Стецюк М.В., PhD, ст. викладач
Дейчук Р.Р., здобувач
Школьняк А.Р., здобувач
Хмельницицький національний університет

АЛГОРИТМ АВТОМАТИЗОВАНОГО СКАНУВАННЯ ВЕБ-РЕСУРСІВ ДЛЯ ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ

Сучасні веб-ресурси є ключовими об'єктами для кібератак, оскільки містять вразливі місця, які можуть використовувати зловмисники для несанкціонованого доступу, крадіжки даних або порушення роботи системи. Основні загрози включають DDoS-атаки, SQL-ін'єкції, XSS-атаки та злам адміністративних панелей шляхом підбору директорій. Для захисту від цих загроз необхідно впроваджувати сучасні методи аналізу та тестування безпеки веб-додатків.[1,2]

Одним із ключових способів пошуку вразливостей є сканування директорій, яке може здійснюватися вручну або автоматично. Ручний аналіз дозволяє досвідченим фахівцям знайти приховані файли, конфігураційні дані або критичні точки входу, проте він займає багато часу та вимагає глибоких знань.

Використання спеціалізованих словників для певних CMS або мов програмування дозволяє підвищити точність пошуку. Оптимізація алгоритмів сканування та адаптація до змін у веб-архітектурах є важливими аспектами розробки сучасних систем кібербезпеки, що дозволяють швидко виявляти потенційні загрози та мінімізувати ризики атак.

Алгоритм реалізує автоматизований механізм сканування директорій веб-ресурсів для виявлення потенційних вразливостей. Він базується на концепції багаторівневої рекурсивної енумерації, яка дозволяє досліджувати структуру веб-сайту вглиб, аналізуючи кожен рівень ієрархії директорій. Основною метою є ідентифікація прихованих файлів і точок входу, які можуть використовуватися зловмисниками для атаки. На рисунку 1зображено ключовий компонент алгоритм – обробка User-Agent.[3,4]

Алгоритм починається з ініціалізації параметрів сканування, включаючи базовий URL, глибину рекурсії, словникову базу та режим багатопоточності. Далі генеруються потенційні URL-адреси на основі попередньо заданих словників і здійснює паралельні HTTP-запити до сервера, аналізуючи отримані відповіді.

Рис. 1 – Алгоритм роботи модуля обробки User-Agent

Критерієм успішного виявлення директорії є статус-коди HTTP-відповідей (наприклад, 200 OK або 403 Forbidden), які свідчать про існування ресурсу.

Ключовою особливістю алгоритму є адаптивний контроль рекурсії, який дозволяє визначати необхідну глибину аналізу залежно від отриманих результатів. Якщо знайдено активну директорію, процес поглиблюється, досліджуючи вкладені каталоги. Одночасно застосовується механізм User-Agent-маскування, що мінімізує ймовірність блокування сканера та підвищує ефективність роботи в обхід систем виявлення ботів.[5]

На фінальному етапі відбувається фільтрація та класифікація знайдених ресурсів. Виявлені URL структуруються за рівнем доступності та потенційної вразливості. Автоматичний аналізатор дозволяє оцінити ризики, зокрема наявність форм введення, можливість завантаження файлів або некоректні конфігурації доступу.[6] Після завершення роботи HWSA формує структурований звіт, який містить повний список знайдених директорій, їх статус-коди та можливі загрози.[7]

Таким чином, алгоритм забезпечує швидке, ефективне та гнучке сканування директорій веб-ресурсів, дозволяючи автоматично виявляти приховані файли, оцінювати рівень їхньої доступності та ідентифікувати потенційні вразливості. Це дає можливість використовувати його в процесах пентестингу та кібербезпеки для оперативного пошуку критичних слабких місць у веб-системах.

Список використаних джерел:

1. Білоусов О. Сучасні методи тестування веб-застосунків на вразливості. Комп’ютерні системи та мережі. 2022. № 2. С. 45–53.
2. Ляшенко В., Іванов Д. Автоматизовані методи аналізу безпеки веб-додатків. Журнал інформаційної безпеки. 2023. Т. 15, № 3. С. 77–85.

3. Тищенко Р. Системи автоматизованого тестування веб-ресурсів: монографія. Харків: Вид-во НТУ "ХПІ", 2023. 214 с.
4. Bojinov H., Bursztein E., Boneh D. XCS: Cross Channel Scripting and Its Impact on Web Applications. Proceedings of the 16th ACM Conference on Computer and Communications Security (CCS). 2022. С. 420–431.
5. Raj R., Patel B. Directory Enumeration for Web Application Security Testing. International Journal of Computer Science and Network Security. 2023. Т. 20, № 5. С. 45–52.
6. Grossman J. The Art of Application Security Testing: A Hands-On Guide to Finding and Fixing Vulnerabilities. Addison-Wesley, 2024. 384 с.
7. Stuttard D., Pinto M. The Web Application Hacker’s Handbook: Finding and Exploiting Security Flaws. 3-тє вид. Wiley Publishing, 2023. 950 с.