Магістерська кваліфікаційна робота

на тему: «Удосконалення методу визначення рівня захищеності web – систем від атак типу cross – site scripting»

Роботу виконала: студентка групи УБ-18м Жаворонок Д.

Науковий керівник: к. т. н., доц Сачанюк - Кавецька Н.В.

Актуальність теми дипломної роботи

Web - сайт є своєрідним діалоговим вікном між покупцем і виробником. Зловмисники можуть як і викрадати персональні дані клієнтів, так і спеціально видозмінювати сайт, або перенаправляти користувачів на інші необхідні хакерам ресурси. Зломи можуть бути абсолютно різні.

Саме тому, удосконалення методів і систем захисту web – ресурсів від атак залишається актуальною науковою проблемою, враховуючи постійне вдосконалення методів та інструментів атак зловмисниками.

Мета дипломної роботи

Мета даної роботи - проведення аналізу існуючих методів визначення наявності вразливих місць у ПЗ, виявлення недосконалостей у аналогів та удосконалення методу визначення рівня захищеності web – систем від атак типу cross – site scripting та підвищення показника виявлених вразлвостей у web – додатках.

Задачі

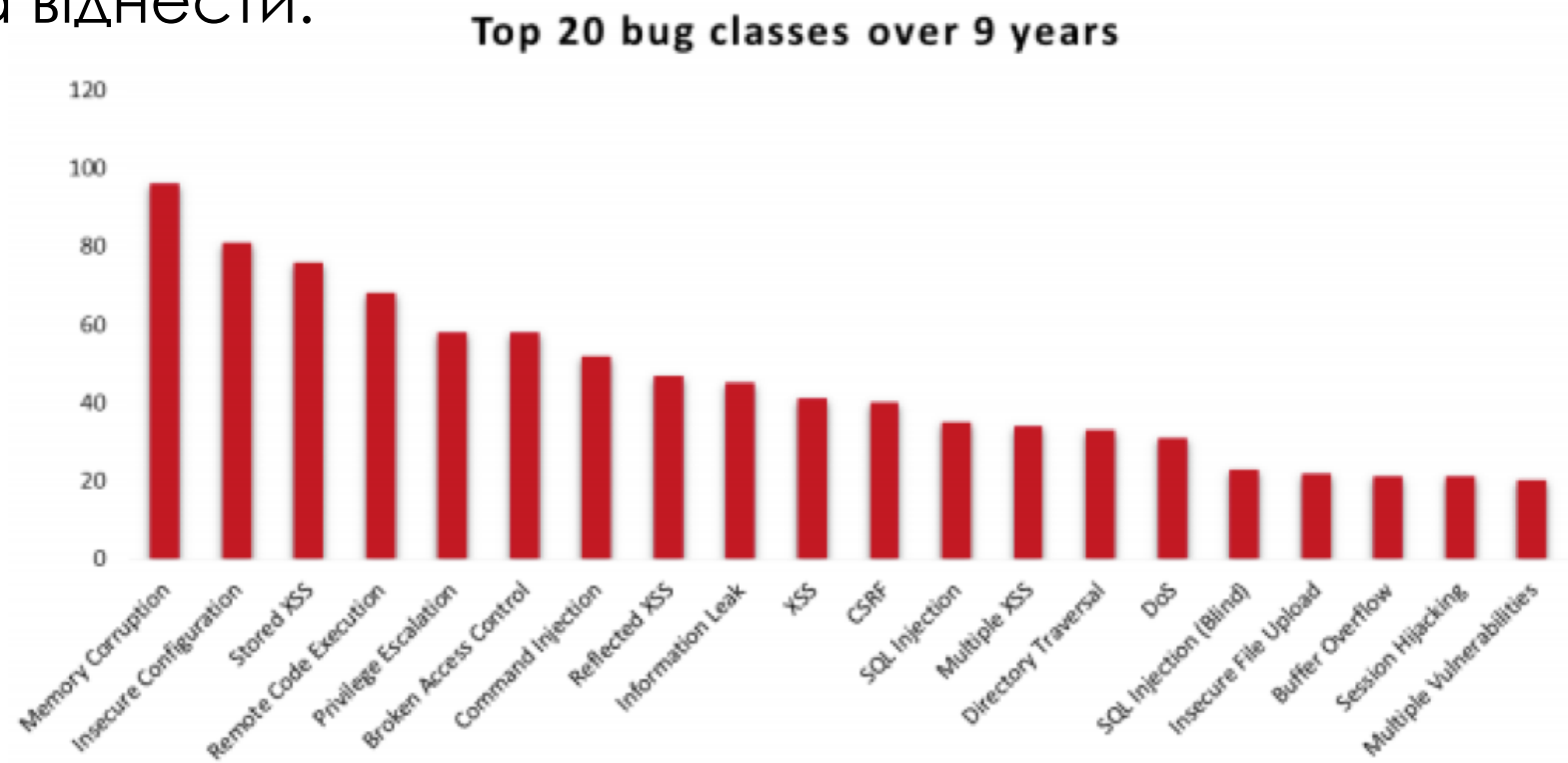
1. Аналіз основних загроз та особоливостей визначення рівня захищеності web – додатку від атак типу Cross – Site Scripting.
2. Аналіз аналогів реалізації методів визначення захищеності додатку.
3. Розробка програмного засобу для реалізації удосконаленого методу.
4. Провести економічний аналіз реалізованого продукту

Відомості про XSS атаку та наслідки

Cross – site scripting – це вразливість безпеки в web – середовищі, яка дозволяє зловмиснику компрометувати взаємодію користувачів з уразливим додатком.

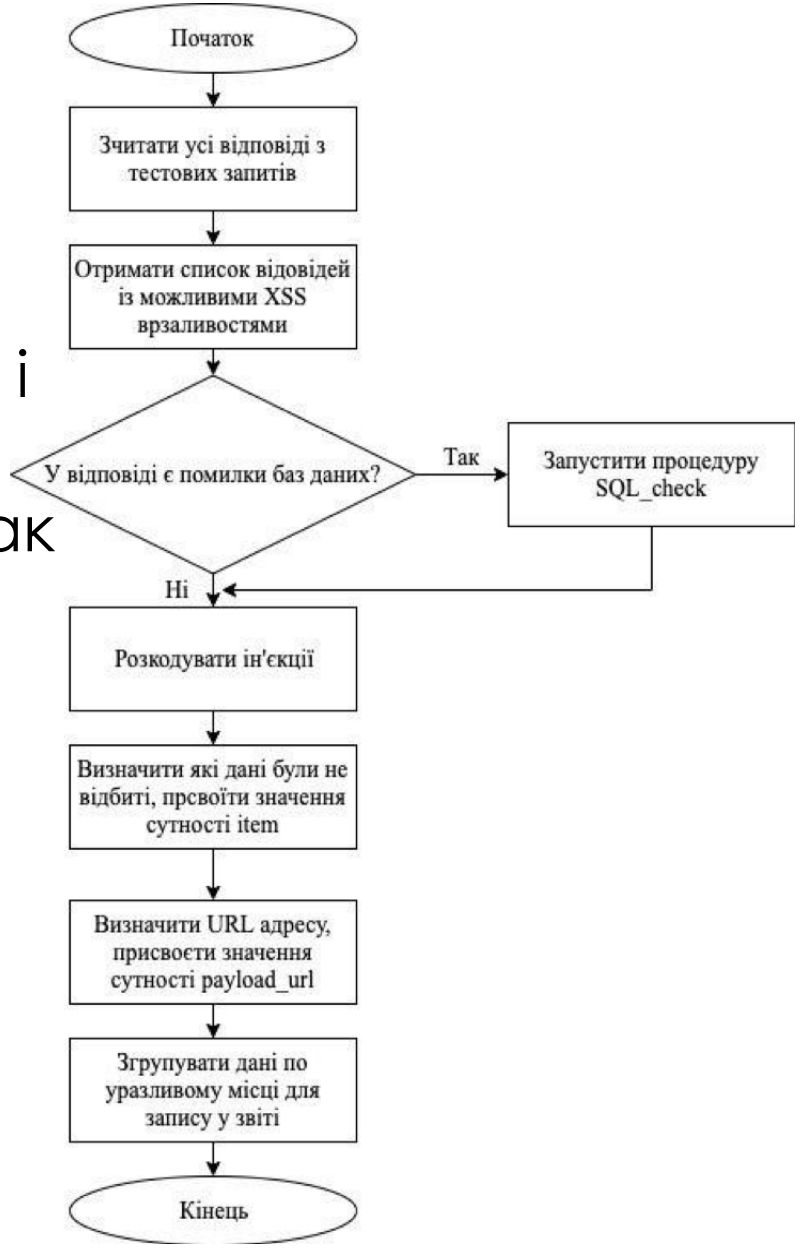
До наслідків можна віднести:

- Крадіжка cookies.
- Keylogging.
- Fishing



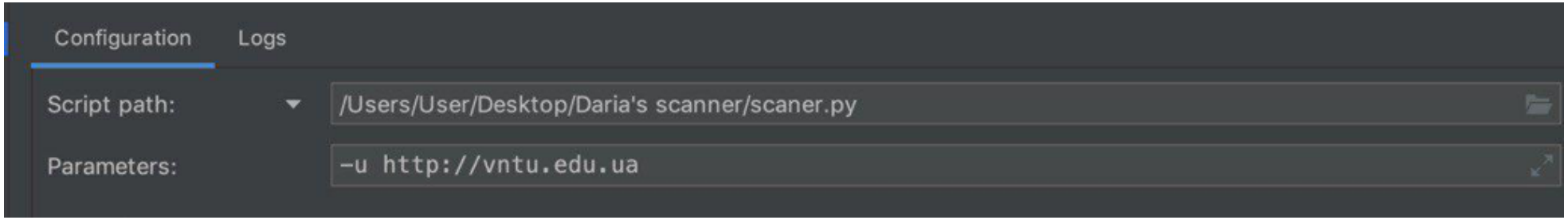
Вигляд розробки удосконаленого методу

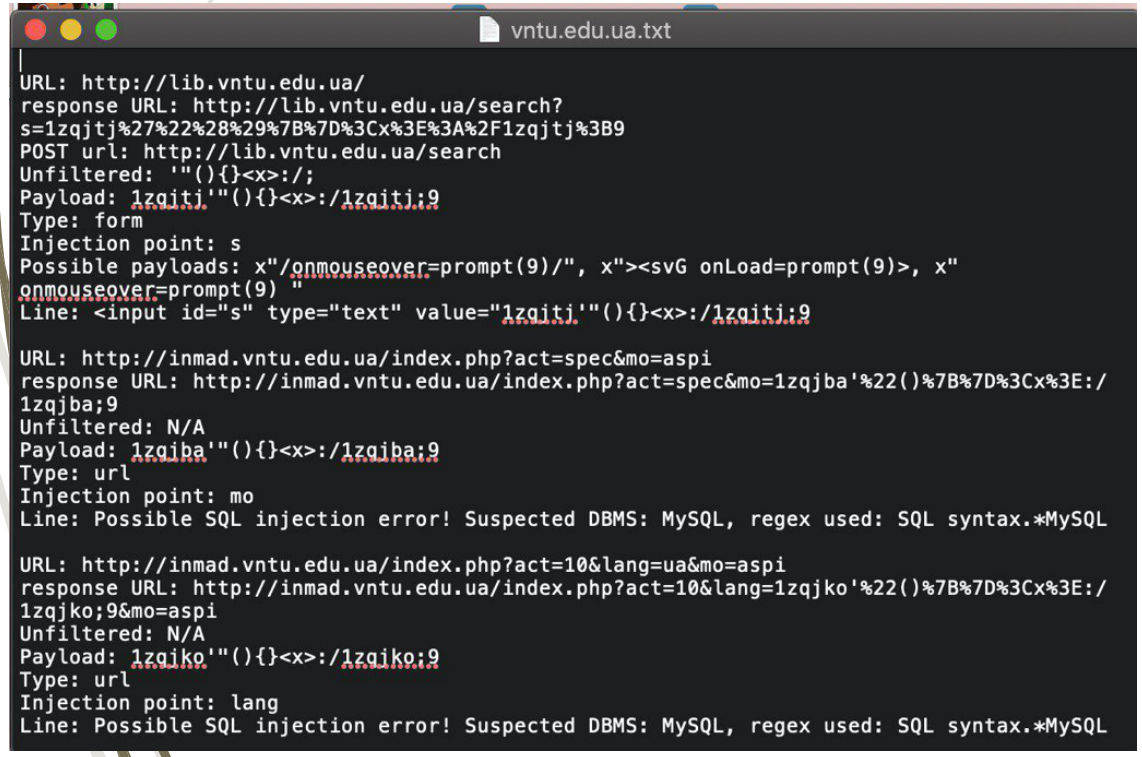
Завдяки запитам, які генеруються, аби спровокувати помилки SQL через XSS атаку та розробленому модулю, який зчитує і визначає тип помилки (а саме SQL) кількість пропущених вразливих місць до атак типу cross – site scripting завдяки модифікації методу зменшується.



Вигляд розробки та результатів сканування

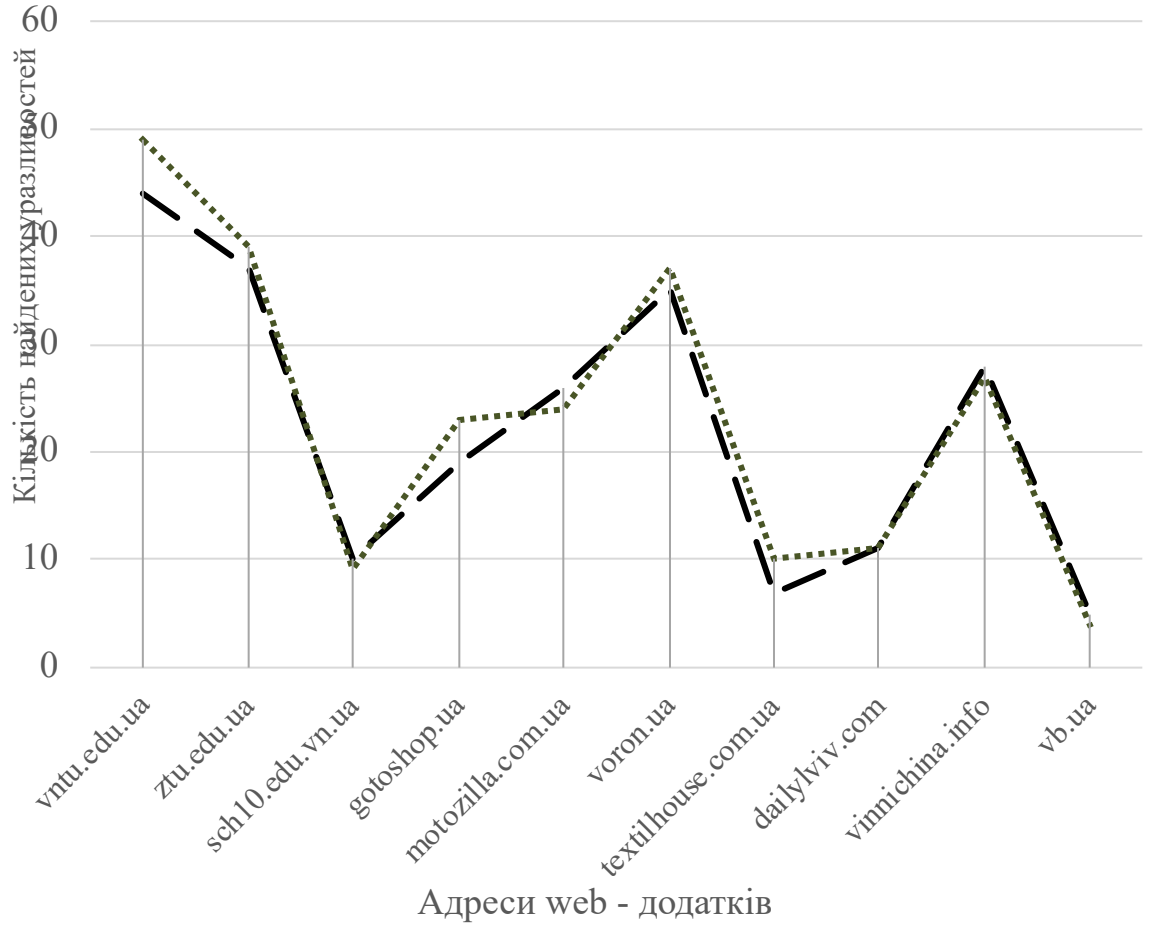
Користувач має вказати адресу web – сайту для початку перевірки:





Як результат, для кожного web – додатку створиться файл .txt із найденими вразливими місцями та детальною інформацією, що допоможе розробнику швидше усунити проблему у коді web - сайту

Апробація удосконаленого методу



Для апробації методу було проведено порівняльне Тестування 10 web – додатків

В наслідок чого, сканер на основі удосконаленого методу показав результат на **4.72 %** кращий, ніж аналог ZAP.

Висновки

Результатом роботи програмна реалізація удосконаленого методу визначення рівня захищеності web – системи від атак типу XSS. Представлені графіки ефективності даного методу.

Програмна реалізація методу має високу швидкодію, що дозволяє говорити про доцільність її використання в поточній розробці та активному використанню, для протидії з'явленню вразливих місць у web – системах із динамічною розробкою.

Дякую за увагу!