BOSTON UNIVERSITY METROPOLITAN COLLEGE

MET CS 695S O2 REG Cybersecurity (2024 Summer 2)

Lab 5 Web Browser Security

Submitted to

Nicklos See, M.S.,

Warren Mansur, M.S.,

Shengzhi Zhang, Ph.D.

MET CS695S O2 REG

Cybersecurity

by

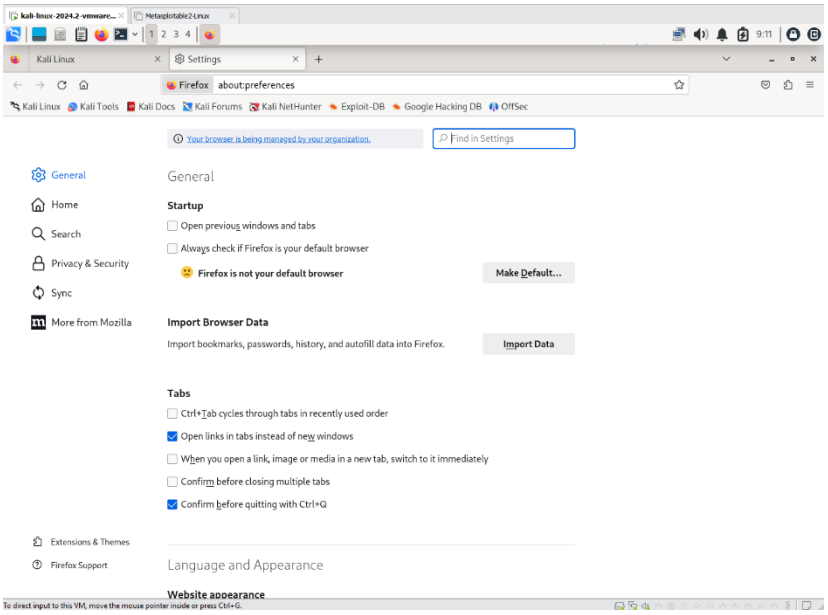
Michael G Nguyen

8/4/2024

Table of Contents

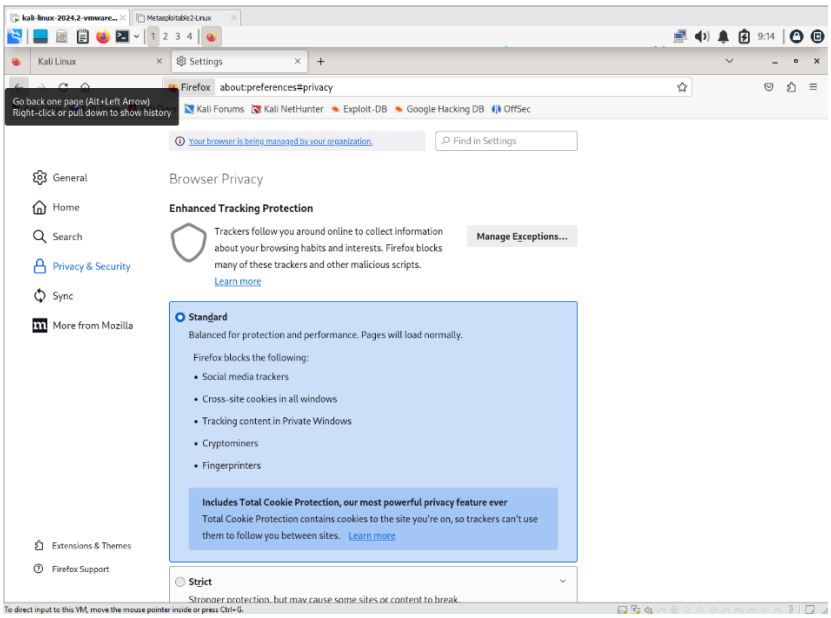
History

1. Open the web browser in Kali, Click the three-lined Open menu icon and select “Settings” from the menu that appears.



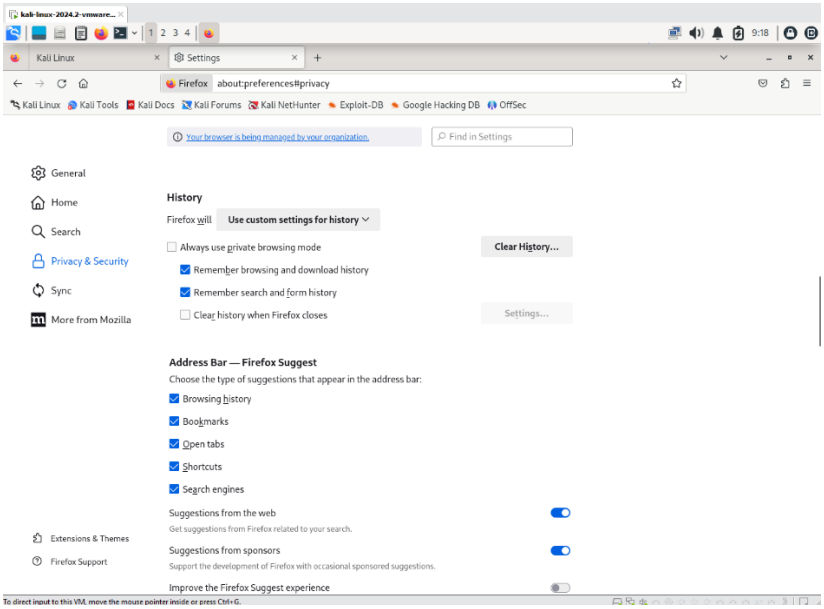
Executing the web browser settings.

2. Open the Browser Privacy settings by clicking the Privacy & Security link.



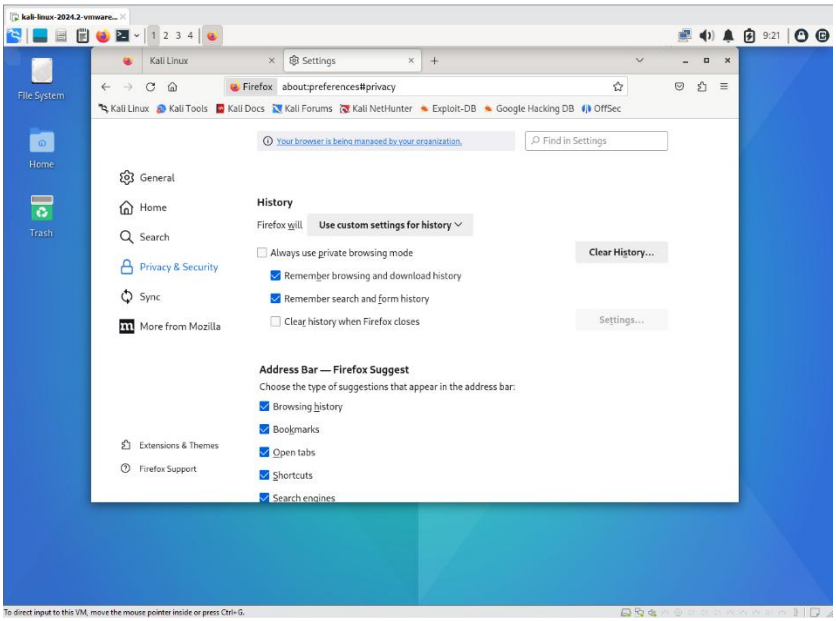
Opening the browser privacy & settings.

3. Scroll down to the History section. The History section determines whether Firefox will retain browsed pages, form contents, and other downloaded information.



Scrolling to the history section of the browser and changing it to “Use custom settings for history”.

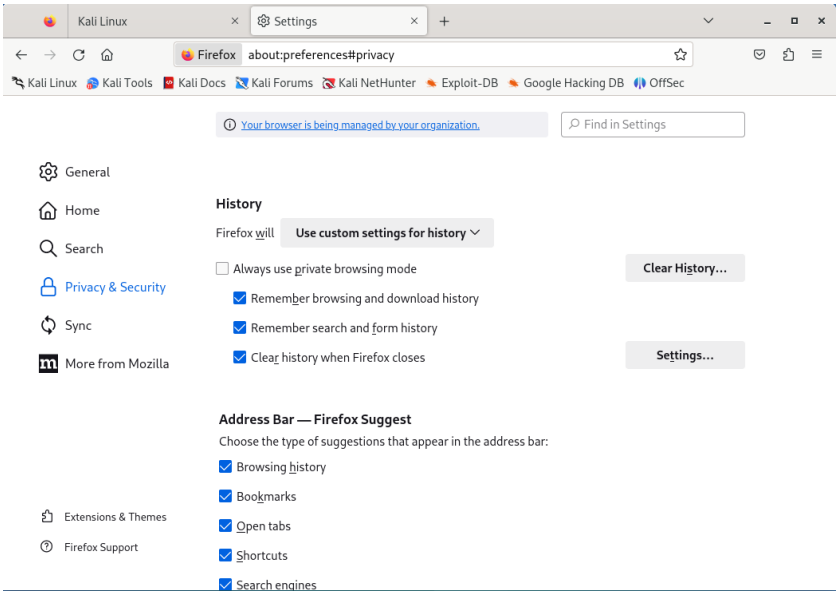
4. Change the History section to Use custom settings for history to see the available options. What does “Always use private browsing mode” mean? Perform online research and answer Question 1.



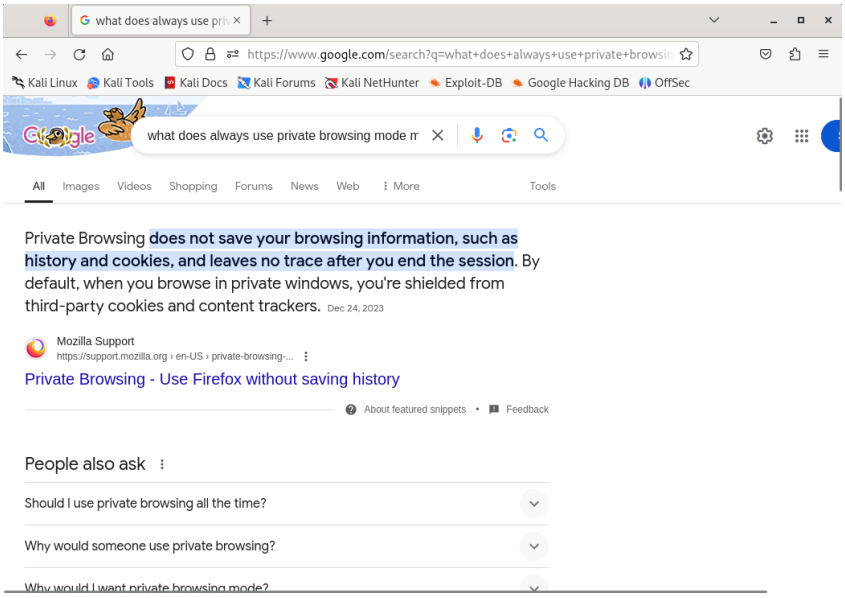
Changing to “Use custom settings for history”.

5. Place a check next to the “Clear history when Firefox closes” checkbox. This option prevents someone else on the computer from gaining access to your browsing history after Firefox closes. It may delete information you wish to retain, though. Try to visit some websites and close the

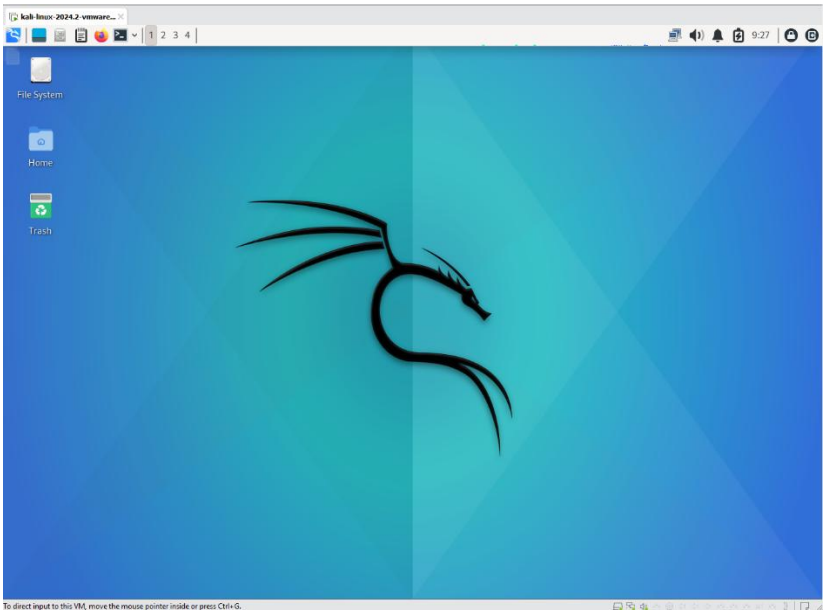
firefox. Reopen the firefox again and see if the history is cleared. You can check browsing history by clicking the three-lined Open menu icon and selecting “History” from the menu that appears. Take some screenshots and state your findings.



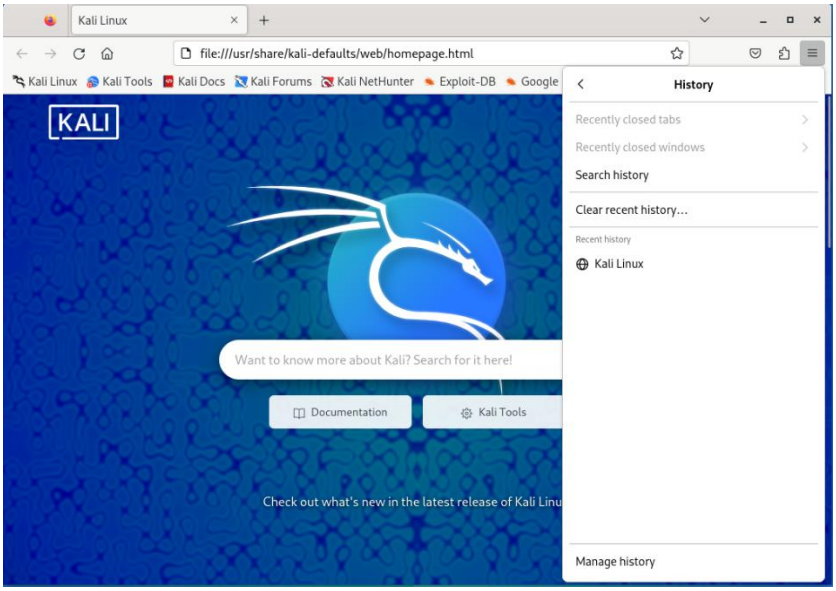
Placing a check mark next to “Clear history when Firefox closes”.



Going to google to check if “Clear history when Firefox closes” works or not.

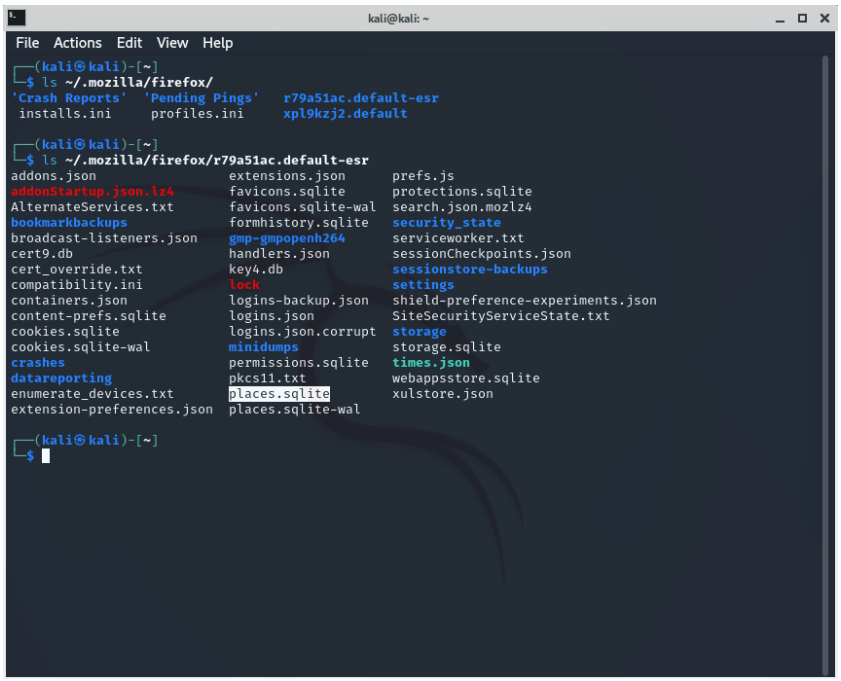


Exiting Firefox.



It worked. “Clear history when Firefox closes” worked and cleared all the histories.

6. Firefox stores history, bookmarks and other information in the following locations: /home//.mozilla/firefox/. The on our computer is called wc581fvu.default-esr. It may be a different name on your computer, but still end with .default-esr. Make sure you replace the profile folder accordingly in the commands below. The places.sqlite file under the profile folder contains all your Firefox bookmarks and lists of all the files you've downloaded and websites you’ve visited. You can find more information about how firefox stores user data at [Profiles - Where Firefox stores your bookmarks, passwords and other user data | Firefox Help (mozilla.org)]

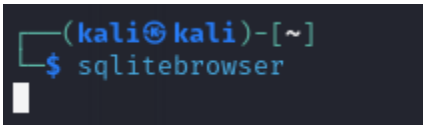


Using list all (ls) command in kali linux terminal to find places.sqlite.

7. We can use a sqlite browser to open the places.sqlite file. To prevent any changes, let us first copy the file into another location, such as ~/lab5.

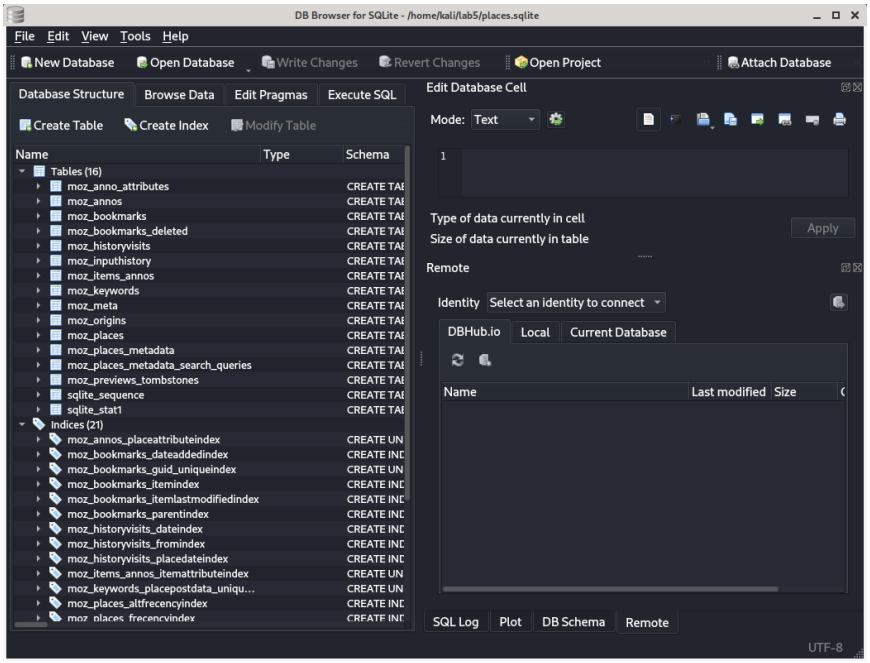
Make directory of lab5, copying files and placing places.sqlite in lab5 directory, and listing all lab5 files.

a. Install sqlitebrowser using “apt install” command if it is not installed (by default it should be). Then open the sqlitebrowser by simply typing “sqlitebrowser” in the terminal.



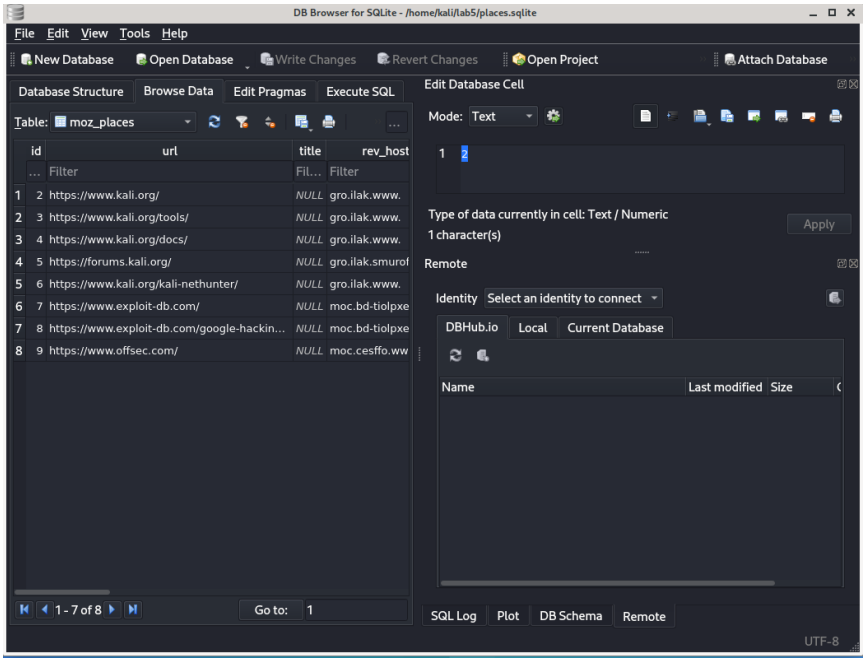
Initializing sqlitebrowser with a terminal command.

b. On sqlitebrowser, click the menu item “File / Open Database …” to open the places.sqlite in the ~/lab5.



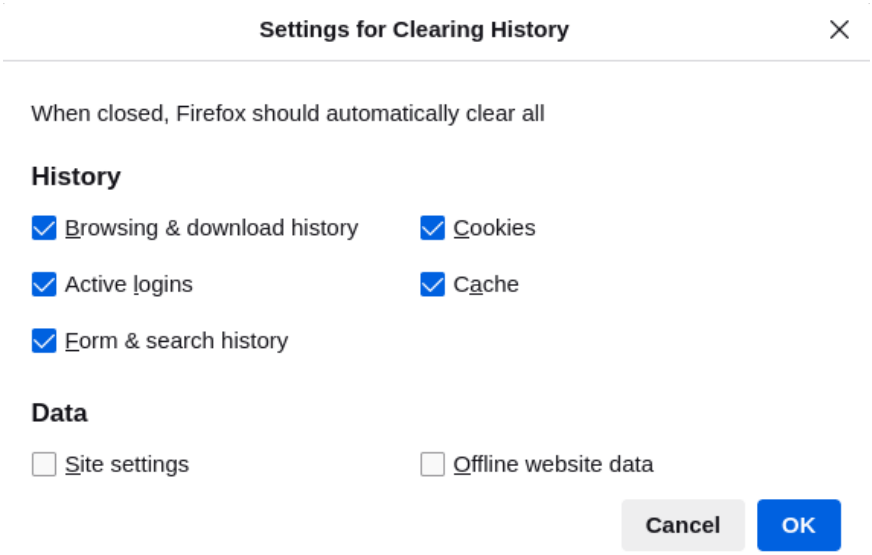
Opening places.sqlite in the ~/lab5.

c. Click on “Browser Data” and choose the “moz_places” table, you can see URLs visited. You can verify if that is correct, and consistent to the history displayed through GUI.



It doesn’t seem correct; I haven’t visited these pages before. However, Kali Linux information are preloaded, so therefore, it might be already there.

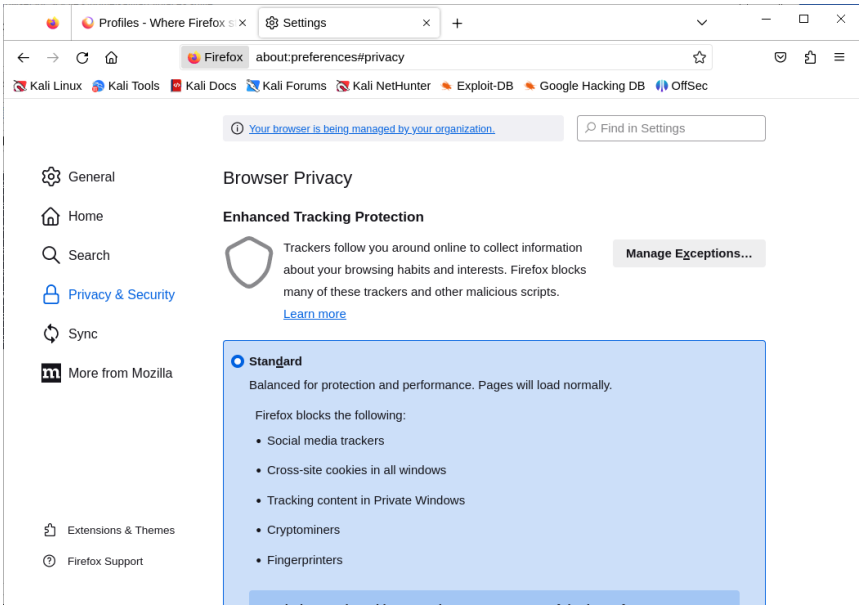
8. Click the “Settings... “ button on Firefox that became enabled with your previous selection in Step 5. The options that appear allow you to further specify what is cleared when Firefox closes. You can find out which items are automatically clearly and which are NOT automatically clearly under this configuration.



Settings under Firefox and which history are being chosen to be cleared.

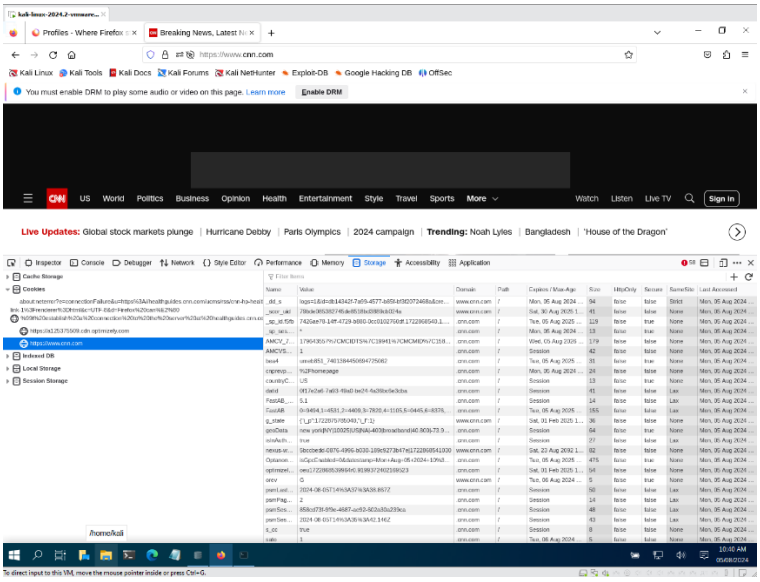
Tracker and Cookies

9. Close the “Settings for Clearing History” box and scroll up to the “Enhanced Tracking Protection” section. Here, you may choose to block some invisible content such as cookies that tracks the sites you visit and profiles you. You can find more information from the “Learn more” link and the following link: https://blog.mozilla.org/firefox/what-is-a-web-tracker/. Perform some online research and answer Question 2.



Scrolling up to the “Browser Privacy” in Privacy & Security.

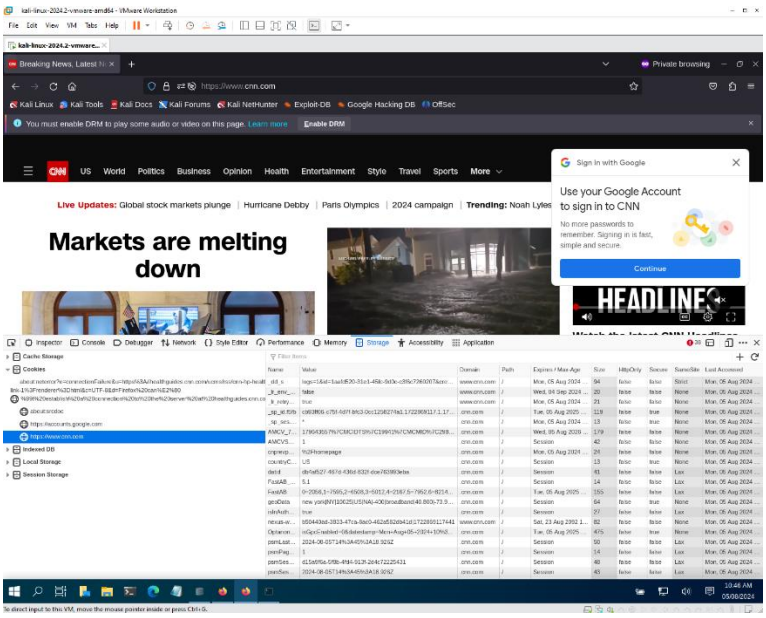
10. To find out what cookies are used by the websites we visit, we can use the developer tool provided in Firefox. Visit https://www.cnn.com. Click the three-lined Open menu icon and click “More tools” from the menu that appears. Then select “Web Developer Tools” from the “More tools” menu. The inspector window will appear at the bottom of the page. Choose the “Storage” tab, and you will find what cookies are used by the website. Identify which are first party cookies and which are third party cookies.



Cnn.com is first party cookies, and a125375509.cdnoptimizely.com is third party cookies.

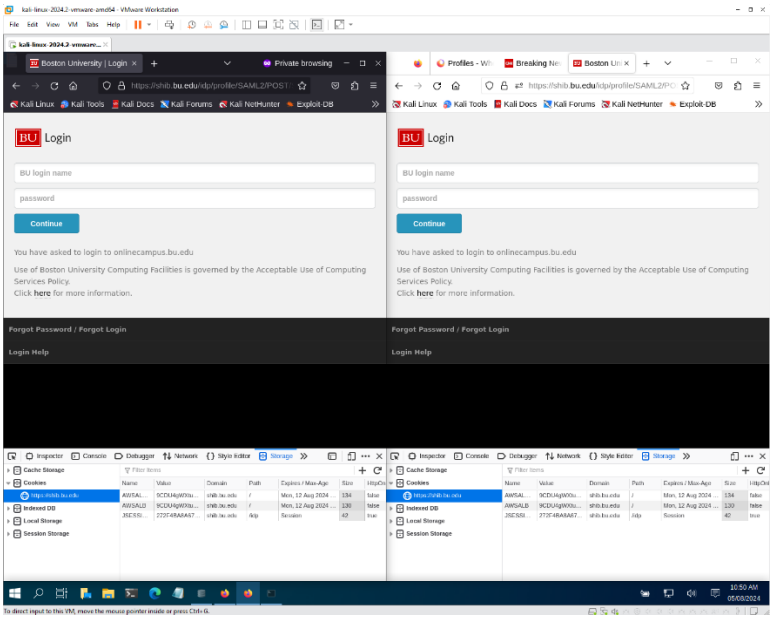
(Professor See, I was being nosy what “Undercover Mode” in Kali Linux does at kali.org website, so I turned it on, my screen might appear to be windows, however, it isn’t.)

11. Now, open a private browsing window by clicking the three-lined Open menu icon and select “New Private Window”. As we see in the previous setting, known trackers are blocked in the private browsing. Visit https://www.cnn.com in this new private window. Then open the More tools -> Web Developer Tools Window again to check cookies in the Storage tab. What are your findings? Answer Question 3.a.

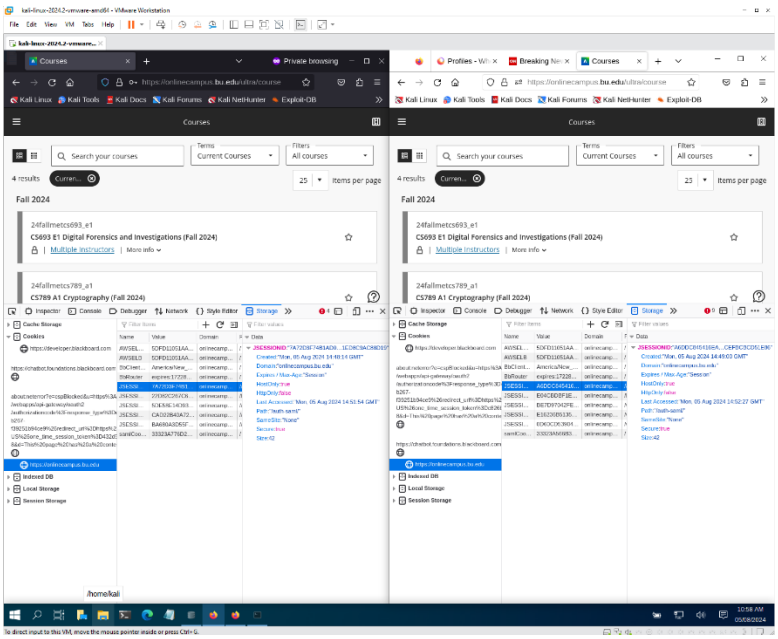


It does not contain any third-party cookies.

12. Now try to visit https://onlinecampus.bu.edu in both normal browsing window and private window. Check the cookies used. Are there any differences? Log into the blackboard site with your bu credentials and then check the cookies again. You should find a session cookie which is usually used for session management. Click on it to find more details. Perform some online research to understand different flags in the cookie such as HttpOnly, HostOnly, and Secure. Are there any vulnerabilities associated with this session cookie? Answer Question 3.b and 3.c.



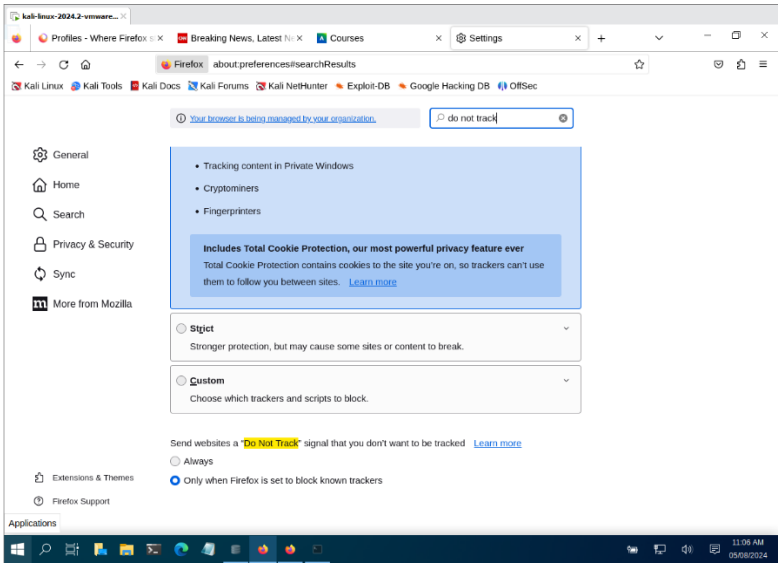
Looks the same.



It has different JSESSIONID: JSESSIONID:"7A72D3F74B1AD01EB1E1ED8C9AC88D19",

and JSESSIONID:"A6DDC845416EA9CB0ACCEFBCBCD51E86"

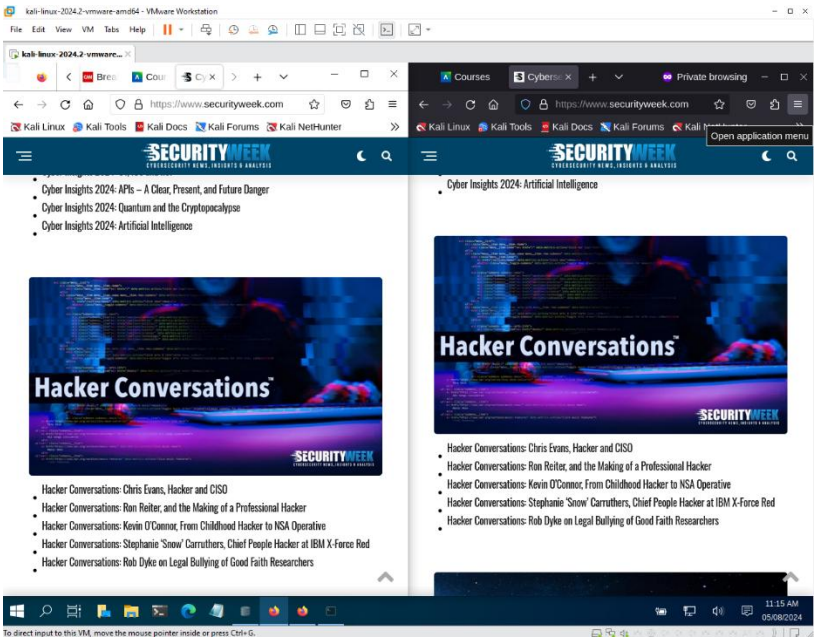
13. At the bottom of the “Enhanced Tracking Protection” section, you should find settings related to Do Not Track. Answer Question 4.



By default its already in “Do Not Track”.

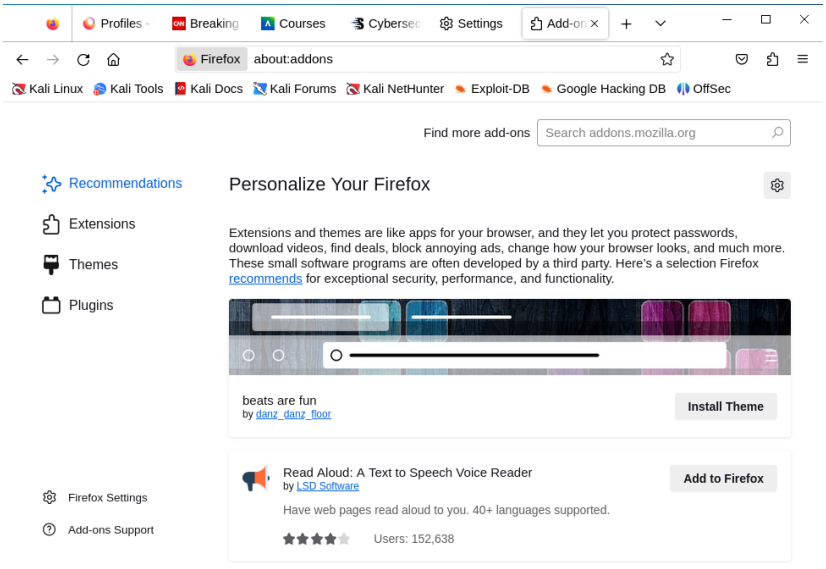
FIREFOX PRIVACY ADD-ONS

14. As you researched, cookies through online advertisements can be a source of privacy leaks and potential malware on the Internet. Visit https://www.securityweek.com. Notice there are advertisements scattered throughout the page – at the top and on the side. In the sample image, a banner ad appears near the top of the page.



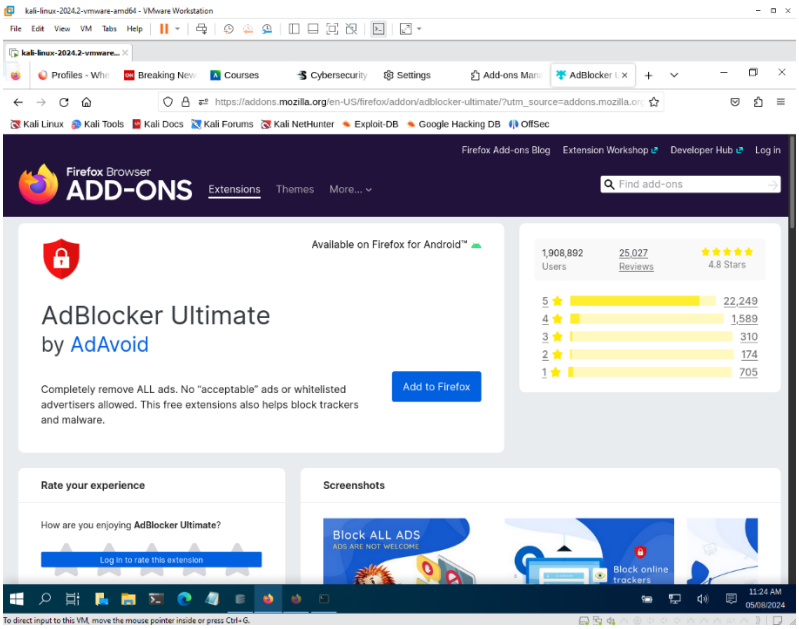
I did it in private and normal browser, both appears the same.

15. Another way to add privacy to Firefox is to use an add-on to prevent ads, and other potential trackers, from displaying on our pages. One important strength of Firefox is its robust add-ons and extensions repository. Click the three-lined Open menu icon and select Add-ons and themes from the menu that appears.



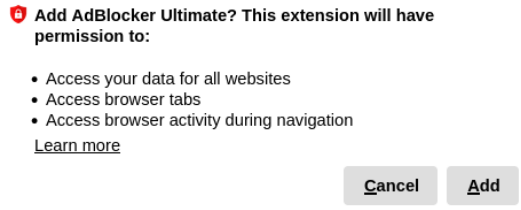
Firefox add-ons window.

16. Click the Extensions item to gain access to Firefox add-ons and extensions. In the search dialog box, search for the Adblocker Ultimate add-on, and press Enter. From the search results, locate the Adblocker Ultimate entry and click on it.



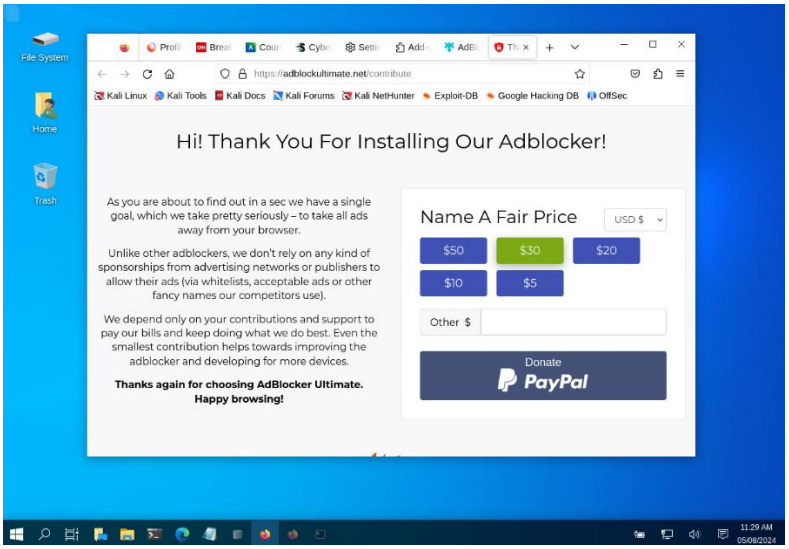
Searching for "AdBlocker Ultimate" within extension.

17. Click the Add to Firefox button for the Adblocker Ultimate add-on. When prompted with a list of permissions Adblocker Ultimate requires, be sure to click the Add button. Click on "Learn more" to get more detailed information. Perform some online research to understand how adblocker works and answer Question 5.



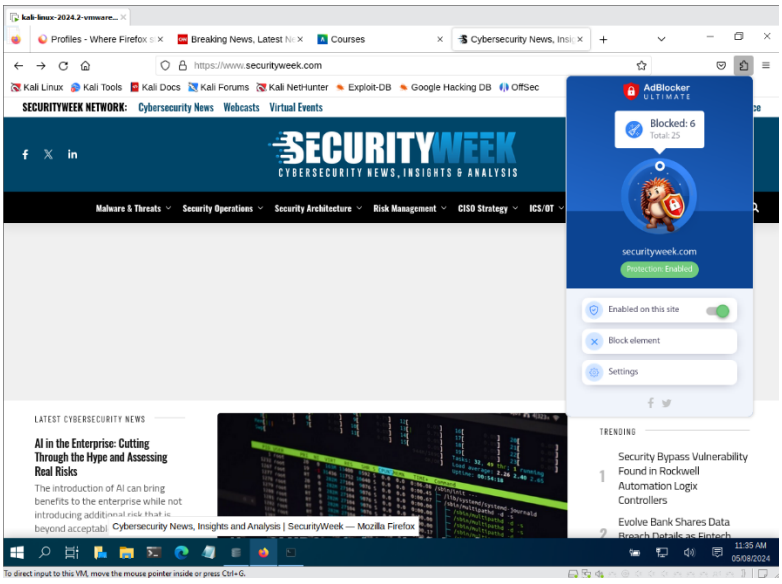
Adding AdBlock Ultimate to extension.

18. Once installation finishes, a page will display, indicating Adblocker Ultimate has been installed. AdBlocker Ultimate for Browsers is a completely free, open source and nonprofit project licensed under GPLv3. It can block ads, malicious websites and online trackers with no exceptions. It is available on all popular web browsers - Google Chrome, Mozilla Firefox, Opera and Microsoft Edge.



The page after installation is executed.

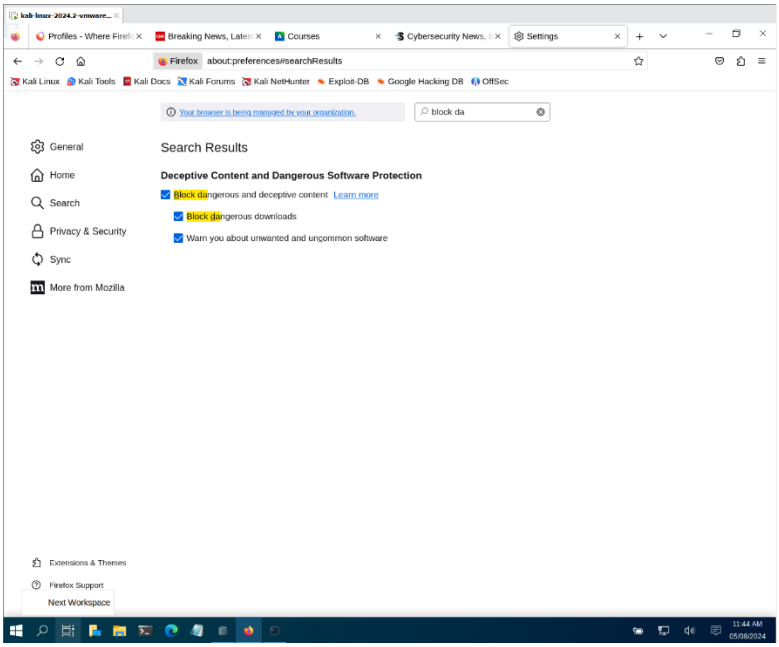
19. Next, return to the previous ad-laden page at https://www.securityweek.com. and refresh it. It should display without the banner ad. In this example, note the top advertisement no longer appears.



Yes, it blocked 6 ads with a total of 25, thus far.

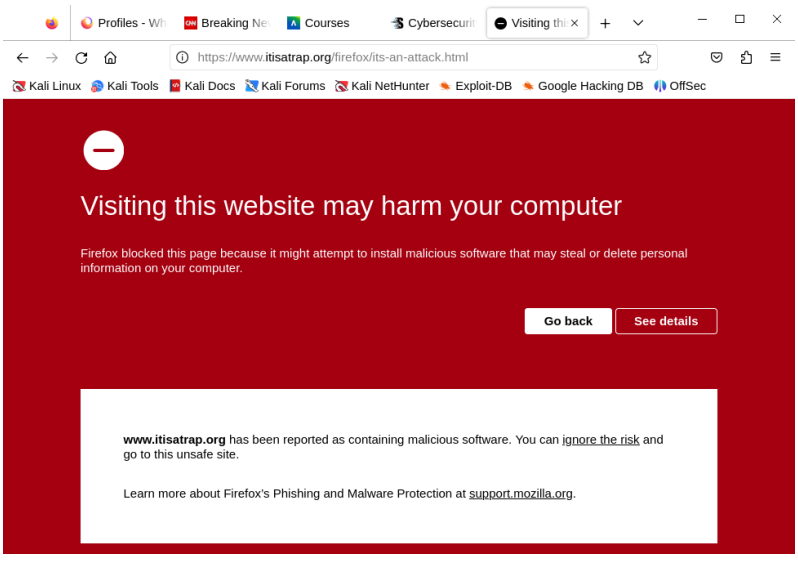
Security

20. The Firefox browser also provides a number of configurable options related to communication security. Return to the Firefox options and open the Privacy & Security panel link. Scroll down to the Security section. A number of security-related options are available here. The “Block dangerous and deceptive content” option alerts you when you are visiting a website that is known to host malware or is a known phishing site.

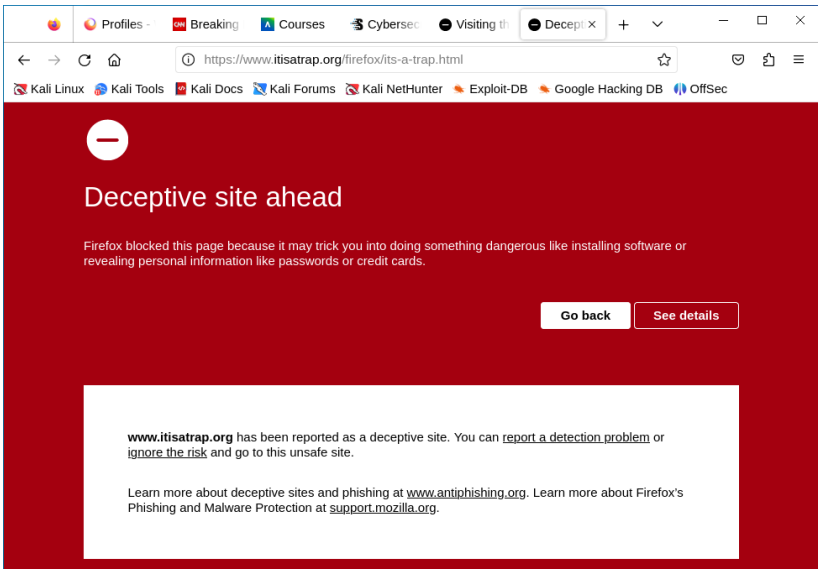


“Block dangerous and deceptive content” is already checked.

21. To test whether the dangerous and deceptive content protection is working, visit https://www.itisatrap.org/firefox/its-an-attack.html. Provide a cropped screenshot showing the attack warning that displayed when visiting the attack site. To test whether the phishing site protection is working, visit https://www.itisatrap.org/firefox/its-a-trap.html. Take screenshots to show the warning displayed when visiting these sites.

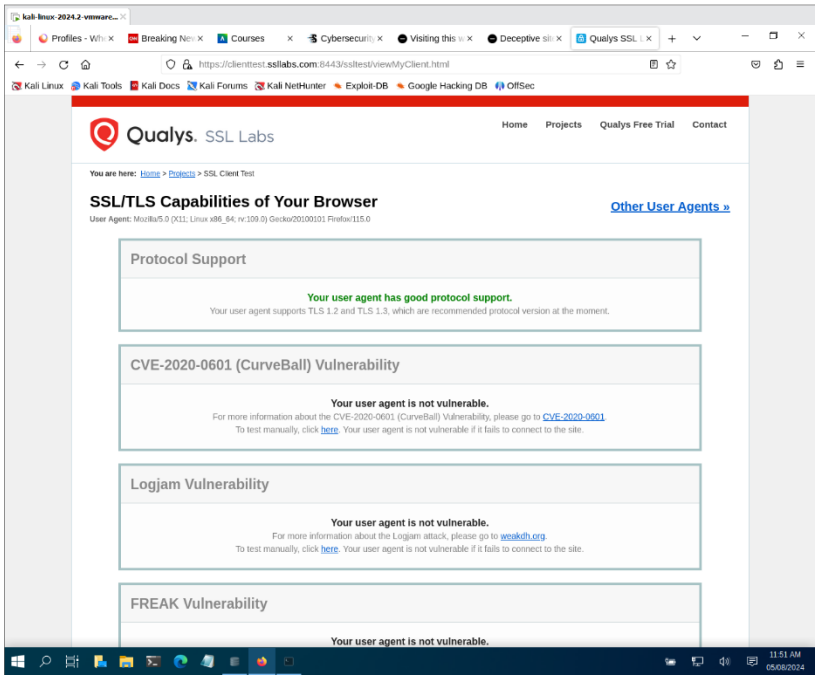


Yes, it worked.

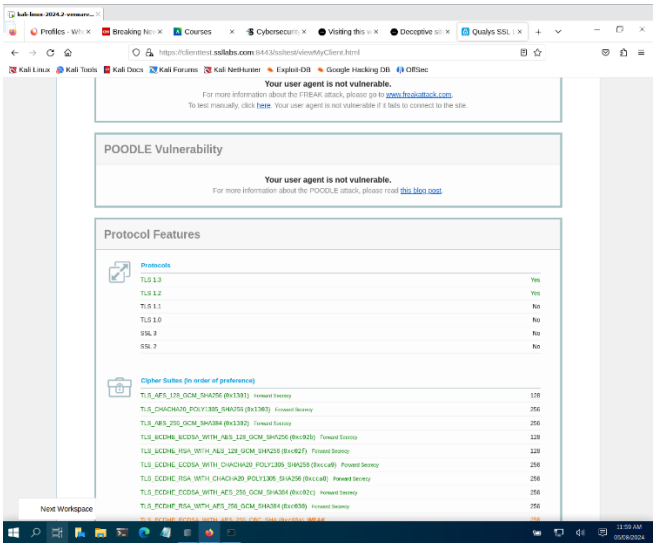


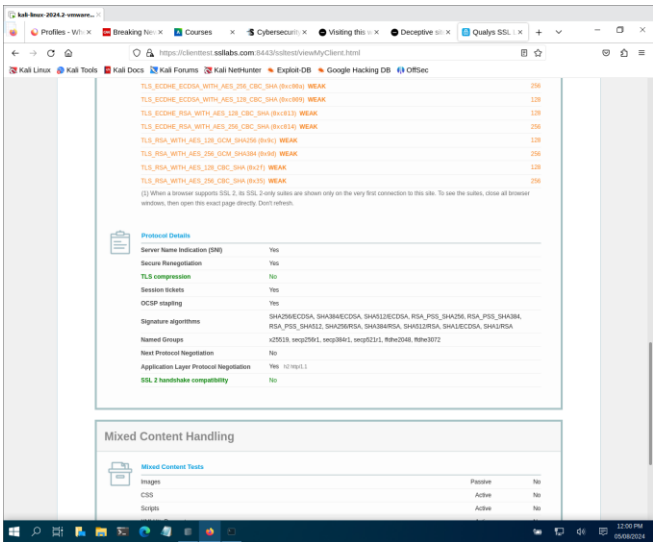
Yes, it worked, along with this website as well.

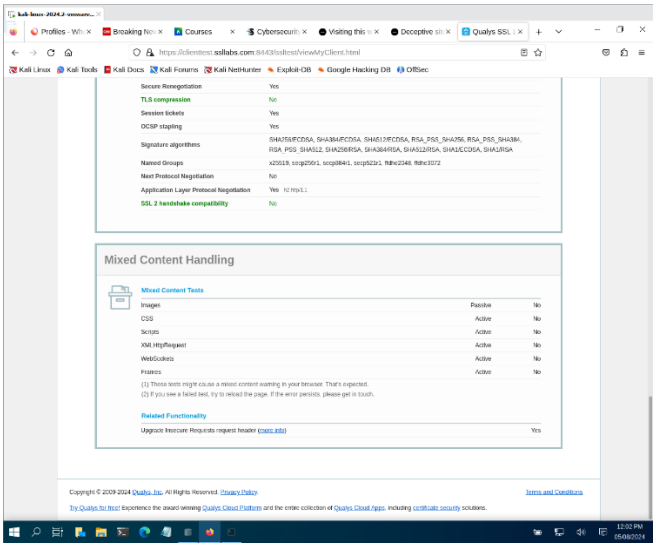
22. One important security component with any web browser is its TLS support. Visit the Qualys SSL Labs site at https://www.ssllabs.com/ssltest/viewMyClient.html to identify security protocol support and potential vulnerabilities with the Firefox browser. Answer Question 6.



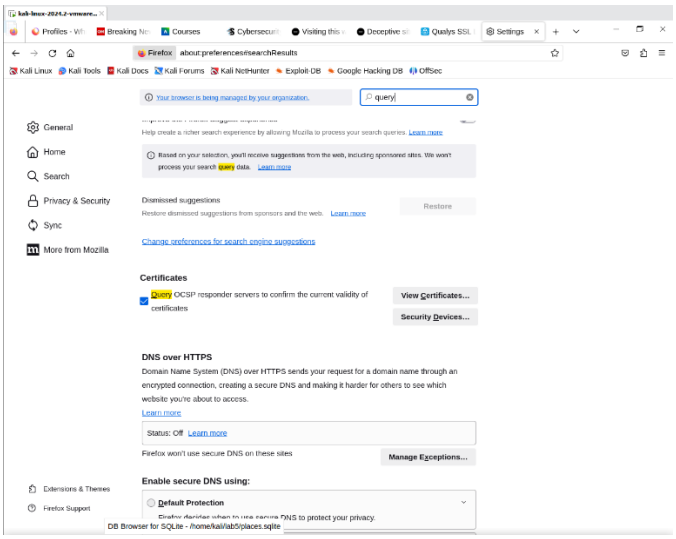
I had not issues accessing the website. Below are some more screenshots.


Your user agent is not vulnerable.
POODLE Vulnerability
Your user agent is not vulnerable.
Protocol Features
Protocols
TLS 1.3 Yes
TLS 1.2 Yes
TLS 1.1 No
TLS 1.0 No
SSL 3 No
SSL 2 No
Cipher Suites (in order of preference)
Next Workspace


Protocol Details
Server Name Indication (SNI) Yes
Secure Renegotiation Yes
TLS compression No
Session tickets Yes
OCSP stapling Yes
Named Groups
Next Protocol Negotiation No
Application Layer Protocol Negotiation Yes
SSL 2 handshake compatibility No
Mixed Content Handling
Mixed Content Tests
Images Passive No
CSS Active No
Scripts Active No

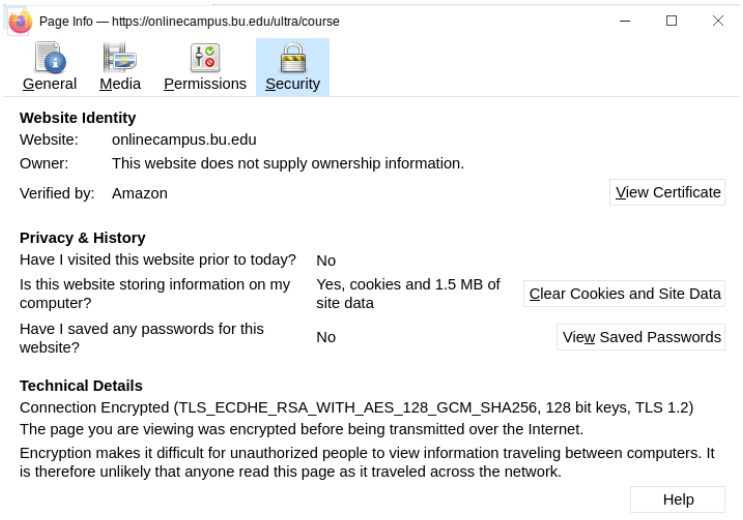

Secure Renegotiation Yes
TLS compression No
Session tickets Yes
OCSP stapling Yes
Named Groups
Next Protocol Negotiation No
Application Layer Protocol Negotiation Yes
SSL 2 handshake compatibility No
Mixed Content Handling
Mixed Content Tests
Images Passive No
CSS Active No
Scripts Active No
XMLHttpRequest Active No
WebSockets Active No
Frames Active No
Related Functionality
Upgrade Insecure Requests request header Yes

23. Return to the Firefox Options and open the Privacy & Security panel link. Scroll down to the Security section. Below Certificates, the Query OCSP responder servers to confirm the current validity of certificates checkbox should be selected by default. Perform online research and answer Question 7.

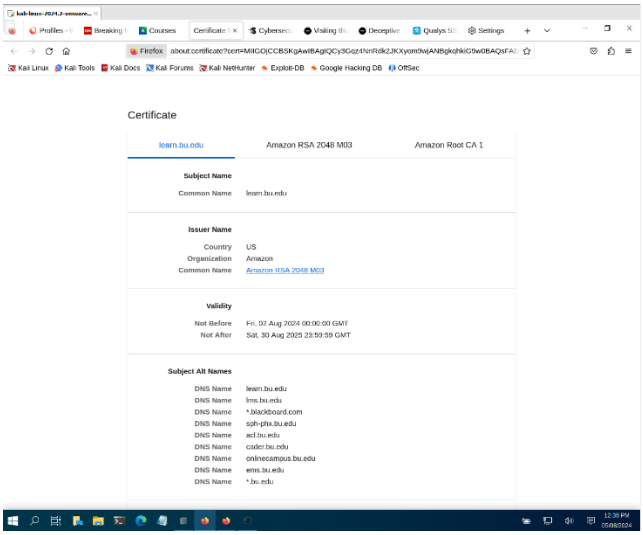


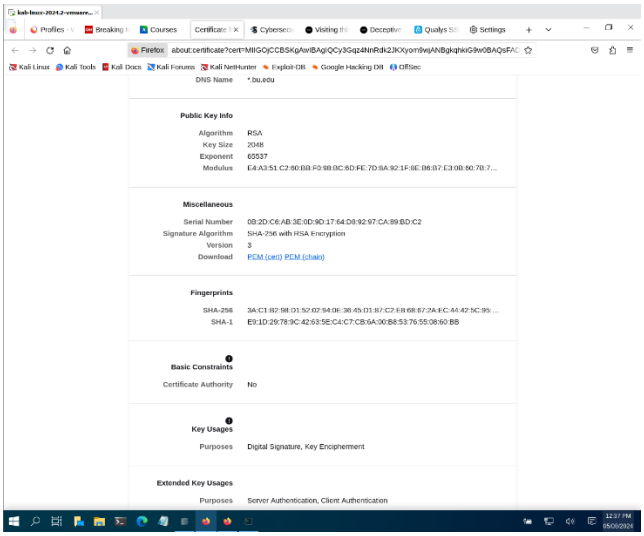
Yes, "Query OCSP responder server to confirm the current validity of certificates" is already checked.

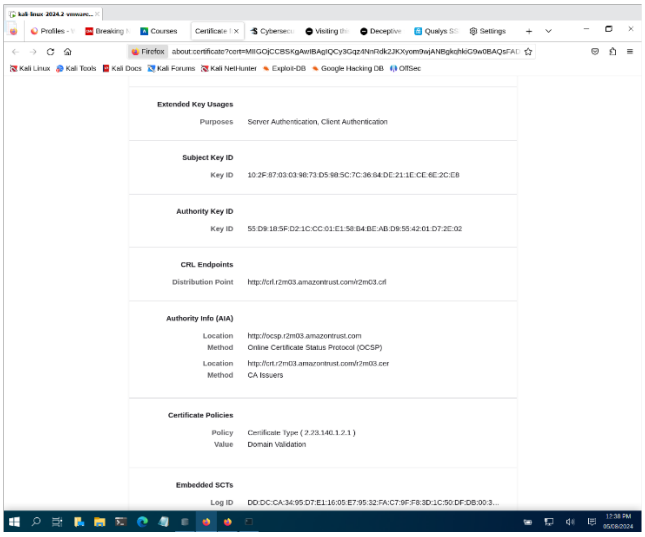
24. In the address bar, visit https://onlinecampus.bu.edu again. Log into the website if you didn't. Click on the information icon (the lock) in the address bar. You can find more information about this website, such as connection, cookies, and permissions. Choose the "Connection secure" item and see who verified the certificate in the next panel. Click the "More Information" button. Click the "View Certificate" button to check the certificate details. Answer Question 8.

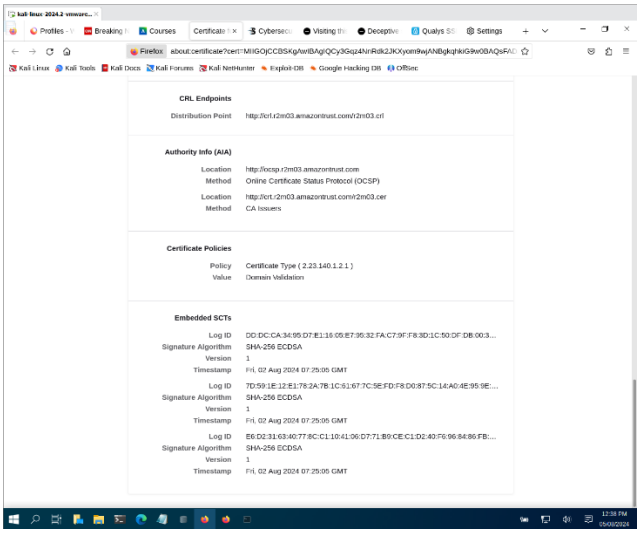


It looks like amazon verify the certificate. Below are more information regarding that.

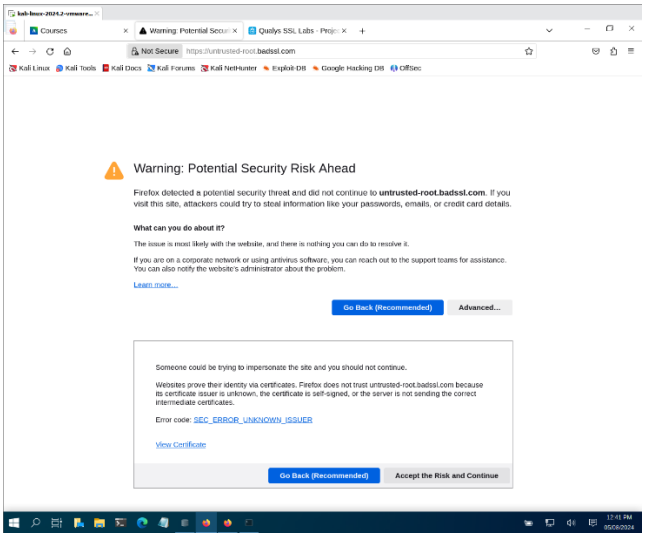

Certificate
learn.bu.edu
Amazon RSA 2048 M03
Amazon Root CA 1
Subject Name
Common Name learn.bu.edu
Issuer Name
Country US
Organization Amazon
Common Name Amazon RSA 2048 M03
Validity
Not Before Fri, 02 Aug 2024 00:00:00 GMT
Not After Sat, 30 Aug 2025 23:59:59 GMT
Subject Alt Names
DNS Name learn.bu.edu
DNS Name lms.bu.edu
DNS Name *.blackboard.com
DNS Name sph-phx.bu.edu
DNS Name acl.bu.edu
DNS Name cader.bu.edu
DNS Name onlinecampus.bu.edu
DNS Name ems.bu.edu
DNS Name *.bu.edu


DNS Name *.bu.edu
Public Key Info
Algorithm RSA
Key Size 2048
Exponent 65537
Modulus E4:A3:51:C2:9D:B8:F0:98:0C:6D:FE:7D:8A:92:1F:8E:D8:87:E3:0B:80:78:7...
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:C1:82:98:D1:52:02:94:0E:36:45:D1:87:C2:F8:68:67:2A:EC:44:42:5C:95:...
SHA-1 E9:1D:29:78:9C:42:63:5E:C4:C7:CB:6A:9D:B8:53:76:55:08:60:BB
Basic Constraints
Certificate Authority No
Key Usages
Purposes Digital Signature, Key Encipherment
Extended Key Usages
Purposes Server Authentication, Client Authentication

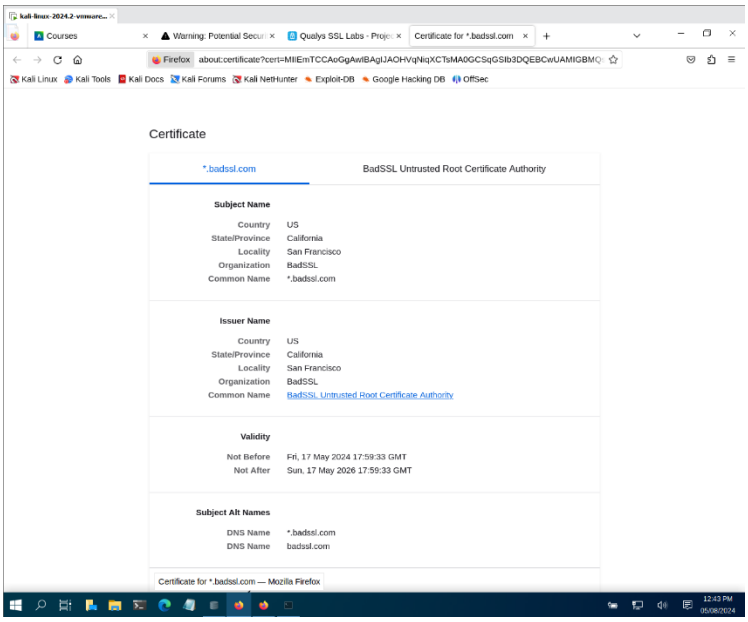

Extended Key Usages
Purposes Server Authentication, Client Authentication
Subject Key ID
Key ID 10:2F:87:03:03:98:73:D5:98:5C:7C:36:84:DE:21:1E:CE:6E:2C:E8
Authority Key ID
Key ID 55:D9:18:5F:D2:1C:CC:01:E1:58:B4:BE:AB:D9:55:42:01:D7:2E:02
CRL Endpoints
Distribution Point http://crl.r2m03.amazontrust.com/r2m03.crl
Authority Info (AIA)
Location http://ocsp.r2m03.amazontrust.com
Method Online Certificate Status Protocol (OCSP)
Location http://crt.r2m03.amazontrust.com/r2m03.cer
Method CA Issuers
Certificate Policies
Policy Certificate Type (2.23.140.1.2.1)
Value Domain Validation
Embedded SCTs
Log ID DD:DC:CA:34:95:D7:E1:16:05:E7:95:32:FA:C7:9F:F8:3D:1C:50:DF:DB:00:3...



25. Now try to access https://untrusted-root.badssl.com. You will receive an error message from your browser, indicating the connection is not secure. Answer Question 9.



Correct, the website has certification issues from badssl.com. Below is more information.



Certification issue at badssl.com

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.

When the "Always use private browsing mode" checkbox is selected, Firefox will not save browsing history, search history, download history, web form history, cookies, or temporary internet files. It essentially acts as if every browsing session is a private browsing session, meaning no trace of your activity is left on your computer after the session ends.

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

a. What are web trackers?

Web trackers are scripts or technologies used by websites to collect data about a user's online behavior. This data can include information about the user's browsing habits, preferences, and interactions with websites. Web trackers are often used for analytics, advertising, and personalized content delivery.

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

A first-party cookie is a cookie that is set by the website that the user is currently visiting. These cookies are typically used to remember user preferences and keep users logged in as they navigate the site.

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

A third-party cookie is a cookie that is set by a domain other than the one the user is currently visiting. These cookies are commonly used by advertisers and social media platforms to track users across different websites for targeted advertising and analytics.

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

Third-party cookies can pose privacy risks because they allow third parties to track a user's browsing behavior across multiple websites. This tracking can lead to the creation of detailed user profiles without the user's consent, which can then be used for targeted advertising and potentially be shared or sold to other entities.

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 visiting CNN.com in a normal browsing window, both first-party and third-party cookies are present. In a private browsing window, third-party cookies are generally blocked, so you should primarily see first-party cookies.

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

When visiting onlinecampus.bu.edu in both normal and private browsing windows, session cookies such as JSESSIONID are used for session management. There might be slight differences in the cookies depending on the login state and whether the site uses persistent cookies for other functionalities.

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

A session cookie is a temporary cookie that is erased when the user closes their browser. These cookies are used to maintain a session state across different pages of a website.

- HttpOnly: This flag ensures that the cookie cannot be accessed via JavaScript, providing protection against cross-site scripting (XSS) attacks.
- HostOnly: This flag specifies that the cookie should only be sent to the specific domain that set the cookie, not to subdomains.
- Secure: This flag ensures that the cookie is only sent over secure HTTPS connections, protecting it from being intercepted by attackers.

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.

The "Do Not Track" setting is a browser option that sends a signal to websites indicating that the user does not want their browsing behavior tracked. However, honoring this request is voluntary, and many websites may choose to ignore it.

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?

An adblocker works by blocking requests to ad servers, hiding ad elements on web pages, and preventing tracking scripts from running. It requires permissions to access and modify web content, as well as to intercept network requests in order to block ads and trackers effectively.

b. Are all extensions safe? Are there any potential security risks and why? Which SSL and TLS protocol versions are supported by your browser?

Not all extensions are safe. Some extensions can pose security risks if they are poorly coded or if they request excessive permissions. Malicious extensions can inject unwanted content, track browsing activity, or compromise personal data.

6. Based on the result from ssllabs.com, answer the following questions:
a. Which SSL and TLS protocol versions are supported by your browser?

From the ssllabs.com test, you can determine the specific versions of SSL and TLS that your browser supports. Modern browsers typically support TLS 1.2 and 1.3, while older protocols like SSL 2.0 and SSL 3.0 are usually disabled due to security vulnerabilities.

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.

The preferred cipher suite is determined by the server and the browser during the TLS handshake. Each component of the cipher suite (e.g., TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) represents the key exchange method, authentication, encryption algorithm, and hashing algorithm used.

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.

Your browser may be checked for various known vulnerabilities like POODLE (SSL 3.0), BEAST (SSL), Heartbleed (OpenSSL), and zero-day (software or hardware). If your browser is vulnerable to any of these, you should update to the latest version to mitigate these risks.

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.

The Online Certificate Status Protocol (OCSP) is used to check the revocation status of digital certificates. It solves the problem of identifying whether a certificate has been revoked by its issuer before it expires, enhancing the security of SSL/TLS connections.

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 for onlinecampus.bu.edu is verified by a trusted certificate authority (CA), such as Amazon. The verification process involves checking the certificate's validity period, the CA's signature, and the certificate chain.

Potential vulnerabilities:

Potential vulnerabilities with certificates include misissued certificates, compromised CAs, and man-in-the-middle attacks. Ensuring certificates are properly managed and validated is crucial for maintaining secure communications.

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://untrusted-root.badssl.com was not secure? What processes did it undertake to definitively state there is a security problem with the connection?

The browser concluded that the connection to untrusted-root.badssl.com was not secure because the certificate presented by the site was not signed by a trusted CA. The browser performs checks on the certificate chain and its validity to determine if it is trustworthy.

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?

To permanently prevent the error message, you can manually add the site's certificate to your browser's trusted store (not recommended for general users due to security risks). Website maintainers should obtain a valid certificate from a trusted CA to prevent this message from displaying.

Bibliography

- Mozilla. (n.d.). Private Browsing - Use Firefox without saving history. Mozilla Support. Retrieved from https://support.mozilla.org/en-US/kb/private-browsing-use-firefox-without-saving-history
- Mozilla. (n.d.). Enhanced Tracking Protection in Firefox for desktop. Mozilla Blog. Retrieved from https://blog.mozilla.org/firefox/what-is-a-web-tracker/
- Mozilla. (n.d.). First-party and third-party cookies. Mozilla Developer Network. Retrieved from https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
- OWASP Foundation. (n.d.). Session Management. OWASP. Retrieved from https://owasp.org/www-project-top-ten/2017/A2_2017-Broken_Authentication.html
- Electronic Frontier Foundation. (n.d.). Do Not Track. EFF. Retrieved from https://www.eff.org/issues/do-not-track
- Adblocker Ultimate. (n.d.). How it works. Adblocker Ultimate. Retrieved from https://adblockultimate.net/
- Qualys SSL Labs. (n.d.). SSL/TLS Capabilities of Your Browser. SSL Labs. Retrieved from https://www.ssllabs.com/ssltest/viewMyClient.html
- Mozilla. (n.d.). Online Certificate Status Protocol (OCSP). Mozilla Developer Network. Retrieved from https://developer.mozilla.org/en-US/docs/Web/HTTP/OCSP
- Mozilla. (n.d.). Secure Websockets with SSL/TLS. Mozilla Developer Network. Retrieved from https://developer.mozilla.org/en-US/docs/Web/API/WebSockets_API/Writing_WebSocket_servers#secure_websockets_with_ssl/tls
- Team, Field Effect Security Intelligence. “Google and Mozilla Patch Browser Zero-Day Vulnerabilities.” *Field Effect*, Field Effect Software, 28 Mar. 2024, fieldeffect.com/blog/google-mozilla-patch-browser-zero-days.