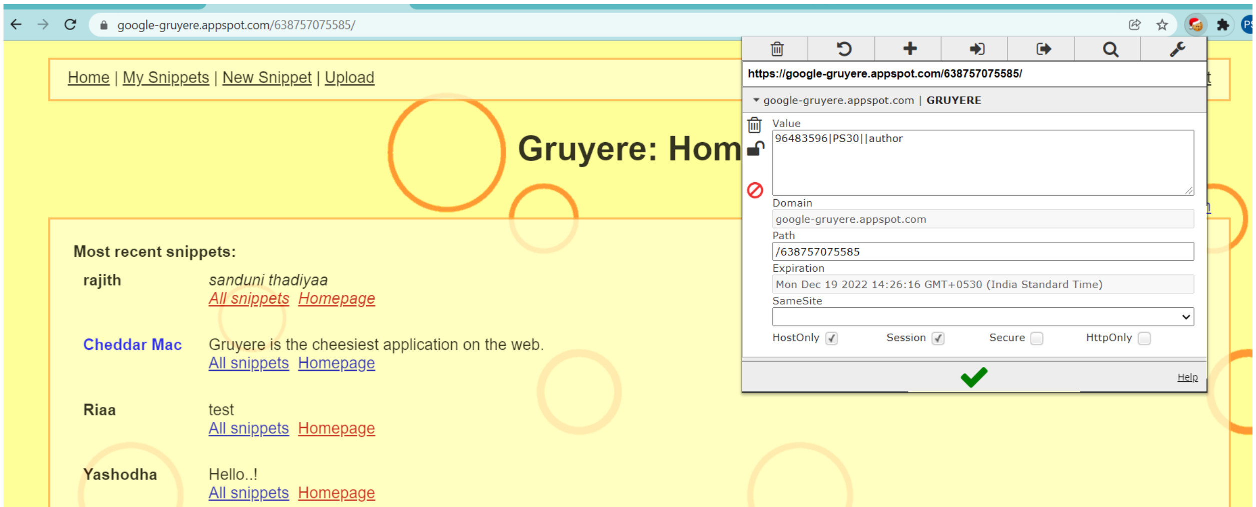
Question 1



google-gruyere.appspot.com/638757075585/

Gruyere: Hom

Most recent snippets:

rajith	*sanduni thadiyaa* *All snippets* *Homepage*
Cheddar Mac	Gruyere is the cheesiest application on the web. All snippets Homepage
Riaa	test All snippets Homepage
Yashodha	Hello..! All snippets Homepage

https://google-gruyere.appspot.com/638757075585/

google-gruyere.appspot.com | GRUYERE

Value: 96483596|PS30||author

Domain: google-gruyere.appspot.com

Path: /638757075585

Expiration: Mon Dec 19 2022 14:26:16 GMT+0530 (India Standard Time)

SameSite:

HostOnly ☑ Session ☑ Secure □ HttpOnly □

- **Explain 2 vulnerabilities of the site at a glance.**

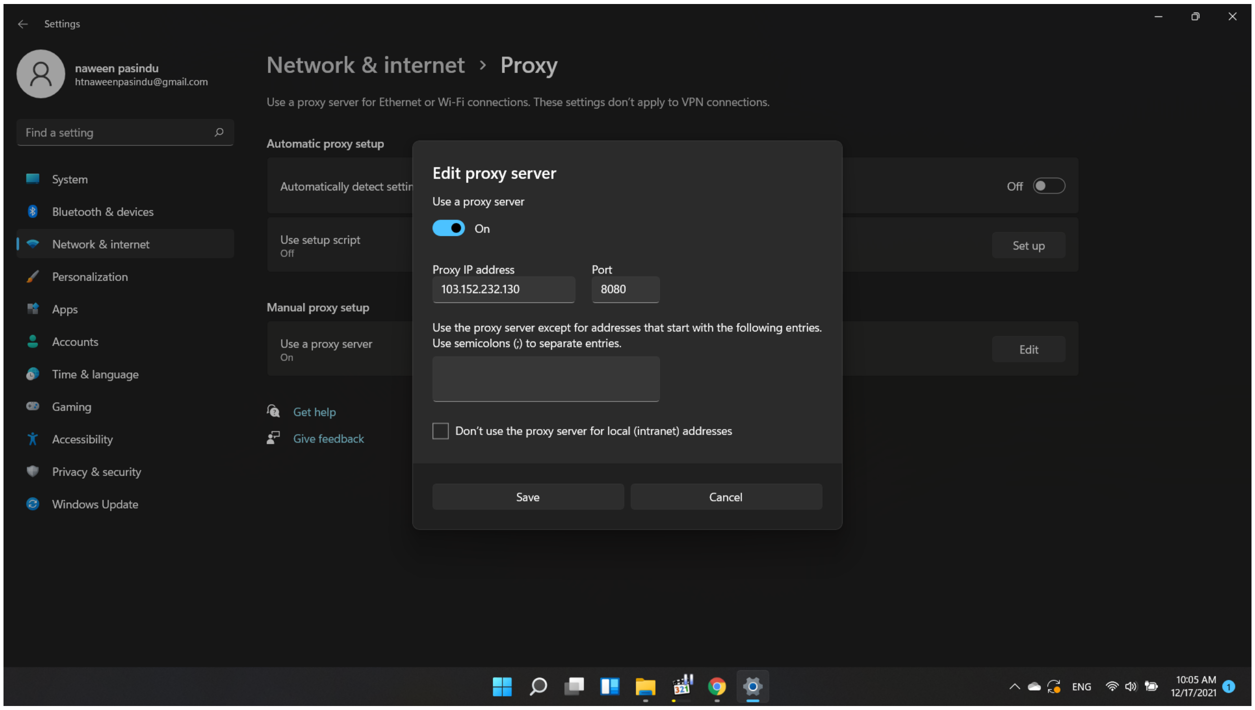
- **Is it legal to perform the above task on this site?**
  Yes, this site is for testing purposes

- **Is it legal to perform the above task on other sites? If not, under which act you will get punished according to the Sri Lankan law?**
  NO,
  The Cookie Law is a privacy law that mandates that websites obtain visitors' permission before storing or retrieving any information on a computer, smartphone, or tablet.
  It was created to defend online privacy by informing customers about how personal data is gathered and used online and providing them the option of allowing or disallowing it.

  Act to Provide for the Regulation of Processing of Personal Data (July 2021)

Question 2

Find your IP address online. Find the location and the owner/provider of the IP address. Use a proxy server and now what is your IP address. What are the advantages of using a proxy server?



Network & internet › Proxy

Use a proxy server for Ethernet or Wi-Fi connections. These settings don't apply to VPN connections.

Automatic proxy setup

Automatically detect settin Off

Use setup script Off Set up

Manual proxy setup

Use a proxy server On Edit

Edit proxy server

Use a proxy server

On

Proxy IP address 103.152.232.130

Port 8080

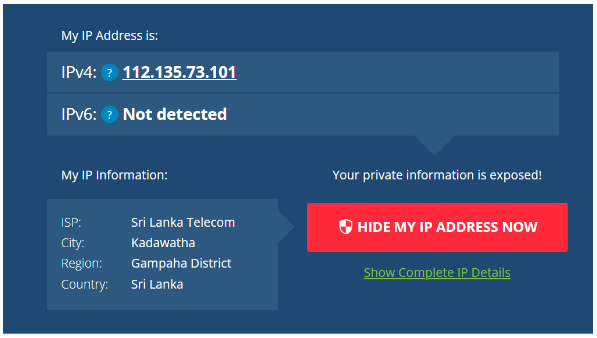
Use the proxy server except for addresses that start with the following entries. Use semicolons (;) to separate entries.

□ Don't use the proxy server for local (intranet) addresses

Save Cancel

How to set a proxy in Windows 11

Before using a proxy server,



My IP Address is:

IPv4: 112.135.73.101

IPv6: Not detected

My IP Information:

ISP:	Sri Lanka Telecom
City:	Kadawatha
Region:	Gampaha District
Country:	Sri Lanka

Your private information is exposed!

HIDE MY IP ADDRESS NOW

Show Complete IP Details

IP Address	: 112.135.73.101
ISP	: Sri Lanka Telecom
City	: Kadawatha
Region	: Gampaha District
Country	: Sri Lanka

After using a proxy server,

IP Address	: 103.152.233.10
ISP	: PT Kingpolah Network Solutions
City	: Bekasi
Region	: West Java
Country	: Indonesia

A proxy server provides a gateway between the users and the internet,resulting in preventing the cyber attacks that try to enter to the private network.Some Advantages of proxy server are,

Keeps a user's IP address hidden from criminals
Ability to access restricted content outside your region and geo blocked content or because your IP address is hidden
Displays cached pages faster when requested(pages will load faster)

Improves security and privacy
Can also be use to restrict unwanted content and filter out malicious websites
System will not be exposed to any malicious sites or phishing attacks easily
Proxy servers can also be used to load-balance workloads across many content HTTP servers, each servicing their own application area, in the reverse manner.
Can act as a firewall and a web filter providing content efficiently.
Balances off internet traffic in order to avoid crashes
Users can browse internet and perform tasks anonymously

Question 3

- **Explain 2 best practices to login to your accounts in a public computer.**

1) Don't Stay Logged Into Websites

   When a user logs into an account through a public or private computer, it automatically prompts him/her to stay signed in even after closing the browser. While this makes life easier for personal surfing, it is not recommended to do so on a public computer. That is because it is a shared computer that someone else could also log on to. If so, the previously logged users data and privacy might be at risk. Therefore, whenever someone logs into their account via a public computer, they should keep an eye out for a “Keep me signed in” or similar box. Sometimes these are checked by default, so the users must make sure to clear the box before logging in. Also, making sure to sign out once a user is done working on a site that requires a login is also a must when using a public computer. Do not assume that closing the browser window will end the session. If by mistake the user does not sign out, their session could be preserved for the next person that comes along. Even if this doesn't expose their credentials, leaving an account open for others to access could lead to them changing settings, sending nasty messages to friends, or similar.

2) Use Private Browsing

   An alternative to deleting the history (and a simpler method) is to use the incognito or private browsing mode. Every modern browser has one; these prevent the browser from saving any history, cookies, or other browsing data from your session. Therefore when a user uses private browsing through a public computer, they don't need to clear the history when they're done, as the browser deletes it all upon closing the window. This also ends any sessions they were signed into, so they don't need to sign out manually.Nothing they do in private browsing is saved. However, private browsing does not make a user invisible, though. The network administrator can still potentially see what he/she is doing.

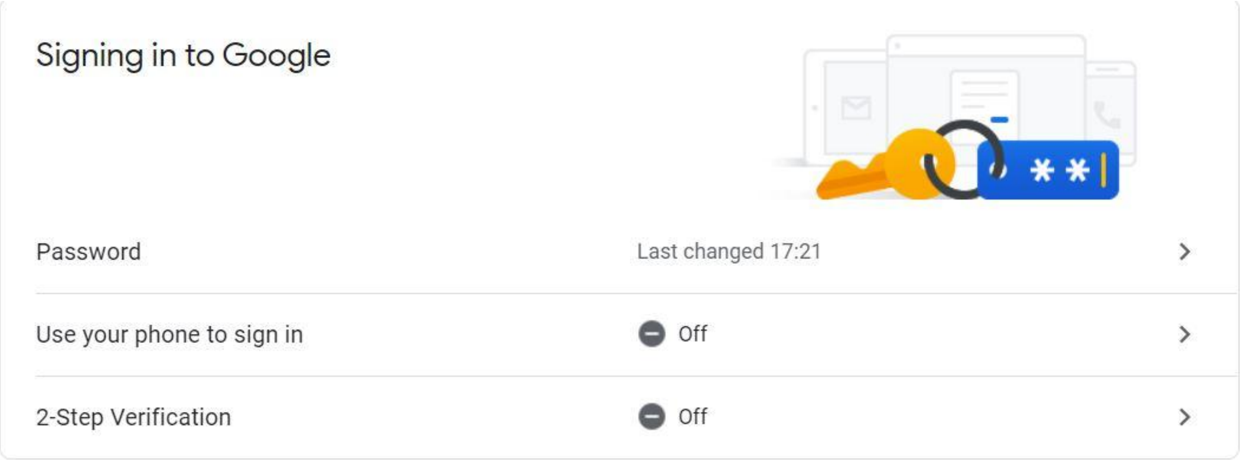
- **Use the above proxy server to login to the Gmail account and explain the security issue and the options provided by google while you are logging in.**

There weren't any security issues. But languages were automatically changed. Some websites required to pass the “I am not a robot test”.

- **What is the threat of submitting passwords through a proxy server?**

Proxies are also vulnerable to security exploits: they can be open to attack, allowing the hackers and other anonymous sources to infiltrate networks or steal private data. Some proxies can still track (and store) users browsing habits, as well as record usernames and passwords – rendering that promise of anonymity null.

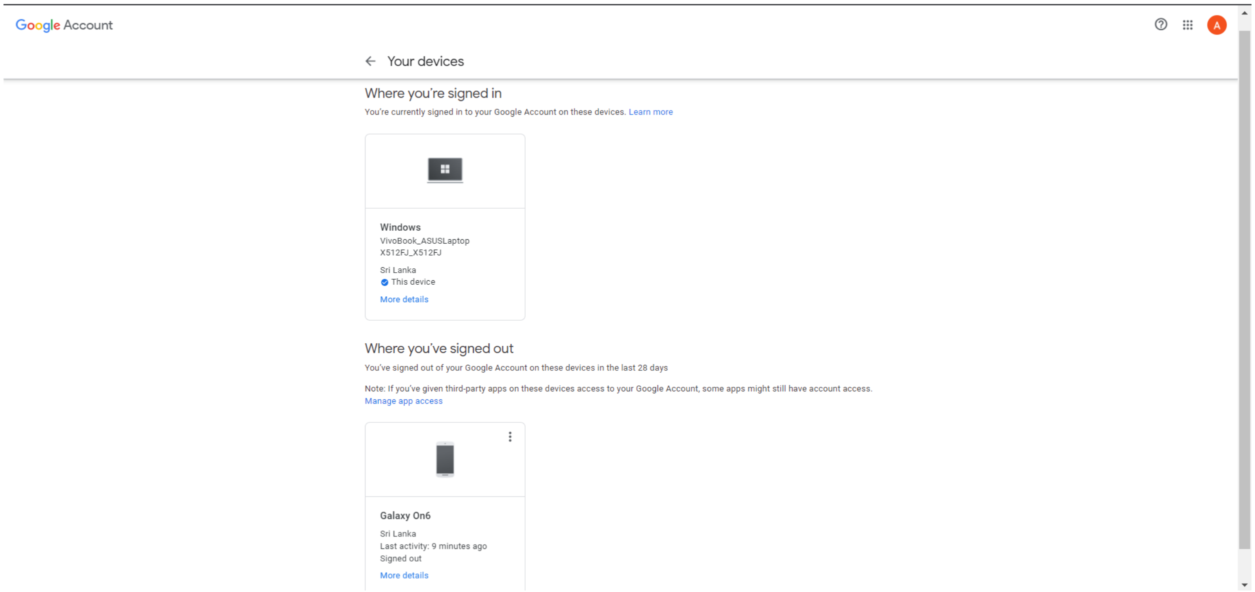
- **Logout from the account and change the password without the proxy server.**



Signing in to Google

Password	Last changed 17:21
Use your phone to sign in	⊖ Off
2-Step Verification	⊖ Off

- **Find out information about the recent devices logged in and suspicious security issues in your account.**



Google Account

Your devices

Where you're signed in

You're currently signed in to your Google Account on these devices. Learn more

Windows
VivoBook_ASUSLaptop
X512FJ_X512FJ
Sri Lanka
✓ This device
More details

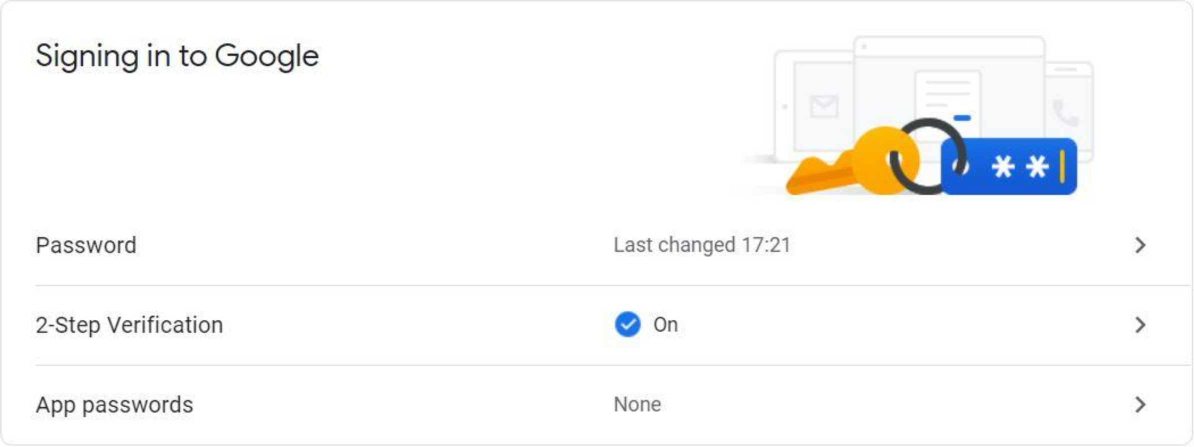
Where you've signed out

You've signed out of your Google Account on these devices in the last 28 days

Note: If you've given third-party apps on these devices access to your Google Account, some apps might still have account access.
Manage app access

Galaxy On6
Sri Lanka
Last activity: 9 minutes ago
Signed out
More details

- **Activate 2-way authentication.**



Signing in to Google

Password	Last changed 17:21	>
2-Step Verification	✓ On	>
App passwords	None	>

- **What are the different options Google gives you to access the account when you forgot your password?**

  1) Follow the steps to recover your Google Account or Gmail.

     - You'll be asked some questions to confirm it's your account. Answer as best you can.
     - If you have trouble, try the tips to complete account recovery steps.

  2) Reset your password when prompted. Choose a strong password that you haven't already used with this account. Learn how to create a strong password.

- **List down modern day authentication mechanisms and their advantages?**

1) Passwords

A password is a shared secret known by the user and presented to the server to authenticate the user. Passwords are the default authentication mechanism on the web today. Advantages of passwords include,

- Least expensive
- No need to install any hardware devices

2) Hard Tokens

Hard tokens are small hardware devices that the owner carries to authorize access to a network service. The device may be in the form of a smart card, or it may be embedded in an easily-carried object such as a key fob or USB drive. The device itself contains an algorithm (a clock or a counter), and a seed record used to calculate the pseudo-random number. Users enter this number to prove that they have the token. The server that's authenticating the user must also have a copy of each key fob's seed record, the algorithm used and the correct time. Advantages of hard tokens are,

- Users don’t need to remember complex passwords
- Can be used for login and transaction authentications
- Can secure user credentials more effectively
- Enhances privacy

3) Soft Tokens

Soft Tokens are software-based security token applications that typically run on a smartphone and generate an OTP for signing on. Users are less likely to forget their phones at home than lose a single-use hardware token. When they do lose a phone, users are more likely to report the loss, and the soft token can be disabled. Soft tokens leverage mobile phones' ability to generate an OTP and, possibly, their communication network. A user can demonstrate possession of his/her previously registered phone by receiving a message sent to that device. An OTP can be sent to the phone by SMS, voice call, or with an app that receives an authentication prompt via the mobile OS notification services, which is then entered by the user into a sign-on screen. In mobile-based solutions, it's more common to rely on an application installed on the mobile device. Instead of sending an SMS to the phone number, the authentication server can send a notification to the mobile app, which prompts the user for some action (e.g., 'Swipe your screen' or 'Apply your fingerprint'). Some advantages of using soft tokens are given below.

- Less expensive
- Easier to distribute
- Greater trust of authenticity

4) Biometric Authentication

Biometric authentication methods include retina, iris, fingerprint and finger vein scans, facial and voice recognition, and hand or even earlobe geometry. The latest phones are adding hardware support for biometrics, such as TouchID on the iPhone. Biometric factors may demand an explicit operation by the user (e.g., scanning a fingerprint), or they may be implicit (e.g., analyzing the user's voice as they interact with the help desk). Advantages of biometric authentication include,

- Difficult to compromise
- Can be used for accessing high-security systems and sites
- As information is unique to each individual, it can identify any person in spite of variations in the time
- Different options such as retina, iris, fingerprint scanner authentication is available

5) Contextual Authentication

Contextual authentication collects signals like geolocation, IP address and time of day in order to help establish assurance that the user is valid. Typically, a user's current context is compared to previously established context (or blacklists/whitelists) in order to spot inconsistencies and identify potential fraud. These checks are invisible to the authorized user, so there are no usability issues, but they can create a significant barrier to an attacker. Contextual signals can be collected by methods such as the web pages where they authenticate, the mobile devices used for MFA, other sensors in proximity to the user (wearables, smart watches). Once collected and aggregated, the authentication server can analyze these signals to look for anomalous patterns that might indicate an attack or fraudulent behavior. Advantages of contextual authentication are,

- Constantly retrieves structured information from users and profile users through active classification and inference.
- Authentication can be done dynamically
- Improves the usability of authentication

Question 4

What is the first step Google would perform in order to classify your email according to the priorities?

Gmail's priority inbox feature isn't turned on by default. This feature separates the contents of your standard inbox into sections: Important and Unread, Important and Unread, Starred, and Everything Else. You have the option of picking and choosing which of them to employ. Gmail determines what you're likely to recognize as important based on variables such as how you treated similar messages in the past, how the message is addressed to you, and other factors, and places those emails in the Important and Unread area.

Each email has a significance marker to the left of the sender's name in the Inbox list. It has the appearance of a flag or an arrow. When Gmail determines that an email is essential based on its criteria, the importance marker turns yellow.

By clicking the importance marker, user can change its status manually at any time. Hover users' cursor over the yellow flag to see why Gmail considered a specific email to be essential. Simply click the yellow flag to dismiss it if you disagree. Gmail will know which emails users consider as important after the user completes this step.