Project 3 – Web Security Part 2

CS155 – Indrajit "Indy" Khare

Outline

- Administrative
- Requirement Overview
- Attack A Defenses
- Attack B Defenses
- Attack C Defenses
- Attack D Defenses
- Extra Fun Defenses
- Other Notes

Administrative

- Due Monday June 1st
- No more late days are allowed
- Setup cgi-bin on your su network account TODAY (linked from instructions)

Requirements

- Defend against all known attacks from Part 1
- Defend against all XSS an XSRF in zoobar.org (except login)
- Make sure you read non-goals section in assignment
  - Don't add any new files
  - Don't change DB
  - Don't edit files in includes/

Attack A Defenses

- The attack is a simple XSS
- How do defend?
  - Do output sanitization
- From class:
- PHP: htmlspecialchars(string)

  & → & " → " ' → '
  < → < > → >

  - htmlspecialchars(
    "Test", ENT_QUOTES);
    Outputs:
    Test

Attack B Defenses

- Simple XSRF (CSRF)
- How to Defend:
  - Secret Token
    - Ideally you use some HMAC with a secret
    - For this project you can simply hash the session token
    - Look at includes/auth.php for a lot of helpful code