CRSF in One Slide

CS 5340

CSRF Picture

- You visit Badguy.com
- But you are logged in to BOA.com
- The webpage for Badguy.com that you are viewing in your browser makes a request to BOA.com. Such a request is called a cross-site request
- The request succeeds because the browser sends your cookies over to BOA.com along with the request to BOA.com, causing it to trust that the request comes from you.
- To do this request, the bad guy could embed a link in his website and hope that the victim clicks it. Or he could do it in an automated way, such as using javascript. But a much simpler way would be using img tags (if the HTTP service being targeted uses GET) as these trigger a GET request as the page loads.
- The bad guy constructs a correct request by doing initial surveillance on BOA.com to see how the transaction of interest sends data.