report

# Отчет по 4 этапу проекта "Использование nikto."

## Подъярова Ксения Витальевна

# Цель работы

Научиться тестированию веб-приложений с помощью сканера nikto.

# Выполнение лабораторной работы

1. Чтобы работать с nikto, необходимо подготовить веб-приложение, которое будем сканировать. Это будет DVWA. Для этого запустила apache2. (рис. 1)  
   Pasted image 20241005135219.png
2. Ввожу в адресной строке браузера адрес DVWA, перехожу в режим выбора уровня безопасности, ставлю минимальный (необязательно, nikto при обычном сканировании для режима impossible и low выдаст одинаковые потенциальные уязвимости, что логично, ведь они остаются, но изменяется сложность, с которой их можно использовать) (рис. 2)  
   Pasted image 20241005135125.png
3. Запускаю nikto (рис. 3)  
   Pasted image 20241005135255.png
4. Проверить веб-приложение можно, введя его полный URL и не вводя порт, попробовала просканировать так (рис. 4)  
   Pasted image 20241005135501.png  
   Pasted image 20241005135555.png
5. Затем попробовала просканировать введя адрес хоста и адрес порта, результаты незначительно отличаются (рис. 5)  
   Pasted image 20241005135740.png

# Анализ результатов сканирования

Кроме адреса хоста и порта веб-приложения, никто выводит информацию о различных уязвимостях приложения:  
Сервер: Apache/2.4.58 (Debian) + /DVWA/: Заголовок X-Frame-Options, защищающий от перехвата кликов, отсутствует. Смотрите: [https://developer.mozilla.org/enUS/docs/Web/HTTP/Headers/X-Frame-Options](https://developer.mozilla.org/en%02US/docs/Web/HTTP/Headers/X-Frame-Options)

• /DVWA/: Заголовок X-Content-Type-Options не задан. Это может позволить пользовательскому агенту отображать содержимое сайта способом, отличным от MIME-типа. Смотрите: [https://www.netsparker.com/webvulnerability-scanner/vulnerabilities/missing-content-type-header/](https://www.netsparker.com/web%02vulnerability-scanner/vulnerabilities/missing-content-type-header/)  
• Корневая страница /DVWA перенаправляет на: login.php  
• Каталоги CGI не найдены (используйте ‘-C all’, чтобы принудительно проверить все возможные каталоги)  
• ОПЦИИ: Разрешенные HTTP-методы: GET, POST, OPTIONS, HEAD .  
• /DVWA///etc/hosts: Установка сервера позволяет считывать любой системный файл, добавляя дополнительный “/” к URL-адресу.  
• /DVWA/config/: Найдена индексация каталога.  
• /DVWA/config/: Информация о конфигурации может быть доступна удаленно.  
• /DVWA/tests/: Найдена индексация каталога.  
• /DVWA/tests/: Это может быть интересно.  
• /DVWA/database/: Найдена индексация каталога.  
• /DVWA/база данных/: Найден каталог базы данных.  
• /DVWA/документы/: Найдена индексация каталога.  
• /DVWA/login.php: Найдена страница входа администратора/раздел.  
• /DVWA/.git/index: Индексный файл Git может содержать информацию о списке каталогов.  
• /DVWA/.git/HEAD: Найден файл Git HEAD. Может содержаться полная информация о репозитории.  
• /DVWA/.git/config: Найден конфигурационный файл Git. Может содержаться информация о деталях репозитория.  
• /DVWA/.gitignore: найден файл .gitignore. Можно разобраться в структуре каталогов.  
• /DVWA/wp-content/themes/twentyeleven/images/headers/server.php?filesrc=/etc/hosts: Обнаружен файловый менеджер с бэкдором на PHP.  
• /DVWA/wordpress/wp-content/themes/twentyeleven/images/headers/server.php?filesrc=/etc/hosts: Обнаружен файловый менеджер с бэкдором на PHP.  
• /DVWA/wp-includes/Requests/Utility/content-post.php?filesrc=/etc/hosts: Найден файловый менеджер с бэкдором на PHP.  
• /DVWA/wordpress/wp-includes/Requests/Utility/content-post.php?filesrc=/etc/hosts: Найден файловый менеджер с бэкдором на PHP.  
• /DVWA/wp-включает в себя/js/tinymce/themes/modern/Meuhy.php?filesrc=/etc/hosts: Найден файловый менеджер бэкдора PHP.  
• /DVWA/wordpress/wp-включает в себя/js/tinymce/themes/modern/Meuhy.php?filesrc=/etc/hosts: Найден файловый менеджер бэкдора на PHP.  
• /DVWA/assets/mobirise/css/meta.php?filesrc=: Найден файловый менеджер бэкдора на PHP.  
• /DVWA/login.cgi?cli=aa%20aa%27cat%20/etc/hosts: Удаленное выполнение какой-либо команды маршрутизатором D-Link.  
• /DVWA/shell?cat+/etc/hosts: Обнаружен черный ход.  
• /DVWA/.dockerignore: найден файл .dockerignore. Возможно, удастся разобраться в структуре каталогов и узнать больше о сайте.

Бэкдор, тайный вход (от англ. back door — «чёрный ход», «лазейка», буквально «задняя дверь») — дефект алгоритма, который намеренно встраивается в него разработчиком и позволяет получить несанкционированный доступ к данным или удалённому управлению операционной системой и компьютером в целом.

Также в результатах nikto отображает код OSVDB 561 и дает ссылку на CVE2003-1418. OSVDB — это аббревиатура базы данных уязвимостей с открытым исходным кодом.

CVE-2003-1418 — это уязвимость в Apache HTTP Server 1.3.22–1.3.27 на OpenBSD, которая позволяет удалённым злоумышленникам получать конфиденциальную информацию через:  
• Заголовок ETag, который раскрывает номер вode.  
• Многочастную границу MIME, которая раскрывает идентификаторы дочерних процессов (PID).

В настоящее время эта проблема имеет среднюю степень тяжести

# Выводы

Научилась использовать сканер nikto для тестирования веб-приложений.