LAB SESSION 4

ACCESS CONTROL
SESSION INFORMATION STEALING

TU/e Technische Universiteit Eindhoven University of Technology

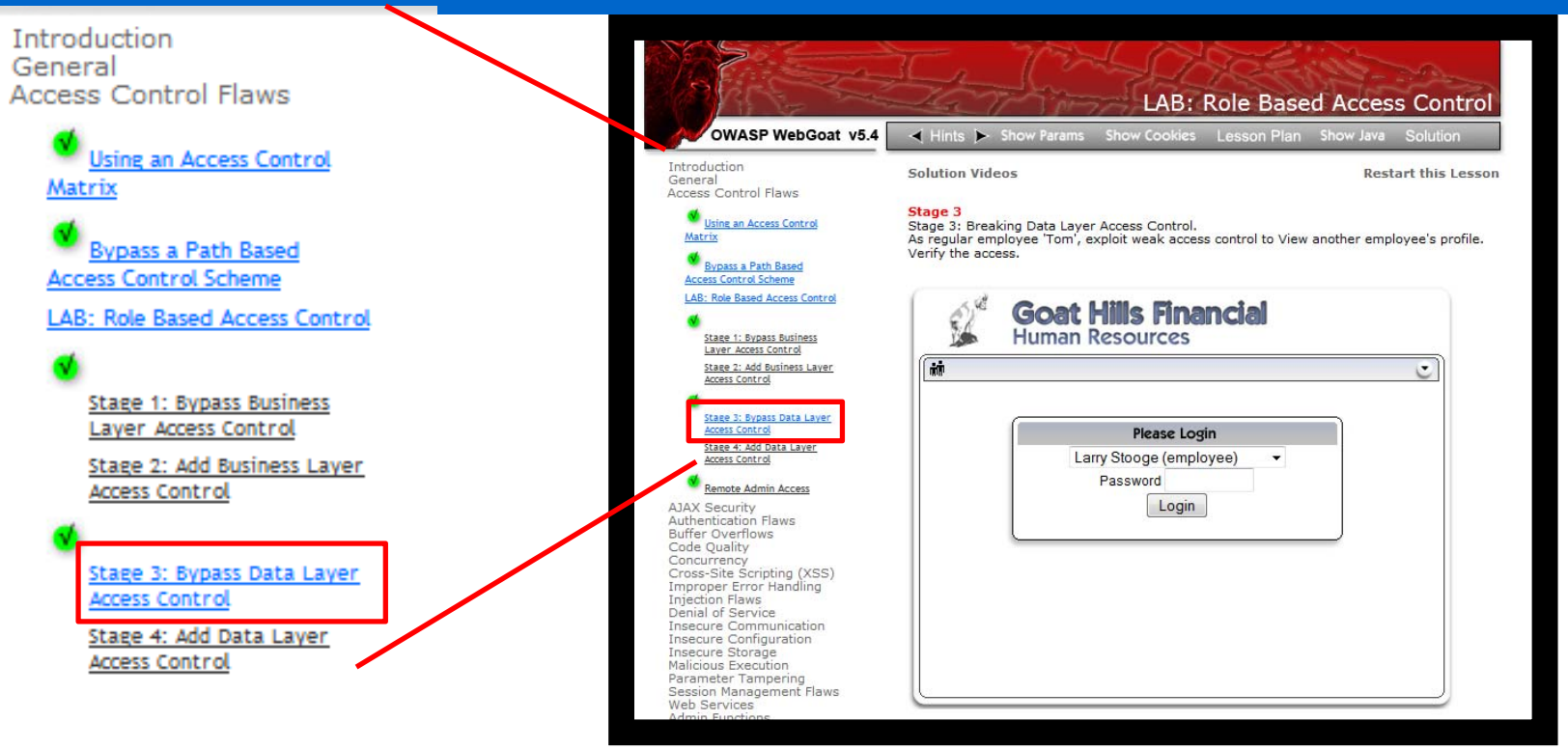
Lab Session 4 Exercises

- ***WebGoat:***
  - Access Control Flaws
    - Stage 3: Bypass Data Layer Access Control

When finished with that can try: `take over image ownership'

- ***Close WebGoat**, reconnect to network*
- *Download lab4-sheldon.bmp from the materials page*
- *Claim `ownership' of this picture*
  - *Find out how and by whom the image is claimed.*
  - *Change the claim to `ownership' by you.*
  - *Get a colleague to validate the claim.*
- *If you don't know how to proceed (hints):*
  1. *Get additional images (lab4-hints-*.bmp) from the materials directory*
  2. *Get the file lab4-hints.pdf from the materials page*
     - *Contains increasingly detailed hints to get you going*

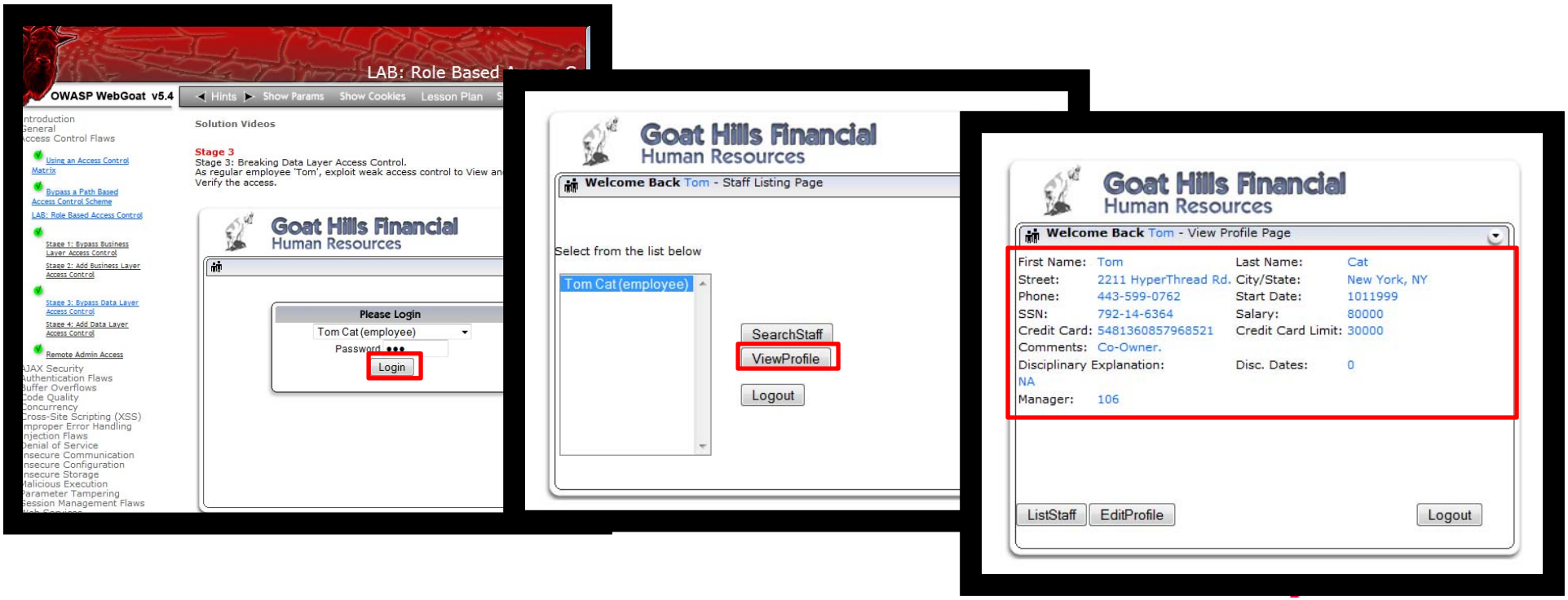
Access Control - Exercise



- Goal: Bypass access control
- Exercise:
  - Go to **Access Control Flaws→ Stage 3: Bypass Data Layer Access Control**
  - You are the employee Tom Cat (your password is still *tom*)
  - Access the profile of another user by modifying the HTTP request

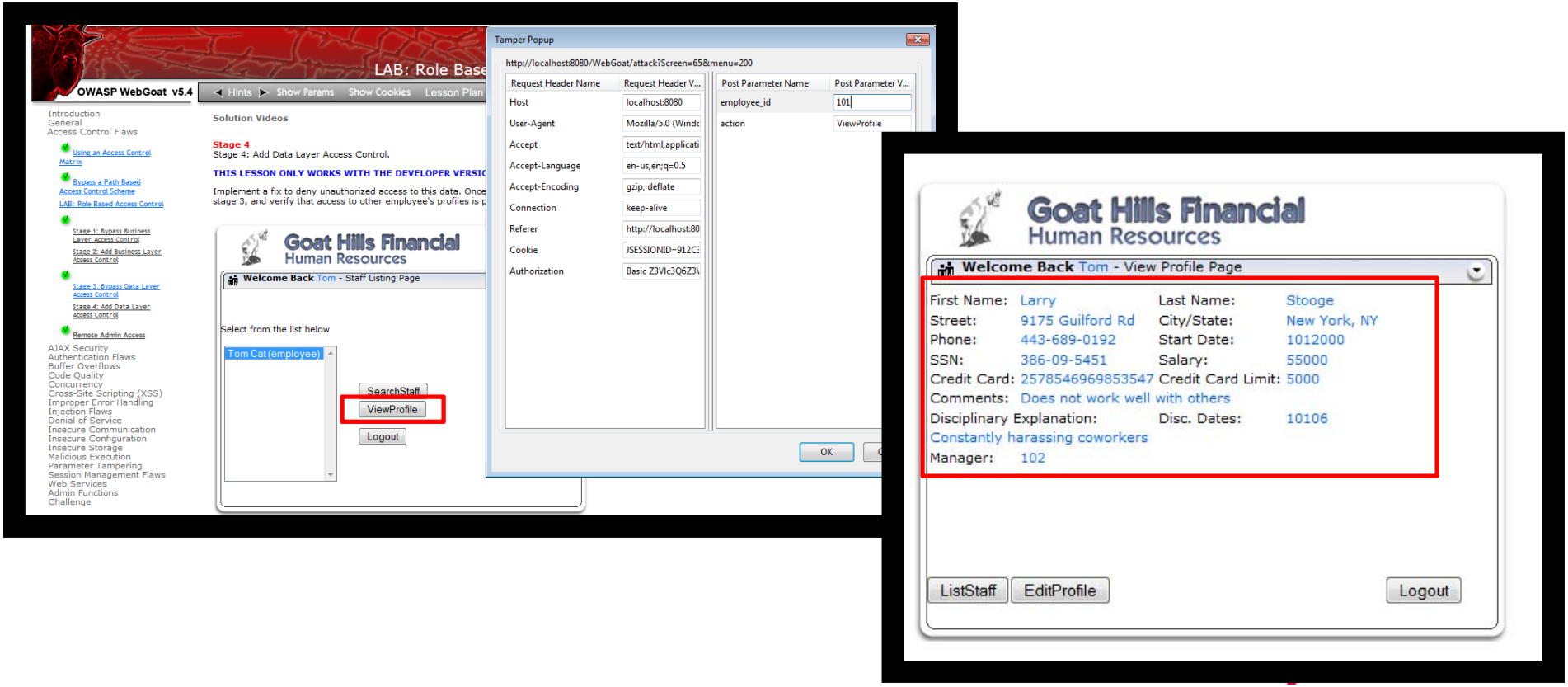
Access Control - Solution (1)

- Login as *Tom Cat* with password *tom*
- Once the login is successful you can press *ViewProfile*
- This command shows Tom's data.



Access Control - Solution (2)

- Start tampering before pressing *ViewProfile*
- Change the parameter *employee_id* from 105 to 101
- In this way you will not visualize Tom's profile, but Larry's



Access Control - Lesson learned

- The web server retrieves data only according to the *employee_id*
  - no double check on the *username* and *password* takes place
- In this way malicious user of the system (that have authorized access only to a limited set of resources) can get unauthorized access to other resources (in this case a colleague profile)