

Кедровский М.А. — рецензент Цурин О.Ф.
УНК «ИПСА» НТУУ «КПИ»

Разработка Web-интерфейса к сканеру уязвимостей Web-сайтов

Эффективность работы любого Internet-сайта определяется скоростью реакции на динамично развивающуюся среду веб-технологий. Современные технологии создания веб-контента в режиме реального времени дали профессиональному веб-мастеру мощнейшие инструменты для управления потоками информации в Internet. Вполне естественно, что столь быстро развивающийся рынок не остался без внимания хакеров, стремящихся нанести вред или завладеть конфиденциальной информацией. В таких условиях актуальной задачей является минимизация уязвимостей web-серверов и сайтов во избежание вредоносных атак и утечки информации.

Во время создания или внесения изменений в структуру и скрипты страниц сайта тяжело оценить возможность такой уязвимости и наиболее уязвимую часть целостной структуры системы. Обнаружить «дыры» в скриптах можно с помощью любого сканера уязвимостей. Для более удобного использования была создана система Nikto-online, которая позволяет сократить время, необходимое на сканирование и автоматизировать процесс поиска слабых мест в безопасности веб-серверов и веб-сайтов.

Система являет собой веб-интерфейс к сканеру уязвимостей Nikto 2.03 с приятным дизайном и удобной навигацией, которая анализирует степень уязвимости сайтов к основным видам хакерских атак, таких как переполнение буфера, вирусы, сетевая разведка, sniffing пакетов, IP-спуфинг, Man-in-the-middle, инъекции и прочие.

Благодаря параллельному сканированию, Nikto-online позволяет быстро выполнять массовое сканирование веб-сайтов. В результате, система классифицирует каждую найденную уязвимость согласно степени потенциальной опасности и отображает результат сканирования в удобной для чтения форме. Таким образом, внимание акцентируется на более опасных ошибках, которые рекомендуются к устранению, а уязвимости, которые не несут вреда для сервера и веб-сайта удаляются из списка результата сканирования.

Nikto-online позволяет получить более подробную информацию об обнаруженной уязвимости и методах ее устранения (если возможно, на русском языке). В дальнейшем планируется просканировать все сайты сети университета и разослать отчеты веб-мастерам с целью обезопасить их от внешнего влияния, а также перевести все описания и методы устранения уязвимостей на русский язык.

Система Nikto-online способна вовремя обнаружить уязвимость, что позволит ограничить несанкционированный доступ к серверам и веб-сайтам НТУУ «КПИ», а в дальнейшем и к другим сетевым ресурсам.

Литература

1. Захист Web-сайтів НТУУ КПІ – <http://bug.kpi.ua/index.php>.
2. Система защиты веб-портала. Часть 1 – Интернет
http://art.thelib.ru/internet/game/sistema_zaschiti_vebportala_chast_1.html.
3. Иерархия защиты веб-серверов – <http://www.citforum.ru/security/web/hierarchy>.
4. Защита сайтов и Web-проектов – ProtectMe –
<http://www.protectme.ru/websec/protection/>.
5. “Inaccessibility of Visually-Oriented Anti-Robot Tests”
<http://www.w3.org/TR/2003/WD-turingtest-20031105/>.