

# Индивидуальный проект №4

## Основы информационной безопасности

---

Боровиков Даниил Александрович

Российский университет дружбы народов им. Патриса Лумумбы, Москва, Россия

Знакомство с базовым сканером безопасности nikto, его применение.

# Вывожу справку об утилите nikto командой *nikto -h*

```
kali@kali: ~  
File Actions Edit View Help  
+ ERROR: Update failed, please notify sullo@cirt.net of the previous line.  
  
(kali@kali)-[~]  
└─$ nikto -h http://127.0.0.1/DVWA/  
- Nikto v2.5.0  
  
+ Target IP: 127.0.0.1  
+ Target Hostname: 127.0.0.1  
+ Target Port: 80  
+ Start Time: 2024-04-20 13:02:51 (GMT-4)  
  
+ Server: Apache/2.4.58 (Debian)  
+ /DVWA/: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options  
+ /DVWA/: 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/  
+ Root page /DVWA redirects to: login.php  
+ No CGI Directories found (use '-C all' to force check all possible dirs)  
+ OPTIONS: Allowed HTTP Methods: GET, POST, OPTIONS, HEAD .  
+ /DVWA//etc/hosts: The server install allows reading of any system file by adding an extra '/' to the URL.  
+ /DVWA/config/: Directory indexing found.  
+ /DVWA/config/: Configuration information may be available remotely.  
+ /DVWA/tests/: Directory indexing found.  
+ /DVWA/tests/: This might be interesting.  
+ /DVWA/database/: Directory indexing found.  
+ /DVWA/database/: Database directory found.  
+ /DVWA/docs/: Directory indexing found.  
+ /DVWA/login.php: Admin login page/section found.  
+ /DVWA/.git/index: Git Index file may contain directory listing information.  
+ /DVWA/.git/HEAD: Git HEAD file found. Full repo details may be present.  
+ /DVWA/.git/config: Git config file found. Infos about repo details may be present.  
+ /DVWA/.gitignore: .gitignore file found. It is possible to grasp the directory structure.  
+ /DVWA/wp-content/themes/twentyeleven/images/headers/server.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.  
+ /DVWA/wordpress/wp-content/themes/twentyeleven/images/headers/server.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.  
+ /DVWA/wp-includes/Requests/Utility/content-post.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.  
+ /DVWA/wordpress/wp-includes/Requests/Utility/content-post.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.  
+ /DVWA/wp-includes/js/tinymce/themes/modern/Meuhy.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.  
+ /DVWA/wordpress/wp-includes/js/tinymce/themes/modern/Meuhy.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.  
+ /DVWA/assets/mobirise/css/meta.php?filesrc=: A PHP backdoor file manager was found.  
+ /DVWA/login.cgi?cli=aaX20aaX27catX20/etc/hosts: Some D-Link router remote command execution.  
+ /DVWA/shelllicat/etc/hosts: A backdoor was identified.  
+ /DVWA/.dockerignore: .dockerignore file found. It may be possible to grasp the directory structure and learn more about the site.  
+ 8074 requests: 0 error(s) and 26 item(s) reported on remote host  
+ End Time: 2024-04-20 13:03:04 (GMT-4) (13 seconds)
```

Сканирую веб-сайт mos.ru на наличие уязвимостей с помощью команды *nikto -h mos.ru*. Утилита показала отсутствие некоторых важных для безопасности заголовков

```
kali@kali: ~  
File Actions Edit View Help  
└─$ nikto -h  
Option host requires an argument  
  
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  
s  
-evasion+       Encoding technique:  
                  1     Random URI encoding (non-UTF8)  
                  2     Directory self-reference (./.)  
                  3     Premature URL ending  
                  4     Prepend long random string  
                  5     Fake parameters
```

# Сканирую локальный хост на наличие уязвимостей с помощью команды *nikto -h 127.0.0.1*

```
(kali㉿kali)-[~]  
$ nikto -h mos.ru  
- Nikto v2.5.0  
  
+ Target IP: 212.11.151.57  
+ Target Hostname: mos.ru  
+ Target Port: 80  
+ Start Time: 2024-04-20 12:52:06 (GMT-4)  
  
+ Server: nginx  
+ /: 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 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/  
+ Root page / redirects to: https://mos.ru/  
+ No CGI Directories found (use '-C all' to force check all possible dirs)  
+ ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: can't connect (timeout): Operation now in progress  
+ Scan terminated: 19 error(s) and 2 item(s) reported on remote host  
+ End Time: 2024-04-20 12:58:04 (GMT-4) (358 seconds)  
  
+ 1 host(s) tested
```

**Figure 3:** Сканирование локалхоста

Сканирую приложение DVWA с помощью команды *nikto -h http://127.0.0.1/DVWA*. *nikto* также указывает на отсутствие важных заголовков и выводит информацию о различных доступных эндпоинтах

```
kali@kali: ~  
File Actions Edit View Help  
+ 1 host(s) tested  
  
(kali@kali)~  
$ nikto -h 127.0.0.1  
- Nikto v2.5.0  
  
+ Target IP: 127.0.0.1  
+ Target Hostname: 127.0.0.1  
+ Target Port: 80  
+ Start Time: 2024-04-20 12:59:15 (GMT-4)  
  
+ Server: Apache/2.4.58 (Debian)  
+ /: 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 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/  
+ No CGI Directories found (use '-C all' to force check all possible dirs)  
+ /: Server may leak inodes via ETags, header found with file /, inode: 29cd, size: 61236d1d67a20, mtime: gzip. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418  
+ OPTIONS: Allowed HTTP Methods: GET, POST, OPTIONS, HEAD .  
+ /etc/passwd: The server install allows reading of any system file by adding an extra '/' to the URL.  
+ /server-status: This reveals Apache information. Comment out appropriate line in the Apache conf file or restrict access to allowed sources. See: OSVDB-561  
+ /wp-content/themes/twentyeleven/images/headers/server.php?filesrc=/etc/passwd: A PHP backdoor file manager was found.  
+ /wordpress/wp-content/themes/twentyeleven/images/headers/server.php?filesrc=/etc/passwd: A PHP backdoor file manager was found.  
+ /wp-includes/Requests/Utility/content-post.php?filesrc=/etc/passwd: A PHP backdoor file manager was found.  
+ /wordpress/wp-includes/Requests/Utility/content-post.php?filesrc=/etc/passwd: A PHP backdoor file manager was found.  
+ /wp-includes/js/tinymce/themes/modern/Meuhy.php?filesrc=/etc/passwd: A PHP backdoor file manager was found.  
+ /wordpress/wp-includes/js/tinymce/themes/modern/Meuhy.php?filesrc=/etc/passwd: A PHP backdoor file manager was found.
```

Я познакомился с nikto, научился его применять на практике для проверки уязвимостей различных сайтов