

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

**Український державний університет науки і технологій**

Кафедра «Комп’ютерні інформаційні технології»

**Лабораторна робота №4  
з дисципліни «Безпека програм та даних»**

**на тему:**

**«**Захист веб-застосунків від OWASP Top 10 вразливостей.»

Виконав:

студент гр. ПЗ2011

Кулик С.В.

Прийняв:

доц. Жеваго О. О.

Дніпро, 2023

**Тема.** Захист веб-застосунків від OWASP Top 10 вразливостей.

**Мета.** Ознайомитись з OWASP Top 10. Навчитись уникати найбільш розповсюджених вразливостей.

**Завдання**

1. Google представив гру, що полягає в пошуку XSS-вразливостей, з метою поширення інформації про цей найнебезпечніший і найпоширеніший тип вразливості. Гра покаже як виявляти XSS, це знання допоможе вам запобігати помилкам у ваших додатках. Загалом у грі 6 рівнів, у разі труднощів у виконанні завдань можна скористатися підказками.

Виконайте всі завдання з пошуку вразливостей до атак XSS на сайті https://xssgame.appspot.com.

2. OWASP Juice Shop - це, мабуть, найсучасніший і найскладніший незахищений веб-додаток! Його можна використовувати в тренінгах з безпеки, ознайомчих демонстраціях, CTF і в якості піддослідного кролика для тестування інструментів безпеки! Juice Shop охоплює вразливості з усієї першої десятки OWASP, а також багато інших недоліків безпеки, знайдених в реальних додатках!

Перейдіть за посиланням https://demo.owasp-juice.shop і опишіть, які вразливості ви тут знайшли і яким чином.

**Індивідуальне завдання (варіант №6)**

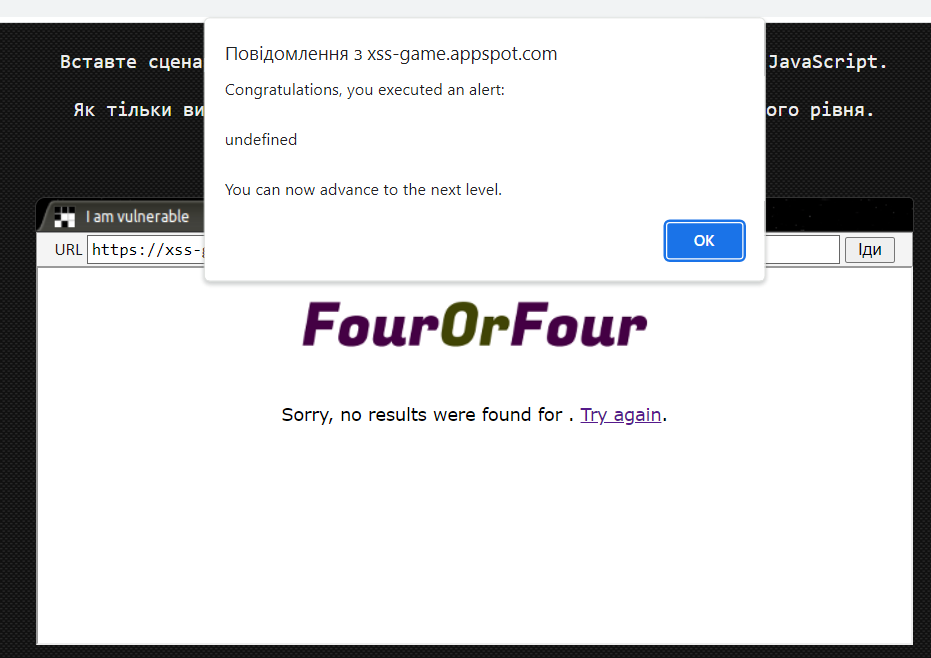
Перейдіть за посиланням і виконайте усі запропоновані дії, щоб ознайомитись з типом вразливості. Опишіть у звіті виконані дії, та проведіть аналіз результатів.

<https://www.hacksplaining.com/exercises/xss-reflected>

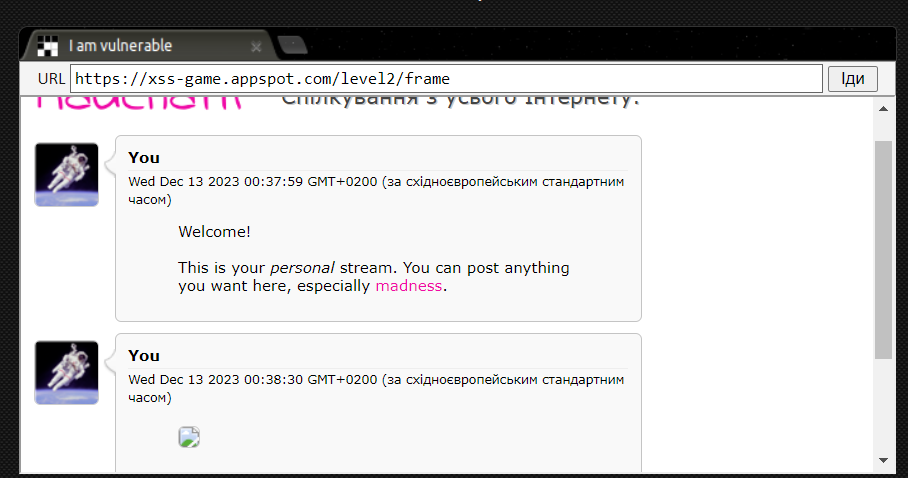
<https://application.security/free-application-security-training/owasp-top-10-user-enumeration>

**Пошук XSS-вразливостей у грі**

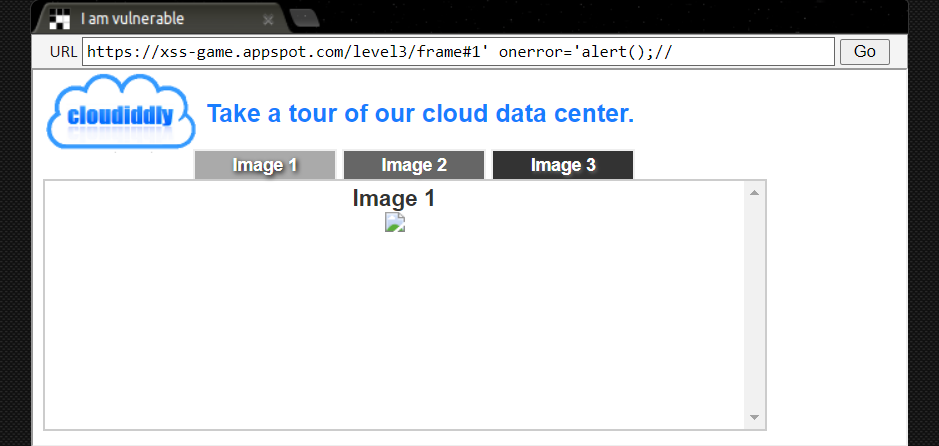
Гра складається з 6 рівнів, на кожному з яких треба виконати пошук вразливостей.  
1. Вставити код в рядок пошуку: <script>alert()</script>



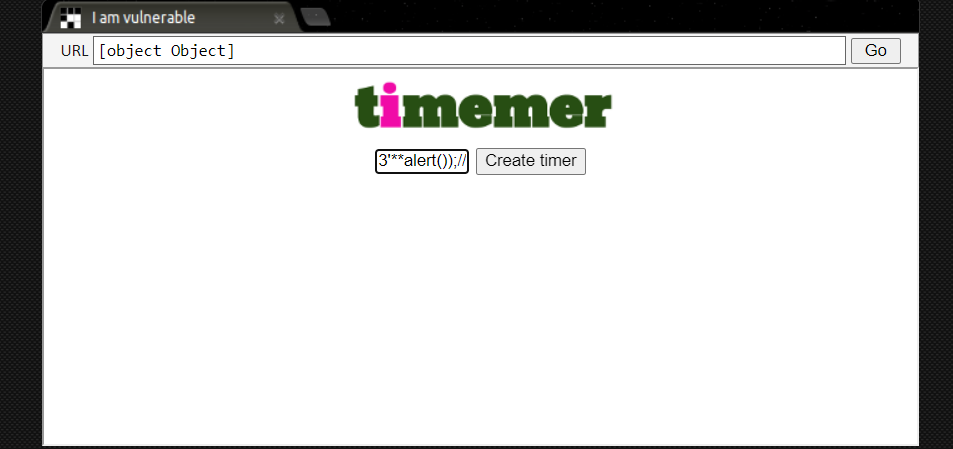
2. Вставити рядок коду в коментарі: <img src='x' onerror='alert()'>



3. Дописати в браузерній строкі рядок коду: 1' onerror='alert();//



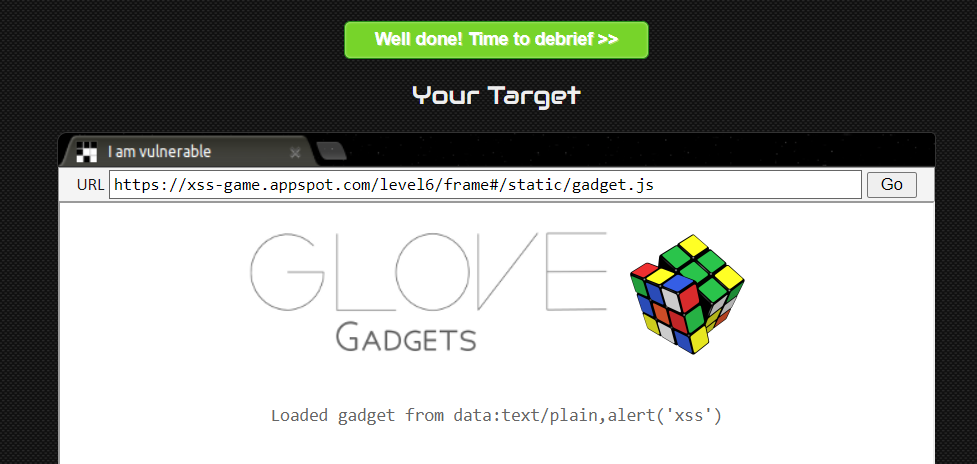
4. Дописати в рядок таймера: '\*\*alert());//



5. Ввести значення почти як рядок: https://xss-game.appspot.com/level5/frame/signup?  
next=javascript:alert()

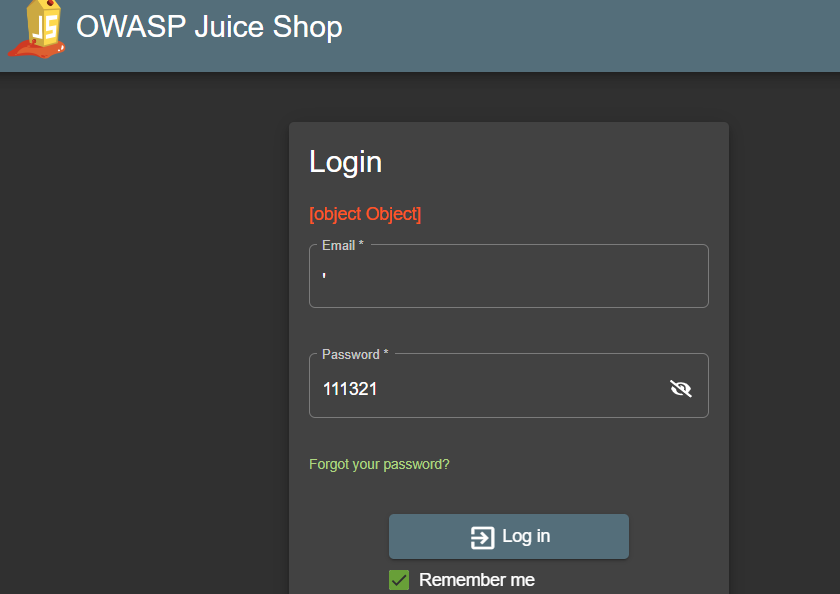


6. Замінити ЮРЛ адресу на наступну: https://xss-game.appspot.com/level6/frame#  
data:text/plain,alert('xss')

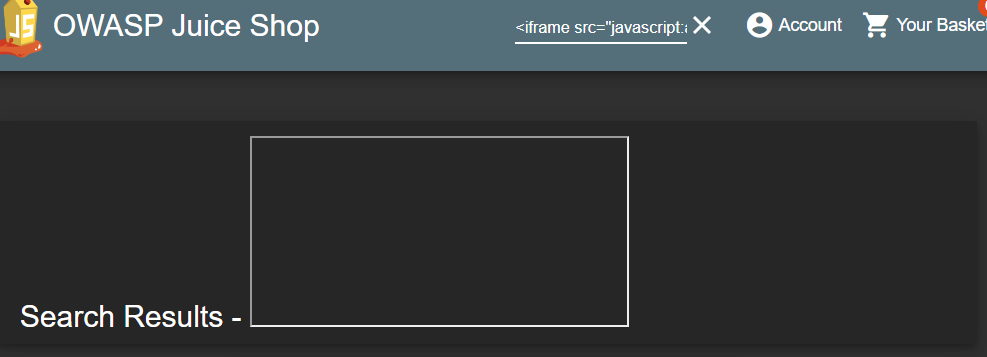


**Пошук вразливостей на сайті OWASP Juice Shop**

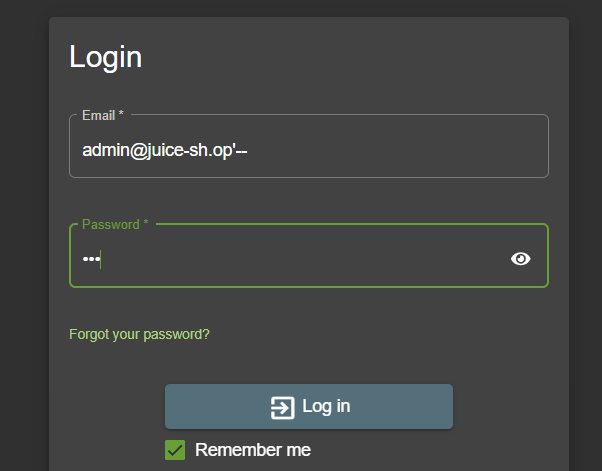
1. SQL-вразливість, вставивши на місце логіну звичайні одинарні лапки отримаємо наступну помилку:

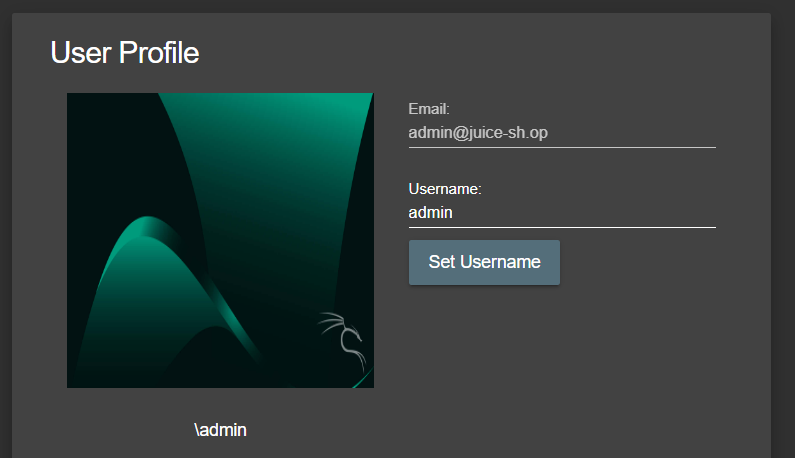


1. XSS – ін’єкція, для використання ми введемо у вікно пошуку наступний текст:

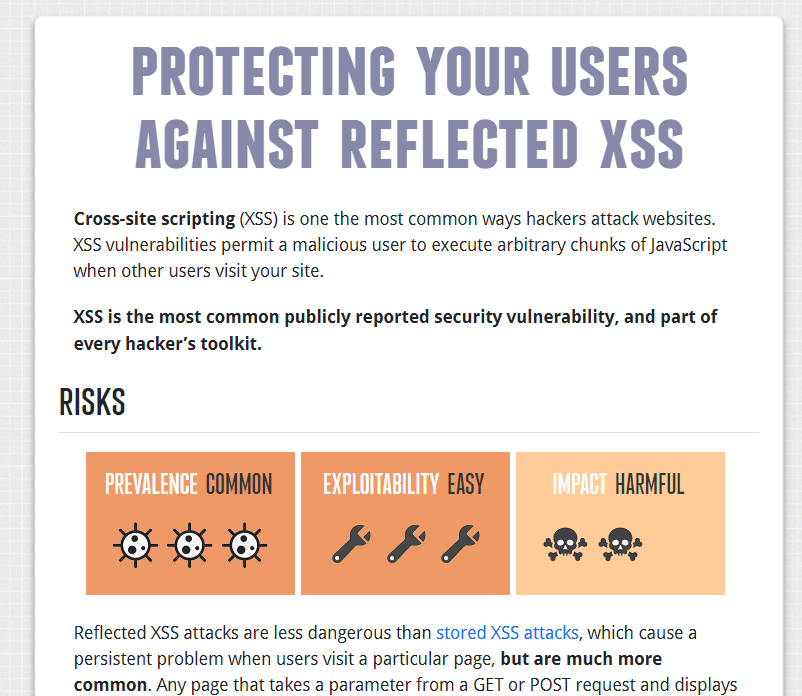


1. Вхід у систему під акаунтом адміністратора за допомогою SQL-вразливості, ввівши будь-які символи замість пароля:





**Індивідуальне завдання**

1. Навчальна сторінка складається з 14 сторінок, на яких розповідається про XSS атаки. Після проходження переходить на сторінку

**Висновки**

Забезпечення безпеки веб-застосунків від вразливостей з OWASP Top 10 - ключовий аспект розробки. На перший план виходить освіта команди та регулярні аудити для виявлення та виправлення вразливостей. Сильна аутентифікація, належна обробка введення та захист від крос-сайт атак є важливими. Крім того, важливо налаштовувати системи, валідувати вхідні дані та захищати сесії та ідентифікатори. Захист від небезпечного коду, обробка небезпечних запитів та захист від незахищених API є також критичними. Ця комплексна підхід допомагає створювати більш безпечні веб-застосунки з ефективним уникненням потенційних загроз.