Cross-site Scripting (XSS)

- Same origin policy
  o Only the creator of the cookie can access it
- XSS is a way to fool the cookie
- Bad guy submits 2 scripts
  o One to the forum on a site to get cookies from users
  o One to get the cookies from the forum site for the use
- Solutions:
  o Filters – white list is more effective because there are many ways to apply JavaScript tag like onMouseClick
  o Custom tags

Cross-site Request Forgery (CSRF)

- Bad guy sends transfer request from your machine.
  1. User clicks a link from the bad guys email or website
  2. His website sends a request to the bank site to attempt to steal his money
  3. The bank site has to have an active session with the user at the time this happens
- Defenses
  o Put a random number in the request so the Bad Guy’s request wouldn’t be executed

Error Messages

- Get error message with SQL information
- Bad guy can cause error to get the message
- Solutions:
  o Standard single page for all errors

Tracfor Beaming Attack

- UNIX
  o Read uid 1001
  o Effective uid 1001->0
  o Program can swap them
- FTP Server
  o After login
  o Event loop(){
  o Do special command ()
  o Set uid(0)
  o if () throw exception
- we are setting the user Id to zero than throwing exception so it goes out of the loop without resetting it to the ordinal value

  - solutions:
    - catch exception: set block to normal
    - only one exit to the function
    - ftp server doesn’t have root
    - every time you come to the event loop rest
    - transaction :
    - control the scope and don’t allow dynamic scoping.