Національний технічний університет України

«Київський політехнічний інститут імені Ігоря Сікорського»

Факультет інформатики та обчислювальної техніки

Кафедра Обчислювальної Техніки

Лабораторна робота №1

з дисципліни "Безпека програмного забезпечення"

Тема: "Базова аутентифікація"

Виконав:

студент групи ІП-93

Домінський В.О.

Київ 2022

**Зміст**

[Вступ: 3](#_Toc120041156)

[1. Повний опис PPP 4](#_Toc120041157)

[1.1 Особливості PPP 4](#_Toc120041158)

[2. Взаємодія з іншими протоколами 4](#_Toc120041159)

[2.1 Компоненти PPP 4](#_Toc120041160)

[2.2 Робота PPP 5](#_Toc120041161)

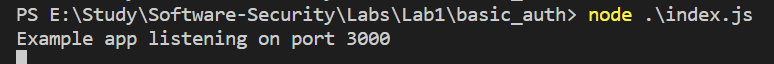
[2.3 Переваги PPP 9](#_Toc120041162)

[Висновок: 10](#_Toc120041163)

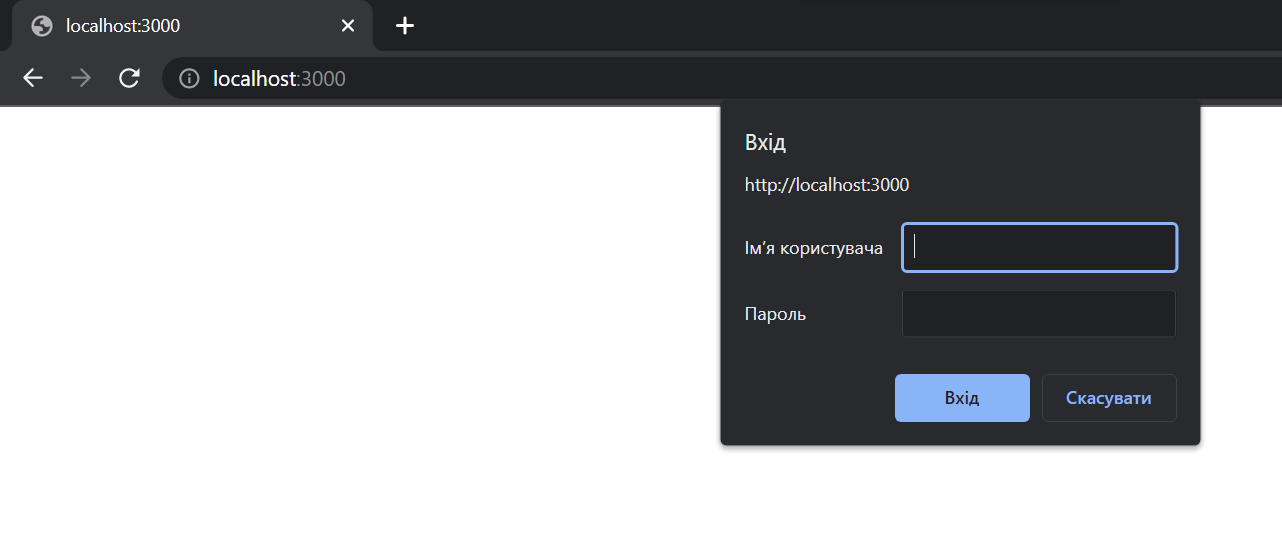
[Посилання: 11](#_Toc120041164)

## Basic\_auth

Для початку давайте запустимо даний файл:

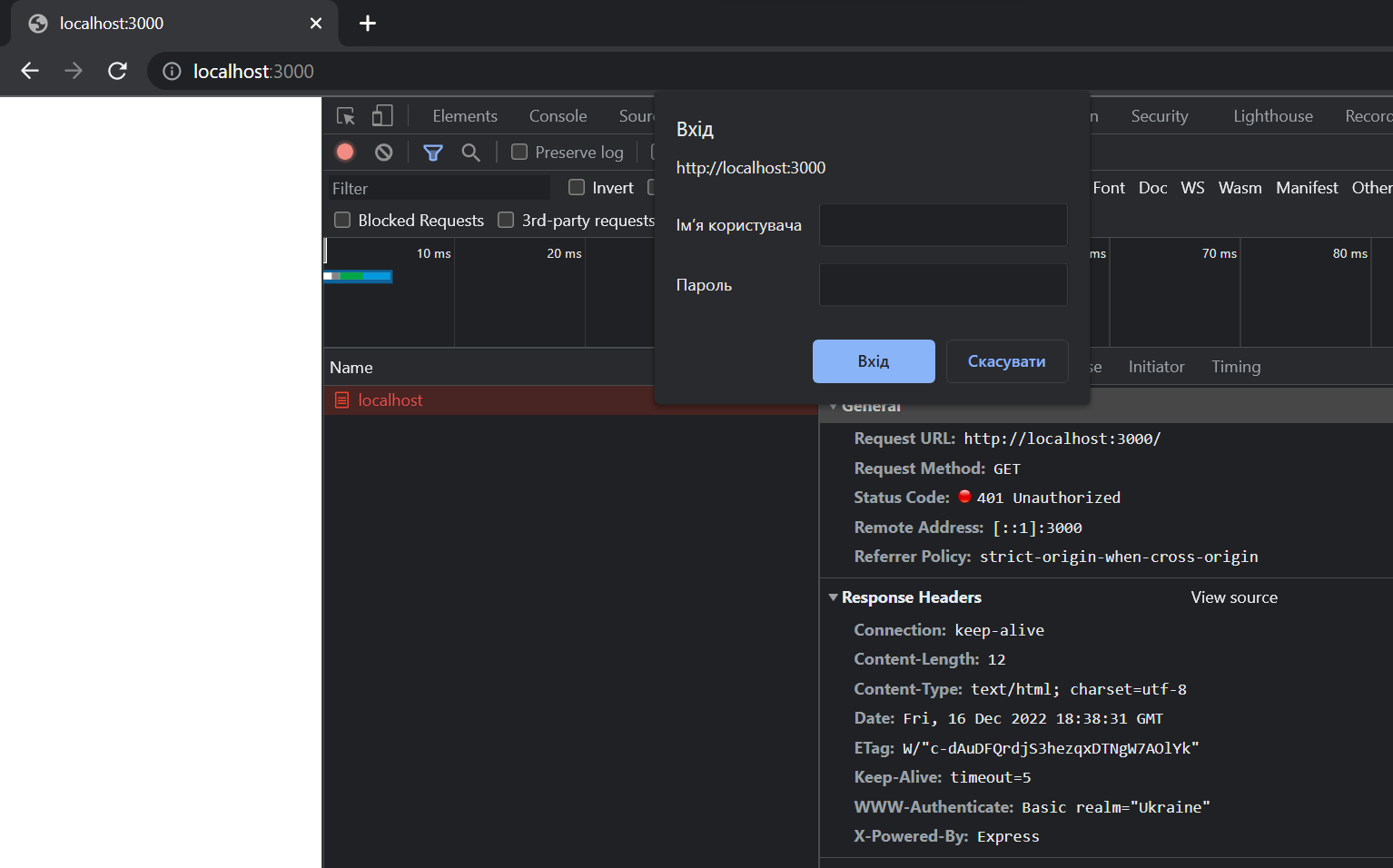


Як видно, він почав працювати на порту 3000

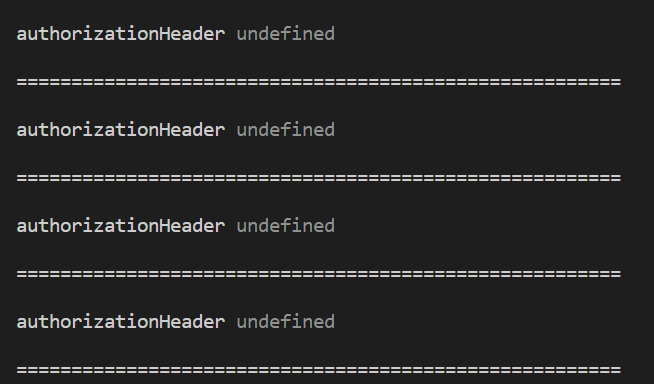


Якщо Ми зайдемо в Response Headers (тобто в запитах), то можемо помітити ось такі важливі значення:

* Status Code – 401
* Вид аутентифікації – Basic

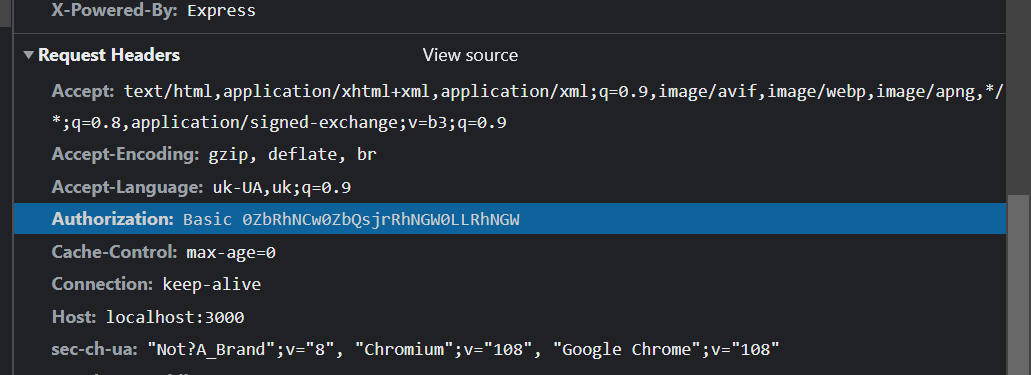


Консоль теж без діла не лежить:

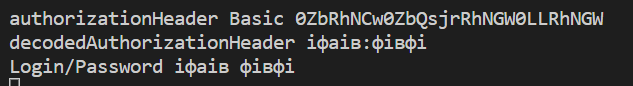


Ось тут виводиться значення одного з хедерів (Authorization), при якому запускається формування Header з базовою аутентифікацією

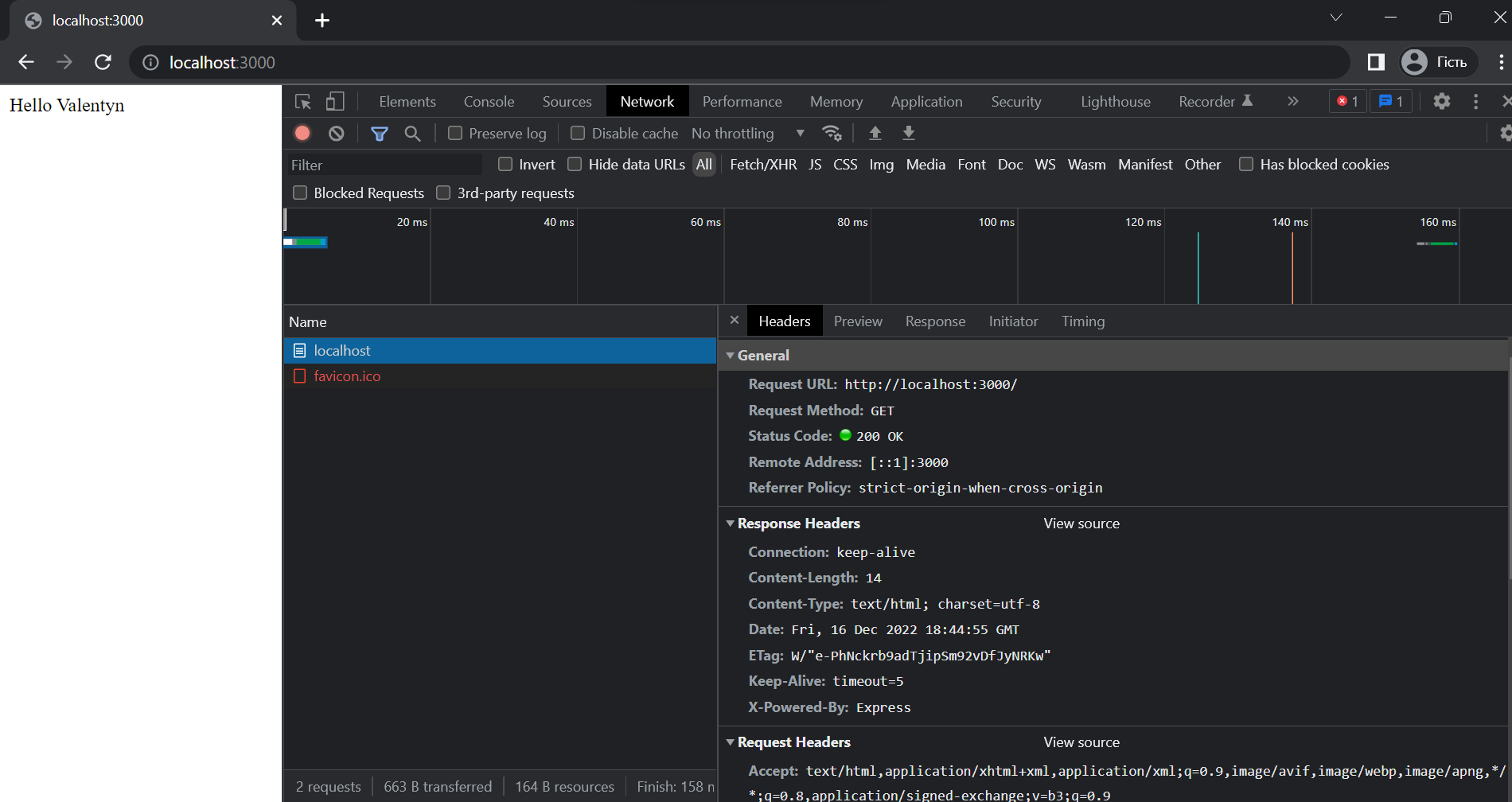
Тепер давайте спробуємо написати неправильні дані. На перший погляд майже нічого не змінилося – додався лише текст на самій сторінці, але це не так! Якщо проглянути Headers, то можна знайти новий хедер від браузеру з назвою «Basic» та Base64 хешом :

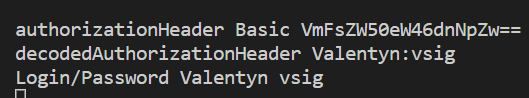


А в консолі Ми можемо побачити ще й розшифровані значення:



Тепер вводимо правильні значення:

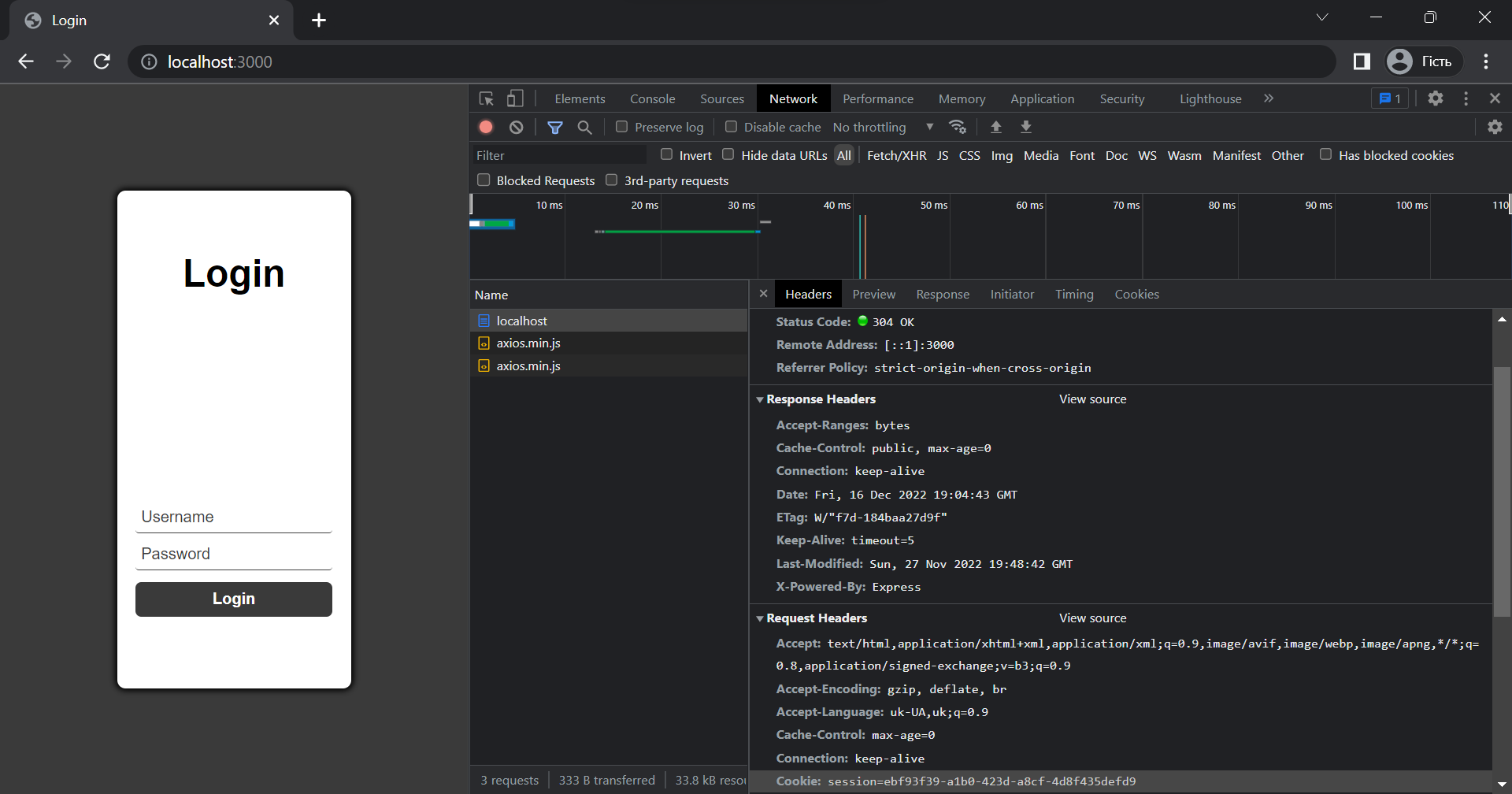




Таким чином Ми зробили найлегшу аутентифікацію!

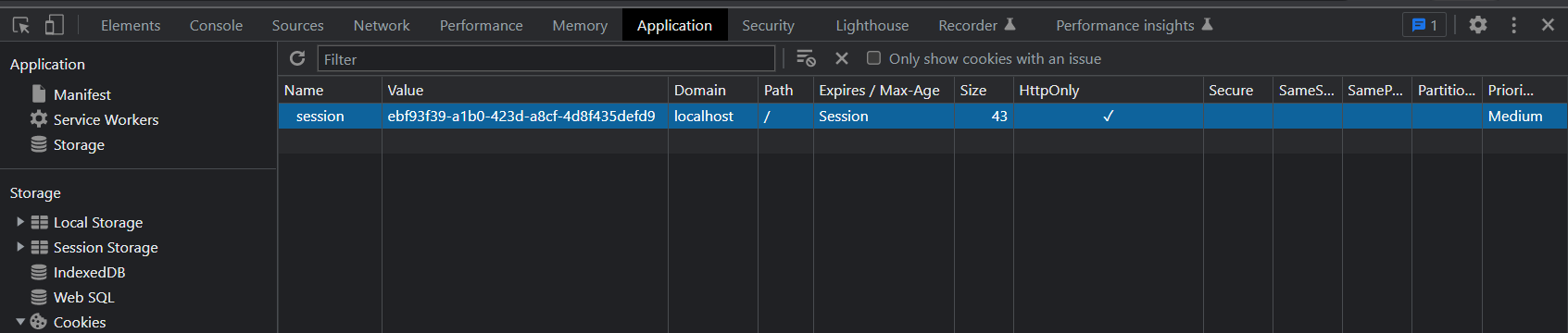
## Forms\_auth

При запуску Нас зустрічає ось таке вікно:



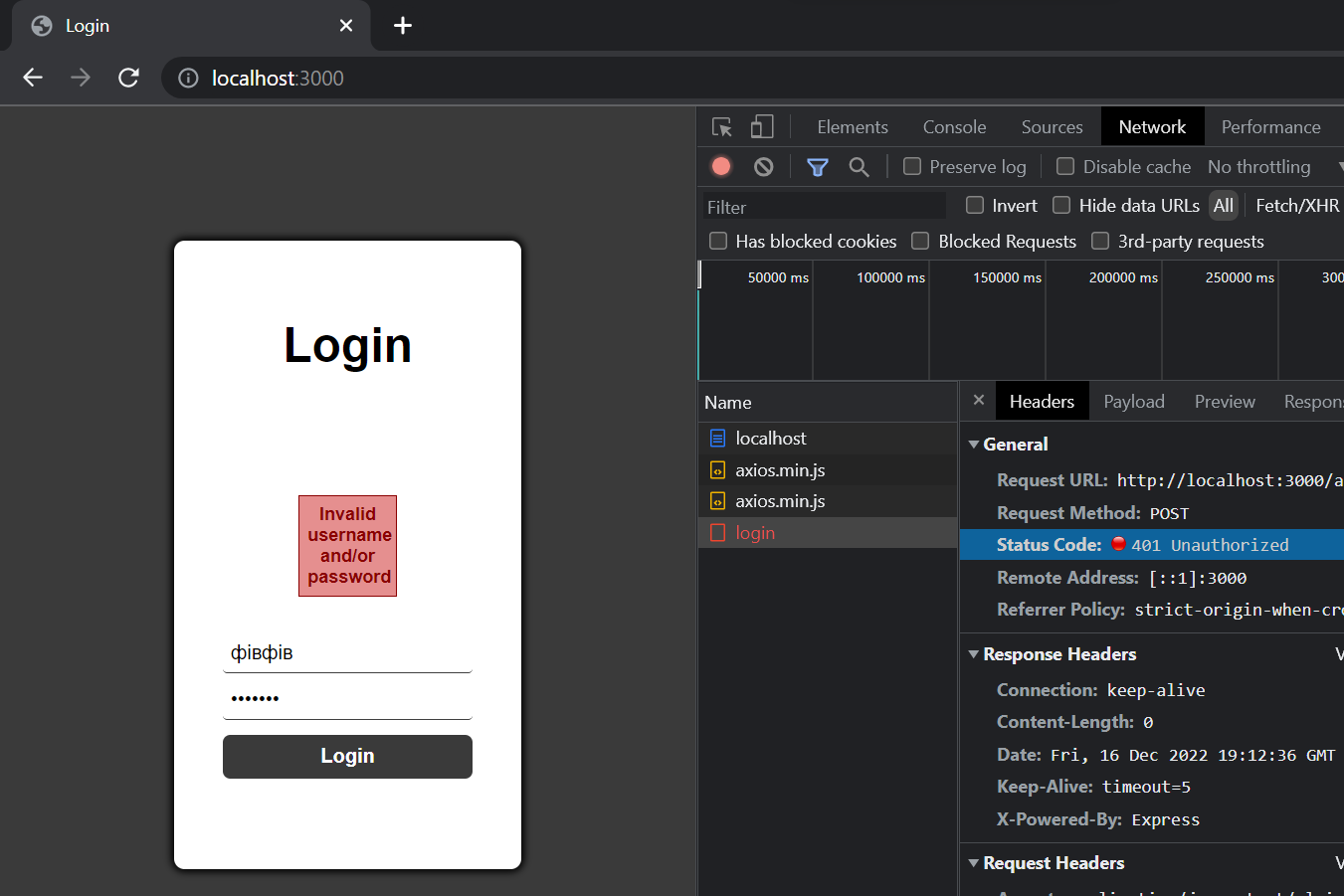
Можна помітити різницю між двома application у тому, що зараз Наш статус код – 304 та створюється значення cookie, тобто позначили цей браузер та сесію певним токеном і додатково створили файл sessions.json, куди його і помістили.

Відкривши додаткове меню з cookies Ми можемо знайти багато інформації щодо Наших токенів:



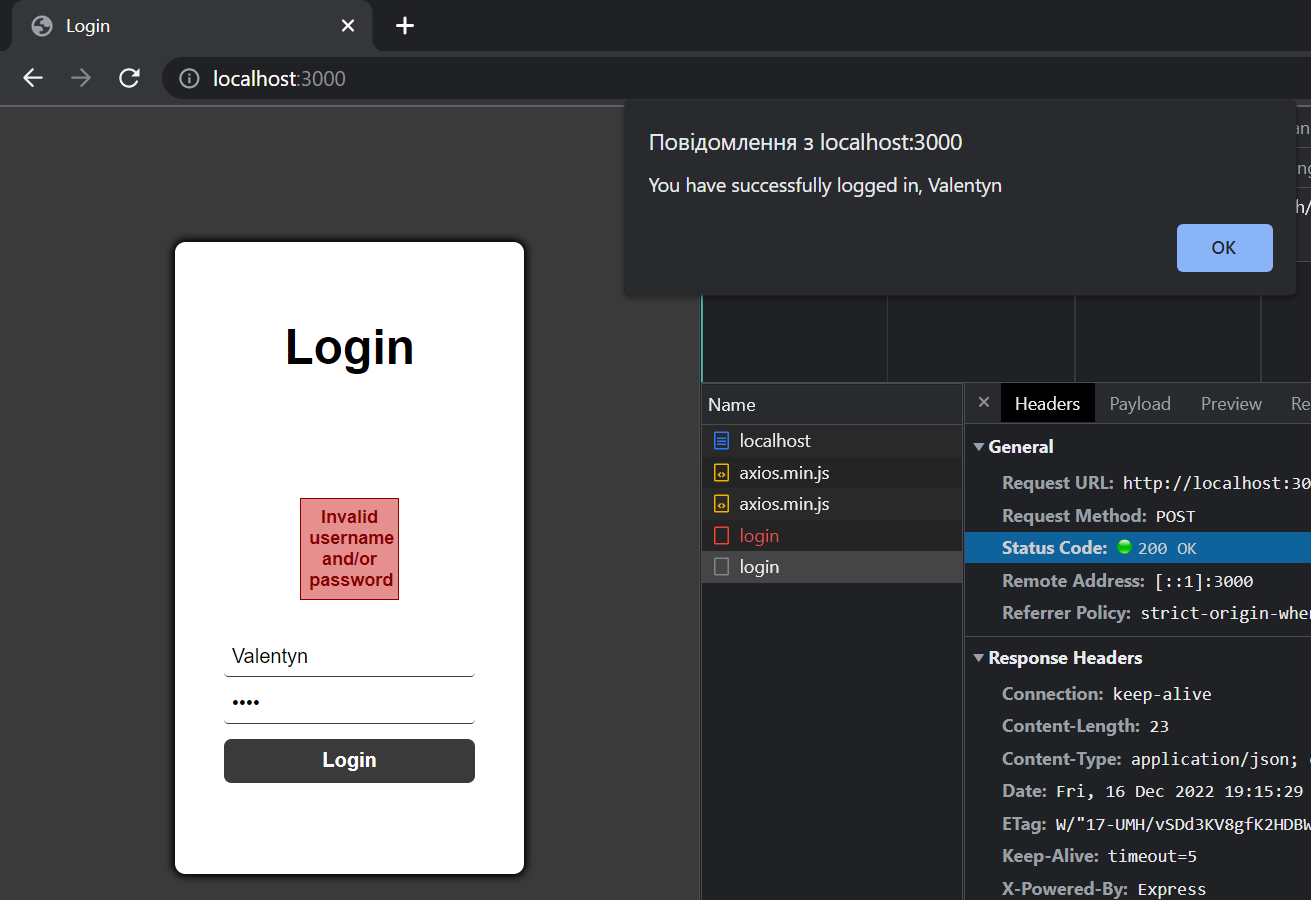
У Нашого cookie є поле HttpOnly, що означає, що вона буде постійно надсилатися на цей домейн, але її не можна редагувати з браузера

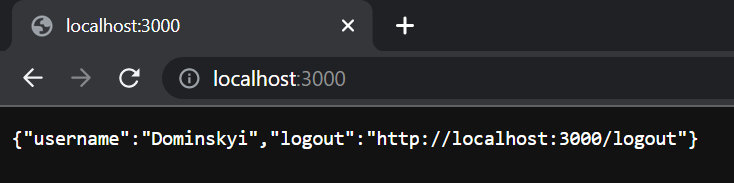
Тепер введемо неправильні логін та пароль:



… та отримаємо загальний текст помилки і статус код 401.

Тепер зробимо все вірно:





Як бачимо перед Нами з’являється нове вікно з повідомленням про вдалу авторизацію та інформацію про Нас.

Якщо ж спробувати вийти зробити logout, то Наш токен сесії буде знищений та створено новий.

# Висновок:

Під час виконання роботи я обрати протокол моделі OSI та дав йому повний опис, а потім перейшов до опису взаємодії протоколу за варіантом (Я розглядав PPP (Point to Point)) з іншими протоколами рівня. Описав його переваги, недоліки

# Посилання:

* [Проект на GitHub](https://github.com/VsIG-official/Software-Security)