Information Systems Security - IS 2109
Practical 1
Group - 7

1.

Web browser

1. The cookie file is stored in your browser's folder or subfolder.[1]

   Mozilla Firefox stores all the cookies, from all the websites that you visit, in a single file called *cookies.sqlite*. [2]

   Google Chrome stores all cookies in a single file called *Cookies*. The file is located at the following path: "**C:UsersYour User NameAppDataLocalGoogleChromeUser DataDefault**." [2]

2. On Windows 7 and Windows 8 computers, Chrome stores temporary internet files at "%LOCALAPPDATA%\Google\Chrome\User Data\Default\Cache" by default.

   Macintosh OS X computers, Chrome stores temporary internet files at "/Users/[user]/Library/Caches/Google/Chrome/Default/Cache" where "[user]" is the current user's username.

   Microsoft's Windows-only browser, Internet Explorer, stores temporary Internet files at "%LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files" by default. This folder is hidden by default.

   Firefox's temporary Internet files directory is "%LOCALAPPDATA%\Mozilla\Firefox\Profiles[profilename].default\Cache" by default for Windows 7 and Windows 8 where "[profilename]" is a sequence of random characters assigned to your profile.

   The Macintosh OS X version of Firefox stores temporary Internet files at "Users/[user]/Library/Caches/Firefox/Profiles/[profilename].default/Cache" where "[user]" is the current user's username and "[profilename]" is a sequence of random characters assigned to your profile.

   Safari, Apple's Mac-only browser, stores a single cache file named cache.db in the directory "/Users/[user]/Library/Caches/com.apple.Safari" where "[user]" is the current user's username. [3]

3. Google Chrome password file is located on your computer at C:\Users\$username\AppData\Local\Google\Chrome\User Data\Default

4. Google Chrome form fields is located on C:\Users\$username\AppData\Local\Google\Chrome\UserData\Default\AutofillStrikeDatabase

5. Bookmarks are stored in the Bookmarks file which is inside the Default folder of the respective web browser.

Internet Explorer keeps all of their bookmarks in your favorites folder (C:\users\<your user name>\favorites) as individual files [4]

On Chrome, it is stored in C:\Users\<pc_name>\AppData\Local\Google\Chrome\User Data\Default\Bookmarks

6. On Chrome, it is stored in C:\Users\<username>\AppData\Local\Google\Chrome\User Data\Default

2.

Web site certificates

1. Digital certificates are also used for sharing keys to be used for public key encryption and authentication of digital signatures.To establish an SSL session, our server always provides a copy of its certificate for validation by the client that requests a connection.

   Using an SSL connection assures the client or end-user that your site is authentic, and provides an encrypted communications session to ensure that data that passes over the connection remains private.

2.
   - Public key being certified
   - Information about the entity that owns the public key
   - Metadata relating to the digital certificate
   - Digital signature of the public key created by the issuer of the certificate.

3. Your web browser downloads the web server's certificate, which contains the public key of the web server. It uses this public key to verify that the web server's certificate was indeed signed by the trusted certificate authority. The certificate contains the domain name and/or ip address of the web server.

4. To validate the digital signature, the person authenticating the certificate will take the message of the certificate and then uses the same hash algorithm. If the two hashes match then the digital signature is valid and the certificate is authenticated.

5. Step 1: Select the Appropriate Certificate for Your Site

   Different types of SSL certificates are classified based on their validation levels as well as their functionality. Select the SSL certificate you wish to purchase, depending on your requirements.

   Step 2: Generate the Certificate Signing Request (CSR)

   A CSR is like an application that contains the details of the domain you're trying to secure using the SSL certificate.

   Step 3: Complete the Order Process

   Once you've completed the certificate signing request, you'll receive an order confirmation email from your certificate authority (CA) of choice with a link where you can submit your CSR.

   Step 4: Validation by Your Chosen Certificate Authority

   Once you've submitted the CSR using the link you received via email, your request will be verified and validated based on which certificate you chose in step 1. After the CA deems your request to be a legitimate one, they'll issue an SSL certificate for your website.

   Step 5: Install the SSL/TLS Certificate on Your Server(s)

You'll typically receive your SSL cert and any other intermediate certificates via your registered email. The SSL/TLS digital certificate, along with its certificate chain, will have to be installed on your server. You can refer to Sectigo's installation guide for additional information about how to install an SSL/TLS certificate on different servers.

6. The main problem related to web site certificates is occuring errors.
    - SSL Certificate Not Trusted Error
    - Name Mismatch Error
    - Mixed Content Error
    - Expired SSL Certificate Error

3.
Private Browsing

1. Private browsing makes sure to prevent information from being stored automatically into devices or being accessible by anyone through browsing histories or prone to cookies. Only files that have been bookmarked or downloaded alone would be accessible by way of private browsing mechanisms. Also it becomes very useful in saving personal details and decrease in unwanted ad pop ups.

2. When using your devices from a public place like restaurants or hotels or from common devices and networks like in a library.

   Where there is a need to login to multiple email accounts at the same time and use them simultaneously.

   To keep your online purchases a secret with regard to the items, price and online banking details.

   To research and find about delicate or intimate topics which you want it to be private. For example, about health concerns.

   To book a trip and travel accommodations. Where you can browse all your wishes without unnecessary ad interruptions and promotions.

3. <u>In Google Chrome</u>

   Here, it was designed to make it easier to share computers in public places. Chrome won't save your browsing history, cookies, site data, or information you enter on forms. It will only keep a record of files you download and your bookmarks.

How to do:

1. Open Chrome. Click on the tools menu in the upper right corner.
2. Choose “New Incognito Window” to open a new private browsing window.

The keyboard shortcut - press **Control+Shift+N** together.

In Safari

In here too, it removes temporary files such as browsing history, form data, and cookies by default when the window is closed.

To enable private browsing on a Mac:

1. Open Safari. Navigate to the menu bar and choose “File.”
2. Click on the “Private Window” option to open a private window.

The keyboard shortcut- press **Shift+Command+N**

To enable private browsing on an iPhone or iPad:

1. Tap the new tab icon in the lower right corner of the screen.
2. Click “Private” in the lower left corner to open a private window.

In Mozilla FireFox

Even though it is similar to the others, it offers an additional feature in the form of tracking protection. With this feature, Mozilla helps protect your browsing history from being gathered by third parties.

To enable private browsing in Firefox:

1. Open Firefox.
2. Go to the menu in the upper right corner and click “New Private Window.”
3. A new private window will appear with a purple mask icon in the top right of the Firefox window.

The keyboard shortcuts- **Control+Shift+N** for Windows, **Command+Shift+N** on a Mac.

You can turn on an additional tracking-protection feature on the purple band that is found across your Firefox private window.

In Internet Explorer

This also provides the same features as the others, where the browser won't save the pages you visit, form data, or web searches. When you close your InPrivate window, Microsoft's browsers also will disable third-party bars that were installed, along with extensions.

To enable Private browsing on Internet Explorer:

1. Open Internet Explorer. Click on the gear icon in the upper right corner.
2. Choose "Safety" from the drop-down menu.
3. Then choose "InPrivate Browsing" to open a private window.

The keyboard shortcut- press **Control+Shift+P**.

To enable Private browsing on Microsoft Edge:

1. Navigate to the menu (three dots in a row) in the upper right corner.
2. Choose "New InPrivate window" to open a private window.

While in this private mode, the browser tabs will say "InPrivate."

In Opera Incognito

Even though this too is similar to the others, an additional feature enables you to turn on its own VPN connection that could further protect your browsing activities.

To enable Opera incognito:

1. Open the Opera browser. Click the menu in the upper left corner.
2. Choose "New Private Window" to open a private browsing window

4.Tracking Protection is a new platform-level technology that blocks HTTP loads at the network level. It is based on the safe browsing technology that powers our phishing and malware protection. It helps to mitigate
invasive tracking of users' online activity by blocking requests to tracking
domains. It was demonstrated that there was a 67.5% reduction in the
number of HTTP cookies set during a crawl of the Alexa top 200 news sites.

5. It never hides our activities on a network level where its still prone to hackers and even higher authorities in your organization.

There's a need to activate it and open especially when needed to use it. So it takes some amount of time to actually get used to the process.

It still allows advertisers to track the searches.

Downloaded data would be present to be seen by all and can be accessible at all times.

You can be browser fingerprinted.

DNS queries can reveal your access.

4.
Using web proxies

1. Every computer on the internet needs to have a unique Internet Protocol (IP) Address. The internet knows how to send the correct data to the correct computer by the IP address.A proxy server is basically a computer on the internet with its own IP address that our computer knows. When we send a web request, our request goes to the proxy server first. The proxy server then makes our web request on your behalf, collects the response from the web server, and forwards you the web page data so you can see the page in your browser.

   When the proxy server forwards your web requests, it can make changes to the data we send and still get us the information that we expect to see. A proxy server can change our IP address, so the web server doesn't know exactly where you are in the world. It can encrypt your data, so your data is unreadable in transit. And lastly, a proxy server can block access to certain web pages, based on IP address.

2. A proxy server will provide us with security and anonymity, the proxy itself has to decode our traffic to send it through. This means it can see everything we're doing, unless you use SSL connections. So we need to trust it.

   A lot of people use TOR, which is a free anonymity network run by volunteers, or some go to underground channels to get so-called "private" proxies, but the problem is we never know if we can trust those servers. It may end up being worse than not using a proxy at all.

   Popular commercial services like Hide My Ass base their business on providing this service, so personally I have more faith in them.

   People think of using them for criminal acts however, since they do state clearly that they cooperate with law enforcement.

   The proxy server is the one party that knows our real IP address.

Using proxies will typically slow our connection down, since we're basically transferring all our data to another location around the world before it goes out to the Internet. As we attempt to connect to various proxy servers, we may find very big differences in speed, so it's a good idea to try them out. Whether we want security, anonymity, or both, proxies provide a good way to surf the net.

3 .

- Reverse Proxy
  This represents the server. In case there are multiple websites on different servers then it is the job of a reverse proxy server to listen to the request made by the client and redirect to the particular web server.

- Web Proxy Server
  This type of proxies forward the HTTP requests. This request is the same as HTTP requests, only the URL is passed instead of a path. Request is sent to which the proxy server responds. Examples of such proxies are Apache, HAPProxy.

- Anonymous Proxy
  This is the type of proxy server that does not make an original IP address. Although these servers are detectable, they still provide rational anonymity to the client device.

- High Anonymity Proxy
  This type of proxy server does not allow the original IP address to be detected and also no one can detect it as a proxy server.

- Transparent Proxy
  This type of proxy server never provides any anonymity to the client, instead, the original IP address can be easily detected using this proxy. Still, it is being used to act as a cache for the websites.

- CGI Proxy
  This type of proxies were developed to make the websites more accessible.

- Suffix Proxy
  This type of proxy server appends the name of the proxy to the URL to the content that has been requested to the proxy. This type of proxy doesn’t preserve a higher level of anonymity.

- Distorting Proxy

Proxy servers can generate an incorrect original IP address of clients once being detected as a proxy server. It uses HTTP headers to maintain the confidentiality of the Client IP address.

- TOR Onion Proxy
  It is a software that aims at online anonymity to the users personal information.

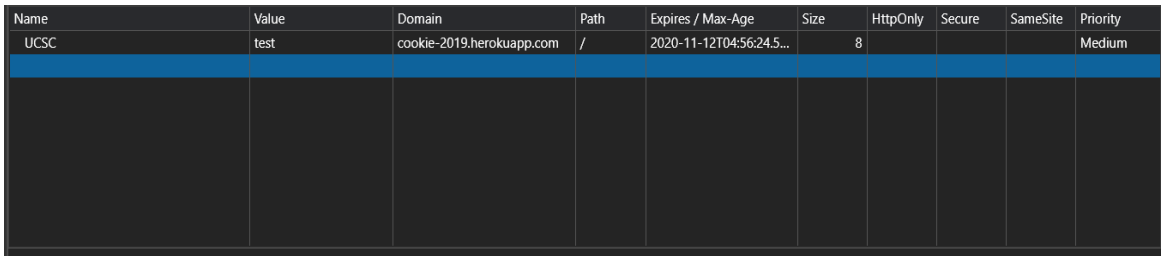
- I2P Anonymous Proxy
  It is an anonymous network enhanced version of Tor onion proxy which uses encryption to hide all the communications at various levels. This encrypted data is then relayed through various network routers present in different locations.

- DNS Proxy
  Unlike other proxies, this type of proxy takes requests in the form of DNS queries and forward them to the Domain server where it can also be cached and flow of requests can also be redirected.

5.

Cookies

i. There is one cookie named UCSC and the value is tested.



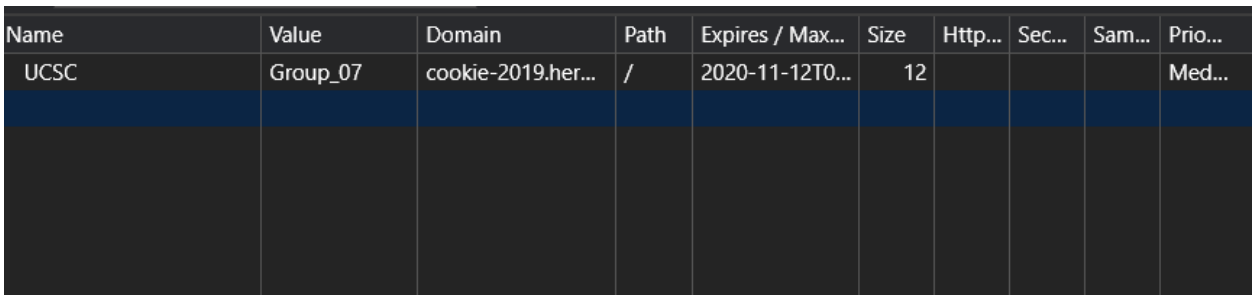
Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Priority
UCSC	test	cookie-2019.herokuapp.com	/	2020-11-12T04:56:24.5...	8				Medium

ii.

```
You set a new cookie
{
name : UCSC
value : University_of_Colombo_School_of_Computing
}
```

New Cookie:
Name: UCSC
Value: University_of_Colombo_School_of_Computing

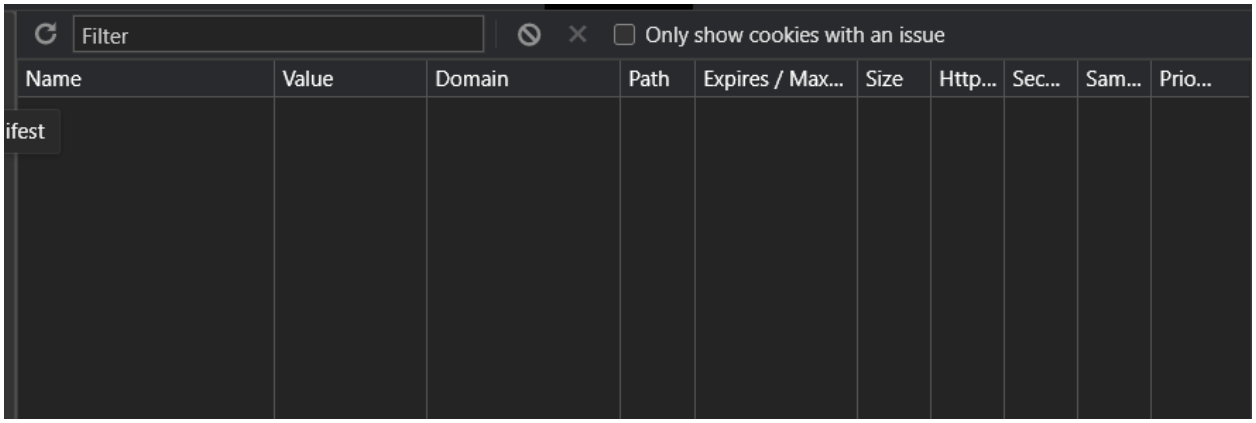
iii.



Name	Value	Domain	Path	Expires / Max...	Size	Http...	Sec...	Sam...	Prio...
UCSC	Group_07	cookie-2019.her...	/	2020-11-12T0...	12				Med...

We have Changed the value of the cookie to “Group_07”

iv.



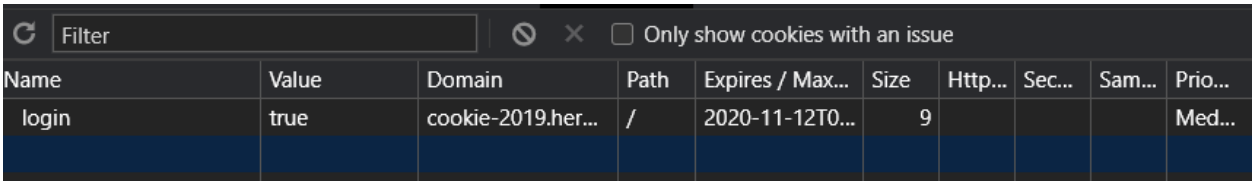
Cookies were destroyed

v.

We cant log in to the provided URL since there are no any cookies created.

```
Internal Server Error
```

With the URL https://cookie-2019.herokuapp.com/v1/login?id=lasith&key=YouCantGuessThis
A cookie is created with the name ‘login’ and value ‘true’ .



Then we can see this .

```
Login successful!!!
Welcome
```

References

[1] - https://www.allaboutcookies.org/faqs/cookie-file.html
[2] - https://www.digitalcitizen.life/cookies-location-windows-10
[3] - https://smallbusiness.chron.com/temporary-internet-files-stored-hard-drive-71225.html
[4] - https://www.ag.ndsu.edu/accs/hardware/bookmarks
[5] - https://support.mozilla.org/en-US/questions/833585

https://us.norton.com/internetsecurity-privacy-your-private-browser-is-not-so-private-after-all.html#:~:text=The%20goal%20of%20private%20browsing,bookmarked%20may%20still%20be%20saved

https://smallbusiness.chron.com/purpose-private-browsing-71226.html

https://www.sciencedirect.com/topics/computer-science/private-browsing

https://us.norton.com/internetsecurity-privacy-what-is-private-browsing.html#:~:text=Private%20browsing%20is%20a%20feature,and%20cookies%20aren't%20retained.

https://wiki.mozilla.org/Security/Tracking_protection#:~:text=Tracking%20Protection%20is%20a%20new,our%20phishing%20and%20malware%20protection.

https://kingpinbrowser.com/blog/disadvantages-incognito-mode/