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?

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

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