

Основы информационной безопасности

Индивидуальный проект. Этап № 4. Использование Nikto

Сунгурова Мариян М.

Российский университет дружбы народов, Москва, Россия

Информация

- Сунгурова М.М.
- Российский университет дружбы народов

Вводная часть

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

Damn Vulnerable Web Application (DVWA) – это веб-приложение PHP/MySQL, которое чертовски уязвимо. Его основная цель – помочь специалистам по безопасности проверить свои навыки и инструменты в правовой среде, помочь веб-разработчикам лучше понять процессы обеспечения безопасности веб-приложений, а также помочь студентам и преподавателям узнать о безопасности веб-приложений в контролируемом классе. обстановка помещения.

Цель DVWA – отработать некоторые из наиболее распространенных веб-уязвимостей различного уровня сложности с помощью простого и понятного интерфейса. В этом программном обеспечении существуют как задокументированные, так и недокументированные уязвимости.

DVWA имеет три уровня безопасности, они меняют уровень безопасности каждого веб приложения в DVWA:

- Невозможный — этот уровень должен быть безопасным от всех уязвимостей. Он используется для сравнения уязвимого исходного кода с безопасным исходным кодом.
- Высокий — это расширение среднего уровня сложности, со смесью более сложных или альтернативных плохих практик в попытке обезопасить код. Уязвимости не позволяют такой простор эксплуатации как на других уровнях.
- Средний — этот уровень безопасности предназначен главным образом для того, чтобы дать пользователю пример плохих практик безопасности, где разработчик попытался сделать приложение безопасным, но потерпел неудачу.
- Низкий — этот уровень безопасности совершенно уязвим и совсем не имеет защиты. Его предназначение быть примером среди уязвимых веб приложений, примером плохих практик программирования и служить платформой обучения базовым техникам эксплуатации

Nikto – бесплатный (open source) сканер для поиска уязвимостей в веб-серверах.

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.

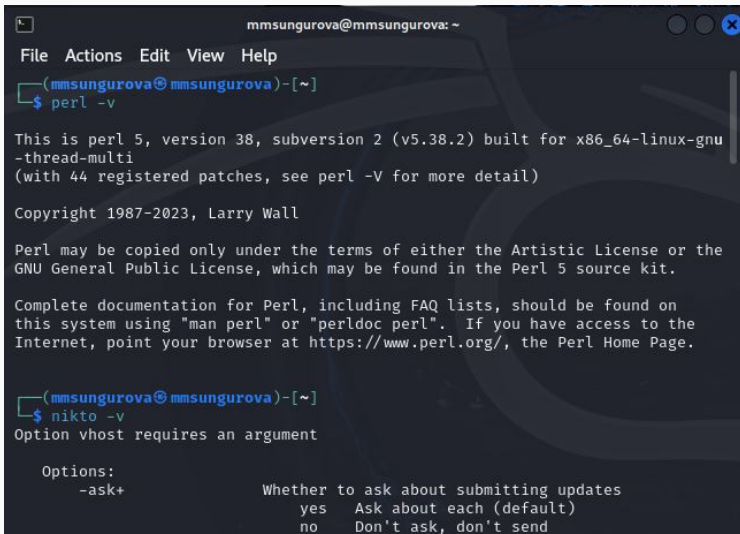
Вывод результатов сканирования имеет несколько форматов:

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.

Выполнение лабораторной работы

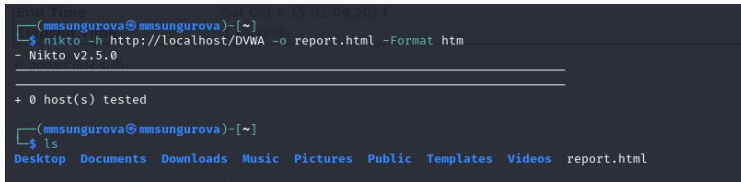
Выполнение лабораторной работы

Проверим, что nikto установлен(рис. (fig:001?))



```
mmsungurova@mmsungurova: ~  
File Actions Edit View Help  
(mmsungurova@mmsungurova)-[~]  
$ perl -v  
  
This is perl 5, version 38, subversion 2 (v5.38.2) built for x86_64-linux-gnu  
-thread-multi  
(with 44 registered patches, see perl -V for more detail)  
  
Copyright 1987-2023, Larry Wall  
  
Perl may be copied only under the terms of either the Artistic License or the  
GNU General Public License, which may be found in the Perl 5 source kit.  
  
Complete documentation for Perl, including FAQ lists, should be found on  
this system using "man perl" or "perldoc perl". If you have access to the  
Internet, point your browser at https://www.perl.org/, the Perl Home Page.  
  
(mmsungurova@mmsungurova)-[~]  
$ nikto -v  
Option vhost requires an argument  
  
Options:  
-ask+          Whether to ask about submitting updates  
                yes   Ask about each (default)  
                no    Don't ask, don't send
```

Затем проверим сайт DVWA, указав опции для сохранения отчета в формате html(рис. (fig:002?),).

A terminal window with a dark background. The prompt is '(mmsungurova@mmsungurova)-[~]'. The command '\$ nikto -h http://localhost/DVWA -o report.html -Format htm' is entered. The output shows 'Nikto v2.5.0' followed by a horizontal line and '+ 0 host(s) tested'. Below this, the prompt is repeated, and the command '\$ ls' is entered. The output of 'ls' is 'Desktop Documents Downloads Music Pictures Public Templates Videos report.html'.

```
(mmsungurova@mmsungurova)-[~]  
$ nikto -h http://localhost/DVWA -o report.html -Format htm  
- Nikto v2.5.0  
+ 0 host(s) tested  
  
(mmsungurova@mmsungurova)-[~]  
$ ls  
Desktop Documents Downloads Music Pictures Public Templates Videos report.html
```

Рис. 2: Проверка уязвимостей по доменному имени

Выполнение лабораторной работы

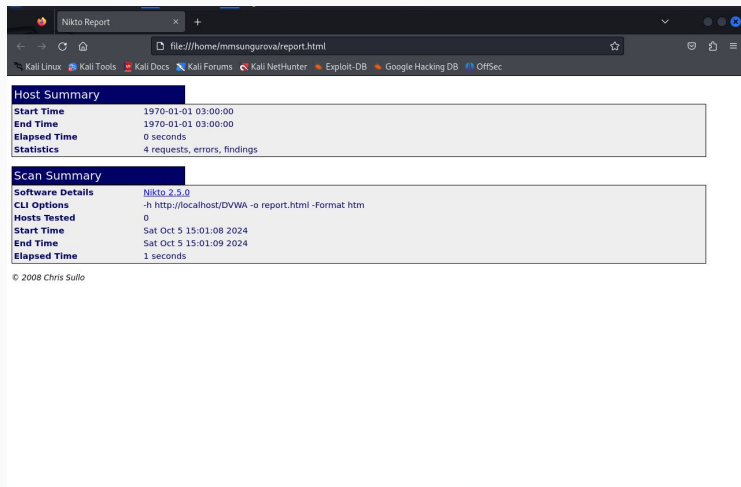
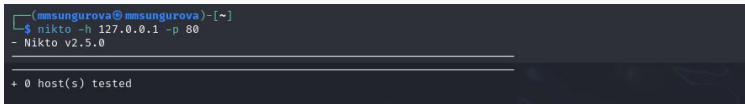


Рис. 3: Отчет об уязвимостях в формате html

Также можно посмотреть информацию об уязвимостях по конкретному порту(в нашем случае порт 80 для локального хоста)(рис. (fig:004?)).

A terminal window with a dark background. The prompt is '(mmsungurova@ mmsungurova)~'. The command '\$ nikto -h 127.0.0.1 -p 80' has been entered. The output shows '- Nikto v2.5.0' followed by a separator line, and then '+ 0 host(s) tested' at the bottom.

```
(mmsungurova@ mmsungurova)~  
$ nikto -h 127.0.0.1 -p 80  
- Nikto v2.5.0  
+ 0 host(s) tested
```

Рис. 4: Проверка уязвимостей с указанием порта

Выводы

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