

# **Индивидуальный проект**

**Этап 4**

Крутова Екатерина Дмитриевна

# Содержание

|                                       |          |
|---------------------------------------|----------|
| <b>Цель работы</b>                    | <b>5</b> |
| <b>Выполнение лабораторной работы</b> | <b>6</b> |
| <b>Выводы</b>                         | <b>8</b> |

## Список иллюстраций

|   |  |   |
|---|--|---|
| 1 | Оptionальные параметры nikto . . . . . | 6 |
| 2 | Сканирование сайта РУДН . . . . .      | 7 |

## **Список таблиц**

## **Цель работы**

Целью данной работы является знакомство с веб-сканером nikto.

# Выполнение лабораторной работы

Выполнение работы (рис. [-@fig:001] - [-@fig:002]).

nikto — базовый сканер безопасности веб-сервера. Он сканирует и обнаруживает уязвимости в веб-приложениях, обычно вызванные неправильной конфигурацией на самом сервере, файлами, установленными по умолчанию, и небезопасными файлами, а также устаревшими серверными приложениями. На Kali Linux nikto предустановлен.

```
(kali@kali)~$ 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)
-Cgldirs+      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 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)
```

Рис. 1: Опциональные параметры nikto

```

(kali@kali)-[~]
$ nikto -h https://www.rudn.ru/
- Nikto v2.5.0

+ Target IP: 195.178.208.57
+ Target Hostname: www.rudn.ru
+ Target Port: 443

+ SSL Info: Subject: /CN=*.rudn.ru
Ciphers: TLS_AES_128_GCM_SHA256
Issuer: /C=BE/O=GlobalSign nv-sa/CN=GlobalSign GCC R3 DV TLS CA 2020
+ Start Time: 2024-10-05 15:46:34 (GMT+4)

+ Server: ddos-guard
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The site uses TLS and the Strict-Transport-Security HTTP header is not defined. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /: Cookie __ddg8_ created without the secure flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Cookie __ddg8_ created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Cookie __ddg9_ created without the secure flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Cookie __ddg9_ created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: IP address found in the '__ddg9_' cookie. The IP is "46.242.14.227".
+ /: Cookie __ddg10_ created without the secure flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Cookie __ddg10_ created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Cookie __ddg1_ created without the secure flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Cookie XSRF-TOKEN created without the secure flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Cookie XSRF-TOKEN created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Cookie rudnru_session created without the secure flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /Ns06QCTI.gif: Uncommon header 'ddg-cache-status' found, with contents: MISS.

```

Рис. 2: Сканирование сайта РУДН

## **Выводы**

Я воспользовалась веб-сканером nikto для поиска уязвимостей.