

# Персональный проект. Этап №4

## Основы информационной безопасности

---

Астраханцева А. А.

27 апреля 2024

Российский университет дружбы народов, Москва, Россия

- Астраханцева Анастасия Александровна
- студентка НКАбд-01-22
- Студ. билет: 1132226437
- Российский университет дружбы народов
- <https://anastasiia7205.github.io/>



Знакомство со сканером безопасности Nikto и применение.

## Выполнение работы

---

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.

# Провесрка версии и просмотр справки

```
(aaastrakhanceva@aaastrakhanceva)-[~]
$ 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 space

  -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)
```

## Проверка работы сканера на сайте rudn.ru

```
(aaastrakhanceva@aaastrakhanceva)-[~]
$ nikto -h rudn.ru
- Nikto v2.5.0

+ Target IP:      185.178.208.57
+ Target Hostname: rudn.ru
+ Target Port:    80
+ Start Time:     2024-04-27 20:39:32 (GMT3)

+ Server: ddos-guard
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/HTTP/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the page as a download, without intent to do so, resulting in an expected display of the wrong content-type-header/
+ Root page / redirects to: https://rudn.ru/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ : Server banner changed from 'ddos-guard' to 'ngjit'.
q
+ ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: can't connect (timeout): Operation now in progress
+ Scan terminated: 20 error(s) and 3 item(s) reported on remote host
+ End Time:       2024-04-27 20:46:36 (GMT3) (424 seconds)

+ 1 host(s) tested
XX packets: 42192 bytes 4166/251 (49.2 Mib)
XX errors: 0 dropped: 0 overruns: 0 frame: 0
XX bytes: 1398617 (13.3 Mib)
XX errors: 0 dropped: 0 overruns: 0 carrier: 0 collisions: 0
XX total: 5 packets, 1398617 bytes, 43.3 Mib
```

Рис. 2: Проверка работы сканера на сайте rudn.ru

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



Спасибо за внимание

---