УДК 004.056:004.056.3

АВТОМАТИЧЕСКАЯ ОЦЕНКА УЯЗВИМОСТЕЙ ВЕБ-ПРИЛОЖЕНИЙ С ПОМОЩЬЮ CVSS RISK EVALUATOR: ПРАКТИЧЕСКАЯ РЕАЛИЗАЦИЯ И СРАВНИТЕЛЬНЫЙ АНАЛИЗ

И. О. ПЕТРОЧЕНКО
(Представлено: канд. пед. наук, доц. П. П. МАТЕЛЕНОК)

В статье представлена реализация приложения CVSS Risk Evaluator, которое позволяет автоматически определять уровень риска уязвимостей веб-сайтов на основе данных из базы NVD. Приведены результаты тестирования реальных веб-ресурсы, определены используемые технологии и зафиксированы CVE-уязвимости. Проведен сравнительный анализ с онлайн-сервисом Pentest Tools.

В настоящее время есть запрос в учреждения образования на качественную проверку веб-ресурсов организации и при этом с минимальным затрачиванием средств на производство программного обеспечения. Представленное программное обеспечение ориентировано на пассивное получение информации о веб-сайтах. Подход, реализованный в разработанном решении, основан на пассивном анализе полученных ответов, то есть сканировании по косвенным признакам без подтверждения факта наличия уязвимости. Основной принцип его работы заключается в считывании HTTP-заголовков и данных, полученных с сайта, с последующим анализом используемых технологий. На основе этой информации производится поиск соответствующих уязвимостей через API открытых баз данных, таких как NVD. В случае обнаружения совпадений система автоматически выводит список уязвимостей, включая их идентификаторы, уровни критичности и краткое описание. Для дополнительного удобства пользователей программный продукт включает CVSS-калькулятор, который позволяет автоматически рассчитывать стандартизированные оценку критичности уязвимостей. Кроме того, система поддерживает функцию просмотра истории сканирований, позволяя пользователям анализировать результаты предыдущих проверок, отслеживать изменения в состоянии безопасности веб-приложения и сравнивать данные для оценки эффективности мер по устранению уязвимостей. Рассмотри м работу ПО более подробно. Пользователь запускает программу, переходит на вкладку «Сканер» и вводит URL сайта в соответствующее поле ввода. После нажатия кнопки «Сканировать» программа выполняет пассивное сканирование, реализованное функцией scan_website (листинг 1), и определяет какие используются технологии. На основе этих технологий программа выполняет поиск уязвимостей через API NVD с помощью функции get_cve_for_tech (листинг 3), возвращая список CVE. Параллельно используются функция analyze_headers (листинг 5), выявляя отсутствие заголовков «CSP» и «STS», и функция проверки сертификата check_ssl. На основе всех полученных результатов формируются рекомендации по безопасности. На рисунке 1 представлен успешный результат пассивного сканирования.

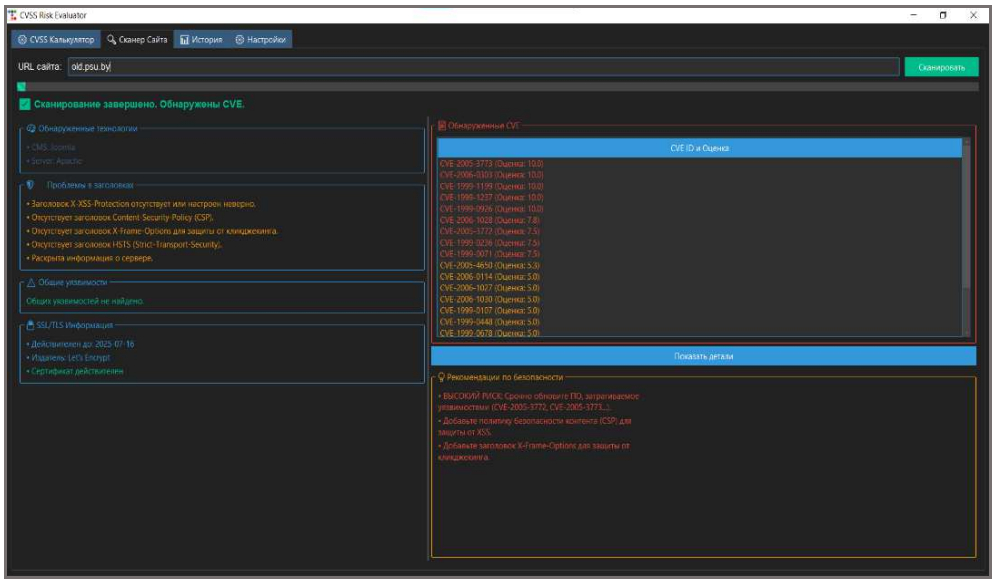

Рисунок 1. – Результат пассивного сканирования

В результате работы программы выявлено, что исходный сайт использует технологии такие, как: CMS: Joomla и Server: Apache. Далее выявлены уязвимости из базы данных NVD API для технологий с оценками CVSS, а также разработаны рекомендации по безопасности, представленные на рисунке 2.

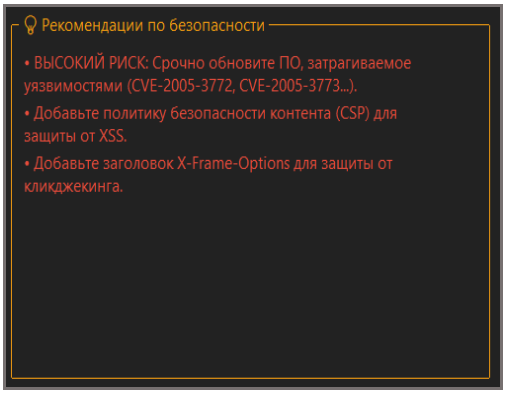

Рисунок 2. – Рекомендации по безопасности

Далее пользователь может перейти на вкладку «CVSS Калькулятор» и выбрать значения метрик для уязвимости. С помощью функции calculate_cvss рассчитывается оценка критичности уязвимости и ее категория. Вкладка «История» позволяет пользователю посмотреть историю оценок сканирований в виде графика и сохранить запись сканирования Для этого пользователю необходимо выбрать нужное ему сканирование и нажать на кнопку «Экспорт в PDF», файл сохранится в типе «txt».

Результат по разработанной программе CVSS Risk Evaluator демонстрирует ее значительный потенциал как эффективного инструмента для пассивного аудита безопасности веб-сайтов. Программа успешно интегрирует ключевые функции, такие как расчет CVSS-оценок, пассивное сканирование, анализ уязвимостей через NVD API, проверка SSL/TLS-сертификатов и исследование HTTP-заголовков, обеспечивая пользователям комплексный анализ рисков без активного воздействия на целевые ресурсы. Интуитивно понятный интерфейс с вкладками «Сканер», «CVSS Калькулятор», «История» и «Настройки» позволяет гибко настраивать процесс (включая ввод ключа NVD, выбор темы и время сканирования) и получать детализированные результаты. Успешная реализация функций, подтвержденная практическим примером на сайте old.psu.by, подчеркивает надежность и практическую ценность программы, делая ее ценным решением для специалистов по информационной безопасности.

Проведем ставнительный анализ представленного ПО с аналогами. Pentest Tools – это специализированный онлайн-сервис, предназначенный для автоматизированного тестирования на проникновение и оценки защищенности веб-ресурсов и сетевой инфраструктуры. Платформа предоставляет широкий набор инструментов, включая сканеры уязвимостей веб-приложений, анализ конфигураций серверов, сбор информации, проверку безопасности CMS и генерацию отчетов. Благодаря удобному веб-интерфейсу и наличию как бесплатных, так и платных функций, Pentest Tools широко применяется специалистами по информационной безопасности для предварительного аудита, выявления уязвимостей и оценки уровня риска, связанного с их эксплуатацией.

В отличие от него, разработанный в рамках настоящей работы программный продукт ориентирован на пассивный сбор информации без активного воздействия на целевой веб-ресурс, что делает его более безопасным для предварительного анализа.

Полученный результат используемых технологий путем сканирования old.psu.by представлены на рисунке 3.

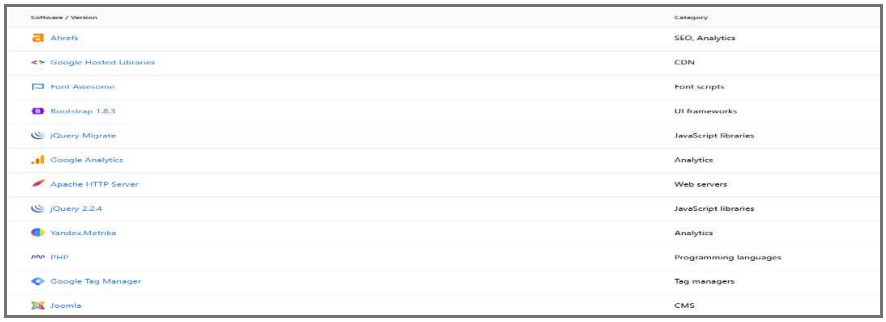

Рисунок 3. – Полученные технологии в результате сканирования

Таблица 1. – Сравнение CVSS Risk Evaluator и Pentest Tools

Критерий	CVSS Risk Evaluator	Pentest Tools
Тип сканирования	Пассивное (анализ без воздействия)	Активное (с возможными тестовыми атаками)
Безопасность для целевого ресурса	Полностью безопасен, не нарушает работу сайта	Может вызвать нагрузку или сбои при интенсивном тестировании
Уровень автоматизации	Полная автоматизация (от сканирования до оценки CVSS)	Частично автоматизирован, требует ручной настройки тестов
Анонимность пользователя	Локальная работа, не требует передачи данных на внешний сервер	Все данные проходят через сервер Pentest Tools
История сканирований	Поддерживается локально, можно экспортировать	Доступна в личном кабинете, ограничена по тарифу
Пользовательская настройка метрик	Поддерживается ручной выбор и коррекция CVSS-параметров	Нет встроенного калькулятора CVSS
Время сканирования	~10 секунд	~1-2 минуты
Установка	Локальное приложение	Веб-сервис, требует учетную запись
Расширяемость	Открытый код, расширяемый	Ограничено возможностями сервиса
Стоимость использования	Бесплатное использование	Ограничено бесплатно, полная функциональность – по подписке

Оба рассмотренных инструмента – CVSS Risk Evaluator и Pentest Tools направлены на решение одной и той же задачи: выявление уязвимостей в веб-приложениях и оценка уровня риска, связанного с их эксплуатацией. Несмотря на общее назначение, подходы к выполнению этой задачи у данных решений существенно различаются.

CVSS Risk Evaluator, разработанный в рамках данной работы, ориентирован на пассивный сбор информации и последующий анализ рисков на основе стандарта CVSS. Программа использует открытые источники данных (веб-сайт и API базы NVD), но все вычисления выполняются локально, что обеспечивает автономность, приватность и гибкость оценки. Пользователь получает возможность вручную управлять метриками и просматривать историю сканирований без ограничений по тарифам.

С другой стороны, Pentest Tools представляет собой облачный сервис с широким набором функций для активного тестирования безопасности. Он позволяет выявлять уязвимости более глубоко, включая эксплуатационные аспекты, но требует подключения к внешним серверам, авторизации и может оказывать влияние на стабильность целевого ресурса при интенсивных тестах.

Таким образом, CVSS Risk Evaluator может эффективно использоваться как первый этап анализа – для безопасной, быстрой и предварительной оценки защищенности, в то время как Pentest Tools может применяться на более позднем этапе для проведения детального и активного тестирования. Совместное применение этих подходов позволяет выстроить комплексную стратегию аудита безопасности веб-ресурсов, начиная с оценки рисков и заканчивая проверкой устойчивости к реальным угрозам.

В результате проведенной работы было разработано программное обеспечение для пассивной оценки защищенности веб-приложений. Инструмент автоматизирует сбор информации о целевом ресурсе, анализирует уязвимости с расчетом уровня риска по метрикам CVSS. В ходе исследования проведено сравнение возможностей разработанного решения с существующими инструментами, что позволило оценить его эффективность и определить направления для дальнейшего развития.

Поставленные задачи выполнены, разработанное программное обеспечение подтвердило свою практическую ценность для предварительного анализа защищенности веб-ресурсов.

Таким образом, несмотря на ряд ограничений, CVSS остается важным инструментом для количественной оценки уязвимостей в информационных системах. Понимание как преимуществ, так и недостатков этой системы позволяет более обоснованно подходить к ее использованию и, при необходимости, комбинировать с другими методами оценки рисков для более точных и комплексных результатов.