

Отчёт по индивидуальному проекту №4

Дисциплина: Основы информационной безопасности

Дудырев Глеб Андреевич НПИбд-01-22

Содержание

1	Цель работы	5
2	Выполнение лабораторной работы	6
3	Выводы	9

Список иллюстраций

2.1	nikto -h	6
2.2	Сканирование сайта gosuslugi.ru	7
2.3	Сканирование локалхоста	7
2.4	Сканирование DVWA	8

Список таблиц

1 Цель работы

Знакомство с базовым сканером безопасности nikto, его применение.

2 Выполнение лабораторной работы

1. Вывожу справку об утилите nikto командой *nikto -h* (рис. 2.1)

```
(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
  -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
```

Рис. 2.1: nikto -h

2. Сканирую веб-сайт youtube.ru на наличие уязвимостей с помощью команды *nikto -h youtube.ru*. Утилита показала отсутствие некоторых важных для безопасности заголовков (рис. 2.2)


```

(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 wa
found.

```

Рис. 2.4: Сканирование DVWA

3 Выводы

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