# Основы информационной безопасности. Индивидуальный проект

## Этап № 4. Использование nikto

Нзита Диатезилуа Катенди

27 сентября 2024 г.

Российский университет дружбы народов, Москва, Россия

# Информация

# Докладчик


- Нзита Диатезилуа Катенди
- студент
- Российский университет дружбы народов
- 1032215220@pfur.ru
- https://github.com/NzitaKatendi

# Вводная часть

# Цели и задачи

**Целью** данной работы является Nikto сканирования уязвимостей веб-приложения.

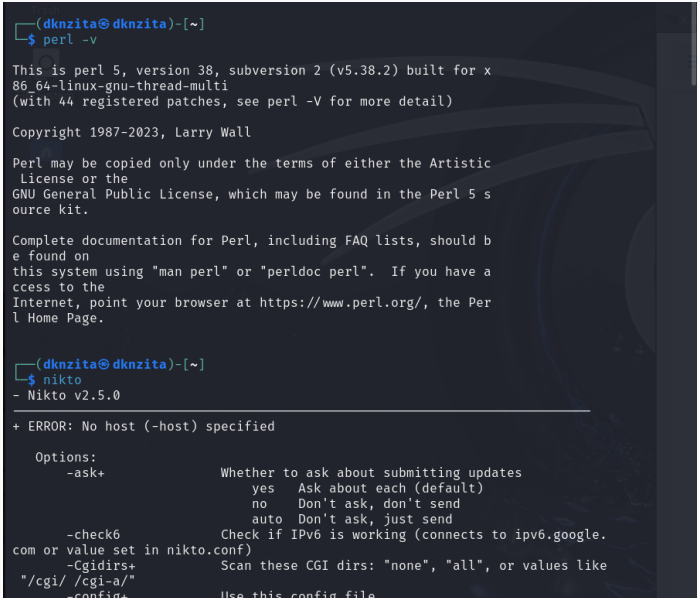
**Задачи:**

- Проанализировать уязвимости веб-приложения DVWA с помощью сканера Nikto.

**Инструмент:** DVWA, Nikto

# Выполнение лабораторной работы

# Установка

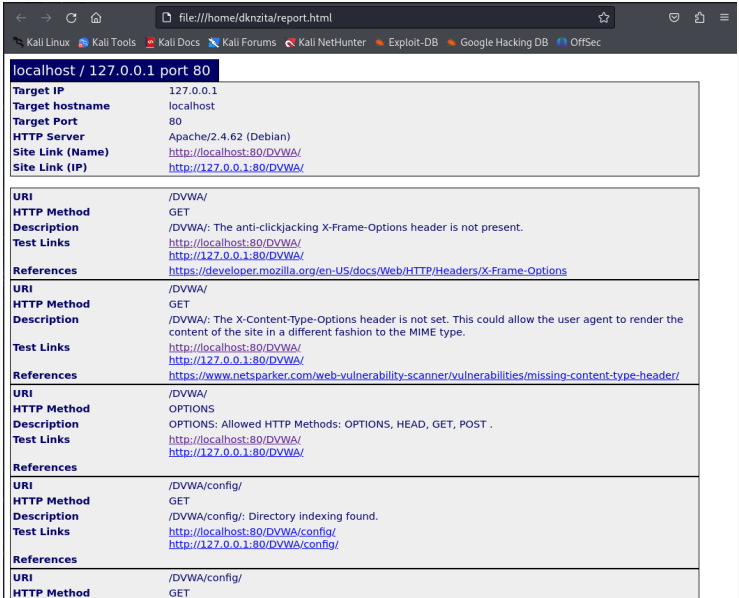

┌──(dknzita㉿dknzita)-[~]
└─$ perl -v
This is perl 5, version 38, subversion 2 (v5.38.2) built for x
86_64-linux-gnu-thread-multi
(with 44 registered patches, see perl -V for more detail)
Copyright 1987-2023, Larry Wall
Perl may be copied only under the terms of either the Artistic
License or the
GNU General Public License, which may be found in the Perl 5 s
ource kit.
Complete documentation for Perl, including FAQ lists, should b
e found on
this system using "man perl" or "perldoc perl". If you have a
ccess to the
Internet, point your browser at https://www.perl.org/, the Per
l Home Page.
┌──(dknzita㉿dknzita)-[~]
└─$ nikto
- Nikto v2.5.0
+ ERROR: No host (-host) specified
Options:
-ask+ Whether to ask about submitting updates
yes Ask about each (default)
no Don't ask, don't send
auto Don't ask, just send
-check6 Check if IPv6 is working (connects to ipv6.google.
com or value set in nikto.conf)
-Cgidirs+ Scan these CGI dirs: "none", "all", or values like
"/cgi/ /cgi-a/"

# Сканирование и анализ

```
┌──(dknzita㉿dknzita)-[~]
└─$ nikto -h http://localhost/DVWA/ -o report.html -Format html
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          127.0.0.1
+ Target Hostname:    localhost
+ Target Port:        80
+ Start Time:         2024-10-02 07:42:22 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.4.62 (Debian)
+ /DVWA/: The anti-clickjacking X-Frame-Options header is not present. See: https://dev
eloper.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-hea
der/
+ Root page /DVWA redirects to: login.php
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ OPTIONS: Allowed HTTP Methods: OPTIONS, HEAD, GET, POST .
+ /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 struct
ure.
+ /DVWA/.dockerignore: .dockerignore file found. It may be possible to grasp the direct
ory structure and learn more about the site.
+ 7850 requests: 0 error(s) and 16 item(s) reported on remote host
+ End Time:           2024-10-02 07:42:35 (GMT-4) (13 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested


      ************************************************************************
```

# Сканирование и анализ



# Сканирование и анализ


Рис. 4: Проверка уязвимостей с указанием порта

# Заключение

# Выводы

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

# Список литературы


1. DVWA [Электронный ресурс]. GitHub, Inc, 2024. URL: https://github.com/digininja/DVWA.
2. Обзор сканера Nikto для поиска уязвимостей в веб-серверах [Электронный ресурс]. 2006–2024, Habr, 2023. URL: https://habr.com/ru/companies/first/articles/731696/.