LAB SESSION 6

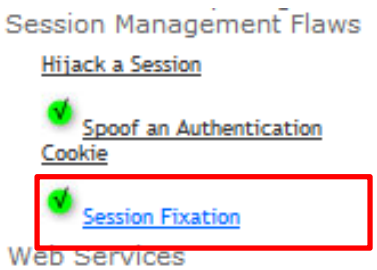
SESSION FIXATION
PHISHING

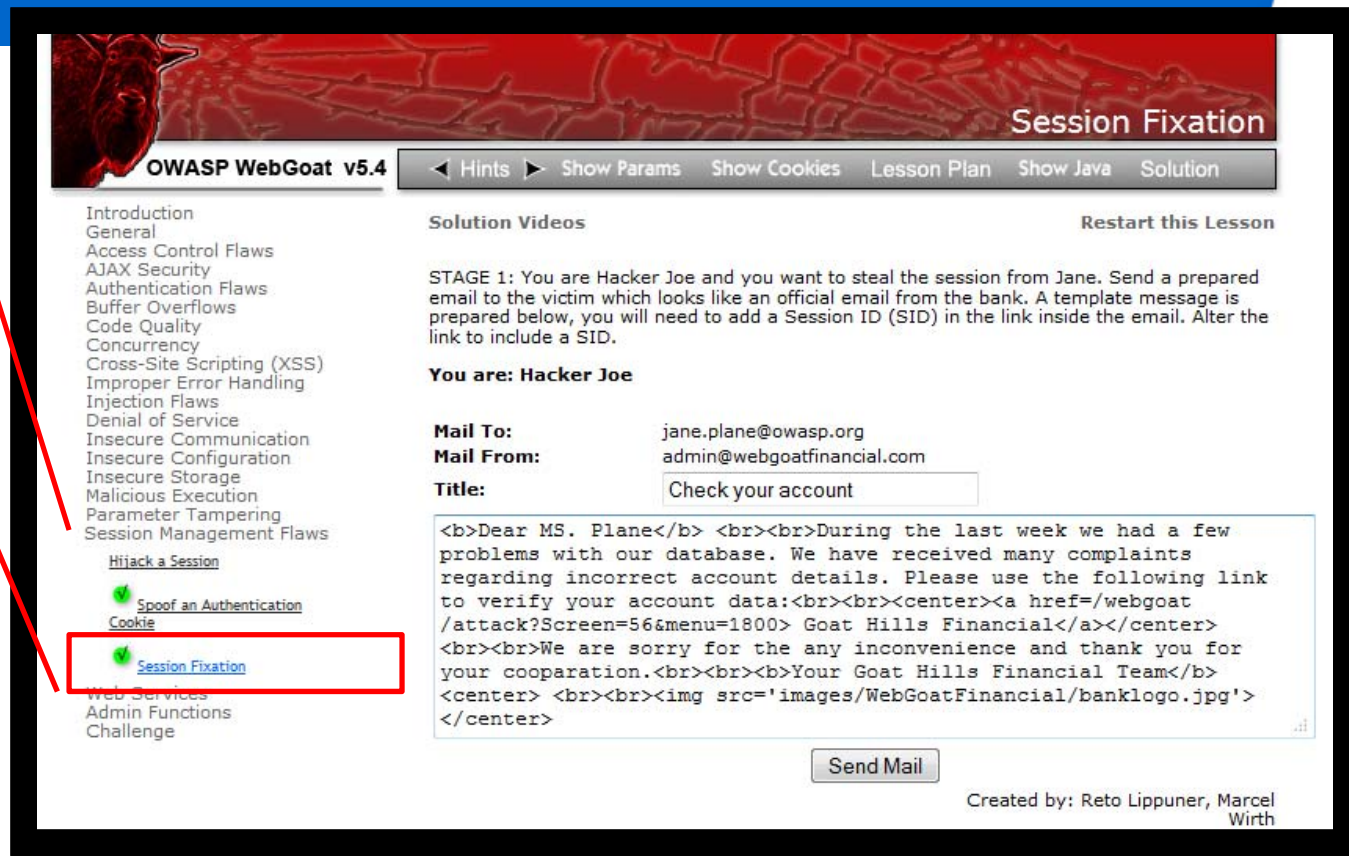
Technische Universiteit
Eindhoven
University of Technology

Session Fixation - Background

- You are Hacker Joe
  - Goal: pretend to be Jane, when communicating to Jane's bank
  - Approach: steal Jane's session when she is logged in at the bank
  - Problem: get the **session identifier (SID)** of Jane's session when she talks to the bank.
  - Solution: induce Jane to start a session with the bank **using a session identifier you chose**.
    - This may be less difficult than you think
    - Use Session Fixation; get Jane to follow a link
      - In which you have chosen the SID

Session Fixation - Exercise





- Goal: steal Jane's credit card information.
- Exercise (Two roles; play both yourself or swap with colleague):
  - Go to **Session Management Flaws→Session Fixation**
  - Attacker: Send a phishing email with a chosen SID.
  - Jane: receive email, follow link and log in. (pwd: tarzan) (As an aside: examine the link.)
  - Attacker: steal the session and use it to read the credit card info.

Session Fixation - Solution

- Stage 1 (Hacker Joe)
  - Write an email to Jane, in which you try to convince her to click on the link you have made:
  - ….. <a href=/WebGoat/attack?... &SID=**1234567**>
- Stage 2 (Jane)
  - By reading the email and clicking on the link, Jane will be redirected to the bank, starting a session with the SID that *Joe has determined*!
- Stage 3 (Jane)
  - If Jane logs in the bank with her username and password, then the session becomes active.
- Stage 4 (Hacker Joe)
  - Hacker Joe can now simply connect to the bank using the SID 1234567.
  - **The bank server will "think" that it is talking to Jane.**
    - As authentication happened earlier in the session.

Session Fixation – Solution Stage 1

- Modify the phishing email by adding a session ID to the URL
  - **href=/WebGoat/attack?Screen=56&menu=1800&SID=123456>**
- Note that the address is case sensitive (‘*webgoat*’ is not the same as ‘*WebGoat*’)

Session Fixation – Solution Stage 2 and 3

- You are now Jane (you play the role of the victim)

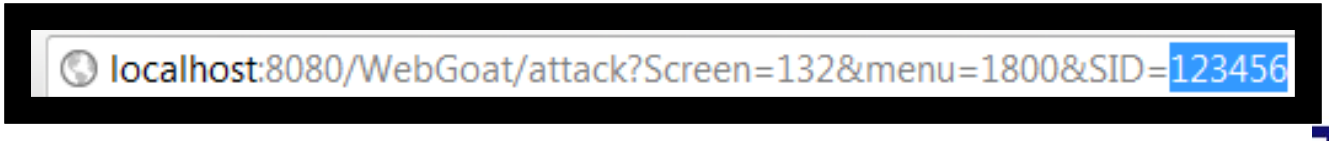
- Stage 2
  - Click on the link
  - This will initiate a session with the bank using the SID provided by Hacker Joe

- Stage 3
  - Log in as Jane (username= Jane, password= tarzan)
  - You are now logged in the bank, with the SID given by Joe

Session Fixation – Solution Stage 4

- Now you play the role of the attacker again

- Follow the link (Goat hill Financial)
- Change the URL (in the address bar) by adding the SID you previously set
- You accomplished your goal,
  - The bank server “thinks” you are Jane
  - you can see her credit card number



Session Fixation – Lesson Learned

- You learned how to carry on a (very basic) “phishing attack” and to use it to steal a session.
- This happens because the bank accepts in a silly way the token to be fixated by the user.
- The bank should fix her own token….
  - Should not rely on token for authentication

Phishing - Exercise

- Phase 1: (Work with a buddy)
  - Send your buddy a mail that seems to come from Bill.Gates@microsoft.com (or use your imagination...)
  - Hints: sendmail or telnet to smtp.tue.nl
  - Have your buddy also check their spam mail.
- Phase 2: Send a phishing e-mail to a colleague in the course
  - Should seem to come from some trusted source.
  - Add some realistic contents to get them to visit website: http://security1.win.tue.nl/~ecostant/SecurityCourse/
    - Have them login/register/...
- What happened and what could you do with this type of attack?

Phising - Solution

- With sendmail you can set the sender to anything you want

- You can also send via smtp.tue.nl by:

telnet smtp.tue.nl 25

HELO smtp.tue.nl

Mail FROM: <*whomeveryouwant*>

RCPT TO: <*whomeveryouwant*>

DATA

Subject: *A Test*

Test mail content

.

Phishing – Lesson Learned

- You carried out a “phishing attack” “in practice”.
- Email can come from anyone.
  - No authentication of sender (How could you solve that?).
- Got you victim to go to a fake site
  - Same look and feel as the real site
  - Data entered goes to an attacker.