TP

1) 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 evil.com. Rewrite integrator.html so the same origin policy will protect the secret.
2) Look at the sop2.html. From subdomain2.html try to read the secret from the integrator, what happens according to SOP? How do you read the secret by using document.domain?

TP cont.

3. 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
- 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 the gadget is inside a script and the cookie is initially set as httpOnly?
- and if the gadget is inside a script and the cookie is initially set as secure?

Justify all your answers with code and explanations.

4. Implement a CSRF attack and explain then demonstrate what kind of SameSite cookie can mitigate this attack.