

Проект

Этап 4

Легиньких Г.А.

Российский университет дружбы народов, Москва, Россия

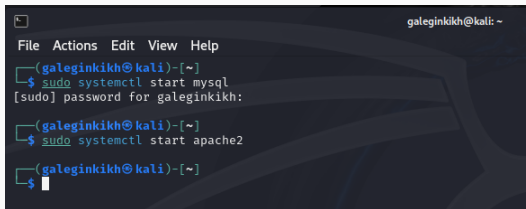
Информация

- Легиньких Галина Андреевна
- НФИбд-02-21
- Российский университет дружбы народов
- 1032216447@pfur.ru
- <https://github.com/galeginkikh>

Выполнение

Использование nikto.

1. Подготовила веб-приложение.



```
galeginkikh@kali: ~  
File Actions Edit View Help  
(galeginkikh@kali)~  
$ sudo systemctl start mysql  
[sudo] password for galeginkikh:  
(galeginkikh@kali)~  
$ sudo systemctl start apache2  
(galeginkikh@kali)~  
$
```

Рис. 1: Подготовка

2. Ввела в адресной строке адрес DVWA, перешла в режим выбора уровня безопасности, и поставила минимальный.

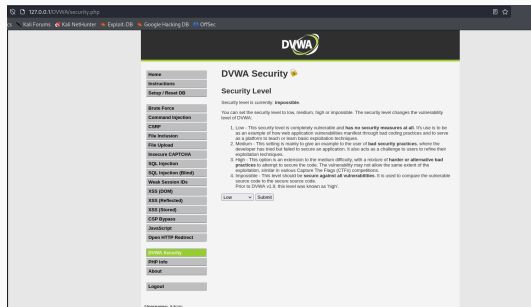
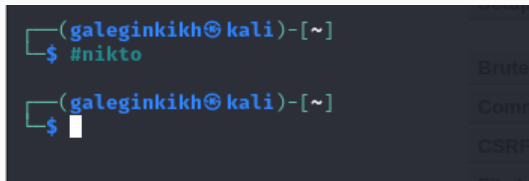


Рис. 2: Уровень безопасности

3. Запустила nikto.



```
(galeginkikh@kali)-[~]  
$ #nikto  
  
(galeginkikh@kali)-[~]  
$
```

The image shows a terminal window with a dark background. The prompt is `(galeginkikh@kali)-[~]`. The user enters `#nikto` on the first line. On the second line, the prompt is shown again with a cursor, indicating the command has been executed. To the right of the terminal, there is a vertical sidebar with buttons labeled `Brute`, `Comm`, and `CSRF`.

Рис. 3: nikto

4. Проверила веб-приложение, введя его URL и не вводя порт.

```
galeginkhh@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: 2024-09-23 12:34:51 (GMT3)

+ Server: Apache/2.4.59 (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.
```

Рис. 4: Через URL

5. Теперь попробовала просканировать введя адрес хоста и адрес порта. Результат немного отличается.

```
[galegashhh@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:     | 2024-09-23 12:38:38 (GMT3) |
+-----+-----+

+ Server: Apache/2.4.59 (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: 621c09e5b7937, mtime: grip. See: http://cve.mitr.org/cgi-bin/cvname.cgi?name=CVE-2003-1410
+ 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 allow d 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.
+ /assets/modirise/css/meta.php?filesrc=/etc/passwd: A PHP backdoor file manager was found.
+ /login.cgi?cli=na200&as2?cat&X0/etc/passwd: Some D-Link router remote command execution.
+ /shell?cat=/etc/passwd: A backdoor was identified.
+ 8074 requests: 0 error(s) and 15 item(s) reported on remote host
+ End Time:      2024-09-23 12:38:57 (GMT3) (19 seconds)

+ 1 host(s) tested
```

Рис. 5: Через адрес хоста и адрес порта

Кроме адреса хоста и адреса порта веб-приложение выводит информацию о различных уязвимостях.

Вывод

Научилась использовать сканер nikto для тестирования веб-приложений.