

АНАЛИЗ ЗАЩИЩЕННОСТИ ВЕБ-РЕСУРСОВ НА ОСНОВЕ МЕТРИКИ CVSS

Ш.Р. Давлатов

С развитием веб-технологий растет и число потенциальных уязвимостей в онлайн-ресурсах. Широкое использование инструментов для реализации угроз информационной безопасности в Интернете определяет актуальность использования систем для анализа безопасности веб-ресурсов. Специалисты по защите информации часто используют объективные количественные показатели защищенности, которые вычисляются на основе метрик открытой системы оценки CVSS (Common Vulnerability Scoring System). Метрика CVSS предлагает простой инструментарий для расчета числового показателя уязвимости по десятибалльной шкале. Чем выше значение метрики, тем более оперативная реакция требуется для исправления проблемы безопасности системы.

В рамках данной работы была разработана система для автоматического сбора информации о веб-ресурсах из открытых источников shodan.io и censys.io. В результате процесса сканирования удалось собрать данные более 19 тысяч наиболее популярных веб-ресурсов Беларуси. Для каждого отдельного домена была получена техническая информация в формате: IP-адреса, открытые порты, географическое расположение веб-серверов и заголовки ответов HTTP. В работе также представлена новая методика оценки безопасности веб-ресурсов на базе метрики CVSS. Установлено, что порядка 10% веб-ресурсов Беларуси из исходной генеральной выборки, в размере 19 тысяч доменов, имеют критическую усредненную оценку уязвимости. На основе данных об уязвимостях построено эмпирическое распределение оценки CVSS. С помощью критерия хи-квадрат проверена гипотеза о том, что данное распределение подчиняется закону Пуассона. В рамках данного исследования были также разработаны RegExp выражения на языке JavaScript для точного определения версий технологий, которые были использованы для создания веб-сайтов. Установлены процентные соотношения используемых технологий, доменов верхнего уровня и географическое расположение серверов, которые обслуживают данные веб-ресурсы.