

Четвертый этап индивидуального проекта

Использование nikto

Беличева Дарья Михайловна

Содержание

1	Цель работы	4
2	Теоретическое введение	5
3	Выполнение лабораторной работы	6
4	Выводы	9
	Список литературы	10

Список иллюстраций

3.1	Запуск mysql и apache2	6
3.2	Страница DVWA	6
3.3	Проверка наличия nikto	7
3.4	Проверка уязвимостей по доменному имени	7
3.5	Отчет об уязвимостях в формате htm	8
3.6	Проверка уязвимостей с указанием порта	8

1 Цель работы

Целью данной работы является использование Nikto для сканирования уязвимостей веб-приложения.

2 Теоретическое введение

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.

В начале сканирования всегда отображается следующий блок с информацией[1]:

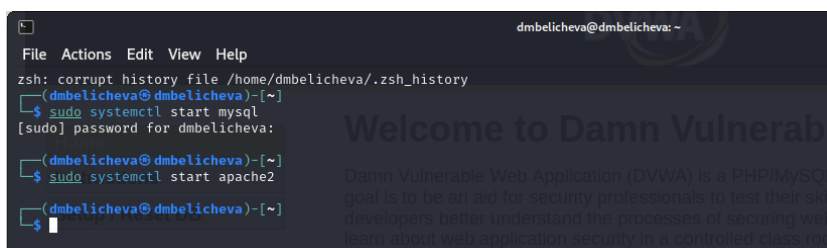
- Target IP: IP адрес сканируемого домена;
- Target Hostname: имя хоста (доменное имя) сканируемого сайта;
- Target Port: порт, на котором находится сайт;
- Start Time: дата и время начала сканирования в формате год-месяц-день час:минута:секунда.

Вывод результатов сканирования имеет несколько форматов:

1. Формат: Тип компонента сайта: Наименование компонента. Пример:
Server: nginx.
2. Описание: Nikto умеет определять, какие компоненты использует сайт. Сюда относят наименование веб-сервера, используемой СУБД, фреймворков, языков программирования, а также их версии. Формат: путь до файла/директории, где найдена уязвимость: описание уязвимости. Пример: /phpinfo.php: Output from the phpinfo() function was found.

3 Выполнение лабораторной работы

Будем проверять работу nikto на веб-приложении DVWA. Для этого запустим mysql и apache2 (рис. 3.1).



```
dmbelicheva@dmbelicheva: ~  
File Actions Edit View Help  
zsh: corrupt history file /home/dmbelicheva/.zsh_history  
(dmbelicheva@dmbelicheva)-[~]  
$ sudo systemctl start mysql  
[sudo] password for dmbelicheva:  
(dmbelicheva@dmbelicheva)-[~]  
$ sudo systemctl start apache2  
(dmbelicheva@dmbelicheva)-[~]  
$
```

Рис. 3.1: Запуск mysql и apache2

Теперь можем в адресной строке открыть DVWA (рис. 3.2).

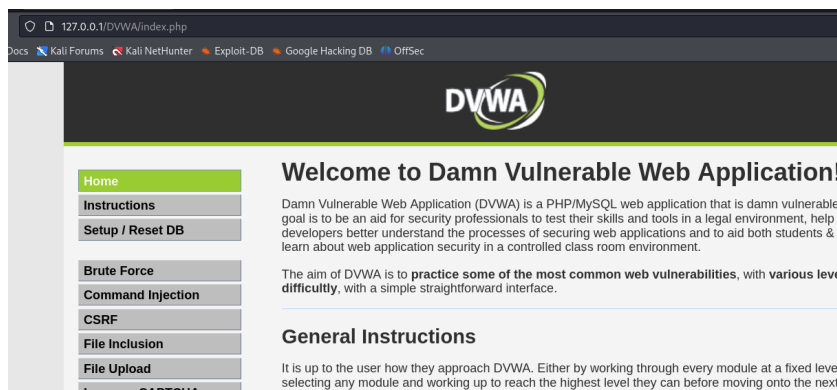


Рис. 3.2: Страница DVWA

Теперь проверим, что nikto установлен (рис. 3.3).

```
(dmbelicheva@dmbelicheva)-[~]
$ nikto
- Nikto v2.5.0

+ ERROR: No host (-host) specified

Options:
  -ask+          Whether to ask about submitting updates
                  yes   Ask about each (default)
  File Upload    no    Don't ask, don't send
                  auto  Don't ask, just send
  In-check6 CAPTCHA Check if IPv6 is working (connects to ipv6.google.com or
  -Cgidirs+      Scan these CGI dirs: "none", "all", or values like "/cg
  -config+       Use this config file
  -Display+      Turn on/off display outputs:
                  1     Show redirects
```

Рис. 3.3: Проверка наличия nikto

Теперь можем проверить сайт DVWA. Минимальный синтаксис для запуска сканирования выглядит следующим образом:

```
nikto -h доменное_имя или IP_адрес
```

Параметр -h обязателен к использованию, иначе программа не сможет запустить сканирование (рис. 3.4). Чтобы получить отчет в удобном формате, можно использовать опцию Format. Я указала формат html.

```
(dmbelicheva@dmbelicheva)-[~]
$ nikto -h http://127.0.0.1/DVWA -o report.html -Format htm
- Nikto v2.5.0

+ Target IP: 127.0.0.1
+ Target Hostname: 127.0.0.1
+ Target Port: 80
+ Start Time: 2024-10-05 21:32:55 (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/
+ /DVWA/: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of
ee: 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.
```

Рис. 3.4: Проверка уязвимостей по доменному имени

Получаем следующий отчет (рис. 3.5).

127.0.0.1 / 127.0.0.1 port 80	
Target IP	127.0.0.1
Target hostname	127.0.0.1
Target Port	80
HTTP Server	Apache/2.4.62 (Debian)
Site Link (Name)	http://127.0.0.1:80/DVWA/
Site Link (IP)	http://127.0.0.1:80/DVWA/
URI	/DVWA/
HTTP Method	GET
Description	/DVWA/: The anti-clickjacking X-Frame-Options header is not present.
Test Links	http://127.0.0.1:80/DVWA/ http://127.0.0.1:80/DVWA/
References	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
URI	/DVWA/
HTTP Method	GET
Description	/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 fa
Test Links	http://127.0.0.1:80/DVWA/ http://127.0.0.1:80/DVWA/
References	https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
URI	/DVWA/
HTTP Method	OPTIONS
Description	OPTIONS: Allowed HTTP Methods: HEAD, GET, POST, OPTIONS

Рис. 3.5: Отчет об уязвимостях в формате html

Можем увидеть, что найдены такие уязвимости как отсутствие защиты от кликджекинга, не установлен заголовок X-Content-Type-Options(в связи с чем пользователь может выполнить вредоносный контент не того типа, который предполагает администратор), возможность удаленного доступа к файлам конфигураций, также найдена скрытая папка git, в которой хранятся данные о структуре сайта. Уязвимость типа This might be interesting... означает, что необходимо дополнительная ручная проверка(скорей всего это незначительная уязвимость раскрытия информации – доступен просмотр файлов каталога). В конце отчета указано, что найдено 26 уязвимостей.

Также можно посмотреть информацию об уязвимостях по конкретному порту (в нашем случае порт 80 для локального хоста) (рис. 3.6).

```
(dmbelicheva@dmbelicheva)-[~]
$ 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: 2024-10-05 21:42:29 (GMT3)

+ Server: Apache/2.4.62 (Debian)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of
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: 6221461e4bd3, mtime: g
VE-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 conf file or
+ /wp-content/themes/twentyeleven/images/headers/server.php?filesrc=/etc/hosts: A PHP backdoor file manager
+ /wordpress/wp-content/themes/twentyeleven/images/headers/server.php?filesrc=/etc/hosts: A PHP backdoor fi
+ /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
+ /wp-includes/is/innocent/themes/modern/Meuhv.php?filesrc=/etc/hosts: A PHP backdoor file manager was found
```

Рис. 3.6: Проверка уязвимостей с указанием порта

4 Выводы

В результате выполнения работы был использован сканер Nikto для сканирования уязвимостей веб-приложения.

Список литературы

1. Обзор сканера Nikto для поиска уязвимостей в веб-серверах [Электронный ресурс]. 2023. URL: <https://habr.com/ru/companies/first/articles/731696/>.