

# Индивидуальный проект. Этап 4

## Основы информационной безопасности

---

Жибицкая Е.Д.

Российский университет дружбы народов, Москва, Россия

Цель

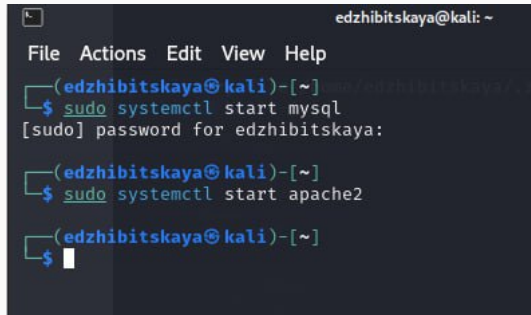
---

- Продолжение выполнения проекта. Освоение приложения nikto

## Ход работы

---

Запускаем сервер и работу DVWA - включаем  
mysql и apache2



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

Рис. 1: Запуск DVWA

Входим в систему, переходим в раздел Security и для удобства устанавливаем уровень low. Это не обязательно, но все равно сделаем.

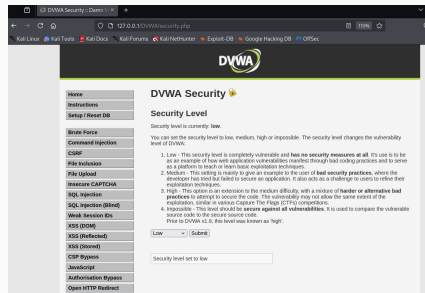


Рис. 2: DVWA Security

```
(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 (0x0d) as a request spacer
```

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. 3: Справка о nikto

```
(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: 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/passwd: 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/passwd: A PHP backdoor file manager was found.  
/DVWA/wordpress/wp-content/themes/twentyeleven/images/headers/server.php?filesrc=/etc/passwd: A PHP backdoor file manager was found.  
/DVWA/wp-includes/Requests/Utility/content-post.php?filesrc=/etc/passwd: A PHP backdoor file manager was found.  
/DVWA/wordpress/wp-includes/Requests/Utility/content-post.php?filesrc=/etc/passwd: A PHP backdoor file manager was found.  
/DVWA/wp-includes/js/tinymce/themes/modern/Meuhy.php?filesrc=/etc/passwd: A PHP backdoor file manager was found.  
/DVWA/wordpress/wp-includes/js/tinymce/themes/modern/Meuhy.php?filesrc=/etc/passwd: A PHP backdoor file manager was found.  
/DVWA/assets/mobirise/css/meta.php?filesrc=/etc/passwd: A PHP backdoor file manager was found.
```

Рис. 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 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: 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 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/hosts: 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 backdoor 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 backdoor file manager was found.
+ /wordpress/wp-includes/js/tinymce/themes/modern/Meuhy.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /assets/mobirise/css/meta.php?filesrc=: A PHP backdoor file manager was found.
+ /login.cgi?cli-aa%20aa%27cat%20/etc/hosts: Some D-Link router remote command 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. 5: Анализ по имени хоста и порту

## Выводы

---

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