oasis digital .com

https://www.MyBank.com

web server

https://www.evil-flash-games.com

web server

POST /transfer

GET /balance

XXXX

POST /highscore

GET blah.swf

Joe User's Web Browser

$$$$$

Transfer $
Read Statement

Fun evil Flash
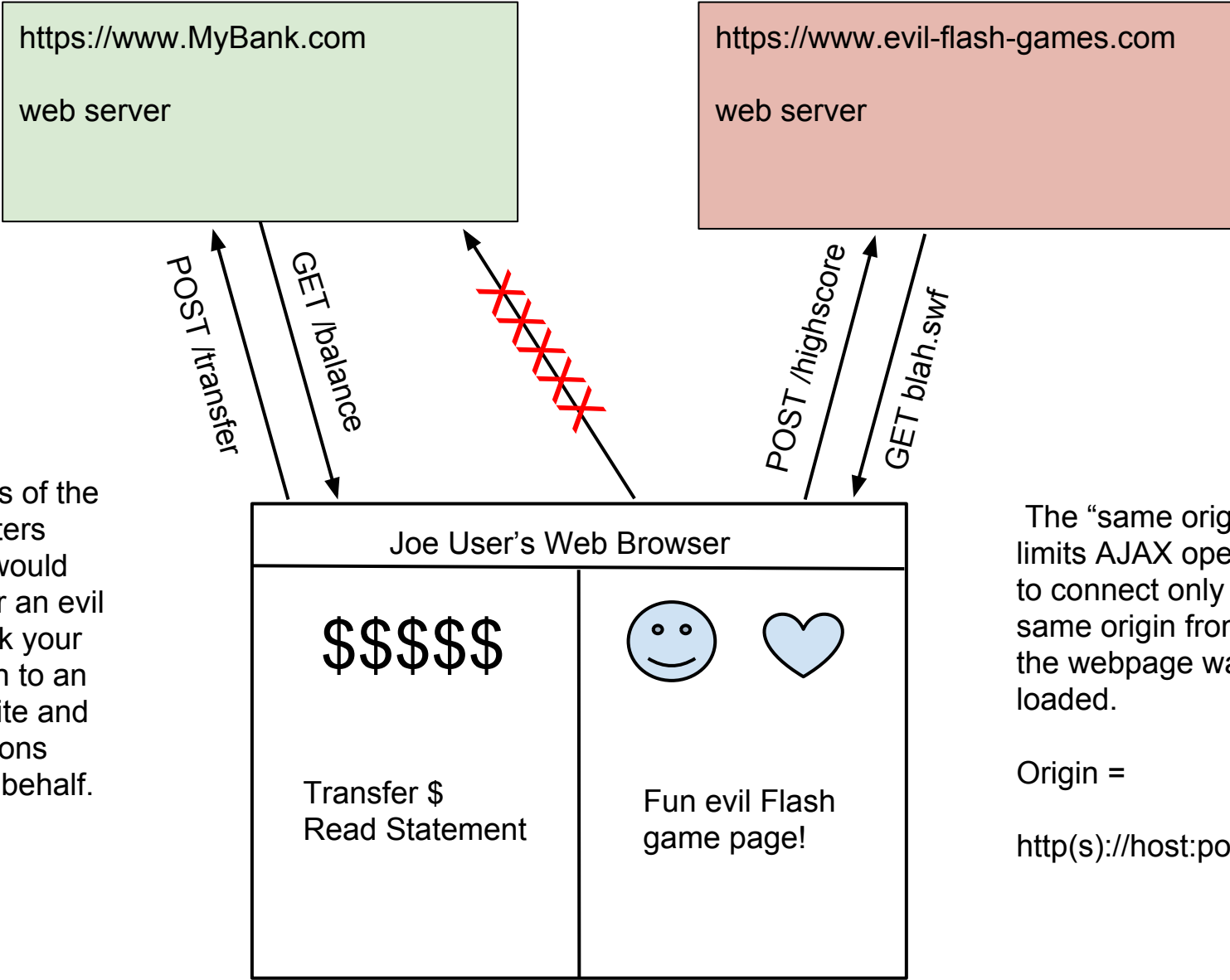game page!

In the early days of the web, implementers realized that it would be very easy for an evil website to hijack your login/connection to an important website and execute operations silently on your behalf.

The "same origin policy" limits AJAX operations to connect only to the same origin from which the webpage was loaded.

Origin =

http(s)://host:port/