Андрусів Соломія

Використовуючи інструментарій розглянутий в попередній темі провести аудит вразливостей Інформаційних ресурсів НаУКМА

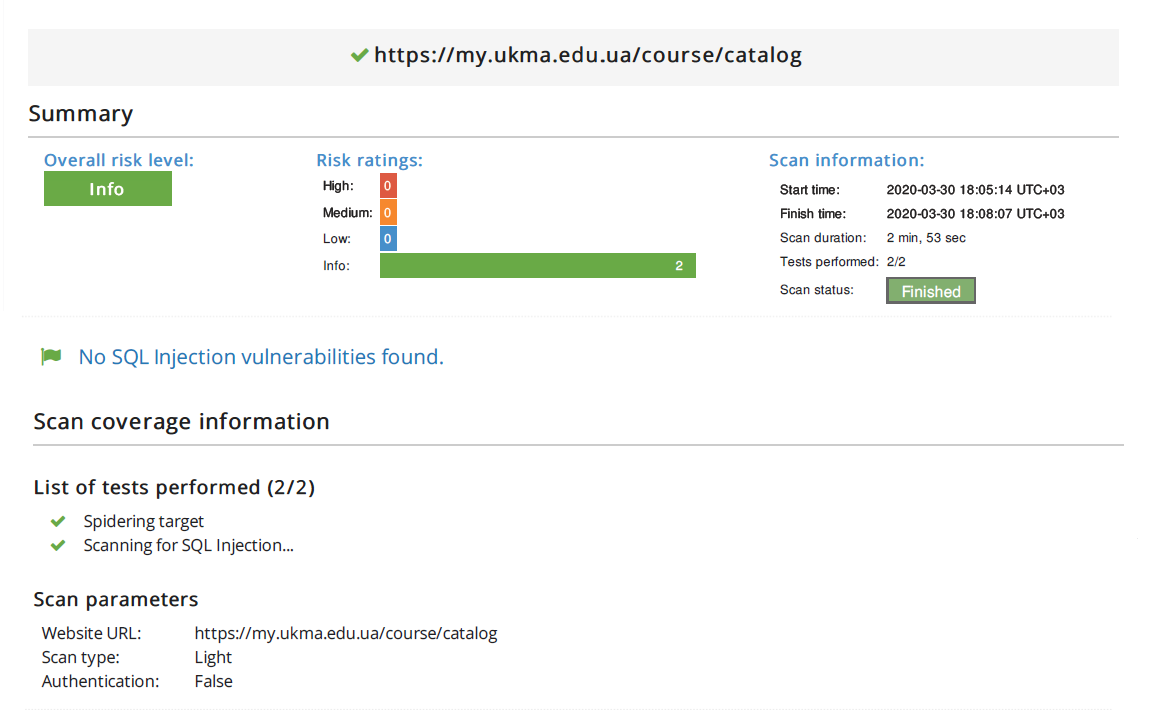
Визначити наявні інформаційні ресурси та стан їх вразливостей

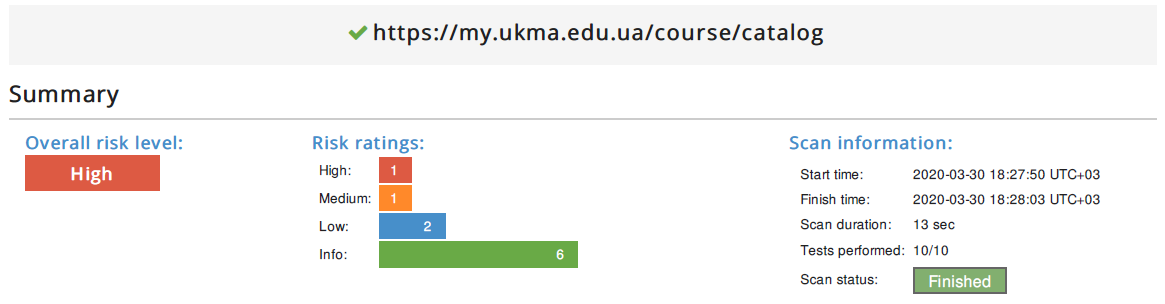
Надати розширений звіт аудиту безпеки

В попередній лабораторній роботі ми розглянули такі основні типи вразливостей для веб-сайтів, як sql-ін’єкції, міжсайтовий скриптінг та багато інших (згідно зі списком OWASP – 10 основних)

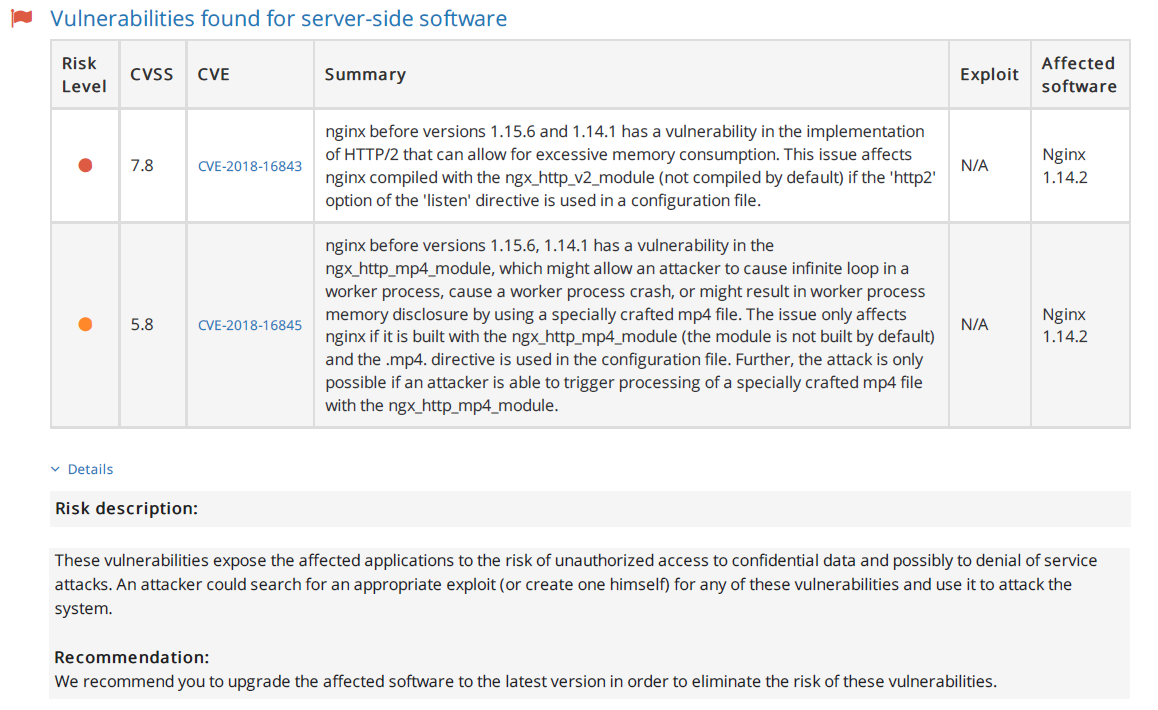
Тому я протестувала два основні сайти НаУКМА – ДістЕду та САЗ на основні типи вразливостей. Для перевірки використала сайт <https://pentest-tools.com>

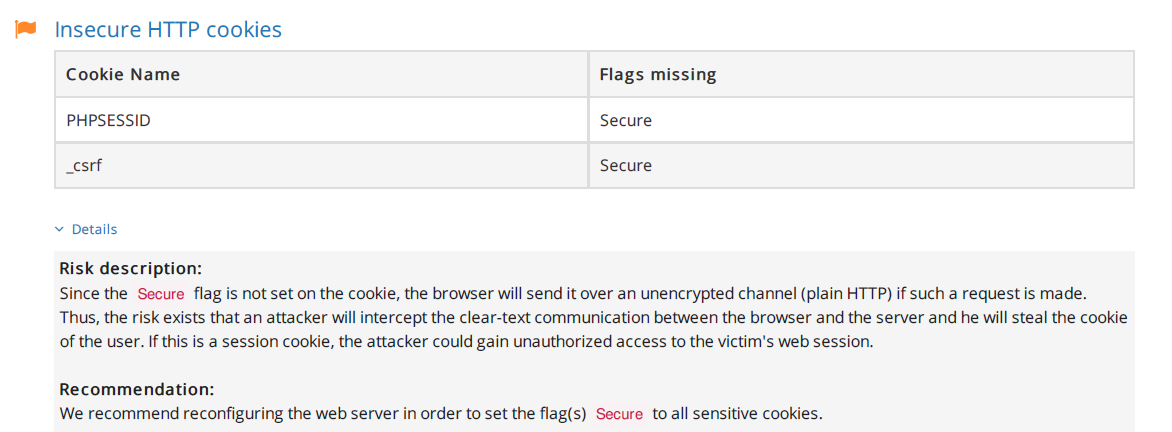
# <https://my.ukma.edu.ua/course/catalog> - САЗ НаУКМА

1. Тестування на SQL-ін’єкції – загроз не виявлено
2. Тестування на найбільш поширені типи вразливостей (застаріле серверне програмне забезпечення, незахищені заголовки HTTP, незахищені налаштування файлів cookie, сертифікат SSL сервера тощо)

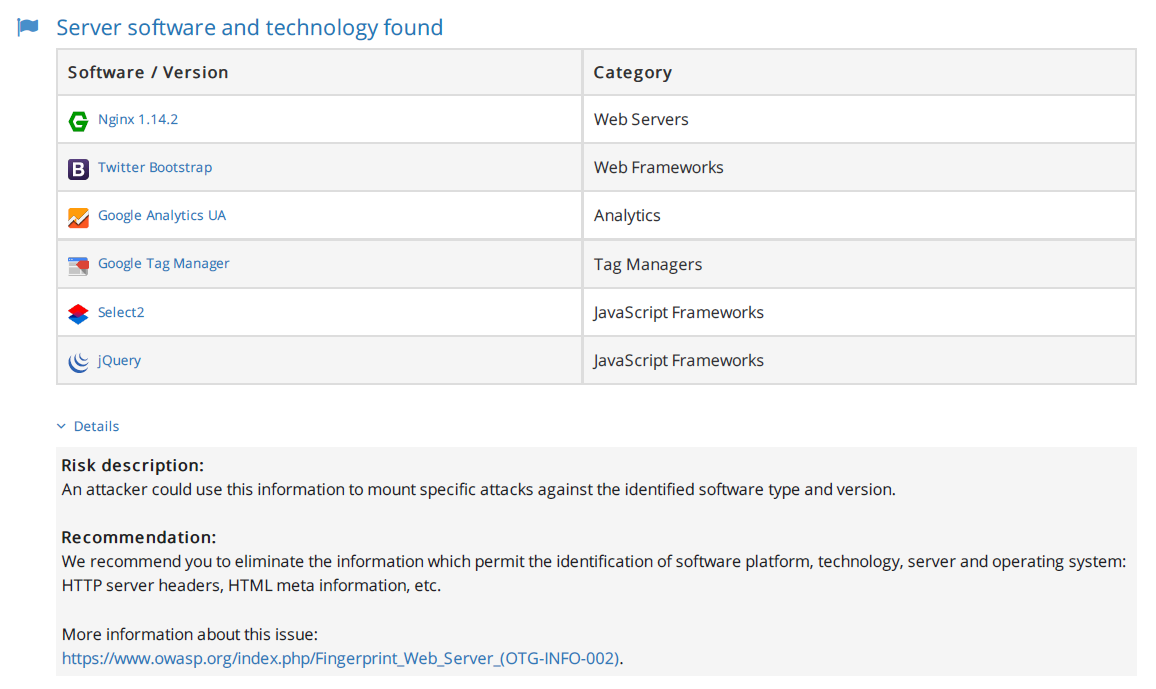
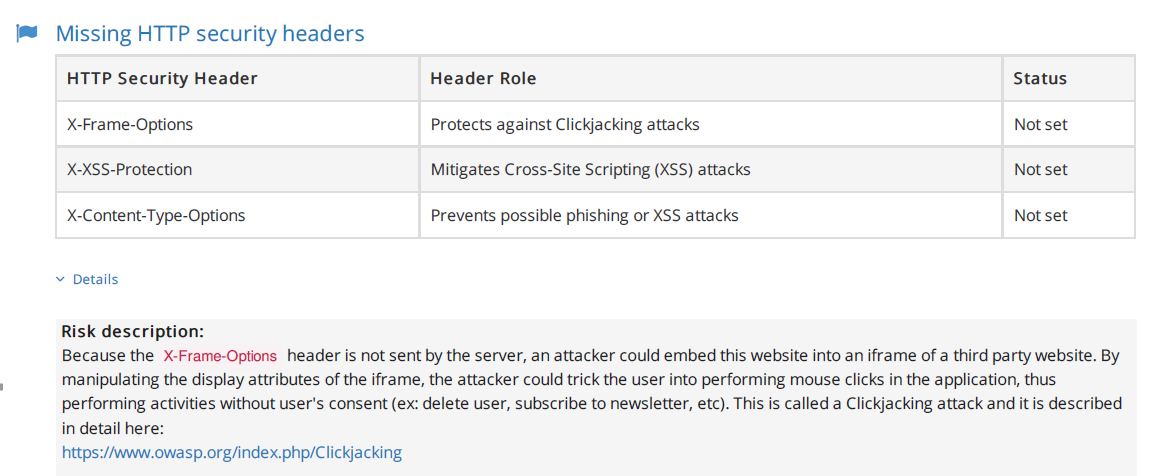


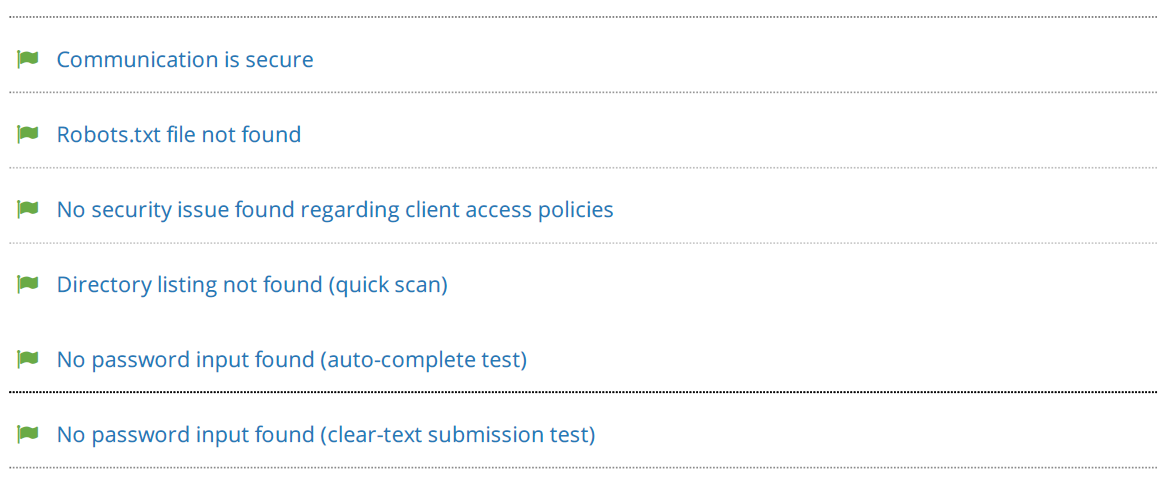
Знайдено деякі проблеми, зокрема:

Не оновлена версія nginx, вразливості якої давно відомі і можуть використовуватись зловмисниками

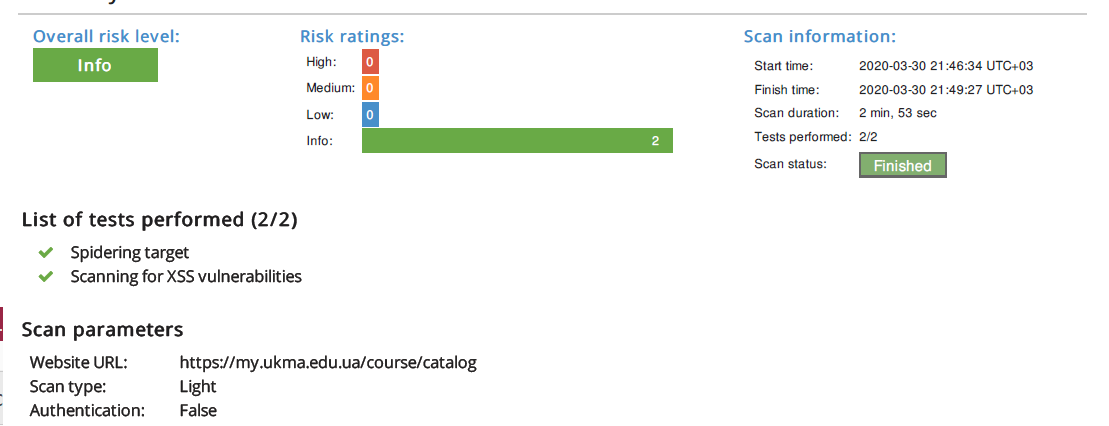
використовуються cookies без помітки secure

відкрита інформація про все основне використане ПЗ

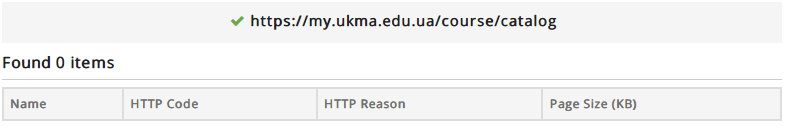
та відкрита можливість для міжсайтового скриптінгу

інші тести пройшли успішно

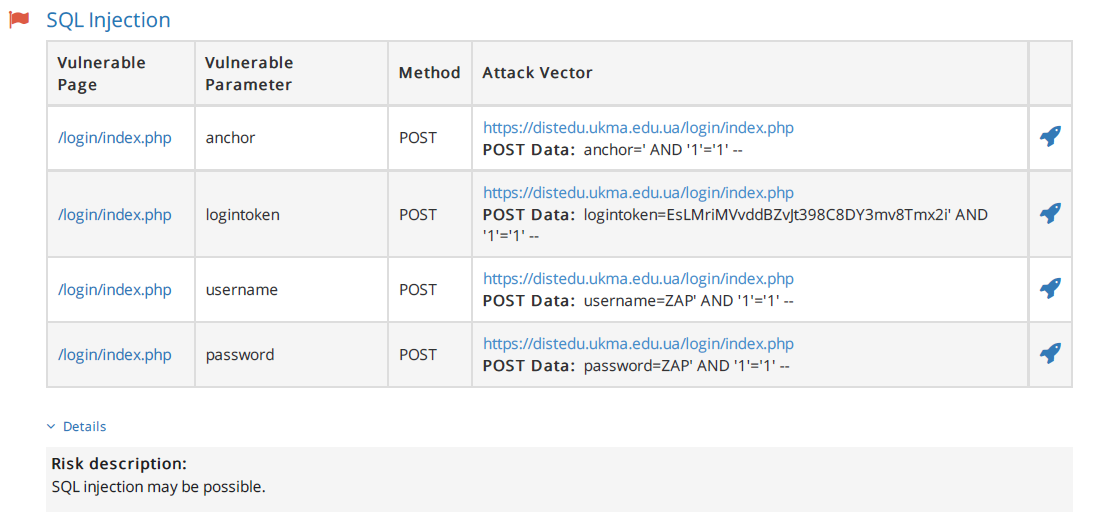
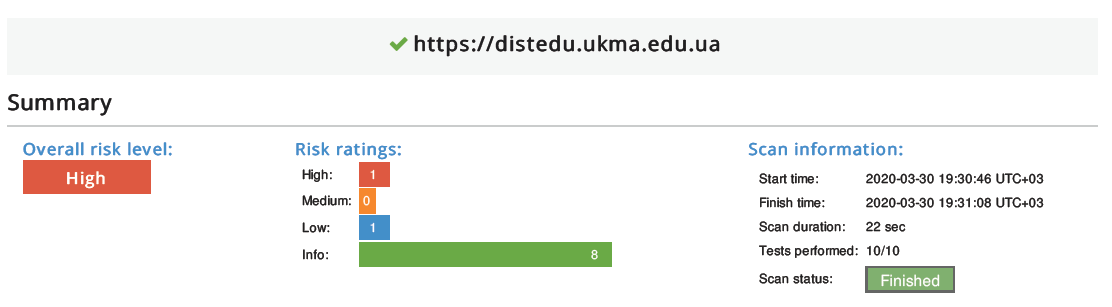
1. Тестування на міжсайтовий скриптінг – вразливостей не знайдено

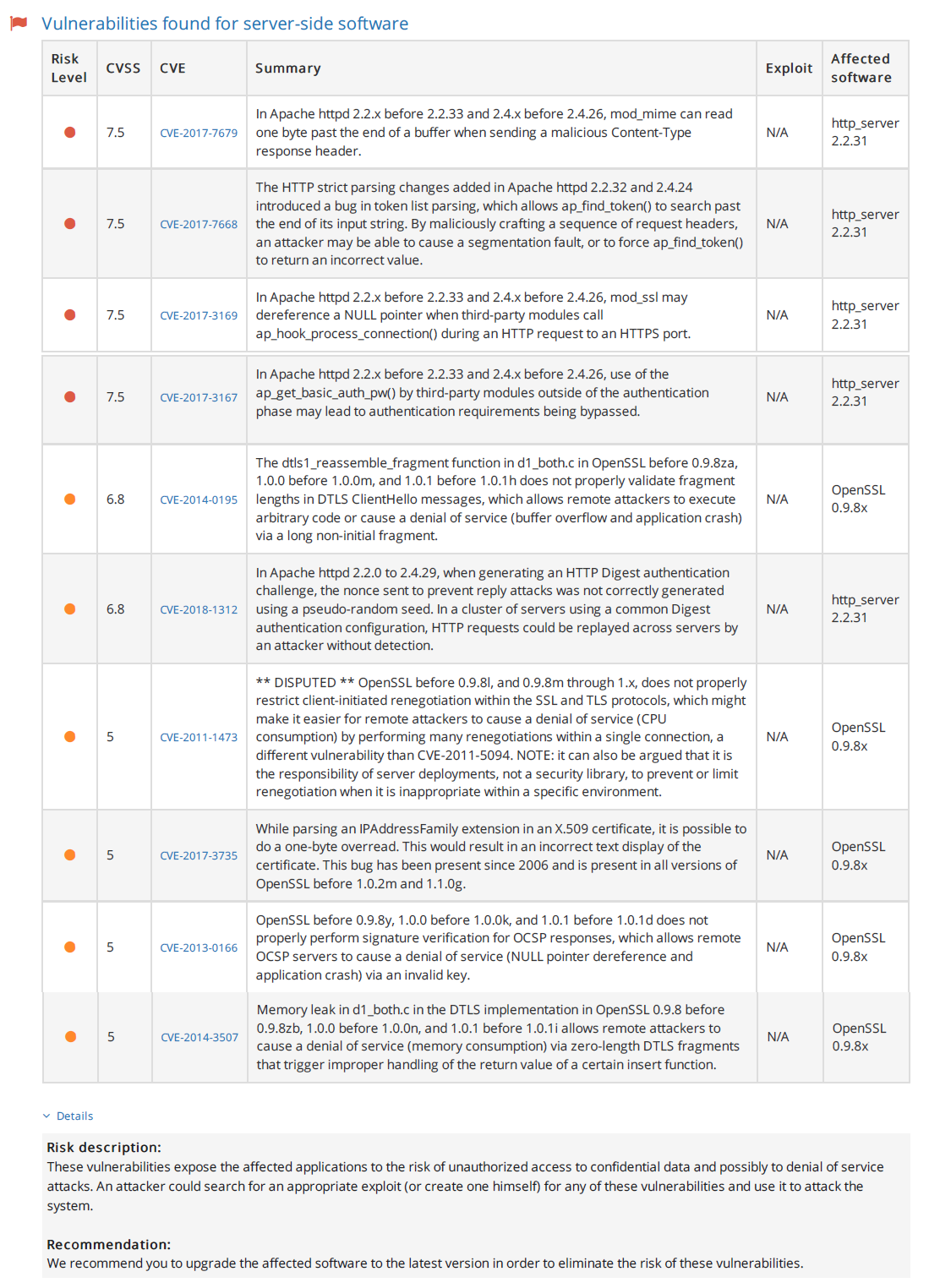


1. Пошук прихованих файлів та папок – прихованих файлів не знайдено

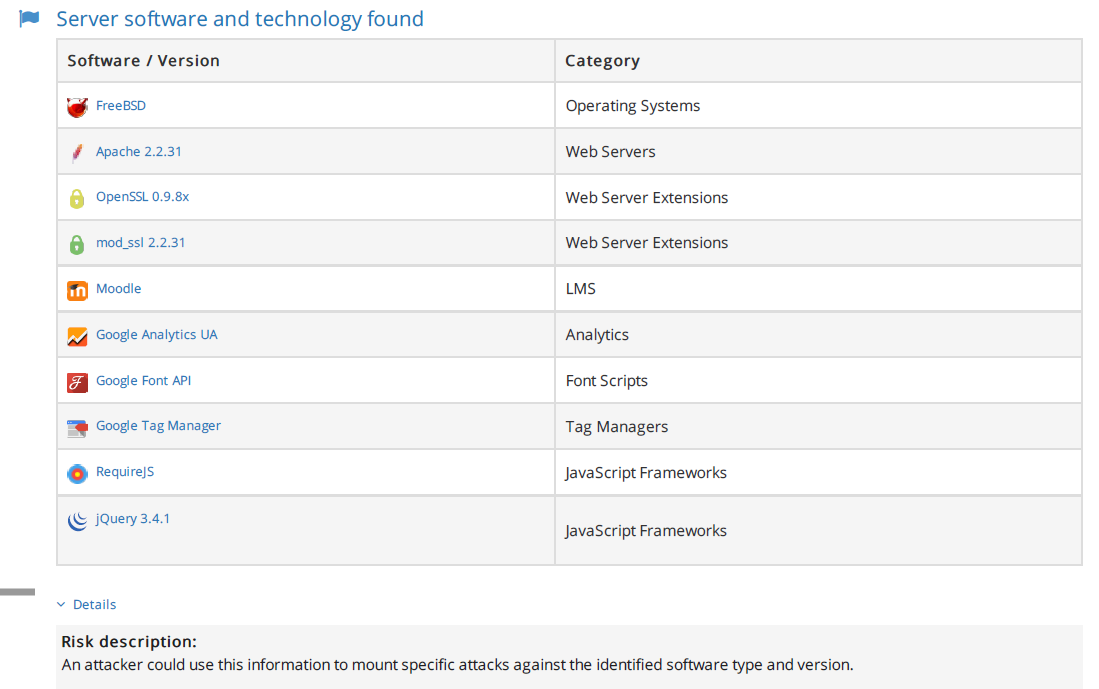


# <https://distedu.ukma.edu.ua> ДістЕду НаУКМА

1. Тестування на SQL-ін’єкції – існує загроза sql-інєкцій, вказані вразливі атрибути
2. Тестування на найбільш поширені типи вразливостей – виявлено деякі проблеми

Деяке програмне забезпечення застаріло та потребує оновлення

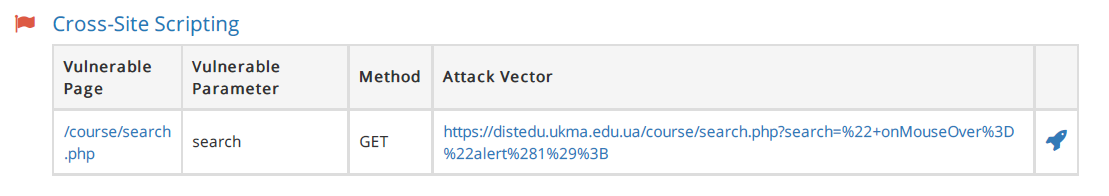
також можна дістати інформацію про версії використаного ПЗ(та, якщо відомі вразливості цих версій, використати їх у своїх цілях)

решта тестів пройшли успішно



1. Тестування на можливість міжсайтового скриптінгу

існує вразливий параметр(при поглибленій перевірці може виявитися що він не один)



1. Пошук прихованих файлів/директорій

Знайдено кілька прихованих директорій, вони не обов’язково мають в собі щось шкідливе, та ця нескладна перевірка може пригодитися при пошуку шкідливих файлів

