

Индивидуальный проект. Этап 4.

Основы информационной безопасности

Тойчубеква А.Н.

02 май 2025

Российский университет дружбы народов, Москва, Россия

Информация

- Тойчубекова Асель Нурлановна
- Студент 2 курса
- факультет физико-математических и естественных наук
- Российский университет дружбы народов
- 1032235033@rudn.ru

Целью данного этапа индивидуального проекта является познакомиться с программой nikto и получение практических навыков работы с ней.

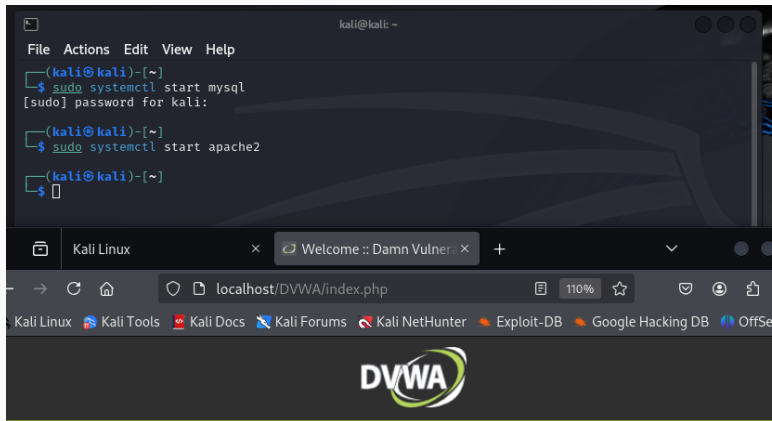
nikto — базовый сканер безопасности веб-сервера. Он сканирует и обнаруживает уязвимости в веб-приложениях, обычно вызванные неправильной конфигурацией на самом сервере, файлами, установленными по умолчанию, и небезопасными файлами, а также устаревшими серверными приложениями. Среди функций Nikto можно выделить следующие:

- поддержка SSL,
- поддержка HTTP прокси;
- создание отчетов в текстовом формате, XML, HTML, NBE или CSV;
- возможность сканирования портов;
- поиск поддоменов;
- поддержка плагинов для расширения функционала сканирования.

Выполнение лабораторной работы

Выполнение лабораторной работы

Мы будем выявлять уязвимости в нашем веб-сайте DVWA, из-за чего нам нужно для начала его запустить.



The image shows a Kali Linux terminal window and a web browser. The terminal window, titled 'kali@kali: ~', has a menu bar with 'File', 'Actions', 'Edit', 'View', and 'Help'. It shows the following commands and output:

```
(kali@kali)-[~]  
$ sudo systemctl start mysql  
[sudo] password for kali:  
  
(kali@kali)-[~]  
$ sudo systemctl start apache2  
  
(kali@kali)-[~]  
$
```

The web browser window, titled 'Welcome :: Damn Vulnerable Web Application', shows the URL 'localhost/DVWA/index.php' and a zoom level of 110%. The browser's address bar includes links to 'Kali Linux', 'Kali Tools', 'Kali Docs', 'Kali Forums', 'Kali NetHunter', 'Exploit-DB', 'Google Hacking DB', and 'OffSec'. The main content area displays the DVWA logo, which consists of the letters 'DVWA' in a bold, sans-serif font, with a green and yellow circular graphic element to the right.

Welcome to Damn Vulnerable Web Application

Damn Vulnerable Web Application (DVWA) is a PHP/MySQL web application that is damn vulnerable

Теперь запускаем программу `nikto` командой `#nikto`. Далее чтобы запустить сканер прописываем команду `nikto -h доменное_имя или IP_адрес`. Параметр `-h` обязателен к использованию, иначе программа не сможет запустить сканирование. Мы видим, что спустя некоторое время на экране появилась некоторая информация.

Выполнение лабораторной работы

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

(kali@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: 2025-05-02 03:20:56 (GMT-4)

+ 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: HEAD, GET, POST, OPTIONS.
+ /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/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/hosts: A PHP backdoor f
+ /DVWA/wordpress/wp-content/themes/twentyeleven/images/headers/server.php?filesrc=/etc/hosts: A PHP
found.
+ /DVWA/wp-includes/Requests/Utility/content-post.php?filesrc=/etc/hosts: A PHP backdoor file manager
+ /DVWA/wordpress/wp-includes/Requests/Utility/content-post.php?filesrc=/etc/hosts: A PHP backdoor fi
+ /DVWA/wp-includes/js/tinymce/themes/modern/Meuhy.php?filesrc=/etc/hosts: A PHP backdoor file manage
+ /DVWA/wordpress/wp-includes/js/tinymce/themes/modern/Meuhy.php?filesrc=/etc/hosts: A PHP backdoor f
+ /DVWA/assets/mobirise/css/meta.php?filesrc=: A PHP backdoor file manager was found.
+ /DVWA/login.cgi?cli-aa%20aa%27cat%20/etc/hosts: Some D-Link router remote command execution.
+ /DVWA/shell?cat=/etc/hosts: A backdoor was identified.
+ /DVWA/.dockerignore: .dockerignore file found. It may be possible to grasp the directory structure
site.
+ 8074 requests: 0 error(s) and 26 item(s) reported on remote host
+ End Time: 2025-05-02 03:21:25 (GMT-4) (29 seconds)

+ 1 host(s) tested
```

В начале сканирования всегда отображается следующий блок с информацией:

- Target IP: IP адрес сканируемого домена.
- Target Hostname: имя хоста (доменное имя) сканируемого сайта;
- Target Port: порт, на котором находится сайт;
- Start Time: дата и время начала сканирования в формате год-месяц-день час:минута:секунда.

Далее идет анализ самого веб-сайта:

- +Server: Apache/2.4.62 (Debian)- Обнаружен веб-сервер Apache версии 2.4.62, установленный на Debian.
- +/DVWA/: The anti-clickjacking X-Frame-Options header is not present.- На странице /DVWA/ отсутствует заголовок X-Frame-Options, из-за чего сайт уязвим к clickjacking — подмене интерфейса с помощью фреймов.
- +/DVWA/: The X-Content-Type-Options header is not set.- Отсутствует заголовок X-Content-Type-Options, что может привести к MIME-sniffing атакам — когда браузер сам определяет тип контента и ошибается.
- +Root page /DVWA redirects to: login.php - Главная страница /DVWA перенаправляет на login.php — это просто уведомление, не уязвимость.

Выполнение лабораторной работы

- +No CGI Directories found (use '-C all' to force check all possible dirs)- CGI-директории не найдены. CGI — устаревшая технология запуска скриптов, иногда содержит уязвимости.
- +OPTIONS: Allowed HTTP Methods: HEAD, GET, POST, OPTIONS .- Сервер разрешает перечисленные HTTP-методы. Это стандартно, но расширенные методы могут быть точкой атаки.
- +/DVWA///etc/hosts: The server install allows reading of any system file...- Критическая уязвимость: при добавлении лишнего / можно прочитать файлы системы — тут файл /etc/hosts.
- +/DVWA/config/: Directory indexing found.- Включена индексация директорий — можно видеть все файлы в /DVWA/config/.

- `+/DVWA/config/`: Configuration information may be available remotely.- Конфигурационные файлы могут быть доступны через интернет — опасность утечки данных.
- `+/DVWA/tests/`: Directory indexing found. , + `/DVWA/tests/`: This might be interesting.- В папке `/tests/` можно увидеть файлы — возможно, есть скрипты, пригодные для атаки.
- `+/DVWA/database/`: Directory indexing found., + `/DVWA/database/`: Database directory found.- Доступна директория базы данных — возможно, можно скачать файлы с настоящими данными.
- `+/DVWA/docs/`: Directory indexing found.- Папка с документацией доступна — это не критично, но может раскрыть структуру проекта.

- `+/DVWA/login.php`: Admin login page/section found.- Найдена страница входа администратора. Это может быть целью для brute force-атак.
- `+/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. -Сайт случайно открывает файлы git-репозитория. Через них можно восстановить весь проект, включая секреты и конфигурации.

- `+/DVWA/wp-content/themes/.../server.php?filesrc=/etc/hosts`: A PHP backdoor file manager was found. ...- Найдено множество PHP backdoor скриптов — это вредоносные файлы, которые дают удалённый доступ к файлам, например, позволяют просматривать `/etc/hosts`. Каждый найденный путь — это отдельный путь к backdoor'у.
- `+/DVWA/login.cgi?cli=aa%20aa%27cat%20/etc/hosts`: Some D-Link router remote command execution. `+/DVWA/shell?cat+/etc/hosts`: A backdoor was identified.- Эти запросы указывают на удалённое выполнение команд на сервере — одна из самых опасных уязвимостей.
- `+/DVWA/.dockerignore`: `.dockerignore` file found...- Файл `.dockerignore` доступен — может раскрыть, какие файлы исключаются из Docker-сборки.

И затем описывается заключение:

- +8074 requests: 0 error(s) and 26 item(s) reported on remote host - Сделано 8074 HTTP-запроса, ошибок не было. Найдено 26 значимых элементов.
- +End Time: 2025-05-02 03:21:25 (GMT-4) (29 seconds)-Время окончания сканирования. Общее время — 29 секунд.

А теперь попробуем вызвать программу nikto указав адрес хоста и порта. Мы видим, что выводится информация, которая незначительно отличается от предыдущей.

Выполнение лабораторной работы

```
(kali@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: 2025-05-02 03:24:34 (GMT-4)

+ 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: 628208420f1c0, mtime: gzip. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ OPTIONS: Allowed HTTP Methods: HEAD, GET, POST, OPTIONS
+ ///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 config 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: 2025-05-02 03:25:04 (GMT-4) (30 seconds)
```

Оба вывода — это результаты сканирования веб-сервера с помощью Nikto, но они отличаются целевыми путями и глубиной анализа, а также количеством найденных потенциальных уязвимостей. Давай по порядку.

Первый скан (`nikto -h http://127.0.0.1/DVWA/`) явно указывает путь `/DVWA/`, то есть Nikto начинает сканирование внутри каталога уязвимого приложения DVWA (Damn Vulnerable Web Application). В результате он находит больше конкретных директорий, таких как `/DVWA/config/`, `/DVWA/tests/`, `/DVWA/database/`, `/DVWA/docs/`, а также `.git`-файлы и даже PHP-бэkdоры.

Второй скан (`nikto -h 127.0.0.1 -p 80`) запускается на корень сайта (`/`). В этом случае он не заходит глубоко в подкаталоги (вроде `/DVWA`), если их не перенаправляет туда сервер. Поэтому он находит только общие уязвимости, характерные для сервера в целом: отсутствие заголовков безопасности, ETag-информацию, открытый `/server-status` и наличие некоторых PHP-бэкдоров, если они лежат прямо в корне или стандартных путях.

В ходе выполнения 4 этапа индивидуального проекта я получила практические навыки работы с программой, выявления уязвимостей веб-сайтов, nikto.