### Assignment 6: The HTML canvas element

The canvas HTML element creates a 2D rectangular area and lets Javascript draw whatever it wants in that area. Canvas is used for client-side graphics such as drawing a path on a map loaded from Google maps. For the purpose of the associated same-origin policy, the origin of a canvas is the origin of the content that created it. In the map example, the origin of the Javascript that creates the canvas is Google. Canvas lets Javascript read pixels from any canvas in its origin using the *GetImageData()* method.

1. Canvas lets Javascript embed images from any domain in the canvas. Suppose a user has authenticated to a site that displays private information. Describe an attack that would be possible if Javascript from one domain could embed an image from another domain in the canvas and then use *GetImageData()* to read pixels from that image.
2. How would you restrict GetImageData() to prevent the attack above?
3. A canvas element can be placed anywhere in the browser content area and can be made transparent so that the underlying content under the canvas shows through. What security problem arises if calling *GetImageData()* always returned the actual pixels shown on the screen at that position?
4. How would you design *GetImageData()* to defend against the vulnerability from part (c)? Propose a design that does not require the browser to test if the requested pixel is over content from another origin.