WAS 2015: TP 2

1. (File: integrator.html) Look at the code of integrator.html and write code for evilGadget.js in such a way that evilGadget.js will send the secret to an untrusted server. How do you rewrite integrator.html so the same origin policy will protect the secret?

2. (File: simplemashup.html)
   - Understand the code and execute the file
   - Disconnect from the internet and execute the file. What happens? Justify.
   - Modify the file so the application uses the method Geocoder of google maps. Instead of using Lat and Lng, let the parameter for the name of a city be sent to the server in order to configure where the map is centered.
   - Insert the gadget (third line, script tag) in a frame. What happens with the functionality now? Justify

3. (No file) Write a web application .php that corresponds to a mashup on a client side (part of the code displayed in the browser comes from your .php server and part of the code, the gadget, comes from another server, you can install apache for another port for example). The application should have an input box: every character entered by the user should be sent to the gadget server. Explain the security risks of this application.

4. (File: cookieweird.php) Execute this file and explain the behaviour.

5. (No file) Write two different services from the same server that set a cookie. On the client side include a gadget and try the following things:
   - let the gadget delete the cookie via JavaScript (a cookie can be deleted by setting a date in the past)
   - Can the second service delete the cookie of the first? Justify why.
   - let the gadget send the cookie to another server (you can use a different port to simulate this)
   - Does the previous item work if the gadget is inside a frame? and if gadget is inside a script and the cookie is initially set as httponly?and if gadget is in script and the cookie is initially set as secure? Justify all your answers.