Индивидуальный проект. Этап 4

Дисцилпина: Основы информационной безопасности

Жибицкая Евгения Дмитриевна

Содержание

Список иллюстраций

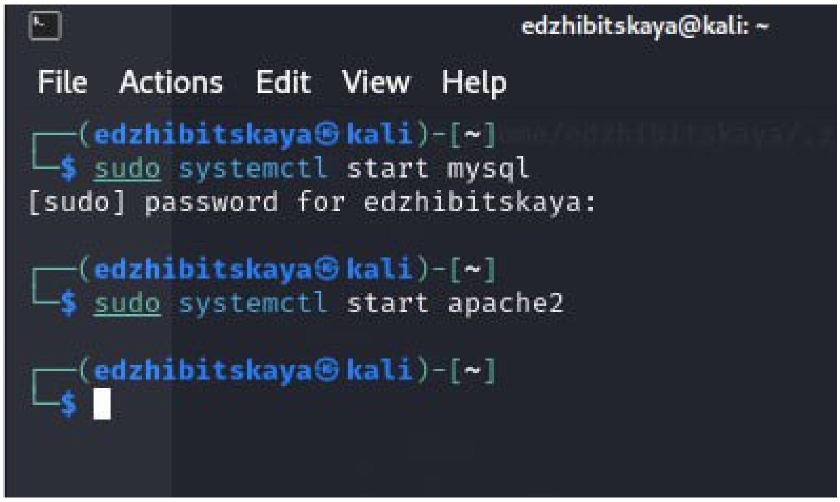
Список таблиц

1 Цель работы

Продолжение выполнения проекта. Освоение приложения nikto

2 Выполнение лабораторной работы

Запускаем сервер и работу DVWA - включаем mysql и apache2(рис. 2.1).



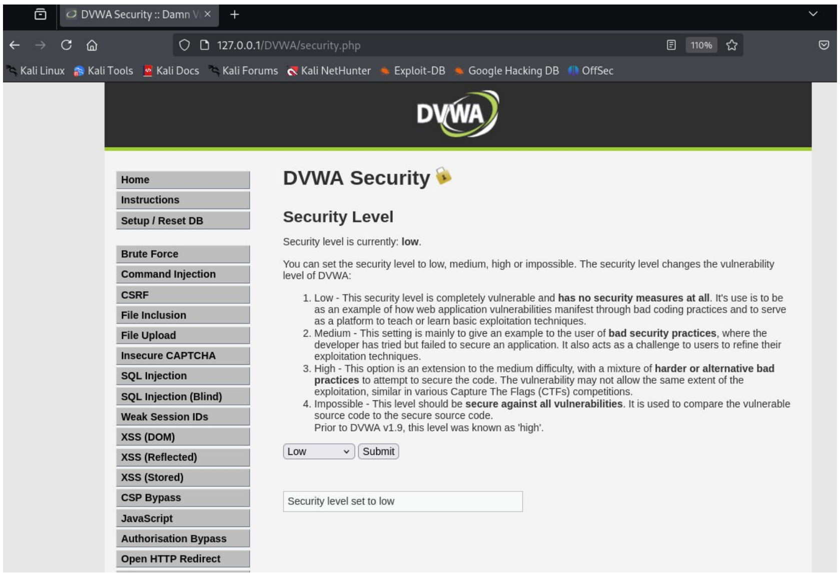
```
┌──(edzhibitskaya㉿kali)-[~]
└─$ sudo systemctl start mysql
[sudo] password for edzhibitskaya:

┌──(edzhibitskaya㉿kali)-[~]
└─$ sudo systemctl start apache2

┌──(edzhibitskaya㉿kali)-[~]
└─$ 
```

Рис. 2.1: Запуск DVWA

Входим в систему, переходим в раздел Security и для удобства устанавливаем уроень low. Это не обязательно, но все равно сделаем(рис. 2.2).



DVWA Security

Security Level

Security level is currently: **low**.

You can set the security level to low, medium, high or impossible. The security level changes the vulnerability level of DVWA:

1. Low - This security level is completely vulnerable and **has no security measures at all**. It's use is to be as an example of how web application vulnerabilities manifest through bad coding practices and to serve as a platform to teach or learn basic exploitation techniques.
2. Medium - This setting is mainly to give an example to the user of **bad security practices**, where the developer has tried but failed to secure an application. It also acts as a challenge to users to refine their exploitation techniques.
3. High - This option is an extension to the medium difficulty, with a mixture of **harder or alternative bad practices** to attempt to secure the code. The vulnerability may not allow the same extent of the exploitation, similar in various Capture The Flags (CTFs) competitions.
4. Impossible - This level should be **secure against all vulnerabilities**. It is used to compare the vulnerable source code to the secure source code.
   Prior to DVWA v1.9, this level was known as 'high'.

Low Submit

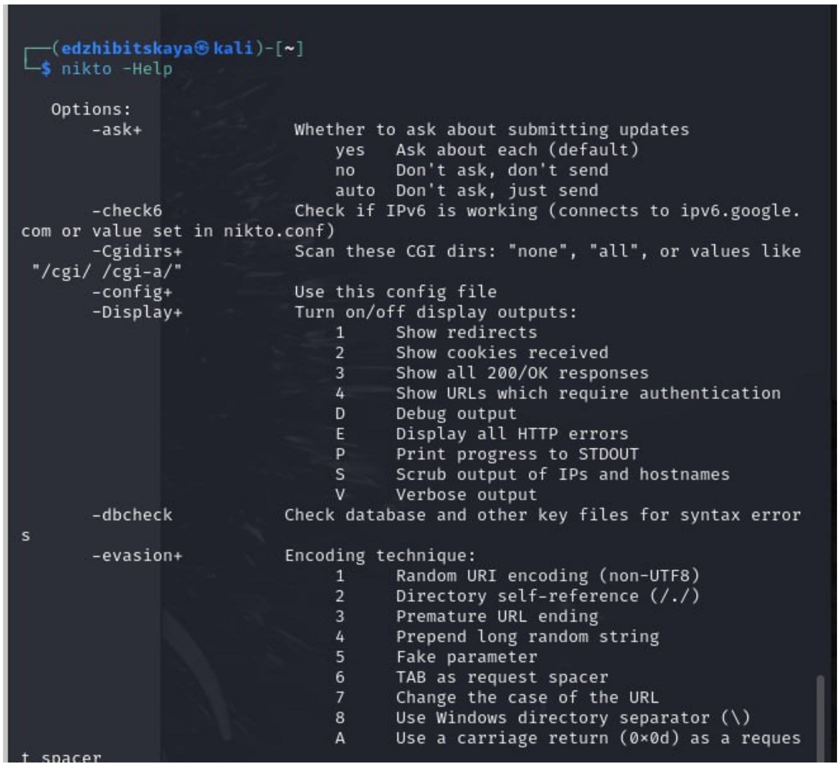
Security level set to low

Рис. 2.2: DVWA Security

Затем запустим nikto. Получим и изучим справку.

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.

(рис. 2.3).

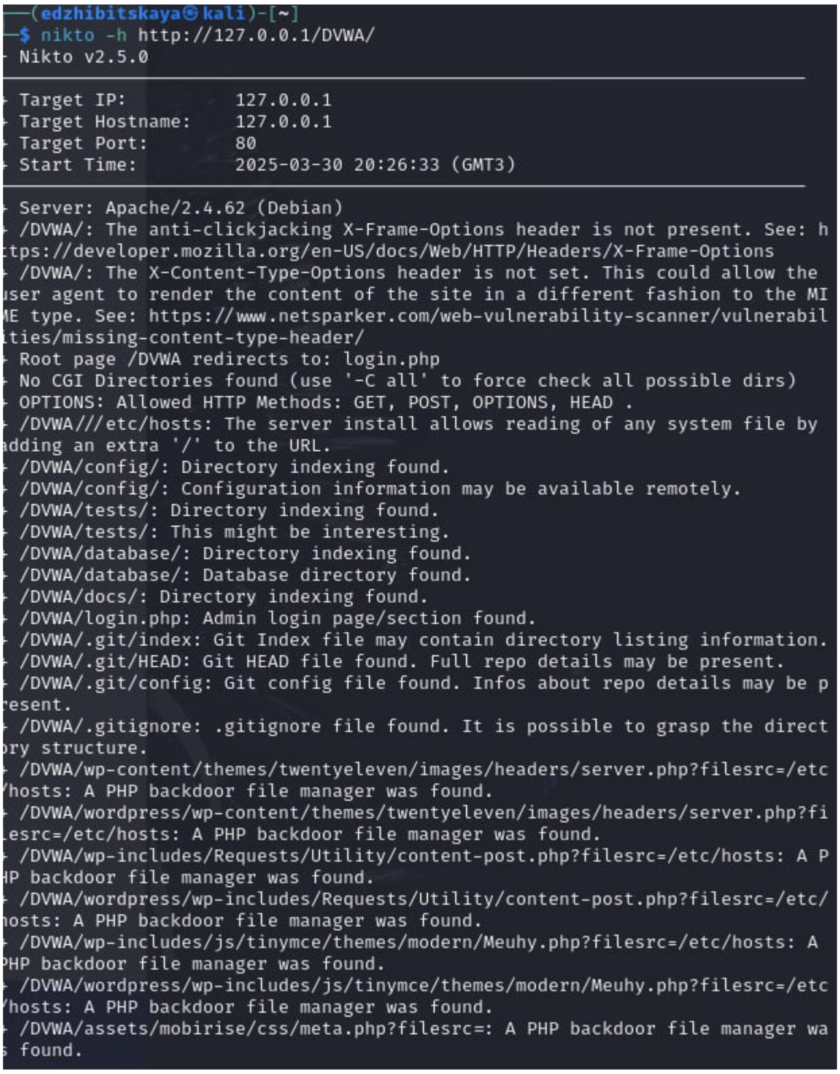


```
┌──(edzhibitskaya㉿kali)-[~]
└─$ nikto -Help

   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)
       -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
                               6     TAB as request spacer
                               7     Change the case of the URL
                               8     Use Windows directory separator (\)
                               A     Use a carriage return (0×0d) as a reques
t spacer
```

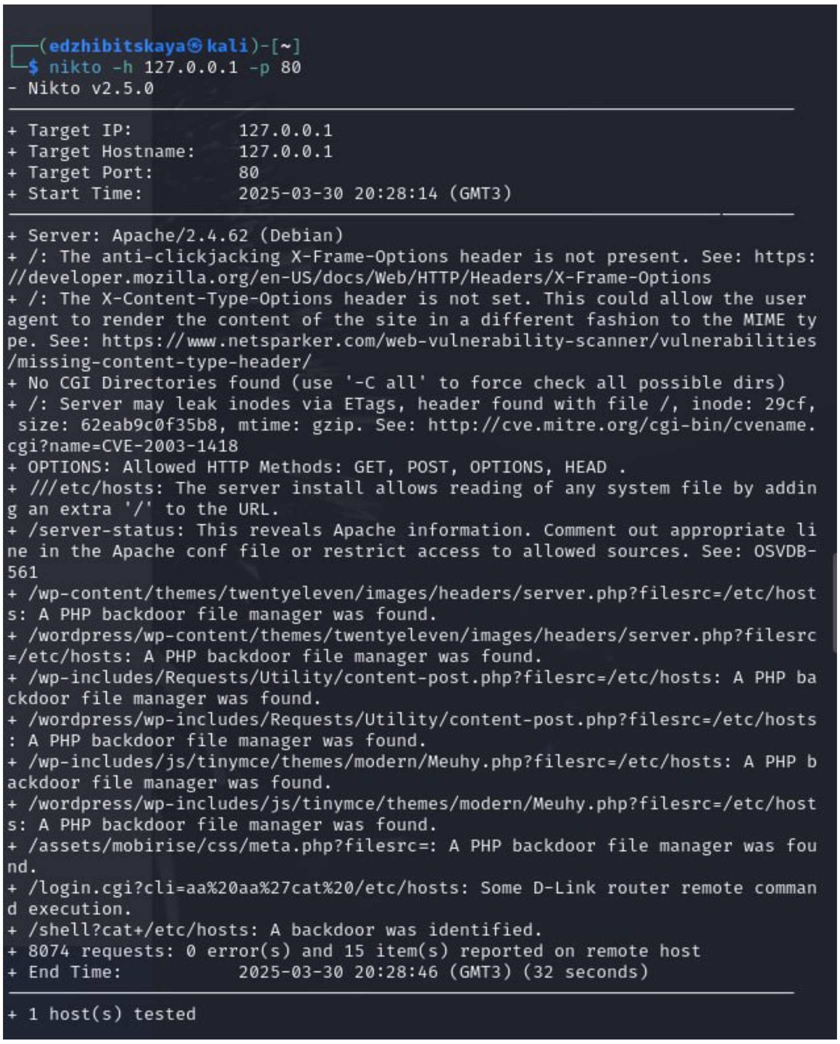
Рис. 2.3: Справка о nikto

Далее перейдем к получению информации и ее анализу. Получим ее двумя разными способами(через адрес и через имя хоста и номер порта)(рис. 2.4) и рис. 2.5).



```
──(edzhibitskaya㉿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:         2025-03-30 20:26:33 (GMT3)
---------------------------------------------------------------------------
- Server: Apache/2.4.62 (Debian)
- /DVWA/: The anti-clickjacking X-Frame-Options header is not present. See: h
ttps://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
ser agent to render the content of the site in a different fashion to the MI
E type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabil
ities/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
dding 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 p
resent.
- /DVWA/.gitignore: .gitignore file found. It is possible to grasp the direct
ry 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?fi
lesrc=/etc/hosts: A PHP backdoor file manager was found.
- /DVWA/wp-includes/Requests/Utility/content-post.php?filesrc=/etc/hosts: A P
HP 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 wa
s found.
```

Рис. 2.4: Анализ через адрес



```
┌──(edzhibitskaya㉿kali)-[~]
└─$ nikto -h 127.0.0.1 -p 80
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          127.0.0.1
+ Target Hostname:    127.0.0.1
+ Target Port:        80
+ Start Time:         2025-03-30 20:28:14 (GMT3)
---------------------------------------------------------------------------
+ Server: Apache/2.4.62 (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 ty
pe. 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: 29cf,
 size: 62eab9c0f35b8, 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 addin
g an extra '/' to the URL.
+ /server-status: This reveals Apache information. Comment out appropriate li
ne in the Apache conf file or restrict access to allowed sources. See: OSVDB-
561
+ /wp-content/themes/twentyeleven/images/headers/server.php?filesrc=/etc/host
s: A PHP backdoor file manager was found.
+ /wordpress/wp-content/themes/twentyeleven/images/headers/server.php?filesrc
=/etc/hosts: A PHP backdoor file manager was found.
+ /wp-includes/Requests/Utility/content-post.php?filesrc=/etc/hosts: A PHP ba
ckdoor file manager was found.
+ /wordpress/wp-includes/Requests/Utility/content-post.php?filesrc=/etc/hosts
: A PHP backdoor file manager was found.
+ /wp-includes/js/tinymce/themes/modern/Meuhy.php?filesrc=/etc/hosts: A PHP b
ackdoor file manager was found.
+ /wordpress/wp-includes/js/tinymce/themes/modern/Meuhy.php?filesrc=/etc/host
s: A PHP backdoor file manager was found.
+ /assets/mobirise/css/meta.php?filesrc=: A PHP backdoor file manager was fou
nd.
+ /login.cgi?cli=aa%20aa%27cat%20/etc/hosts: Some D-Link router remote comman
d execution.
+ /shell?cat+/etc/hosts: A backdoor was identified.
+ 8074 requests: 0 error(s) and 15 item(s) reported on remote host
+ End Time:           2025-03-30 20:28:46 (GMT3) (32 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Рис. 2.5: Анализ по имени хоста и порту

3 Выводы

В ходе работы мы познакомились с приложением nikto. Также был произведен анализ DVWA, получена информация о нем.

Список литературы

- Парасрам, Ш. Kali Linux: Тестирование на проникновение и безопасность : Для профессионалов. Kali Linux / Ш. Парасрам, А. Замм, Т. Херианто, и др. – Санкт-Петербург : Питер, 2022. – 448 сс.