



LAB SESSION 4

ACCESS CONTROL

SESSION INFORMATION STEALING

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

Introduction
General
Access Control Flaws

✓ [Using an Access Control Matrix](#)

✓ [Bypass a Path Based Access Control Scheme](#)

[LAB: Role Based Access Control](#)

✓ [Stage 1: Bypass Business Layer Access Control](#)

[Stage 2: Add Business Layer Access Control](#)

✓ [Stage 3: Bypass Data Layer Access Control](#)

[Stage 4: Add Data Layer Access Control](#)

OWASP WebGoat v5.4

LAB: Role Based Access Control

Introduction
General
Access Control Flaws

✓ [Using an Access Control Matrix](#)

✓ [Bypass a Path Based Access Control Scheme](#)

[LAB: Role Based Access Control](#)

Stage 1: [Bypass Business Layer Access Control](#)

Stage 2: [Add Business Layer Access Control](#)

Stage 3: [Bypass Data Layer Access Control](#)

Stage 4: [Add Data Layer Access Control](#)

Remote Admin Access

AJAX Security
Authentication Flaws
Buffer Overflows
Code Quality
Concurrency
Cross-Site Scripting (XSS)
Improper Error Handling
Injection Flaws
Denial of Service
Insecure Communication
Insecure Configuration
Insecure Storage
Malicious Execution
Parameter Tampering
Session Management Flaws
Web Services
Admin Functions

Solution Videos Restart this Lesson

Stage 3
Stage 3: Breaking Data Layer Access Control.
As regular employee 'Tom', exploit weak access control to View another employee's profile. Verify the access.

Goat Hills Financial
Human Resources

Please Login

Larry Stooge (employee)

Password

Login

- 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.

The image displays three sequential screenshots from the OWASP WebGoat v5.4 application, illustrating the login and profile viewing process for the user Tom Cat.

Left Screenshot: Shows the "Please Login" form. The username field is populated with "Tom Cat (employee)" and the password field contains "tom". The "Login" button is highlighted with a red box.

Middle Screenshot: Shows the "Staff Listing Page" with the heading "Welcome Back Tom". A dropdown menu is open, showing "Tom Cat (employee)" selected. The "ViewProfile" button is highlighted with a red box.

Right Screenshot: Shows the "View Profile Page" for Tom Cat. The profile information is displayed in a table format, with the entire content area highlighted by a red border.

Goat Hills Financial Human Resources			
First Name:	Tom	Last Name:	Cat
Street:	2211 HyperThread Rd.	City/State:	New York, NY
Phone:	443-599-0762	Start Date:	1011999
SSN:	792-14-6364	Salary:	80000
Credit Card:	5481360857968521	Credit Card Limit:	30000
Comments:	Co-Owner.		
Disciplinary Explanation:	NA		
Disc. Dates:	0		
Manager:	106		

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

The screenshot illustrates a tampering session in OWASP WebGoat v5.4. The main application window displays the 'Goat Hills Financial Human Resources' interface. A 'ViewProfile' button is highlighted with a red box. A 'Tamper Popup' window is open, showing the request parameters for the 'ViewProfile' action. The 'employee_id' parameter is changed from 105 to 101. A separate window shows the resulting profile for 'Larry Stooge'.

Tamper Popup

Request Header Name	Request Header V...	Post Parameter Name	Post Parameter V...
Host	localhost:8080	employee_id	101
User-Agent	Mozilla/5.0 (Wind...	action	ViewProfile
Accept	text/html,applicati...		
Accept-Language	en-us,en;q=0.5		
Accept-Encoding	gzip, deflate		
Connection	keep-alive		
Referer	http://localhost:80...		
Cookie	JSESSIONID=912CE...		
Authorization	Basic Z3Vlc3Q6Z3V...		

Goat Hills Financial Human Resources

Welcome Back Tom - Staff Listing Page

Select from the list below

Tom Cat (employee)

SearchStaff
ViewProfile
Logout

Welcome Back Tom - View Profile Page

First Name:	Larry	Last Name:	Stooge
Street:	9175 Guilford Rd	City/State:	New York, NY
Phone:	443-689-0192	Start Date:	1012000
SSN:	386-09-5451	Salary:	55000
Credit Card:	2578546969853547	Credit Card Limit:	5000
Comments:	Does not work well with others Constantly harassing coworkers		
Disciplinary Explanation:		Disc. Dates:	10106
Manager:	102		

ListStaff EditProfile Logout

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)