

# **Индивидуальный проект. Этап №4**

**Основы информационной безопасности**

Астраханцева А. А.

# Содержание

1	Цель работы	4
2	Теоретическое введение	5
3	Выполнение	7
4	Выводы	9
5	Список литературы. Библиография	10

## Список иллюстраций

3.1	Провесрка версии и просмотр справки . . . . .	7
3.2	Проверка работы сканера на сайте rudn.ru . . . . .	8

# **1 Цель работы**

Знакомство со сканером безопасности Nikto и применение.

## 2 Теоретическое введение

Nikto – бесплатный (open source) сканер для поиска уязвимостей в веб-серверах. Утилита относится к классу blackbox сканеров, т. е. сканеров, использующих стратегию сканирования методом черного ящика. Это значит, что заранее неизвестно о внутреннем устройстве программы/сайта (доступ к исходному коду отсутствует) и упор сделан на функциональность. Программа может обнаруживать более 6700 потенциально опасных файлов и уязвимостей. Новые уязвимости добавляются в базу данных программы по мере их возникновения. Помимо поиска уязвимостей, сканер производит поиск на наличие устаревших версий, используемых библиотек и фреймворков. Nikto не позиционируется как стелс сканер (стелс сканеры никогда не устанавливают TCP-соединения до конца, тем самым сканирование происходит скрытно) – при сканировании сайта в логах сайта или в любой другой системе обнаружения вторжений, если она используется, будет отображена информация о том, что сайт подвергается сканированию.

Среди функций Nikto можно выделить следующие:

поддержка SSL,

поддержка HTTP прокси;

создание отчетов в текстовом формате, XML, HTML, NBE или CSV;

возможность сканирования портов;

поиск поддоменов;

поддержка плагинов для расширения функционала сканирования [1].

## 3 Выполнение

Проверяем, установлен ли Nikto, запрашивая его версию: `nikto -Version`. После этого для ознакомления читаем справку по команде `nikto`: `nikto -Help` (рис. 3.1).

```
(aaastrakhanceva@aaastrakhanceva)-[~]labr.com
$ nikto -Version
Nikto 2.5.0 (LW 2.5)

(aaastrakhanceva@aaastrakhanceva)-[~]
$ nikto -Help

Options:
  -ask+          Whether to ask about submitting updates
                  yes    Ask about each (default)
                  no     Don't ask, don't send
                  auto   Don't ask, just send
  -check6+       Check if IPv6 is working (connects to ipv6.google.
com or value set in nikto.conf)
  -cgidirs+      Scan these CGI dirs: "none", "all", or values like
"/cgi/" /cgi-a/"
  -config+       Use this config file
  -Display+      Turn on/off display outputs:
                  1      Show redirects
                  2      Show cookies received
                  3      Show all 200/OK responses
                  4      Show URLs which require authentication
                  D      Debug output
                  E      Display all HTTP errors
                  P      Print progress to STDOUT
                  S      Scrub output of IPs and hostnames
                  V      Verbose output
  -dbcheck       Check database and other key files for syntax error
  -evasion+      Encoding technique:
                  1      Random URI encoding (non-UTF8)
                  2      Directory self-reference (/./)
                  3      Premature URL ending
                  4      Prepend long random string
                  5      Fake parameter
                  6      TAB as request spacer
                  7      Change the case of the URL
                  8      Use Windows directory separator (\)
                  A      Use a carriage return (0x0d) as a request
spacer
                  B      Use binary value 0x0b as a request spacer
  -followredirects Follow 3xx redirects to new location
  -Format+       Save file (-o) format:
                  csv    Comma-separated-value
                  json   JSON Format
                  htm    HTML Format
                  nbe    Nessus NBE format
                  sql     Generic SQL (see docs for schema)
```

Рис. 3.1: Проверка версии и просмотр справки

Попробуем запустить сканер на сайте `rudn.ru` (рис. 3.2).





## 4 Выводы

Познакомилась со сканером безопасности Nikto и применила его для сканирования сайта.

## 5 Список литературы. Библиография

[1] Обзор сканера Nikto для поиска уязвимостей в веб-серверах: <https://habr.com/ru/companies/otus>

[2] Проверяем на уязвимости любой сайт с помощью Nikto: <https://habr.com/ru/companies/otus>