Web Application Hacking Lesson Session Fixation Attack

Objectives

- Review lecture
- Complete lab on Session Fixation Attack

Lecture for Session Fixation

Session Fixation is an attack that permits an attacker to hijack a valid user session. The attack explores a limitation in the way the web application manages the session ID, more specifically the vulnerable web application. When authenticating a user, it doesn't assign a new session ID, making it possible to use an existent session ID. The attack consists of inducing a user to authenticate himself with a known session ID, and then hijacking the user-validated session by the knowledge of the used session ID. The attacker has to provide a legitimate Web application session ID and try to make the victim's browser use it.

The session fixation attack is a class of Session Hijacking, which steals the established session between the client and the Web Server after the user logs in. Instead, the Session Fixation attack fixes an established session on the victim's browser, so the attack starts before the user logs in.

There are several techniques to execute the attack; it depends on how the Web application deals with session tokens. Below are some of the most common techniques:

• **Session token in the URL argument:** The Session ID is sent to the victim in a hyperlink and the victim accesses the site through the malicious URL.

• **Session token in a hidden form field:** In this method, the victim must be tricked to authenticate in the target Web Server, using a login form developed for the attacker. The form could be hosted in the evil web server or directly in html formatted e-mail.

• **Session ID in a cookie:**

o Client-side script

Most browsers support the execution of client-side scripting. In this case, the aggressor could use attacks of code injection as the XSS (Cross-site scripting) attack to insert a malicious code in the hyperlink sent to the victim and fix a Session ID in its cookie. Using the function document.cookie, the browser which executes the command becomes capable of fixing values inside of the cookie that it will use to keep a session between the client and the Web Application.

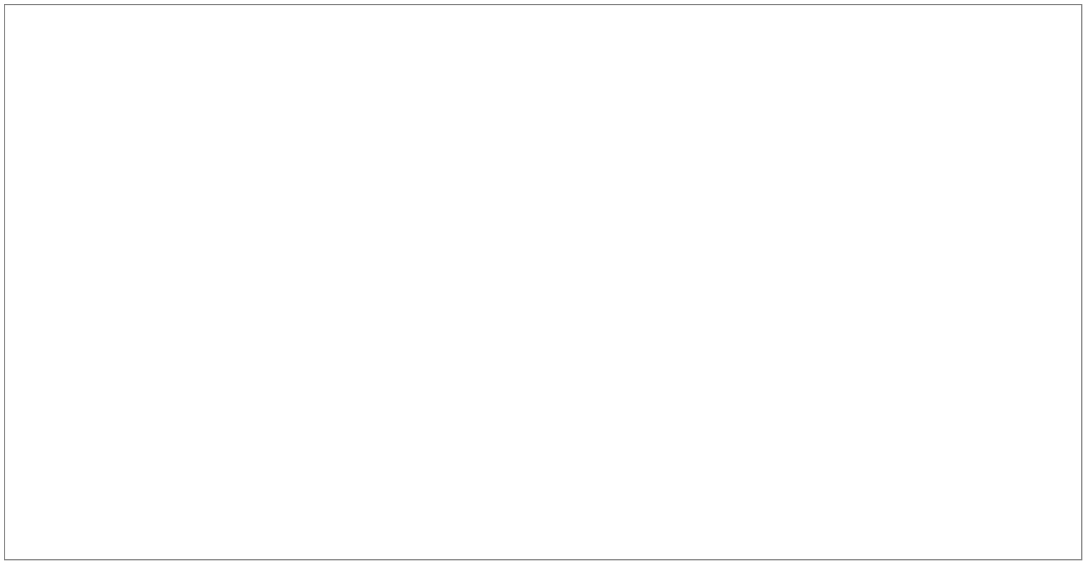
Lab for Session Fixation Attack

Lab Prep

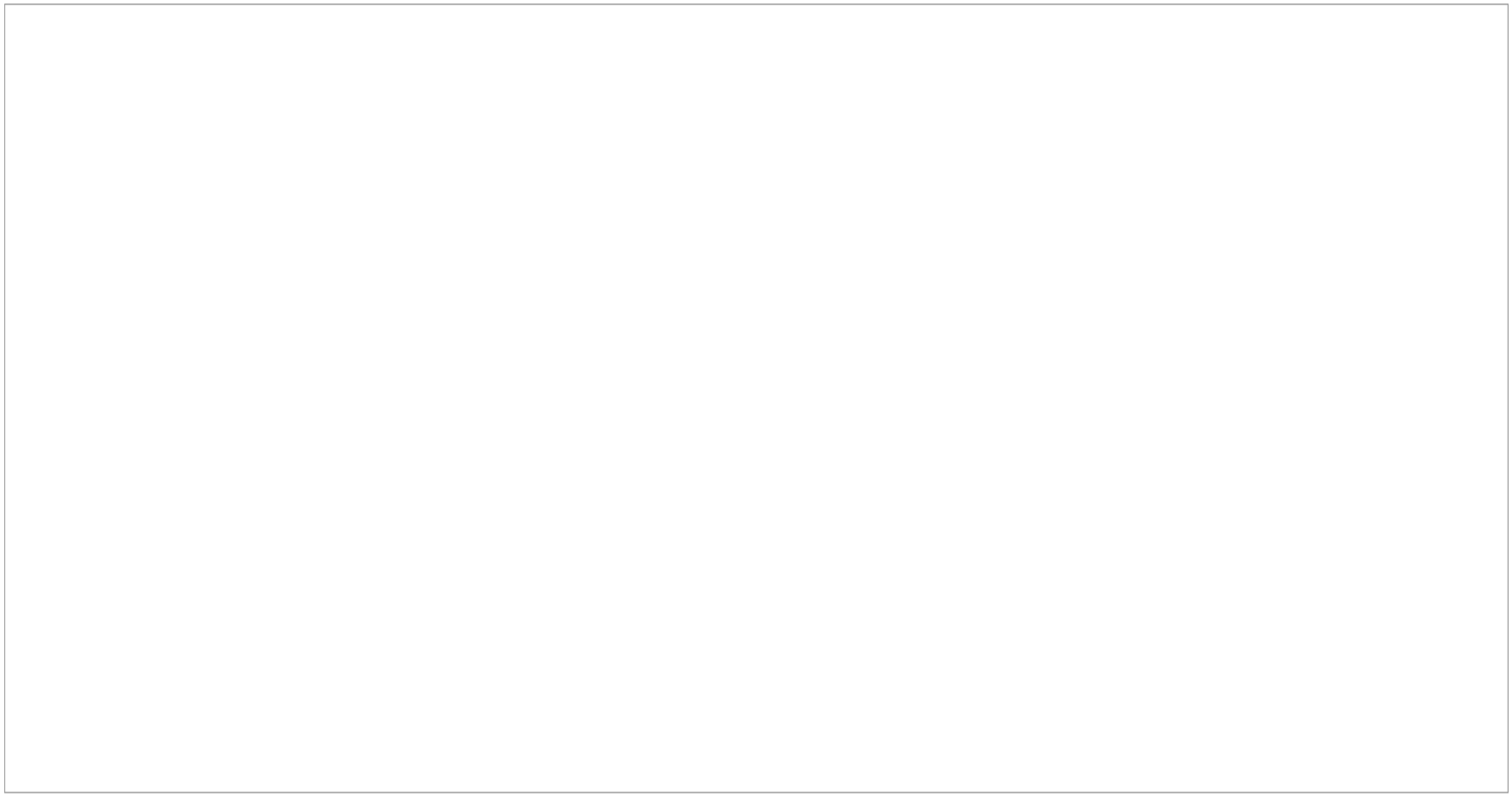
In Firefox, add the “Cookie Manager +” extension

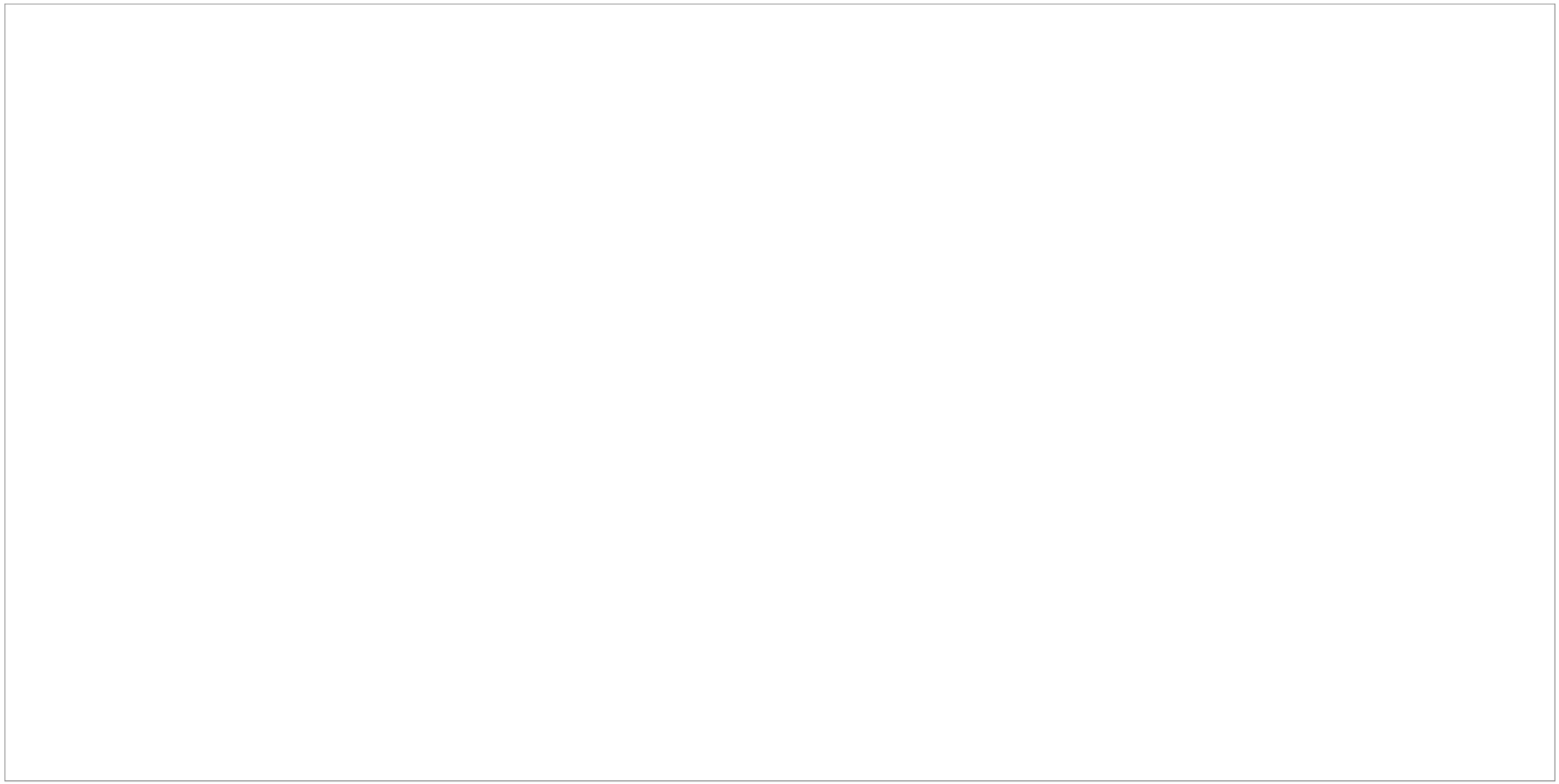
Open the link to http://playground.nebulassolutions.com/index.phphttp://playground.nebulassolutions.com/index.php

Click on login



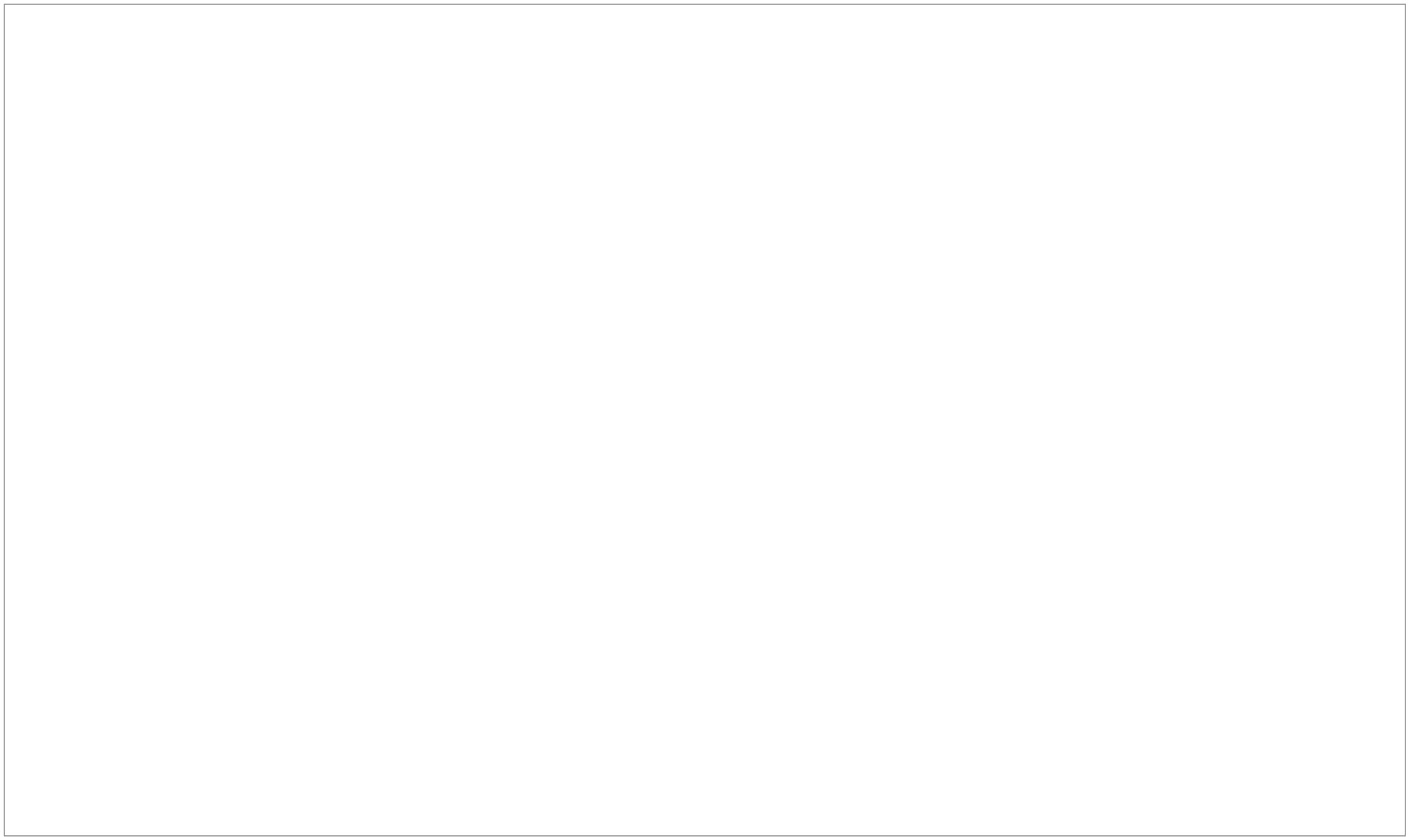
Login with the username of 'John' and the password of monkey.



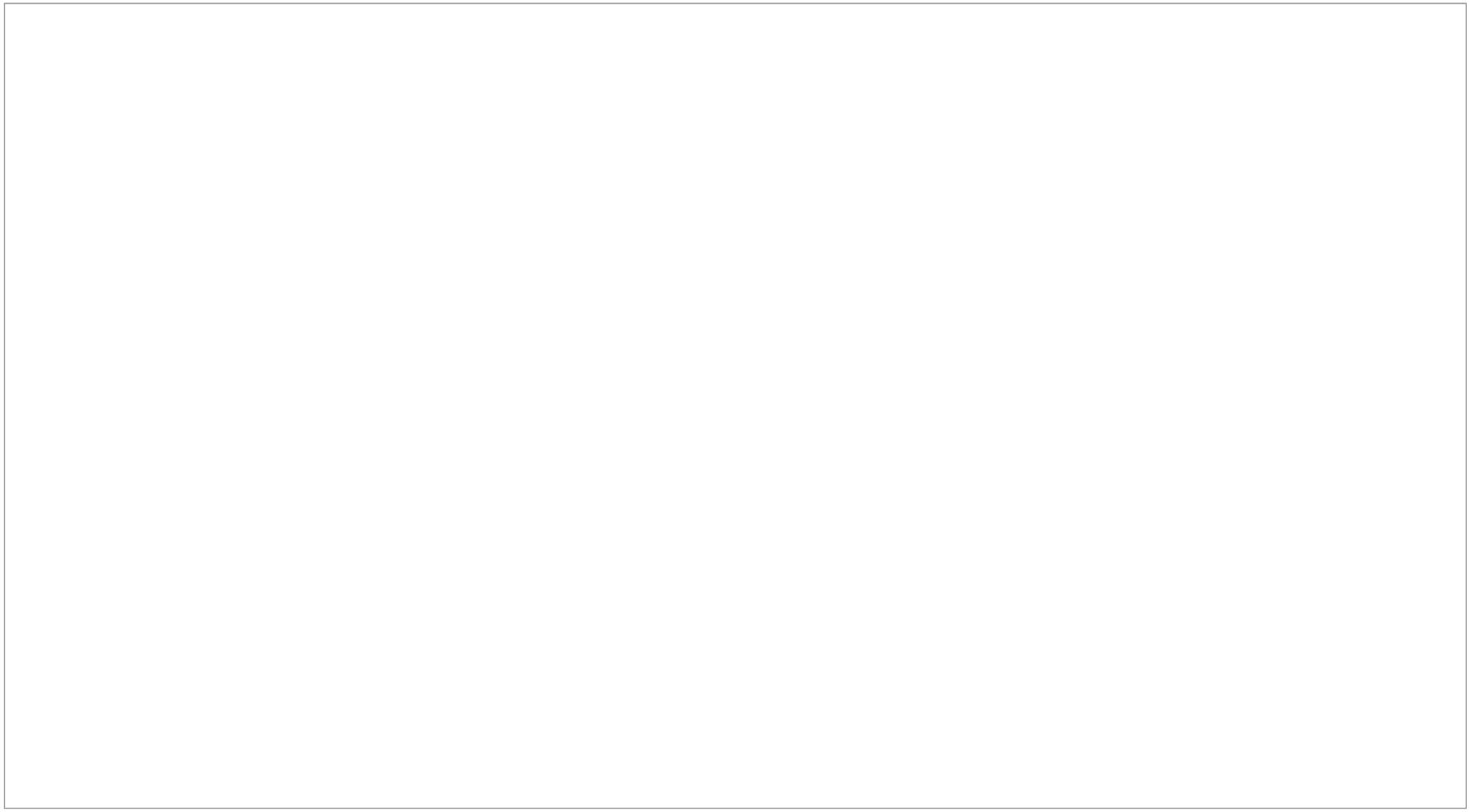


Notice how you are now logged in as the user “John”

Open cookie manager+ and look at the two cookies related to this URL. Edit the one that labled UID . The UID here is #3. This number is the session ID given by the application to the user. We will edit this number and see if we can login as another user. Change the value of 3 to 1.



Click save and click close. After closing cookie manager refresh the browser.



After refreshing the screen, notice we have now taken over the session of the administrator. Look at the top right screen and notice we are now logged in as the administrator!!

1. Describe in your own words what a Session Fixation Attack?
2. What OWASP ranking is CRSF?
3. Google and explain some of the dangers that Session Fixation attacks poses?

    - **Proof of Lab Instructions**:
        1. Do a <PrtScn> of lab
        2. Paste into a word document
        3. Post to teambox
    -