

# Индивидуальный проект. Этап 4

Дьяконова С.Ф., НКАбд-01-22

# Цель работы

Знакомство со сканером безопасности nikto и его применение

**Выполнение**

```
-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

-dbccheck     Check database and other key files for syntax errors
-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)
              txt    Plain text
              xml    XML Format
              (if not specified the format will be taken from the file extension passed to -output)

-Help         This help information
-host+        Target host/URL
-id+          Host authentication to use, format is id:pass or id:pass:realm
-ipv4         IPv4 Only
-ipv6         IPv6 Only
-key+         Client certificate key file
-list-plugins List all available plugins, perform no testing
-maxtime+     Maximum testing time per host (e.g., 1h, 60m, 3600s)
-mutate+      Guess additional file names:
              1      Test all files with all root directories
              2      Guess for password file names
              3      Enumerate user names via Apache (/~user type requests)
```

# Проверка веб-сайта

```
(sadjyakonova@sadyakonova)~  
$ sudo apt-get install nikto  
[sudo] password for sadjyakonova:  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
nikto is already the newest version (1:2.5.0+git20230114.90ff645-0kali1).  
nikto set to manually installed.  
0 upgraded, 0 newly installed, 0 to remove and 267 not upgraded.  
  
(sadjyakonova@sadyakonova)~  
$ nikto -h mos.ru  
- Nikto v2.5.0  
  
+ Target IP: 212.11.151.57  
+ Target Hostname: mos.ru  
+ Target Port: 80  
+ Start Time: 2024-04-27 15:23:18 (GMT3)  
  
+ Server: nginx  
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://develop  
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to  
+ Root page / redirects to: https://mos.ru/  
+ No CGI Directories found (use '-C all' to force check all possible dirs)
```

## Выводы

Я ознакомилась со сканером безопасности nikto и научилась его применять.

**Спасибо за внимание!**