CSE 4402: Lab Design Document Cookies

Luke Pepin, Tommy Jiang, Mohamed Makhlouf, Jan Feyen

### ***Abstract - In this lab, we will analyze the security and management aspects of cookies in web applications, especially in authenticating (login) cookies. We will discuss how security flags are configured across different sites and their implications for user data protection. We will also evaluate the relationship between cookie lifespan and security, emphasizing the trade-offs between convenience and risk. We will analyze the role of authenticating cookies in mitigating security breaches and examine the various types of trust established between the server and client. Additionally, we will cover common attacks against cookies, particularly cross-site scripting (XSS), and effective defenses against these vulnerabilities. Finally, we will consider the performance impact of using cookies for user sessions on website load times, along with an overview of essential cookie components and the distinctions between functional and security flags. By the end of this lab, we hope to address the following questions below:***

* ***How are security flags are configured for cookies across different sites?***
* ***What is the relationship between cookie life span and security?***
* ***How are authenticating cookies used to mitigate security breaches?***
* ***How is trust between the server and client formed?***
* ***What are some common attack techniques (like XSS) on cookies, and how can they be mitigated or defended?***
* ***What is the performance impact of using cookies for user sessions on website load times and speed?***
* ***What are the essential components of a cookie, and how do functional and security flags differ in purpose?***
* ***What methods were used for managing state and sessions in web applications before the introduction of cookies?***

### **Introduction:**

* **Background:**

Cookies in web security are data stored on a user’s device that helps websites remember important information about that user such as login credentials and maintain session states. They enhance the user experience by tracking user activity but must be securely managed to prevent unauthorized access (XSS) and/or data breaches. Some protection mechanisms include Security Flags like *HttpOnly, Cross-origin policy* and *SameSite* in order to mitigate risks.

* **Objective:**

This lab's objective is to retrieve and analyze login cookies from secure websites. By examining these cookies and their associated security flags, we aim to understand the purpose of each flag and assess their effectiveness in the current security environment. This includes evaluating how these flags contribute to the security of user authentication processes, protecting against common threats such as cross-site scripting (XSS) and cross-site request forgery (CSRF). The goal of this lab is to better understand the security functions of login cookies and how they affect user behavior and application security.

* **Scope:**

The scope of this lab will cover the retrieval and analysis of multiple different ookies (primarily login) under numerous different protocols. These cookies will be reviewed, documented, and tested based off their security attributes. Specifically, the lab will:

* Examine how security flags are configured for cookies across different sites and their impact on security.
* Explore common attacks against cookies, such as cross-site scripting (XSS), and defenses against these attacks.
* Understand the essential components of a cookie and the purpose of different security flags.

### **Methodology:**

* **Research Approach:**

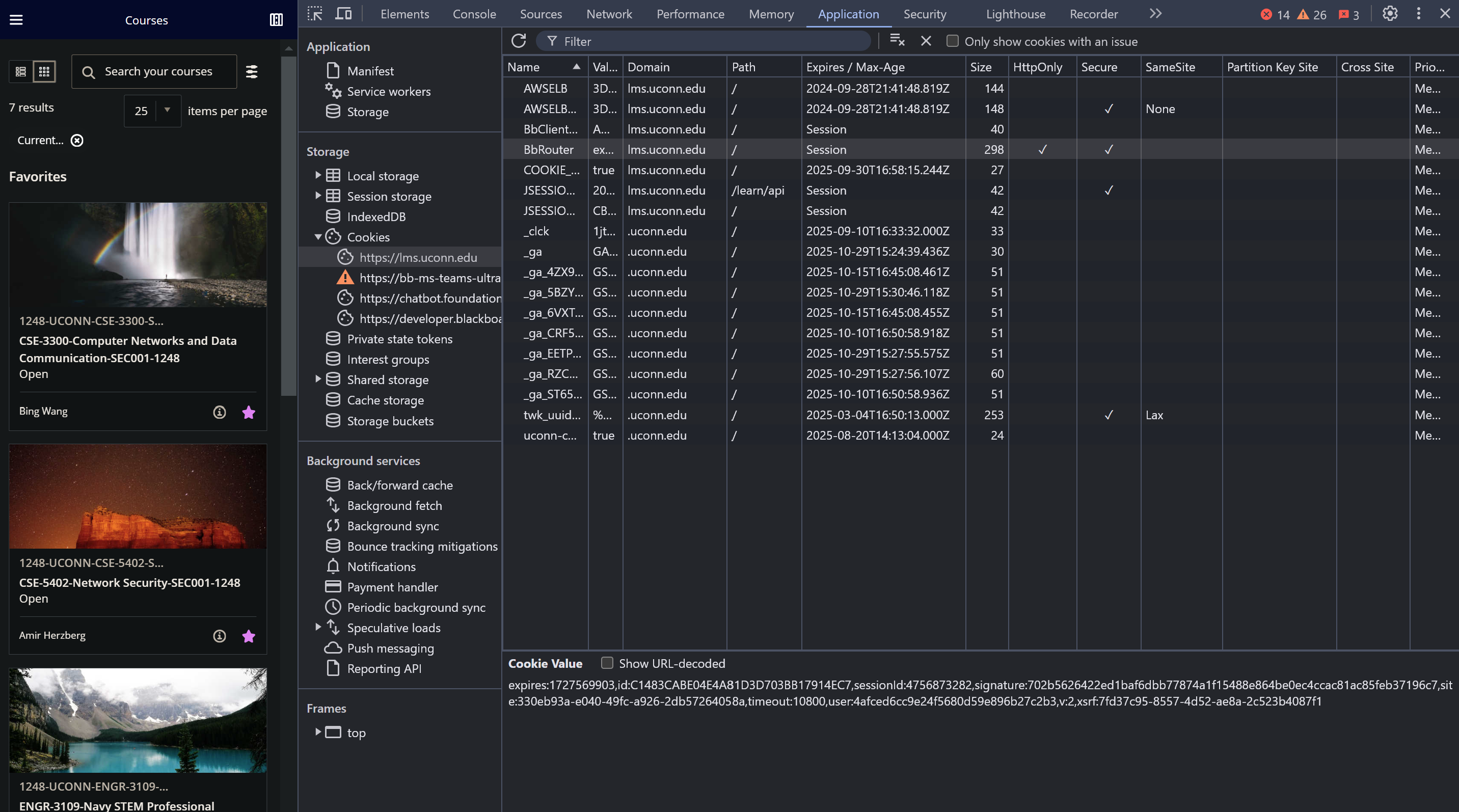
To survey the use of different cookie security flags, we will:

1. Identify Target Websites: Select a diverse range of secure websites to analyze their login cookies.
2. Retrieve Cookies: Use web developer tools, such as Google Chrome DevTools, to inspect and retrieve login cookies from these websites.
3. Analyze Security Flags: Document and analyze the security flags associated with each cookie, focusing on attributes like Secure, HttpOnly, and SameSite.
4. Evaluate Security Impact: Assess how these security flags contribute to the overall security of user authentication processes and protect against common threats like cross-site scripting (XSS) and cross-site request forgery (CSRF).

* **Tools and Technologies:**

The primary tools we will be using are the built-in Google Chrome DevTools, which will be very helpful for manual cookie analysis and understanding the use of authenticating cookies. We will utilize these tools to inspect cookies and analyze their attributes, including name, value, domain, path, expiration time, size, and various security attributes.

Additionally, we may use Wireshark to get granular details of the network packet traffic and cookie transmission, especially for unencrypted HTTP traffic.



*Fig 1. Screenshot of a group members cookies using Chrome DevTools, showcasing each cookies name, value, domain, path, expiration time, size and various security attributes*

* **Data Collection:**

In our group project, we will analyze cookie security flags from various popular websites using different browsers. Using the respective browser’s developer tools, we will inspect HTTP responses to identify security flags like Secure, HttpOnly, and SameSite. This organized data will allow us to identify trends in cookie security practices across different industries. Additionally, we will ensure proper documentation using established research technique.

### **Data Processing:**

* **Data Analysis:**

To analyze the collected data on cookie security flags, we will first clean the dataset to remove duplicates and irrelevant entries, ensuring the accuracy and reliability of our analysis. Next, we will categorize the cookies by their security attributes, such as Secure, HttpOnly, and SameSite, and calculate the prevalence of each flag across different websites. This categorization will help us identify patterns and trends in cookie security practices. Finally, we will visualize our findings using graphs and charts, which will highlight the distribution and effectiveness of various security flags across different industries. The web tools we have selected will clearly display all the enabled security flags for each website’s cookies with a checkmark. By recording each cookie and its associated security flags, we aim to understand their effectiveness and purpose in different scenarios and industry settings.

* **Documentation:**

Our research will be documented in a comprehensive research paper. This paper will include an abstract summarizing the key points, an introduction outlining the background and objectives, a detailed methodology section describing our research approach and tools, and a thorough analysis of our findings. Each section will be carefully crafted to provide a clear and concise overview of our study, ensuring that our research is accessible and informative for readers.

### **Conclusion:**

* **Review:**

This lab was designed to analyze the security and management of cookies in web applications by examining login cookies from various secure websites. Our focus was on understanding the configuration and effectiveness of security flags, the relationship between cookie lifespan and security, and the role of authenticating cookies in mitigating security breaches.

* **Final Notes:**

Our findings underscore the critical role and purposes of security flags in login cookies. Work expansion could build on this study by exploring additional security mechanisms and their impact on cookie management. Extensions could also include a more detailed related works section, enhanced data visualization techniques, and investigating the use of cookies in emerging web technologies to further enhance our understanding and effectiveness in web security practices.

**Contacts:**

Luke Pepin [LUKE.PEPIN@UCONN.EDU](mailto:LUKE.PEPIN@UCONN.EDU)

Mohamed Makhlouf [MOHAMED.MAKHLOUF@UCONN.EDU](mailto:MOHAMED.MAKHLOUF@UCONN.EDU)

Tommy Jiang [TOMMY.JIANG@UCONN.EDU](mailto:TOMMY.JIANG@UCONN.EDU)

Jan Feyen [JAN.FEYEN@UCONN.EDU](mailto:JAN.FEYEN@UCONN.EDU)