Лайчук А.А., магістрант,
Єфіменко А. А., к.т.н., доцент
Державний університет «Житомирська політехніка»

ПРИНЦИПИ СТВОРЕННЯ ЗАВДАНЬ ЗА НАПРЯМКОМ WEB ДЛЯ ПРОВЕДЕННЯ НАВЧАЛЬНИХ КІБЕРБЕЗПЕКОВИХ ДОСЛІДЖЕНЬ ТА CTF-ЗМАГАНЬ

Створення безпечних веб-додатків має вирішальне значення через конфіденційні дані, які часто ними обробляються. Стрімкий розвиток технологій супроводжується появою нових вразливостей, що можуть призводити до крадіжки даних, фінансових збитків і репутаційних втрат. В таких умовах, навчання та підготовка фахівців у галузі кібербезпеки стає все більш важливим завданням.

Метою цього дослідження є розробка та формулювання принципів створення завдань за напрямком Web для проведення навчальних кібербезпекових досліджень та CTF-змагань, що дозволять студентам і початківцям у галузі кібербезпеки практично освоювати методи захисту веб-додатків і глибше розуміти механізми кіберзагроз. Це сприятиме підвищенню їхнього рівня професійної підготовленості та навичок у виявленні та усуненні вразливостей, а також застосуванні сучасних інструментів і технологій для забезпечення безпеки в реальних умовах.

У сфері кібербезпеки змагання «Захоплення прапора» (Capture the Flag, CTF) — це вправи, під час яких учасники, працюючи самостійно або в командах, виявляють та використовують вразливості системи для здобуття «прапора» — певного фрагмента інформації. Завдання в веб-безпеці включають веб-програми з вразливостями, які потрібно виявити та експлуатувати.

Розробка завдань для CTF-змагань з категорії Web складається з шести основних етапів: визначення цільової аудиторії та навчальних цілей, проектування веб-додатків і завдань, встановлення рівня їхньої складності, вибір інструментів для розробки, створення вразливих веб-додатків, а також тестування та експлуатація вразливостей. При дотриманні цього циклу розробки слід враховувати наступну інформацію:

- Актуальність завдань категорії Web, що розробляються і в подальшому слугують для навчання, тісно пов'язана з поширеністю сучасних вразливостей. Станом на 2021-2024 роки серед найпоширеніших вразливостей веб-додатків можна виокремити порушення контролю доступу, розкриття конфіденційних даних, підробку запитів на стороні сервера (SSRF), а також SQL-ін’єкції. До цього списку додаються міжсайтовий скриптинг (XSS), порушення автентифікації, неправильна конфігурація безпеки, недостатній захист від атак грубою силою, слабкі паролі користувачів і використання компонентів із відомими вразливостями. [1]
- Категорія веб-безпеки є досить складною, тому в першу чергу слід орієнтуватися на початківців у сфері тестування на проникнення та студентів університетів для того, щоб надати можливість отримати базові навички кібербезпеки в практичних умовах.
- Існує широкий вибір технологій для розробки веб-сайтів, але підбір інструментів значною мірою залежить від завдань та креативності автора. Найчастіше у ході розробки вразливих веб-сайтів використовується веб-сервер Apache, мови програмування Python та PHP, мікрофреймворк Flask та база даних MySQL.
- Для роботи з завданнями з веб-безпеки учасники зазвичай використовують дистрибутив Kali Linux, а також інструменти, що необхідні для експлуатації конкретної вразливості. У випадку, коли завданням передбачене встановлення інструментів із відкритих джерел, слід залишати підказки для учасників, що наштовхнуть їх на ці дії.

Це дослідження є цінним як з теоретичної, так і з практичної точки зору, оскільки дозволяє глибше зрозуміти принципи створення завдань Web-напрямку для CTF-змагань, спрямованих на підвищення рівня підготовки фахівців із кібербезпеки. Такі завдання дають змогу не лише освоїти методи захисту веб-додатків, а й розвинути навички виявлення та усунення вразливостей, використовуючи сучасні інструменти та технології тестування на проникнення. Студенти та початківці набувають практичного досвіду, що є важливим для їхньої кар'єри в кібербезпеці. Крім того, розробка таких завдань також є корисною для авторів, оскільки дозволяє їм досліджувати вразливості, вдосконалювати свої знання та застосовувати їх на практиці, що сприяє кращому розумінню методів захисту від цих вразливостей.[2]

У доповіді буде наведено приклад розробки завдання за напрямком Web із використанням вищеописаних засобів, технологій та дотриманням принципів створення завдань для CTF-змагань.

Список використаних джерел

1. OWASP Top 10:2021. OWASP Foundation, the Open Source Foundation for Application Security | OWASP Foundation. URL: https://owasp.org/Top10/ (date of access: 02.12.2024).
2. Why Is Capture the Flag (CTF) Important in Cyber Security?. Cybersecurity Exchange. URL: https://www.eccouncil.org/cybersecurity-exchange/ethical-hacking/capture-the-flag-ctf-cybersecurity/ (date of access: 02.12.2024).