2025 0... | 130 | false | false | None | Sun, 20 Apr 2025 0...
JSESSIO... | B5E4AB977F26ADABF3D3CE665243F7DC | shib.bu.edu | /idp | Session | 42 | true | true | None | Sun, 20 Apr 2025 0...


Boston University | Login
https://shib.bu.edu/idp/profile/SAML2/POST/SSO?execution=e1s1
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
BU Login
BU login name
Inspector
Console
Debugger
Network
Style Editor
Performance
Memory
Storage
Accessibility
Application
Cache Storage
Cookies
https://shib.bu.edu
Indexed DB
Local Storage
Session Storage
Filter Items
Name | Value | Domain | Path | Expires / Max-Age | Size | HttpOnly | Secure | SameSite | Last Accessed
AWSALB... | acYf3RmIA63atNjAirs5/S74WZHcgArzreulxvVtj1Ts4XibfQim4UsEWz/ZIyVO... | shib.bu.edu | / | Sun, 27 Apr 2025 0... | 134 | false | true | None | Sun, 20 Apr 2025 0...
AWSALB | acYf3RmIA63atNjAirs5/S74WZHcgArzreulxvVtj1Ts4XibfQim4UsEWz/ZIyVO... | shib.bu.edu | / | Sun, 27 Apr 2025 0... | 130 | false | false | None | Sun, 20 Apr 2025 0...
JSESSIO... | E594A5336D9D09123DA2200D9FE0CCA7 | shib.bu.edu | /idp | Session | 42 | true | true | None | Sun, 20 Apr 2025 0...



13)



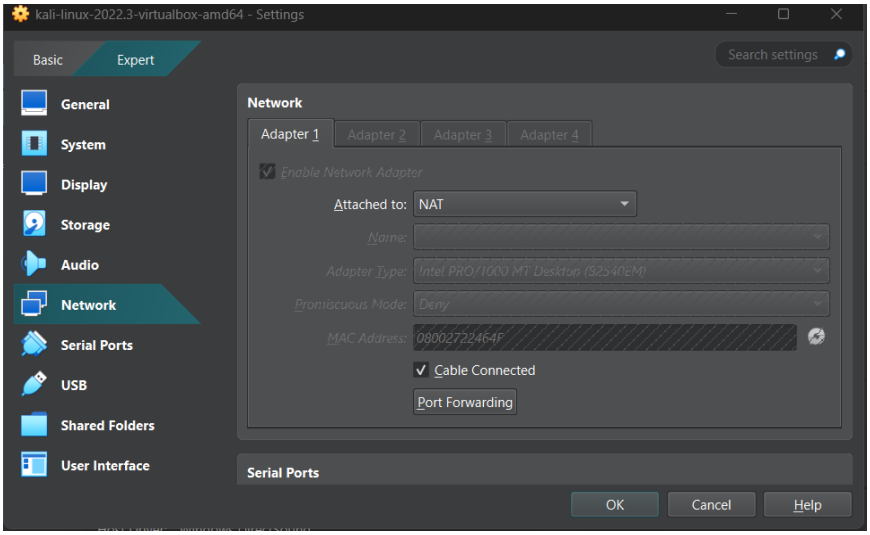


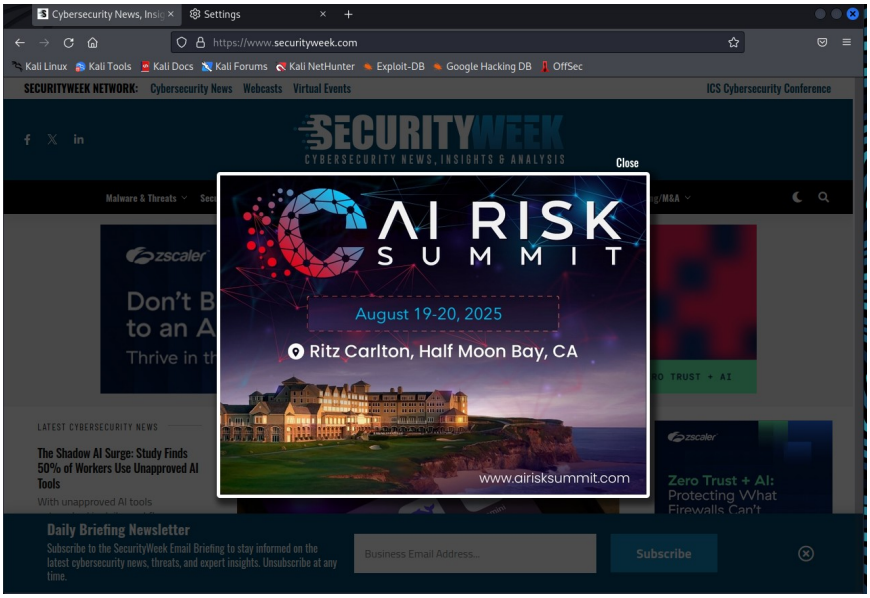
Interestingly, after clicking on the "learn more" link, Mozilla included a disclaimer that the "Do Not Track" setting will be removed starting in Firefox version 135.

Part 3 – Firefox Privacy Add-ons

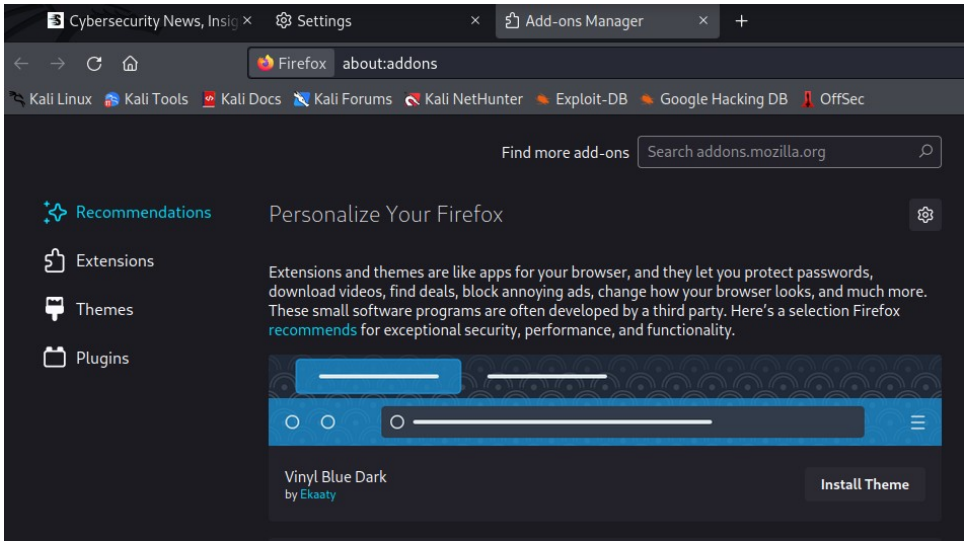
14)

Initially, the page would not load and I would get stuck on a cloudflare “verifying you are a human” page that would freeze. I tried changing the network from bridged connection to NAT, and that seemed to fix the issue.



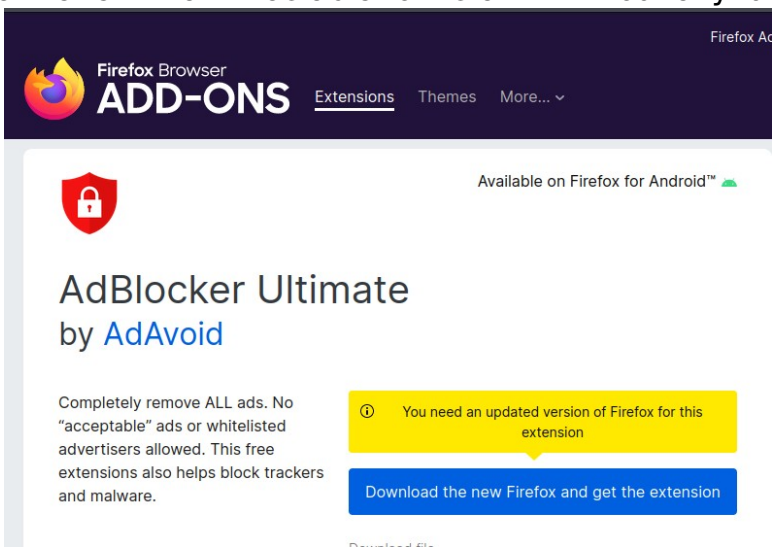


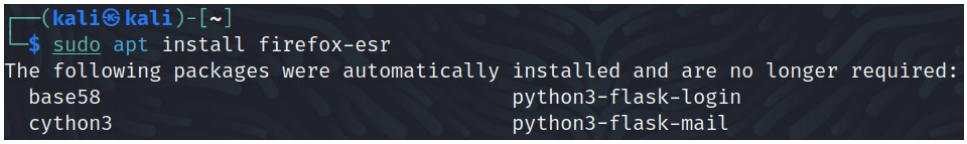
15)

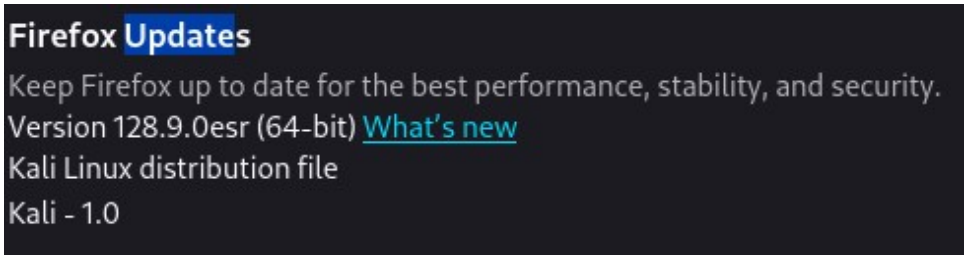


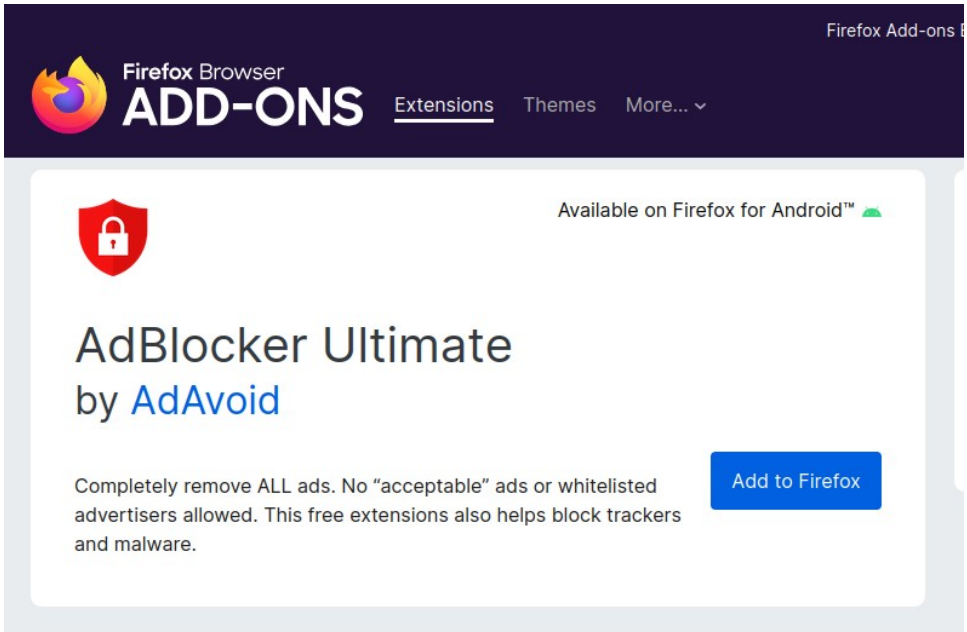
16)

I could not install AdBlocker Ultimate at first due to Firefox being out of date, however after updating it via the terminal I was able to install it without any further issues.

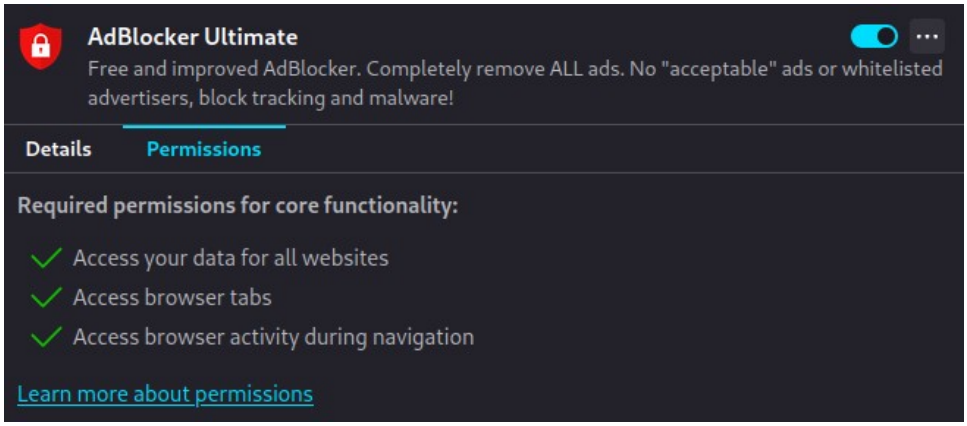








17)

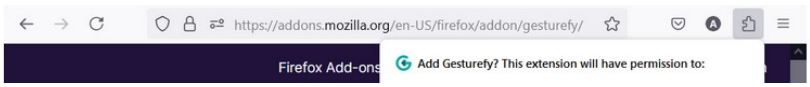


Home / Firefox / Add-ons, extensions, and themes / Permission request messages for...

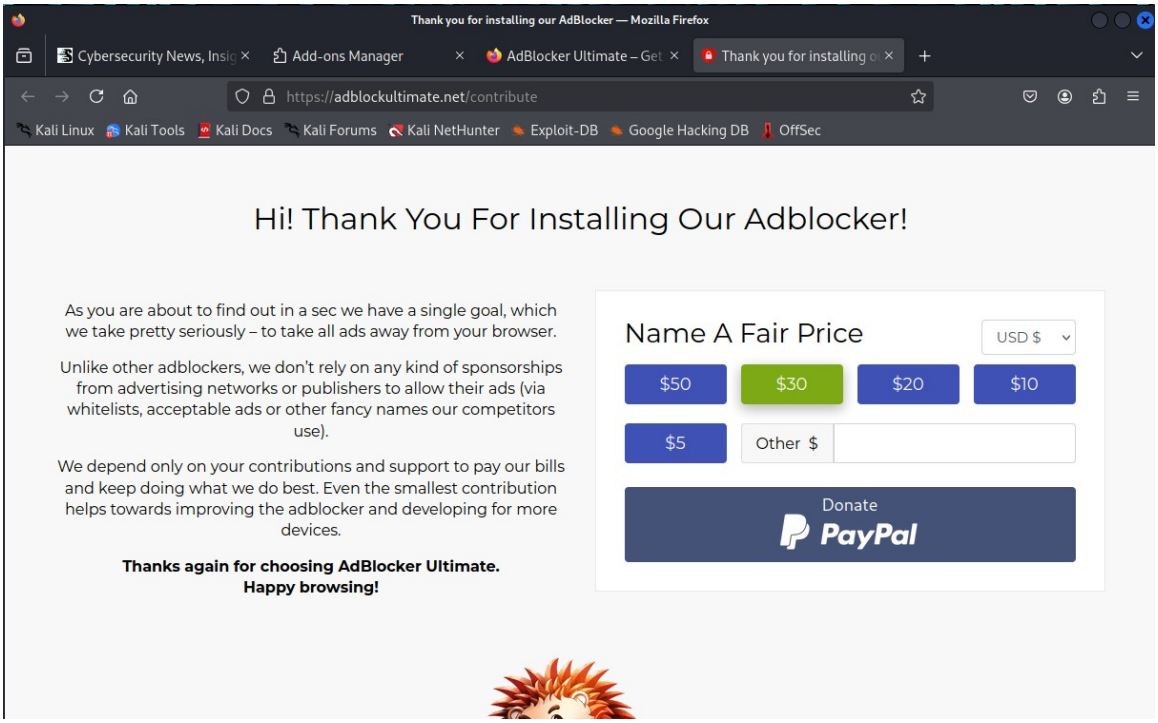
Permission request messages for Firefox extensions

Firefox **Last updated:** 10/24/24 **64%** of users voted this helpful

When you install an extension into Firefox, you may be presented with a message similar to this one:



18)


Thank you for installing our AdBlocker — Mozilla Firefox
Cybersecurity News, Insic
Add-ons Manager
AdBlocker Ultimate – Get
Thank you for installing o
https://adblockultimate.net/contribute
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Hi! Thank You For Installing Our Adblocker!
As you are about to find out in a sec we have a single goal, which we take pretty seriously – to take all ads away from your browser.
Unlike other adblockers, we don't rely on any kind of sponsorships from advertising networks or publishers to allow their ads (via whitelists, acceptable ads or other fancy names our competitors use).
We depend only on your contributions and support to pay our bills and keep doing what we do best. Even the smallest contribution helps towards improving the adblocker and developing for more devices.
Thanks again for choosing AdBlocker Ultimate.
Happy browsing!
Name A Fair Price
USD $
$50
$30
$20
$10
$5
Other $
Donate
PayPal

19)


SECURITYWEEK NETWORK:
Cybersecurity News
Webcasts
Virtual Events
ICS Cybersecurity Conference
SECURITYWEEK
CYBERSECURITY NEWS, INSIGHTS & ANALYSIS
Malware & Threats
Security Operations
Security Architecture
Risk Management
CISO Strategy
ICS/OT
Funding/M&A
LATEST CYBERSECURITY NEWS
The Shadow AI Surge: Study Finds 50% of Workers Use Unapproved AI Tools
With unapproved AI tools entrenched in daily workflows, experts say it's time to shift from monitoring to managing Shadow AI use across the enterprise.
In Other News: 4chan Hacked, Android Auto-Reboot, Nemesis Admin Charged
Noteworthy stories that might have slipped under the radar: 4chan hacked, auto-reboot security feature coming to
The Shadow AI Surge: Study Finds 50% of Workers Use Unapproved AI Tools
With unapproved AI tools entrenched in daily workflows, experts say it's time to shift from monitoring to managing Shadow AI use across the enterprise.
TRENDING
1 In Other News: 4chan Hacked, Android Auto-Reboot, Nemesis Admin Charged
2 Fresh Windows NTLM Vulnerability Exploited in Attacks
3 MITRE Warns CVE Program Faces Disruption Amid US Funding Uncertainty
4 The Shadow AI Surge: Study Finds 50% of

Part 4 – Security

20)

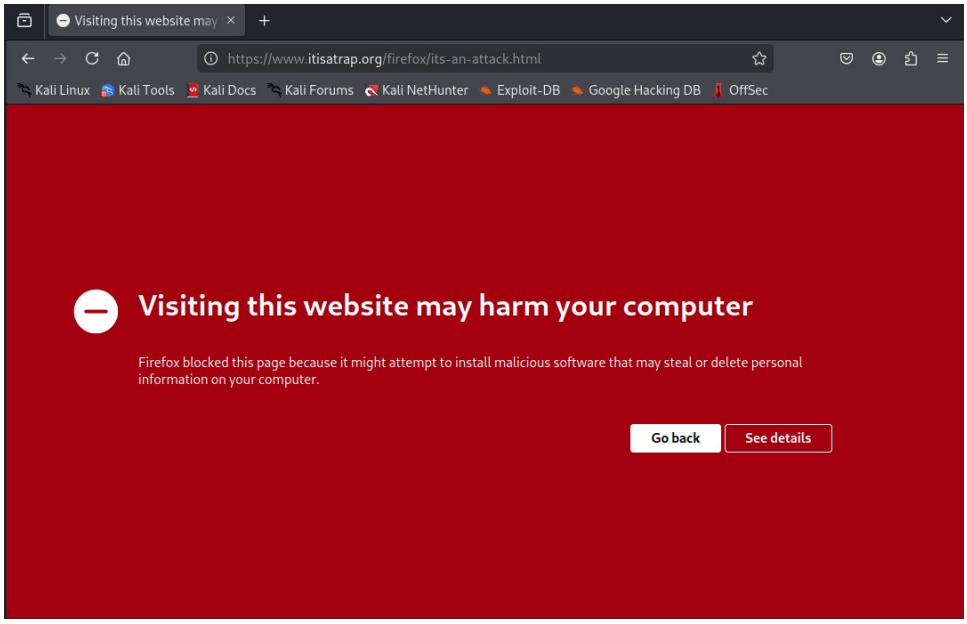
How does built-in Phishing and Malware Protection work?

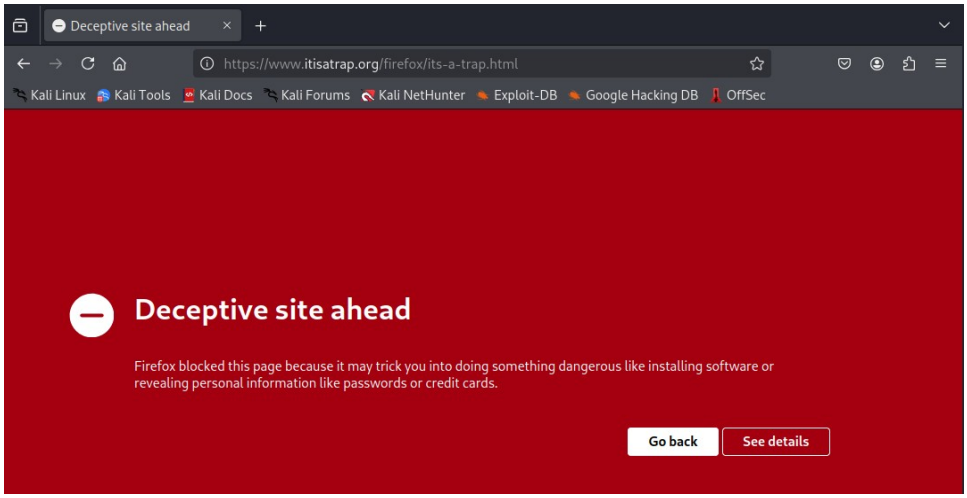
Firefox **Last updated:** 1/12/24 **68%** of users voted this helpful

Firefox contains built-in Phishing and Malware Protection to help keep you safe online. These features will warn you when a page you visit has been reported as a deceptive site (sometimes called "phishing" pages), as a source of unwanted software or as an attack site designed to harm your computer. This feature also warns you if you download files that are detected as malware.

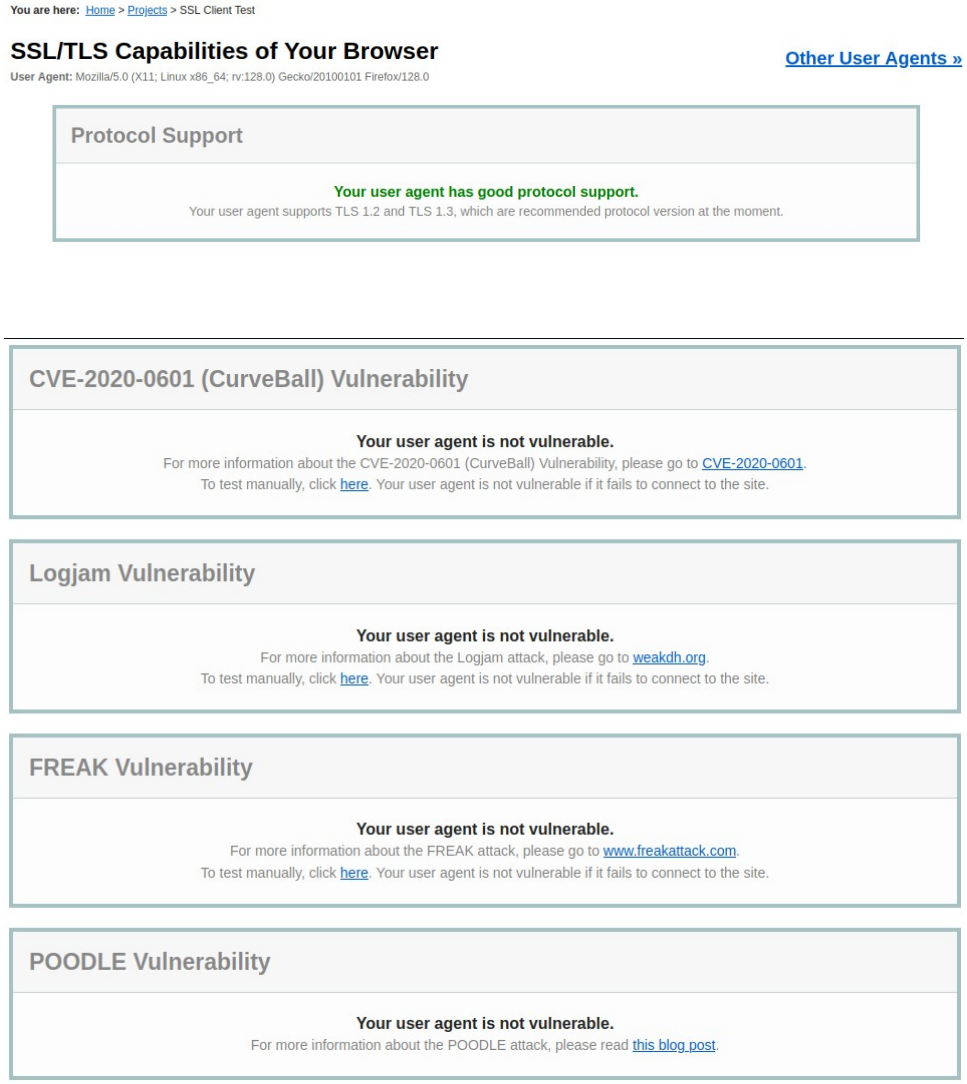
Table of Contents

21)

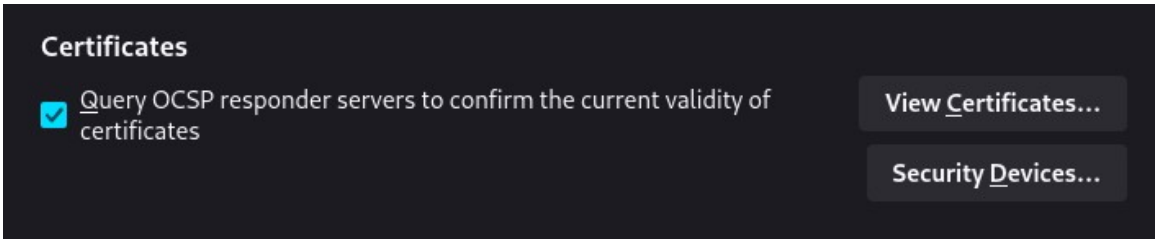



Deceptive site ahead
https://www.itisatrap.org/firefox/its-a-trap.html
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Deceptive site ahead
Firefox blocked this page because it may trick you into doing something dangerous like installing software or revealing personal information like passwords or credit cards.
Go back
See details

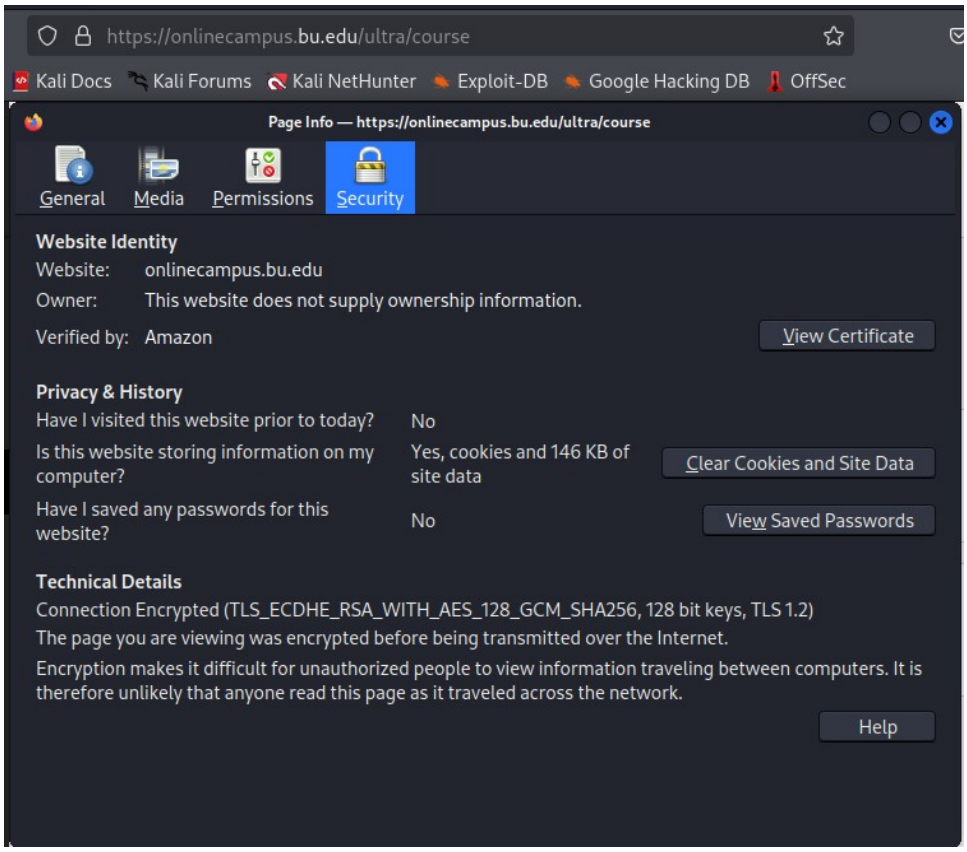
22)


You are here: Home > Projects > SSL Client Test
SSL/TLS Capabilities of Your Browser
User Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Other User Agents »
Protocol Support
Your user agent has good protocol support.
Your user agent supports TLS 1.2 and TLS 1.3, which are recommended protocol version at the moment.
CVE-2020-0601 (CurveBall) Vulnerability
Your user agent is not vulnerable.
For more information about the CVE-2020-0601 (CurveBall) Vulnerability, please go to CVE-2020-0601.
To test manually, click here. Your user agent is not vulnerable if it fails to connect to the site.
Logjam Vulnerability
Your user agent is not vulnerable.
For more information about the Logjam attack, please go to weakdh.org.
To test manually, click here. Your user agent is not vulnerable if it fails to connect to the site.
FREAK Vulnerability
Your user agent is not vulnerable.
For more information about the FREAK attack, please go to www.freakattack.com.
To test manually, click here. Your user agent is not vulnerable if it fails to connect to the site.
POODLE Vulnerability
Your user agent is not vulnerable.
For more information about the POODLE attack, please read this blog post.

23)


Certificates
Query OCSP responder servers to confirm the current validity of certificates
View Certificates...
Security Devices...

24)


https://onlinecampus.bu.edu/ultra/course
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Page Info — https://onlinecampus.bu.edu/ultra/course
General
Media
Permissions
Security
Website Identity
Website: onlinecampus.bu.edu
Owner: This website does not supply ownership information.
Verified by: Amazon
View Certificate
Privacy & History
Have I visited this website prior to today? No
Is this website storing information on my computer? Yes, cookies and 146 KB of site data
Clear Cookies and Site Data
Have I saved any passwords for this website? No
View Saved Passwords
Technical Details
Connection Encrypted (TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, 128 bit keys, TLS 1.2)
The page you are viewing was encrypted before being transmitted over the Internet.
Encryption makes it difficult for unauthorized people to view information traveling between computers. It is therefore unlikely that anyone read this page as it traveled across the network.
Help

Certificate

learn.bu.edu | Amazon RSA 2048 M03 | Amazon Root CA 1

Subject Name

Common Name	learn.bu.edu

Issuer Name

Country	US
Organization	Amazon
Common Name	Amazon RSA 2048 M03

Validity

Not Before	Fri, 02 Aug 2024 00:00:00 GMT
Not After	Sat, 30 Aug 2025 23:59:59 GMT

Subject Alt Names

DNS Name	learn.bu.edu
DNS Name	lms.bu.edu
DNS Name	*.blackboard.com
DNS Name	spb-pbx.bu.edu

Public Key Info

Algorithm	RSA
Key Size	2048
Exponent	65537
Modulus	E4:A3:51:C2:60:BB:F0:98:BC:6D:FE:7D:8A:92:1F:8E:B6:B7:E3:0B:60:7B:7E:5...

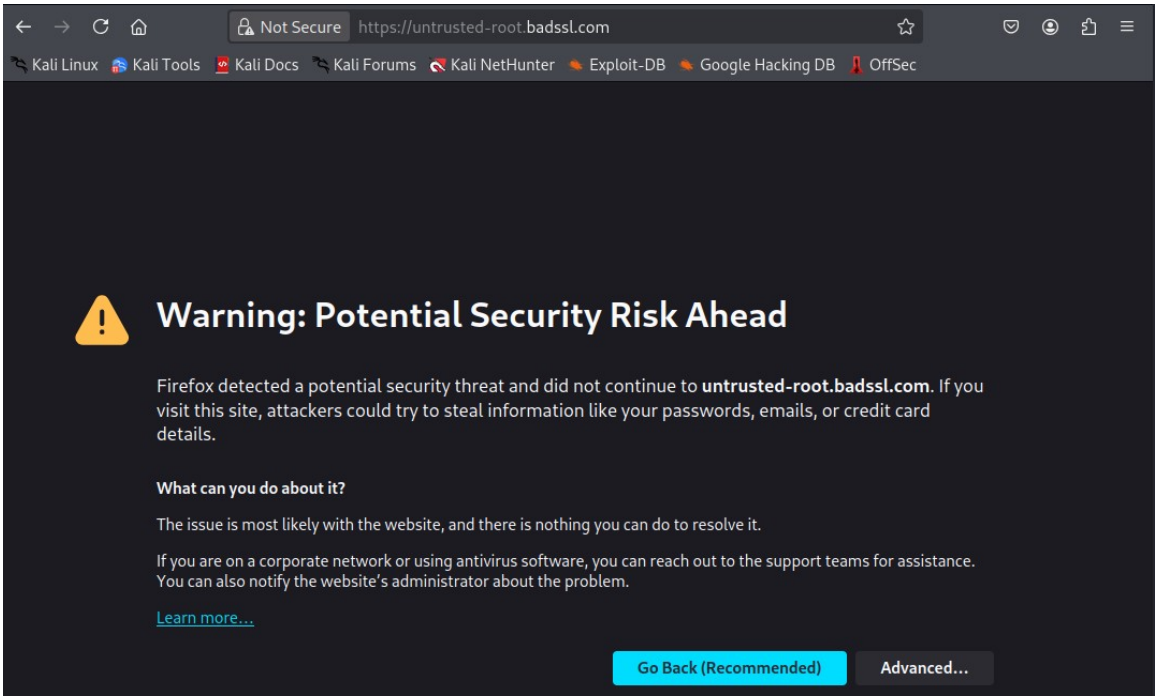
Miscellaneous

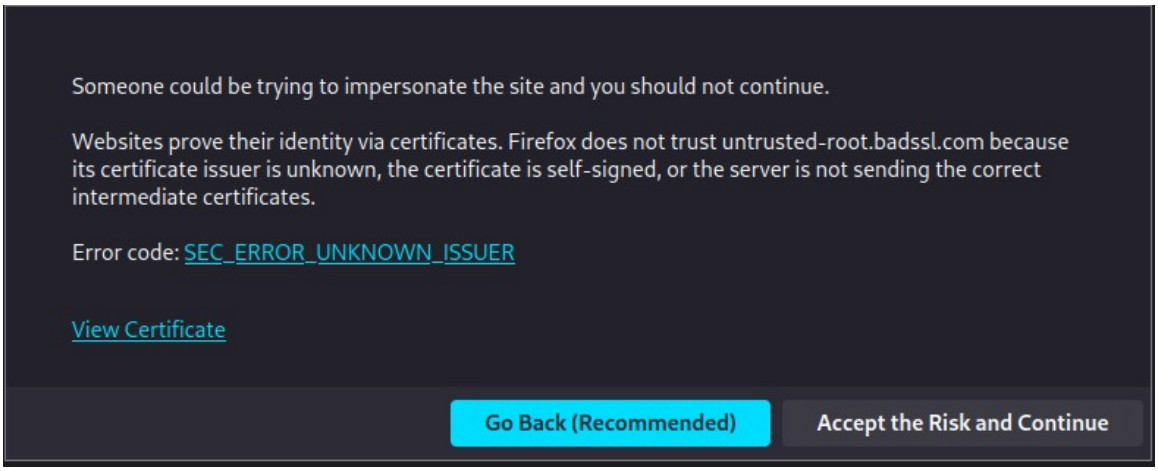
Serial Number	0B:2D:C6:AB:3E:0D:9D:17:64:D8:92:97:CA:89:BD:C2
Signature Algorithm	SHA-256 with RSA Encryption
Version	3
Download	PEM (cert) PEM (chain)

Fingerprints

SHA-256	3A:C1:B2:98:D1:52:02:94:0E:36:45:D1:87:C2:E8:68:67:2A:EC:44:42:5C:95:C8:...
SHA-1	E9:1D:29:78:9C:42:63:5E:C4:C7:CB:6A:00:B8:53:76:55:08:60:BB

25)


Not Secure
https://untrusted-root.badssl.com
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Warning: Potential Security Risk Ahead
Firefox detected a potential security threat and did not continue to untrusted-root.badssl.com. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.
What can you do about it?
The issue is most likely with the website, and there is nothing you can do to resolve it.
If you are on a corporate network or using antivirus software, you can reach out to the support teams for assistance. You can also notify the website's administrator about the problem.
Learn more...
Go Back (Recommended)
Advanced...


Someone could be trying to impersonate the site and you should not continue.
Websites prove their identity via certificates. Firefox does not trust untrusted-root.badssl.com because its certificate issuer is unknown, the certificate is self-signed, or the server is not sending the correct intermediate certificates.
Error code: SEC_ERROR_UNKNOWN_ISSUER
View Certificate
Go Back (Recommended)
Accept the Risk and Continue

Questions

1) Perform online research to identify what kind of browsing history information is saved when the "Always use private browsing mode" checkbox is selected. Be sure to cite your source(s) of information.

According to Mozilla's private browsing page and "common myths about private browsing" page, private browsing mode keeps no history of the sites you visit and does not save cookies, however any files downloaded and addresses bookmarked will be saved on your computer despite using private browsing mode. In particular, Mozilla makes a point to highlight that any malicious files downloaded while using private browsing such as keyloggers or spyware will still be on the device, emphasizing that private browsing does not protect against those kinds of threats.

2) Perform online research and answer the following questions. Be sure to cite your source(s) of information:

a) What are web trackers?

The Mozilla blog Distilled has an entry on web tracking, and it breaks web trackers down to scripts on websites that are designed to "derive data points" that can help show your preferences and how you interact with the sites that you visit.

b) Provide a definition for the term first-party cookie.

The same blog entry from part A includes information on first-party cookies, and defines them as cookies that come from the same website you are visiting and can include information such as a saved login or suggested content for the site.

c) Provide a definition for the term third-party cookie.

The same blog entry from part A has a section on third-party cookies, where they are defined as trackers belonging to an entity other than the site you are visiting at the time. They could be from "ad networks" or websites you have never been to or heard of, but collect data and share it with other groups.

d) What kind of privacy risk could third-party cookies possibly represent?

MDN Web Docs has a page on third-party cookies, where some of the risks identified include the ability to target users via spam emails and calls, "chasing" users with targeted advertisements when searches on particular products are performed, and can even lead to identity theft when information if collected from multiple different third-party cookies across the web of a particular user.

3) Perform online research and answer the following questions. Be sure to cite your source(s) of information.

a) What are your findings regarding cookies when visiting https://www.cnn.com in the normal browsing window and in the private browsing window?

When using a normal browsing window, there are a collection of third-party cookies that are present from groups such as Pubmatic, Google, and Amazon. However, in the private browsing window the only cookies that are loaded are first-party from the CNN domain.

b) What are your findings when visiting https://onlinecampus.bu.edu in the normal browsing window and in the private browsing window?

In both the normal window and private window, the only cookie present is from shib.bu.edu, which is used for authentication.

c) What is a session cookie? What are the purposes of the following flags: HttpOnly, HostOnly, secure. Are there any vulnerabilities related to the session cookie used by https://onlinecampus.bu.edu?

The Geeks for Geeks page on cookies includes information on session cookies, explaining that they are temporary cookies that are "present as long as the user's browser is open," and are deleted either when the browser is closed or the time that the session cookie is valid for expires.

For security flags, the MDN Web Docs cookie.Cookies API page includes information for the httpOnly, hostOnly, and secure flags. The 'httpOnly' flag is set to true when the cookie is inaccessible to client-side scripts, the 'hostOnly' flag is set to true when the request's host must **exactly** match the domain of the cookie, and the 'secure' flag is set to true when the cookie's scope is limited to secure channels such as HTTPS.

4) Perform online research to determine what the "Do Not Track" setting does and whether websites are required to honor it. Be sure to cite your source(s) of information.

In the Firefox settings, there is a link to a Mozilla page on the "Do Not Track" feature, and it's removal from the browser. The setting, when toggled on, tells the websites that are accessed that you do not want your browsing behavior tracked. The reason this was removed is that the option is entirely voluntary to honor on the website's side – they do not need to respect the choice. Mozilla recommends that the Global Privacy Control (GPC) feature can be used and is "enforced with legislation in some regions."

5) Perform online research and answer the following questions. Be sure to cite your source(s) of information.

a) Briefly describe how the adblocker works. Why does it require those permissions?

Both the Mozilla Distilled blog and Cybernews have informative pages on how adblockers work as well as trusted ones that are recommended. According to both sites, adblockers are able to prevent ads from displaying on a page by viewing and modifying the content of a webpage before it is rendered for you to see. Since they are modifying the code of a page before it loads for you, access is required to browser tabs, data for websites, and browsing activity in order for them to work correctly.

b) Are all extensions safe? Are there any potential security risks and why?

Absolutely not, extensions should be treated with caution and only installed when their authenticity and services are verified. Since extensions can request access to the data within your browser, information such as your login information passed to sites, browsing history, and activity on each page can be seen by a bad actor via malicious programs in an extension.

6) Based on the result from ssllabs.com, answer the following questions:

a) Which SSL and TLS protocol versions are supported by your browser?

Firefox version 128 has support for both TLS 1.2 and TLS 1.3.

b) Which cipher suite is preferred by your browser? Describe each of the components in your preferred cipher suite. Each component should be separated by an underscore character. So, explain what each item between the underscores means. Be sure to cite your source(s) of information.

Cipher Suites (in order of preference)

TLS_AES_128_GCM_SHA256 (0x1301)	Forward Secrecy	128
TLS_CHACHA20_POLY1305_SHA256 (0x1303)	Forward Secrecy	256
TLS_AES_256_GCM_SHA384 (0x1302)	Forward Secrecy	256
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)	Forward Secrecy	128
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	Forward Secrecy	128
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca9)	Forward Secrecy	256
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8)	Forward Secrecy	256
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)	Forward Secrecy	256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	Forward Secrecy	256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)	WEAK	256
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)	WEAK	128
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	WEAK	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	WEAK	256
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c)	WEAK	128
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d)	WEAK	256
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	WEAK	128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)	WEAK	256

(1) When a browser supports SSL 2, its SSL 2-only suites are shown only on the very first connection to this site. To see the suites, close all browser windows, then open this exact page directly. Don't refresh.

Firefox version 128 prefers the cipher suite TLS_AES_128_GCM_SHA256. The information provided on ciphersuite.info and scanigma.com break down the components that make up the ciphersuite name:

TLS → Protocol Layer
AES_128 → Encryption type - Advanced Encryption Standard with 128 bit key size
GCM → Encryption mode – Galois/Counter Mode
SHA256 → Hashing algorithm – Secure Hashing Algorithm with 256 bit hash size

c) Several vulnerabilities are checked against your browser. Is your browser vulnerable to any of them? Choose one vulnerability and perform online research. Briefly explain that vulnerability.

Of the vulnerabilities listed in step 22 (CurveBall, Logjam, FREAK, and POODLE) Firefox was determined to not be vulnerable to any of the four.

The FREAK attack in particular stands out to me as interesting, and pages on Digicert, FreakAttack, and SmackTLS contained some background information on the vulnerability. Standing for “Factoring RSA-Export Keys,” the attack is a type of man in the middle attack where an attacker intercepts HTTPS connections between vulnerable clients and servers, then forces a weaker encryption to be used. This weakened encryption is known to the attacker, which is then broken and allows the bad actor to steal and/or manipulate the data being communicated between the target clients and servers.

7) Perform online research to identify what OCSP is and what problem it is trying to solve. Be sure to cite your source(s) of information.

Online Certificate Status Protocol, or OCSP, is defined by Mozilla in their security blog to address the problem of obtaining certificate revocation information. Certificate revocation had been prioritized in order to determine when events such as the CA issuing certificates with incorrect information, transferring ownership of a domain, website operators losing control of their private key, or the theft a private key. With OCSP, the browser asks the CA who issued the certificate for the site if there are any issues, and the CA can respond with a signed confirmation if the certificate is valid or revoked.

8) Based on the information provided by the certificate, describe how the https://onlinecampus.bu.edu certificate is verified in detail. What are potential vulnerabilities associated with certificates?

The certificate from onlinecampus is verified by Amazon by confirming details like the validity range (in this case "not before August 2nd, 2025" and "not after August 30th, 2025") and the fingerprints containing the signatures of the certificate that can be verified by the issuer. Potential vulnerabilities associated with certificates can include spoofed issuer names, signatures, and using the certificate after it has expired.

9) Perform online research and answer the following questions. Be sure to cite your source(s) of information.

> **a)** How did your browser conclude the connection to https://untrustedroot.badssl.com was not secure? What processes did it undertake to definitively state there is a security problem with the connection?
>
> The error that caused the browser to conclude that the connection was not secure was the certificate having an unrecognized issuer. When Firefox did not recognize the CA that issued the certificate, it showed the warning page before going to the site.
>
> **b)** What do you need to do to permanently prevent that error message from displaying in your own browser? What do the website maintainers need to do in order to prevent this message from displaying for all visitors' browsers?
>
> For a user to prevent the error message, they have to first see the error code by clicking the "Advanced..." button, then can choose "accept the risk and continue." For website maintainers to prevent this message for all visitors' browsers they must have their certificate signed by a trusted CA such as Amazon or Entrust.

Reflection

a) What is the purpose of the lab in your own words?

This lab, in my opinion, was made to introduce us to the security standards that web browser like Firefox employ to make browsing the internet a safer experience. Through the use of security settings, viewing cookies in developer settings, and becoming familiarized with different security standards used on the web, we were able to gain an understanding of some of the security checks that are performed that many users are unaware of in their day-to-day browsing.

b) What did you learn? Did you achieve the objectives?

I believe I accomplished the objective, and throughout this lab I learned about the ciphersuite that Firefox uses, how websites are able to verify their authenticity through the browser, and the "background" work that browsers like Firefox perform in order to combat against exploits and human error.

c) Is this lab hard or easy? Are the lab instructions clear?

The instructions for this lab were well written and clear, however there were two steps that were difficult to accomplish due to the browser being outdated (at least for the Kali Linux that I was using). It would seem that my browser being out of date was the cause for the issues mentioned in steps 14 and 16, however aside from those all other steps were made approachable through the instructions.

d) What do you think about the tools used? What worked? What didn't? Are there other better alternatives?

While I am familiar with Firefox, SQLiteBrowser, and extensions like adblockers, I had not delved into the settings and information they provided as much before. It is particularly interesting to me how much information is available in Firefox such as cookie information, certificate hashes, and browsing information databases that most users aren't even aware of. All of the tools in the lab worked except for the issues in steps 14 and 16 that were easily fixed with a Firefox update. There are plenty of alternatives for browsers, however I don't think that any are better than Firefox as Mozilla has a strong interest in privacy and data protection compared to most of the competitors.

e) Other feedback

I enjoyed this lab as it turned a daily used application like Firefox into a valuable tool for learning about web privacy and data tracking. The thing I would suggest is to include a step for students to verify that Firefox is updated and able to work as intended for the websites accessed and extensions installed.