

Презентация по 5-ому этапу индивидуального проекта

Основы информационной безопасности

Бережной И. А.

Российский университет дружбы народов, Москва, Россия

Информация

- Бережной Иван Александрович
- студент 2-ого курса
- Российский университет дружбы народов
- 1132236041@pfur.ru

Научиться тестировать веб-приложения с помощью сканера nikto

Использовать nikto на DVWA

Nikto – бесплатный сканер для поиска уязвимостей в веб-серверах. Утилита относится к классу blackbox сканеров, т. е. сканеров, использующих стратегию сканирования методом черного ящика. Это значит, что заранее неизвестно о внутреннем устройстве программы/сайта (доступ к исходному коду отсутствует) и упор сделан на функциональность. Программа может обнаруживать более 6700 потенциально опасных файлов и уязвимостей. Новые уязвимости добавляются в базу данных программы по мере их возникновения. Помимо поиска уязвимостей, сканер производит поиск на наличие устаревших версий, используемых библиотек и фреймворков. Nikto не позиционируется как стелс сканер (стелс сканеры никогда не устанавливают TCP-соединения до конца, тем самым сканирование происходит скрытно) – при сканировании сайта в логах сайта или в любой другой системе обнаружения вторжений, если она используется, будет отображена информация о том, что сайт подвергается сканированию.

Выполнение задания

Для начала запустим зависимости, а затем и сам DVWA.

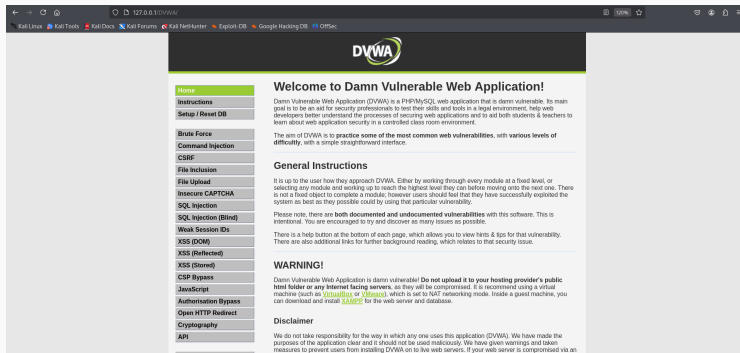


Рис. 1: Запуск mysql и apache

Выполнение задания

Теперь запустим nikto следующей командой: `nikto -h http://127.0.0.1/DVWA/`

```
iaberezhnoy@iaberezhnoy:~$ 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:     2025-05-03 19:10:11 (GMT3)

+ Server: Apache/2.4.63 (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.
+ /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 file manager was found.
+ /DVWA/wordpress/wp-content/themes/twentyeleven/images/headers/server.php?filesrc=/etc/hosts: A PHP backdoor file manager 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 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 was found.
+ /DVWA/login.cgi?cli=aaK20aaX27catX20/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 and learn more about the site.
+ 8074 requests: 0 error(s) and 26 item(s) reported on remote host
+ End Time:      2025-05-03 19:10:34 (GMT3) (23 seconds)

+ 1 host(s) tested
```

Рис. 3: Использование nikto

Из вывода в терминале можем заключить следующее:

Отчёт Nikto выявил несколько уязвимостей и проблем безопасности в DVWA.

1. Обнаружены несколько PHP-скриптов, позволяющих управлять файлами на сервере:
 - /DVWA/wp-content/themes/twent/vector/images/headers/server.php?filesrc=/etc/hosts.
 - /DVWA/login.cgi?cli=a&z9aaxZ7catX20/etc/hosts (возможна RCE для D-Link роутеров).
 - /DVWA/shell?cat+/etc/hosts (подозрительный бэкдор).
2. Отсутствуют заголовки безопасности:
 - Нет X-Frame-Options (риск clickjacking).
 - Нет X-Content-Type-Options (возможна подмена MIME-типов).
3. Доступны директории с конфигурационными данными: /DVWAconfig/, /DVWA/database/, /DVWA/tests/ (индексация включена).

В ходе выполнения этапа проекта мы попрактиковались в использовании инструмента Hydra для брутфорса паролей DVWA.