Индивидуальный проект №4

Основы информационной безопасности

Дудырев Г. А.

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

Докладчик

- Дудырев Глеб Андреевич
- НПИбд-01-22
- Российский университет дружбы народов
- [1132222003@pfur.ru]

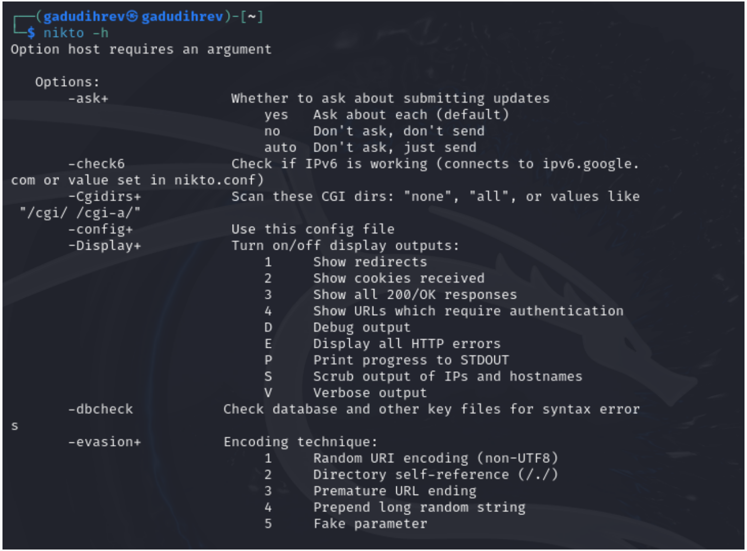
Вводная часть

Цели и задачи

Знакомство с базовым сканером безопасности nikto, его применение.

Выполнение лабораторной работы

Вывожу справку об утилите nikto командой *nikto -h*

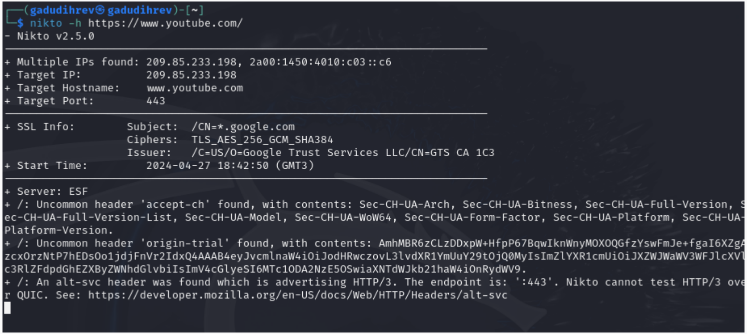


```
┌──(gadudihrev㉿gadudihrev)-[~]
└─$ nikto -h
Option host requires an argument

   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 parameter
```

Figure 1: nikto -h

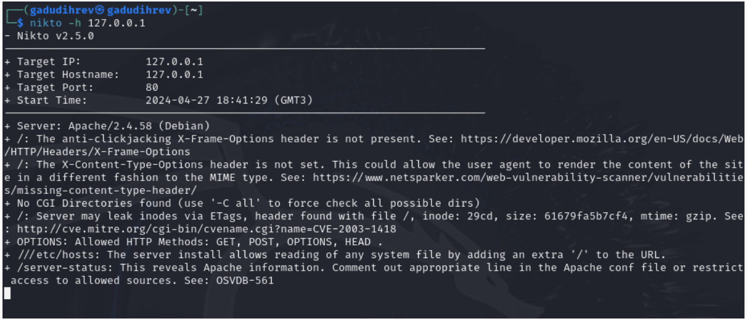
Сканирую веб-сайт gosuslugi.ru на наличие уязвимостей с помощью команды *nikto -h gosuslugi.ru*. Утилита показала отсутствие некоторых важных для безопасности заголовков



```
┌──(gadudihrev㉿gadudihrev)-[~]
└─$ nikto -h https://www.youtube.com/
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Multiple IPs found: 209.85.233.198, 2a00:1450:4010:c03::c6
+ Target IP:          209.85.233.198
+ Target Hostname:    www.youtube.com
+ Target Port:        443
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /CN=*.google.com
                   Ciphers:  TLS_AES_256_GCM_SHA384
                   Issuer:   /C=US/O=Google Trust Services LLC/CN=GTS CA 1C3
+ Start Time:         2024-04-27 18:42:50 (GMT3)
---------------------------------------------------------------------------
+ Server: ESF
+ /: Uncommon header 'accept-ch' found, with contents: Sec-CH-UA-Arch, Sec-CH-UA-Bitness, Sec-CH-UA-Full-Version, S
ec-CH-UA-Full-Version-List, Sec-CH-UA-Model, Sec-CH-UA-WoW64, Sec-CH-UA-Form-Factor, Sec-CH-UA-Platform, Sec-CH-UA-
Platform-Version.
+ /: Uncommon header 'origin-trial' found, with contents: AmhMBR6zCLzDDxpW+HfpP67BqwIknWnyMOXOQGfzYswFmJe+fgaI6XZgA
zcxOrzNtP7hEDsOo1jdjFnVr2IdxQ4AAAB4eyJvcmlnaW4iOiJodHRwczovL3lvdXR1YmUuY29tOjQ0MyIsImZlYXR1cmUiOiJXZWJWaWV3WFJlcXVl
c3RlZFdpdGhEZXByZWNhdGlvbiIsImV4cGlyeSI6MTc1ODA2NzE5OSwiaXNTdWJkb21haW4iOnRydWV9.
+ /: An alt-svc header was found which is advertising HTTP/3. The endpoint is: ':443'. Nikto cannot test HTTP/3 ove
r QUIC. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/alt-svc
█
```

Figure 2: Сканирование сайта gosuslugi.ru

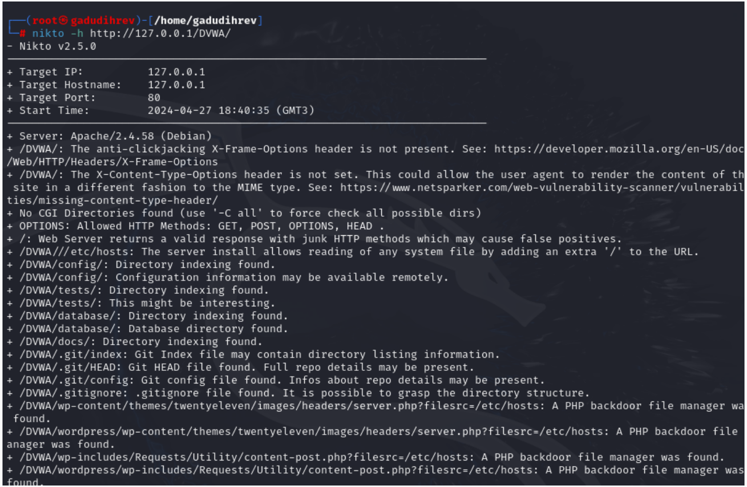
Сканирую локальный хост на наличие уязвимостей с помощью команды *nikto -h 127.0.0.1*



```
┌──(gadudihrev㉿gadudihrev)-[~]
└─$ 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:         2024-04-27 18:41:29 (GMT3)
---------------------------------------------------------------------------
+ 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 sit
e in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilitie
s/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: 61679fa5b7cf4, mtime: gzip. See
: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ OPTIONS: Allowed HTTP Methods: GET, POST, OPTIONS, HEAD .
+ ///etc/hosts: 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
█
```

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



```
┌──(root㉿gadudihrev)-[/home/gadudihrev]
└─# 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:         2024-04-27 18:40:35 (GMT3)
---------------------------------------------------------------------------
+ Server: Apache/2.4.58 (Debian)
+ /DVWA/: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/doc
/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 th
 site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabil
ties/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ OPTIONS: Allowed HTTP Methods: GET, POST, OPTIONS, HEAD .
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ /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/.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 wa
 found.
+ /DVWA/wordpress/wp-content/themes/twentyeleven/images/headers/server.php?filesrc=/etc/hosts: A PHP backdoor file
anager 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.
```

Вывод

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