**Міністерство освіти і науки України**

**УДУ імені М.П.Драгоманова**

Факультет математики, інформатики та фізики

*Кафедра комп’ютерної та програмної інженерії*

ЛАБОРАТОРНА РОБОТА № 12

з курсу

*«Автоматизація тестування»*

## *Тема роботи: «*Тестування безпеки»

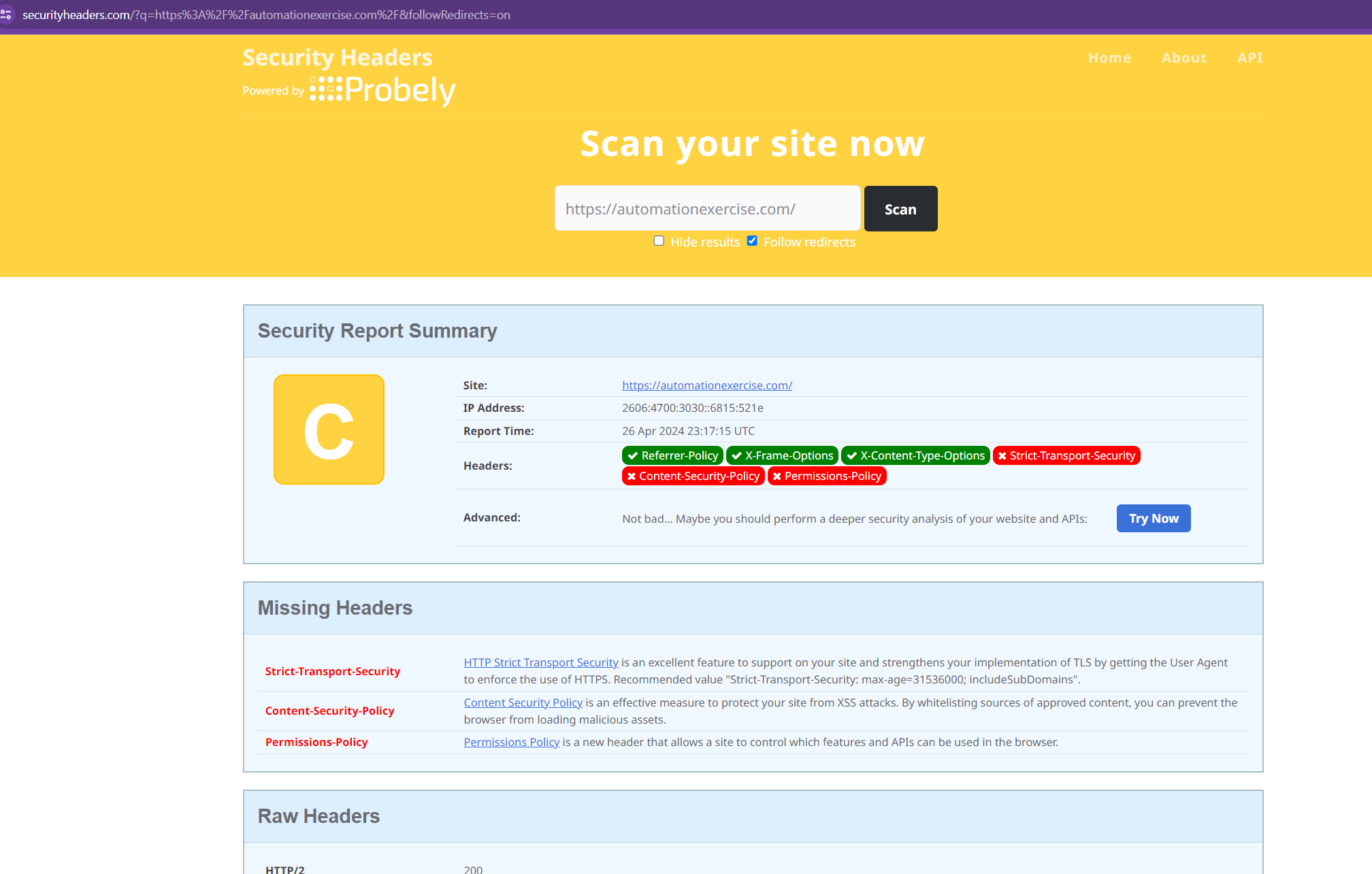
Студент:

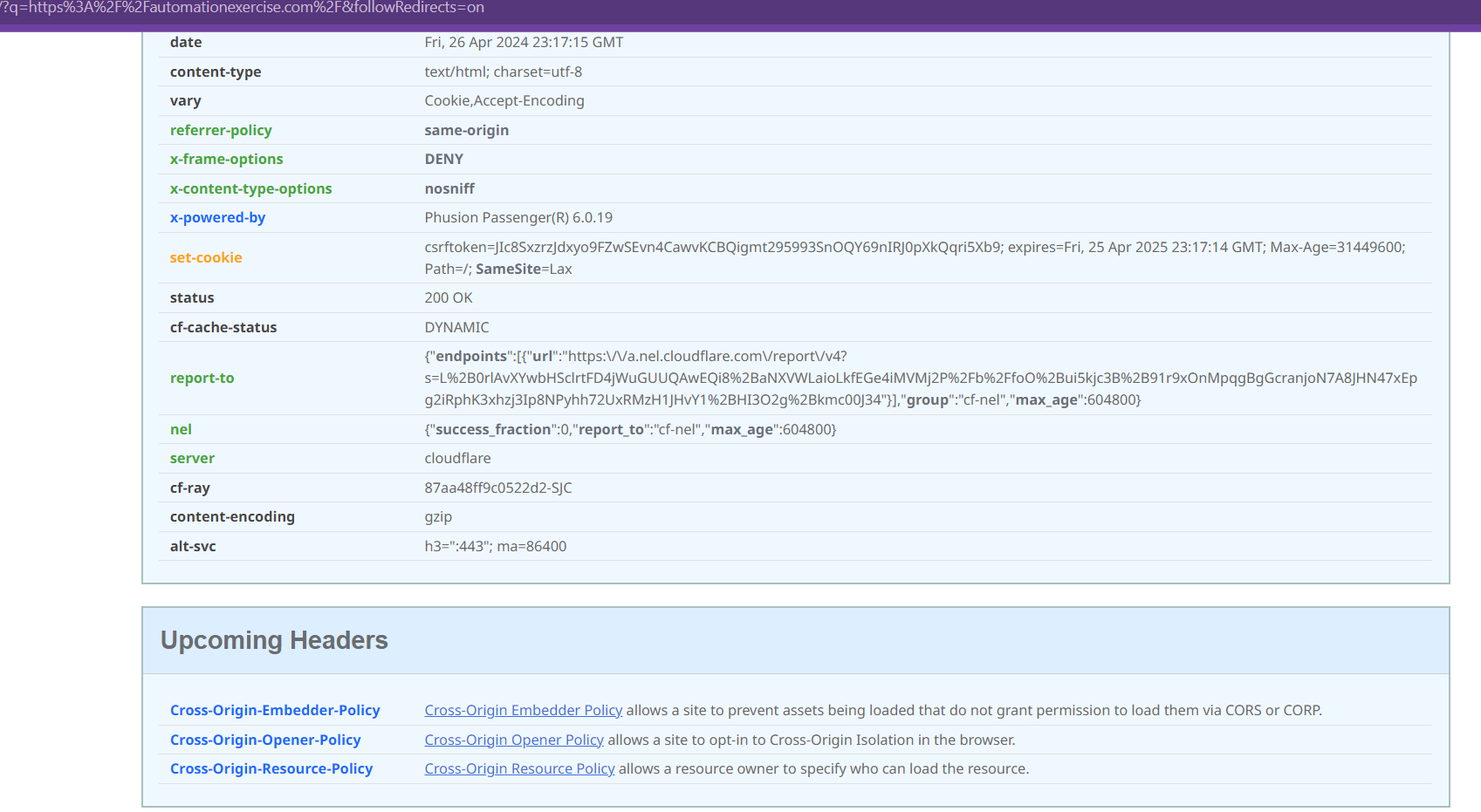
Коваленко Євгеній Андрійович

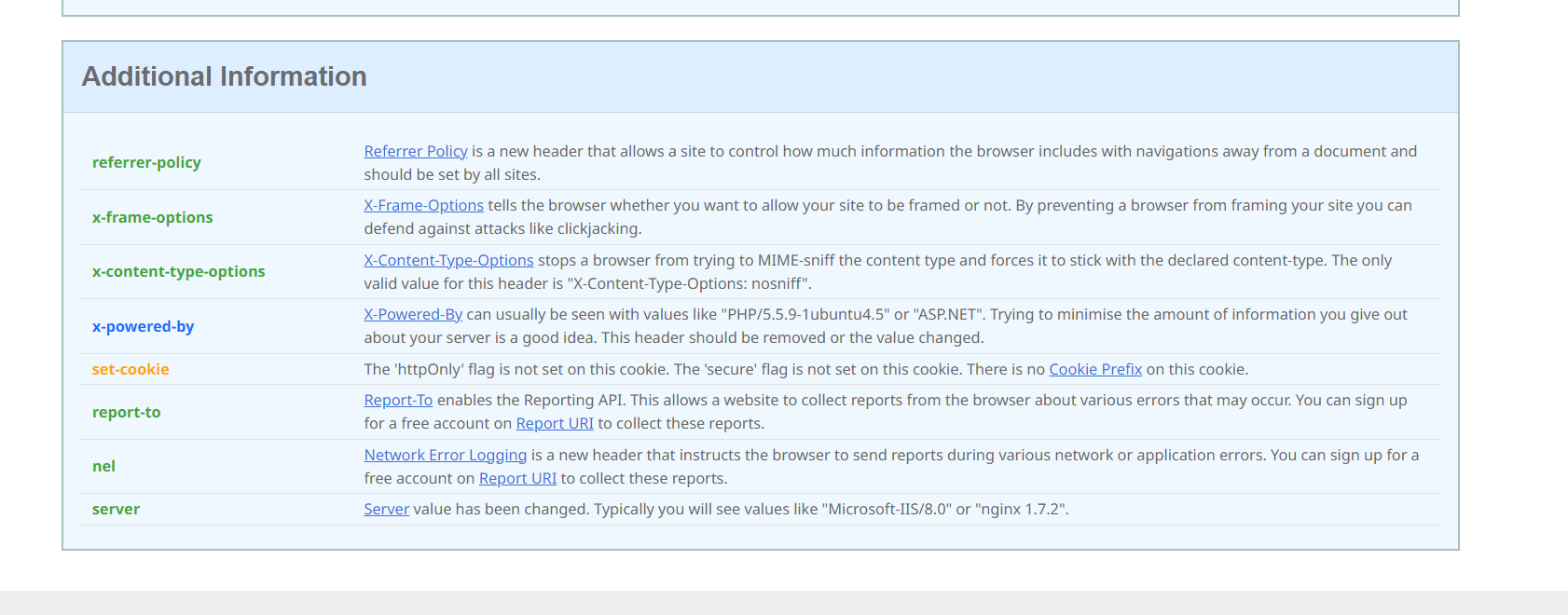
Група   41 ІПЗ

Факультет   інформатики

Викладач: Кархут В.Я.







1. Повідомлення про Strict-Transport-Security відноситься до заголовка HTTP відповіді, відомого як HTTP Strict Transport Security (HSTS). Цей заголовок використовується веб-серверами для того, щоб вказати веб-браузерам або іншим клієнтам, що сайт має бути доступний тільки через безпечні з'єднання HTTPS. Якщо цей заголовок налаштовано, то всі спроби доступу до сайту через незахищений HTTP автоматично перенаправляються на HTTPS, що збільшує безпеку, запобігаючи атакам типу "людина посередині".

Що це може означати для безпеки сайта:

Захист від перехоплення: Заголовок HSTS допомагає убезпечити користувачів від атак, які можуть використовувати перехоплення нешифрованих запитів. Наприклад, якщо користувач спробує ввести URL сайту без вказівки протоколу "https" (замість цього вводить "http"), браузер автоматично перенаправить на безпечну версію сайту.

Примусове використання HTTPS: Завдяки HSTS сайт може забезпечити, що всі комунікації з користувачами проходять через HTTPS, замість HTTP, що підвищує безпеку шляхом шифрування даних.

Захист від "downgrade attacks": Атаки, які знижують рівень безпеки з'єднання, наприклад, змушуючи браузер перейти з HTTPS на HTTP, блокуються HSTS.

2. Повідомлення про Content-Security-Policy (CSP) стосується заголовка HTTP, який допомагає запобігти деяким типам атак, таким як Cross-Site Scripting (XSS) та інші вектори внесення шкідливого коду. Заголовок CSP дозволяє адміністраторам веб-сайтів контролювати ресурси, які користувач може завантажувати для даної сторінки, зазначаючи легальні джерела виконання скриптів, стилів та інших ресурсів.

Ось основні аспекти, що їх означає наявність та правильне використання CSP:

Захист від XSS та інших ін'єкцій

CSP може значно знизити ризик XSS атак, оскільки веб-додаток декларує, які джерела є довіреними. Наприклад, якщо атакувальник спробує вставити шкідливий скрипт у веб-сторінку, браузер не виконає його, якщо джерело не відповідає зазначеним у політиці CSP.

Контроль джерел ресурсів

За допомогою CSP, адміністратори можуть вказувати, звідки можна завантажувати різні типи ресурсів, такі як скрипти, стилі, зображення, шрифти, медіа та інші. Наприклад, можна дозволити скрипти лише з домену CDN, що підвищує безпеку, обмежуючи виконання потенційно шкідливих скриптів з ненадійних джерел.

3. Повідомлення про Permissions-Policy відноситься до заголовка HTTP, який дозволяє веб-сайтам керувати дозволами на використання певних можливостей у сучасних браузерах. Цей заголовок дає можливість сайту вказувати, які API і функції можуть бути використані всередині браузера, тим самим підвищуючи безпеку та контроль над функціональністю.

Що означає Permissions-Policy:

1) Контроль доступу до API: За допомогою заголовка Permissions-Policy веб-сайт може обмежити доступ до певних веб-API, таких як камера, мікрофон, геолокація, вібрація, сповіщення тощо. Це допомагає запобігти зловживанням цих API шкідливими скриптами.

2) Покращення конфіденційності користувачів: Керування доступом до API може значно підвищити приватність користувачів, оскільки сайт має явно вказати, що він хоче доступ до певних функцій браузера.

3) Зменшення вразливостей: Шляхом обмеження доступу до потенційно небезпечних функцій, сайти можуть зменшити ризик атаки через уразливості в цих API.