# Персональный проект. Этап №4

Основы информационной безопастности

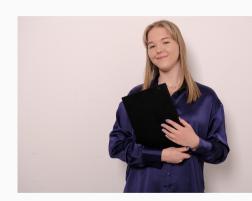
Астраханцева А. А.

27 апреля 2024

Российский университет дружбы народов, Москва, Россия

#### Докладчик

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





Знакомство со сканером безопастности Nikto и применение.

Выполнение работы

### Теоретическое введенние

Nikto – бесплатный (open source) сканер для поиска уязвимостей в веб-серверах. Утилита относиться 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 ТСР-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

```
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)
                          Scan these CGI dirs: "none", "all", or values like
                          Use this config file
                          Turn on/off display outputs:
       -Display+
                                    Show redirects
                                    Show cookies received
                                    Show all 200/OK responses
                                    Show URLs which require authentication
                                    Debug output
                                    Display all HTTP errors
                                    Print progress to STDOUT
                                    Scrub output of IPs and hostnames
                                    Verbose output
       -dhcheck
                         Check database and other key files for syntax error
                         Encoding technique:
                                    Random URI encoding (non-UTF8)
                                    Directory self-reference (/./)
                                    Premature URL ending
                                    Prepend long random string
                                    Fake parameter
                                    TAR as request spacer
                                    Change the case of the URL
                                    Use Windows directory separator (\)
                                    Use a carriage return (0×0d) as a reques
                                    Use binary value 0×0b as a request space
       -followredirects Follow 3xx redirects to new location
       -Format+
                          Save file (-o) format:
                              csv Comma-separated-value
                              ison JSON Format
                                    HTML Format
                                   Nessus NBE format
                                    Generic SQL (see docs for schema)
```

## Проверка работы сканера на сайте rudn.ru

```
s 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-clicklacking X-Frame-Options header is not present. See: https://developer.mozil
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render t
ing-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 'ngiit'.
+ ERROR: Error limit (20) reached for host, giving up, Last error; opening st
ream: can't connect (timeout): Operation now in progress
+ Scan terminated: 20 error(s) and 3 item(s) reported on remote host
                      2024-04-27 20:46:36 (GMT3) (424 seconds)
+ End Time:
+ 1 host(s) tested
```

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



Познакомилась со сканером безопастности Nikto и примениа его для сканирования сайта.

Спасибо за внимание