

Индивидуальный проект - Этап 4

Основы информационной безопасности

Чистов Д. М.

03 мая 2025

Российский университет дружбы народов, Москва, Россия

Объединённый институт ядерных исследований, Дубна, Россия

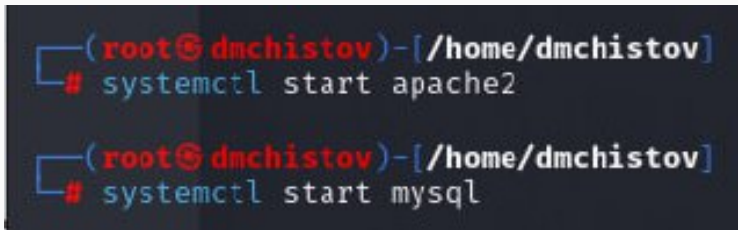
Цель работы

Получение навыков пользования nikto.

nikto - это базовый сканнер веб-приложений на уязвимости серверного уровня, т.е. ищет уязвимые файлы, скрипты, делает HTTP-запросы.

Выполнение лабораторной работы

Перед работой надо запустить apache2 и mysql, буду тестировать nikto на dvwa.

A terminal window with a dark background. The prompt is (root@dmchistov)-[/home/dmchistov]. The first command entered is # systemctl start apache2. The second command entered is # systemctl start mysql.

```
(root@dmchistov)-[/home/dmchistov]  
# systemctl start apache2  
  
(root@dmchistov)-[/home/dmchistov]  
# systemctl start mysql
```

Рис. 1: Запуск сервисов для DVWA

В начале работы я думал протестировать dvwa на разных уровнях защиты, однако оказалось это бесполезно, ведь никто проверяет веб-приложения на уязвимости другого типа, а DVWA выставляет уровни защиты, которые проявляются в логике работы самого веб-приложения, а не его серверную структуру.

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

Пишем команду

```
nikto -h http://127.0.0.1/dvwa
```

Здесь -h - задаём хоста (кого будем анализировать), и дальше идёт URL нашего хоста. Также можно написать -o (имя) и после этого -F (формат) и это отправит результаты нашего сканирования в файл, чьё имя и формат мы сами задали

Выполнение лабораторной работы

Команда вывела следующее:

```
(dmchistov@dmchistov) [~]
$ 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 20:28:37 (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/
+ 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/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.
+ /dvwa/login.cgi?cli=aa%20aa%27cat%20/etc/passwd: Some D-Link router remote command execution.
+ /dvwa/shell?cat=/etc/passwd: A backdoor was identified.
+ 8073 requests: 0 error(s) and 13 item(s) reported on remote host
+ End Time: 2025-05-03 20:29:05 (GMT3) (28 seconds)

+ 1 host(s) tested
```

Здесь есть на что обратить внимание:

1. Можно узнать версию Apache, а это может помочь хакеру найти уязвимости, если уже известны уязвимости для этой версии
2. X-Frame-Options — отсутствие защиты от clickjacking (встраивание сайта в чужого сайта - т.е. так ввести в сайт свой функционал, который может принести вред пользователю)
3. X-Content-Type-Options — отсутствие от MIME-атаки (когда браузер может неадекватно интерпретировать тип файла, например подали серверу файл txt, содержащий вредоносный код, а веб-приложение этот файл проинтерпретирует как раз как нам надо и этот код запустит.)
4. Nikto отправляет запросы к разным путям, подставляя ?filesrc=/etc/hosts и сервер возвращает содержимое файла hosts. Т.е. получается можно просматривать любые файлы. Такие скрипты часто называются “file manager backdoors”

Выводы

При выполнении данной работы я успешно получил навыки работы с nikto.

Список литературы

Индивидуальный проект

Краткое введение в nikto (видео на английском)