Сучасні засоби пошуку вразливостей Web-сайтів та серверів та аналіз їх можливостей і практичного використання

Виконав: студент групи ДА-22
Унгул Володимир Валерійович
Керівник: доцент, к.т.н.
Цурін Олег Пилипович

- Мета : Метою роботи є огляд і оцінка можливостей сучасних засобів пошуку вразливостей. Кінцевою метою є збір та аналіз результатів, наведення шляхів боротьби зі знайденими вразливостями за допомогою обраних засобів, на основі сканування переліку сайтів:
- kpi.ua;
- cad.kpi.ua;
- cad.edu.kpi.ua;
- iasa.kpi.ua;
- its.kpi.ua.
- Опис роботи з обраними засобами реалізовано у вигляді сторінки Web-сайту.

Актуальність поставленої задачі

- Актуальність даної дипломної роботи пов’язана з тим, що Web-сервери та Web-сайти - це об’єкти, які постійно піддаються небезпеці. І для їх нормальної роботи потрібний постійний моніторинг.

Класифікація вразливостей і атак

- Аутентифікація
- Авторизація
- Атака на клієнтів
- Виконання коду

Етапи роботи сканерів

- Збір інформації про мережу.
- Виявлення потенційних вразливостей.
- Підтвердження обраних вразливостей.
- Генерація звітів.
- Автоматичне усунення вразливостей. (Цей етап дуже рідко реалізується).

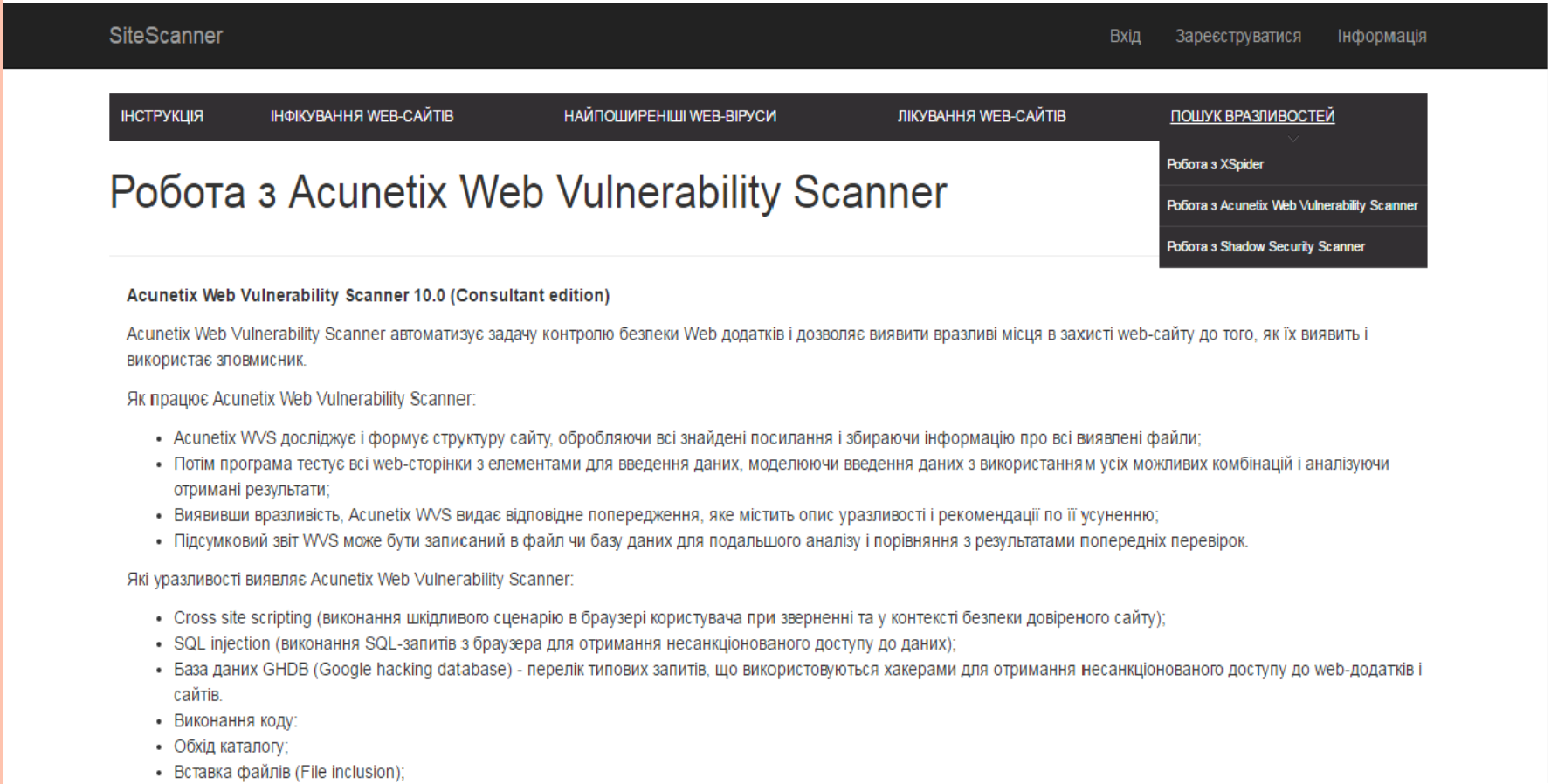
Порівняння загальних можливостей обраних сканерів

Назва	XSpider	Acunetix	SSS
Інтерфейс	Досить простий	(Багато функціоналу) Складний у порівнянні з іншими	Простий та зрозумілий(кожен елемент має спливаючі підказки)
Мова інтерфейсу	Російська	Англійська	Російська або Англійська
Можливість планувати сканування	+	+	+
Боротьба зі знайденими вразливостями	Опис, спосіб рішення, корисні посилання для вирішення.	Опис, спосіб рішення, корисні посилання для вирішення	Опис, спосіб рішення, корисні посилання для вирішення
Звіти	Декілька видів звітів. Звіти генеруються в html (xml, rtf в нових версіях)	Reporter (окрема програма для звітів). Багато різновидів. Детальне налаштування. Експорт у різні формати	Формати: html, xml, chm, pdf, sql, user формат. Вибір аудитів та розділів звіту.
Оновлюваність	База вразливостей поповнюється фахівцями Positive Technologies+автоматичне оновлення баз і модулів програми	Можливість завантажувати оновлення та нові збірки через програмний інтерфейс	Майстер оновлень оперативно оновлює базу даних вразливостей системи і виконавчі модулі. Можливість ручного додавання аудитів через Base SDK.

Порівняння результатів сканування

Назва сканера	Опис результатів
XSpider	Вразливості – 3(вразливість сервісів 80/tcp – HTTP та 443/tcp HTTP SSL). Знайдені вразливості дають доступ до переліку директорій на перегляд, а також можливість визначення наявності користувача в системі. Доступна інформація – 19
Acunetix WVS	високий рівень – 1(SQL ін’єкція у скрипті), середній рівень – 16(скриптова вразливість, незахищена HTML форма, доступні облікові данні користувача, відмова в обслуговуванні), низький рівень – 1, інформаційна вразливість – 289
SSS	1 вразливість з високим ступенем ризику (порт 53 – атакуючий має доступ до кеша)

Опис роботи з обраними засобами



Висновки

- Проаналізовано основні вразливості
- Описана робота з обраними сканерами
- Проведено сканування, порівняно результати та надано рекомендації по їх усуненню
- Розроблена сторінка Web-сайту, яка містить опис роботи з обраними сканерами вразливостей

Дякую за увагу!