# Computer Security (COM-301)

## Monday Live Exercises

## Adversarial Thinking -CWEs

**Carmela Troncoso**

SPRING Lab

carmela.troncoso@epfl.ch

# Integrity means safety

Recall Cross Site Request Forgery (CSRF), in which an adversary exploits the use of cookies in HTTP sessions to act as the user in a website.

(a) Would CSRF be avoided if we ensure that browser and server agree on a symmetric key and use a MAC to ensure integrity of the message?

# Integrity means safety

Recall Cross Site Request Forgery (CSRF), in which an adversary exploits the use of cookies in HTTP sessions to act as the user in a website.

(a) Would CSRF be avoided if we ensure that browser and server agree on a symmetric key and use a MAC to ensure integrity of the message?

(b) Would CSRF be avoided if we digitally sign the content **of the message sent to the** website?

# Integrity means safety

Recall Cross Site Request Forgery (CSRF), in which an adversary exploits the use of cookies in HTTP sessions to act as the user in a website.

(a) Would CSRF be avoided if we ensure that browser and server agree on a symmetric key and use a MAC to ensure integrity of the message?
(b) Would CSRF be avoided if we digitally sign the content **of the message sent to the** website?

**Answer**
CSRF is not an integrity problem. The adversary **does not** modify the information that is sent to the server. They also do not spoof the identity of the sender (the browser).
The vulnerability the adversary exploits is the fact that the browser uses ambient authority, to misuse the cookies stored by the browser.

Therefore, integrity-oriented mechanisms (MAC / Digital signature) or origin authentication mechanisms (Digital signature) are not a good mitigation for this problem.

# Which of these are true?

To do a cross site scripting attack (XSS) it is essential that:

(a) Cookies hold authentication information

(b) It is possible to abuse the privileges of a confused deputy

(c) There is a web form to feed Javascript code to the server

(d) The input received by the server is not correctly sanitized

# Which of these are true?

To do a cross site scripting attack (XSS) it is essential that:

(a) Cookies hold authentication information

(b) It is possible to abuse the privileges of a confused deputy

(c) There is a web form to feed Javascript code to the server

(d) The input received by the server is not correctly sanitized

**Answer**
(d) XSS works because input are not sanitized.

They do not use cookies, or do not abuse ambient authority. There needs not to be a webform, code can be injected in other ways

# Protecting from web attacks

TRUE or FALSE. Justify.

(a) http://www.coolvids.com:3000/index.html is in the same origin as http://coolvids.com:3000/index.html.

(b) If Tyrion uses a browser with no code vulnerabilities and uses a unique, long password for every website he visits, then he will be safe against phishing attacks.

(c) The Same Origin Policy prevents XSS attacks if a browser implements it correctly

(d) Sanitization can help preventing phishing

# Protecting from web attacks

TRUE or FALSE. Justify.

(a) http://www.coolvids.com:3000/index.html is in the same origin as http://coolvids.com:3000/index.html.

(b) If Tyrion uses a browser with no code vulnerabilities and uses a unique, long password for every website he visits, then he will be safe against phishing attacks.

(c) The Same Origin Policy prevents XSS attacks if a browser implements it correctly

(d) Sanitization can help preventing phishing

**Answer**

(a) **False**: those addresses resolve to different IPs, i.e. hosts => different origin

(b) **False**: phishing does not rely on vulnerabilities or on learning/inferring credentials. Tyrion can be spoofed by using a mock of one of the websites, and his unique, long, excellent password will be stolen

(c) **False**: XSS does not depend on origin!

(d) **False**: similar to Tyrion's case (b), sanitizing does not prevent phishing. A web with no dangerous elements, but from a wrong / spoofed origin, can still be used to steal credentials.
**True**: an argument that a SPAM filter sanitizing links can exist could be considered as support for phishing prevention